Vadim Makarov

Quantum cryptography and quantum cryptanalysis

Thesis for the degree doktor ingeniør

Trondheim, March 2007

Norwegian University of Science and Technology
Faculty of Information Technology, Mathematics
and Electrical Engineering
Department of Electronics and Telecommunications

NTNU
Norwegian University of Science and Technology

Thesis for the degree doktor ingeniør

Faculty of Information Technology, Mathematics
and Electrical Engineering
Department of Electronics and Telecommunications

ISBN 978-82-471-1478-0 (printed version)
ISBN 978-82-471-1481-0 (electronic version)
ISSN 1503-8181

Doctoral theses at NTNU, 2007:67

In this electronic version, resolution of large color photographs has been reduced to 300 dpi, in order to reduce file size

This thesis (including full-resolution version), as well as a slide presentation from its defence,
are available electronically on author`s website at
http://www.vad1.com/publications/

Abstract

This doctoral thesis summarizes research in quantum cryptography done at the Department of Electronics and Telecommunications[1] at the Norwegian University of Science and Technology (NTNU) from 1998 through 2007.

The opening parts contain a brief introduction into quantum cryptography as well as an overview of all existing single photon detection techniques for visible and near infrared light. Then, our implementation of a fiber optic quantum key distribution (QKD) system is described. We employ a one-way phase coding scheme with a 1310 nm attenuated laser source and a polarization-maintaining Mach-Zehnder interferometer. A feature of our scheme is that it tracks phase drift in the interferometer at the single photon level instead of employing hardware phase control measures. An optimal phase tracking algorithm has been developed, implemented and tested. Phase tracking accuracy of ±10° is achieved when approximately 200 photon counts are collected in each cycle of adjustment. Another feature of our QKD system is that it uses a single photon detector based on a germanium avalanche photodiode gated at 20 MHz. To make possible this relatively high gating rate, we have developed, implemented and tested an afterpulse blocking technique, when a number of gating pulses is blocked after each registered avalanche. This technique allows to increase the key generation rate nearly proportionally to the increase of the gating rate. QKD has been demonstrated in the laboratory setting with only a very limited success: by the time of the thesis completion we had malfunctioning components in the setup, and the quantum bit error rate remained unstable with its lowest registered value of about 4%.

More than half of the thesis is devoted to various security aspects of QKD. We have studied several attacks that exploit component imperfections and loopholes in optical schemes. In a large pulse attack, settings of modulators inside Alice's and Bob's setups are read out by external interrogating light pulses, without interacting with quantum states and without raising security alarms. An external measurement of phase shift at Alice's phase modulator in our setup has been demonstrated experimentally. In a faked states attack, Eve intercepts Alice's qubits and then utilizes various optical imperfections in Bob's scheme to construct and resend light pulses in such a way that Bob does not distinguish his detection results from normal, whereas they give Bob the basis and bit value chosen at Eve's discretion. Construction of such faked states using several different imperfections is discussed. Also, we sketch a practical workflow of breaking into a running quantum cryptolink for the two abovementioned classes of attacks. A special attention is paid to a common imperfection when sensitivity of Bob's two detectors relative to one another can be controlled by Eve via an external parameter, for example via the timing of the incoming pulse. This imperfection is illustrated by measurements on two different single photon detectors. Quantitative results for a faked states attack on the Bennett-Brassard 1984 (BB84) and the Scarani-Acin-Ribordy-Gisin 2004 (SARG04) protocols using this imperfection are obtained. It is shown how faked states can in principle be constructed for quantum cryptosystems that use a phase-time encoding, the differential phase shift keying (DPSK) and the Ekert protocols.

[1] Department of Physical Electronics before 2004.

Furthermore we have attempted to integrate this imperfection of detectors into the general security proof for the BB84 protocol. For all attacks, their applicability to and implications for various known QKD schemes are considered, and countermeasures against the attacks are proposed.

The thesis incorporates published papers [J. Mod. Opt. **48**, 2023 (2001)], [Appl. Opt. **43**, 4385 (2004)], [J. Mod. Opt. **52**, 691 (2005)], [Phys. Rev. A **74**, 022313 (2006)], and [quant-ph/0702262].

Acknowledgements

Although this thesis mainly presents author's own work and ideas, it contains substantial contributions by Torbjørn Nesheim, Kirill Vylegjanine, Alexei Brylevski, Artem Vakhitov, Mikhail Chizhov, Andrey Anisimov, Johannes Skaar, with each of whom the author has collaborated at various times, and by my supervisor Dag Roar Hjelme, who has initiated, obtained funds for, supervised and supported most of this work as well as my education.

Parts of research presented in the thesis have been made in collaboration with Telenor Research and Development (1997–2000) and SINTEF Photonics (1999–2001). I thank Andre Mlonyeni and Knut Øvsthus of Telenor, Astrid Dyrseth, Lars Johnsen, and Noralf Ryen of SINTEF for their contributions to the project.

I thank Dag Roar Hjelme, people of the Depertment of Electronics and Telecommunications, administration of the Faculty of Information Technology, Mathematics and Electrical Engineering, Tore Jørgensen and Ragnar Hergum personally, for their support and patience during the many years it has taken me to complete this thesis.

I thank the team of researchers at the Fiber Optics Lab at the St. Petersburg State Polytechnic University, and Oleg Kotov personally, for their hospitality, readiness to give expert advice, and willingness to divert resources from other projects towards my activity. I thank the lively quantum optics community in St. Petersburg for the opportunity to attand seminars and regular lectures and always learn something new.

Anders Karlsson and his colleagues at the Quantum Electronics and Quantum Optics group at KTH, as well as Sergei Kulik and colleagues at the Laboratory of Spontaneous Parametric Down-Conversion at the Moscow State University are thanked for their hospitality during my short stays with them.

Financial support from the Norwegian Research Council (1998–2001, grant No. 119376/431) is acknowledged.

I thank everybody else who has hepled but is not mentioned here by name. Please accept my apologies for curtailing the list.

Contents

1. Quantum cryptography

1.1. Introduction to cryptography

Cryptography is an art of transforming information into something unintelligible for anyone but the intended recipient. This process of transformation is called encryption, and the reverse process is called decryption. The initial information to be encrypted is called plaintext, and the same information in an encrypted state is called ciphertext.

Cryptography has been used for diplomatic, military, commercial, and private communication, and also historically for obstructing religious texts. The earliest known methods of encryption date back to the first millennium B.C., and consist of simple transposition and substitution ciphers: Greek *skytale*, Caesar cipher, Hebrew traditional *atbash* [1, 2].

Security of ciphers initially depended on an adversary not having the knowledge of the encryption algorithm. As ciphers evolved, security begin to depend instead on the knowledge of a short secret key (e.g., a keyword or keyphrase) combined with the lack of knowledge how to deduce this key from the ciphertext. Until the middle of the 20th century, nobody has managed to rigorously prove that a given cipher could not be broken. Indeed, almost the whole history of cryptography has consisted of a cipher being broken, subsequently replaced by another (perceivingly stronger) one, the latter being broken after some time, and so on. People who work on breaking ciphers are called cryptanalysts.

The first provably secure cipher, a “one-time pad”, was proposed around 1920 by Gilbert Vernam [3, 4]. The cipher is very simple and can be performed manually: each symbol of a plaintext is added modulo alphabet size with a symbol of a random secret key to form a ciphertext; on the receiving end, the same operation with an identical copy of the key is used to extract the plaintext. The security of one-time pad was, in fact, not proven until 1949, when Claude Shannon showed in his theory of information that the security was guaranteed if the key was as long as the message, and never reused [5]. The latter condition is obligatory: if the key is reused, plaintext of all messages encoded with it can be, and routinely has been, extracted by cryptanalysts.

Although the one-time pad has been employed for sensitive communications (e.g., with spies), for most uses it remained impractical because of the need for a large and constant supply of key material. Distributing this secure key between users prior to the communication is the most troublesome part of the one-time pad. Any communication channel could in principle be eavesdropped on and a copy of the key obtained (but, as we’ll see a couple pages later, this is only true for any *classical* communication channel; a quantum channel can be made non-eavesdroppable). A personal meeting is not an option for many uses, and even if it is, there is an additional problem of storing the key securely. Modern cryptography employs other solutions for mass encryption and for key distribution.

1.2. Modern cryptography

After mid-1970s, cryptography became ubiquitous, used by ordinary people in everyday life (often without realizing it). Also, a definition of cryptography broadened: once concerned solely with encryption, it now encompassed other tasks, such as signing and various forms of authentication. Two major developments occurred in that decade.

One development was that a public standard of a symmetric cipher, Data Encryption Standard (DES), was released. A symmetric cipher uses a relatively short identical key at both sides, and can quickly encrypt a large amount of information with this key. Although the original DES is no longer considered secure (its limited key length of 56 bits later allowed it to be cracked on a dedicated hardware in less than 24 hours), there are other newer symmetric ciphers with longer keys in use today, e.g., Advanced Encryption Standard (AES) [6].

Another develpment was the discovery of an entirely new class of cryptography, public key cryptography. It utilizes pairs of keys, a private key and a public key. The public key can only be used for encryption, and the private key for decryption. These two keys are connected to one another via a one-way function, which is easy to compute in one way (to obtain the public key from the private key) but extremely hard to compute in the opposite way (to deduce the private key from the public key). The public key is widely announced and the private key is kept secret. Anyone can encrypt a message using the public key, but it can only be decrypted by the recipient holding the private key. One example of such one-way function is miltiplication of two large prime numbers: their product is easy to compute, but factoring the product is hard; this is ised in the Rivest-Shamir-Adleman (RSA) encryption system [7]. Besides encryption, public key cryptography allows signing (the holder of a private key can compute a signature of a message, which everyone can verify using his public key, but not forge) and authentication (veryfying the integrity and origin of a message). Public key cryptography is relatively computationally intense, and is unsuitable for rapid encryption of a large amount of data.

In most modern cryptographic systems, public key cryptography and symmetric ciphers are used in tandem. Such is the suite of cryptographic protocols used on the internet. There is an established public key infrastructure consisting of a hierarchy of certificate authorities. Certificate authorities confirm, through a chain of signatures, or certificates, that a given public key indeed belongs to a given party (identified by a business address and domain name). Then, public key cryptography can be used to share a random secret key with that party. This random key is subsequently used in a symmetric cipher to encrypt the data transmission.

The security of these systems hinges on the strength of symmetric ciphers, and on the existence of one-way functions. Neither has been proven. In particular, it has not been ruled out that an efficient factorization algorithm exists. To the contrary, an algorithm for a *quantum computer* that does factorization in polynomial time has been devised by Peter Shor [8] and experimentally tested in the simplest case (the number 15 was factorized into its prime factors 3 and 5 on a nuclear magnetic resonance quantum computer) [9]. It is an open question whether a quantum computer of a practically useful size can be built or an efficient classical factorization algorithm be found.

However, the probability that either of these two developments happen in the future cannot be neglected. Then, not only public key cryptography does become insecure, but it becomes insecure retroactively: all encrypted communication intercepted in the past will be read. This creates an unacceptable risk for those applications of cryptography where data keep value for a long time. It should be also noted that an efficient classical factorization algorithm is a mathematical advance that may happen behind closed doors of a government lab, and be not publicly announced. In any case, when it is announced that public key cryptography is broken, all remaining public key cryptosystems would have to be replaced by something else.

Thus, using public key cryptography for key distribution is convenient but risky. Using modern symmetric ciphers instead of the one-time pad also bears some risk, but is necessary for encryption of large amount of data modern secure communications require (such as virtual private networks encrypting all traffic exchanged between remote offices of a company).

Until the advent of quantum cryptography, the only alternative to public key cryptography was distributing secret keys via trusted couriers, or exchanging them at a personal meeting.

1.3. Idea of quantum cryptography. BB84 protocol

Quantum cryptography offers something not possible in the classical domain. It allows to distribute (or more accurately said, randomly generate) a secret key over an *open* communication channel. The laws of physics as we know them today guarantee that any attempt of eavesdropping on this open channel will introduce errors into the key, and thus eavesdropping is guaranteely revealed.

Quantum cryptography cannot securely transmit a predetermined information; it can only securely generate a random key. Once generated, this random key can be subsequently used in a symmetric cipher, such as the one-time pad or one of the modern symmetric ciphers, to securely transmit data over a classical communication channel. A running quantum cryptography channel will steadily generate new secret key material. Thus, quantum cryptography is solving the most difficult problem in modern cryptography, that of *key distribution.*

Quantum cryptography uses quantum states, such as polarizations of single photons, to transmit bits of information. It is not possible to make a perfect copy of an unknown quantum state [10], which precludes its precise measurement by an eavesdropper. Perhaps the reader would remember the Heisenberg uncertainty principle: if one measures the precise position of a particle, all information about its momentum is lost, and vice versa. There are many pairs of properties which cannot be precisely measured simultaneously: for example, horizontal-vertical and diagonal states of photon polarization is one such pair. The idea to use this property of quantum states to securely encode information originated with Stephen Wiesner in the early 1970s [11].[2] In his

[2] Wiesner initially submitted his paper to *IEEE Transactions on Information Theory,* which promptly rejected the submission because computer scientists did not comprehend the physics jargon in which it was written [12]. The paper in its original form was published more than a decade later in another journal [11].

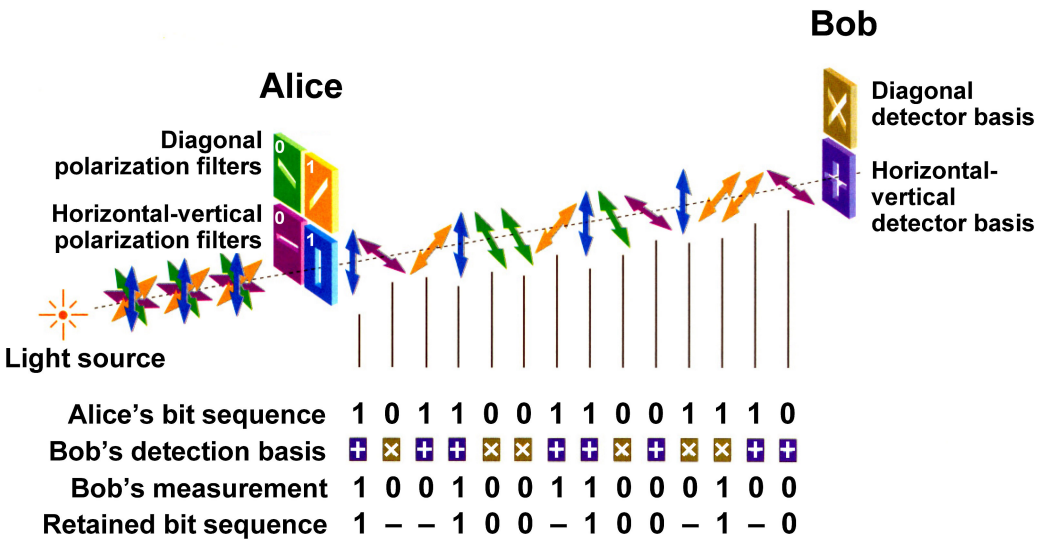


Fig. 1. Principle of the BB84 protocol (reprinted from [20]).

paper, he described two ideas, one of which was "money... physically impossible to counterfeit" that needed what we would today call a long-term quantum memory, which was not and is still not practically realized. By 1984, Wiesner's idea was taken forward by Charles Bennett and Gilles Brassard (who knew of it through personal contacts) in a more practical form: now, quantum states of photons propagating through an optical channel encoded a secure key. The transmission protocol they have devised, Bennett-Brassard 1984 (BB84) quantum key distribution (QKD) protocol [13, 14], is still in use today.

Let's see how a secret key can be transmitted over an open channel in the BB84 protocol. The sender, commonly called Alice, transmits a sequence of photons to the receiver, commonly called Bob (Fig. 1). Alice prepares each photon in one of the four linear polarizations: horizontal or vertical (belonging to the horizontal-vertical basis), or one of the two 45° diagonal ones (belonging to the diagonal basis). It is agreed that one of the polarizations in each basis represents bit 0 and the other bit 1. For each photon, Alice chooses the basis and bit value at random. Bob tries to measure the polarization of each photon, choosing at random between the horizontal-vertical and diagonal measurement basis. Bob's measurement apparatus for each basis can, for example, be a birefringent prism separating the incoming photons into orthogonal polarizations, followed by a pair of single photon detectors. Bob has only one attempt at measuring polarization, because in the process of measurement the photon is destroyed. He remembers his basis and the result of measurement. After a certain number of photons has been transmitted, Alice and Bob talk to one another via a conventional communication channel, e.g., via an internet connection, and publicly compare the transmission and detection bases for each photon (but not the bit values). In approximately half the cases Bob has happened to detect the photon not in the basis in which it has been transmitted. In these cases, his detection result is random and uncorrelated with Alice; these bits are discarded from the key. In the remaining half of the cases,

Bob has detected the photon in the same basis in which it has been transmitted by Alice. In these cases, Bob gets the same bit value as Alice; these bits form a secret key now shared between Alice and Bob.

Let's consider what happens if an eavesdropper, commomly called Eve, tries to intercept the key. At the time of photon transmission, neither Alice's nor Bob's basis has been announced. Eve knows neither in which basis each photon has been prepared by Alice nor in which basis it is to be detected by Bob. She has to randomly guess the basis and detect the photon herself. After detection, she has to regenerate the photon and send it to Bob, so that he detects it and uses this bit in the key (if Bob fails to register a photon, it does not contribute to the key). With 50% probability, Eve's basis is different from Alice's basis. Eve regenerates the photon in the basis she has chosen, with the bit value she has obtained from her detection. The photons intercepted and resent by Eve in the wrong basis that are detected by Bob in the correct (i.e. Alice's) basis cause detection results uncorrelated with Alice, i.e. 50% error probability for these photons at Bob. Thus, if Eve intercepts and resends every photon in the transmission, she introduces on average 25% errors in the secret key. Alice and Bob measure the error rate (called the quantum bit error rate, or QBER) by publicly comparing a randomly chosen subset of the sectret key. The presence of errors reveals eavesdropping.

The straightforward intercept-resend strategy described above is not the optimal one. There are subtler and more complex attacks Eve can carry out that introduce fewer errors. However, it has been generally shown that no attack obtaining full information about the key can introduce less than 11% QBER.[3]

Up to now, we have assumed that equipment is perfect. In reality, there are losses in the apparatus and in the transmission channel, leading to Bob failing to register a photon in the majority of bit slots. There are also inevitable imperfections that lead to errors in the key even in the absence of eavesdropping (due to misalignment in the optics, environmental perturbations, noise in the detectors).

Losses are dealt with simply: those bit slots where Bob has not registered a photon are not used in the key. In a real system, losses and inefficiencies are large: Bob registers one photon per several hundred or thousand bit slots on average. Thankfully, all the failures to register a photon can be simply discarded, proportionally reducing the key transmission rate but otherwise not affecting the security.[4]

The security proofs say that all errors in the key should be attributed to eavesdropping, regardless of their probable real source. It turns out that it is possible to recover a shorter error-free *and* secure key from a longer key with errors, provided QBER is less than 11%. After having discarded incompatible bases, Alice and Bob correct errors by comparing block parities of their copies of the key over the classical communication channel [14]. During this error correction step, they necessarily announce some information about the key over the classical channel, where it can be watched by Eve. After

[3] The 11% lower bound for QBER is valid for a sufficiently well built equipment that conforms to the idealised model used in the security proof, and for a true single photon source; see Section 4.2. Various non-idealities in the equipment may give additional advantage to Eve and further lower the bound. We have been researching some of these non-idealities, see Chapter 4.

[4] With non-ideal photon sources and noisy detectors, there unfortunately are limits on how much loss can be tolerated; see Section 4.2.1.

the error correction, they have two identical copies of the key, partial information about which is known to Eve. Eve could have obtained some information by eavesdropping at the time of photon transmission (her amount of information upper bound by the QBER), and she has watched the discussion during the error correction. In order to obtain a shorter key about which Eve knows nothing, Alice and Bob estimate the maximum amount of information that could be available to Eve, given the QBER they have measured, and given the actual performance of their error correction algorithm (for the theoretical function of available secure information vs. QBER, see Fig. 36 on p. 76). Then, Alice and Bob perform a privacy amplification step by compressing the key using hash functions, by the amount they have determined. The resulting key is shorter, but it is guaranteed that Eve knows a negligible amount of information about it.

Need for authentication

In the QKD protocol described above, it is assumed that Eve listens to all information transmitted over the classical channel between Alice and Bob, but cannot change this information. To prevent the classical transmissions from being tampered with, they must be authenticated. Unconditionally secure authentication techniques exist [15]. They require spending some amount of secret key material. Fortunately, a fraction of the secure key obtained in each key generation cycle is sufficient for authentication in the next cycle, so the overall balance of key generation is positive. A subtler problem arises when Alice and Bob have to do their very first key generation cycle. If the first exchange is not authenticated, then in principle a man-in-the-middle attack is possible: Alice and Bob could in fact be talking to Eve who has inserted herself in both quantum and classical communication channels and simultaneously impersonates Bob for Alice and Alice for Bob. The first exchange must be authenticated with a small secret key delivered by the usual means (personal meeting) at the time of equipment installation. Because of this, quantum key distribution would be more correctly called *quantum key growing.*

The need for initial authentication is not a requirement unique for quantum cryptography. It is universal to all secure communication: you cannot say whom you are communicating with unless you share a common secret with him. The public key cryptography is not an exception: to satisfy the need for initial authentication, a set of puiblic keys of several certificate authorities is usually delivered with the operating system or inside a copy of communication software (e.g., a web browser); further authentication is provided through the public key infrastructure. QKD could also be authenticated through the public key infrastructure: such an authentication would be secure from being cracked retroactively (because, once authenticated, the security of key exchange no longer depends on public key cryptography). However, as we have noted in Section 1.2. , relying on public key cryptography is not a good idea in the long run. Should QKD receive widespread use in a form of a network, an alternative authentication infrastructure could be developed. Research into this is currently underway.

When we talk in the previous paragraph about the possibility of using public key infrastructure for authentication of QKD, it touches an interesting point. One additional advantage of quantum cryptography over classical cryptography is that the former

cannot be cracked retroactively. We'd rather say of course that quantum cryptography cannot be cracked at all, but suppose a practical loophole is left unnoticed in its early implementations. In order to exploit the loophole, Eve needs to have the knowledge of it and the necessary technology at the time of quantum transmission. Once the key is generated by QKD, it cannot be cracked retroactively — unlike classical cryptography, where intercepted (i.e. copied) transmissions can be cracked later.

Phase coding

When optical fiber is used as the transmission channel, polarization becomes an inconvenient choice for encoding qubits. Standard singlemode optical fiber of the type commonly used in communication networks changes the polarization of propagating light in a random and unstable way. Rather than track these changes in real time, it is more convenient to encode qubits in another property of light well-preserved under propagation in the fiber, namely the relative phase of two closely spaced light pulses. A scheme using such an encoding is shown in Fig. 2. It is, in essence, a single Mach-Zehnder interferometer with a phase modulator in each arm. To make the interferometer stable and to reduce the number of transmission fibers required, the two arms are multiplexed into a single fiber before leaving Alice, and demultiplexed after entering Bob. The arms in Alice's and Bob's halves of the interferometer have different lengths, so that the pulses from different arms are separated by the length (or time) $L_A–S_A = L_B–S_B$ while travelling the transmission line. As long as environmental perturbations in the transmission line have a characteristic time scale much longer than the time separating the pulses, the two pulses suffer the same polarization transformation and time delay in the line. Hence they interfere well at the rightmost Bob's coupler. The result of interference (determining which of the Bob's single photon detectors D_0 and D_1 clicks) depends on the difference between the phase shifts applied at Alice's and Bob's phase modulators, $\varphi_A–\varphi_B$. Alice chooses the bit value and transmission basis by applying one of the four phase shifts $–3\pi/4$, $–\pi/4$, $\pi/4$, $3\pi/4$ at her modulator. Bob chooses the detection basis by applying either $–\pi/4$ or $\pi/4$ phase shift at his modulator (all possible phase combinations and interference outcomes are listed in Table 1 on p. 24).

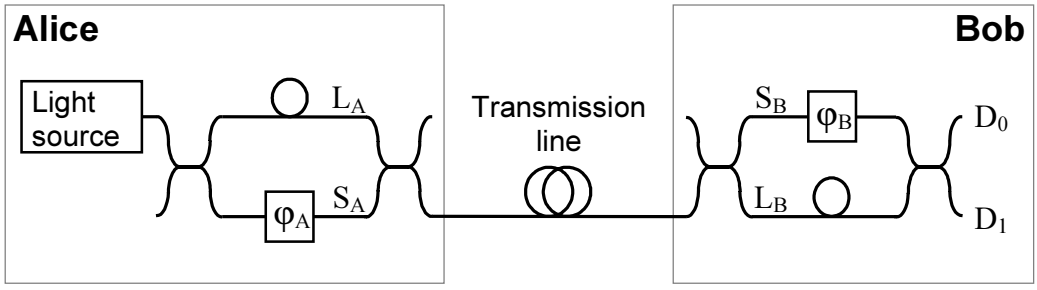


Fig. 2. Interferometric QKD channel with phase coding. The two arms of the Mach-Zehnder interferometer are multiplexed into a sinlgle transmission line.

The two encodings discussed above are, unsurprisingly, called polarization coding and phase coding. It can be shown that they are isomorphic to one another [16]. The transmission protocol for both encodings is exactly the same: each phase shift value used in phase coding has its polarization state counterpart in polarization coding.

Phase coding and its variations are used in all today's fiber optic QKD systems. Polarization coding has only been used in the first fiber-based experiments [17, 18]. However, polarization coding is entirely suitable for and is used in QKD systems with a line-of-sight free space transmission channel, because air does not distort polarization.

For additional popular introductions, see Refs. 19, 20, 21. A good description of the BB84 protocol is given in Ref. 14.

1.4. Review of quantum cryptography research[5]

Over fifteen years, QKD moved from a proof-of-the-principle experiment set up on an optical table to production-ready equipment using installed fiber optic cables several tens of kilometers long.

In the first experimental demonstration of QKD completed in 1989 [14], the quantum channel was a thirty centimeter long path of air in a laboratory. Soon afterwards, experiments moved towards using optical fiber as the quantum communication channel. In the list that follows, we single out the maximum achieved transmission distance as the figure of merit; however, for any given application, other parameters such as the key generation rate or complexity of equipment can be more important. After the first experiments by Muller et al. in Geneva with 1.1 km long fiber [17, 22], the transmission distance was extended in 1995 to 23 km over an undersea fiber optic cable [23, 18]. At about the same time, Townsend at British Telecom demonstrated 30 km transmission [24]. He later tested it with various configurations of optical network [25, 26] and improved the distance to ~50 km [27]. An experiment over the same distance was later repeated by Hughes et al. at Los Alamos [28]. In 2001, Hiskett et al. in the UK reported 80 km transmission distance [29]. In 2004–2005, two groups in Japan and one in the UK reported QKD and single-photon interference experiments at over 100 km distance [30, 31, 32]. The current record is held by the Los Alamos — NIST collaboration at 184 km [33], using a sub-Kelvin cooled transition edge sensor for single photon detection (see Section 3.1.). However, if we restrict ourselves to practical detectors based on avalanche photodiodes (APDs), the earlier experiment over 122 km done by researchers at Toshiba in Cambridge, UK remains the leader [31].

Transmission distances claimed by experimenters must be viewed with some caution. All the experiments listed above use attenuated laser pulses instead of true single photon sources. They typically set attenuation at an arbitrarily chosen level, when light leaving Alice contains on average, depending on the attenuator setting, 0.1 to 0.5 photons per pulse (statistically, of course: there will be pulses where you register no photons, pulses with one photon, and fewer pulses with two or more photons, their

[5] For a comprehensive review of developments in quantum cryptography until 2001, please see Ref. 16. We only recap the milestone experiments in this section, without going into detail.

probabilities given by the Poisson distribution). Then, the experimenters increase the transmission distance, and thus the attenuation in the line, until so few photons reach Bob that randomly occurring dark counts in his single photon detectors contribute enough errors to raise the QBER to almost 11%. This, they claim, sets the distance limit. Of course, the history of distance improvements is mostly the history of making less noisy single photon detectors, together with switching from 800 nm to 1300 nm to 1550 nm transmission window in order to get lower attenuation per kilometer. The problem is, this estimate of the transmission distance does not take into account some powerful attacks Eve in principle is allowed to do when Alice's source has a multi-photon component (even though these attacks are not practically possible with today's technology). When accurately accounted for an unlimited Eve (i.e., Eve limited only by the laws of physics), the maximum transmission distance in these experiments shortens severalfold. For example, the last experiment listing 184 km for limited Eve can only provide transmission up to 67.5 km with unconditional security [33]. These issues have slowly been realized by the community, and ways to bring the unconditional-security distance closer to the original estimates are currently being developed, in a form of new and modified protocols, such as the decoy state protocol. Please see Section 4.2.1. for a more detailed discussion of the issues introduced in this paragraph.

Another issue is that the key generation rate near the maximum distance can be miniscule, less than a few bits per second. To get more useful rates on order of hundreds and thousands of secure bits per second (these rates are attainable with current QKD setups), one must abstain from making the link length close to the limit.

Although fiber-based transmission is probably optimal for terrestrial communications, several experimens on free space line-of-sight QKD have been done. The ultimate rationale for these experiments is to pave the way for QKD between a low-orbiting satellite and earth-bound users. Since the satellite circles the planet, it could in successive short sessions establish a secret key shared by widely separated users (the satellite is considered a trusted party by all of them). The obstacles to implement the satellite-earth QKD are losses due to scattering in the atmosphere, diffraction and atmospheric turbulence, a need for spectral, temporal and spatial filtration for daylight use, suitable telescopic optics, and accurate tracking. The loss and filtration issues have been addressed in the latest experiments to an extent satisfying or exceeding the requirements that a real satellite link would impose. From this standpoint, a satellite QKD link has been shown feasible; the question of implementing it hinges on commercial interest (i.e., a lack thereof for the time being). Free space experiments use polarization coding and photons in the 600–900 nm wavelength range, for which very good detectors based on silicon APDs exist (see Section 3.1.). After the first demonstration over 300 m in 1996 [34], several experiments in the 0.5–2 km transmission range followed [35, 36, 37, 38]. In 2002, QKD experiments over 10 km distance in daylight at Los Alamos [39] and over 23.4 km at night in Germany [40, 41] were reported. A feasibility study of a satellite system exists [42]. In the other extreme, an ultrashort range free space QKD setup has been developed, allowing secure generation of key over several tens of centimeters (or at most a few meters) between a portable storage card and a "quantum ATM" [43].

It is theoretically possible to extend the transmission distance over a terrestrial QKD link via the use of quantum repeaters and nested purification protocol [44, 45]. In this protocol, a link is divided into segments. Entangled pairs of photons are transmit-

ted over each segment; thereafter, a pair of of high fidelity is obtained from several pairs of lower fidelity by entanglement purification, first over each segment, then over groups of segments, nesting until the desired length of the link is reached. The protocol in principle allows to obtain an entangled pair of high fidelity over an arbitrary distance, and thus be able to do QKD over an arbitrary distance, with required resources (which are measured in time or in the total number of initial entangled pairs in all segments) scaling only polynomially with distance. However, an experimental demonstration of quantum repeaters is likely some years away, and of course their practical security (e.g., Eve exploiting imperfections of components) has not been studied.

The only practical way to extend the distance beyond that of a single point-to-point link today is to build a chain of these QKD links with trusted secure nodes in connection points. This approach can be generalized to a multiuser key distribution network with trusted nodes [46]. Possible architectures and protocols for such a network are being developed.

Since 2004, quantum cryptography systems have been commercially availabe. Presently, two small companies, *id Quantique* and *MagiQ Technologies* [47], are ready to deliver a complete QKD link paired with standard virtual private network (VPN) classical encryption equipment. As of 2006, they have reportedly served very few, if any, customers. The present cost of QKD equipment is of the order of 100,000 U.S. dollars for a complete point-to-point set [48], so expensive due to being the first commercial samples, practically hand-made. However, there is nothing intrinsically expensive about quantum cryptography hardware: in mass production and with mature technology, it should not cost much more than any other computer component. Several other companies and organizations (e.g., Toshiba, NIST, QinetiQ, SmartQuantum [49]) have production-ready QKD technology. In the currently advertised commercial applications, a high-throughput (gigabits per second) VPN link is encrypted with key material generated by QKD. Typical VPN data rates rule out the use of one-time pad; a symmetric cipher such as AES with a frequently updated key (e.g., a new key supplied several times per second) has to be used. This is barely a modest incremental improvement in the level of security; the main benefit of the existing commercial quantum cryptography systems seems to be that an automatic system replaces manual key distribution. QKD will never match classical network links in speed, but improvements allowing a couple orders of magnitude faster key generation rate than available today are being researched. Then, it is a question of management to select the most sensitive traffic for one-time pad encryption, while the rest can be encrypted by a modern symmetric cipher with frequently changed key.

In general, quantum cryptography is a diverse interdisciplinary field where many opportunities for academic research and for trying new ideas exist. It has stimulated development of new mathematical and experimental techniques useful outside the context of quantum cryptography. The use of intrinsically analog optical signals in the quantum communication channel make the design of devices in several ways more intricate than that of purely digital encryption equipment or software.

1.5. Thesis outline

We joined the field of quantum cryptography in 1998, when it was already moderately advanced. This thesis presents the results produced by our small group at NTNU over the eight years.

The rest of the thesis is organized as follows. Chapter 2 presents the background for QKD over optical fibers, details of our QKD setup (excluding the single photon detector) and experimental results obtained with this setup. Chapter 3 presents a review of existing single photon detection techniques, and a description of the single photon detector used in our setup. Chapter 4 presents our view of the security of QKD systems, new attacks we have proposed and studied; it ends with our latest paper. In Conclusion, results are recapped and possible directions of further research are outlined.

2. Quantum key distribution over optical fibers

Today, optical fibers are the most promising media for quantum key distribution. Commercial QKD systems are already available [47]. Several recent experiments have demonstrated QKD over distances exceeding 100 km [33, 30, 31, 32]. Protocols that provide truly secure transmission over large distances using an attenuated semiconductor laser as the light source are being developed (see Section 4.2.1.). The distance is currently limited by the noise level (measured in dark count probability) of commercially available single photon detectors (SPDs) for the 1550 nm fiber transmission window. APD-based SPDs continue to improve. Moreover, superconducting SPDs that exist today (see Section 3.1.) could be used in a QKD system, further improving the transmission distance [33].

Sending quantum states over an optical fiber presents an unique set of challenges. These challenges are briefly discussed below, followed by a description of our implementation of a QKD setup, results of a QKD experiment, and a phase tracking technique that we have thoroughly studied and implemented in our setup.

2.1. Technical issues and choice of coding

A number of issues can present a problem for QKD over optical fibers:

- Polarization transformation in standard singlemode comunication fibers, random and changing with time. When a laser source is used in a QKD system, polarization transformation in the fiber can be tracked. However, with wideband sources like a parametric downconversion source of entangled photons (typically ~5 nm emission linewidth), a standard singlemode fiber several kilometers long becomes depolarizing [50].
- Polarization dependence of components in Bob's (and, in the case of a "plug and play" scheme considered below, Alice's setup). Notably, a practical high-speed phase modulator used in phase coding schemes, $LiNbO_3$ planar waveguide modulator, usually is a polarizing component. A scheme exists for a polarizing phase modulator to work as a polarization-insensitive component [51, 52] and is used in a QKD implementation [53], but it adds complexity. Another solution is not to use a phase modulator at Bob at all, but make a scheme with passive basis choice.
- Phase drift in the interferometer (see Section 2.3.) harmful in phase coding schemes. Solutions to this problem include active phase tracking, and a stable interferometer construction. The latter can be either heavily isolated fibers, or

small integrated interferometers reported stable over hours [54], especially polarization-insensitive ones [30].

- Chromatic dispersion effects in standard single-mode fibers. In some QKD experiments reported to date, chromatic pulse broadening becomes a concern [30, 32, 55].

There isn't an ideal solution to all these problems at once. Every invented optical scheme for QKD has its advanteges and drawbacks. Also one must keep in mind eavesdropping, because some optical schemes are more vulnerable to attacks than other (see Chapter 4.).

The first experimental implementations of QKD over optical fibers used polarization coding [17, 18]. Although it is in principle possible to track polarization accurately, the community has quickly switched to phase coding schemes. Relative phase of pulses closely following one another in fiber does not change, unlike their polarization. In some of the phase coding schemes, it is still desirable to track polarization (when Bob's setup is polarization-dependent), but accuracy requirements for polarization tracking are somewhat relaxed.

Two main phase coding schemes are considered below. One is a straightforward scheme with one-way pulse propagation. Another is a "plug and play" scheme with two-way pulse propagation, where both phase drift in the interferometer and polarization transformation in the fiber are compensated automatically, without the need for stabilization and active tracking.

2.1.1. One-way phase coding scheme

The first common scheme with phase coding (introduced by Bennett in 1992 theoretically [14] and by Townsend et al. in 1993 experimentally [56]) consists of just a Mach-Zehnder interferometer, with arms multiplexed into a single fiber at Alice and demultiplexed at Bob. As an example, we reprint here a version of this scheme by Marand and Townsend [24], where demultiplexing the pulses at Bob is done on a polarization splitter (Fig. 3). The polarization splitter allows to separate the pulses coming from the transmission fiber into the arms with a loss lower than the 3 dB a scheme with a common 50/50 coupler in this place would have. In exchange however, this scheme requires polarization tracking at Bob.

Schemes of this general type (differing in details) are used in several other experiments [28, 31, 57].

2.1.2. "Plug and play" scheme

The second common scheme with phase coding (introduced by Muller and coworkers in 1997 [58]) features light pulses travelling first *from Bob to Alice*, getting reflected by a Faraday mirror at Alice, and travelling back to Bob through the same transmission fiber (Fig. 4). The two-way propagation with a Faraday reflector automatically compensates for all polarization fluctuations in the transmission channel: the

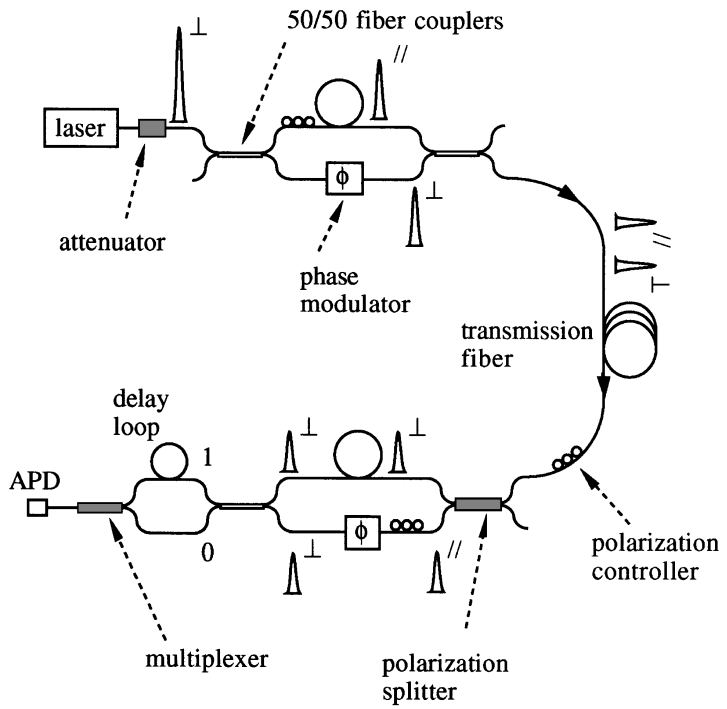


Fig. 3. Reprinted from [24]: interferometric quantum cryptography scheme.

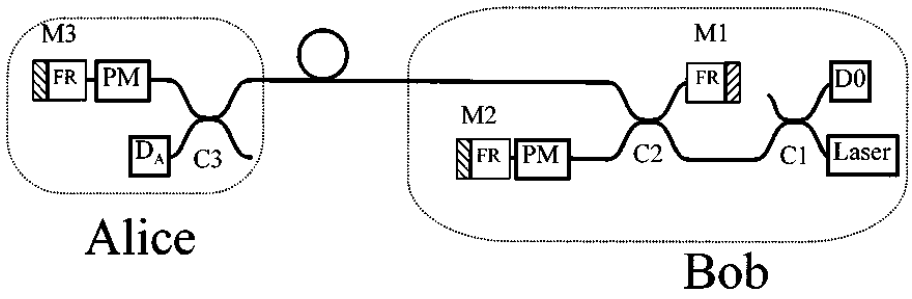


Fig. 4. Reprinted from [58]: "plug and play" system with phase coding. A short laser pulse sent by Bob is split into two at coupler C2. The first part, P1 goes straight to Alice, while the second one, P2, is first delayed by the M2–M1 delay line. Both pulses are reflected back towards Bob at M3. Alice measures the intensity of the incoming pulses, and attenuates them to single-photon levels. The phase modulators (PM) modulate the path length between the two pulses. On arrival to Bob's side, part of P1 is delayed by M1–M2, and thus interferes with incoming P2. The interference pattern at D0 gives the relative phase settings of Alice and Bob. Use of the Faraday rotators (FR) before the mirrors makes it possible to cancel out all birefringence effects in the fibers.

pulses always return to Bob in a polarization orthogonal to the one they left in [59, 60, 16]. Phase drift in the interferometer is also automatically compensated in this scheme. Fig. 4 depicts the first scheme that uses the Bennett 1992 (B92) protocol with one detector.[6] A version of this scheme exists [62, 63] that uses two detectors and can implement the BB84 or the Scarani-Acin-Ribordy-Gisin 2004 (SARG04) [64, 65, 66] protocols.

The "plug and play" scheme is convenient for implementation, because it does not require complex adjustments during operation. It has its own limitations and risks noted below in Section 2.3. Schemes of the "plug and play" type are used in a few other experiments [e.g., 67, 68, 69, 70] and in both commercial systems [47].[7]

Besides the two types of schemes presented above, more schemes with phase coding exist. Among them are the frequency coding scheme [72] using the B92 protocol, phase-time coding scheme [73], differential phase shift keying (DPSK) schemes [32, 74, 75]. However, security of these schemes and protocols has not been studied to the same depth as for the first two schemes. Also, we do not consider here schemes using a source of entangled photons [76, 77, 78, 50, 55]. Even though similar challenges exist for them, entangled photon sources are not just yet suitable for a commercial system.

2.2. Our implementation of one-way phase coding scheme

We chose to build a QKD setup based on the Marand-Townsend scheme [24] with a time- and polarization-multiplexed Mach-Zehnder interferometer and time-multiplexed detector (Fig. 3). The main difference of our interferometer was the use of polarization-maintaining (PM, *not to confuse with* phase modulator) fiber in Alice's and Bob's setups, which eliminated polarization controllers from the scheme (but not the polarization controller at the input of Bob). We also planned to improve the laser pulse rate, and hence the key generation rate, through the use of afterpulse blocking technique at the detector, described in Chapter 3. We use the BB84 protocol [13, 14].

Althoug this straightforward, one-way optical scheme required active phase and polarization tracking, we preferred it over the "plug and play" type scheme. In the latter scheme, the light pulses were accessible to Eve before they were modulated and attenuated to a single photon level inside Alice's setup. We decided that the security of the "plug and play" scheme was insufficiently studied to choose it for implementation. In the following years, our reservations have been partially confirmed. It has turned out to be more difficult to protect the "plug and play" scheme from a large pulse attack

[6] The B92 protocol is different from the BB84 in that it relies on coherent states instead of the single photon (number) states, encodes bits using just two states instead of the four, and implements a homodyne measurement at Bob. See Ref. 61 for the definition of B92.

[7] Details of the commercial QKD systems [47] have not been openly published in writing, to our best knowledge. However, we can infer the type of scheme used by id Quantique from prior publications by the Geneva group, and the one used by MagiQ Technologies from several U.S. patent applications their employees have recently submitted. Recent conference talks given by representatives of both companies (e.g., [71]) confirm this. If you buy a system from either company, you get one with the "plug and play" type of optical scheme.

(see Section 4.3.1.), and it has been shown that the phase information Eve has in the "plug and play" scheme can give her additional information unless a phase randomizer is included into Alice's setup [79]. On the other hand, our one-way scheme has demanded extra work in implementing active phase tracking (see Section 2.3.).

Please keep in mind that we had to make our choice of scheme in 1998, when many of the newer schemes mentioned above were not known.

2.2.1. Polarization-maintaining double Mach-Zehnder interferometer

The optical part of the QKD setup consists of a laser, Mach-Zehnder interferometer, and a single photon detector (Fig. 5). The 1310 nm laser (semiconductor gain-switched laser, Fujitsu FLD3F6CX) emits 100 ps wide pulses at 10 MHz repetition rate. The pulses (already strongly linearly polarized) pass through a polarizer (OZ Optics) and are split into two arms of interferometer on a variable ratio PM coupler (evanescent-wave all-fiber, Canadian Instrumentation and Research Ltd.). The interferometer in Alice's and Bob's setups is made of PM fiber (Fujikura PANDA) and all components are oriented such that the light is polarized along the slow axis of the fiber. One arm of the interferometer is short on Alice's side and goes straight to the polarization combiner (OZ Optics). The other arm is long and contains a four meter delay line, a variable delay line (50 mm variation, Princeton Optics) to get the length of the two interferometer arms exactly equal, and Alice's phase modulator (polarizing $LiNbO_3$ planar waveguide, Alenia Marconi; half-wave voltage 3.5 V). Pulses from the two arms on Alice's side are combined into a single fiber (standard SM fiber) on the polarization combiner, such that they are separated by a delay and have at this point orthogonal linear polarizations. Then they pass through a variable attenuator (JDS Fitel VA4; set at ca. 60 dB) in order to get the average photon number per pulse pair down to sub-photon level. We thus use not a true single photon source in our system, but a weak coherent state source (see Section 4.2.1.).

As the two pulses pass through the communication line consisting of standard single mode (SM) fiber, they undergo a polarization transformation. However, this transformation is the same for both pulses, and their polarizations, although being arbitrary elliptical at the output of the line, remain orthogonal to one another. With the help of a polarization controller (all-fiber type PFPC, OZ Optics) at Bob, their polarization can be restored back to linear and properly oriented so that the pulses are routed each into its own arm of interferometer on a polarizing splitter (OZ Optics). The pulse that has travelled the long arm at Alice now goes into the short arm. The pulse that has travelled the short arm at Alice goes into the long arm at Bob that contains a delay line and Bob's phase modulator (polarizing $LiNbO_3$ planar waveguide, Uniphase[8]; half-wave voltage 8.2 V). Both pulses come to the 50/50 PM coupler (evanescent-wave all-fiber variable ratio coupler, Canadian Instrumentation and Research Ltd.; set at 50/50 splitting ratio) at the same time and are oriented to have the same polarization, so they

[8] The phase modulators at Alice and Bob were initially identical ones made by Uniphase, but we had to replace one of them after an experimental mishap (see Appendix A).

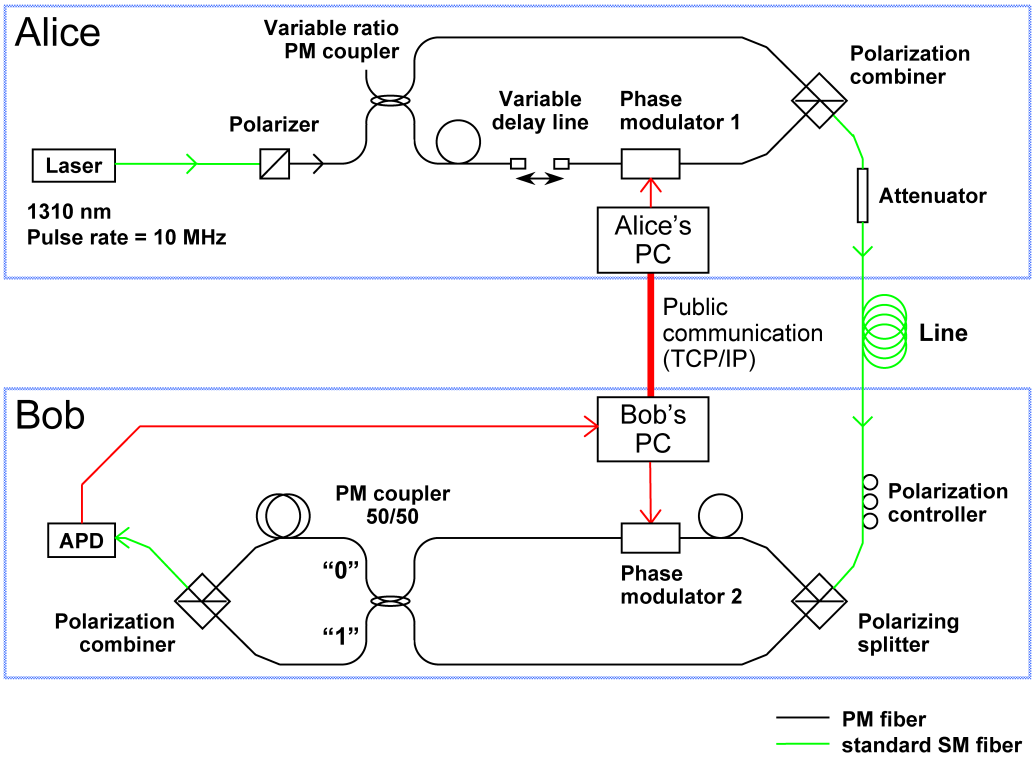


Fig. 5. QKD setup. Optical scheme.

Table 1. Implementation of the BB84 protocol in our setup.

Alice		**Bob**		
Bit value	φ_A	φ_B	$\varphi_A-\varphi_B$	Bit value
0	$-\pi/4$	$-\pi/4$	0	0
0	$-\pi/4$	$\pi/4$	$-\pi/2$	?
1	$3\pi/4$	$-\pi/4$	π	1
1	$3\pi/4$	$\pi/4$	$\pi/2$	?
0	$\pi/4$	$-\pi/4$	$\pi/2$	?
0	$\pi/4$	$\pi/4$	0	0
1	$-3\pi/4$	$-\pi/4$	$-\pi/2$	?
1	$-3\pi/4$	$\pi/4$	π	1

interfere. The outcome of interference, i.e. which output port at the coupler the resulting pulse takes, depends on the difference between phase shifts in Alice's and Bob's phase modulators $\varphi_A-\varphi_B$ (Table 1). One of the output ports is agreed to represent "0" bit value, and the other "1" bit value in the protocol. When the phase difference equals 0 or π, the interference outcome is definite; with other phase differences the photon appears randomly at one of the output ports.

In principle, we could use two SPDs: one at each output port of the coupler. However, following Townsend, we multiplex the ports into a single fiber using a ten meters long delay line and a polarization combiner (OZ Optics). Then we use one detector gated at double the laser pulse rate, i.e., at 20 MHz. Our SPD is APD-based and is described in Chapter 3. The approximately ten meters long delay line is legth-adjusted so that its delay equals the gate pulse period (50 ns) with a precision better than the detector gate width (gate width ~1 ns, desired precision better than 100 ps; the actual splicing precision happened to be better than 25 ps or 5 mm, as the measurement of detector sensitivety curves described in Section 4.3.3.2. incidentally revealed).

The interferometer was initially assembled on an optical table (Fig. 6), and its operation was checked. Then, Alice's and Bob's halves of the interferometer were mounted onto 6 mm thick aluminium plates (Figures 7, 8), covered with thermoisolation, and put each into a box sized approximately 420x420x150 mm (Fig. 9).

Our system requires active tracking and compensation of phase drift in the interferometer, which we have implemented (see Section 2.3.). Tracking of polarization transformation in the communication line would also be desired, because proper splitting of pulses into the arms at Bob's polarizing splitter depends on the accurate polarization. However, some inaccuracy in polarization is tolerable: it would send some fraction of the pulses into a wrong arm, where they do no harm arriving at the detector outside its gating windows. This inaccurate splitting only leads to additional loss. In principle one could forgo polarization adjustment altogether, which in this scheme would result in average >50% reduction of the key generation rate, and periods of total fading. The speed with which the polarization transformation in the line changes depends on the environment around the communication cable. In lab demonstrations with spooled fiber, as well as in underground and undersea fiber optic cables, polarization can remain stable for tens of minutes [18, 80, 81]. However, in aerial cables it can change quickly [81]. Techniques for polarization tracking developed for coherent optical communication systems in the 1980s could be adapted for our system [82]. We have not implemented polarization tracking, because for initial demonstrations manual adjustment of the polarization controller before each test run would suffice.

2.2.2. Electronics and control systems

The electrical diagram of our system is shown in Fig. 10. Alice's and Bob's setups are controlled by two PCs connected via internet (10 Mbps LAN) used as a public channel. Each PC is equipped with a high-speed arbitrary waveform generator card (National Instruments NI 5411) used for driving the phase modulators. Amplifiers placed in Box 1 and Box 2 boost the voltage for phase modulators. Bob also has a digital I/O card (DIO D32HS) used for generating the trigger signal and for reading detector data. Data acquisition from the APD is done by Box 3, which contains 512 KiB buffer memory with 20 MHz serial input. This memory can store up to 2097152 consecutive pairs of detection outcomes received from the APD electronics described in Chapter 3. The buffer memory is needed because a PC cannot reliably read serial data at the required rate. The memory in Box 3 fills up with detector data automatically in about 210 ms following the trigger, and then Bob's PC can read its contents byte by byte using the digital I/O card.

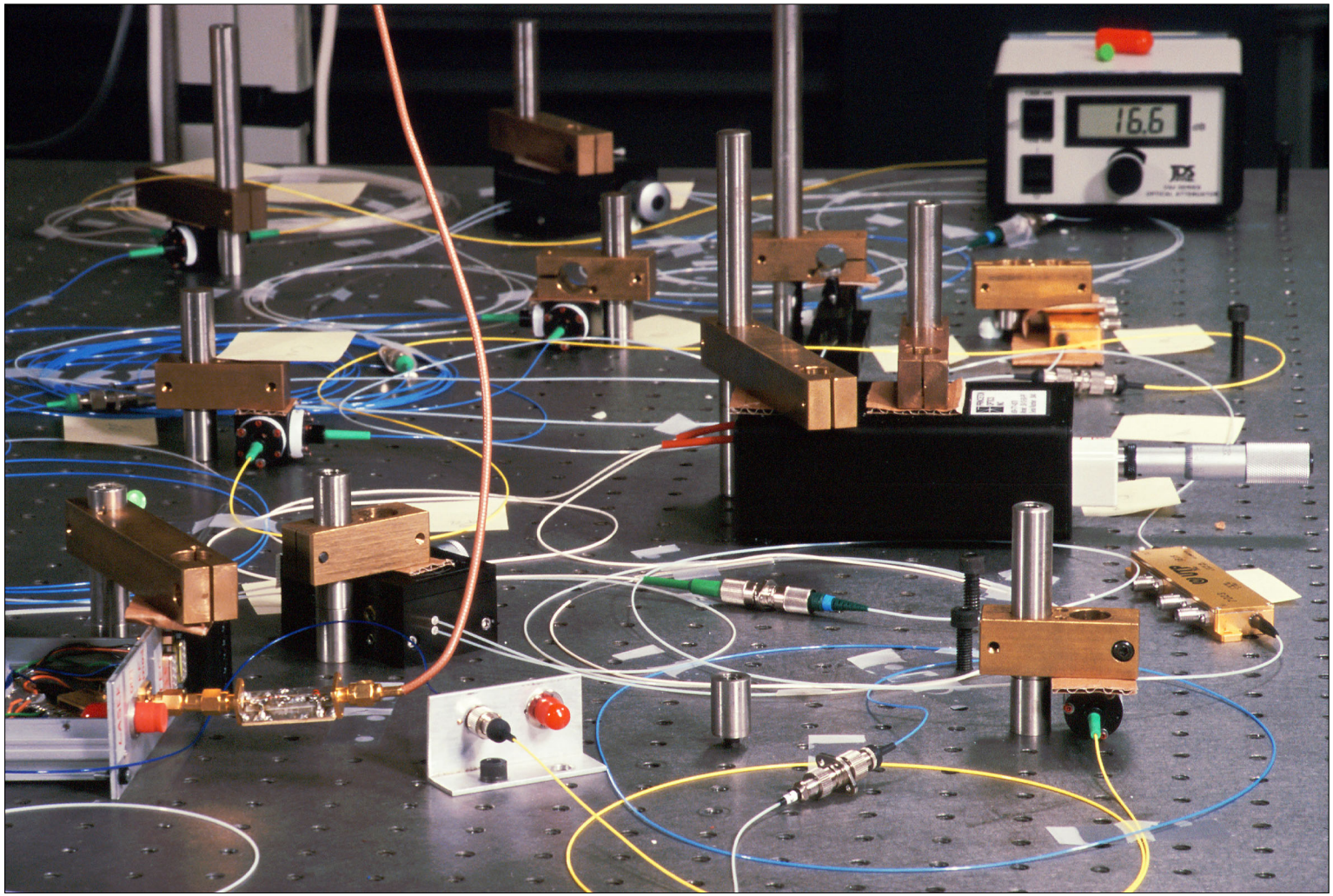


Fig. 6. Interferometer in testing stage, laying on the optical table. For the fringe visibility test, the surface of the optical table with the interferometer was covered by a layer of styrofoam granules (not shown on photo).

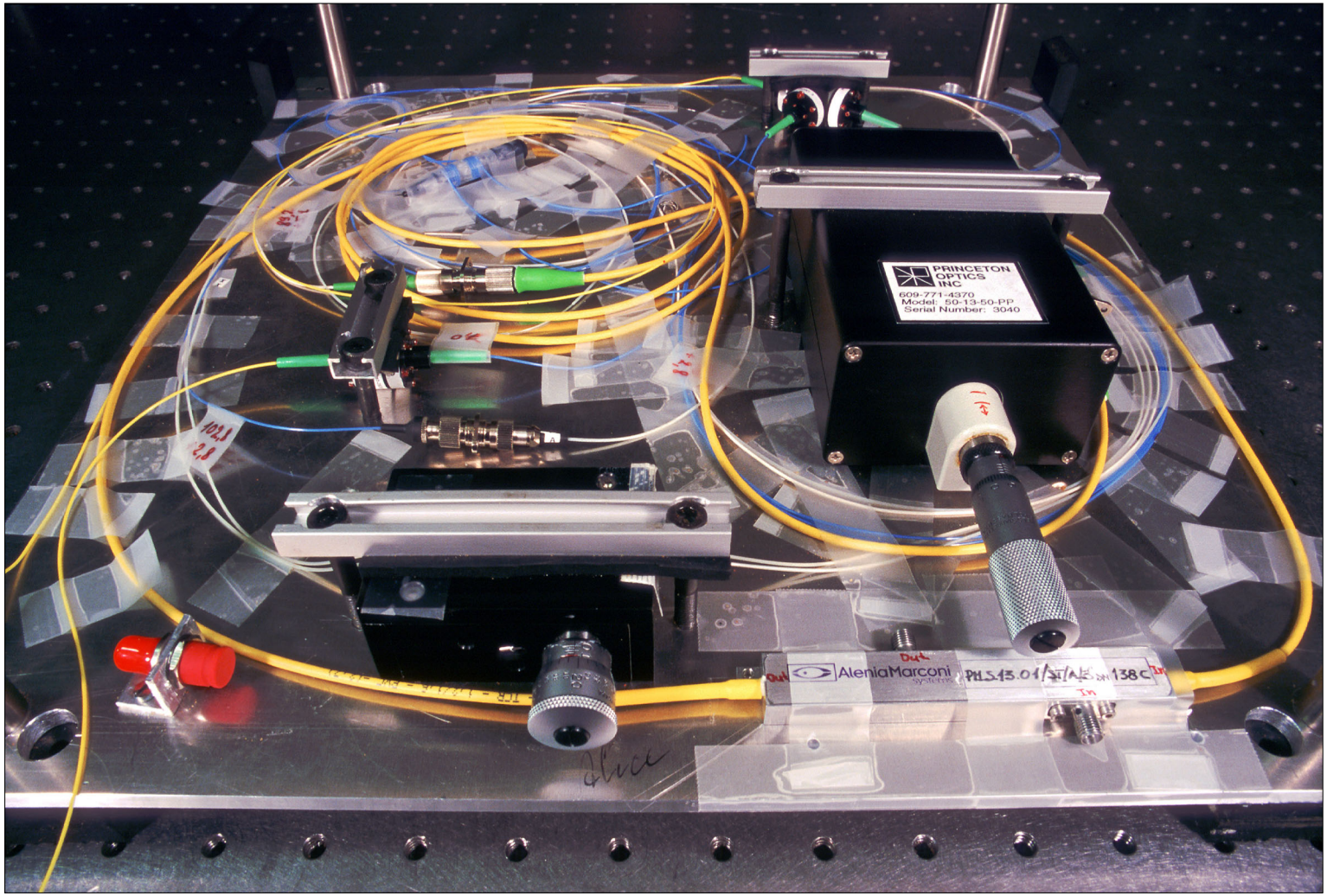


Fig. 7. Alice's interferometer (uncovered, no thermoisolation installed). Components: variable ratio PM coupler, at front left; phase modulator; at front right; polarizer, at middle left; variable delay line, at middle right; polarization combiner, at back right. Laser module not shown.

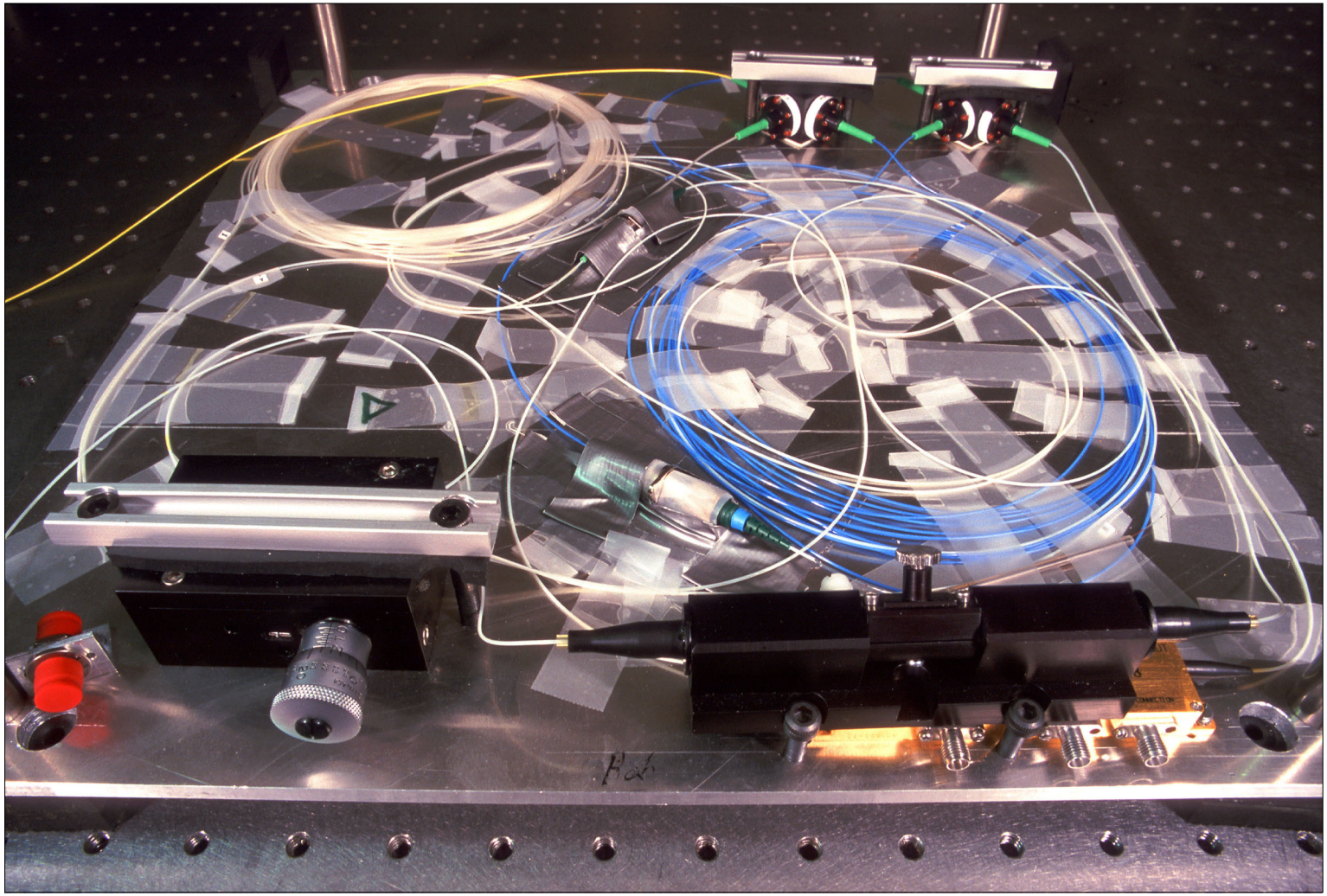


Fig. 8. Bob's interferometer (uncovered, no thermoisolation installed). Components: variable ratio PM coupler, at front left; polarization controller mounted atop phase modulator, at front right; polarization splitters/combiners, at back. Single-photon detector not shown.

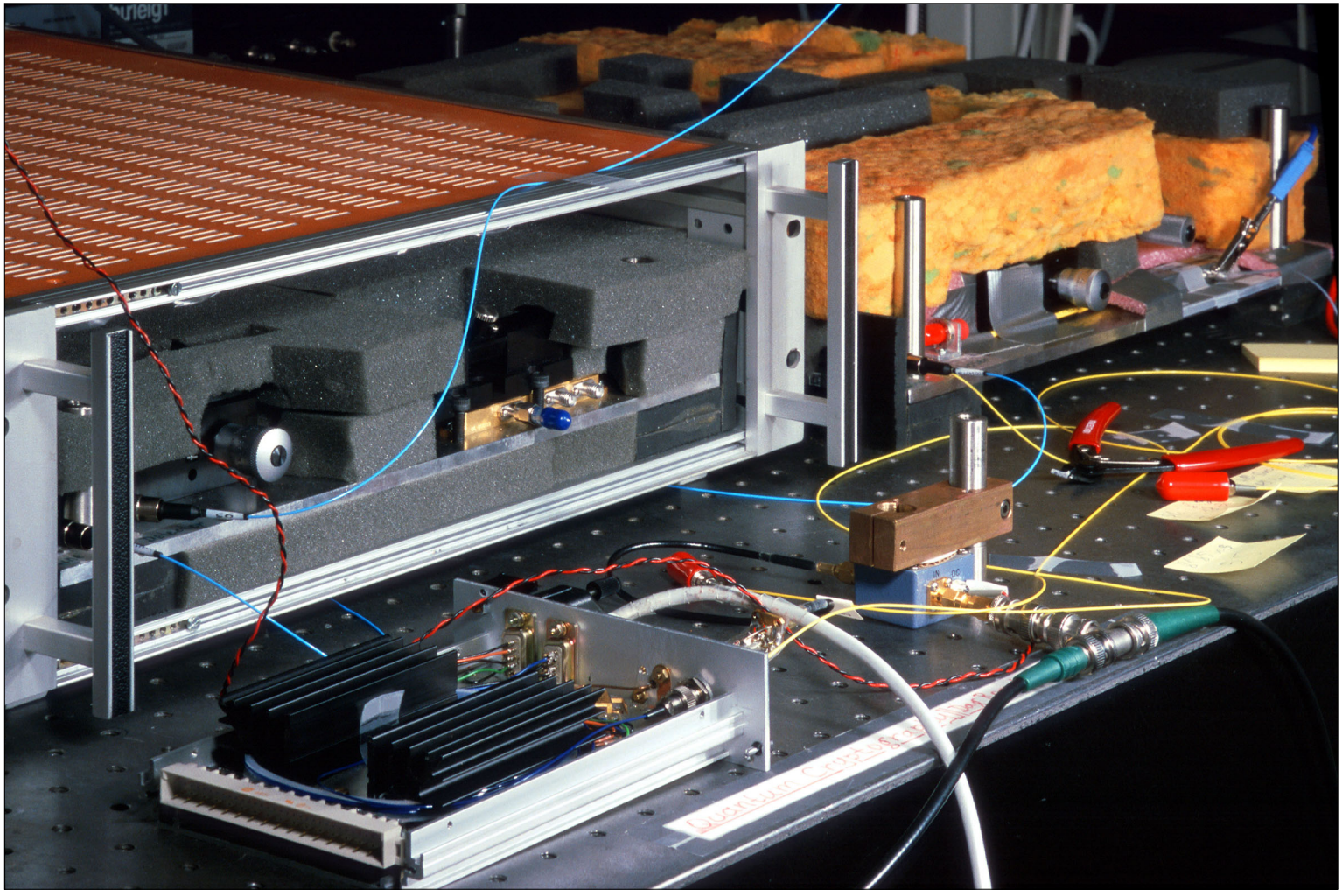


Fig. 9. Optical setup during experiments. Bob's (left) and Alice's (right) interferometers, thermoisolation mostly installed. Laser module on the foreground.

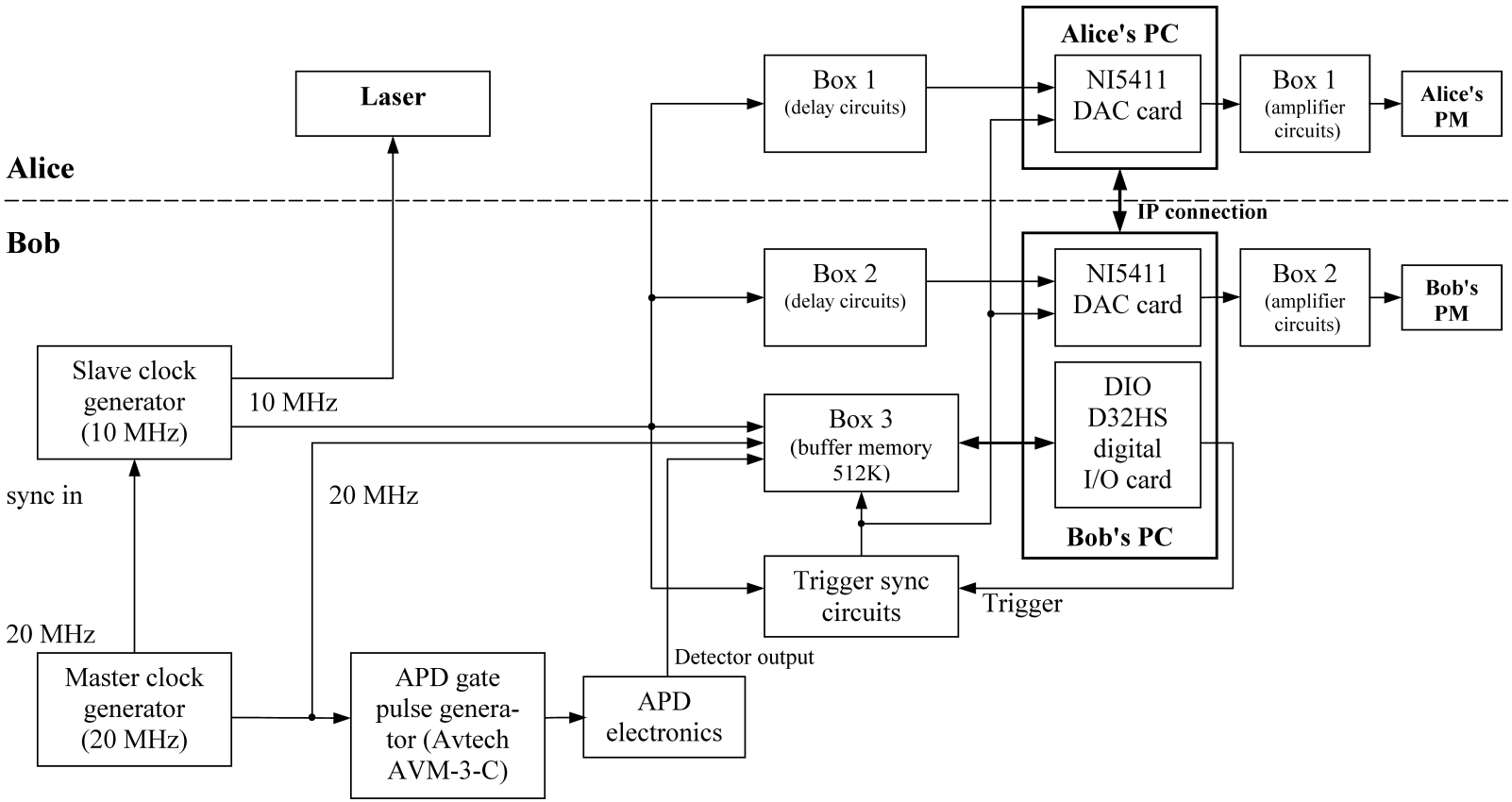


Fig. 10. QKD setup. Electrical interconnections diagram (reprinted from [83]). PM, phase modulator.

The synchronization of the whole system is done with the help of several generators. The master clock generator (SRS DS345) outputs a stable 20 MHz signal. This signal synchronizes Box 3, the 20 MHz generator that produces gate pulses for the APD, and the 10 MHz slave clock generator (consisting in reality of two generators: E-H Research Laboratories Inc. EH129 and Datapulse 101). The 10 MHz clock from the slave generator is sent to the laser electronics, to Box 3 (to initiate data acquisition in phase with the laser pulse) and, through manually adjustable phase delay circuits (in Box 1 and Box 2), to the phase locked loop (PLL) inputs of Alice's and Bob's arbitrary waveform generator cards.[9] The laser electronics (not shown on the diagram) consists of a step recovery diode circuit, which sharpens the falling edge of the 10 MHz signal from the EH129 generator, which has 500 ps fall time, and allows to obtain relatively short light pulses with 100 ps full width at half maximum (FWHM) from the laser. Also not shown on the diagram is a distribution buffer between the master clock generator and receivers of the master clock signal, which contains repeaters and a frequency divider for synchronization of the 10 MHz generators.

A typical transmission cycle consists of Alice and Bob loading the memory in their waveform generator cards with waveforms for the phase modulators. Then Bob generates the trigger signal, which simultaneously starts waveform generators in Alice's and Bob's cards, and detector data acquisition into the buffer memory in Box 3, all of which now proceeds automatically without software control. Alice and Bob simply wait 210 ms, after which the buffer memory is full and Bob can read and process a part of, or all its content.

The control software is written in LabVIEW with some C++ inserts to speed up processing large amount of data, namely reading and initial processing detector data from Box 3. The software loops through two parts: the phase adjustment routine (described in Section 2.3.) and the QKD routine. All intermediate data from these two routines, as well as the measured QBER, are displayed.

More details on the electronics and software, including a detailed electrical and optical interconnections diagram of the setup, can be found in Mikhail Chizhov's master thesis [84].

Although this electronics can be used, with some amount of trouble, for laboratory experiments, it would require several modifications for a production system. Firstly, the buffer memory in Box 3 should be made smarter: it should record only the bit slots where the detector has clicked (e.g., record slot numbers with clicks). Since most of the slots normally contain no clicks, this greatly reduces the amount of data Bob's PC has to read and process, easing the processor load. Secondly, random waveform generation for phase modulators must be made in hardware, the basis and bit values temporarily stored in a memory there, and only the basis and bit values where Bob's detector has registeres a click should be read from the memory of waveform generators into the PCs. This also eases the processor and I/O load. These two measures together would enable continuous operation of the system at the laser pulse rate we use (10 MHz) or at

[9] We could not get the National Instruments NI 5411 arbitrary waveform generator cards live up to their specification and synchronize reliably with the rest of the setup, despite having tried different modes of external synchronization of the cards. Only unreliable, intermittent synchronization was achieved, which hampered our experiments greatly. This appeared to be a problem with the card design.

a higher pulse rate. Without them in our impementation, we had to take a shortcut by generating 256-bit long pseudorandom waveforms for phase modulators in a loop, and processing the detector data in a time much longer than it takes to record it into the buffer memory in Box 3.[10]

Besides smarter electronics, a production system must have a separate channel for transmitting the 10 MHz clock and the trigger signal from Bob to Alice (in our setup the signals are carried by three 50 Ohm electrical cables, i.e. it is not yet suitable for a separate-locations experiment). The synchronization channel could use a separate optical fiber [55, 53, 29], or an optical signal that is wavelength division multiplexed into the same fiber that carries qubits [57, 31, 29].

2.2.3. Results of quantum key distribution

We initially tested the assembled interferometer spread on the optical table (Fig. 6) and measured fringe visibility at 1310 nm. The fringe visibility in both "0" and "1" time windows attained after adjustments of variable couplers was better than 0.96, and loss in Bob's part of the interferometer averaged over the "0" and "1" time windows was 4.2 dB. We have also tested several samples of different APDs and located a sample of FD312L Ge APD that had sufficiently low dark count probability ($5 \cdot 10^{-5}$ at 16% quantum efficiency) to run QKD over at least 20 km of single-mode fiber at a reasonably low average photon number at the output of Alice μ=0.2 (if we disregarded the PNS attack, see Section 4.2.1.). This looked sufficiently good.

However, to demonstrate QKD, a good amount of electronics and control software described in the previous section needed to be built around the interferometer. Also, we needed to mount the interferometer into portable boxes, and implement active phase tracking described in the next section before we could do QKD. In the meantime, we had started to use the setup for studies of practical security, and a mishap occurred during the large pulse attack experiment (see Section 4.3.1.). One of the phase modulators in the interferometer was irreparably damaged, as shown in Appendix A. The shifted focus of studies towards security, combined amount of work to complete the QKD system and this mishap put off the demonstration of QKD towards the end of author's stay in Trondheim, after some of the other results presented in this thesis had already been obtained. By the time we were ready to demonstrate QKD, it turned out both the optical scheme and the electronics had developed additional problems.[11]

[10] It takes 210 ms to fill the buffer memory. Our C++ routine calling a generic I/O memory range access driver for each byte takes about 30 s on a 400 MHz PC to read the entire memory. If we took the trouble of writing our own Windows driver that can directly access the I/O port, this time would probably be down to under 2 s. Programming I/O access certainly was simpler in the days of MS-DOS.

[11] Alice's part of the setup had acquired very high attenuation (as much as 51 dB: the suspected culprit was the variable delay line that had probably came out of alignment internally). This required adding a makeshift attenuator in the other arm, by winding PM fiber in the short arm at Alice on a mandrel with a low curvature radius. Still the interferometer remained barely controllable and unstable, not being able to attain the high fringe visibility initially measured. To make things worse, the 10 MHz pulse generator died (we had to replace it with another model) and Alice's NI 5411 DAC card began sporadically losing synchronization with the rest of the setup.

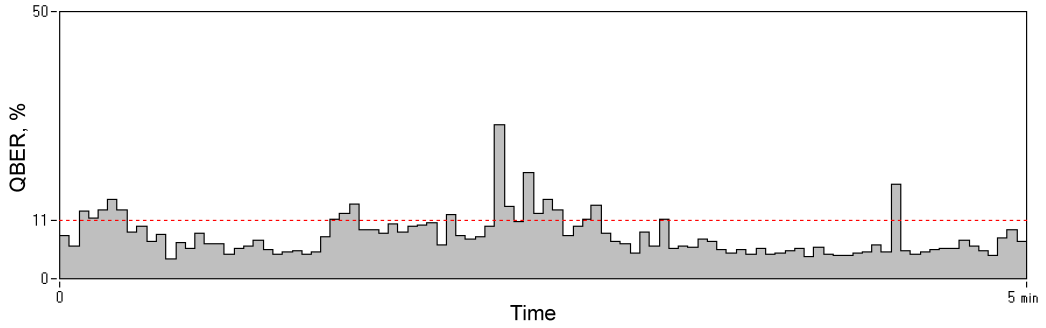


Fig. 11. QKD run no. 1. QBER vs. time. Each transmission cycle takes ca. 3 s; the chart shows 100 cycles.

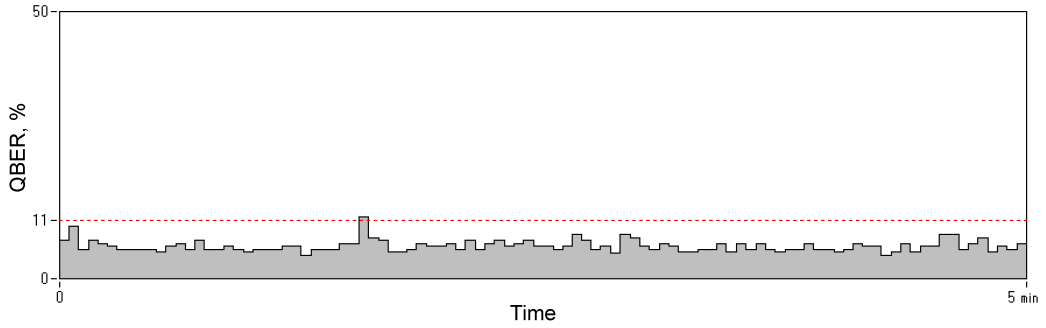


Fig. 12. QKD run no. 2. QBER vs. time. Each transmission cycle takes ca. 3 s; the chart shows 100 cycles.

In the little time left, we only managed to demonstrate operation with a rather high QBER and no communication line (i.e. Alice's setup connected to Bob's setup via a variable attenuator and a short five-meter optical cable), as described below.

Result of one of the best test runs with Alice connected directly to Bob is shown in Fig. 11. The best (lowest) QBER during the "calm" periods on the chart was about 4%. The peaks are due to an unstable 10 MHz pulse generator. Having replaced the pulse generator with yet another one, and having added a variable optical attenuator between Alice and Bob to simulate the loss in the communication line, we have made another test run (Fig. 12) which has shown an average value of QBER = 5.7%. Virtually all of the QBER on the charts is due to bad fringe visibility and intermittent problems with synchronization; detector dark counts only account for $QBER_{det} = 0.1\%$. In these tests, 256-bit long pseudorandom sequences in a loop were used for basis and bit values at Alice's and Bob's modulators. Key extraction in software was not implemented: we only had the sifting stage and the stage that compares the raw keys to calculate the QBER. Also, in these test runs, the average number of photons at the output of Alice was set to 5.1 photons/pulse, to make manual adjustments in the poorly controllable interferometer prior to the test run easier. Instead of afterpulse blocking (which in these tests was set to 0 blocked pulses), we implemented software-only afterpulse discarding,

with twenty bit pairs following every count discarded [85];[12] however we could not measure its effect on the QBER because the bad fringe visibility masked any other effect.

The number of problems with poorly behaving electronics and faulty components we have encountered on the way to demonstrate QKD, and incompleteness of our implementation show that we have underestimated the effort required to build a robust and complete QKD system. Also, the goal of the higher pulse rate turned out to be too much of a burden for a research lab. Among the experiments and theoretical studies presented in the thesis, the QKD demonstration experiment described in this section is the one where the author is the least happy with the results.

2.3. Phase control techniques

Our choice of optical scheme implied that in order to do QKD, active phase tracking and control must be employed. When we started implementing it, we realized that the task was in fact general to many QKD schemes. It might be especially actual for entanglement-based schemes (the first implementations of which had recently been demonstrated [76, 77, 78]) if they were to work over long distance and at the same time avoid heavy constructive phase stabilization measures. Additionally, efficient measurement of phase at low light level might be applicable outside the quantum communication domain, e.g., in optical measurements. We thus decided to study the phase tracking problem more thoroughly than would be needed just to get it solved in our setup.

This section consists of our paper published in the Journal of Applied Optics **43**, 4385–4392 (2004); figures numeration and references in the paper have been integrated with the rest of the thesis, otherwise the paper is equivalent to the published version sans language changes made by the journal copy editor.

After that, we discuss two assumptions that were taken for granted in the paper. One of these assumptions was not quite correct. In result, the required number of counts may increase by as much as +56% under certain conditions (namely, when QBER is not zero as assumed in the paper but approaches 10%).

[12] We came to the idea of afterpulse discarding independently of Yoshizawa and coworkers of Ref. 85.

Real-time phase tracking in single-photon interferometers

VADIM MAKAROV, ALEXEI BRYLEVSKI, and DAG R. HJELME

A new technique for phase tracking in quantum cryptography systems is proposed that adjusts phase in an optimal way, using only as few photon counts as necessary. We derive an upper bound on the number of photons that need to be registered during phase adjustment in order to achieve a given phase accuracy. It turns out that most quantum cryptosystems can successfully track phase on single-photon level, fully in software, without any additional hardware components and extensive phase stabilization measures. The technique is tested experimentally on a quantum cryptosystem.

OSIC codes: *030.5260, 040.5570, 060.5060, 120.5050, 270.1670.*

1. Introduction

Quantum key distribution systems (QKD systems) are the new generation of cryptographic systems. They transmit a random key securely over an optical fiber ("quantum channel"). This random key is then used for encryption and decryption of confidential information, which then can be sent in encrypted form over any non-protected communication channel. Over the last decade, quantum cryptosystems have been actively developed.

Most of the systems are based on fiber optic interferometers. An inevitable problem for these interferometers is the phase drift. The phase between the interferometers' arms has to be matched for transmission, in order for interference results to be controllable. If no special measures are taken during the assembly of interferometer, the relative phase between the two arms can drift rather quickly (e.g., 0.6 rad/min as reported in [24] or 2 rad/min in our experiment described later in this paper).

Just how much inaccuracy is acceptable in phase matching? The error probability is the ratio of error counts to the total number of counts. In an interferometric system, that would correspond to the lower part of the $\sin^2$ interference curve. Thus, the contribution of phase mismatch $\Delta\varphi$ to the quantum bit error rate (QBER) is

$$\mathrm{QBER}_{\mathrm{opt}\,\Delta\varphi} = \sin^2\left(\frac{\Delta\varphi}{2}\right),$$

which rises quadratically for small $\Delta\varphi$ (Fig. 13).

The key extraction algorithm can handle QBER up to a certain threshold value. This threshold value, according to some recent security analyses, is approximately 11% [86, 16, 87]. The larger the QBER, the bigger part of the key has to be discarded during key extraction, leaving us with lower key exchange rate, which approaches zero as QBER approaches 11%. QBER value of 11% could be caused by 38° phase mismatch if it were the only error source.

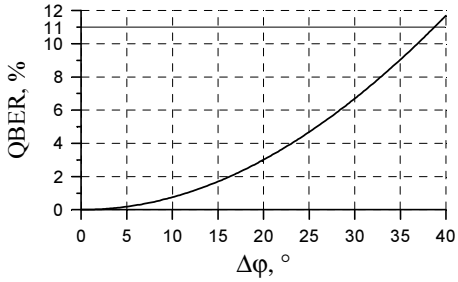


Fig. 13. QBER vs. interferometer phase mismatch in absence of other error sources.

In real systems, other sources of error as well as $QBER_{opt\ \Delta\varphi}$ contribute to the total QBER. Some of these other sources of error (e.g., detector dark counts) are much harder to control than phase accuracy. We therefore want to keep $QBER_{opt\ \Delta\varphi}$ within about one percent (less if possible), to minimize its impact on the key exchange rate. This translates into a required phase accuracy of 10° or better.

2. Existing solutions

There are three known ways to deal with phase drift:

(1) "Plug & play" interferometer configuration (round-trip light propagation, auto-compensating).
(2) Strict thermo- and mechanical isolation (slows down phase drift).
(3) Periodical switching to bright light regime for active phase tracking.

(1) "Plug & play" system presents an elegant solution both for polarization fluctuations and for phase drift. In this approach, light pulses travel from Bob to Alice, get reflected by a Faraday mirror and then travel back to Bob: this automatically compensates for all polarization fluctuations in the transmission channel [59, 60]. The two interfering pulses also follow exactly the same path in Alice's and Bob's interferometers, albeit in different directions: this automatically compensates for phase drift, eliminating the need for active adjustments [88]. A system of this type is easier to develop into a product than the other quantum cryptosystems, and is the first one being deployed commercially [63, 47].

Unfortunately, "plug & play" configuration has limitations, which stem from bidirectional light propagation:

- This configuration can only be used for QKD with faint laser pulses and with modulators in Alice's and Bob's setups. There are no "plug & play" configurations for entangled-pair-based schemes.
- The system is difficult to protect from external interrogation attacks ("Trojan horse" attacks), and it appears to be more vulnerable to implementation attacks [89].
- It has a penalty factor of ~3 in the key generation rate comparing to an equivalent non-plug and play configuration, because one cannot let light pulses propagate in opposite directions in the transmission channel at the same time, due to Rayleigh backscattering from bright pulses. Pulses have to be transmitted

in batches with pauses between them, and a fiber delay line in Alice's setup employed [90].

(2) Passive measures like thermo- and mechanical isolation can, if done properly, keep phase sufficiently stable without adjustment for several hours. This is enough for many laboratory experiments, where initial adjustment or calibration is performed manually and is followed by a test run of limited duration. The phase, however, eventually drifts away. In a production system, automatic phase tracking would always be needed.

For example, the group in Geneva took careful measures to stabilize their interferometers, so that experimental tests could be performed without continuous phase tracking. They keep interferometer arms reasonably short, few tens of centimeters [76, 91]. Their bulk optics interferometer is built on a base made of material with low thermal expansion coefficient, and is thermoisolated well [50]. When it comes to fiber optics interferometers, they are packed into sand-filled copper tubes and are actively thermostabilized at a constant temperature, by incorporating a heater and temperature sensor into the assembly [92].

In another example, the EQUIS project aims at manufacturing Alice's and Bob's interferometers as integrated planar silica waveguide structures [93]. These devices are inherently more stable owing to their small size and monolithic construction. Each of them is thermostabilized by a thermoelectric heater/cooler, and the phase is reported to be "very stable" [54].

Thermostabilization can also be used to track phase if the heater/cooler is included into a feedback loop. It has an obvious disadvantage of very long (hours) warm-up time [76]; moreover, it also takes long time to stabilize the phase after any mechanical or thermal impact on the system.

(3) For rapid phase tracking, Townsend used two additional components to perform phase adjustment: a piezoelectric transducer to adjust the length of one of the arms of Alice's interferometer, and an electrically switched attenuator [24]. The adjustment was performed by switching to low attenuation and scanning the phase by piezoelectric transducer until the photon count rate at one of the Bob's output ports was minimized. The thermal phase drift rate reported by Townsend was ~0.6 rad/s.

Although it is possible to achieve very slow phase drift rates by constructive measures, they make production more expensive, and can also add bulk and weight to the equipment. It would be of advantage if standard fiber optic assembly technology could be used, with standard splicing equipment, no severe restrictions on the length of fiber pigtails, and possibly with only light foam insulation around the assembled interferometer. Such an interferometer exhibits rather fast phase drift and makes it necessary to adjust phase every few seconds, like in Townsend's setup [24]; the phase adjustment itself should therefore be quick. There is, however, a problem of achieving desired phase accuracy in a short time: existing quantum cryptosystems generate limited count rates at the detectors during normal operation (typically a few thousand counts per second), and statistical noise is significant.

For faint pulse systems that contain a laser and a strong attenuator, one can use an electrically switched attenuator to temporarily increase count rates during phase adjustment as in [24]. This extra optical component, however, adds cost and lowers

reliability (the system does need to employ some kind of adjustable attenuator to set the mean photon number at the time of installation, but it need not be fast nor even electrically-controlled). It should also be possible to electrically control the energy of the laser pulse (by changing its brightness and/or duration), but we are not aware of any tests of this technique in quantum cryptosystems.

Most importantly, for systems based on single-photon and photon pair sources (e.g., parametric downconversion sources) increasing light output of the source can be impractical or impossible.

We therefore decided to find a technique that does not require any extra components and performs phase adjustment fully in software, at single-photon level, utilizing only as few detector counts as necessary to achieve required phase accuracy.

The research that comes closest to this idea is the experiment at Los Alamos National Laboratory. They suggested deriving the feedback signal for phase tracking from key data ("from the key error rate and key bias") [28]. However, no further details have been published, to our knowledge. Their interferometer contains PZT-driven air gaps to control the phase, both on Alice's and Bob's side. The published experimental results hint at constructive isolation as well: phase appears to be stable without adjustment over time span of 10 minutes, and the interferometer boxes are quite bulky.

3. Phase tracking algorithm

The quantum key distribution setup we consider consists of Mach-Zehnder interferometer with a phase modulator in each arm. The phase modulator in one arm resides on Alice's side, and phase modulator in another arm resides on Bob's side. Single-photon detector(s) reside on Bob's side. For more details we refer the reader to Section 4 and to [24, 94].

For the whole duration of adjustment, Alice sets her phase modulator to zero (0 V) and transmits photons as usual. Only Bob's phase modulator is used.

The software phase tracking algorithm we devised consists of two stages; stage 1 for rough phase adjustment, and stage 2 for fine phase compensation.

Stage 1. Rough phase compensation.

In this stage, Bob scans the whole phase range (0° to 360°) in a small number of steps using his modulator, and records the number of detector counts collected at each step by "0" and "1" photon detectors (or in "0" and "1" detector time slots if only one photon detector is used in the system). He then notes the phase settings of his modulator at which the smallest number of counts occurred in "0" detector time slot and "1" detector time slot, respectively. The value of this phase setting for "1" time slot can be either less or greater than the value of phase setting for "0" time slot, depending on the position of the interference curves in the scanning range. In the former case, we add 180° to the value of phase setting for "1" time slot; the latter case, we subtract 180° from the value of phase setting for "1" time slot. After this, we calculate an average of the values for "0" and "1" time slots, which improves accuracy. This is assumed to be the "roughly determined phase compensation", φ_0.

This scan allows Bob to quickly determine the position of minima of interference curves with an accuracy of 20–30°. Further improvement of precision requires a differ-

ent method, because the $\sin^2$-shaped interference curves are both flat and have the highest relative statistical fluctuations near their minima. To get the best accuracy in a given counting time, we propose to count photons at the points on the interference curves where they have the maximum slope-to-statistical-deviation ratio. To the first approximation, these points are $\varphi_0+90°$ and $\varphi_0-90°$. We do this counting in stage 2.

The purpose of stage 1 is to quickly provide a rough estimate of these points. However, stage 1 need not be repeated on subsequent runs of phase adjustment if it is known that the phase has not deviated much. This can be inferred from successful key exchange immediately prior to the phase adjustment, or guaranteed by the time since the last run combined with the fastest estimated drift rate.

Stage 2. Fine phase compensation.

In this stage, Bob switches his modulator between $\varphi_0+90°$ and $\varphi_0-90°$ in a symmetric square-wave pattern, and records the number of photon counts at each phase setting. This results in four count values:

N_{0+} – the number of photons detected at $\varphi_0+90°$ phase setting in "0" time slot;
N_{0-} – the number of photons detected at $\varphi_0-90°$ phase setting in "0" time slot;
N_{1+} – the number of photons detected at $\varphi_0+90°$ phase setting in "1" time slot;
N_{1-} – the number of photons detected at $\varphi_0-90°$ phase setting in "1" time slot.

On Fig. 14, Function 0 is our assumption of the position of the interference curve $N(\varphi)$ after performing the first stage of phase adjustment, with the minimum at φ_0. Function 1 is a more accurate position of the interference curve $N(\varphi)$, with the minimum at φ_1, which is unknown to us at this point.

$$\text{Function 0:}\quad \mathrm{N} = \left(N_{\max} - N_{\min}\right)\sin^2\left(\frac{\varphi-\varphi_0}{2}\right) + N_{\min}$$

$$\text{Function 1:}\quad \mathrm{N} = \left(N_{\max} - N_{\min}\right)\sin^2\left(\frac{\varphi-(\varphi_0+\delta)}{2}\right) + N_{\min}$$

$$\delta = \varphi_1 - \varphi_0$$

Using the equations above, one can derive correction δ as a function of N_{0+}, N_{0-}, N_{1+}, N_{1-}, $N_{\min}$ and $N_{\max}$ (for full derivation, see [83]). $N_{\min}$ and $N_{\max}$ can be actually different for "0" and "1" time slots, so we split them into $N_{\min 0}$, $N_{\min 1}$, $N_{\max 0}$, and $N_{\max 1}$. The correction becomes

$$\delta = \frac{1}{4}\left[\arccos\left(2\frac{N_{\min 0}-N_{0+}}{N_{\max 0}-N_{\min 0}}+1\right) - \arccos\left(2\frac{N_{\min 0}-N_{0-}}{N_{\max 0}-N_{\min 0}}+1\right)\right.$$
$$\left. + \arccos\left(2\frac{N_{\min 1}-N_{1-}}{N_{\max 1}-N_{\min 1}}+1\right) - \arccos\left(2\frac{N_{\min 1}-N_{1+}}{N_{\max 1}-N_{\min 1}}+1\right)\right]. \qquad (1)$$

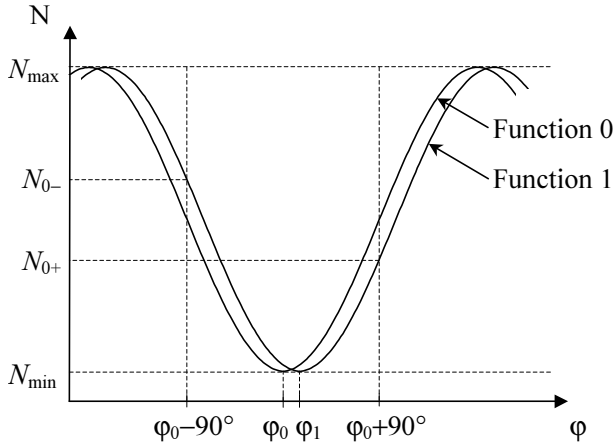


Fig. 14. Illustration of phase adjustment at stage 2. Only the interference curve for "0" time slot is shown.

In the experiment, we assumed $N_{min0}=N_{min1}=0$, $N_{max0}=N_{0+}+N_{0-}$ and $N_{max1}=N_{1+}+N_{1-}$. N_{min0} and N_{min1} are in practice non-zero, due to imperfect fringe visibility and detector dark counts. They could be estimated more precisely should it be necessary.

The resulting correction δ is added to φ_0 to get the more accurate value of phase compensation, φ_1. The voltage corresponding to φ_1 is applied as an offset voltage to Bob's phase modulator during the key transmission session that follows phase adjustment.

There will be some random error in φ_1, due to statistical fluctuations in the number of counts N_{0+}, N_{0-}, N_{1+}, N_{1-}. We can calculate how many counts need to be collected in order to achieve a given phase accuracy with a certain probability.

The interference curve is given by

$$\mathrm{N} = \left(N_{\max} - N_{\min}\right)\sin^2\left(\frac{\varphi - \varphi_1}{2}\right) + N_{\min},$$

such that

$$\frac{\mathrm{dN}}{\mathrm{d}\varphi} = \frac{1}{2}\left(N_{\max} - N_{\min}\right)\sin\left(\varphi - \varphi_1\right)$$

Thus, at our ±90° counting points the slope of interference curve approximately is

$$\frac{\Delta \mathrm{N}}{\Delta\varphi} = \frac{1}{2}\left(N_{\max} - N_{\min}\right). \qquad (2)$$

N obeys Poisson distribution, which approaches Gaussian distribution for the relatively

large mean number of counts involved. Assuming $N_{\min}=0$ and $N=\frac{N_{\max}}{2}$, the statistical error level ΔN follows as

$$\Delta N = k\sigma = k\sqrt{\frac{N_{\max}}{2}}, \tag{3}$$

where σ is the standard deviation and k is the number of standard deviations corresponding to a given probability of the actual number of counts falling within $(N-\Delta N, N+\Delta N)$. Combining Eqs. (2) and (3), we obtain

$$N_{\max} = 2\frac{k^2}{\Delta\varphi^2}.$$

Assuming $N_{\max}=N_{0+}+N_{0-}$, we have

$$N_{0+} + N_{0-} = 2\frac{k^2}{\Delta\varphi^2}. \tag{4}$$

This is the number of counts needed to achieve phase error of $\Delta\varphi$ or less, where the probability of not exceeding this phase error is set by the number of standard deviations k. Actually, we are collecting counts in both detection windows, not in just one, and obtain phase correction by averaging over all four count values according to Eq. (1). Averaging works in such a way that the same right-hand side of Eq. (4) would then estimate the total number of counts

$$N_{0+} + N_{0-} + N_{1+} + N_{1-} = 2\frac{k^2}{\Delta\varphi^2}. \tag{5}$$

For example, to achieve our goal of 10° or better accuracy in, say, 95% of the phase adjustment attempts (k=2), it would suffice to register approximately

$$N_{0+} + N_{0-} + N_{1+} + N_{1-} = 2\frac{2^2}{\left(\frac{10^\circ}{180^\circ}\pi\right)^2} = 262 \text{ counts} \tag{6}$$

in stage 2 of phase adjustment. We have also determined empirically that stage 1 requires fewer counts than stage 2 (this is illustrated later).

Equation (5) provides an upper bound estimate for the number of counts required. Whether a more count-efficient phase adjustment algorithm exists, remains an open question.

Using the estimate given in Eq. (6), one could check if a quantum cryptosystem can function with software-only phase tracking, or it needs one of the additional measures

reviewed in Section 2. To do the check, we need to know the fastest phase drift rate in the interferometer, and the lowest photon counting rate possible in the specified range of operating conditions in which the system will be used. The operating conditions that affect phase drift rate will be the environment in which the end equipment is installed (temperature, humidity, vibration etc.). The operating condition that determines the photon counting rate will primarily be the line attenuation (currently limited by the dark count rate of the detectors). Knowing these two rates, one can check how far the phase can drift during the time required to collect ca. 200 counts. If the phase drifts away by significantly less than 10° during that time, it can be tracked easily using only periodic phase adjustment described in this paper; only a fraction of the channel time would be spent on phase tracking, leaving most of the channel capacity to QKD. If, however, the phase drifts away by more than 10°, additional hardware measures are needed to slow down phase drift and/or speed up phase adjustment. This is just a rule of thumb. If the actual drift rate falls close to this figure, the necessity of hardware measures would depend on the exact design of the system, tradeoffs and reliability margins; discussing this gray zone is beyond the scope of this paper.

4. Experiment

We have tested the phase adjustment algorithm on our QKD setup.

A. Experimental setup

The QKD setup uses time- and polarization-multiplexed Mach-Zehnder interferometer (general scheme first proposed by Townsend et al. in [94]) and BB84 protocol [13]. The optical scheme is shown on Fig. 15.

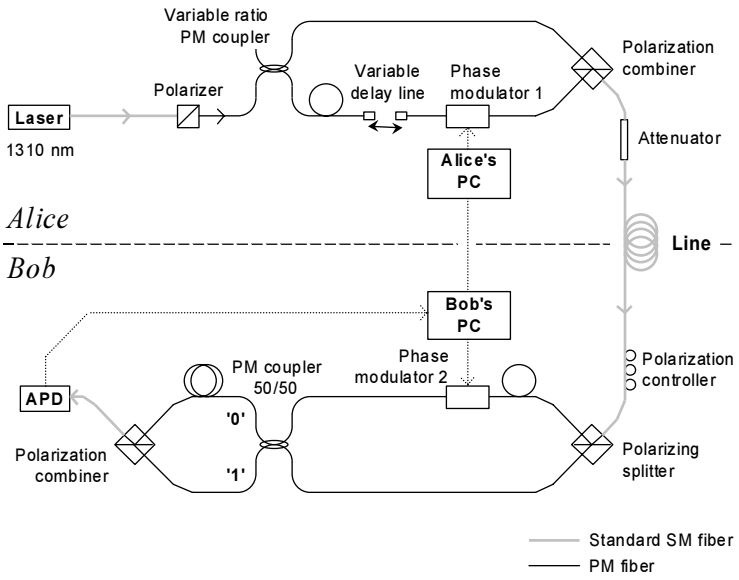


Fig. 15. QKD setup.

100 ps-wide light pulses are emitted by a 1310 nm semiconductor laser at 10 MHz rate. The arms of the interferometer are made from polarization-maintaining (PM) fiber (Fujikura PANDA fiber); everything is aligned such that light propagates in the slow-axis mode of PM fiber. One arm of the interferometer in Alice's setup is ~2 m long whereas the other arm is ~6 m long; the arms in Bob's setup are also ~6 m and ~2 m long. The phase modulators are of lithium niobate planar-waveguide type (Alenia Marconi-made at Alice's side and Uniphase-made at Bob's side); they only pass one polarization. The phase modulators have half-wave voltage of several volts and are each controlled by a high-speed DAC card. The pulses from the two arms of interferometer have orthogonal polarization in the line and are also separated by time. Polarization controller restores the polarization state of the pulses after the line so that they split into two arms properly. Imperfect adjustment of this polarization controller and small polarization fluctuations in the line should neither affect phase tracking nor QKD, because if a part of the pulse is split into the wrong arm, the wrongly split part arrives at the detector outside its detection windows, and because phase tracking is not sensitive to fluctuations in absolute light level.

Alice's and Bob's setups are mounted onto an aluminium plate (Fig. 16) and covered with thermoisolation. As it turned out, this kind of construction exhibits phase drift rate of up to 2 rad/min when left at rest in normal indoor conditions (in an optical lab).

The APD is gated at 20 MHz. This relatively high gating frequency is made possible by the use of afterpulse blocking technique [95]. Data from the APD is buffered in a 4 Mbit FIFO memory before it is read into Bob's PC. We use Soviet-made Ge APD (standard part number FD312L, developed by NPO Orion), placed inside a liquid nitrogen tank. The best APD sample we have has $5 \cdot 10^{-5}$ dark count probability at 16% quantum efficiency. Given 4.2 dB measured loss in Bob's optical setup, 0.5 dB/km losses in fiber at 1310 nm, acceptable contribution of detector dark counts

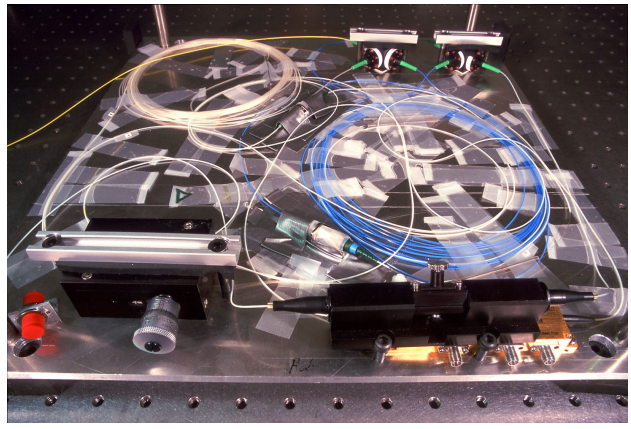


Fig. 16. Bob's interferometer. All components are mounted on a 400x400x6 mm aluminium plate, and their fiber pigtails are affixed to the plate surface with pieces of adhesive tape. Everything is covered by custom-cut pieces of foam insulation (not shown on the photo) and mounted inside a box. Alice's interferometer is similar.

to the bit error rate $QBER_{det}$ of, say, 4%, and mean photon number per pulse at Alice's output μ=0.2, the APD we have would allow for about 20 km long QKD link.

With the APD we have, the photon counting rate in the system at the longest possible link length would be no less than 5000 counts per second (at which rate $QBER_{det}$ would closely approach 11%). The 200 counts required for a phase adjustment would be accumulated in at most 40 ms. Given the fastest phase drift rate measured, a drift of up to 0.08° can occur in this time. Thus, according to the criterion given in the end of Section. 3, the system is well suited to software-only phase tracking. $QBER_{opt\ \Delta\varphi}$ and time spent on phase adjustment would not reduce the key generation rate much.

At the time of phase tracking experiment, our system was not ready for demonstrating QKD (most notably due to poor fringe visibility of about 0.8, which has since been improved to 0.92, and due to faulty Alice's DAC card). However, this has not affected the phase tracking algorithm, which we have successfully tested.

B. Results for phase tracking

In our tests, phase adjustment is performed every 3 seconds, which corresponds to phase drift of up to 6° between adjustments. The data is captured into the FIFO memory in less than 40ms, but processing them actually takes much longer than that, because readout from the memory and other operations are slow due to inefficient software (mostly written in LabVIEW for the purposes of the experiment). To reduce readout time, μ has been increased to 0.37 and no transmission line is used (i.e. Alice connected straight to Bob). This should not affect test results for phase tracking, however.

In the first test run, we performed both stage 1 and stage 2 phase adjustment each time, using rough phase compensation φ_0 from stage 1 as a starting point for stage 2. Fig. 17 shows typical data collected in stage 1. Statistical noise at such a low average number of counts yields wildly varying shapes, which are hardly recognizable as interference curves at the first look. If we collected much more counts on stage 1, we would indeed see nice sine- and cosine-shaped curves. However, even this noisy data allows reliable determination of φ_0 with accuracy of 20–30°, as the upper graph in Fig. 18 illustrates. φ_0 is then used as input to stage 2. Results of stage 2 are shown on the lower graph in Fig. 18. The graph is less noisy and shows that stage 2 works well with this input data.

In fact, stage 1 is not very important and is treated here in such detail only to study the whole problem better. In a properly working system, one can always take the phase compensation from the previous phase adjustment and use it as input to stage 2. This is what we did on the second test run, illustrated in Fig. 19.

Judging from the width of noise trace on Fig. 19, the goal of "10° or better phase accuracy most of the time" is achieved. It is not possible to assess statistical fluctuations quantitatively, because in this experiment we do not know the underlying phase drift with a better accuracy. However, the smoother parts of the curve suggest that the level of statistical fluctuations is close to what is expected in our phase tracking algorithm. To quantify the error level accurately, we would need to run a control phase measurement in parallel, which is what our setup is not equipped to do. It would be also possible to confirm the performance of phase tracking by the results of QKD if

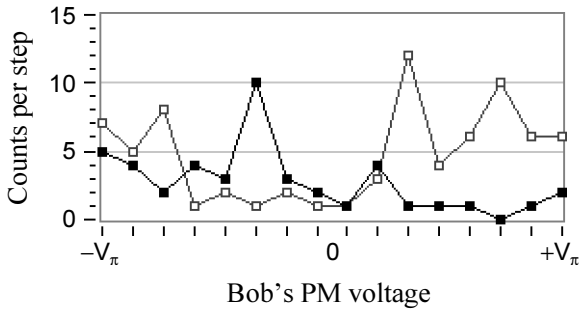


Fig. 17. Interference curves for "0" and "1" time slots, plotted from data measured in a single run of stage 1 phase adjustment. The 2π phase range was scanned in 16 steps, and on average 150 counts were collected on stage 1. Curve with solid points is for "0" time slot and curve with hollow points is for "1" time slot.

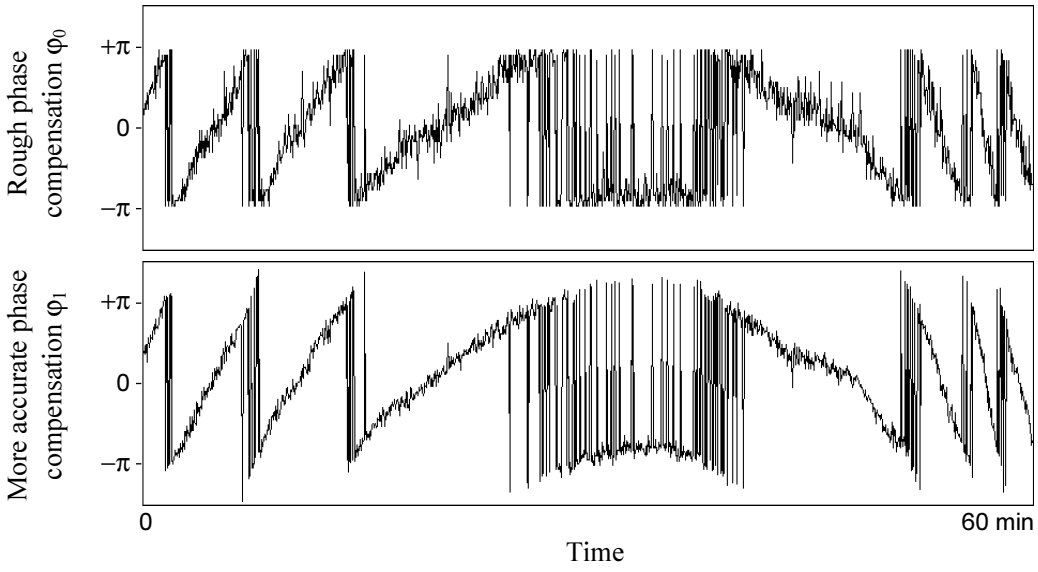


Fig. 18. Voltage on Bob's phase modulator, scaled to the equivalent phase shift. A one-hour fragment of phase tracking data from a test run with both stage 1 and stage 2 phase adjustment performed each time. Phase adjustment is run every 3 seconds; the average number of counts collected in stage 1 is 150, and in stage 2 – 230. Vertical hops on the graphs do not represent any phase discontinuity (phase is cyclic over 2π), but do represent jumps in phase modulator voltage, because we had to stay within the voltage range of our phase modulators limited to just over $\pm V_\pi$. If we neglected jumps in phase modulator voltage and printed cylindrically-shaped graphs for phase, there would be no hops on them.

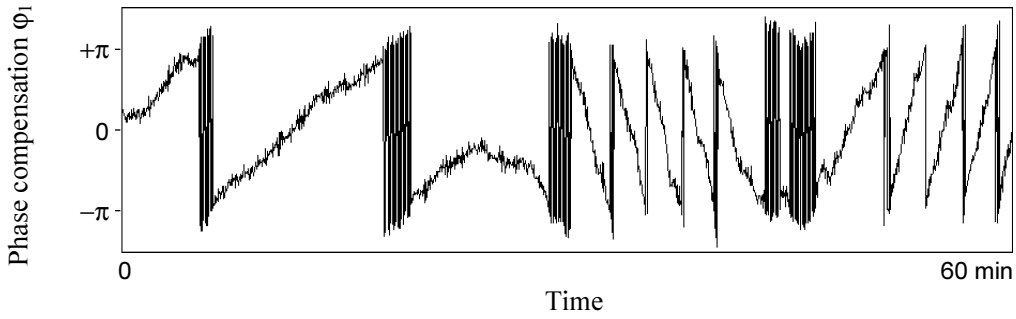


Fig. 19. Voltage on Bob's phase modulator, scaled to the equivalent phase shift. A one-hour fragment of phase tracking data from a test run with only stage 2 of the phase adjustment performed each time. Phase compensation from previous phase adjustment is used as input to stage 2. Phase adjustment is run every 3 seconds, and the average number of counts is 230 for each adjustment.

$QBER_{opt\ \Delta\varphi}$ were a mayor contribution to the total QBER (which is not the case with our setup: the contribution due to poor fringe visibility would dominate, masking $QBER_{opt\ \Delta\varphi}$).

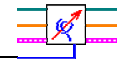
Looking at the graphs, it is easily noted that phase drift in our interferometer is not entirely random, but mostly occurs with slowly changing rate. This may allow us to further reduce the number of counts required for phase adjustment, i.e. do better than Eq. (5), because the phase could be partly predicted by extrapolating recent tracking data.

5. Conclusion

The phase adjustment technique described in this paper tracks phase drift in interferometers at low light levels, typical for single-photon applications. This gives the designer of a quantum cryptography system new degrees of freedom. Using these results, one can accurately estimate requirements for successful phase tracking. In most cases, it is possible to construct interferometers without heavy thermoisolation and without additional components like fast electrically controlled variable attenuator, at the cost of some programming. In effect, expensive hardware measures are replaced by software.

We hope that this work will ease the development of advanced and more secure types of quantum cryptosystems into commercial products.

[End of included paper]



On choice of points for stage 2 of phase tracking algorithm

In the paper we wrote: "To get the best accuracy in a given counting time, we propose to count photons at the points on the interference curves where they have the maximum slope-to-statistical-deviation ratio. To the first approximation, these points are φ_0+90° and φ_0–90°." Let's show that this assumption is correct.

The slope of the interference curves for the "0" and "1" detectors (assuming symmetrical curves for both detectors) depends on phase φ as

$$\begin{aligned} S_0 &= \frac{d}{d\varphi}\left[(1-2e)\sin^2(\varphi/2)+e\right] = S_1 = \frac{d}{d\varphi}\left[(1-2e)\cos^2(\varphi/2)+e\right] \\ &= \frac{(1-2e)\sin\varphi}{2} \propto (1-2e)\sin\varphi, \end{aligned} \tag{7}$$

where e is a parameter that depends on the fringe visibility and detector dark count level and shows how far the lowest ponts on the curve are from zero. The parameter e is chosen to be equivalent to QBER in the case when imperfect fringe visibility and detector dark counts are the only contributions to QBER (which is nearly always so in the absence of eavesdropping). Let's call e the base level. A typical QKD setup will work at the values of e ranging from less than two percent (at short distances and with good optical alignment) to around 10% at the distance limit.

The statistical deviations (in approximation of Gaussian distribution) depend on phase as

$$\begin{aligned} D_0 &= \sqrt{\langle N_0(\varphi)\rangle} \propto \sqrt{(1-2e)\sin^2(\varphi/2)+e} \\ D_1 &= \sqrt{\langle N_1(\varphi)\rangle} \propto \sqrt{(1-2e)\cos^2(\varphi/2)+e}. \end{aligned} \tag{8}$$

It can be shown that, if we have two channels carrying the same useful signal with amplitudes S_0 and S_1 mixed with statistically independent Gaussian noise with root-mean-square amplitudes D_0 and D_1 respectively, these two channels can be added together with weights m/S_0 and $(1-m)/S_1$, where

$$m = \frac{1}{\left(\frac{D_0}{S_0}\frac{S_1}{D_1}\right)^2 + 1}, \tag{9}$$

in order to obtain a single channel with the best signal to noise ratio. Our two interference curves present the same situation: they have the slope, which directly translates to the amplitude of the useful error signal, and different statistical deviations (i.e. noise). The *effective* slope-to-statistical-deviation ratio after summing as described above is

$$\frac{S_{\text{eff}}}{D} \propto \frac{S_0}{D_0}\frac{S_1}{D_1}\sqrt{\left(\frac{D_0}{S_0}\right)^2 + \left(\frac{D_1}{S_1}\right)^2} = \frac{(1-2e)\sin\varphi}{\sqrt{\frac{(1-2e)^2}{4}\sin^2\varphi + e(1-e)}}. \tag{10}$$

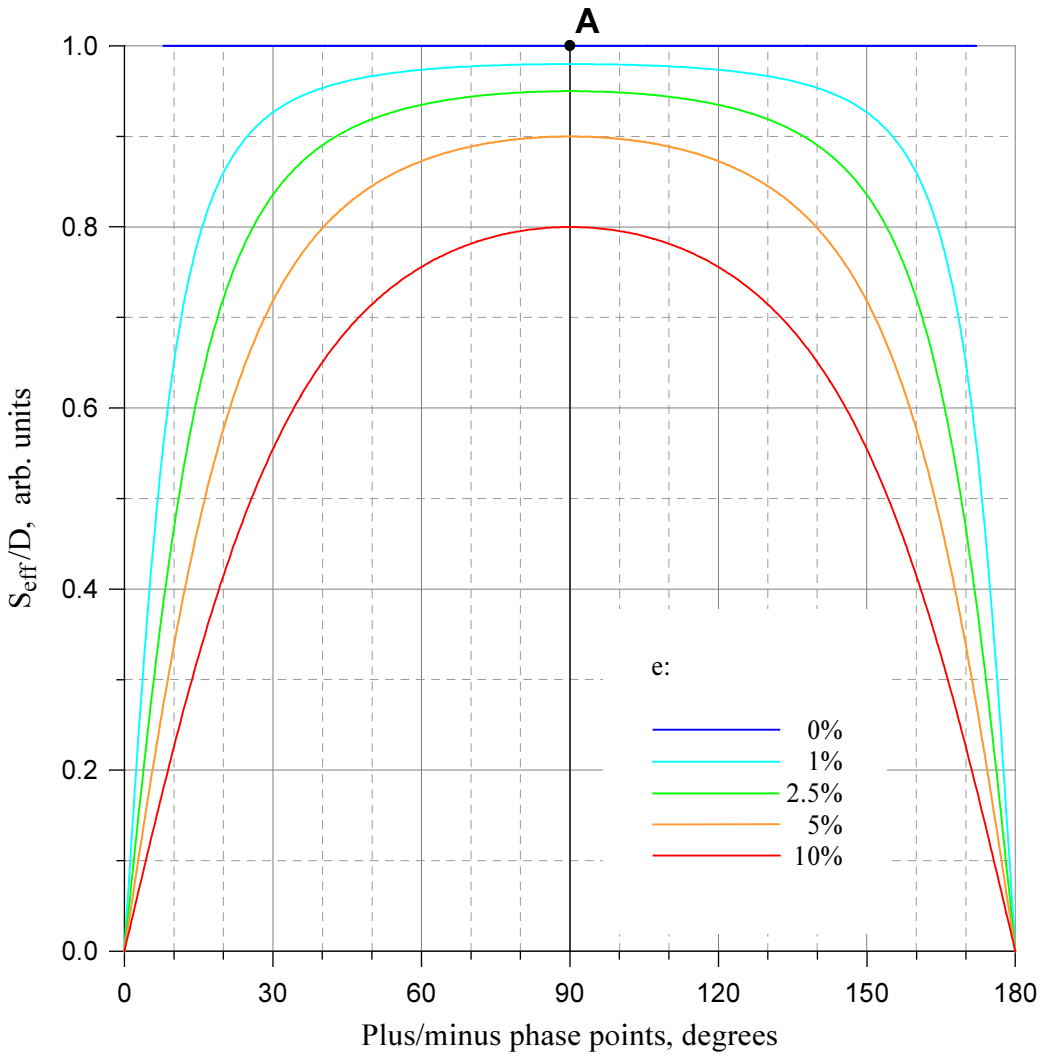


Fig. 20. Effective slope to statistical deviation ratio S_{eff}/D as a function of φ (Eq. 10) plotted for several values of base level *e* typical for quantum cryptography setups (*e*=0.01 (1%) to *e*=0.1 (10%)) as well as for *e*=0. Note that the Gaussian approximation assumed in the derivation may not hold near 0° and 180° for the *e*=0 curve.
A: point used for all derivations in the above paper.

Let's plot S_{eff}/D as a function of φ for several values of the base level *e* (Fig. 20). We see that for non-zero values of *e*, the best S_{eff}/D is actually achieved at the chosen ±90° points, so the assumption in the paper is correct.[13]

[13] Only S_{eff}/D peaks at ±90°. S_0/D_0 and S_1/D_1, i.e., the slope-to-statistical-deviation ratios for individual interference curves (not plotted), peak at phase points less than ±90° off the minimum of each interference curve; however, their values are always lower than the peak value of S_{eff}/D.

Effect of non-zero QBER on required number of counts

In the paper, the assumption of $N_{\min}=0$ was made when deriving Eqs. (3)–(6). In fact, $N_{\min}>0$, i.e. $e=\mathrm{QBER}>0$, leads to gentler slope of the interference curves, so more counts need to be collected in stage 2 to achieve the same phase accuracy. Figure 20 can be used to estimate the difference. The point marked **A** corresponds to the S/D ratio used in the paper. The actual S/D ratio depends on e and is in practice lower (see where the curves cross the 90° vertical line). To obtain the actual number of counts required, the right hand side of Eqs. (5) and (6) should be multiplied by the factor of

$$\left(\frac{\text{S/D for } e=0}{\text{S/D for a given } e>0}\right)^2=\left(\frac{1}{1-2\cdot\mathrm{QBER}}\right)^2. \tag{11}$$

This factor can be as large as 1.56 for systems working around their distance limit (i.e., at QBER=10%). This correction is sufficiently large and must be taken into account.

Using data discarded during sifting for phase tracking

One may notice that the key bits discarded by Alice and Bob on the sifting stage (i.e. those bits detected by Bob in a basis incompatible with Alice) could be used for phase tracking. Indeed, these Bob's detections are at the ±90° points from the extrema of the interference curves. Perhaps this is what Hughes and coworkers have meant in Ref. 28. However, this would require Alice to divulge her bit values for these bits to Bob (and to Eve) over the public channel. One should be very careful to see if such a disclosure fits well with the general security proof. This remains an open question. If it can't be shown that the security proof holds in such a case, then the phase adjustment must be performed separately from key generation.

2.4. Conclusion

In this chapter, the design of an interferometric fiber optic QKD system and results of QKD experiments have been presented. We have successfully developed and demonstrated an optimal phase tracking technique for the interferometer that works in the single photon mode and keeps the phase error within ±10° when acquiring approximately 200 photon counts per cycle of adjustment. The results of QKD demonstration have been poor, limited by unfixed problems in equipment. QBER values of 4 and 5.7% have been measured in two test runs conducted without a real communication line.

It is interesting to note that we have seemingly been the first to use PM fiber in a QKD setup. Later, PM fiber has also been used in Geneva group's "plug and play" setup [62, 63].

Regarding phase tracking, several other groups have implemented active phase tracking in some form [e.g., 57, 55]. We do not know yet if anybody benefits from our optimal calculation. Anyway, it has been interesting to find a possible fundamental limit on phase tracking performance. In the future, transmission distances for QKD will keep getting longer (and the line attenuation higher), so our results would hopefully be useful some day.

Trying to build a working QKD system from scratch has been an educating experience. If the author had to do it again, he would set different priorities and obtain publishable results quicker. However, this part of our research project has stimulated other directions of research. A single photon detector with afterpulse blocking developed for the QKD system is described in the next chapter. The focus of our studies has gradually shifted towards security, where the author thinks we have got our most interesting results, explored in Chapter 4.

3. Single photon detection

The ability to detect single quanta of light at the wavelength of interest plays a critical role in quantum communication systems. In QKD, characteristics of detectors determine such vital parameters as the longest transmission distance and the key generation rate. QKD requires detectors working in the transmission windows of telecommunication fiber (1300 nm and 1550 nm) for long-distance communication, and also in the 600–850 nm range for detection of entangled photons inside Alice's setup and for use in free space communication channels.

We have implemented a gated APD-based SPD for the 1300 nm and 1550 nm transmission windows. Our detector has been the first to include an afterpulse blocking technique that allows to increase the gating rate beyond the limitations imposed by the afterpulsing effect in APDs. The detector and test results are described later in Sections 3.2. and 3.3. The original contribution by the author is the afterpulse blocking technique and its implementation, described at the end of the chapter in Section 3.3.

Although APD-based SPDs remain the most practical and universally used, several other types of SPDs with superior characteristics have been developed, especially in the recent years. It is important to keep track of new developments in this area, both from the perspective of possible improvements in quantum communication and computation experiments resulting from the use of better detectors, and from the perspective of illustrating possibilities accessible to Eve today. Different types of SPDs are briefly reviewed below, ending with a comparison table on p. 62, before we present our APD-based detector.

3.1. Review of single photon detection techniques for visible and near IR light

The eye

Like many things man tries to construct, single photon detectors exist in nature: they have evolved in living beings. For example, rods in dark-adapted retina of vertebrates function in photon counting mode, each rod producing a current pulse after absorbing a photon [96, 97, 98, 99, 100, 101, 102]. Humans require detection of 5–8 photons in different rods to become consciously aware of a weak flash of light (which corresponds to ca. 100 photons entering the pupil) [96]. For other animals, such as toad, this threshold might be lower [98]. Since the response is invoked by discrete detection events, photon statistics of incident light plays a role, producing a distinct effect when super-Poissonian light is used in an experiment [102]. The sensitivity of vision (and how the signals from photoreceptors are processed by the nervous system) appears to be limited by the dark count level. The dark count level is primarily determined by the rate of random thermal isomerization, indistinguishible from photoisemerization, of rhodopsin molecules in rods [98, 99, 100]. The exact inner workings of the rod are not fully known. Curiously, modern human-made single photon detectors

for visible light around 500 nm wavelength working at non-cryogenic temperatures have much higher dark count rates than that of a single rod. A rod produces on average one dark count per several tens of seconds [99, 101].

No use of animals in QKD setups has been reported. There are at least eleven different types of artificial devices that allow us to do single photon counting.

Geiger-Müller counter

The first single photon detector sensitive to visible light was probably the one developed by G.L. Locher in 1932 [103]. It employed a Geiger-Müller gas-filled tube with photosensitive cathode coated with an alkali or alkaline earth metal (several metals were tried: Na, K, Cs, Sr). The Geiger-Müller tube was connected to a three-stage vacuum tube amplifier followed by an oscilloscope, a loudspeaker, or a mechanical counter. The latter consisted of a modified wrist watch; such was the state of the art of automatic digital counting at that time. The use of photosensitive Geiger-Müller counters continued into the following decades, in scintillation counters [104].

Photomultiplier

The first photomultiplier tubes (PMTs) were constructed in 1935–1936 [105, 106]. Although their first application (sound pickup in movie projection) did not imply single photon resolution, eventually PMTs became used in the photon counting mode. Modern PMTs are employed today in many scientific applications, especially in those that require very large photosensitive areas.

Wavelength sensitivity of PMTs, just as that of Geiger-Müller counters, is determined by the coating of photocathode. Many decent materials are available for visible light and UV-sensitive photocathodes. However, near IR sensitivity is not easily attainable. Hamamatsu has developed InP/InGaAs(P) photocathodes that have about 1% quantum efficiency up to 1600 nm and a smaller efficiency up to 1700 nm. R5509-73 PMT using this photocathode with a sensitive area of 24 mm^2 is available [107].

A version of PMT called hybrid photodetector (HPD) exists in which the series of dynodes is replaced with an avalanche diode [106]. A photogenerated electron is accelerated by a large voltage (>4 kV) towards the surface of a semiconductor avalanche diode mounted inside the vacuum tube. The initial amplification by a factor of >1000 due to bombardment by a high-energy electron is followed by ca. $\times 50$ avalanche multiplication. HPD has a lower multiplication noise than PMT and is able to distinguish between one- and two-photon detection events most of the time, albeit with a significant error probability. (VLPC/SSPM devices described later in this review have yet lower multiplication noise and are able to resolve the photon number more reliably than HPD.)

Avalanche photodiode

APD is a solid-state counterpart of PMT and Geiger-Müller tube. In the APD, a photon is absorbed in the bulk of a semiconductor, where it generates an electron-hole pair. If a sufficiently high electric field is present, carriers would be accelerated to speeds where they can generate more electron-hole pairs through impact ionization, resulting in avalanche multiplication. In semiconductor, both elecrons and holes cause ionization, though the ionization coefficients for electrons and holes would generally be different, depending on the material. Depending on the structure of the diode (one

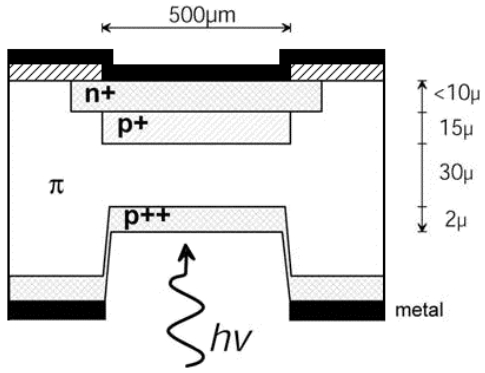


Fig. 21. Schematic cross-section of Si APD with reach-through structure developed by McIntyre and Webb in 1970s (reprinted from [108]).

example structure is shown in Fig. 21), the initial electron-hole pair can be photogenerated in the high-field multiplication region where it causes an avalanche immediately, or the pair can be photogenerated in another region (called an absorption layer) but either electron or hole subsequently drifts or diffuses into the multiplication region.

Initial studies of the APD behavior and theory of avalanche multiplication (including detection of single photons) were done in the 1960s–70s [109, 110, 111]. For a review of single photon detection using APDs, see Ref. 108 (and for an older review, also [112]).

The multiplication gain M the APD achieves strongly depends on the reverse bias voltage applied to the diode. Depending on the structure and thickness of the depletion zone, APDs operate at bias voltages ranging from 10 to 500 V [113].

The APD can be operated with a finite gain M at a bias voltage set below the breakdown voltage V_B, or it can be operated in a so-called Geiger mode when the bias voltage exceeds V_B (Fig. 22). In the finite gain mode (point A in the figure) photogenerated carriers are multiplied on average M times, resulting in a larger photocurrent than without multiplication. The APD can be used in a conventional photoreceiver in this mode, e.g., in telecommunication applications. In principle, the finite gain mode can also be used for single photon detection if a sufficiently low-noise amplifier and sensitive comparator are connected to the APD [111]. However, constructing a low-noise electronics and making a good single photon detector in this mode of operation is, in practice, difficult [114, 115, 116]. Instead, Geiger mode is almost universally used for photon counting. If the APD is biased above V_B and no current flows through it (point B in Fig. 22), a single carrier can trigger a self-sustaining avalanche that quickly leads to a macroscopic current, in the milliampere range (point C in the figure), which can be easily registered by the electronics. To quench the avalanche, an external circuit lowers the bias voltage at the APD, then raises it back to the operating point (i.e. point B) so that the APD is ready to detect another photon.

The rise of the avalanche and its quenching are both statistical processes. The photogenerated carrier may fail to generate more carriers before leaving the junction. The avalanche that has started can quench before reaching the self-sustaining state, due to statistical fluctuations in the number of carriers present in the junction at any given instant (the probability of spontaneous quenching is significant for current less than

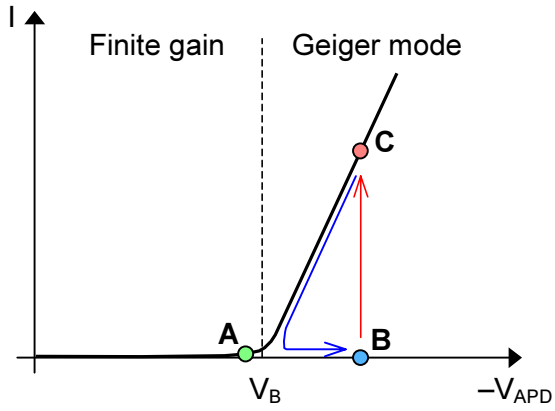


Fig. 22. Regions of APD operation (at low intensity of incident light) in the reverse *I–V* characteristics of a p–n junction.

ca. 100 μA). Similarly, when the bias voltage is being lowered slowly in order to quench a self-sustaining avalanche, the avalanche would quench at a random time before the voltage is lowered to V_B.

The quantum detection efficiency (QE) of an APD-based SPD is a product of two factors: the probability of the photon being absorbed in the active volume of the APD, and the probability of the photogenerated carriers to initiate an avalanche that gets successfully registered by an external circuit. These two factors are largely independent. The photon absorption probability depends on the photon wavelength and on the APD construction. The avalanche initiation probability increases with the excess voltage V_E, which is defined as the difference between the bias voltage and V_B.

There are three main methods of quenching the avalanche in Geiger mode [113].

- **Passive quenching.** In this method, the APD is biased through a large resistor (typically hundreds of kiloohms). During the avalanche, the capacity of the APD and the stray capacitance (combined, they can be as low as a few picofarads) are quickly discharged, and the voltage at the APD drops to the point when the avalanche quenches. Then, the capacitance is slowly recharged through the bias resistor, and the voltage is restored.
- **Active quenching.** In this method, the onset of the avalanche is sensed by an external circuit that lowers the bias voltage at the APD below V_B via an active feedback loop. After a certain hold-off time, the bias voltage is quickly restored by the same active circuit.
- **Gated mode of operation.** If the expected time of arrival of a photon is well known, the bias voltage can be raised above V_B shortly before this time, and lowered shortly after. The rest of the time it is kept below V_B (Fig. 23). If an avalanche is triggered during the gating pulse, it can be registered by an external circuit, and is quickly quenched when the gating pulse ends.

There is some probability that an avalanche starts without photon absorption. These events are called dark counts. In QKD, dark counts contribute directly to the QBER,

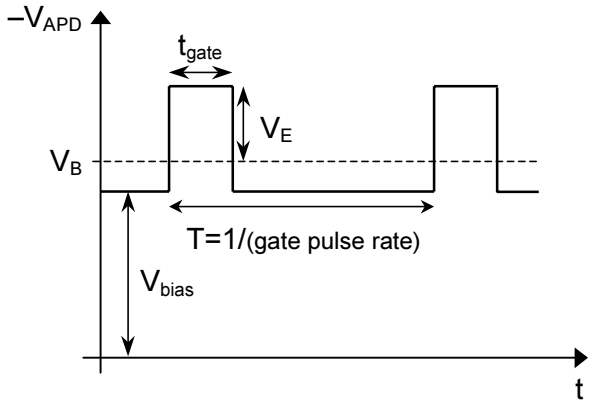


Fig. 23. Voltage at the APD in the gated mode of operation. The expected time of photon arrival is periodic in the depicted case.

limiting the maximum tolerable attenuation in the transmission channel and thus the maximum transmission distance of today's QKD systems (i.e. the distance at which QBER is still lower than 11%, allowing for extraction of a secure key). The three main effects that cause dark counts are the following [110, 108].

- **Thermal generation** of carriers through generation-recombination (GR) centers, i.e., local levels with mid-gap energy. This effect can be strongly reduced by lowering temperature, and by improving the semiconductor technology to reduce the density of GR centers.
- **Band-to-band tunneling** under strong electric field. This effect does not strongly depend on the temperature. Although in properly constructed APDs the tunneling probability is small, it sets the ultimate limit on the dark count rate.
- **Emission of minority carriers trapped in deep trap levels**, i.e., energy levels between mid-gap and band edge. The carriers get trapped in these levels during the avalanche and are subsequently randomly released. The density of trap levels can be reduced by improving the semiconductor technology. The population of trap levels does not come close to saturation under normal operating conditions in Geiger mode. Thus, the number of trapped carriers increases linearly with the total charge that flows through the junction during the avalanche. The lifetimes of the traps increase as the temperature is lowered. Dark counts caused by release of trapped carriers are called *afterpulses.* Afterpulsing is a major problem limiting the photon counting rate in many applications; more on this in Section 3.3.

The choice of semiconductor material determines the wavelength sensitivity (related to the bandgap of the material), dark count rate and other properties of the APD. APDs employed for photon counting have so far been made of three different semiconductor materials: Si, Ge, and a heterostructure made of InGaAs/InP.

- **Silicon.** Si APDs are sensitive to light in the wavelength range from at least 400 nm through 1100 nm. Sensitivity at the edges of this range depends on optimizations in the APD construction: at shorter wavelengths photons tend to be quickly absorbed in a shallow surface layer, while at longer wavelengths the absorption coefficient in Si is low and a deep collection zone is required. Silicon APDs have very good characteristics: dark count rate of several tens of counts per second, QE routinely exceeding 65% in the middle of their wavelength range (76% demonstrated at 702 nm [117]), counting rate of several MHz, low level of afterpulses. Specially designed devices can achieve photon timing resolution, or jitter, of as low as 27 ps FWHM [108]. All methods of quenching the avalanche can be used with Si APDs. Single photon counting modules based on diodes specifically designed for photon counting are commercially available [118, 114].

  Si APDs have low dark count rate and low level of afterpulses because the silicon technology is highly refined, unlike that of other semiconductor materials. Unlike Si APDs, all existing commercial models of the two other types of APDs listed below have primarily been designed for finite gain mode. They are adopted for photon counting applications with varying success.
- **Germanium.** Wavelength sensitivity of Ge APDs [112, 119, 120] cooled to liquid nitrogen temperature (77 K) extends to 1.4 μm. Cooling to this temperature is required to lower the dark count rate, which is several orders of magnitude greater than in Si APDs. Afterpulsing probability is also higher than in Si. However, both passive quenching and gated mode of operation are possible.

  In order to further reduce tha dark count rate, Ge and InGaAs/InP APDs are most often operated at a lower V_E than Si devices, yielding QE in the 10 to 20% range.
- **InGaAs/InP heterostructure.** In this type of APDs [121, 122, 123, 124, 125, 126, 127, 128, 129], photons are absorbed in a narrower bandgap InGaAs layer while the avalanche multiplication of photogenerated carriers takes place in an InP layer. The heterostructure is used because InGaAs is a material poorly suited for avalanche multiplication: tunneling breakdown may occur at the field intensity required for ionization. Also, the ionization coefficients for electrons and holes in InGaAs are comparable, which in the finite gain mode would lead to a higher noise level. The cut-off wavelength of InGaAs shortens as the temperature is lowered: the device loses sensitivity to 1.55 μm photons around –100°C. This is a temperature that can be reached with a multistage thermoelectric cooler. Afterpulsing is a severe problem in this type of APDs, especially at lower temperatures when trap lifetimes soar. Only active quenching and gated mode of operation are used with these APDs. In a given application, there will be an optimum temperature somewhere in the –100 to –20°C range at which the dark counts due to thermal generation and those due to afterpulsing, when combined, give the lowest overall dark count rate in the application. Commercial single photon counting modules based on InGaAs/InP APDs are available [130]. Research on diodes specifically designed for Geiger mode has begun [131].

The reader will find a description of the APD-based SPD we have constrcted, as well as further treatment of engineering issues, in Sections 3.2. and 3.3.

Solid state photomultiplier, visible light photon counter

The last two detector types utilizing avalanche multiplication are solid state photomultiplier (SSPM) [132] and visible light photon counter (VLPC) [133]. They use impurity-band ionization in arsenic-dopes silicon, as opposed to the valence to conduction band ionization in APDs. Much lower electric field is required for ionization of As impurity-band levels, which lay 54 meV below the conduction band of Si. To prevent thermal excitation of dopant atom's electrons to the conduction band, the device must be cooled below 7 K.

SSPM and VLPC are closely related devices sharing the avalanche mechanism and fabrication technology. They differ only in the order in which the absorption and multiplication layers are stacked. Here we only consider the structure of the VLPC (Fig. 24). A photon absorbed in the intrinsic region (undoped Si) generates an electron-hole pair. The hole drifts to the gain region (As-doped Si), where it excites multiple electrons from the impurity levels to the conduction band. These electrons are accelerated by the field and cause more ionizations, creating an avalanche. The holes in the impurity state have much lower mobility and do not acquire enough energy to cause ionizations; they slowly drift by hopping between dopant atoms, and leave the device well after the avalanche.

The avalanche in the gain region is restricted to a small area of the detector and is self-limiting, because the electric field in the avalanche area is lowered below the ionization threshold by the space charge formed by the holes in the impurity state. The amount of charge flowing through the device per avalanche is on the order of $3 \cdot 10^4$ electrons (exact value depends on the temperature and bias voltage), and has a small statistical uncertainty for any given operating conditions. Due to the self-limiting mechanism, the multiplication noise is record low, with the excess noise factor measured to be 1.015–1.03 [134, 133]. Each avalanche is localised to an area several micrometers in size, while the total photosensitive area can be 1 mm in diameter. Simultaneous absorption of several photons in different points within the photosensitive area leads to independent avalanches. The total output charge of the device is approximately proportional to the number of photons absorbed. One- and two-photon events can be reliably distinguished [135, 133].

Rather high QE values in excess of 88% at 694 nm have been achieved with VLPCs [136]. On the other hand, SSPMs have been shown to be sensitive to photons throughout a wide wavelength range 0.4–28 μm [132].

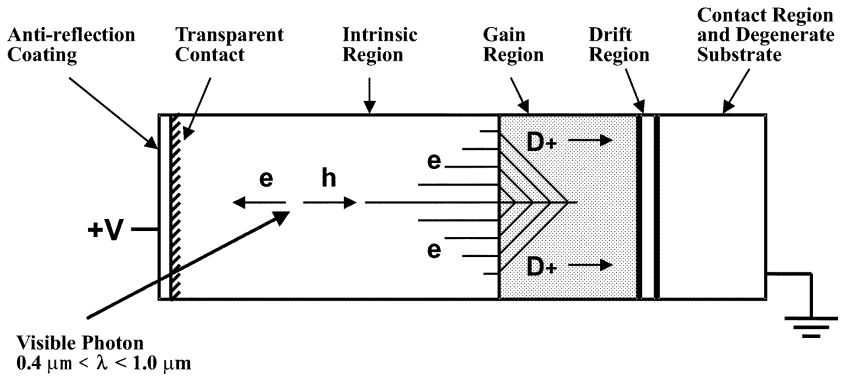


Fig. 24. Schematic structure of the VLPC detector (reprinted from [133]).

Superconducting detectors

The next three types of SPDs utilize weird effects in low temperature superconductors to achieve each some combination of unique parameters not available in other detector constructions. All three types of superconducting detectors can have extremely low dark count rate and flat wavelength sensitivity extending far down into IR. In addition, two of the three types allow energy resolution (translating into the ability to resolve either photon number at a fixed wavelength, or wavelength of a single photon) combined with QE that can approach 100% when proper optical coupling is provided (a resonant cavity structure around the sensitive element). The third type does not have these qualities, but instead has a very fast sub-nanosecond response with no hold-off time and no afterpulsing. The drawback of superconducting detectors, making them impractical for many applications, is the need to cool them down to a fraction of kelvin (fisrt two types) or just to the liquid helium temperature (third type). However, closed cycle coolers for sub-kelvin temperatures are commercially available [137].

The energy of a near IR photon is orders of magnitude larger than the bandgap 2Δ of a superconductor. A photon absorbed in a superconducting material breaks a large number of Cooper pairs into quasiparticles (i.e. unpaired electrons); this can be considered as the initial amplification mechanism in all three types of superconducting detectors.

Superconducting tunnel junction (Josephson junction) detector

Superconducting tunnel junction (STJ) single photon detector consists of a thin insulating barrier between two layers of aluminium, which in order are sandwiched between layers of niobium or tantalum (Fig. 25) [138, 139]. The device is cooled far below the critical temperature T_c of both materials. A photon absorbed in an outer layer creates a large number of quasiparticles. The quasiparticles are quickly collected and trapped in the Al layers, which have a lower bandgap than the outer layers. A magnetic field is applied parallel to the barrier to suppress tunneling of Cooper pairs. When a bias voltage $V_b < 2\Delta/e$, where e is the charge of electron, is applied to the device, the only tunneling process that can take place is transfer of a charge carrier across the barrier. A single quasiparticle typically crosses the barrier many times in both directions before dissipating (the mean number of crossings before dissipating depends on the geometry and size of the device [139]), providing further amplification of the number of electrons flowing through the detector per photon absorbed. The total charge transferred per photon is proportional to the photon energy and has a rather small statistical uncertainty, making the device photon number resolving at the near IR or shorter wavelengths. The lifetime of quasiparticles ranges from microseconds to tens of microseconds, defining the duration of the output current (which has the shape of a fast rising and slowly exponentially decaying pulse) and limiting the counting rate.

Detectors based on this physical principle provide sensitivity from X-ray [140] (having been used for X-ray spectroscopy for decades) to as far into infrared as 500 μm [141] (not yet single photon resolving in that wavelength range[14]). A small array of STJs has been fabricated and used for visible light astronomical observation [143], providing energy and time resolution in addition to the pixel position X, Y in the array.

[14] Single photon resolution in the submillimeter wavelength range has been achieved with another type of detector based on a single-electron transistor made of two quantum dots [142].

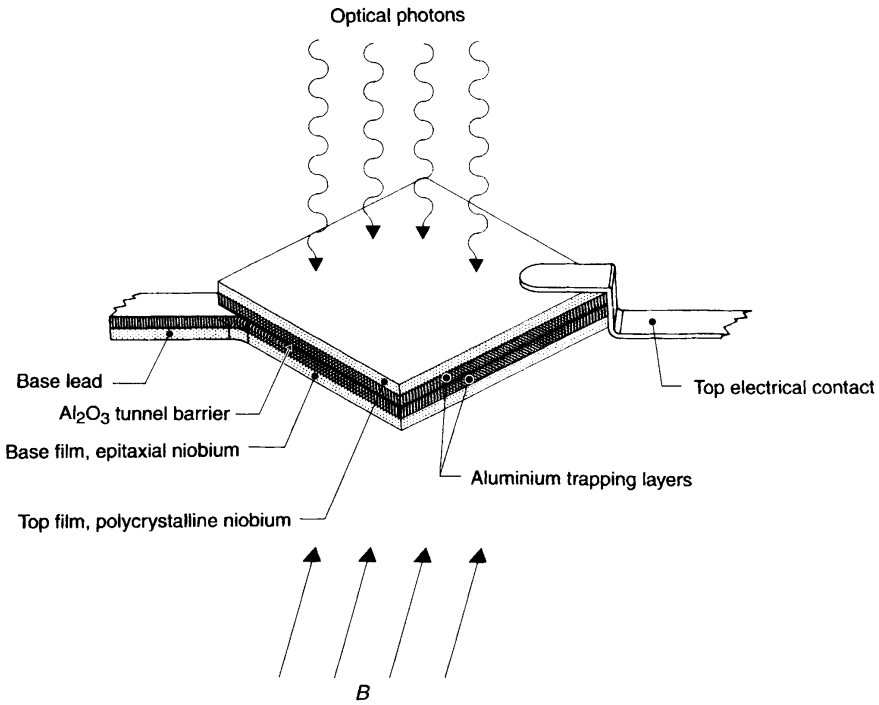


Fig. 25. A diagram of a 20×20 μm STJ device (not to scale). It was fabricated from a 'sandwich' of Nb/Al/Al_2O_3/Al/Nb deposited on polished sapphire. The base and top niobium films have a thickness of 100 nm; both the aluminium films are 120 nm thick; the aluminium oxide barrier has a thickness of ~1 nm (reprinted from [138]).

We think that this type of detector should have no intrinsic limitations of QE at the visible and near IR wavelengths. All photons absorbed within the device are registered. In theory, it should be possible to achieve absorption efficiency closely approaching 100% at a chosen wavelength with a suitable light coupling to the detector.

Transition edge sensor

Transition edge sensor (TES) microcalorimeter consists of a piece of wolfram film (Fig. 26) [144, 145, 146]. The sensor is cooled below 100 mK, which is lower than T_c of the W film. The film, however, is kept at the superconducting to normal transition by Joule heating provided by the current from a biasing circuit (Fig. 27). The biasing is stable due to the negative feedback: an increase in the sensor temperature and thus an increase in its resistance causes a decrease in Joule heating. In operation, a photon is absorbed in the W producing a photoelectron which heats the W electron system, raises its resistance and causes a drop in the current. The integral of the drop in the current multiplied by the bias voltage gives, with no free parameters, the energy absorbed by the W. The current pulse is read by a SQUID array followed by a room-temperature amplifier (Fig. 27). The pulse shape has a fast rise followed by an exponential decay; the decay time constant is tens of microseconds, limiting the counting rate. TESes generally have slightly better energy resolution than STJs.

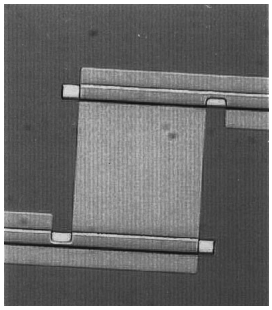


Fig. 26. Photograph of a TES with 18×18 μm W sensor and Al voltage rails. The thickness of the W film deposited on a Si substrate is 40 nm (reprinted from [144]).

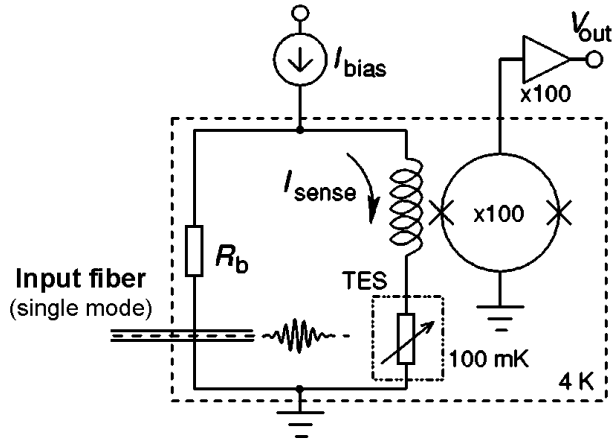


Fig. 27. Schematic of a TES device biasing and readout. The voltage bias for the device is provided by a room-temperature current source (I_{bias}) and a 100 μOhm shunt resistor (R_b) at 4 K. The device signal I_{sense} is amplified by a 100-element array of dc-SQUID amplifiers and processed with room-temperature pulseshaping electronics (reprinted from [145]).

Just like the previous detector, TES has no intrinsic limitations of QE. With a suitable optical construction, efficiency close to 100% at a chosen wavelength can be achieved. QE of 88% at 1550 nm has been demonstrated with an optical cavity integrated into the detector [147].

Superconducting single photon detector

Superconducting single photon detector (SSPD) consists of a thin superconducting stripe biased in such a way that a current I slightly lower than the critical current I_c is flowing through the stripe (Fig. 28) [148, 149, 150, 151, 152, 153, 154, 155]. When a photon is absorbed within the stripe (Fig. 29a), it quickly creates a non-superconducting hot spot (b). The current I is forced to flow through a smaller cross-section of the stripe around the hot spot. The current density now exceeds the critical

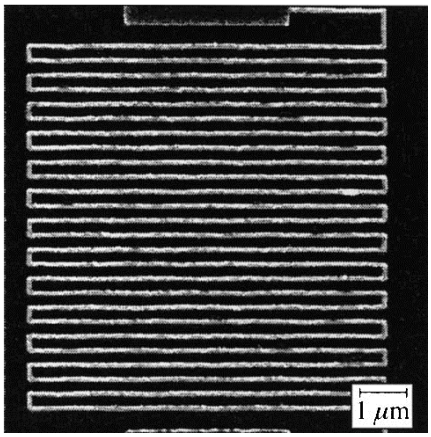


Fig. 28. A scanning electron microscope image of a 10×8 μm^2, 10 nm thick meander-type SSPD, NbN superconducting stripe on a sapphire substrate. The stripe width is ~130 nm and the filling factor f = 0.2 (reprinted from [151]). This filling factor is due to a particular technology used for fabricating the depicted sample, and is not the highest achievable: f ~0.5 is possible with other technologies.

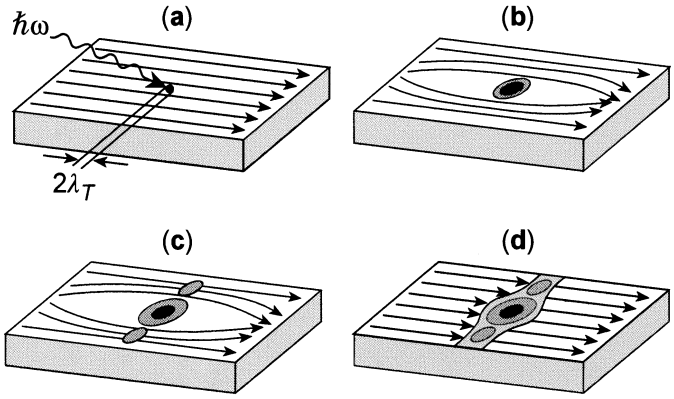


Fig. 29. Schematics of the hotspot-generated and supercurrent-assisted formation of a resistive barrier in an ultrathin and submicrometer-width superconducting stripe, kept at a temperature far below T_c. The arrows indicate the flow direction of a supercurrent biasing the stripe (reprinted from [151]).

current density, phase slip centers appear (c) and a normal-conductivity bridge is formed across the stripe (d). After a few picoseconds, the hotspot disappears because the electrons in it have cooled through electron-phonon scattering, and superconductivity is restored to the original state (with no effects remaining in the detector). The temporary formation of a non-superconducting bridge leads to a voltage pulse registrable by electronics, e.g., as a 30 ps long 200 mV peak-to-peak amplitude pulse obtained after a 40 dB amplifier [150]. This detector is fast, allowing counting rates in excess of a gigahertz. The biasing scheme required for the fast self-resetting operation described

Table 2. Selected examples of performance of different single photon detector types. Remarkable values of parameters are printed in bold.

Detector	Mechanism of initial amplification	Temperature, K	λ, nm	Counting rate, Hz[a]	QE, %	Jitter, ps	Dark count rate, s^{-1}	Energy or photon number resolving?[b]
Geiger-Müller counter [103]	Avalanche ionization in gas	room	up to 750	100	N/A	N/A	0.1	No
PMT:	Multiplication of electrons via secondary emission on a series of dynodes							No
Hamamatsu R5509-73 [107]		193	up to 1700	10^7	< 1	1500	$1.6 \cdot 10^5$	
APD:	Avalanche ionization of valence band in semiconductor							No
Si, Perkin-Elmer SPCM-AQR [118]		room (Peltier cooled)	700	$5 \cdot 10^6$	**65**	350? [108]	**25**	
Si, planar epitaxial device [108]			500		40	**27**		
Ge FD312L – our SPD, see Sect. 3.2. , 3.3.		77	1310	(gated at $\mathbf{2 \cdot 10^7}$)	7		($5 \cdot 10^{-5}$ per gate)	
InGaAs/InP [30, 164, 165]		165	1550	(gated at 10^6)	10		(**$2 \cdot 10^{-7}$** per gate)	
InGaAs/InP, id Quantique id200 [130]		N/A (Peltier cooled)	900–1700	(gated at up to $4 \cdot 10^6$)	> 10 at 1.3, 1.55 μm	580	(<$5 \cdot 10^{-5}$ ns^{-1})	
VLPC [136]	Avalanche ionization of shallow impurity band in Si	6.9	694	~10^6	**88.2±5**	N/A	$2 \cdot 10^4$	Photon number
STJ	Single photon creates many free electrons in superconductor; each electron crosses the tunnel junction multiple times	~0.3		~10^5			**~0**[c]	Energy or photon number

(*table continued*)

Detector	Mechanism of initial amplification	Temperature, K	λ, nm	Counting rate, Hz[a]	QE, %	Jitter, ps	Dark count rate, s^{-1}	Energy or photon number resolving?[b]
TES:	Temperature sensitivity of resistance at superconducting transition						**~0**[c]	Energy or photon number
[147, 146]		< 0.1	1550	~10^5	**88.6 ±0.4**	N/A	N/A	
[33]			1550	~10^5	65	90 ns	10	
SSPD:	Disruption of near-critical current in a small hotspot in a thin stripe spreads to the whole stripe cross-section	< 10		**> 10^9**		**18** [150]	10^{-3} to 10^7 [152, 155][d]	No
[153]		1.8	1550		57	41	N/A	
Wavelength converter + Si APD [157]		room (heated)	1560 into 710	$5 \cdot 10^6$?	46	350?	$8 \cdot 10^5$	No

[a] Due to statistical nature of photon counting, and different saturation mechanisms in different types of SPDs, the listed counting rate is a very rough estimate.

[b] Photon number resolving means being able to reliably distinguish at least between "one", "two", and "three or more" photons absorbed simultaneously at the detector. Photon number resolution in energy resolving detectors listed in the table is implemented when the incoming radiation is narrowband, via dividing the total measured absorbed energy by the energy of a single photon at the working wavelength. When a detector is not photon number resolving, it distinguishes between the "no photon" and "one or more photons" events. It should be noted that a photon number resolving detector unit could in principle be made with a 1-to-N beam-splitter and multiple non-photon-number-resolving detectors, or with an equivalent approach using time multiplexing [163].

[c] Dark counts in STJs and TESs are caused by blackbody radiation entering the detector. When no cold filters on a fiber input are used, the dark count rate is ~10^2 Hz. However, it is estimated that a bandpass filter for 1550 nm with 40 dB out-of-band suppression would reduce the dark count rate to below 0.1 Hz [166].

[d] The dark count rate for a SSPD varies greatly depending on how close the operating current I is to the critical current I_c of the stripe. Lower dark count rates can be achieved at a sacrifice in QE.

above [149] seems to prevent formation of more than one non-superconducting bridge at a time; thus the detector is not photon number resolving. The theoretical model [148] predicts a weak dependence of the integral of the voltage pulse on the photon energy; however, energy resolution is yet to be experimentally demonstrated.

There has been a rapid progress in development of SSPDs. Just five years after the first experimental demonstration of the hotspot-triggered, supercurrent-assisted formation of a resistive barrier across the superconducting stripe [149], a small series of devices with an integrated optical cavity has been fabricated, showing a QE reliably exceeding 40% at 1550 nm [153].

Wavelength conversion

While not a detection method in itself, the ability to change the wavelength of incoming photon towards a shorter one can be very useful. In general, detectors for shorter wavelengths (e.g., Si APDs) have much better parameters than the existing detectors of comparable complexity for near IR. One could change wavelength of the photon and use a cheaper, smaller detector. It turns out, efficient wavelength conversion for weak light (up to 100% efficient in theory) is possible via sum frequency generation in nonlinear media. Although this technique is not new [156], efficient conversion has been demonstrated experimentally in the last two years in fiber-coupled periodically poled lithium niobate waveguides [157, 158, 159, 160] and in bulk periodically poled lithium niobate [161]. Moreover, the process of nonlinear conversion is noise-free and preserves the quantum state of the photon [162, 160], which opens up for interesting possibilities in constructing quantum communication setups.

The present generation of wavelength converters is plagued by rather high intensity of parasitic output light at the same wavelength as the converted photon. This makes them, when used together with Si APDs, barely comparable in dark count level to InGaAs/InP APDs used directly. Hopefully the origins of this problem would be tracked down and dealt with in the coming years. If this problem is solved, we'd have a very good detector for telecom wavelengths without the burden of cryogenic cooling.

Summary

Performance of selected SPDs of different types is summarized in Table 2. Only the types of detectors that might be practically useful today for visible and near IR photon counting have been reviewed. There are a few more detector types in development using other physical principles. For instance, two more types of detectors have been demonstrated, both operating at cryogenic temperatures. One detector is based on the thermoelectric effect [167, 168]. Another one is based on dependence of the channel conductivity in a field effect transistor on the exact number of electrons trapped in a layer of quantum dots placed between the channel and the gate [169].

While APDs and PMTs are most widely used, other types of detectors show promise and may in the future be employed in a number of more demanding applications and experiments (this process has already begun [33, 143]). For us, it is satisfying to see that Eve can not only have perfect detectors *in principle,* but, at a large cost, can manufacture close-to-perfect detector units for her eavesdropping activity today (see Chapter 4).

3.2. Single photon detector based on avalanche photodiode

In our QKD system, the expected time of photon arrival is well known and periodic. In such a case, the gated mode of operation is the best choice. With a sufficiently short gate, it minimizes the dark count rate and the amount of charge flowing through the APD (thus reducing afterpulsing).

The use of a short gate pulse presents a peculiar problem: the rising and falling edges of the gate pulse result in spikes of current of opposite polarity flowing through the APD capacitance. These spikes are present in all gates, with and without avalanche, and are of a magnitude comparable to the avalanche current. The detection circuit has to distinguish between an avalanche and these current spikes. There are several possible solutions to this problem. It is possible to use a longer gate pulse with a sufficiently high V_E that induces a large avalanche current, and set the threshold in the detection circuit above the spikes. However, this results in substantially increased afterpulse and dark count probabilities [165, 170]. The most common solution is to cancel the spikes with a counterphase arm that includes a trimming capacitor adjusted to match the capacitance of the APD [171, 172]. Another solution for cancelling the spikes in a gated detector employs an H-shaped network of transmission lines where the pulses of opposite polarity reflected from the ends of the lines cancel each other [173, 174]. Alternatively, if a gated detector for QKD has two APDs, they can be connected in a single detection circuit [30] such that, in the absence of avalanche, currents through the APDs approximately cancel each other; in the presence of avalanche in one of the APDs, the polarity of the output signal shows which of them has had the avalanche; however, this circuit has the drawback of missing the events when both APDs have had an avalanche simultaneously. In another approach, the spikes are not cancelled but a voltage discriminator that senses the peak amplitude of the discharge (i.e., second) spike is employed [170, 175], in fact creating a detector that senses an order of magnitude smaller avalanche charge flows than would be possible by a straightforward approach. This detector, together with an afterpulse discarding technique (mentioned in the next section), allows 10 MHz gate pulse rate in a QKD system, achieving a projected 30 Kbit/s secure key generation rate over 10 km of fiber at 1550 nm [175]. In other approach, the current flowing through the APD is integrated, after which an amplitude discriminator detects avalanches with a good sensitivity [176]; it is used to select only the longest avalanche pulses for a given gate width, filtering out most of the dark counts.

Our detector scheme implemented by Torbjørn Nesheim [177] has a design that fully cancels the spikes. It employs a differential amplifier with two arms connected to its inputs (Fig. 30). One arm connects to the APD submerged into liquid nitrogen in a dewar flask. The compenating arm of exactly the same length contains a ~1 pF trimming capacitor rigged from two short pieces of insulated wire intertwined together. The length of the compensating arm is adjusted, by cutting and re-soldering, to match that of the APD arm, and the trimming capacitor is adjusted, by winding and unwinding the wires, to match the capacitance of the APD under the operating bias (the APD capacitance drops slightly as the bias voltage is increased). The adjustment is done

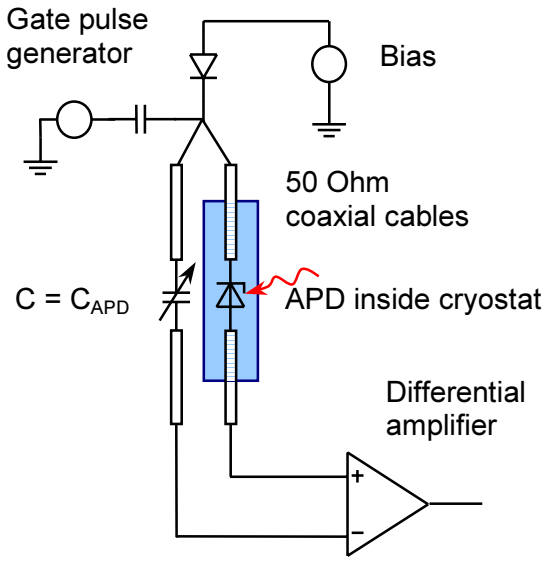


Fig. 30. Single photon detector with a balancing circuit to compensate for the APD capacitance. All cables are 50 Ohm terminated (termination resistors are not shown).

while observing the output signal of the differential amplifier. When properly adjusted, the current spikes from the gate pulse fully cancel; only avalanche pulses are present at the output of the differential amplifier. The gate pulse generator (Avtech AVM-3-C) provides 2 ns wide gate pulses with 100 ps rise time and 600 ps fall time at the repetition rate of 20 MHz or less; the desired peak-to-peak amplitude of the gate pulse at the APD is set by adding radio frequency (RF) attenuators at the output of the generator. The differential amplifier has a bandwidth of ~1 GHz.

We have tested several APDs in this scheme: one InGaAs/InP Fujitsu FPD5W1KS, several samples of Ge Soviet/Russian-made FD312L, FD312, FD322. Out of the tested APDs, only two samples of FD312L had a sufficiently low dark count rate to be of use in a QKD system. Just as other groups, we have found that the best (i.e. lowest) *dark count probability to QE ratio* for APDs tends to be achieved at lower values of V_E and QE [123, 124, 127, 128, 69]. We planned to do QKD experiments at the largest tolerable attenuation of the communication line, which could be made larger if this ratio is low. We therefore set V_E at roughly the lowest value at which avalanche pulses could still be reliably registered by a counter, in practice limited by the level of electrical noise at the output of the differential amplifier. In such operating conditions, the best sample of FD312L had the dark count probability of $5 \cdot 10^{-5}$ per gate and 16% QE, measured with 1310 nm attenuated laser pulses.

3.3. Afterpulse blocking

Trapping charge carriers at the trap levels during the avalanche and their subsequent release is a major problem in many photon counting applications. The carriers are released for some time following the avalanche, and can cause dark counts called afterpulses. It has been experimentally determined that there are several (three to four) trap levels with different lifetimes varying from tens of nanoseconds to tens of microseconds [178, 128]. The severity of the afterpulsing effect depends on the semiconductor material and technology of the APD. Ge and especially InGaAs/InP APDs have much higher densities of trap levels than Si APDs. Afterpulsing also depends on the operating mode of the APD in the SPD. Most of the research groups who construct SPDs (including our group) do not have direct control over the technology: they have to use APDs made by commercial manufacturers. However, a proper operating mode and SPD electronics in a particular photon counting application often allow to mitigate the afterpulsing effect to a significant degree. Afterpulsing can be reduced by the following measures.

- **Reduction of charge** flowing through the junction during the avalanche. This can be accomplished by speedier quenching and more sensitive electronics that can sense pulses of lower amplitude (occurring at lower V_E). The fastest quenching is achieved in the gated mode with narrow gate pulses.
- **Introduction of a hold-off time** after each avalanche during which the voltage at the APD is kept belov V_B, so that most of the trapped carriers are released during this time and dissipate without causing afterpulses. The APD is insensitive to photons during the hold-off time. In the gated mode, the hold-off time is the reciprocal of the gating rate. When Ge and InGaAs/InP APDs are used in QKD systems, the gating rate is usually restricted to 0.1–1 MHz because of afterpulsing.
- **Additional time selection of avalanches** in the gated mode. While not preventing afterpulses from happening, it does not count those of them whose onset falls outside a set time window. However, this measure becomes unnecessary with sufficiently short gate pulses whose width approaches the jitter of the SPD or is matched to the width of the incoming light pulse, whichever is narrower.
- **Selecting the temperature** of the APD. Lowering the temperature reduces the dark count probability, but tends to increase the lifetime of the trap levels. In a QKD system, for any combination of the gating rate and other parameters there is an optimal temperature of the APD at which the highest key generation rate is achieved [179].
- **Afterpulse discarding** in gated mode (a technique introduced after we implemented afterpulse blocking described in the following paragraphs). In this technique, post-selection of detector data is performed, and all detection events *preceded by a detection event no farther that a set number N of time slots away* are discarded [85, 180, 175]. While not preventing afterpulses from happening, it effectively filters them out within the hold-off time (N+1)/(gating rate).

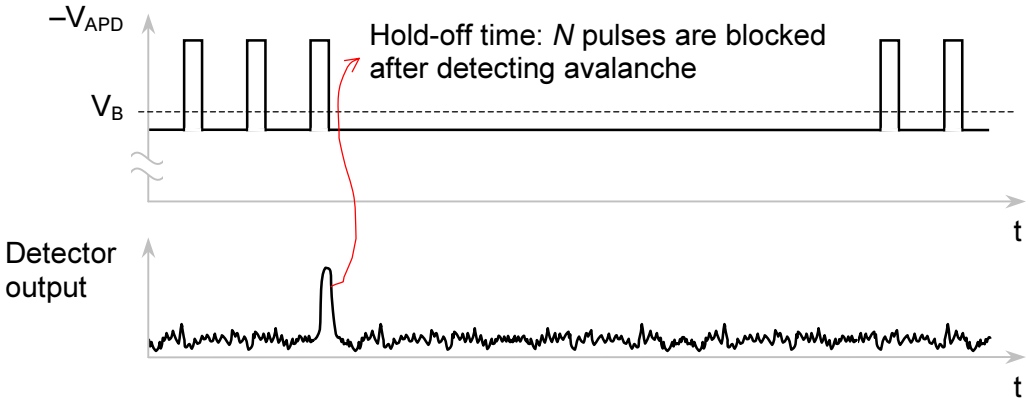


Fig. 31. Principle of afterpulse blocking.

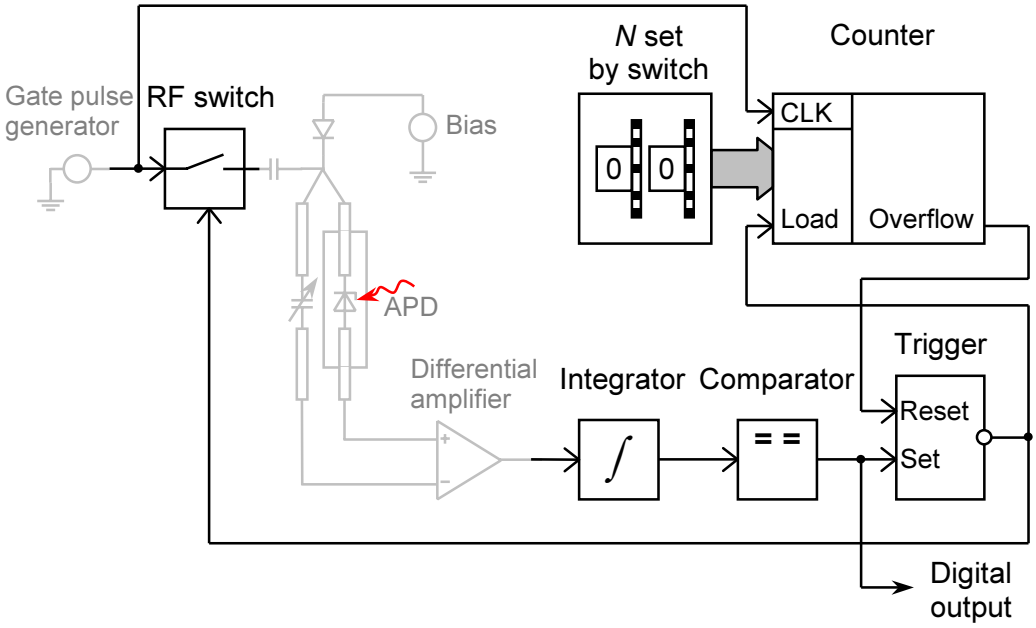


Fig. 32. Hardware implementation of afterpulse blocking. Grayed out parts are those inherited from the SPD without afterpulse blocking (Fig. 30); parts drawn in black lines form the afterpulse blocking circuitry.

In our QKD system, we wanted to use a gating rate of 20 MHz, which was more than an order of magnitude higher than afterpulsing would allow in a standard gated mode. To make this rate possible, we introduced a hold-off time, for which a discrete number of gating pulses after a registered avalanche is blocked from passing to the APD, eventually calling this technique *afterpulse blocking*[15] (Fig. 31). It prevents

[15] The term was coined by Jason M. Smith.

afterpulses from happening, and thus compares favorably with afterpulse discarding, especially at higher gate rates. In a typical QKD system, the probability of photon detection per gating pulse is low, typically one detected photon per several hundred gate pulses. If a few tens of gate pulses are blocked after each photon detection (as we have estimated would be necessary at our gating rate), this is *not* going to reduce the overall detection probability per gate considerably. Thus, the key generation rate in the QKD system is allowed to grow almost linearly with the gating rate.

The hardware implementation of afterpulse blocking (Fig. 32) consists of a switch (MAX4544 CMOS analog switch) placed between the pulse generator and the APD, a trigger and a counter (assembled from 74AC series high-speed CMOS ICs). *N* is settable via a set of manual switches to any number in the range 2–2050, or 0 (no blocking) [95]. The addition of the analog switch spoiled the shape of the gating pulse, making it close to triangular with FWHM of about 2 ns. In result, QE dropped in half at the same dark count probability as before. If we used a proper RF pulse switching technique instead of the CMOS switch, this detrimental effect would be absent or reduced.

Results of a test of our SPD with afterpulse blocking are shown in Fig. 33. The APD was gated at 12 MHz and the number of gate pulses blocked after each avalanche was varied from 0 (i.e., blocking switched off) to 2050. Both the dark count probability and the count probability when the APD was illuminated at 0.005 photons per pulse were measured. The count probabilities were calculated per gate pulse *before* the afterpulse blocking circuitry. The illumination level of 0.005 photons per pulse was chosen because it was of the order of magnitude typically found in a QKD system. We can see from the chart that when no afterpulse blocking is employed at 12 MHz gating rate, for every photon count or for every dark count not caused by trapped carriers there are as many as four afterpulsing counts. However, when we start blocking a few pulses after each detected avalanche, the count probability quickly drops down to a steady value. The further smooth drop off in the photon count probability (Fig. 33, lower chart) is caused by the increasing fraction of time the SPD is insensitive to light when a larger number of gate pulses is blocked. From this test, we can deduce that blocking approximately 30 pulses (or perhaps slightly more at 20 MHz) is sufficient to reduce afterpulsing counts' contribution to QBER to at least a manageable value, without noticeable impact on the photon detection probability.

The accuracy of measurement in this test only allows us to make a qualitative conclusion. It has been planned to make a more accurate quantitative measurement of how the number of blocked pulses affects QBER when the SPD is working as a part of our QKD system. Unfortunately, the QKD experiment has so far not allowed us to do this, due to unstable setup with low fringe visibility that masks all other effects (Section 2.2.3.).

We think that afterpulse blocking would keep afterpulse counts manageable without significantly affecting detection efficiency at gate pulse rates of at least an order of magnitude higher than 20 MHz. However, we have not explored limits of its performance, because in our system many other components restrict the pulse rate to 20 MHz. Finally, we note that afterpulse blocking can be used together with other measures directed at reducing afterpulsing, for a better cumulative effect.

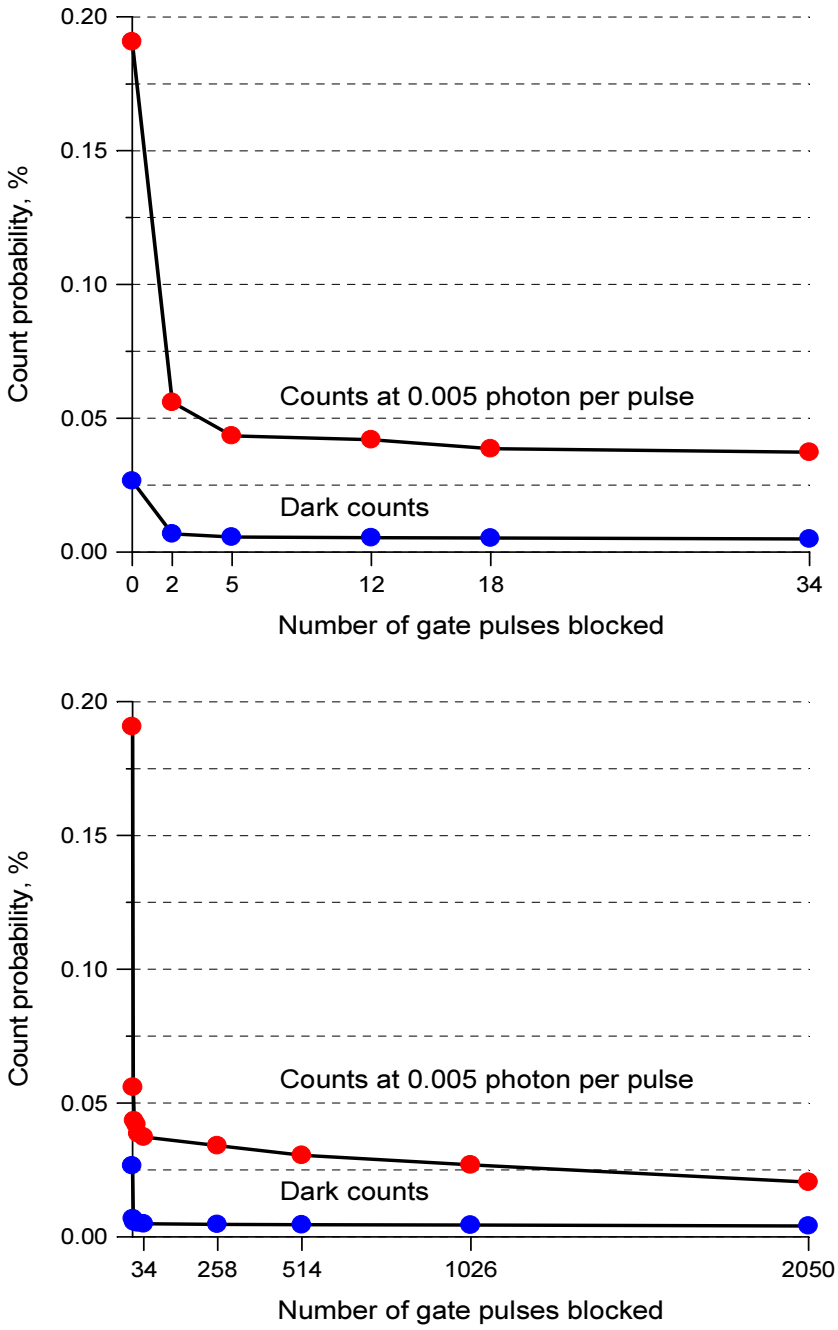


Fig. 33. Test of afterpulse blocking: count probability vs. number of gate pulses blocked after each detected avalanche. Results of a single experiment are shown on two charts in different scales of the horizontal axis. The upper curve on each chart represents an average count probability of the SPD when it is illuminated with weak coherent 1310 nm pulses at 0.005 photon per pulse; the lower curve represents average count probability when there is no input light. The gate pulse rate is 12 MHz, gate pulse width is ~2 ns. APD: Ge FD312L (s/n 1VUL1752), cooled to 77 K.

3.4. Conclusion

The single photon detector described in this chapter has operated stably and served us well. The achieved quantum efficiency of 7% at 1.3 μm and the dark count probability of $5 \cdot 10^{-5}$ per gate would be adequate for operation of a QKD system over 20 km of optical fiber. The afterpulse blocking technique we have developed has allowed to increase the gating rate of detector to 20 MHz, which would result in a roughly proportional increase of the key generation rate comparing to a similar QKD system operating at a lower detector gating rate.

After we presented the afterpulse blocking technique[16], it has been used by other groups for QKD [63], photon counting [126, 127], in a commercial single photon detection module [130], and to shorten acquisition times in the photoluminescence microscope of Ref. 181 by as much as two orders of magnitude [182].

[16] We have implemented afterpulse blocking in hardware by mid-1999 [95]. The author presented the idea and implementation of afterpulse blocking at the 1st QIPC Workshop in Potsdam, September 27–29, 2000. To the best of our knowledge, we were the first to implement and report it. Unfortunately, we have never written a paper about the SPD with afterpulse blocking, so we don't get credited for it. To be fair, the group in Geneva also had this idea no later than in 1998 [123], but did not develop it before we reported our results.

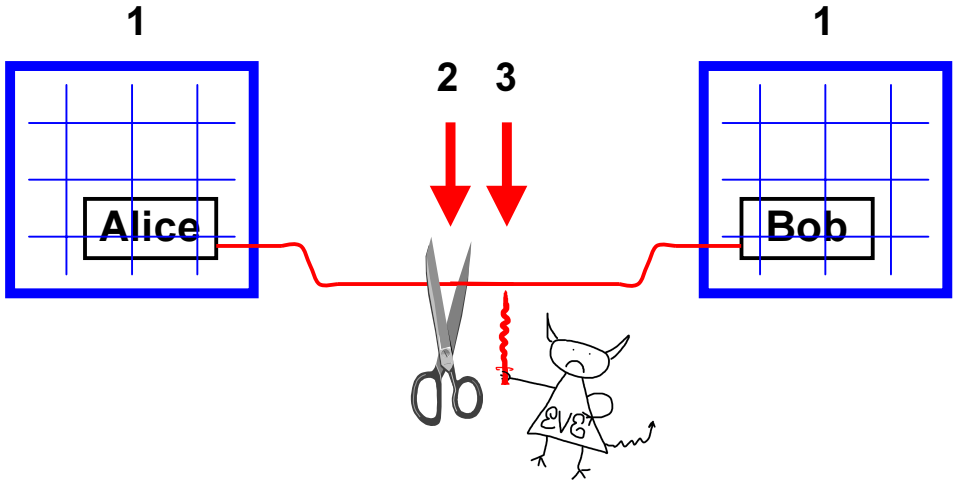
4. Security

The two-millennia long history of cryptography is a history of failures. For the most of it, the security of ciphers has depended on a *perceived* inability of adversary to crack the cipher, while such cracking was possible and, for the majority of cipher systems, sooner or later done thanks to the ingenuity of enemy codebreakers. Then, another crackable cipher (invariably declared "perfectly secure" and "incrackable" by those touting it) replaced the broken one.

It was only in the 20th century that ciphers and other cryptographic primitives whose security was rigorously proven based on the laws of Nature appeared. Around 1920, Gilbert Vernam proposed a simple "one-time pad" cipher where each symbol of the message was added modulo alphabet size with a symbol of a random secret key to form a ciphertext; on the receiving end, the same operation was used to extract the message [3, 4]. In 1949, Claude Shannon mathematically proved the security of this cipher was perfect provided the key material was never reused [5]. Around 1980, provable secure authentication techniques were developed [15]. In the last two decades of the century, another cryptographic primitive — secure key distribution given a quantum channel and an authenticated public channel — whose security is also based on the laws of Nature has been developed; this is the QKD. The proofs of its security have been developed by several authors during the last decade; more on this below in Section 4.2. The one-time pad cipher and QKD (with authentication techniques as a part of it), when employed together, form a complete cryptographic system for transmission of messages that is provably secure.

However, the theoretical proof is only one component to the security of any real-world cryptographic system. The proof forms the basis, but there are three components in total (Fig. 34). The first component is classical security: access control, proper operational procedures, electromagnetic and acoustic shielding, etc. at the end points where the cryptographic equipment is located and where the messages are handled in the unencrypted form. The second component is the security proof itself: a proof inevitably based on an idealized model of the real system. The third component is what differs the real system from the idealized model in the proof: unexpected implementation loopholes not *yet* accounted in the theoretical proof.

The whole security chain is only as strong as its weakest link. All the links are equally important. Should a quantum cryptography (QC) researcher then pay equal attention to them? The classical security component is not something unique to QC; it is mostly the same as for other cryptographic systems. It is not researcher's business then to care for this component, but that of the security specialists at the end customer (though we will have some remarks on it in the next section). The security proof, however, is definitely the business of a QC researcher. It has been at the very heart of QC from its beginning, and now we can be reasonably sure QC has been shown to be secure for a somewhat idealized model of the equipment. What about the remaining component, the loopholes in particular implementations that can assist Eve but are not described in the model? Searching for and closing these loopholes is the responsibility of a QC researcher, because they are intrinsic to the setups he constructs and technical



1. Conventional security; trusted equipment manufacturer
2. Security proof against quantum attacks
3. Loopholes in optical scheme

Fig. 34. Components of security in a quantum cryptosystem.

solutions he chooses. There wasn't time to worry about them when QKD setups were in the proof-of-the-principle stage (assembled on a single optical table [14], or the first experiments over optical fiber). However, many laboratory experiments have since grown ready to be commercialized, competing on such parameters as the ease of installation, key generation speed and transmission distance [30, 31, 32, 159]; commercial offers are already available [47]. It's time to pay attention to this last component of the security then?

When we looked at it several years ago, there had been almost no studies of component imperfections and loopholes outside of the several generic imperfections accounted in the proof (which were: non-ideal optical alignment leading to errors, loss in the transmission line and components, non-single-photon source statistics, and two imperfections in single photon detectors: non-zero dark counts and uniformly lower than 100% quantum efficiency). We saw several potential possibilities for Eve to use *other* imperfections to stage a successful attack, and went on to investigate them. Our ultimate goal has since been, after finding new loopholes and showing how Eve could use them for eavesdropping, to close them by either suggesting which specific protection measures could be applied or by incorporating the relevant component imperfection into the proof.

This chapter is organized as follows. Remarks on conventional security are given in the next section. A brief summary of existing security proofs is given in Section 4.2. For the rest of the chapter, in Section 4.3. we present several attacks using implementation loopholes we have investigated. The attacks have been studied to various depth: some of them thoroughly with experiments (large pulse attack, faked states attack using detector efficiency mismatch), some only theoretically (faked states attack on

schemes with passibe basis choice), and for some only the theoretical possibility of the attack is stated (light emission by APDs, high-power damage).

4.1. Conventional security

Quantum cryptography (with properly implemented and authenticated key extraction [183]) only provides security against attacks on the quantum and conventional communication lines. The end equipment and its usage is not and can not be intrinsically secure. The conventional security measures at Alice and Bob are required, just as for any other non-quantum cryptolink. They are just as critical links in the whole chain as security against attacks specific to quantum cryptosystems is.

The users and providers of a quantum cryptolink should follow the same set of security procedures they would use for a conventional cryptolink that uses the type of conventional encryption that is now supplied with a quantum-distributed key. (The conventional encryption could be the one-time pad, or a symmetric cipher with frequently changed key as currently implemented in MagiQ Technologies QPN quantum cryptosystem [184].)

The additional security procedures specific to the quantum cryptosystem as they look to the end user would be:

a) the *seed key* distribution at the time of installation;

b) monitoring the single indicator for functionality of the quantum cryptosystem. A properly implemented quantum cryptolink should monitor all parameters responsible for its security automatically and summarize them in a single "working / not working" indicator for the end user. Should any problem possibly leading to a security breach be detected, the key generation is automatically halted and the service or the link provider is called to check the problem.

Please note that the equipment manufacturer and the provider must be trusted, just as in the case of any conventional cryptosystem. We highly doubt that verifying security of the end equipment is in principle possible, given that the manufacturer can in principle conceal arbitrary devices and modifications inside the equipment and that there is a convenient optical communication channel for their remote activation and for information exchange.

To illustrate how a covert communication device could be concealed inside the setup, consider for example fiber optic lithium niobate phase modulators used in many QKD schemes. Lithium niobate modulators come from the factory as a sealed box, typically about ten centimeters long, a couple centimeters wide and a centimeter or so thick (see Fig. 35). This sealed box

a) has full information about bit values in Alice's setup (modulation voltage carrying bases and bit values is supplied directly to its connectors);

b) sits on the fiber;

c) has a significant electrical power supplied to it (through modulation connector);

d) cannot be non-destructively opened for inspection (see Appendix A for depiction of consequences).

Fig. 35. Lithium niobate phase modulator (JDS Uniphase UTP PM-130-080 travelling-wave 8 GHz, manufactured in 1998), cover removed. Reproduced here in 1:1 scale. Package size 89×23×10 mm (not including protruding elements). The coaxial connectors are of the SMA type.

This makes it quite possible to conceal a covert optical communication device inside an otherwise normally functioning phase modulator, that would report the bit values via the fiber channel. Moreover, a skillfully implemented device would be hard to discover even when the modulator package is opened. The covert circuitry could be hidden inside the thick metal base of this box, which appears to be feasible given the state of miniaturization of necessary electronic and fiber optic components. In a working equipment, such a device can lie silent for a long time, waiting either for a pre-set date or for activation by an external optical signal. By the way this is about how close you can come in this field to the original meaning of the term “Trojan horse” (according to the classification given in [185], this is a *pre-lurked Trojan horse*).

This is just one of the uncounted possibilities the manufacturer and the suppliers of components have in their disposal to break the security, if they are not absolutely trustworthy parties.

J. Larsson has shown [186] for the Ekert protocol [187] that when both Alice and Bob are trojaned, there is no need for communication back from them into the optical fiber.

To emphasize the importance of conventional security measures and security practices once more, let’s quote a somewhat discordant passage by Bruce Schneier:

„Security is a chain; it’s as strong as the weakest link. Mathematical cryptography, as bad as it sometimes is, is the strongest link in most security chains. The computer security, the network security, the people security — these are all much worse.

Cryptography is the one area of security that we can get right. We know how to make that link strong. Maybe quantum cryptography can make that link stronger, but why would anyone bother? There are far more serious security problems to worry about, and it makes much more sense to spend money securing those.

It's like defending yourself against an approaching attacker by putting a huge stake in the ground. It's useless to argue about whether the stake should be fifty feet tall or a hundred feet tall, because the attacker is going to go around it.**"** [188]

While we don't agree with his pessimistic verdict regarding quantum cryptography, this comparison underlines the role of conventional security quite well.

4.2. Security proofs

Security of the BB84 protocol [14] for an idealized model of equipment including several common component imperfections has been proven beyond reasonable doubt. Following the work of Mayers [189], several proofs with slightly different model assumptions appeared [190, 191, 192, 193]. The latest GLLP proof [194] simultaneously allows for such imperfections as small basis-dependent flaws at the source and detector, and sources that emit weak coherent states. The inner workings of the proofs differ, but perhaps the most interesting is the version of the proof establishing the formal equality of the BB84 protocol with an imaginable protocol using entanglement distillation and the Calderbank-Shor-Steane quantum error correction codes [190, 194].

For an idealised model, the available bit rate after privacy amplification (i.e. the yield of the final secret key bits per bit of the sifted key) is [190]:

$$R = 1 - 2\mathrm{H}(QBER), \tag{12}$$

where H is the binary Shannon entropy $\mathrm{H}(x) = -x \log_2 x - (1-x) \log_2(1-x)$, and QBER is the quantum bit error rate measured by Bob. This function is plotted in Fig. 36. Existing error correction protocols that use two-way communication between Alice and Bob allow the bit rate in a real system to come close to within a few percent of this limit function.

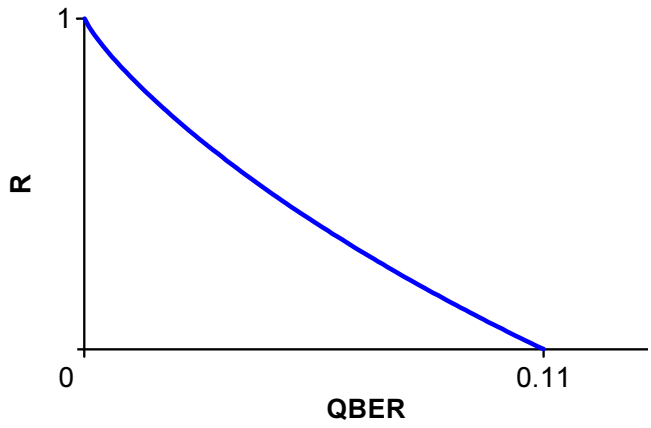


Fig. 36. The available bit rate after privacy amplification as a function of the measured QBER (Eq. 12).

The most of our work presented later in this Chapter falls outside of the model in these security proofs. We consider imperfections and countermeasures separately from the proof. In the latest paper, however, we've made an attempt to integrate the parameter describing detector efficiency mismatch with the results of the proof and obtain a security bound (see Section 4.3.3.2.).

Security of protocols other than BB84 has not been analysed to the same extent. For some of them, proofs considering individual attacks (i.e. attacks where Eve does not interact coherently with many qubits at once) exist (for SARG04, see [66]; for six-state, see [195, 196]), while for other only the simplest attacks have been considered (for DPSK, see [75, 32]).

4.2.1. Use of light source with multiphoton component

Sources that emit weak coherent states (as opposed to true single photon sources) provide an educating example of an imperfection that was initially not in the proof model, but is now fully incorporated into it. Moreover, several methods have been proposed to mitigate the detrimental effect of coherent states on the protocol performance (such as the reduction of the key generation rate and the maximum transmission distance). Systems using a weak coherent source at Alice can now be built that approach the performance of ones with a true single photon source. We review this important imperfection and countermeasures below.

For an experimenter, a very convenient and cheap light source is a laser followed by an attenuator. The state of a coherent light [197, 198]

$$\left|\mu e^{i\theta}\right\rangle = \sum_{n=0}^{\infty} \frac{\sqrt{\mu} e^{\mu/2}}{\sqrt{n!}} e^{in\theta} \left|n\right\rangle, \tag{13}$$

from such a source is actually a mixed state of

$$\rho_u = \frac{1}{2\pi} \int_0^{2\pi} \left|\mu e^{i\theta}\right\rangle\left\langle\mu e^{i\theta}\right| \mathrm{d}\theta = \sum_n P_n(\mu) \left|n\right\rangle\left\langle n\right|, \tag{14}$$

where

$$P_n(\mu) = \mu^n e^{-\mu}/n! \,, \tag{15}$$

provided the phase θ is unknown. In the case of a pulsed laser source the phase is unknown (it arises from random fluctuations every time laser generation is started); for a continuous laser source or a reflection type "plug and play" scheme the phase can be randomized by an auxiliary phase modulator.

Unfortunately, such a light pulse could be found, with the probability defined by the Poisson distribution (15), to contain more than one photon. This allows Eve to stage a powerful photon number splitting (PNS) attack.

It took some time for the research community to recognize the implications of this attack. The PNS attack is known at least since the works [14, 199], and has been ana-

lyzed in more recent works [200, 201, 202, 203]. In the most powerful version of the attack, Eve splits multiphoton pulses in the channel letting one photon pass undisturbed to Bob while keeping the rest of the photons in a quantum memory until the basis is announced, blocks all single photon pulses, and decreases the channel attenuation in order to keep Bob's detection rate the same. After the basis is announced, she measures the stored photons and obtains the full information about the key. To execute the attack, Eve should have the ability to perform the photon number measurement (and a photon splitting operation), the ability to substitute the optical channel with a lossless one (either a better physical channel or 100%-efficient quantum teleportation), quantum memory, and perfect, zero-loss optical components and detectors. The attack makes QKD insecure when the channel transmittance t becomes less than the average photon numer at Alice's output μ halved: $t < \mu/2$ (assuming $\mu << 1$; the exact insecurity bound is $t < (1 - e^{-\mu} - \mu e^{-\mu})/\mu$). Less powerful versions of the attack involving only existing technology also exist [200]. For example, with beamsplitters and perfectly efficient single photon detectors Eve could run an intercept-resend attack probabilistically measuring three-photon pulses; it would work for $t < \mu^2/24$. Although the technologies for running the most powerful version of the PNS attack are not available today, we shall not underestimate Eve, and shall consider her be only limited by the laws of physics. The most powerful version of the PNS attack severely reduces the key generation rate and the maximum transmission distance [201, 202, 203]. It turned out, several early fiber optic QKD experiments (e.g., [28]) were in fact not secure against this attack.

One way to mitigate the PNS attack is to use quantum states with low multiphoton component, which is cited as the principal advantage of entangled pair based schemes [50]. Although experimental demonstrations have been made, entangled pair sources and other single photon sources [204, 205] remain impractical outside the laboratory. Another way is to include a strong reference pulse that must be always detected by Bob [65].

Around 2003, two solutions requiring minimal modifications to the existing implementations of QKD using the BB84 protocol have been proposed. One is the SARG04 protocol, which uses the same physical setup as the BB84 and only differs in classical processing of the detection results (see Section 4.3.1.1.). It does not eliminate the effects of a weak coherent source, but allows for higher bit rates and longer transmission distances than BB84 while requiring only software modification. Another ingenious solutuion is a decoy state protocol [206, 207, 208, 209, 210, 197, 211]. The decoy state protocol is designed to guaranteely *detect* the PNS attack should Eve try to run it. Following the original proposition of Hwang [206], Alice sends coherent states choosing at random between two different average photon numbers: a normal coherent state $\left|\mu e^{i\theta}\right\rangle$ with $\mu << 1$, and a decoy coherent state $\left|\mu_{\text{decoy}} e^{i\theta}\right\rangle$ with $\mu_{\text{decoy}} \geq 1$. Besides this, she encodes into all states her qubits normally. After the transmission, Alice announces to Bob which of the two photon numbers was used for each bit. Bob divides his received bits into two groups by the announced photon number, and estimates the channel transmittances t and t_{decoy} based on the detection rate in each group. If the estimates of transmittance differ significantly, this signals Eve's PNS attack. Indeed, suppose Eve does a photon number measurement on Alice's pulse and obtains $n = 2$. Can she tell which of the two average photon numbers this pulse has had? No. If she is to proceed with the PNS attack, she has to split this pulse. However, since $\mu < \mu_{\text{decoy}}$, Eve would send on to Bob disproportionally more photons from split multiphoton pulses

for the decoy state than for the normal state (and, conversely, find $n = 1$ in normal state pulses more often than in decoy state pulses, so that normal pulses get blocked more often). This reveals her.

After Hwang's proposal [206], theoretical proofs and more efficient versions of the decoy state protocol quickly appeared. In the limit of infinite number of decoy states, the protocol completely eliminates the PNS attack and allows for a much higher optimal average photon number for any given line attenuation. Realistic protocols approaching the limit closely are possible. For instance, in Ref. 210 two decoy states — a vacuum and a very weak decoy state — are used. Examples of protocol performance for realistic sizes of data set of about 1 Gbit and 84 Gbit are given, with the latter falling 10 km short of the limit of the transmission distance (130 km instead of 140 km), while providing key generation rates for the most of the possible transmission distance range comparable to those in a system using a true single photon source. The modification to the setup required to implement the decoy state protocol is minimal: one needs to add a fast electrically controlled attenuator. The first experimental demonstration has already been done [211].

4.3. Attacks through optical loopholes

In this section, results of our studies are presented and three papers are reprinted.

Note on terminology. These and other attacks of this kind are often called *Trojan horse attacks* in the literature. However, we have not yet seen a formal definition of a Trojan horse attack in the context of a quantum cryptosystem. To us, it is difficult to draw parallels with the usage of this term in computer security (where it denotes a program with malicious payload disguised as something benign). Neither is it always easy to draw exact figurative parallels with the original, historical use of the Trojan horse[17]

[17] The Trojan Horse is part of the myth of the Trojan War.

The Greek siege of Troy had lasted for ten years. The Greeks devised a new ruse — a giant hollow wooden horse. It was filled with Greek warriors led by Odysseus. The rest of the Greek army appeared to leave and the Trojans accepted the horse as a peace offering. A Greek spy, Sinon, convinced the Trojans the horse was a gift despite the warnings of Laocoon and Cassandra. The Trojans celebrated hugely and when the Greeks emerged from the horse the city was in a drunken stupor. The Greek warriors opened the city gates to allow the rest of the army access and the city was ruthlessly pillaged — all the men were killed and all the women taken into slavery [212].

There is a small museum within the territories of ancient city Troy. The museum includes the remnants of the city and a symbolic wooden horse built in the garden of the museum to depict the legendary Trojan horse (Fig. 37).

Photo by Andreas Köhler

Fig. 37. Wooden horse in Troy.

when you consider attacks on quantum cryptosystems (unlike the usage of this term in computer security where such parallels are clear). These attacks do not always contain a signal which the legitimate parties are explicitly made aware of, hence the parallel with the horse often fails. We therefore prefer to use the term *conventional optical eavesdropping* for the large pulse attack and detection of light emission from APDs, and *faked states attack* for the attacks presented in Section 4.3.3. *Conventional optical eavesdropping* is defined as the class of eavesdropping where Eve gets information through the optical channel used to transmit quantum states, without interacting with the quantum states. Note that some of attacks in this class initially get information this way, and then interact with the quantum states using the obtained information. These attacks are also classified into conventional optical eavesdropping.

4.3.1. Large pulse attack

This section consists of our paper published in Journal of Modern Optics **48**, 2023–2038 (2001); reprinted verbatim on the following pages, with its own list of references on p. 95 and own figures numeration inside the paper.

The paper is then followed by notes on the SARG04 protocol and a single-detector BB84 protocol patent, both of which have been introduced after the paper was published, as well as a review of a quantitative evaluation of Eve's information given by Gisin et al. [213].

JOURNAL OF MODERN OPTICS, 2001, VOL. 48, NO. 13, 2023–2038

Large pulse attack as a method of conventional optical eavesdropping in quantum cryptography

ARTEM VAKHITOV†, VADIM MAKAROV‡§ and DAG R. HJELME‡

†Department of Quantum Electronics, St Petersburg State Technical University (SPbSTU), Politechnicheskaya street 29, 195251 St. Petersburg, Russia

‡Department of Physical Electronics, Norwegian University of Science and Technology (NTNU), N-7491 Trondheim, Norway

§http://www.vad1.com

(*Received 15 January 2001; revision received 12 June 2001*)

Abstract. In this paper so-called 'large pulse attack' is investigated. This attack is one of the possible methods of conventional optical eavesdropping, a new strategy of eavesdropping on quantum cryptosystems, which eliminates the need of immediate interaction with transmitted quantum states. It allows the eavesdropper to avoid inducing transmission errors that disclose her presence to the legal users. As an object of the eavesdropping, phase-state fibre optic schemes are considered. With large pulse attack, settings of transmitting and/or receiving apparatus are interrogated by external high-power light pulses. Applicability conditions of this method are given. Type and amount of information learned by the eavesdropper is estimated, depending on parameters of the interrogating pulse and apparatus. An experimental set-up for an eavesdropping experiment is proposed and results of successful preliminary measurements are presented. It is concluded that additional protection is necessary for currently implemented quantum key distribution systems. The paper suggests several security measures against this kind of attack.

1. Introduction

Many studies of eavesdropping in quantum cryptography have been made over the last few years [1–16]. In these papers, security of quantum cryptography against different kinds of quantum attacks was analysed—from simple beamsplitting and intercept/resend attacks to complex generalized joint attacks, which manipulate all transmitted quantum states as a whole. The eavesdropper's capabilities are typically assumed to be limited only by the laws of physics, not by the current level of technology, and in this paper we shall follow this tradition. Security of quantum cryptography was proven in general for all individual attacks [10, 11], where every single transmitted state is treated separately by Eve. It was also proven for all collective attacks [7, 13], where each transmitted state is attached to a separate probe, but after that, measurement is performed collectively on all probes. Finally, the proof was generalized for any eavesdropping attack [12, 15, 16], provided, however, an ideal single-photon source is used. Practical limits of security were established for the case of a noisy environment and imperfect

Journal of Modern Optics ISSN 0950–0340 print/ISSN 1362–3044 online
http://www.tandf.co.uk/journals
DOI: 10.1080/09500340110074691

detection as well as non-ideal light sources [6, 8–11]. The common feature of all these attacks is the fact that Eve performs her measurements on the quantum states transmitted from Alice to Bob, therefore inevitably disturbing these states and inducing transmission errors. However, this is not the only possibility for eavesdropping on quantum key distribution (QKD) systems.

We will call *conventional optical eavesdropping* the strategy where Eve can get information by using loopholes in Alice's and Bob's optical set-up rather than by measuring the transmitted quantum states. Here are the possibilities we have found so far for this kind of eavesdropping.

(1) *Large pulse attack*. In a wide class of QKD schemes, the states forming the quantum alphabet are prepared by modulation of certain parameters of propagating light, such as polarization or phase. It can be done with phase modulators (e.g. Pockels cells) situated inside transmitter and receiver. With these kinds of QKD schemes, let us consider Eve launching a bright light pulse into the transmission line towards Alice's or Bob's set-up. Some part of this pulse will be reflected back from different optical components inside the set-up, because any real component has a non-zero reflection coefficient. On its way, the pulse can pass internal modulators and be modulated one or more times. Measuring characteristics of reflected pulses, Eve can make some conclusions on the modulator's settings and, as we will show later, if not learn the transmitted bits directly, then at least know transmission or detection bases, which will allow her to detect transmitted quantum states unambiguously. This attack was briefly mentioned in [17] and discussed a bit more in detail in a recent IBM paper [18], where it was called a 'large pulse attack'.

(2) *High-power destruction of optical components*. High-power external pulses can in principle make intentional changes in Alice's and Bob's optical components, which may facilitate further attacks. For example, damaging Alice's output attenuator in a way that will reduce its attenuation would make both beamsplitting (as well as other quantum attacks) and large pulse attack more efficient.

(3) *Light emission from avalanche photodiodes (APDs) during detection*. APDs are currently used as single-photon detectors in QKD schemes. An APD junction emits light over a broad spectrum during avalanche [19]. Part of this light leaks back into the communication fibre, where it can be detected by Eve. A recent study hints that the amount of light leaking back into the APD fibre pigtail is a few orders of magnitude less than one photon per avalanche [20]. However, more studies are necessary, notably for InGaAs detectors over a wide emission spectral range including wavelengths longer than 1.6 μm, which currently presents some experimental difficulty.

In this paper, we will consider in detail the first of these possibilities—large pulse attack, including several important features that have been missed in the two papers [17, 18] mentioned above. We will restrict our study to fibre-optic phase state QKD systems using protocols BB84 [21] and B92 [22]. As an example, Townsend's scheme [23] will be considered, but most results are also applicable to other existing fibre-optic and free-space QKD schemes. A special discussion will be devoted to 'plug & play' schemes [17, 18].

2. Eavesdropping set-up

The general structure of the eavesdropping set-up for performing large pulse attack is shown on figure 1. Light pulses emitted by the laser are divided into scanning and reference pulses on the coupler. Scanning pulses propagate towards Alice's or Bob's set-up through the optical multiplexer, then, after reflecting back, through the same multiplexer and coupler, enter the detection scheme. We assume that Eve will use the most sensitive detection method, i.e. homodyne detection, and hence will need reference pulses. They are delayed in the reference arm to arrive at the detection scheme simultaneously with the chosen reflected pulses. The particular content of the detection scheme depends on what parameter of the signal Eve measures. The optical multiplexer is necessary for the photons sent by Alice to pass undisturbed to Bob.

If only time domain multiplexing is used, it may cause problems due to Rayleigh backscattering: if Alice's photon and Eve's scanning pulse meet somewhere, then some amount of backscattered light from the scanning pulse can reach Bob's detector, which is undesirable to Eve, because it can cause additional detection errors at Bob. Eavesdropping on a wavelength different from that used for transmission and, correspondingly, wavelength domain multiplexing can eliminate this effect.

Before starting to consider how Eve can extract information in phase state QKD systems, we should explain the necessary details of phase modulator operation and also make some assumptions.

Standard telecommunication voltage-controlled phase modulators would normally be used in Alice's and Bob's set-ups. With the BB84 protocol, there are four voltage levels corresponding to the four possible values of phase shift used at Alice's modulator, and two levels used at Bob's modulator corresponding to the two possible detection bases. With B92, two voltage levels on either side are used. All these voltage levels change in a random order from one bit to another, according to the protocol. Let us call *transmission cycle* the full time interval needed for transmission of a single bit. In figure 2, two sequential transmission cycles are presented. Each transmission cycle consists of three parts.

(1) Rise time or fall time, depending on whether the phase shift value in the previous cycle corresponds to a lower or a higher voltage level. The parameter τ_{rf} will denote here the longest possible rise/fall time.
(2) Settling time. For correct detection, phase shift at the modulator must be set with certain precision (estimates made for our QKD set-up [24] require

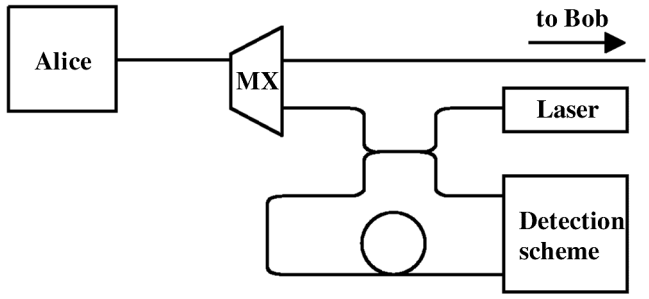


Figure 1. General structure of eavesdropping set-up.

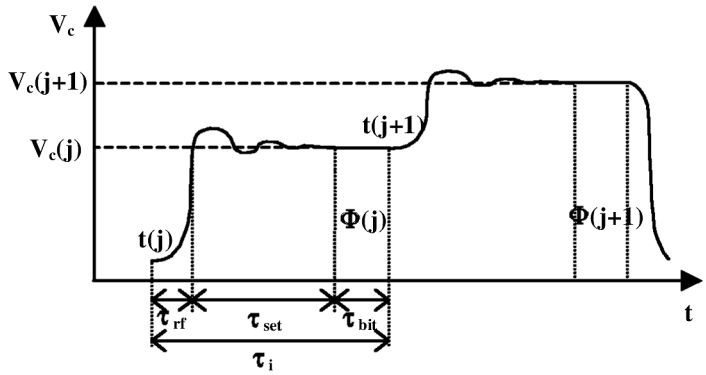


Figure 2. Transmission cycle and time parameters.

precision of about $\pm(5-10)^\circ$). The control voltage cannot settle immediately to the required accuracy, and during a certain period of time denoted τ_{set} some ringing will always occur.

(3) Bit slot, during which a photon passes the modulator and acquires phase shift. This time is denoted as τ_{bit}.

Besides this, $t(j)$ and $t(j+1)$ denote the beginning of the jth and the $(j+1)$th transmission cycles, correspondingly, $\Phi(j)$ and $\Phi(j+1)$ are phase shifts coding the information bits transmitted in these cycles, and $V_{\text{c}}(j)$ and $V_{\text{c}}(j+1)$ are the corresponding phase modulator voltages.

Assumptions and constraints to Eve's interrogation pulses.

(a) First, it is clear that Eve's pulses should not pass modulators during the rise/fall time of the control voltage, otherwise her measurement will be greatly complicated.

(b) The situation when the phase modulation efficiency for Eve's pulses and for transmission pulses is the same results in some special cases that we consider below. We will assume this by default. Modulation efficiency will be the same if Eve's interrogation wavelength is close to Alice's transmission wavelength.

(c) If Eve chooses not to employ wavelength domain demultiplexing, her pulses must not coincide in time with photons transmitted as they exit Alice's set-up, otherwise she will not be able to separate them. That is to say, Eve's pulses being *on the way out* must not pass the modulator during the bit slot. Thus, the only time interval allowed here is τ_{set}. With wavelength domain multiplexing, this constraint is not necessary.

(d) Since positions of reflecting elements inside Alice's and Bob's set-ups are not in Eve's control, she will not always be able to arrange her measurements in such a way that her pulses will pass the modulator during the bit slot or very close to it. In many cases this will occur in the middle or even at the beginning of the settling time. Oscillations of control voltage during this interval can result in phase errors of 10°–20° (according to the measurements made on our own set-up), but this is acceptable for Eve since she does not need high accuracy to learn most of the bits, and it also helps that she uses multiphoton pulses.

(e) Eve may be practically tempted to use as wide interrogation pulses as possible to increase their energy and level of the signal she has to detect. We will neglect the facts that Eve's interrogating pulses have a non-zero width and the control voltage varies during τ_{set}.

Each of the interrogation pulses sent by Eve will produce a number of reflected pulses. The most important characteristics of these reflected pulses are (a) resulting phase shift acquired by them due to the modulation(s) in Alice's or Bob's set-up, and (b) delay between two successive modulation events in the case of multiple modulation. These characteristics, which Eve must consider given, determine what information Eve can learn by detecting a specific reflected pulse. Here we restrict ourselves to the cases of single and double modulation. Three scenarios are then possible for Eve: (a) learning transmission/detection bases; (b) guessing the raw key from a few possible variants; and (c) learning the raw key immediately.

3. Direct and indirect detection of information bits

To get the raw key directly, Eve can detect the pulses reflected from Alice's set-up and modulated only once during their travel inside it (if such pulses exist). It is clear that the modulation in this case must occur *either* on the way in, before the reflection, *or* on the way out, after the reflection. The possible values of the phase shift can be determined unambiguously, assuming that the bright interrogation pulses sent by Eve return her multiphoton reflections.

Consider now an interrogation pulse launched by Eve into Alice's set-up and modulated there twice during two adjacent transmission cycles: first time on the way in, during τ_{set} or the τ_{bit} time slots of the first transmission cycle, and second time on the way out, during τ_{set} or the τ_{bit} time slots of the second transmission cycle (see figure 3). Note that if only time-domain multiplexing is used, the second τ_{bit} interval must be excluded because the reflected pulse must not coincide in time with Alice's transmitted photon, as mentioned above. The delay between the two modulation events will be further referred to as $2\tau_R$. Neither of these events must occur during the τ_{rf} slot, so the general constraint for the delay in this case is

$$\tau_{rf} < 2\tau_R.$$

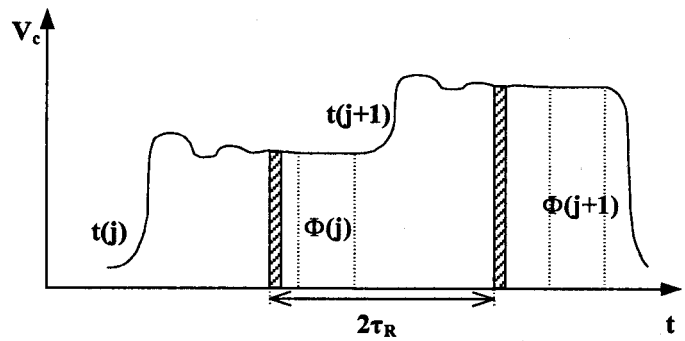


Figure 3. Eve's pulse passing the phase modulator for indirect detection of information bits.

Table 1. Illustration of indirect detection of information bits (BB84).

Alice's bits	1	0*	0	1	1*
Alice's phase shifts	π	$\pi/2$	**0**	π	$3\pi/2$
Phase shifts detected by Eve	—	$3\pi/2$	$\pi/2$	π	$\pi/2$
Possibilties for phase shifts in key sequence	0?	$3\pi/2$	π	0	$\pi/2$
	$\pi/2$?	π	$3\pi/2$	$3\pi/2$	π
	$3\pi/2$?	0	π	0	$\pi/2$
	π?	$\pi/2$	**0**	π	$3\pi/2$

The phase shift acquired by Eve's pulse will be equal to the sum of phase shifts in both transmission cycles:

$$\Phi_{\mathrm{E}} = (\Phi(j) + \Phi(j+1)) \bmod 2\pi.$$

Note that the value of Φ_{E} itself will be equal to one of the possible phase shift values used in the protocol. Detection of this phase shift will give Eve an ambiguous result, because she does not know the phase shift acquired in the first transmission cycle. However, there are only a few possible values for this phase shift, i.e. four in BB84 and two in B92. It means that Eve will have to guess the right key sequence from only four or even two variants. In practical cryptography, this is equivalent to the knowledge of the key. Table 1 illustrates this guessing procedure.

The above discussion is also applicable to interrogating Bob's modulator, but only with the B92 protocol, since in BB84 Bob's phase shifts determine only detection bases, not bit values.

What if $2\tau_{\mathrm{R}}$ is so long that the two modulation acts are not in adjacent transmission cycles? In general, if the first modulation act happens in the jth transmission cycle and the second in the $(j+n)$th transmission cycle, then the number of possible key sequences is 4^n for BB84 and 2^n for B92.

If, however, Eve is using a substantially different wavelength, then it might happen, due to different phase modulation efficiency for her pulse, that even with double modulation she can learn information bits, not only bases.

4. Detection of transmission bases

Security of the BB84 protocol, at least in the QKD schemes considered now, is based on the fact that during the transmission Eve knows neither bases in which Alice encodes key bits nor bases in which Bob attempts to detect them. If Eve somehow manages to get the value of either Alice's or Bob's basis *before* Alice's photon reaches Bob's location, then the whole scheme is no longer secure, and Eve can implement an ideal 'intercept/resend' attack without being caught. Now we will show that determining transmission and/or detection bases is possible by means of large pulse attack.

(1) The first and also obvious case is when Eve's pulse is modulated once during its travel inside *Bob's* set-up, and two possible values of acquired phase shift correspond to Bob's two possible detection bases. Similarly to the case of direct detection of information bits, Eve's pulse passes Bob's modulator *either* on the way in *or* on the way out, but not on both. If τ_{PM} is

the time required for an optical pulse to propagate from Eve to Bob's phase modulator, and τ_{back} is the time required for the pulse to propagate back to Eve after the reflection, then the condition for a successful attack is

$$\tau_R + \tau_{back} + \tau_{PM} < \tau_{set}.$$

One can easily check that if this condition is satisfied, Eve will have enough time to receive the reflected pulse modulated in Bob's modulator during τ_{set}, determine Bob's detection basis that he is preparing to use, then 'catch' Alice's photon before it enters Bob's site, detect it in this basis, and re-send it further to Bob in this basis. This way, Eve ideally never causes additional errors that would reveal her presence.

(2) If Eve's pulse is modulated twice inside Bob's set-up, once before and once after being reflected, so that both modulation events occur during the τ_{set} time interval for a the same transmission cycle, then the condition of successful attack will be

$$2(\tau_R + \tau_{PM}) < \tau_{set}.$$

(3) Yet another case is when the interrogation pulse is modulated twice inside *Alice's* set-up, once before and once after being reflected, so that the modulation events occur during the τ_{set} time interval of the same transmission cycle (see figure 4). Parameter τ_R of the chosen reflected pulse must satisfy the condition

$$2\tau_R < \tau_{set}.$$

In cases 2 and 3, the value of the phase shift acquired by the pulse will double:

$$\Phi_E = 2\Phi(j) \bmod 2\pi.$$

It is easy to see that the resulting phase value will be determined by the transmission or detection basis: $\Phi_E = 0$ if $\Phi(j) = 0$ or π, and $\Phi_E = \pi$ if $\Phi(j) = \pi/2$ or $3\pi/2$.

Let us also note that Eve's intercept/resend equipment in practice would introduce additional delay to the transmitted photons. If we assume that propagation delay for all communication between Alice and Bob is not authenticated, then Eve can introduce a constant delay into all communication between them to compensate for her processing delay. Alternatively, Eve can exploit the fact that the signal propagation speed in a free-space radio link is faster than that in optical

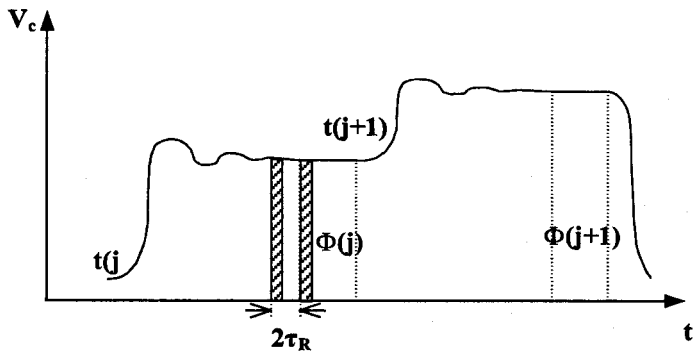


Figure 4. Eve's pulse passing the phase modulator for bases detection.

fibre, and employ such radio links in her set-up to cancel her processing delay [25]. An appropriately constructed electrical cable connection could also be used.

5. Notes on bases detection at Bob's site

It should be pointed out that even if Eve gets information about detection basis only after the photon enters Bob's site, she can still learn some additional information about the key. Let us consider Eve performing, in addition to detection of transmission bases at Bob's site, the well-known beamsplitting attack. The following is typically assumed [18].

(1) If f is the fraction Eve is splitting off from each transmitted pulse and μ is the average photon number per pulse, then she will get a fraction $[1 - \exp(-f\mu)]$ of all transmitted pulses, or $\sim f\mu$ for small $f\mu$. This gives Eve a fraction $f\mu/2$ of the error-corrected key, where the factor of $\frac{1}{2}$ is due to the necessity of applying random detection bases to split pulses.
(2) If Eve tries to store photons until the public discussion, when the bases are announced, Alice and Bob can always delay this discussion by arbitrary time sufficient for most stored photons to decay.

However, if τ_{PM}, τ_{back} and τ_R delays in Bob's set-up are such that Eve gets basis information in a short time after the transmitted pulse has left her location, then Eve can simply delay the split pulse for this short time and after that detect it in the correct basis. Thus, with bases detection the estimate of $f\mu/2$ is wrong, and it should be assumed that Eve can obtain the whole $f\mu$ fraction of the transmitted key through a beamsplitting attack, which is the same as if she were granted the ability to store photons for unlimited time.

6. Security measures

The greater part of this section will assume the BB84 protocol, and only the last paragraphs will be devoted to B92.

As a security measure against large pulse attack, it was proposed in [17, 18] for 'plug & play' systems to monitor intensity of incoming light in Alice's set-up, presumably over a wide range of wavelengths. In these systems, which are essentially asynchronous, *Bob* first sends to Alice relatively intense light pulses, which serve *inter alia* to provide synchronization signals upon registering by a special timing detector in Alice's set-up (figure 5). Thus, one can make this detector alarm honest participants when average power and/or peak intensity of an incoming pulse rises above a specified level. However, attention was not paid to the fact that the system remained insecure against detection of transmission bases at Bob's site.

We will now offer simple passive security measures against large pulse attack. These measures are different for Alice and Bob.

For practical security of Bob's site against detection of *transmission bases*, it would be sufficient that, for any possible potentially 'harmful' reflection, one of the following conditions is satisfied:

$$\tau_R + \tau_{back} + \tau_{PM} > \tau_{set}$$

or

$$2(\tau_R + \tau_{PM}) > \tau_{set},$$

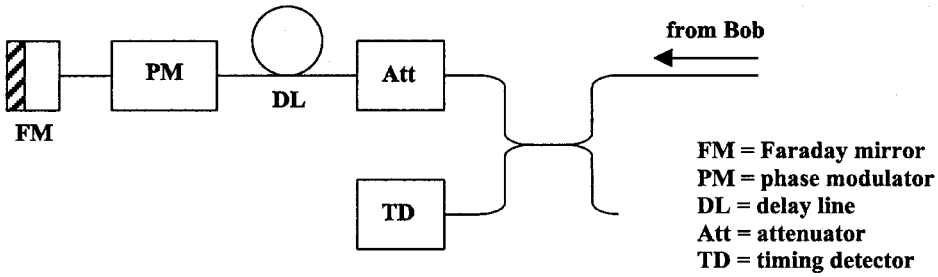


Figure 5. Alice's set-up in the 'plug & play' scheme.

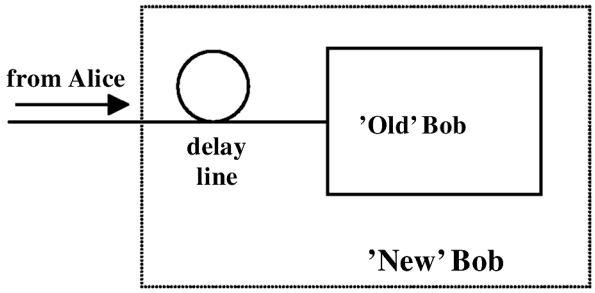


Figure 6. Passive security measures for Bob's set-up.

depending on the type of large pulse attack (single or double modulation, respectively). Normally, Bob will not know Eve's position, but it is enough to satisfy the inequalities assuming that she is sitting right at the input of Bob's set-up. If they are not satisfied, the solution is to put a delay line of appropriate length at the input of Bob's set-up (inside the secure site), thereby increasing τ_{back} and τ_{PM} delays, as shown on figure 6. Really, if one makes this delay line long enough to provide one-directional propagation delay of $\tau_{\text{set}}/2$, security conditions will be automatically satisfied. In fact, in many high-speed QKD systems this condition will be satisfied without any additional delay line, but one should be aware of the problem. This solution can be applied to any QKD scheme, including 'plug & play'.

The problem of security of Bob's site against direct and indirect detection of *information bits* appears only with the B92 protocol and will be discussed later.

The passive measures for Alice's site described below are not suitable for 'plug & play' systems, so the proposals made in [17, 18] are still valid. Now our description will concern Townsend's scheme.

First, the existing set-up must be slightly revised. In practice, instead of true single-photon states, Alice uses weak coherent pulses prepared by attenuating light from a laser to average intensity of about 0.1 photon per pulse. The attenuator can be situated immediately at the laser output (upper half of figure 7) or at the very output of Alice's set-up (lower half of figure 7), and there is no obvious reason not to do it the latter way. Indeed, for Eve this will mean a significant increase of power required of her laser: namely, if the attenuator at the output of Alice's set-up is set to A dB, then Eve's required laser power increases by $2A$ dB at once. In our QKD set-up [24], a standard telecommunication laser diode is used as the light

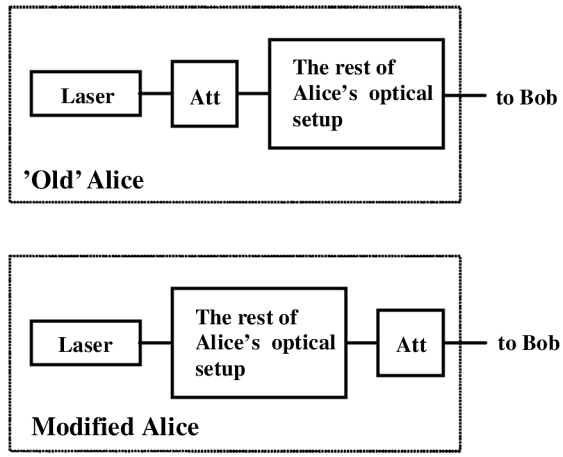


Figure 7. Modification of Alice's set-up.

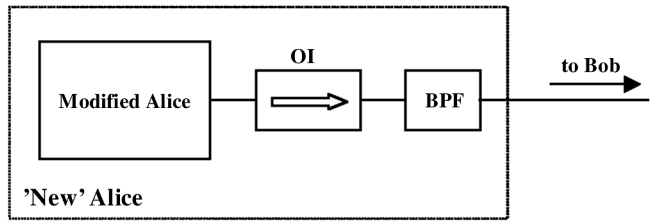


Figure 8. Passive security measures for Alice's set-up.

source (1310 nm, 100 ps wide pulses of about 1 mW peak power), and the output attenuator is set to about 60 dB, which introduces 120 dB of attenuation for Eve's pulse. We will refer to this set-up as the 'modified Alice's set-up'.

Then, we must add a couple of optical components. In figure 8, Alice's set-up modified as described above is connected with the communication channel through an optical isolator (OI) and band-pass filter (BPF). The optical isolator does not affect much the signal propagating from Alice, but strongly reduces the signal propagating in the opposite direction (for existing isolators, attenuation is about 50 dB). Efficiency of this device is wavelength dependent (its characteristics are typically stable in a range of several tens of nanometres), but the band-pass filter helps to cope with this problem. Thus, this construction introduces an overall attenuation $A_{\text{sum}} \approx 120 + 50 = 170$ dB for the pulse interrogating Alice's set-up. Now we can make an estimate of the minimum required laser power for Eve.

The following equation holds:

$$\mu h\nu = 10^{(-A_{\text{sum}}/10)} RP\tau,$$

where μ is the minimum average photon number per pulse that Eve requires for successful detection, h is Planck's constant, ν is the optical frequency, R is the coefficient of reflection from the rest of Alice's set-up, P is the peak power of Eve's interrogation pulse and τ is the width of Eve's interrogation pulse. Then the minimum peak power of Alice's interrogation pulse will be

$$P = \mu h\nu (10^{(-A_{\text{sum}}/10)} R\tau)^{-1}.$$

Let us assume $A_{\text{sum}} = 170\,\text{dB}$, $R = 1$ (really it is less than 0.1), $\nu = 10^{14}\,\text{Hz}$ (near infrared radiation), $\mu = 1$, and calculate P for two values of τ: $\tau_1 = 10^{-10}\,\text{s}$ (this is a typical width of pulses used by Alice and Bob) and $\tau_2 = 10^{-8}\,\text{s}$ (because Eve may want to use a broader pulse to increase its energy). By an order of magnitude, $P(\tau_1) \sim 10^8\,\text{W}$ and $P(\tau_2) \sim 10^6\,\text{W}$.

As you may see, even with our somewhat conservative assumptions, such a high-power fibre-optic laser, which Eve needs, is something close to science fiction (the most powerful commercially available fibre-optic pulsed lasers have peak power of about 1–10 kW [26]). Nevertheless, to make things more demonstrative, let us now calculate the power density S it would induce in the fibre, assuming a typical core area of $\sigma^2 = 100\,\mu\text{m}^2 = 10^{-6}\,\text{cm}^2$:

$$S(\tau_1) = P(\tau_1)/\sigma = 10^8\,\text{W}/10^{-6}\,\text{cm}^2 = 10^{14}\,\text{W cm}^{-2}$$

and

$$S(\tau_2) = P(\tau_2)/\sigma = 10^6\,\text{W}/10^{-6}\,\text{cm}^2 = 10^{12}\,\text{W cm}^{-2}.$$

Thus, even for long pulses, the required power density will significantly exceed the damage threshold of the fibre, which we assume is about $10^9\,\text{W cm}^{-2}$.

Let us remind the reader that these estimates are valid for Townsend's scheme with an attenuated light source. If, however, one uses a *true* single-photon source instead of an attenuated light source, then it makes no sense to put an attenuator at Alice's output, and the proposed protection is not applicable. Also, round-trip systems like 'plug & play' do not allow the use of non-reciprocal devices such as optical isolators, and this is why our solution for Alice is not suitable for 'plug & play' systems.

If the B92 protocol is used instead of BB84, it makes it more difficult to defend Bob's site against large pulse attack. Eve can now learn information bits by interrogating Bob, not only detection bases. Passive security measures against it are impractical, because any additional component will introduce loss and thus impair the maximum transmission distance and key generation speed. We cannot put an attenuator at the input of Bob's set-up, like we did with Alice, and an optical isolator itself does not have enough attenuation to provide security. Thus, one has to monitor the intensity of the incoming light. Bob will have to split off some part of the incoming light (figure 9) to a special sensitive alarm detector (AD) and probably install additional components into the optical path. Note that Eve can interrogate Bob's site with signals of very low intensity.

Unlike 'plug & play' systems, Townsend's scheme allows here the variation shown on figure 10, which reduces requirements to sensitivity of Bob's alarm detector. The incoming light propagates freely in an optical circulator (OC) from port 1 to port 2 and then to Bob's 'old' set-up, and most of the reflected light propagates from port 2 to port 3 to the alarm detector (Det). The optical band-pass filter (BPF) serves to compensate somewhat for changes in the characteristics of the optical circulator at different wavelengths.

To conclude, using the B92 protocol does not seem very practical. Luckily, it is also considered less secure for other reasons and is rarely used now.

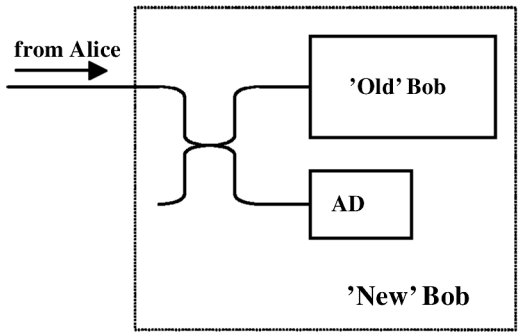


Figure 9. Active security measures for Bob's set-up with the B92 protocol.

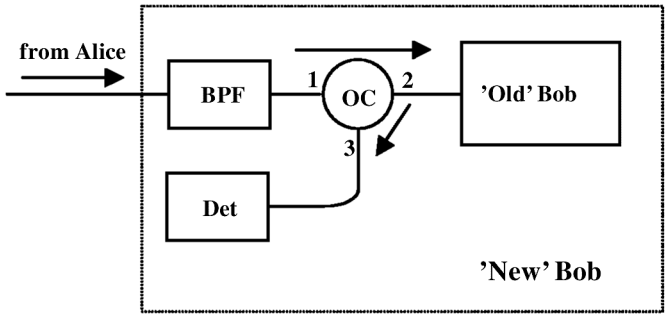


Figure 10. Active/passive security measures for Bob's set-up with the B92 protocol, with low additional losses and weaker requirements to the sensitivity of the alarm detector.

7. Simple experiment

Reflection coefficients of modern optical components are indeed made very low thanks to good anti-reflection coatings, but they are non-zero anyway. It is also good to remember that an anti-reflection coating is made for specific wavelengths, so if Eve chooses for interrogation a wavelength different from that specified for the coating, then she can get much larger reflection. Figure 11 shows typical values of return loss for different optical components. As one can see from the chart, the most suitable reflecting components for large pulse attack are free fibre ends, non-angled polished optical connectors, lasers and detectors. All in all, large pulse attack seems to be extremely feasible.

We arranged a simple experiment using the optical part of our QKD scheme [24], which has a structure similar to Townsend's system. The experimental set-up is shown on figure 12. Eve's equipment is built around a standard optical time domain reflectometer (OTDR)—millimetre resolution OTDR system produced by Opto-Electronics, Inc., which in this configuration provides us with a medium-power 1300 nm pulsed laser, sensitive time-selective detector and 50/50 coupler. Eve's laser pulses are divided on the coupler into a scanning and a reference pulse. After entering Alice's half of the interferometer, the scanning pulse propagates through its long arm which contains the phase modulator, and after being reflected from the free fibre end it propagates back through the same arm. We should note that reflection from the free fibre end in our QKD scheme existed well before we

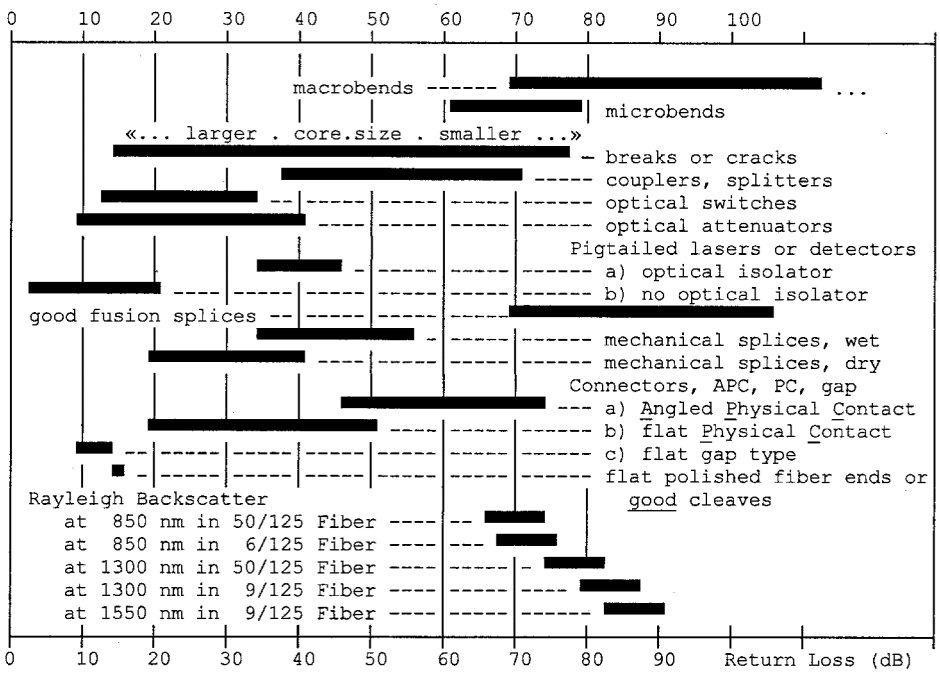


Figure 11. Typical values of reflection coefficients for different fibre-optic components. Courtesy of Opto-Electronics, Inc. (http://www.opto-electronics.com/).

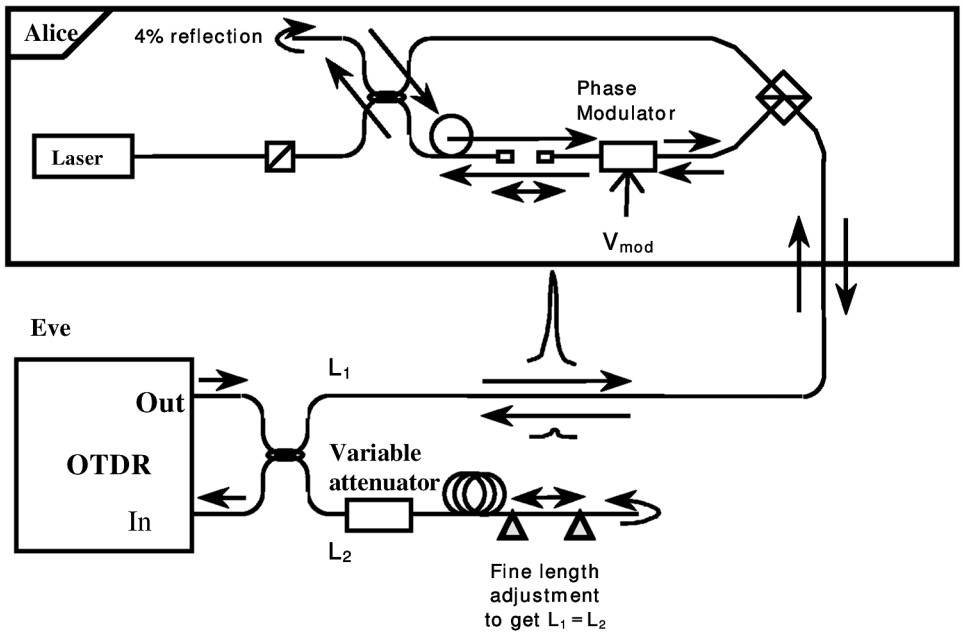


Figure 12. Schematic of our eavesdropping experiment. Interrogating Alice's phase modulator.

realized it could be used by Eve, as were several other reflections. The returned scanning pulse at the input of the OTDR detector was delayed by 88.85 ns and its level relative to the outgoing scanning pulse was −58 dB. The reference pulse was attenuated to the same level and delayed for the same time, to obtain interference with high fringe visibility on Eve's coupler. Polarization controllers not shown on the figure were used to steer the scanning pulse into Alice's proper arm and to match the polarization of the reflected and the reference pulses. The result of interference between reflected and reference pulses was registered by an APD-based detector. Since the laser that we used did not have enough power and the OTDR system was indeed not optimized for eavesdropping tasks, we removed the optical attenuator from Alice's set-up; no other changes to it were made.

Assuming the BB84 protocol, four static voltage levels were used to control the phase shift on Alice's modulator: 0, 2, 4 and −2 V, which corresponded to phase shift values for a scanning pulse of 0, $\pi/2$, π and $3\pi/2$. A static modulator voltage is equivalent to one infinite transmission cycle, so the experiment reproduces the situation with bases detection. Applying these static voltages, we observed constructive interference when the phase shift on the modulator was 0 or π, and destructive interference when the phase shift was $\pi/2$ or $3\pi/2$. Fringe visibility was about 0.9, and the phase drift constant was around $2\,\mathrm{min}/2\pi$ by its order of magnitude (some thermo-isolation was used for Eve's reference arm to slow the phase drift down). Thus, the experiment confirmed that remote reading of internal modulator settings by an external optical pulse is possible.

8. Conclusions

The following important conclusions can be made on large pulse attack and conventional optical eavesdropping (statements regarding Townsend's scheme may be applicable to other fibre-optic [27–29] and free-space [30] schemes, and of course to the original ones [21, 22]):

(1) QKD systems without internal optical modulators such as the Koashi–Imoto set-up [31] or EPR-based systems [32] are intrinsically immune to large pulse attack, because signals reflected from these systems cannot carry any information on quantum states transmitted. However, only one such system has been recently implemented [33].
(2) The BB84 protocol is generally preferable over B92. With Townsend's scheme, B92 does not allow passive security measures for Bob's set-up. With 'plug & play' schemes, B92 places strong requirements on the sensitivity of Bob's alarm detector.
(3) Large pulse attack with bases detection can double the amount of information that Eve obtains through a conventional beamsplitting attack. Note that granting Eve the ability to store photons for unlimited time leads to the same result.
(4) Security measures against large pulse attack include the following.
    (a) For Townsend's scheme with the BB84 protocol—passive measures both for Alice (figure 8) and Bob (figure 6). *It seems to be the easiest scheme to protect.*
    (b) For Townsend's scheme with the B92 protocol—passive measures for Alice (figure 8) and active/passive for Bob (figure 10).

(c) For 'plug & play' schemes with the BB84 protocol—active measures for Alice (figure 5) and passive for Bob (figure 6).
(d) For 'plug & play' schemes with the B92 protocol—active measures both for Alice (figure 5) and Bob (figure 9).

(5) Using a true single photon source (except in EPR-based schemes) will make passive defense of Alice's site against large pulse attack impossible.
(6) Feasibility of large pulse attack is experimentally confirmed.
(7) Further studies are required on the methods of conventional optical eavesdropping other than large pulse attack, such as light emission from an APD and high-power destruction of optical components.

To answer skeptics, we do believe that quantum cryptography is secure, but there are more issues to be carefully considered.

Acknowledgments

The study was supported by the Norwegian Research Council (NFR), project no. 119376/431; visit our project Web site at http://www.fysel.ntnu.no/Optics/qcr/ We also thank Andre Mlonyeni, Telenor R&D and Professor S. Cova, Politecnico di Milano for helpful discussions.

References

[1] Huttner, B., and Ekert, A. K., 1994, *J. mod. Optics*, **41,** 2455.
[2] Bennett, C. H., Brassard, G., Crepeau, C., and Maurer, U. M., 1995, *IEEE Trans. Inf. Theory*, **41,** 1915.
[3] Fuchs, C. C., and Peres, A., 1996, *Phys. Rev.* A, **53,** 2038.
[4] Hwang, W. Y., and Koh, I. G., 1997, quant-ph/9702037 v2.
[5] Lütkenhaus, N., 1996, *Phys. Rev.* A, **54,** 97.
[6] Mayers, D., and Yao, A., 1998, quant-ph/9809039.
[7] Biham, E., and Mor, T., 1997, *Phys. Rev. Lett.*, **78,** 2256.
[8] Brassard, G., Lütkenhaus, N., Mor, T., and Sanders, B. C., 1999, quant-ph/9911054.
[9] Dusek, M., Jahma, M., and Lutkenhaus, N., 1999, quant-ph/9910106.
[10] Lütkenhaus, N., 1999, quant-ph/9806008 v2.
[11] Lütkenhaus, N., 2000, quant-ph/9910093 v2.
[12] Mayers, D., 1998, quant-ph/9802025 v4.
[13] Biham, E., Boyer, M., Brassard, G., van de Graaf, J., and Mor, T., 1998, quant-ph/9801022.
[14] Yuen, H. P., 1996, *Quantum semiclass. Optics*, **8,** 939.
[15] Biham, E., Boyer, M., Oscar Boykin, P., Mor, T., and Roychowdhury, V., 2000, *Proceedings of the Thirty-Second Annual ACM Symposium on Theory of Computing*, Portland, Oregon, USA, 21–23 May, New York: Association for Computing Machinery, pp. 715–724.
[16] Shor, P., and Preskill, J., 2000, *Phys. Rev. Lett.*, **85,** 441.
[17] Ribordy, G., Gautier, J.-D., Gisin, N., Guinnard, O., and Zbinden, H., 2000, *J. mod. Optics*, **47,** 517.
[18] Bethune, D. S., and Risk, W. P., 2000, *IEEE J. quantum Electron.*, **36,** 340.
[19] Lacaita, A. L., Zappa, F., Bigliardi, S., and Manfredi, M., 1993, *IEEE electron. Devices*, **40,** 577.
[20] Kurtsiefer, C., Zarda, P., Mayer, S., and Weinfurter, H., 2001, *J. mod. Optics* '*Technologies for Quantum Communications*', to appear.
[21] Bennett, C. H., and Brassard, G., 1984, *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, pp. 175–179.

[22] Bennett, C. H., 1992, *Phys. Rev. Lett.*, **68,** 3121.
[23] Marand, C., and Townsend, P. D., 1995, *Optics Lett.*, **20,** 1695.
[24] Results of our work are not published yet, but some information is available at http://www.fysel.ntnu.no/Optics/qcr/
[25] Vakhitov, A., 2000, MSc thesis, Department of Quantum Electronics, St. Petersburg State Technical University: available at http://www.fysel.ntnu.no/Optics/qcr/ artem/
[26] See, for example, pulsed erbium fibre laser ELPD-1K, http://www.ire-polusgroup.com/erbLas/EFLGuide.htm
[27] Zbinden, H., BehcmannPasquinucci, H., Gisin, N., and Ribordy, G., 1998, *Appl. Phys.* B, **67,** 743.
[28] Sun, P. Ch., Fineman, E., and Mazurenko, Yu., 1995, *Optics Spectrosc.*, **78,** 887.
[29] Mérolla, J.-M., Mazurenko, Yu., Goedgebuer, J.-P., and Rhodes, W. T., 1999, *Phys. Rev. Lett.*, **82,** ??.
[30] Jacobs, B. C., and Franson, J. D., 1996, *Optics Lett.*, **21,** 1854.
[31] Koashi, M., and Imoto, N., 1997, *Phys. Rev. Lett.*, **79,** 2383.
[32] Ekert, A., 1991, *Phys. Rev. Lett.*, **67,** 661.
[33] Ribordy, G., Brendel, J., Gautier, J.-D., Gisin, N., and Zbinden, H., 2001, *Phys. Rev.* A, **63,** 012309.

[End of reprinted paper]

In Fig. 38 on the next page, you can see how Eve's setup looked like in the lab.

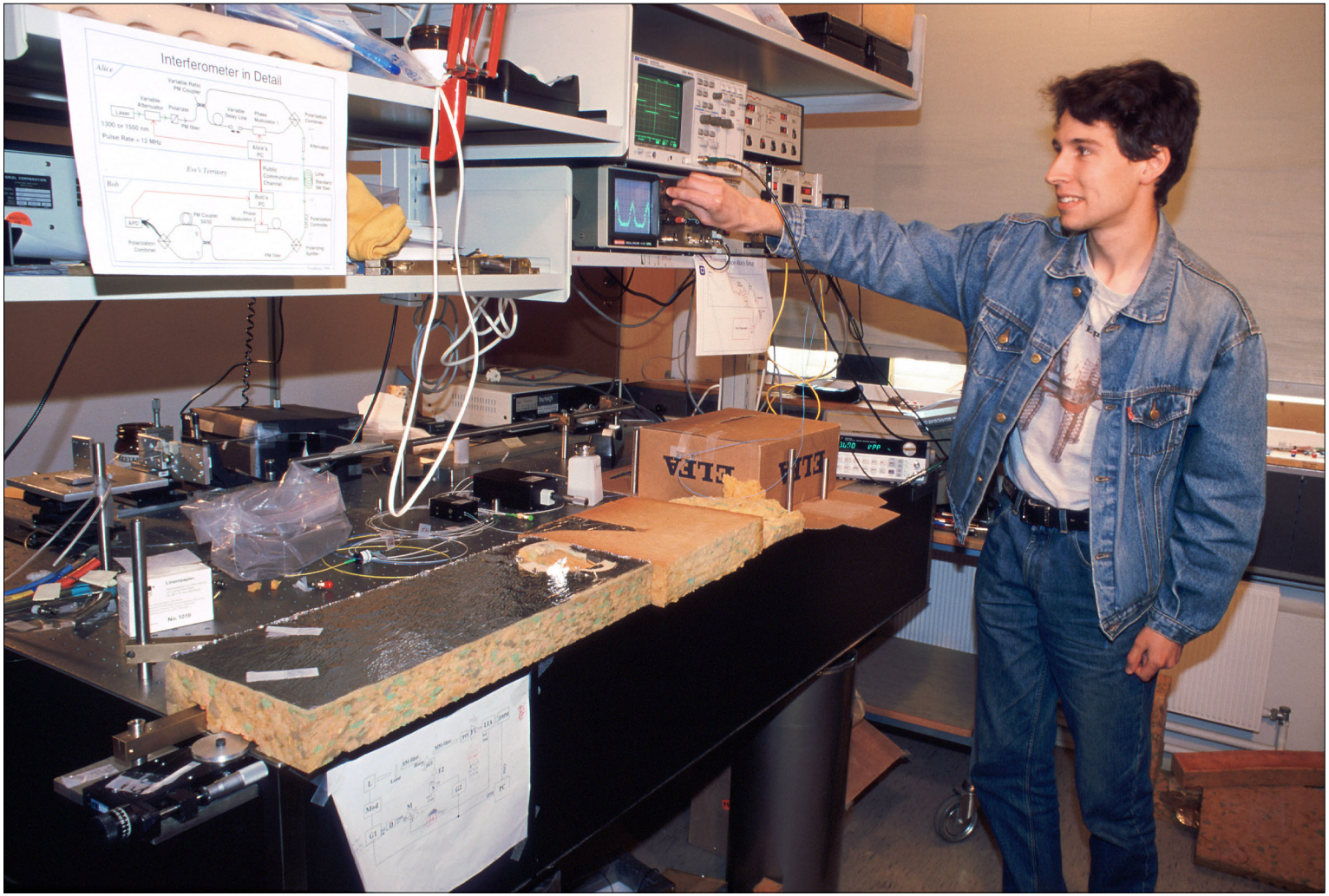


Fig. 38. Artem Vakhitov tunes up Eve's setup described in our paper [89]. In the foreground: thermoisolated Eve's interferometer.

4.3.1.1. Large pulse attack and newer protocols

Since the paper was published, a new QKD protocol, the Scarani-Acin-Ribordy-Gisin 2004 (SARG04), was proposed [64, 65, 66].[18] The protocol has improved characteristics against the PNS attack described in Section 4.2.1. The SARG04 is a simple variation of the BB84 protocol intended for QKD schemes that use a weak coherent source. We'll show shortly that it is, unlike the BB84, vulnerable to the large pulse attack.

The SARG04 protocol can be made equivalent to the BB84 protocol in what states and bases are used in the quantum channel, and differ only at the sifting stage (Fig. 39(*a*)). Alice sends randomly one of the four states $|0_a\rangle$, $|0_b\rangle$, $|1_a\rangle$ or $|1_b\rangle$. Bob measures either in 0 or 1 detection basis. At the sifting step, Alice announces publicly one of the four pairs of non-orthogonal states $\{|0_a\rangle,|1_a\rangle\}$, $\{|0_a\rangle,|1_b\rangle\}$, $\{|0_b\rangle,|1_a\rangle\}$ or $\{|0_b\rangle,|1_b\rangle\}$. For definiteness, suppose that for a given qubit Alice has sent $|0_a\rangle$, and that she has announced the set $\{|0_a\rangle,|1_a\rangle\}$ (one state in the announced set is always the state which was sent, and the other is a state randomly picked from the opposite basis). If Bob has measured in the 0 basis, he has certainly got the result 0_a; but since this result is possible for both states in the set $\{|0_a\rangle,|1_a\rangle\}$, he has to discard it. If Bob has measured in the 1 basis and got 1_a, he again cannot discriminate. But if he has measured in the 1 basis and got 1_b (which happens with overall probability 1/4), then he knows that Alice has sent $|0_a\rangle$, and adds a 0 to his key.

As it is shown in Ref. 64, this simple modification of the protocol makes it more difficult for Eve to eavesdrop using the PNS attack: now she can obtain full information only if she can block all pulses containing one and two photons, and a fraction of pulses containing three photons. This typically increases the critical channel attenuation above which it cannot be considered secure by 10 dB or more, which translates

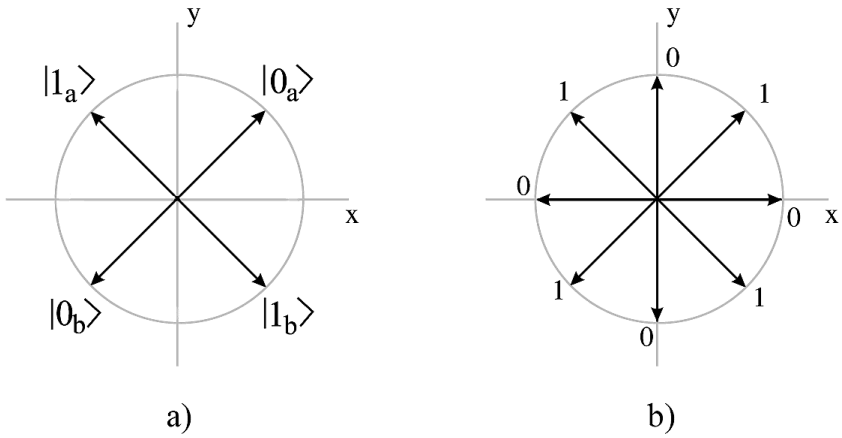


Fig. 39. States configuration for QKD protocols robust to PNS attack: (*a*) SARG04 protocol: two pairs of non-orthogonal states on the equator of the Poincare sphere, physically equivalent to the states used in the BB84 protocol; (*b*) bit encoding in a PNS-resistant protocol using four bases (reprinted from [65]).

[18] Perhaps in an intended pun, the word *sarg* means *coffin* in German.

into additional ~50 km of transmission distance at 1550 nm (shifting the distance limit from ~50 km for the BB84 protocol to ~100 km). A more accurate, though not yet general, security bound for SARG04 is derived in Ref. 66.

However, there is a problem. While the SARG04 protocol provides protection against the attack which is not technologically feasible today, ironically it makes the system vulnerable to the large pulse attack. **The measurement bases at Bob directly represent bit values.** As we know from the above paper, reliable protection against Eve reading Bob's modulator settings is difficult to construct. The SARG04 protocol is just as vulnerable to the large pulse attack as the B92 protocol.

A generalization of the SARG04 protocol to six or more non-orthogonal states has been proposed (a possible configuration with eight states is shown in Fig. 39(*b*)). Using increased number of states further extends the safe transmission distance [65]. However, the measurement basis at Bob still necessarily represents the bit value, and the protocol remains vulnerable to the large pulse attack.

Another recent example of an "improvement" that makes the system vulnerable to the large pulse attack is a single-detector BB84 protocol described in Ref. 214. It proposes to apply at random four phase shift values instead of two at Bob's phase modulator, and eliminate one single photon detector from Bob's setup (at the expense of halving the yield of the key bits). In this case as well, the phase shift value at Bob's phase modulator represents the bit value.

Table 3 summarizes the required protection agaist the large pulse attack for the protocols and schemes we have studied.

Finally, we note recently proposed multipass quantum cryptographic protocols, in which a quantum state transmitted from Alice over the communication line to Bob is modulated and transmitted back from Bob to Alice (and in some of these protocols, once more from Alice to Bob) [215, 216, 217, 218]. Besides being not very practical because losses in the communication line multiply over the two or three passes, these protocols imply no attenuation whatsoever for light pulses being modulated and reflected. Thus, they are wide open to the large pulse attack, and would be very difficult, if not impossible, to make practically secure.

4.3.1.2. Bound on Eve's information

In the recent paper by Gisin et al. [213], a quantitative bound on the amount of information Eve could obtain through the large pulse attack has been given. The bound assumes that the interrogating pulse returning to Eve is attenuated to a sub-photon level. In the case where Eve possesses the phase reference, her information is

$$I_{Eve}^{Trojan}(|\alpha|^2) \approx \frac{1}{\ln(2)}|\alpha|^2 + O(|\alpha|^4), \tag{16}$$

where $|\alpha|^2$ is the photon number of the coherent state Eve receives. If the setup being interrogated uses an auxiliary phase modulator to remove Eve's phase reference (which might be a good idea for some types of setups anyway [79]), Eve's information is reduced to

Table 3. Summary of security measures against the large pulse attack for different schemes and protocols.

Scheme	**Protocols**	**Protection**		
		at Alice	*at Bob*	*
Townsend's	BB84	Passive (attenuator + isolator)	Passive (delay)	Yes
	B92, SARG04, single-detector BB84		Active (detector)	
"Plug and play"	BB84	Active (detector)	Passive (delay)	Yes
	B92, SARG04, single-detector BB84		Active (detector)	

*Eve is granted quantum memory (in reality she could use bases detection on Bob's side, not needing long storage).

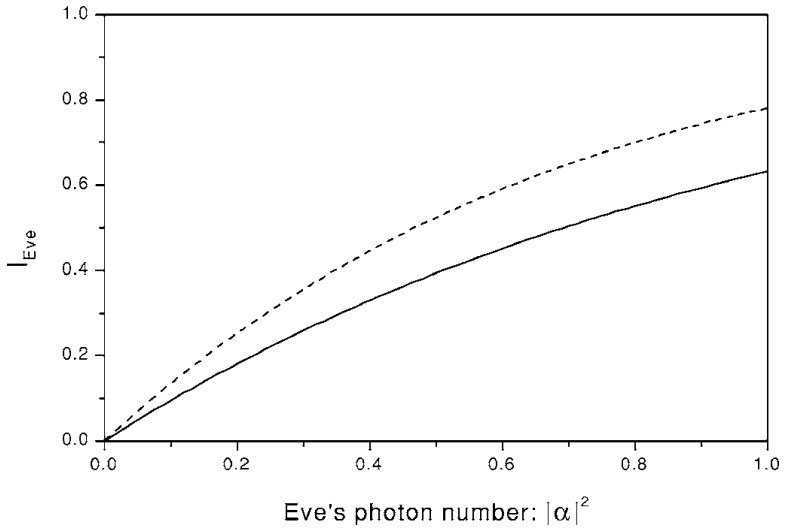


Fig. 40. Reprinted from [213]: Eve's optimal information gain per qubit in the function of the mean photon number $|\alpha|^2$ that she can collect without being detected by Alice and Bob. The upper curve corresponds to Eq. 16, the lower curve to the case that Alice and/or Bob applies phase randomization, Eq. 17. For example, if Alice's monitoring detector sets a limit to Eve's backscattered signal of 0.1 photon, then Eve may gain 0.135 and 0.095 bits if Alice does not apply or applies phase randomization, respectively.

$$I_{Eve}^{reduced}(|\alpha|^2) = 1 - \exp(-|\alpha|^2) \approx |\alpha|^2 . \quad (17)$$

Eve's information in these two cases is plotted in Fig. 40.

4.3.2. High-power damage

An ultimate way for Eve to assist or enable other types of attacks would be to modify characteristics of components inside Alice's and Bob's setups. Controlled changes in components could potentially be made through a well-known effect of high-power laser damage.

Let's discuss briefly what changes in Alice's and Bob's setups Eve might want to make.

Consider, for example, Alice's optical setup in one of the two present-day commercial QKD schemes, the one sold by id Quantique [63], shown in Fig. 41 (exact details of the other commercial QKD scheme sold by MagiQ Technologies have not been openly published, but it is likely of the same type).

The detector D_A serves a dual purpose. Firstly, it implements a feedback loop: D_A measures the energy of the incoming bright pulse from Bob and sets the attenuation of the electrically controlled attenuator VA accordingly to obtain a proper average photon number for the pulse going back into the communication line (the pulse passes through the delay line DL, phase modulator PM_A where it acquires the basis and bit values, and reflects off the Faraday mirror FM). Secondly, thanks to the feedback loop, the detector automatically monitors for the large pulse attack and negates it by increasing attenuation, or it can raise an alarm. The detector also generates a trigger signal used to synchronize Alice's clock with Bob's clock.

If the detector sensitivity to incoming light drops significantly, or if the attenuation of the variable attenuator reduces significantly comparing to its factory calibration scale, the scheme becomes insecure. This is because the average number of photons per outgoing pulse will increase (allowing a classical deterministic detection by Eve), or the large pulse attack described in Section 4.3.1. becomes possible. Eve can try to damage components in order to achieve this:

- try to burn out the detector;
- damage connectors in the detector arm (so that they increase attenuation);
- damage the beamsplitter BS (hoping its splitting ratio alters favorably to her);
- finally, consider what happens to the attenuator after its intensity damage threshold: if it actually decreases attenuation, this also can be exploited.

Eve can try to control the place and character of damage by varying such parameters as the wavelength, polarization, energy and time profile of her laser pulse.

Consider another example: in non-"plug and play" schemes like our scheme, the last optical component in Alice's setup before the line is a variable attenuator set at rather high attenuation (50–60 dB). If the construction of the particular attenuator turns

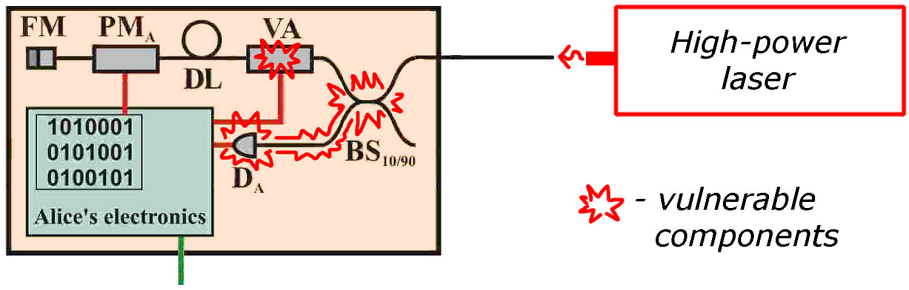


Fig. 41. Optical parts potentially vulnerable to a high-power damage attack in Stucky's *et al.* setup [63]. Alice's part of the optical scheme is shown in the diagram (FM, Faraday mirror; PM_A, phase modulator; DL, delay line; VA, variable attenuator; D_A, detector; $BS_{10/90}$, asymmetric beamsplitter).

out to be such that it *lowers* its attenuation when damaged, the scheme becomes insecure for the same two reasons as in the above case (increased average photon number and facilitation of the large pulse attack).

As yet another example, some of the faked states attacks on schemes with passive basis choice considered in Section 4.3.3.1. depend on finding suitable parasitic reflections in Bob's scheme. If a slightly damaged component or optical interface exhibits increased backreflection, it may facilitate a subsequent faked states attack.

The possibility of high-power damage is potentially very dangerous for security and at the same time challenging for study: nobody has looked into it. The topic of laser damage is well studied [219], but not in relation to this application in quantum cryptography. Experimental tests of high-power damage and eventually tests of protection measures would be destructive to at least some of the components. We would like to study this type of attack; however, acquiring the laser and expendable components would requre a notable amount of money.

4.3.3. Faked states attack

Along the line of our security research, we have come upon a new class of possible practical attacks, *faked states attacks,* and begun to study it. This class of attacks is introduced in the next paper below; it details attack application to schemes with *passive* basis choice. In this paper we also consider Eve's workflow, whose steps are generally applicable to the faked states attack *and* to the large pulse attack described above in Section 4.3.1.

In the following two papers reprinted in Section 4.3.3.2. , we continue the study of the faked states attack and consider a generic detector imperfection: an efficiency mismatch between the 0 and 1 detectors as a function of a control parameter accessible to Eve. This imperfection allows the faked states attack on several protocols and schemes, including schemes with *active* basis choice.

4.3.3.1. Attack on schemes with passive basis choice on Bob's side

This section consists of our paper published in Journal of Modern Optics **52**, 691–705 (2005); figures numeration and references in the paper have been integrated with the rest of the thesis, otherwise the paper is equivalent to the published version sans language changes made by the journal copy editor.

Faked states attack on quantum cryptosystems

VADIM MAKAROV and DAG R. HJELME

Abstract. A new type of attack on quantum cryptography systems is proposed. In this attack, Eve utilizes various optical imperfections in Bob's scheme and constructs light pulses so that Bob does not distinguish his detection results from normal, whereas they give Bob the basis and bit value chosen at Eve's discretion. Applying this attack to systems with passive basis choice on Bob's side is considered. Also, a general workflow of breaking into a running quantum cryptolink using this or Trojan horse attack is discussed.

1. Introduction

Quantum cryptography was introduced as a perfectly secure way of communication based on the laws of physics. However, as the field matured and moved towards more and more practical implementations, it was slowly realized that their security consists of many components and that there are many fine points in the protocol and hardware.

A thorough discussion of quantum attacks gradually evolved to include such imperfections of physical apparatus as faint pulse sources (as opposed to true single-photon sources), loss in the transmission line and non-ideal detectors [193, 194]. Realistic key extraction protocols involving necessary authentication steps and probability estimates have been developed [183]. It has been realized that the equipment manufacturer must be trusted because there is no way for the user to verify the equipment [186]. Finally, the search came down to optical loopholes in particular implementations and classes of schemes, and eventually to electronic and software loopholes [220, 89]. It should also not be forgotten that 'classical' security at the end points of the communication link is just as important (even though this is not a task for the designer or manufacturer of communication equipment).

The whole security is only as strong as the weakest link in it. While it is still true that the laws of physics form the foundation of security in quantum cryptography, its real security will probably be determined by technological implementations, technical measures and unexpected loopholes in them [16].

So far, search for such loopholes has attracted a limited interest. One reason for the lack of interest is that these issues have little connection with fundamental physics that most of the people working in the field have background in. Another reason is that quantum cryptosystems have not really taken off into widespread practical use (only few devices have been sold), thus lacking much of the motivation to try and crack them, and to protect from the crackers. Nevertheless we think that a researcher has to pay attention to possible loopholes in implementations because it reflects on the technology he can use.

In this paper, we introduce a new class of practical attacks which we named *faked states attacks.* The point of this paper is not so much to estimate how easy or difficult would it be to carry out these attacks, but to raise awareness of their existence. Attacks that have not been discussed at all and have been blissfully ignored may end up as real security holes.

The structure of the paper is as follows. In section 2, we define the faked states attack, discuss it on the example of one particular implementation of quantum cryptosystem, and consider protective measures. In section 3, we give an idea of how Eve could proceed with breaking into a running cryptolink in practice. We discuss the general steps involved, what factors influence them, and what present-day technology Eve can employ.

2. Faked states attack

Definition. Faked states attack on a quantum cryptosystem is an intercept-and-resend attack where Eve does not try to reconstruct the original states, but generates instead light pulses that get detected by the legitimate parties in a way controlled by her while not setting off any alarms.

It is well known that intercept-and-resend attack is a strategy doomed to fail if it attempts to regenerate the quantum states as close to the original as possible after detection. However, legitimate parties could sometimes be fooled, using imperfections of their setups, into thinking they are detecting original quantum states while they are in fact detecting light pulses generated by Eve. We call these light pulses *faked states.* Faked states are specific to each particular scheme or even particular sample of equipment being attacked.

A successful faked states attack gives Eve full knowledge of the key. (A partially successful faked states attack gives Eve partial information about the key.)

We have chosen to explain the attack on the example of entanglement-based quantum key distribution (QKD) system developed by the Geneva group [50]. While we don't consider any other system in this paper, the above attack definition is applicable to any type of quantum cryptosystem. In particular, faked states attack can also be run against a system with *active* basis choice on Bob's side, which we would like to detail in our next paper.

The QKD system in [50] we consider here exploits photon pairs entangled in energy-time, where the sums of both the energy and the momenta of the down-converted photons equal those of the pump photon. We recap here how the system works. The photon pair source is located at Alice and is asymmetric, producing pairs where one photon in the pair has wavelength optimized for detection (810 nm) and the other photon in the pair has wavelength optimized for long-distance transmission (1550 nm); see figure 42. The 810 nm photon goes into Alice's interferometer, while the 1550 nm photon is sent to Bob over optical fibre and goes into Bob's interferometer. Unbalanced Mach-Zehnder interferometers are used: an open-path, bulk optics interferometer at Alice, and a fibre-optic interferometer at Bob. While the interferometers have different construction, the path difference between the short and long arm is matched to a fraction of wavelength between them. Photons can propagate in four ways: both photons through the short arms at Alice and Bob, both photons through the long arms at Alice and Bob, one through the short arm at Alice and the other through the long arm at Bob, one through the long arm at Alice and the other through the short arm at Bob. The short-short and long-long processes are indistinguishable and yield two-photon interference, registered as coinciding counts at Alice's and Bob's photon detectors. Actually, whenever one of Alice's four detectors registers a count, it generates a pulse that

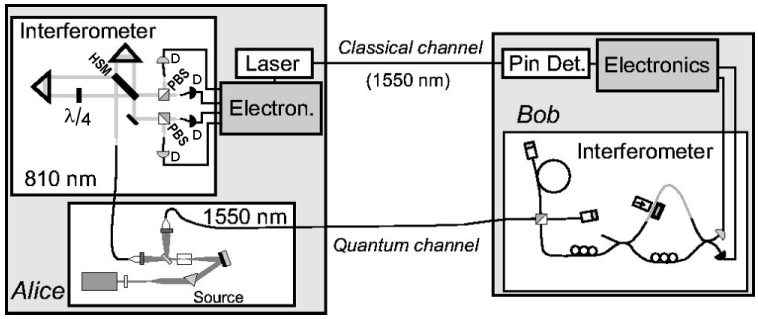


Figure 42. Reprinted from [50]: asymmetric system for quantum key distribution utilizing photon pairs (PBS, polarizing beam splitter; D, single-photon detector; λ/4, quarter-wave plate; HSM, half-silvered mirror).

is transmitted to Bob via a classical channel and gates his detectors in order to try to detect the other photon in the pair.

In order to do QKD, Alice and Bob must implement two incompatible measurement bases in their interferometers. The basis can be selected in each interferometer by randomly introducing either 0 or $\pi/2$ phase shift in one of the interferometer arms. In this system, the basis choice is passive on both Alice's and Bob's side. In Alice's interferometer, the $\pi/2$ phase shift is introduced at $\lambda/4$ plate (see figure 42) for one linear polarization of the beam only. The two linear polarizations get separated from one another at the polarizing beam splitters (PBS). Photons are inserted into the interferometer polarized such that they have about equal probability of experiencing 0 or $\pi/2$ phase shift and going either way at the PBSes; the basis for each photon is known by which pair of detectors registered it. In Bob's setup, each photon chooses its detection basis at the PBS (see figure 43) and experiences a different delay for the two bases. Bob's detectors are gated twice and the detection basis is known by the gate that yielded a click. For additional details about this scheme, we refer the reader to [50].

We show that passive basis choice on Bob's side in this scheme in fact represents a vulnerability that can be exploited in a faked states attack.

Let's consider how faked states attack can be implemented (from Eve's standpoint) and how it can be thwarted (from Bob's standpoint) for several *attack—countermeasure* iterations.

In all implementations considered below, Eve's attack is dependent on forcing Bob to detect not in randomly chosen basis, but in the basis chosen by Eve. Eve cuts into the line and connects the fibre running from Alice to an equivalent of Bob's setup, noting the detection basis and bit value for every quantum state she detects. Then, she sends a faked state towards Bob for every quantum state detected, programming her detection basis into the faked state. Bob always detects it in the basis programmed by Eve. Eve's presence remains hidden, because after the sifting step all the bits in the raw key have been detected by her in the proper basis, and the subsequent check by Alice and Bob shows no increase in quantum bit error rate (QBER).

(1) *Basis choice via polarization.*

In the original setup used in the experiment, each photon chooses its detection basis in Bob's setup randomly at the polarizing beam splitter (PBS), see figure 43 [50]. The

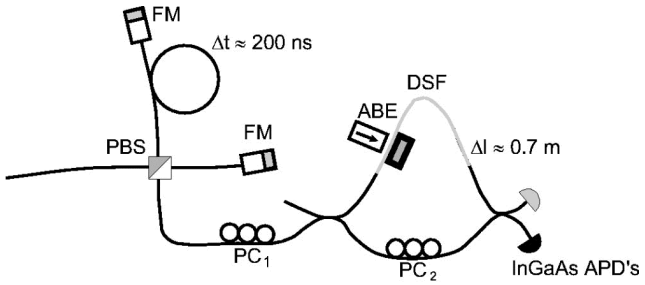


Figure 43. Reprinted from [50]: schematic diagram of Bob's interferometer (PBS, polarizing beam splitter; FM, Faraday mirror; PC, polarization controllers; ABE, adjustable birefringent element; DSF, dispersion-shifted fibre).

choice is random because the photons in the setup are depolarized after travelling the line that connects Alice and Bob.

In the original paper, it is noted that 'Eve could devise a strategy where she could benefit from forcing detection of a given qubit in a particular basis, we must introduce a polarizer aligned at 45° or a polarization scrambler in front of the PBS'. Indeed, without this component Eve could launch polarized photons, so that they are directed into one or another PBS output port at Eve's discretion, thus allowing her to choose Bob's basis and run a successful faked states attack as described above.

(2) Basis choice via polarization using polarizer imperfections.

Let's suppose Bob uses the first of the named defenses, a polarizer aligned at 45°.

Eve's task would be to make sure her photons have the desired polarization (0° or 90°) *after* the polarizer. No polarizer is perfect. We speculate in Appendix A that there always exist two input polarization states (close to the maximum extinction state of the polarizer), for which the output polarization states become the required 0° linear and 90° linear. The polarizer may have high attenuation for these polarization states (several tens of dB), but Eve can easily compensate for this by increasing the intensity of her pulses.

Thus, the polarizer alone is not a viable defense.

Let's now suppose Bob uses the second of the named defenses, a polarization scrambler. An active polarization scrambler driven from a random-number generator would transform the incoming polarization state in a way unpredictable to Eve at each moment in time. This would be a sufficient defense against this attack.

(3) *Basis choice via timing using reflections off optical interfaces.*

Unable to force basis choice via polarization, Eve can now exploit the fact that Bob's gated detectors are not sensitive to incoming light most of the time, and use parasitic reflections that always exist in the setup.

The normal path for light pulses in Bob's setup would be to reflect off the Faraday mirrors (FM) (figure 43). Let's suppose the timing of the light pulse reflected off the FM in the short arm is such that it strikes Bob's detectors during their detection window. Then, should this same pulse or some part thereof take the path in the long arm and reflect off the FM there, it would also strike the detectors during their another detection window. The timing of the two detection windows at Bob is chosen such that

both parts of Alice's pulse arrive during the windows — the one that has travelled the short arm, and the one that has travelled the long arm.

The two arms in Bob's interferometer would, however, likely contain other reflection points besides the FMs at the ends. There will be weaker reflections off splices, off connectors in the arms, and also off collimating optics at the PBS ports. These reflections will likely *not* be time-matched between the arms, i.e. a pulse reflected off such a parasitic reflection in one arm and hitting the detectors during their detection window will not be reflected at the corresponding point in the other arm and won't reach the detectors during the other detection window.

Thus Eve gets to choose the basis again by sending a pulse timed to reach the detectors during only one of the two detection windows, via a suitable loophole reflection path.

If a suitable single parasitic reflection does not exist for one or for both bases, Eve can search for more complex multiple-reflection paths.

Reflection levels from optical components and connectors vary widely depending on the nature, specifications and quality of the component, measuring −10 dB to −70 dB (see Appendix B for some examples). Using a weak parasitic reflection to route light pulse into the detector during its detection window means a much stronger pulse that has travelled the normal path hits the detector *outside* the detection window.

If the residual sensitivity of the detector outside the detection window is high enough, this may cause an error count at Bob, which is no good for Eve. In APDs used as single-photon detectors, we envision two possible mechanisms of residual sensitivity:

(a) An APD reverse-biased below breakdown has a sensitivity to incoming light. Its A/W ratio is determined by how close to the breakdown voltage it is biased. If a light pulse causes a current through the APD comparable to the current during an avalanche, the electronics may react to it and register a 'photon count' (provided it is able to register a count timed off the normal avalanche).

(b) Current flowing through the APD caused by light outside the detection window may leave charges trapped in the junction and cause an equivalent of afterpulsing effect at the next detection window. We shall note, however, that Bob's detection system must cope with afterpulses caused by normal avalanches. This ensures that there are at least some time zones during which a current flowing through the APD won't have a substantial probability of causing an avalanche in the next detection window.

A possible countermeasure to this attack from Bob's side would be to eliminate Michelson interferometer from his setup, and use two identical Mach-Zehnder interferometers and four detectors instead of one interferometer and two detectors.

(4) *Basis and bit value choice via timing using non-overlapping parts of detection window.*

A perfect alignment of detection windows between the bases is not necessary for Bob's operation. It is enough for him if Alice's pulse arrives at the detector during the time when the detection windows for both bases overlap (figure 44); the setup is probably adjusted to achieve this and nothing more. The detection windows, however,

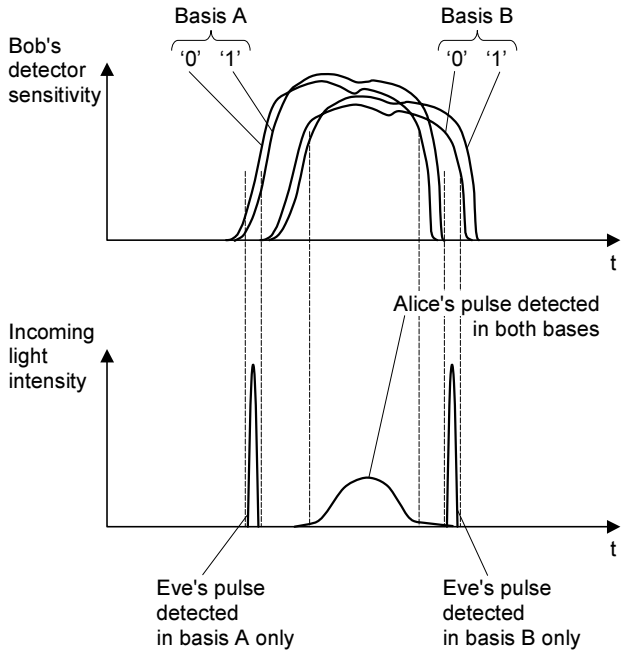


Figure 44. Bob's detection windows shown in the time frame of the incoming light pulses. Bob's detection windows may be shifted relative to each other between the bases and bit values. This does not affect normal operation: Alice's pulse is shown arriving during the time when all the windows overlap. However, if well defined non-overlapping zones exist like on this drawing, Eve may exploit them to choose the basis (her pulses shown on the diagram), and also the bit value.

may and most likely will remain shifted relative to one another. By using a short pulse timed to the non-overlapping parts of the detection windows, Eve can choose the basis.

The detection windows for '0' and '1' detectors may likewise have some non-overlap between them, allowing to choose the bit value. This attack may be useful in combination with the attack (3). Suppose Eve has found optical paths allowing her to choose the basis, but is having difficulty injecting light with properly aligned linear polarization into the Mach-Zehnder interferometer via these paths in Bob's setup (or more generally, can't align the polarizations at the coupler where the pulses should interfere). Thus she is unable to obtain interference with good visibility to choose the bit value interferometrically. She may then try to choose the bit value via timing, using non-overlapping parts of '0' and '1' detection windows.

Bob's defense would be to check that his detection windows are aligned sufficiently well and don't have any non-overlap between them. This is an additional manufacturing step, or at least design step to take care of.

We would love to verify experimentally whether the vulnerabilities described in (3) and (4) exist, and if they can be practically exploited. However, this would require access to the Geneva group's experimental setup, which we don't have. Besides, there is only a limited value in testing particular vulnerabilities of a laboratory setup. If the

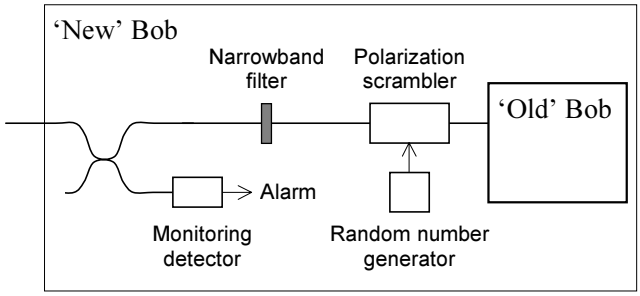


Figure 45. Additional security equipment needed to protect Bob (who is using passive basis choice) from the faked states attack described in this paper. In addition to what is shown on the diagram, Bob must match the timing of his detection windows to each other exactly.

setup makes it to the production version, these vulnerabilities would not be exactly like in the lab prototype, and new vulnerabilities may be introduced in development.

Note that up to this point, we've implied Eve uses the same wavelength as Alice. However, Eve may use various wavelengths for her pulses, in order to exploit wavelength-dependent properties of Bob's setup and have additional flexibility in constructing faked states. Wavelength-dependent properties useful for Eve would be different reflection and transmission coefficients, different detector sensitivity, and different light speed in the fibre. In particular, antireflection coatings can have very large reflection coefficients outside the wavelength range they are designed for.

The difference in group speed can be useful in timing attack if the path length is different between the bases and between the bit values. For example, in the scheme that we are considering, the two arms of the Michelson interferometer have the path difference of 200 ns (figure 43). If we assume that the long arm is made of Corning SMF-28 fibre, the path difference would be smaller by about 80 ps when Eve uses 1310 nm wavelength pulses instead of 1550 nm used by Alice [221]. While this 80 ps imbalance is not sufficient alone for the timing attack, it may contribute towards the total detection windows misalignment required for a successful attack.

To protect from the attacks (1)–(4), Bob can employ a combination of measures (figure 45): a sensitive monitoring detector, a narrowband filter that only passes Alice's wavelengths, and a polarization scrambler. He must also make sure all detection windows are aligned.

In addition, the control software should perform all kinds of 'sanity checks' on the detector data. For example, Eve may have difficulty creating faked states for one particular basis, bit value, or basis/bit value combination, in which case she would send it less frequently or avoid altogether. Bob should check that his detector data contains a proper mix of all possible detection outcomes (including 'double clicks' etc.), and preferably also check that the relative ratio of different outcomes does not fluctuate in time more than would be expected statistically.

(5) *Incapacitation of monitoring detector.*

A possible strategy for Eve would be now to render the monitoring detector insensitive. It could be possibly done by damaging it with a very strong light pulse when the system is not operational (or if Bob would disregard a single alarm resulting from this action).

If the detector is employed, it is therefore advisable to power the detector and alarm trigger circuit from a battery-backed power supply. A single registered alarm, or a detection circuit downtime due to power failure should both be regarded as potential security breach events.

At this point we stop conjecturing ways to attack and note that Bob now has several extra optical components in his setup while it is still possible for Eve to successfully compromise the link if she is lucky. Some readers will surely say that the above attacks are difficult and not very likely to succeed, or that more studies are needed to claim the attack will work. Note, however, that neither *not likely to succeed* nor *more studies are needed* is a definition that equals *perfect security,* — which is what quantum cryptosystems have been supposed to be.

3. Workflow of breaking into cryptolink

While breaking into a cryptolink, four factors influence Eve's workflow:

(1) The ability to stage the attack on samples or replicas of Alice's and Bob's apparatus. In a commercial environment, Eve would be able to buy the equipment for detailed study of its innards and for troubleshooting the attack sequence. If, however, neither the equipment nor information about its detailed construction is available for Eve, this doesn't make the attack impossible, just more difficult.

(2) The ability to install a tap on the optical quantum channel while it is not in use. If the channel is constantly running and an interruption of the connection for the time needed to connect to the line by conventional methods (cutting and splicing) would raise alarm, Eve must use a more elaborate technology for a non-interrupting tap.

(3) How much time elapses between quantum transmission and public discussion between Alice and Bob about this quantum transmission. By watching the public discussion, Eve can infer the QBER Alice and Bob perceive. Monitoring QBER, especially QBER for groups of bits or for particular bits, provides Eve important feedback to tune parameters of her attack (see section 3.C below). The quicker she has the feedback, the faster she can optimize the parameters until the full eavesdropping can be run. We assume here that Alice and Bob use a bi-directional (interactive) error correction protocol, which is more practical but leaks information about error positions to Eve [183]. If Alice and Bob, however, implement a uni-directional error correction, it will not provide Eve information about error positions.

(4) The presence of a continuous monitoring detector in the equipment being attacked. This one can make Eve's life considerably more difficult, if done properly.

The worst case Eve can face is that of breaking into a running cryptolink, not having detailed knowledge of the setups, and very long time between the quantum trans-

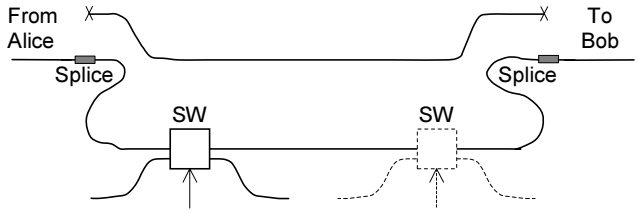


Figure 46. Tap on fibre channel that can be installed before installation of quantum cryptolink or when a quantum cryptolink is temporarily not in use (SW, electro-optical switch).

mission and public discussion usable for inferring QBER for this transmission. This worst case combination is only a deterrent but no guarantee the attack is impossible. If any of the factors (1)–(3) turn to Eve's advantage, that makes the attack easier and more likely to succeed.

The presence of monitoring detector (4) can be a formidable deterrent in many cases. However, some types of faked states attack do not in principle require significant excess optical power at Bob. Eve can manage to keep below the detector's threshold, especially if the threshold is known to Eve from staging (1). For example, two of the attacks discussed in section 2 run with little optical power: *basis choice via polarization,* and *basis and bit value choice via timing using non-overlapping parts of detection window.*

Let's now consider the general workflow, which can be divided into three stages: establishing an optical connection with the line, optical time domain reflectometry (OTDR) measurements, and testing/optimizing the attack parameters.

A. Establishing optical connection with the line

There are three possible cases.

(1) Installing a tap before installation of quantum cryptolink. If Eve knows about installation plans in advance, this is the easiest case for her. Eve just installs her equipment onto a dark fibre and waits until Alice and Bob begin to use it for a quantum cryptolink.

The equipment Eve installs may consist of an electro-optical switch. She connects to the line with two standard fusion splices (figure 46). Depending on the timing requirements of the attack, Eve may need two switches, one for splitting off photons from the line, and another for injecting pulses later down the line. The electrical signal speed in Eve's equipment can be made faster than the speed of light in the fibre line (which is about $^2/_3c$) through the use of e.g. free-space radio signals with travel speed close to c. She can compensate for her processing delay and even inject pulses at the second switch earlier than Alice's photon would have passed it.

The second switch can be substituted by a simple weak-coupling-ratio coupler. Electro-optical switches may be substituted by mechanical ones if their switching speed is sufficient to perform the attack.

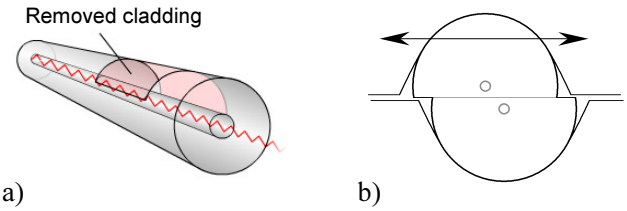


Figure 47. Evanescent-wave technology: (a) using side-polishing techniques, a small portion of the cladding is removed to access the evanescent tail of the propagating wave in the fibre. The removed cladding is replaced with a material to facilitate the function required for the component. The method is non-invasive to the optical core and the components modify the wave propagation by locally changing the guiding conditions, rather than impinging the propagation path (image courtesy Phoenix Photonics); (b) cross-section of a variable-ratio evanescent-wave coupler. The coupling ratio is varied from 0% to 100% by laterally shifting the fibres relative to each other (image courtesy Canadian Instrumentation & Research Ltd.).

(2) Installing a tap into a quantum cryptolink when it is not in operation. The times when the link is temporarily not in use may include maintenance, upgrade, equipment failure, and power outage. Some of these events can be anticipated and even arranged by Eve.

If the link is not in use for the time sufficient to make two splices, Eve can employ the same approach as in (1). There are two possible differences, however: Eve may need to take care of the optical delay in the line (it shouldn't change after installing the tap), and of the additional attenuation she introduces (it should be small enough so that Alice and Bob do not become aware of the tap).

(3) Installing a tap into a quantum cryptolink when it is constantly running. Conventional splicing cannot be used in this case. To do the tap, Eve needs a technology that neither interrupts the line nor introduces a noticeable attenuation for a significant time spell.

Though the authors admit that they are unaware of any commercially available technology that fits this requirement, there are some ideas on how it may look like. The existing evanescent-wave fibre technology would be a good place to start looking. In this technology, a part of the fibre cladding is polished away, allowing access to the mode field (figure 47a). A number of passive and active devices based on this technology are available: fixed and variable attenuators, shutters, polarizers and depolarizers, optical fibre taps, fixed- and variable-ratio couplers [222, 223]. A variable-ratio coupler consists of two fibres with parts of their claddings removed, placed in contact to one another for the length of several millimeters (figure 47b). By laterally shifting the fibre, the coupling ratio can be varied from 0% to 100%. An added advantage of this device is virtually zero intrinsic insertion loss.

Perhaps such couplers could be manufactured on a running quantum cryptolink (figure 48). Then, either both of them are quickly switched from 0% to 100% coupling ratio to connect Eve's devices into the line, or the coupling ratio of the first coupler is slowly varied from 0% to 100% as the attack progresses while the second one is used in weak-coupling mode for pulses injection.

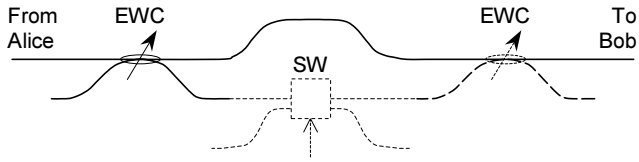


Figure 48. Tap on fibre channel that can be installed while the quantum cryptolink is in continuous operation (EWC, evanescent-wave coupler; SW, electro-optical switch).

Many QKD implementations also utilize a dedicated fibre-optic channel between Alice and Bob to carry synchronization signals and sometimes the public discussion. The same technology used to tap into the quantum channel can be used to tap into this classical channel.

B. OTDR measurements on Bob's setup

After installing the tap, Eve might want to measure exact time delays to and between various reflections in Bob's setup. She can use standard OTDR technique to study reflections in Bob's setup. This is especially needed if Eve doesn't have complete information about Bob's setup.

There are two dangers for Eve to avoid on this stage.

(1) Getting OTDR probing pulses into Bob's detection windows, increasing QBER and setting off alarms. To avoid this, Eve can start probing with weak pulses and monitor public discussion between Alice and Bob for QBER. She can adjust the timing of her pulses, scan the whole time interval and gradually increase their brightness, until a slight raise in QBER is detected. Thus she can learn the positions of Bob's detection windows.

(2) Detection of the scanning activity by a continuous monitoring detector, if Bob has one. Perhaps, in this case Eve could use weak and infrequent pulses, performing OTDR over long time.

C. Optimizing the attack parameters

Eve tries to proceed with attack, substituting at first not all photons in the line, but only few randomly chosen photons. To do this seamlessly, a high-speed switch at the tap is required. However, if the tap has been made with a single coupler, simply changing its coupling ratio and substituting those photons that get split off at the coupler and detected by Eve may be good enough.

Monitoring detection probability and QBER for those photons Eve substitutes with faked states is crucial at this stage. Eve listens to the public discussion and adjusts the parameters of the pulses she sends until they become indistinguishable from real quantum states for Bob.

After that, Eve switches to substituting every photon in the link. To say more accurately, she blocks all Alice's light from reaching Bob, diverts it to Eve's detectors, and

substitutes enough detected photons with faked states so that Bob experiences the same detection rate as before.

Stages B and C are optional. For a well-tested attack sequence, Eve may not need them.

The technology for breaking into a quantum cryptolink discussed above is also applicable to executing Trojan horse attacks, for example large pulse attack [89].

6. Conclusion

(1) Use of passive basis choice on Bob's side is risky from security standpoint. Employ a random number generator and an optical modulator to set the detection basis explicitly. This way, Bob knows the basis for sure.

To ensure true randomness of the basis, it is advisable to use a physical random number generator, for example the quantum random number generator described in [224].

(2) Installing a narrowband filter and sensitive, continuous monitoring detector on both Alice's and Bob's sides as a standard security equipment may be a good idea, whether with passive basis choice or not. Given that several attacks have been discovered that depend on shining light into legitimate parties' setups, this would be a justified precaution to hinder future exploits.

An interesting question arises if Eve does not find sufficiently strong vulnerabilities to run a successful faked states attack, but finds nevertheless *some* imperfections in Bob's setup that would allow her to influence Bob's detection probabilities, e.g., depending on the time delay or polarization of Alice's quantum states. This can ultimately contribute towards Eve's quantum attack and allow her to execute an attack that causes smaller increase in the QBER level than the theoretically optimal quantum attack on a perfect setup would cause [194]. This means the threshold QBER taking such inevitable setup imperfections into account should be *lower* than follows from the pure theory (e.g., *less* than 11%), and Alice and Bob should compress the key more during the privacy amplification — but, by how much? While this problem is addressed theoretically to some extent in [194], the task of finding the imperfections, quantifying them and refining the theoretical model remains.

The most general conclusion we've come to in our security study is that the perfect basic principles behind quantum cryptography are *not* a magic bullet that automatically provides perfect, unbreakable security. The real security story is still the perpetual cat-and-mouse game that has kept busy generations of codemakers and codebreakers over the centuries. The game continues at the next level of technology.

Also, the widespread belief that the danger of quantum cryptography being broken down overnight is negligible, should be amended. This belief rests on two points [16]:

(1) QKD is futureproof in the sense that any advances in technology in the future cannot be used to attack QKD keys that are created today, contrary to cryptosystems based on mathematical assumptions.

(2) Progress in technology is much easier to monitor than progress in mathematics.

While we don't dispute the first point, the second one does not appear to be always valid. An implementation loophole like one of those discussed in this paper may be

discovered in secrecy and the first expoits can be made rather quickly. Depending on the diversity of installed base of quantum cryptosystems, such an implementation loophole can temporarily compromise anything from a small percentage of systems to nearly all of them. The loophole will require a *hardware* fix once it becomes known to the public.

Is it really possible for a determined intruder to explore these attack possibilities, some of them seemingly extremely effort- and time-consuming? We find the historical example of cracking Enigma cipher inspiring in this regard. The task required increasingly larger effort, the use of an expertise unconventional to the codebreaking field at the time (mathematics), and new complex technology (electromechanical automated machines) [1]. Nevertheless, the German communications were routinely deciphered by Polish cryptanalysts and then by the Allies during 1933–1945. At the end of the war, several thousand cryptanalysts had to work to provide the British command with daily intelligence. Still, it was done. And of course, the German High Command never believed their *unbreakable* cipher was cracked (and so were unsuspecting former British colonies using the Enigmas in the years following the war).

In the present-day world, three-letter government agencies might be content with the fact that quantum cryptography equipment provides potential loopholes that may be exploited given a large budget and qualified dedicated staff, just like these agencies have, plus some motivation. So that they can listen to the quantum-encrypted communications while everybody else can't.

Acknowledgements

We thank Dr. Norbert Lutkenhaus for his valuable comments on the manuscript.

Appendix A: Preparing linear polarization states through an imperfect polarizer

Any linear optical component can be represented by its Jones matrix $\mathbf{T}$. The Jones matrix determines its effect on the polarization state and intensity of the incident wave $|s\rangle$, i.e. it relates the output Jones vector $|t\rangle$ to the input Jones vector $|s\rangle$ via $|t\rangle = \mathbf{T}|s\rangle$. To generate a particular output state $|t\rangle$ we need to apply an input state $|s\rangle = \mathbf{T}^{-1}|t\rangle$. Provided the Jones matrix is non-singular we can in principle generate an arbitrary output polarization state.

The Jones matrix of an ideal polarizer is singular, however, a real polarizer would have imperfections rendering the Jones matrix non-singular in general (albeit close to singular). The Jones matrix of a real polarizer rotated 45° can be written $\mathbf{T} = \mathbf{T}_{\mathrm{LIN}} + \mathbf{T}_{\mathrm{SC}}$, where $\mathbf{T}_{\mathrm{LIN}}$ represents the ideal polarizer and $\mathbf{T}_{\mathrm{SC}}$ represents the small imperfections. The inverse of $\mathbf{T}$ will have large components, on the order of the inverse of the elements in $\mathbf{T}_{\mathrm{SC}}$. Thus to generate a linear polarized output state $|t\rangle$ oriented at +/−45° to the extinction axis will require high input power with polarization state $|s\rangle$ close to the extinction axis.

Some of the best commercially available polarizers based on birefringent prisms have extinction ratio of the order of 50 dB [225]. The attenuation of up to ~50 dB such

a polarizer would inflict on Eve's pulses can be easily compensated by their increased energy. Obtaining the proper output polarization states would require, however, a very precise setting of the input polarization states at the polarizer, which will require precise polarization control at Eve. Slight polarization instabilities in the path between Eve and Bob's polarizer may present an additional difficulty for Eve, and even effectively act as a random polarization scrambler.

Appendix B: Reflection coefficients for different fibre-optic components

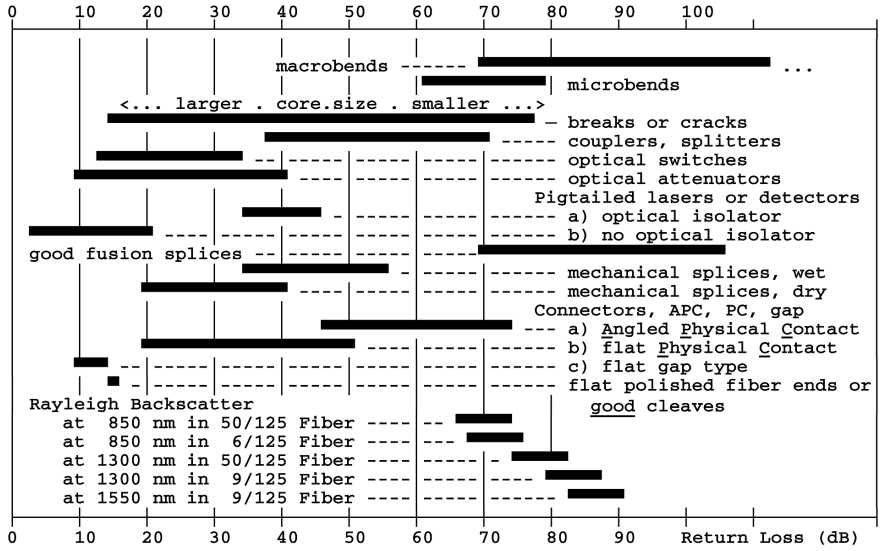


Figure 49. Reflection coefficient values of common fibre-optic features, components and faults. Note that the measured Rayleigh Backscatter coefficients depend on the OTDR distance resolution; on this diagram, they are specific to the OFM130 system by Opto-Electronics, Inc., which has better than 1 m distance resolution in Rayleigh measurement mode. Courtesy of Opto-Electronics, Inc. (http://www.opto-electronics.com/).

[End of included paper]

4.3.3.2. Attack on schemes with active basis choice on Bob's side using detector efficiency mismatch

This section consists of two papers.

The first paper published in Physical Review A **74**, 022313 (2006) is reprinted verbatim on the following pages, with its own list of references and own figures numeration inside the paper. Derivation of bounds in this paper has been made by Johannes Skaar.

A preprint quant-ph/0702262 of the second paper submitted to the Journal of Modern Optics is reprinted verbatim after that, with its own list of references and own figures numeration inside the preprint. We note that the ideas developed in it have originally been presented in May 2006 [228].

Effects of detector efficiency mismatch on security of quantum cryptosystems

Vadim Makarov,[1,2,*] Andrey Anisimov,[2] and Johannes Skaar[1]
[1]*Department of Electronics and Telecommunications, Norwegian University of Science and Technology, NO-7491 Trondheim, Norway*
[2]*Radiophysics Department, St. Petersburg State Polytechnic University, Politechnicheskaya street 29, 195251 St. Petersburg, Russia*

(Received 4 November 2005; revised manuscript received 15 May 2006; published 17 August 2006)

We suggest a type of attack on quantum cryptosystems that exploits variations in detector efficiency as a function of a control parameter accessible to an eavesdropper. With gated single-photon detectors, this control parameter can be the timing of the incoming pulse. When the eavesdropper sends short pulses using the appropriate timing so that the two gated detectors in Bob's setup have different efficiencies, the security of quantum key distribution can be compromised. Specifically, we show for the Bennett-Brassard 1984 (BB84) protocol that if the efficiency mismatch between 0 and 1 detectors for some value of the control parameter gets large enough (roughly 15:1 or larger), Eve can construct a successful faked-states attack causing a quantum bit error rate lower than 11%. We also derive a general security bound as a function of the detector sensitivity mismatch for the BB84 protocol. Experimental data for two different detectors are presented, and protection measures against this attack are discussed.

DOI: 10.1103/PhysRevA.74.022313 PACS number(s): 03.67.Dd

I. INTRODUCTION

Quantum cryptography enables secure communication between two parties Alice and Bob, given a quantum channel and an authentic public channel [1–4]. The security is guaranteed by the laws of quantum mechanics [5–8] rather than assumptions about the resources available to a potential adversary. Although the protocol for secret key distribution, quantum key distribution (QKD), can be proved secure in principle, in the real world the system is not perfect. Flaws in the source and/or detector may be exploited by an eavesdropper (commonly called Eve) to collect information about the key without being discovered. Intuitively, it seems clear that when the imperfections are sufficiently small, the QKD protocol may still be secure. The impact of several imperfections has been discussed previously, and corresponding security bounds have been established [6,9–11].

Before we go on to consider a specific detector imperfection, let us discuss the place of our studies in the picture of security. For any system where security is required, the set of all possible input signals can be divided into three subsets (Fig. 1). The subset A are the input signals for which the system is guaranteed to function normally (e.g., for a key distribution system, generate a secret key). The subset C are the input signals for which the system fails to perform the required function explicitly (e.g., fails to generate the secret key and alarms legitimate users about it). The subset B are input signals for which the system behaves in a way the developers are not quite sure about, thus potentially including subversions by a third party (e.g., generation of a key known to Eve while not raising an alarm). The last subset ideally should not exist and subsets A and C should ideally border one another, or at least the developers should be reasonably sure they do.

With classical digital systems requiring security, input data are binary strings, and the situation where the system is reasonably guaranteed to have empty subset B is achievable. For example, implementations of common cryptographic primitives are usually known to be reasonably secure. However, developers of protocols and applications with more complex functionality (e.g., most software for personal computers) often release them knowing that the subset B is likely nonempty; successful attacks would be found with time, and closed by applying patches on an *ad hoc* basis. The latter situation is clearly not acceptable for QKD.

The problem is that input data for Bob in a QKD system are not binary strings which are well defined and could be directly checked by an algorithm running on a classical computer. The input data for Bob are states of light that we, at the present level of technology, are having considerable difficulty detecting at all, and that have more degrees of freedom than binary data. This makes the important task of developing a complete security proof (and building a QKD system that fully corresponds to the model in the proof) intricate. We contribute to this effort by first showing that the subset B is still nonempty in the currently used model: some subset B_1 of input light states exists that results in a compromise of security, or that has merely not been considered before. Then, we try to find ways to expand the subsets A and C to cover B_1 via both extending the model in the proof and suggesting modifications to QKD setups.

More concretely, we will consider a specific imperfection at the detector; a mismatch in detector timing that occurs in most practical implementations of QKD over optical fibers.

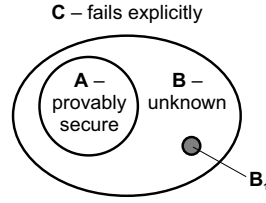


FIG. 1. Set of all possible input signals for a secure system.

*Electronic address: makarov@vad1.com

Most of today's quantum cryptosystems operating in the 1300 and 1550 nm telecommunication windows use gated avalanche photodiodes (APDs) as single-photon detectors. The detector is sensitive to an incoming photon for a short time (a few nanoseconds) called the detection window, and has practically zero sensitivity outside the detection window. The systems operate in a pulsed mode, where the expected time of photon arrival is synchronized with the middle part of the detection window. The systems have at least two separate detection windows or two separate detectors at Bob's side (for 0 and 1 bit values). These detection windows, while both covering the time when the photon comes, are inevitably shifted relative to each other, due to finite manu facturing tolerances. The shift may arise due to small optical path length differences or wire length differences, as well as other imperfections and variations in the detector electronics. Although the detector sensitivities might seem well matched when characterized with Alice's pulses, there may exist rapidly varying differences at the edges that can only be resolved with extremely short pulses.

Eve may exploit a detector timing mismatch by using a version of the so-called faked-states attack [12]. A faked-states attack on a quantum cryptosystem is an intercept-resend attack where Eve does not try to reconstruct the original states, but instead generates (quantum mechanical or classical) light pulses that get detected by the legitimate parties in a way controlled by her while not setting off any alarms. In this case, she may adjust the timing of her states in order to change the sensitivity of the 0 detector relative to that of the 1 detector, and vice versa. By using very short pulses she may take advantage of any rapidly varying features in the detector sensitivity curves not visible to Alice and Bob.

The paper is organized as follows. In Sec. II we introduce the faked-states attack in the "ideal" case where either detector can be totally blinded on Eve's choice. This attack gives Eve full information about the key while Bob registers no increase in the quantum bit error rate (QBER). In Sec. III we derive efficiency figures of a practically possible intercept-resend attack in a more realistic situation with partial efficiency mismatch. Section IV contains a discussion of the security for any eavesdropping attempts. Measurements of detector sensitivity curves for two different detectors are presented in Sec. V. Finally, we discuss protection measures against this attack and conclude the paper in Sec. VI. Although the attack is exemplified using the Bennett-Brassard 1984 (BB84) protocol [1], other protocols that use four states in two bases may also be vulnerable.

II. TOTAL DETECTOR SENSITIVITY MISMATCH

To explain the attack, let us consider an ideal case when the detector sensitivity curves are significantly shifted in time relative to one another, so that time zones exist when one detector is completely blind while the other remains sensitive. Such a situation is depicted in Fig. 2. The figure also shows the last part of the scheme with a Mach-Zehnder interferometer, a scheme example on which we will consider

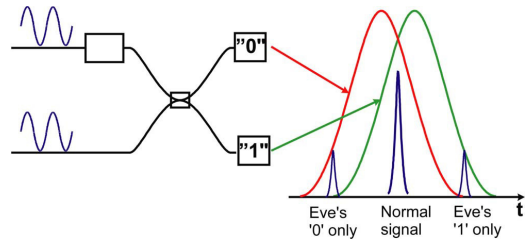


FIG. 2. (Color online) Bob's part of the setup. Bob chooses the basis with the phase modulator (PM). The large detector efficiency mismatch is shown on the plot to the right.

this attack[1]. During normal operation, Alice's pulse (denoted "Normal signal") is timed to the middle of the detector sensitivity curves, and both detectors are sensitive to it. Now if Eve mounts a faked-states attack, she cuts into the line and measures Alice's quantum states (choosing the basis randomly), and replaces them with faked states. She can construct faked states of pulses shifted in time to the sides of Bob's detector sensitivity curves, so that only one of the two detectors can fire in each case (the other one is blinded by timing). Thus she can set her bit value for Bob. Unlike the bit value, she has no direct control over which basis Bob applies with his phase modulator. However, Eve can make sure Bob never detects anything if he chooses a basis incompatible with Eve's measurement (which happens randomly in 50% of the cases). To do this, she sets the relative phase of the pulses in the two arms of the interferometer such that, if Bob chooses an incompatible basis and applies the corresponding phase shift to his phase modulator (PM), the interference outcome at the 50-50 coupler (BS) leads all light toward the detector that is blinded by timing. If, however, Bob chooses another basis (compatible with Eve's), the interference outcome at the coupler will be 50%-50% and the other detector will click. This trick works because, with today's components and transmission lines, Bob detects only a small fraction of the photons sent by Alice. The click at Bob's detector in the case of attack occurs with a reduced probability, but Eve can easily compensate by increasing the brightness of her faked states and thus keeping Bob's average detection rate the same as before mounting the attack. It is also easy to see that the bit statistics obtained by Bob is the same as that obtained in the absence of the attack. As you see, Eve now gets a complete copy of the key, and remains hidden.

The case of total detector sensitivity mismatch is not only convenient for explaining the principle of the attack, but can also occur in practice, as the experimental data later show. However, much more common and, indeed, *unavoidable* in reality would be the case when the detector sensitivities vary relative to each other in time but the ratio between them does

[1]Although a scheme with phase encoding is given as an example in Sec. II, the attack and all obtained results equally apply to polarization encoding, owing to the formal isomorphism between the two encodings [4].

TABLE I. The intercept-resend attack when Alice sends a 0 in the Z basis (as indicated in the first column). The second column contains the basis chosen by Eve and the measurement result; the third column shows the basis, bit, and timing as resent by Eve. In the next columns Bob's basis choice and measurement results are given. For the case with partial detector sensitivity mismatch, the probabilities for the different results are shown, given Eve's basis, bit value, and timing in addition to Bob's basis. Note that, for ease of discussion, the first two rows are repeated so that each row in the table occurs with probability 1/8.

Alice	→Eve	Eve→	Bob	Results, Probability	Sifting
$Z0$	$Z0$	$X1t_0$	Z	$0,\ \frac{1}{2}\eta_0(t_0)$	Keep
				$1,\ \frac{1}{2}\eta_1(t_0)$	Keep
				$—,\ 1-\frac{1}{2}\eta_0(t_0)-\frac{1}{2}\eta_1(t_0)$	Lost
$Z0$	$Z0$	$X1t_0$	X	$0,\ 0$	Discard
				$1,\ \eta_1(t_0)$	Discard
				$—,\ 1-\eta_1(t_0)$	Lost
$Z0$	$Z0$	$X1t_0$	Z	$0,\ \frac{1}{2}\eta_0(t_0)$	Keep
				$1,\ \frac{1}{2}\eta_1(t_0)$	Keep
				$—,\ 1-\frac{1}{2}\eta_0(t_0)-\frac{1}{2}\eta_1(t_0)$	Lost
$Z0$	$Z0$	$X1t_0$	X	$0,\ 0$	Discard
				$1,\ \eta_1(t_0)$	Discard
				$—,\ 1-\eta_1(t_0)$	Lost
$Z0$	$X0$	$Z1t_0$	Z	$0,\ 0$	Keep
				$1,\ \eta_1(t_0)$	Keep
				$—,\ 1-\eta_1(t_0)$	Lost
$Z0$	$X0$	$Z1t_0$	X	$0,\ \frac{1}{2}\eta_0(t_0)$	Discard
				$1,\ \frac{1}{2}\eta_1(t_0)$	Discard
				$—,\ 1-\frac{1}{2}\eta_0(t_0)-\frac{1}{2}\eta_1(t_0)$	Lost
$Z0$	$X1$	$Z0t_1$	Z	$0,\ \eta_0(t_1)$	Keep
				$1,\ 0$	Keep
				$—,\ 1-\eta_0(t_1)$	Lost
$Z0$	$X1$	$Z0t_1$	X	$0,\ \frac{1}{2}\eta_0(t_1)$	Discard
				$1,\ \frac{1}{2}\eta_1(t_1)$	Discard
				$—,\ 1-\frac{1}{2}\eta_0(t_1)-\frac{1}{2}\eta_1(t_1)$	Lost

not get very large. The implications of this property of detectors for security are analyzed in the rest of the paper.

III. PARTIAL DETECTOR SENSITIVITY MISMATCH

We will now consider the case when the sensitivity curves are slightly shifted, i.e., the detectors can only be partially blinded. For analysis in this section, we shall choose an eavesdropping strategy that is not necessarily optimal, but could clearly be implemented today. Let us simply adopt the intercept-resend strategy as described in the previous section for that.

Having chosen the strategy, let us consider all the possible basis and bit combinations during the attack. If we look at the relative phase of the pulses that Eve generates, we can note that, formally, she always chooses to resend to Bob the opposite bit value in the opposite basis compared to her detection. For example, if Eve detects a 0 in the Z basis, she sends a 1 bit in the X basis to Bob. She also chooses the timing so as to suppress 1 detection, i.e., a timing $t=t_0$ for which the ratio $\eta_1(t)/\eta_0(t)$ is small, where $\eta_0(t)$ and $\eta_1(t)$ denote the time-dependent detector efficiencies. The different events are shown in Table I for the special case where Alice sends a 0 in the Z basis (the other three cases are symmetrical to this case). Initially, we assume that all states involved in the protocol and the attack are single-photon states. Later we will discuss the case where Alice and Eve use states with other photon statistics, e.g., faint laser pulses. Also, for now it is assumed that Bob's detectors have no dark counts (which is of course not true but we account for that later on). We assume that Eve's detectors and optical alignment are perfect, and that Eve generates faked states that match the optical alignment in Bob's setup perfectly. Based on the probabilities in the table we can now estimate the efficiency figures for this strategy in terms of the QBER and the mutual information between Eve and Alice, and Bob and Alice.

We discard all cases where Alice and Bob have chosen incompatible bases. When Alice sends a 0 in the Z basis, the probability that the qubit arrives at Bob is

$$P(\text{arrive}|A=Z0)=\frac{1}{4}[\eta_0(t_0)+\eta_0(t_1)+2\eta_1(t_0)]. \quad (1)$$

The probability of arrival averaged over Alice's four choices is found by symmetrization of this expression, yielding

$$P(\text{arrive})=\frac{1}{8}[\eta_0(t_0)+3\eta_0(t_1)+3\eta_1(t_0)+\eta_1(t_1)]. \quad (2)$$

Similarly, we find the QBER,

$$(\text{QBER})=\frac{P(\text{error})}{P(\text{arrive})}=\frac{2\eta_0(t_1)+2\eta_1(t_0)}{\eta_0(t_0)+3\eta_0(t_1)+3\eta_1(t_0)+\eta_1(t_1)}, \quad (3)$$

where $P(\text{error})$ accounts for the cases when Bob detects a bit value different from what Alice has sent.

Having established the QBER, we will now compare Bob's and Eve's amount of relevant information [13]. Denoting the mutual information between Alice and Bob $H(A:B)$, and the mutual information between Alice and Eve $H(A:E)$, the security is guaranteed when $H(A:B)>H(A:E)$ [14]. This condition is sufficient and necessary for protocols with only one-way classical communications (no advantage distillation [15]; with advantage distillation it is not necessary). For intercept-resend attacks, it is clear that $A\rightarrow E\rightarrow B$ is a Markov chain. Hence, $H(A:B)\leq H(A:E)$, so Bob's key is generally not secure. Note that advantage distillation is not pos-

sible because intercept-resend attacks remove any entanglement between Alice's and Bob's qubit.

To analyze in more detail how this particular attack performs we will evaluate the mutual information between Alice and Eve $H(A:E) \equiv H(A) - H(A|E)$. After the basis has been revealed, A takes only two possible values (0 and 1) while Eve's result is $Z0$, $Z1$, $X0$, or $X1$. We assume that Alice and Bob have used the Z basis (by symmetry in the QKD protocol and the eavesdropping strategy we need only consider this basis choice). The entropy $H(A)$ is found from the probabilities $P(A)$, which, in turn, can be calculated from the arrival probabilities (1) and (2):

$$P(A=0) = \frac{\eta_0(t_0) + \eta_0(t_1) + 2\eta_1(t_0)}{\eta_0(t_0) + 3\eta_0(t_1) + 3\eta_1(t_0) + \eta_1(t_1)}, \quad (4a)$$

$$P(A=1) = 1 - P(A=0). \quad (4b)$$

To identify the conditional entropy $H(A|E)$, we need the conditional probabilities $P(E|A)$, and also $P(A|E)$ which can be found using Bayes' rule:

$$P(A|E) = \frac{P(A)}{P(E)} P(E|A). \quad (5)$$

The conditional probabilities $P(E|A)$ are calculated using Table I:

$$P(E=Z0|A=0) = \frac{\eta_0(t_0) + \eta_1(t_0)}{\eta_0(t_0) + \eta_0(t_1) + 2\eta_1(t_0)}, \quad (6a)$$

$$P(E=Z1|A=0) = 0, \quad (6b)$$

$$P(E=X0|A=0) = \frac{\eta_1(t_0)}{\eta_0(t_0) + \eta_0(t_1) + 2\eta_1(t_0)}, \quad (6c)$$

$$P(E=X1|A=0) = \frac{\eta_0(t_1)}{\eta_0(t_0) + \eta_0(t_1) + 2\eta_1(t_0)}. \quad (6d)$$

In the case $A=1$ we find the conditional probabilities directly from (6) using the symmetry. The probabilities $P(E)$ are found using the relation

$$P(E) = \sum_a P(E|A=a)P(A=a), \quad (7)$$

and the conditional entropy is

$$H(A|E) = -\sum_{e,a} P(A=a)P(E=e|A=a)\log P(A=a|E=e). \quad (8)$$

After substitution of the probabilities above, the result is simple: $H(A|E) = (\text{QBER})$, where the QBER is given by Eq. (3). Hence,

$$H(A:E) = H(A) - (\text{QBER}). \quad (9)$$

The mutual information between Alice and Bob, $H(A:B) \equiv H(A) - H(A|B)$, is found by a similar procedure. After the basis has been revealed A and also B take only two values (0 and 1). The conditional probabilities $P(B|A)$ are

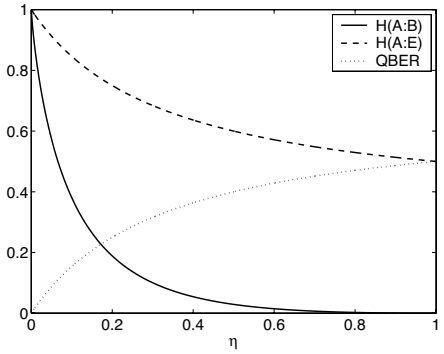


FIG. 3. The QBER, the mutual information between Alice and Bob, $H(A:B)$, and the mutual information between Alice and Eve, $H(A:E)$, as functions of the normalized efficiency of the blinded detector, η.

$$P(B=0|A=0) = \frac{\eta_0(t_0) + \eta_0(t_1)}{\eta_0(t_0) + \eta_0(t_1) + 2\eta_1(t_0)}, \quad (10a)$$

$$P(B=1|A=0) = 1 - P(B=0|A=0), \quad (10b)$$

$$P(B=1|A=1) = \frac{\eta_1(t_1) + \eta_1(t_0)}{\eta_1(t_1) + \eta_1(t_0) + 2\eta_0(t_1)}, \quad (10c)$$

$$P(B=0|A=1) = 1 - P(B=1|A=1). \quad (10d)$$

In the special case with symmetric detector efficiency curves, i.e., $\eta_0(t_0) = \eta_1(t_1)$ and $\eta_0(t_1) = \eta_1(t_0)$, we find $H(A:B) = 1 - h(\text{QBER})$ and $H(A:E) = 1 - \text{QBER}$, where h is the binary Shannon entropy function $h(x) = -x\log_2 x - (1-x)\log_2(1-x)$. Thus all quantities, the QBER, $H(A:B)$, and $H(A:E)$, depend only on one parameter; the normalized efficiency $\eta \equiv \eta_1(t_0)/\eta_0(t_0)$. The result is plotted in Fig. 3. As mentioned previously, it is apparent that Eve has always more mutual information with Alice than does Bob. For $\eta = 1/3$ the difference $H(A:E) - H(A:B)$ reaches its maximum $h(1/3) - 1/3 \approx 0.58$ for a corresponding QBER of $1/3$. If Bob is not aware of his detector efficiency mismatch, he thinks that the key is secure when the QBER is less than 0.11 (symmetric protocols with one-way classical communications [8]). Thus Eve can compromise the security of the system if $\eta \leqslant 0.066$. The privacy amplification [16] Alice and Bob apply will not save them from this attack and will not produce a secret key because the mutual information between Alice and Eve is always greater than that between Alice and Bob.

In a real installation, Alice and Bob may expect the QBER to stay at some level below 0.11, which leaves Eve less room for the attack. Also in the practical scenario considered in this section, the contribution of dark counts in Bob's detectors to the total QBER is independent of other error sources and is beyond the control of Eve. Only the part of QBER *not* caused by dark counts in Bob's detectors can be used by Eve.

Let us consider any side effects this attack may produce that may divulge it. Although the attack may not give any alarm in terms of the QBER, it might be detected as a result of different measurement statistics at Bob's detector. From (4) and (10) and their analogs for the case where Bob used the X basis (incompatible basis), we observe that the measurement statistics has changed as a result of Eve's attack. However, the changes may be reduced or even eliminated by choosing suitable t_0 and t_1. (For example, the bit rates are equal in the symmetric situation analyzed above.) Similar skews in statistics may be produced in the absence of Eve's attack by random drifts and optical misalignments during operation, and may lie within what Bob normally expects.

So far we have assumed that Alice and Eve use single-photon states. Then Bob can detect the attack as a decreased bit rate, because P(arrive) usually would be less than the detection probability Bob has with no attack. Any reasonably well implemented Bob would monitor the bit rate and raise alarm if it drops significantly. To compensate for the reduced detection probability, Eve could increase the brightness of her pulses (several photons in each pulse, and possibly different photon statistics for the t_0 and t_1 pulses). However, this compensation might be possible to detect from the coincidence count rates at Bob's detectors. Alternatively, Eve could place her intercept unit and resend unit at two separate locations along the transmission line, thus winning the photons that would be lost in the line between these two locations. In the limit we have to assume she would place the intercept unit near Alice and the resend unit near Bob, getting the whole amount of normal loss in the line to cover for the reduction in detection probability caused by her attack.

If Alice uses faint laser pulses, the attack is still possible. However, now Eve must consider the basis-dependent coincidence count rates at Bob's detectors. If we grant Eve a future technology, namely, the ability to do photon number measurement, she would be able to retain the coincidence rates: Eve could measure the photon number first, and run the faked-states attack only on those pulses that contain one photon, using a single-photon source to generate faked states. Those of Alice's pulses that contain two or more photons can be passed undisturbed to Bob at the expense of a small part of the key becoming unavailable to Eve. Alternatively they can be eavesdropped on using the photon number splitting (PNS) attack [17–19], provided a version of the PNS attack that does not alter coincidence counts could be constructed in this case [20].

Watching the rates and coincidence statistics for different bit-basis combinations is useful as a general precaution and should be built into the key distribution protocol. But it does not necessarily provide security against this attack.

IV. SECURITY BOUND

The intercept-resend attack described in the previous section is not necessarily the optimal attack. Alice and Bob want, of course, their protocol to be secure against any attack permitted by quantum mechanics. Note that Eve can exploit rapidly varying features in the detector sensitivity behavior even though she does not regenerate the pulses. She may perform a quantum nondemolition measurement of Bob's pulses to collapse them into much shorter ones, obtaining the associated timing information of the resulting pulse. As shown in the Appendix, this measurement will not disturb the degrees of freedom encoding Bob's qubit.

The following discussion of security will be based on the proofs by Lo and Chau [7] and Shor and Preskill [8]. Here, Eve is allowed to do collective attacks and perform arbitrary quantum operations on each block of data. Alice and Bob use only one-way classical communications in the QKD protocol. Note that higher bit error rates can be tolerated if they use two-way classical communications [21] (advantage distillation).

The critical point in the Lo-Chau and Shor-Preskill proofs is to bound the so-called bit and phase error rates. In the entanglement purification protocol used in the proof, this corresponds to bounding the fidelity of the Bell pairs received by Alice and Bob, and therefore the mutual information Eve has with their measurement results. In the QKD protocol, Alice and Bob measure the error rate by sampling a subset of the qubits randomly. Bob measures the qubits in two bases (chosen randomly for each qubit). The error rate as measured in the random sampling process is denoted the bit error rate; the error rate if Bob had chosen the opposite basis is denoted the phase error rate. In the case where Eve can control the detector efficiencies, we distinguish between the measured bit error rate (QBER) and the actual bit error rate. The measured bit error rate (QBER) is the error rate as measured by Bob, while the actual bit error rate is the error rate that Bob would measure if his detectors were perfect.

An analysis of several attacks where the eavesdropper has some information on the basis used by Bob is described by Gottesman *et al.* [11]. In the Trojan pony attack (Ref. [11]), the eavesdropper can control the efficiency of the detectors to create an asymmetry between the bit error rate (which is measured by Bob) and the phase error rate (which is not measured). In the optimal case (as seen from Eve's viewpoint) all errors that Eve eliminates are bit errors. Note that, in this case, the bit error rate as measured by Bob is the actual bit error rate since Eve does not control the two detector efficiencies separately (as opposed to the situation analyzed in this paper). Bob's problem is rather that he cannot measure bit and phase errors on the same qubit.

Now, consider the case relevant to the present paper, where Eve has no information on the basis used by Bob. Instead she can control the 0 and 1 detector efficiencies separately, by appropriate timing of the qubits. Since Eve does not know Bob's basis, the actual bit and phase error rates will be equal. However, since Eve can force the efficiencies of the two detectors to be different, the measured bit error rate will be different from the actual bit error rate. Therefore, Bob has to estimate the actual bit error rate from the measured bit error rate and *a priori* knowledge of Eve's power (that is, he must characterize his detector sensitivity curves).

The available bit rate from the QKD after privacy amplification is [8]

$$R = 1 - 2h(\delta), \tag{11}$$

where δ is the actual bit error rate and h is the binary Shannon entropy function $h(x) = -x \log_2 x - (1-x)\log_2(1-x)$. The

actual bit error rate is related to the measured error rate and the detector efficiencies. The two detector efficiencies are denoted $\eta_0(t)$ and $\eta_1(t)$, and at a certain time t, they may be different. For example, take $\eta_0(t) > \eta_1(t)$. In a worst-case scenario, Eve minimizes the measured bit error rate (QBER) for a given δ. Assuming a large number N of qubits, δN of them would be detected as errors if the detectors were perfect. For Bob's detectors, in the worst case this number is reduced to $\eta_1(t)\delta N$ provided Eve uses the timing t. At the same time, the number of qubits detected as correct bits is only reduced from $(1-\delta)N$ to $\eta_0(t)(1-\delta)N$. The associated QBER becomes $\eta_1(t)\delta/[\eta_1(t)\delta+\eta_0(t)(1-\delta)]$. Minimizing with respect to t, we obtain[2]

$$(\mathrm{QBER}) = \frac{\eta\delta}{1+\eta\delta-\delta}, \tag{12}$$

where

$$\eta = \min\left\{\min_t \frac{\eta_1(t)}{\eta_0(t)}, \min_t \frac{\eta_0(t)}{\eta_1(t)}\right\}. \tag{13}$$

In other words, the estimate for δ,

$$\delta = \frac{(\mathrm{QBER})}{\eta+(1-\eta)(\mathrm{QBER})}, \tag{14}$$

and not the QBER, should be used to determine the required amount of privacy amplification. The QKD protocol is secure provided $\delta < 0.11$ [0.11 is the zero of $1-2h(\delta)$], which means approximately that $(\mathrm{QBER}) < 0.11\eta$.

The bound above might be a little pessimistic: Eve needs at least a "partial" qubit measurement to decide which timing to use for the pulses going to Bob. This measurement must certainly be performed before Eve gets information on the basis used by Alice and Bob. The Shor-Preskill bound assumes that Eve may wait with her measurement until the basis choice is made public.

The security findings that have been made in the paper are summarized in Fig. 4.

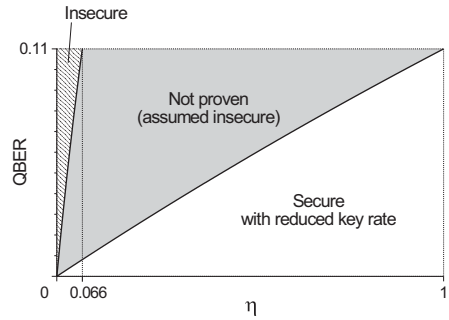


FIG. 4. Security state of a QKD system as a function of the normalized efficiency of the blinded detector η and the measured QBER. In the "Secure" zone, the required amount of privacy amplification is larger than without considering this attack, being determined by δ given in Eq. (14). In order to make this plot, we have allowed for some simplifications. The border between "Not proven" and "Insecure" zones is drawn assuming the special case of symmetric detector efficiency curves discussed in Sec. III. The QBER for the "Insecure" zone is assumed to be without contribution from dark counts in Bob's detectors.

V. EXPERIMENTAL DATA

In this section we present measured detector sensitivity curves of two different single-photon detectors. Both devices under test were laboratory prototypes of detectors that were a part of or intended for use in quantum cryptography systems.

A. Detector model 1

The first detector we tested was a time-multiplexed detector, i.e., a single detector registering 0 and 1 counts in different time slots. The light pulses corresponding to the 0 and 1 bit values were combined into a single fiber (one of the pulses was delayed in an optical delay line), and fed to the detector. The detector was gated at double the pulse rate, with 0 pulses coming in odd gates and 1 pulses coming in even gates. The model operated at 1310 nm and used a Soviet-made Ge APD (standard part number FD312L, developed by NPO Orion) cooled to 77 K. Gate pulses at the APD in this detector were made as narrow as practically possible, around 2 ns full width at half maximum (FWHM). The laser pulse in the test was 100 ps wide (FWHM) and was actually the same pulse normally used by Alice: we simply employed the entire QKD setup described in Ref. [22] to do the detector test, only changing the time delay of the laser pulse in order to measure the sensitivity curves. The measured curves are presented in Fig. 5.

Since the same detector is used for 0 and 1 detections, we would expect the shapes of sensitivity curves to be highly identical. This is indeed the case. Also the curves have almost no time shift relative to one another, which means the fiber optic delay line in our setup was cut and spliced with good precision (from these data we can estimate the cutting inaccuracy to be less than ±25 ps or ±5 mm). Nevertheless the time range (encircled on the chart) where the laser pulse impinges the APD at the closing edge of the gate shows sensitivity mismatch $\eta \approx 1/2$. It is possible the mismatch is actually larger than this, but we could not resolve it unless we used narrower laser pulses and did a more detailed measurement in this time range. The other side of the peak where the laser pulse impinges the APD before and at the opening edge of the gate shows no discernible sensitivity mismatch, because the APD sensitivity in this time range rises smoothly. This is consistent with the presence of a trailing tail in a typical APD time response [23,24].

The measured curves suggest that the practical attack described in Sec. III would be impossible, but the general security bound (14) would impose a significant penalty on the

[2]Eve may certainly use several different t's for different qubits. However, since $\Sigma_i p_i/\Sigma_i q_i \geq \min_i(p_i/q_i)$ for any positive p_i and q_i, the minimum QBER is still given by the minimum of $\eta_1(t)\delta/[\eta_1(t)\delta+\eta_0(t)(1-\delta)]$ and $\eta_0(t)\delta/[\eta_0(t)\delta+\eta_1(t)(1-\delta)]$ for all t.

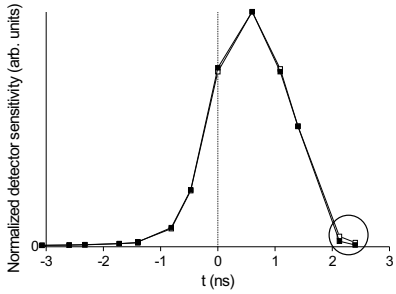


FIG. 5. Detector model 1. Sensitivity curves for the 0 (open squares) and 1 (filled squares) time slots, at low mean number of photons at the APD ($\mu \ll 1$). Dark counts were subtracted. The curves, originally of different height, were scaled so that their peak points coincide. t is the relative time of arrival of the laser pulse at the APD; $t=0$ was the actual arrival time of Alice's pulse in the operational QKD setup before this measurement.

key rate and maximum allowed QBER. It is also clear that a better measurement with narrower laser pulse (no wider than few tens of picoseconds), smaller time increments, and extended time range would generally be desired for detector testing.

The precision with which the fiber delay line was cut in this setup was actually unnecessary for normal operation of the QKD. Should less care be taken in cutting the delay line, there would typically be larger mismatch at both sides of the curve. In the worst possible case one of the curves could end up shifted to the left by 1.1 ns, providing the same sensitivity for Alice's pulse as we have now while leaving sufficiently large mismatch at the sides for Eve to attempt the practical attack described in Sec. III.

B. Detector model 2

The second detector we tested was a dual detector, consisting of two identical single-photon detectors registering 0 and 1 counts in parallel. This detector was one of the several different test prototypes developed at the Radiophysics Department at the St. Petersburg State Polytechnic University. Each of the two detector channels had its own APD, gating, and detection electronics, while the thermoelectric cooler for the APDs, power supply, and external synchronization were shared. JDS Uniphase EPM239BA (former Epitaxx EPM239BA) single-mode fiber pigtailed APDs were used, cooled to ≈ -48 °C. The APDs were gated at 100 kHz, with gate pulses having magnitude of 8 V and width of 3.5 ns (FWHM). The laser pulse in the test had wavelength of 1560 nm and was less than 200 ps wide (FWHM). The detector was set into a mode that would be suitable for its operation in a QKD system. The peak efficiencies in both channels were made to be roughly equal, by adjusting the bias voltage separately on each APD. The laser pulses impinged both APDs almost simultaneously; the remaining small difference in the optical paths, 9 mm or 45 ps between the channels, was later accounted for when plotting the

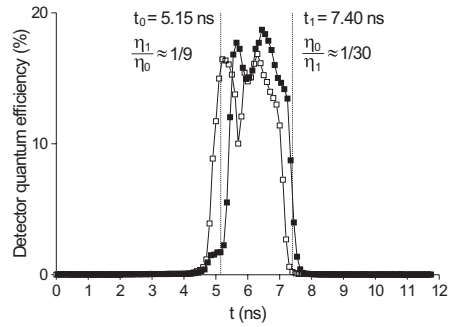


FIG. 6. Detector model 2. Sensitivity curves for the 0 (open squares) and 1 (filled squares) time slots, at mean number of photons at the APD $\mu=0.5$. Dark counts were subtracted.

charts so they represent the response to a laser pulse impinging both APDs at exactly the same time.

With this detector, we tried to do a more thorough measurement than with the previous one. The sensitivity curves are shown in Fig. 6. Although the curves overlap in a 1.6 -ns-wide zone (well enough for use in QKD), there are significant mismatches at the sides. Using the time t_1 marked on the chart, and a t_0 where both detector efficiencies are small, Eq. (3) gives QBER ≈ 0.061. This may give an impression that the attack described in Sec. III is possible. However, any properly implemented Bob would raise an alarm if the 0 and 1 detection rates were significantly different. To achieve more similar detection rates, Eve can increase the brightness of her t_0 pulses and/or tune t_0. In the limit where the two detection rates are equal, she chooses the t_0 as marked on the chart to obtain the minimum QBER of 0.119. This means that the attack would be discovered (however, it is close to the threshold). Nevertheless, the QKD system with this detector will be rendered inoperative by the general security bound (14), which for $\eta=1/30$ allows a QBER of no more than 0.0036. Note that shifting the curves relative to one another never eliminates large sensitivity mismatch.

In the measurement above, we could not see the quantum efficiency in the long tails, because it was masked by dark counts. It was therefore natural to repeat the measurement using three orders of magnitude brighter pulses. The expected result is complete saturation in the middle, and elevated, well-resolved tails. The result we obtained, however, was quite surprising (Fig. 7). Although the measurement did resolve the tails (showing a significant mismatch around 1 ns), the detector performance in the middle part of the chart was erratic, with sensitivity plunging to zero where there should have been saturation. Using this behavior of the detector, Eve could likely run the attack in conditions close to the total sensitivity mismatch described in Sec. II.

Forced to explain this detector behavior, we turned to the schematic of its electronics. The feature of this particular test prototype was that it used signal reflected from the APD, so that only one electrical waveguide had to be connected to each APD, thus reducing the thermal flow and easing cooling (Fig. 8). To split off the reflected signal, a microstrip coupler was used, forming a circulator at frequencies above 1 GHz.

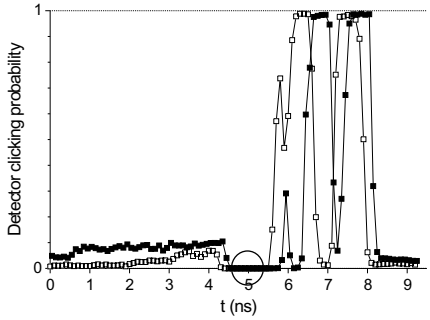


FIG. 7. Detector model 2. Sensitivity curves for the 0 (open squares) and 1 (filled squares) time slots, at mean number of photons at the APD $\mu=500$. In the encircled time range (4.65–5.30 ns) the clicking probability in both detectors measured exactly zero (0 counts registered per $>10^5$ gates). Unfortunately the time reference in this plot is not accurately matched with that in Fig. 6, and the curves' features cannot be directly compared between the two figures.

The following amplifier had the bandwidth of ca. 2.5 GHz. Thus the whole tract for the reflected signal suppressed spectral components outside the 1–2.5 GHz band. There was no balancing circuit for spikes in the reflected signal that resulted from the gate front and back edges causing current through the APD capacitance, and also the spikes seeping into the reflected signal tract through other electrical imperfections. These unwanted spikes were partially suppressed spectrally: most of the spectrum of the spikes lay below 1 GHz, as the front and back edges of the gate pulse were less steep than the front edge of the avalanche signal. The comparator threshold was fine tuned to be lower than the avalanche signal, but higher than the parasitic signal at the output of the tract in the absence of avalanche. This all worked fine for avalanches caused by absorption of 1-2 photons, as Fig. 6 illustrated. However, with avalanches caused by almost simultaneous absorption of hundreds of photons from every laser pulse, this spectral-selective circuit connected to a finely tuned comparator produced the gaps seen in Fig. 7. The use of a spectral-selective circuit was a necessary condition for this abnormal behavior. The spectrum of the avalanche pulse was a function of two varying parameters: the pulse length and the shape of its front edge. The fraction of the avalanche pulse that passed through the spectral-selective tract to the comparator thus depended on these two parameters. Small changes in them due to the use of brighter light pulses resulted in the observed behavior of the output signal. Exact details of APD operation with brighter pulses, however, proved to be elusive to measure with the equipment we had.

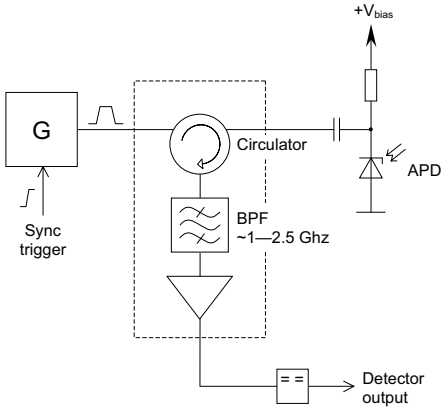


FIG. 8. Detector model 2. Equivalent diagram of a single channel. G is a single-shot generator that forms the gate pulse for the APD. BPF is an equivalent band-pass filter representing the frequency bandwidth of the tract for the reflection signal.

Although we were able to eliminate the abnormal detector behavior with $\mu=500$ laser pulses by making adjustments in the electronics, this test prototype together with the idea of using reflected signal and/or spectral-selective detection tract had to be scrapped. It is simply too risky from the security standpoint to use detectors based on this or any other "advanced" approach in QKD systems, even if you test them well. More straightforward detection schemes have to be preferred.

VI. DISCUSSION AND CONCLUSION

We have seen that when the detection of 0 and 1 bits can be blinded separately by timing, Eve can obtain full information about the key while she is hidden. In the case with only partial sensitivity mismatch, a similar attack is possible which will not provide alarm to Alice and Bob in terms of the QBER when the mismatch is sufficiently large. Although the specific intercept-resend attack given in Sec. III only works in certain conditions, more sophisticated attacks may exist which are able to exploit small sensitivity mismatches. Hence, to ensure secure QKD it is crucial to characterize Bob's detectors and specify maximum sensitivity mismatch. Based on this information, the worst-case estimate for δ given in (14), and not the QBER, should be used to determine the required amount of privacy amplification.

Specific measures aimed to specify and/or limit the sensitivity mismatch might be the following.

(1) Measure detector characteristics (especially sensitivity vs time) over a variety of input signals, including those well *beyond* the normal operating range. Use sufficiently short pulses so that all features of the sensitivity curves are captured. Employing a simple, straightforward detector circuitry can help lower the likelihood of hidden surprises, both discovered and undiscovered by testing.

(2) Introduce intentional random jitter in the detector synchronization to "smear" the curves and lower the mismatch.

(3) Implement active protection by checking timing of incoming pulses at Bob. This can be done through random shifting of Bob's detection time window, by registering the time of avalanche onset within the window, or with additional detectors.

In the future it would be desirable to see if the general security bound, as implied by (14), can be narrowed. The

security bound as it stays now is rather strict, and requires the amount of privacy amplification to be corrected in most practical quantum cryptosystems that use four-state protocols.

Not all QKD protocols are vulnerable to this attack. For example, the Bennett 1992 (B92) protocol [25–28] is not affected, because it uses just one detector for quantum states (however, Bob should be careful not to allow Eve to make a "faked" reference pulse which is accepted by Bob's classical detector but causes no clicks at his single-photon detector; using a local oscillator as proposed in Ref. [26] is a good solution to this problem; insecure implementations of B92 that do not use homodyne measurement have to be avoided [29,30]). The modification of the BB84 protocol in Refs. [31,32], with a single detector randomly chosen via phase modulator setting to detect either a 0 or 1 bit, is not vulnerable for the same reason.[3] The six-state protocol [33–35] seems not to be vulnerable (though we note that a faked-states attack along the lines of Sec. II on the six-state protocol gives 25% QBER in the case of total efficiency mismatch, while the straight intercept-resend attack results in 33.3% QBER).

On the other hand, the SARG04 protocol [36–38] is vulnerable to this attack. Also, faked states exploiting detector efficiency mismatch can be constructed for energy-time encoding and differential phase shift keying QKD schemes [39–43]; see examples of faked states in Ref. [44].

Implementations with a source of entangled pairs placed *outside* of Alice and Bob (as opposed to using it inside Alice to prepare the states) give Eve additional degrees of freedom to run this attack. When photons travel from Alice to Bob, Eve can completely block only one of Bob's bases (one detector is blocked by timing and the other by destructive interference in this basis). This allows to eavesdrop on the protocols that use two bases (BB84, SARG04), but not on the protocols that use three bases (six-state protocol, Ekert protocol [3] if it is implemented with an entangled pair source inside Alice). However when photons travel from the entangled pair source to Alice and Bob with both paths accessible to Eve, she can replace the entangled pair source with a faked one, generating two faked states synchronously: one for Alice and one for Bob. She can generate a pair of faked states that block completely one basis at Alice and another basis at Bob. Then Alice and Bob only get coincidence clicks in the same basis when they choose the third basis in the protocol. This allows to eavesdrop on the six-state protocol [33,34] if it is implemented in an entangled pair version, with the source of entangled pairs placed between Alice and Bob. Also a set of faked states can be constructed for the Ekert protocol (at least if it is implemented as described in Ref. [3] with no additional consistency checks besides checking that $S=-2\sqrt{2}$ [44]).

Throughout the paper, Eve used time t as a control parameter to alter detector efficiencies. We note that t could in principle be regarded as a general control parameter allowing Eve to change Bob's detector efficiencies. It could be not necessarily time but, e.g., polarization or wavelength. For instance, in up-conversion single-photon detectors [45–47] hardware gating of detectors is removed, but a narrow wavelength selectivity is introduced instead. Eve could try to use the wavelength of pulses instead of time to run this attack.

Finally we note that Qi *et al.* have recently proposed an interesting modification of our attack [48].

APPENDIX: QUANTUM NONDEMOLITION MEASUREMENT OF QUBIT TIMING

Here we will show that Eve can perform quantum nondemolition measurements of the timing of the qubits, and collapse Alice's photon pulses into arbitrarily narrow pulses. This measurement does not affect the degrees of freedom encoding the qubit. While (time-bin) phase-encoded qubits are considered here, one may treat other encodings in a similar way.

The phase-encoded qubit is denoted $|\varphi\rangle_{t_0}$. Here, φ is the phase difference between the two pulses (0°, 90°, 180°, or 270°), and t_0 is the (absolute) timing of the pulses, i.e., the time of the peak of the first pulse. If we assume that $|\varphi\rangle_{t_0}$ is a single-photon state,[4] it can be expressed as

$$|\varphi\rangle_{t_0}=\frac{1}{\sqrt{2}}(a^{\dagger}_{t_0}+e^{i\varphi}a^{\dagger}_{t_0+\tau})|0\rangle, \tag{A1}$$

where $|0\rangle$ is the vacuum state of the single optical mode, τ is the time delay between the two pulses, and

$$a^{\dagger}_{t_0}=\int dt\ \xi(t,t_0)a^{\dagger}(t). \tag{A2}$$

In Eq. (A2), $a^{\dagger}(t)$ is the continuous-time creation operator [49] of the optical mode. The operator satisfies the commutator relation $[a(t),a^{\dagger}(t')]=\delta(t-t')$. The function $\xi(t,t_0)$ represents, for instance, a Gaussian pulse shape:

$$\xi(t,t_0)=(2\Delta^2/\pi)^{1/4}\exp[-i\omega_0(t-t_0)-\Delta^2(t-t_0)^2]. \tag{A3}$$

Here ω_0 and Δ are the central frequency and pulse bandwidth, respectively. The duration t_Δ of the pulse is of the order $1/\Delta$, and satisfies $t_\Delta \ll \tau$.

If Eve wants to measure the timing of a qubit pulse pair, she should do a nondemolition measurement that does not affect the degrees of freedom encoding the qubit. She divides the pulse time range $[t_0-t_\Delta/2,t_0+t_\Delta/2]$ into small intervals $T_i=[t_0-t_\Delta/2+i\Delta t,t_0-t_\Delta/2+(i+1)\Delta t]$, where i is a positive

[3] Although the B92 protocol and the modification of the BB84 protocol in Refs. [31,32] are not affected by the attack described in the present paper, they are instead vulnerable to another attack. These protocols apply the key bit values directly at Bob's phase modulator, encoded in the phase shift settings. This makes them vulnerable to the large-pulse attack [51,52]: The phase shift settings could be read by Eve from Bob's modulator using external light pulses which do not have to be very bright. The Scarani-Acin-Ribordy-Gisin 2004 (SARG04) protocol [36–38] also applies the key bit values at Bob's modulator. Other protocols only apply detection bases at Bob's modulator, which makes them less vulnerable to the large-pulse attack.

[4] Coherent pulses can be treated along the same lines.

integer and Δt is her time resolution. [We assume that she has rough estimates of t_0 and t_Δ *a priori*, with precision better than (of the order of) t_Δ. Moreover, she knows τ with precision better than Δt.] The non-demolition measurement is described formally by the projectors

$$P(T_i) = \int_{T_i} dt[a^\dagger(t)|0\rangle\langle 0|a(t) + a^\dagger(t+\tau)|0\rangle\langle 0|a(t+\tau)]. \tag{A4}$$

Note that $P(T_i)P(T_j) = \delta_{ij}P(T_i)$ and $\Sigma_i P(T_i) = 1$ in the Hilbert space spanned by the signal states (A1), so this is a valid quantum mechanical projective measurement [50]. Moreover, when the projectors $P(T_i)$ act on the state (A1) the pulse width of each of the two pulses collapses to a smaller pulse width Δt; however the qubit encoding is not affected. In other words, Eve compresses the pulses and obtains the timing information i.

One way to implement this measurement is first to switch the two pulses into two optical modes a and b. The first pulse is then delayed by τ so that the two pulses arrive at the measuring device simultaneously. The signal state (A1) can now be expressed as $|\varphi\rangle = \frac{1}{\sqrt{2}}(a^\dagger + e^{i\varphi}b^\dagger)|00\rangle = \frac{1}{\sqrt{2}}(|10\rangle + e^{i\varphi}|01\rangle)$, omitting the time notation for simplicity. Now, Eve lets a probe (a simple quantum computer) interact unitarily with the signal state, described as follows: $|00\rangle|0\rangle \to |00\rangle|0\rangle$, $|01\rangle|0\rangle \to |01\rangle|1\rangle$, $|10\rangle|0\rangle \to |10\rangle|1\rangle$. Here the last state in the product denotes that of the probe. Since $|00\rangle|0\rangle \to |00\rangle|0\rangle$ and $|\varphi\rangle|0\rangle \to |\varphi\rangle|1\rangle$, Eve will detect the presence of the qubit without disturbing it. Moreover, if her measurement device is sufficiently fast, she is able to obtain the timing (and the pulses will collapse into shorter ones).

[1] C. H. Bennett and G. Brassard, in Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing (IEEE Press, New York, 1984), pp. 175–179.
[2] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, J. Cryptology **5**, 3 (1992).
[3] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).
[4] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002).
[5] D. Mayers, in Advances in Cryptology—Proceedings of Crypto'96, *Lecture Notes in Computer Science, Vol. 1109*, edited by N. Koblitz (Springer, New York), pp. 343–357.
[6] D. Mayers, J. Assoc. Comput. Mach. **48**, 351 (2001).
[7] H.-K. Lo and H. F. Chau, Science **283**, 2050 (1999).
[8] P. W. Shor and J. Preskill, Phys. Rev. Lett. **85**, 441 (2000).
[9] M. Koashi and J. Preskill, Phys. Rev. Lett. **90**, 057902 (2003).
[10] H. Inamori, N. Lütkenhaus, and D. Mayers, e-print quant-ph/0107017.
[11] D. Gottesman, H.-K. Lo, N. Lütkenhaus, and J. Preskill, Quantum Inf. Comput. **4**, 325 (2004).
[12] V. Makarov and D. R. Hjelme, J. Mod. Opt. **52**, 691 (2005).
[13] C. Shannon, Bell Syst. Tech. J. **27**, 379 (1948).
[14] I. Csiszár and J. Körner, IEEE Trans. Inf. Theory **24**, 339 (1978).
[15] U. M. Maurer, IEEE Trans. Inf. Theory **39**, 733 (1993).
[16] C. H. Bennett, G. Brassard, C. Crépeau, and U. M. Maurer, IEEE Trans. Inf. Theory **41**, 1915 (1995).
[17] S. Felix, N. Gisin, A. Stefanov, and H. Zbinden, J. Mod. Opt. **48**, 2009 (2001).
[18] G. Brassard, N. Lütkenhaus, T. Mor, and B. C. Sanders, Phys. Rev. Lett. **85**, 1330 (2000).
[19] N. Lütkenhaus, Phys. Rev. A **61**, 052304 (2000).
[20] N. Lütkenhaus and M. Jahma, New J. Phys. **4**, 44 (2002).
[21] D. Gottesman and H.-K. Lo, IEEE Trans. Inf. Theory **49**, 457 (2003).
[22] V. Makarov, A. Brylevski, and D. Hjelme, Appl. Opt. **43**, 4385 (2004).
[23] A. Lacaita, F. Zappa, S. Cova, and P. Lovati, Appl. Opt. **35**, 2986 (1996).
[24] F. Zappa, A. Lacaita, S. Cova, and P. Lovati, Opt. Eng. (Bellingham) **35**, 938 (1996).
[25] C. H. Bennett, Phys. Rev. Lett. **68**, 3121 (1992).
[26] M. Koashi, Phys. Rev. Lett. **93**, 120501 (2004).
[27] A. Muller, T. Herzog, B. Huttner, W. Tittel, H. Zbinden, and N. Gisin, Appl. Phys. Lett. **70**, 793 (1997).
[28] J.-M. Mérolla, Y. Mazurenko, J.-P. Goedgebuer, and W. T. Rhodes, Phys. Rev. Lett. **82**, 1656 (1999).
[29] W. T. Buttler, R. J. Hughes, P. G. Kwait, S. K. Lamoreaux, G. G. Luther, G. L. Morgan, J. E. Nordholt, C. G. Peterson, and C. M. Simmmons, Phys. Rev. Lett. **81**, 3283 (1998).
[30] T. Durt, Phys. Rev. Lett. **83**, 2476 (1999); W. T. Buttler *et al.*, *ibid.* **83**, 2477 (1999).
[31] M. LaGasse, U.S. Patent No. 20050190922 (pending).
[32] P. M. Nielsen, C. Schori, J. L. Sørensen, L. Salvail, I. Damgård, and E. Polzik, J. Mod. Opt. **48**, 1921 (2001).
[33] D. Bruß, Phys. Rev. Lett. **81**, 3018 (1998).
[34] H. Bechmann-Pasquinucci and N. Gisin, Phys. Rev. A **59**, 4238 (1999).
[35] C. H. Bennett, G. Brassard, S. Breidbart, and S. Wiesner, IBM Tech. Discl. Bull. **26**, 4363 (1984).
[36] V. Scarani, A. Acin, G. Ribordy, and N. Gisin, Phys. Rev. Lett. **92**, 057901 (2004).
[37] A. Acin, N. Gisin, and V. Scarani, Phys. Rev. A **69**, 012309 (2004).
[38] C. Branciard, N. Gisin, B. Kraus, and V. Scarani, Phys. Rev. A **72**, 032301 (2005).
[39] W. Tittel, J. Brendel, H. Zbinden, and N. Gisin, Phys. Rev. Lett. **84**, 4737 (2000).
[40] Y. Nambu, T. Hatanaka, and K. Nakamura, Jpn. J. Appl. Phys., Part 2 **43**, L1109 (2004).
[41] K. Inoue, E. Waks, and Y. Yamamoto, Phys. Rev. Lett. **89**, 037902 (2002).
[42] W. T. Buttler, J. R. Torgerson, and S. K. Lamoreaux, Phys. Lett. A **299**, 38 (2002).
[43] H. Takesue, E. Diamanti, T. Honjo, C. Langrock, M. M. Fejer, K. Inoue, and Y. Yamamoto, New J. Phys. **7**, 232 (2005).
[44] V. Makarov, J. Skaar, and A. Anisimov, http://www.iet.ntnu.no/groups/optics/qcr/poster-minsk-200605/ .
[45] R. T. Thew, S. Tanzilli, L. Krainer, S. C. Zeller, A. Rochas, I. Rech, S. Cova, H. Zbinden, and N. Gisin, New J. Phys. **8**, 32 (2006).

[46] C. Langrock, E. Diamanti, R. V. Roussev, Y. Yamamoto, M. M. Fejer, and H. Takesue, Opt. Lett. **30**, 1725 (2005).
[47] E. Diamanti, H. Takesue, T. Honjo, K. Inoue, and Y. Yamamoto, Phys. Rev. A **72**, 052311 (2005).
[48] B. Qi, C.-H. Fung, H.-K. Lo, and X. Ma, e-print quant-ph/0512080.
[49] R. Loudon, *The Quántum Theory of Light* (Oxford University Press, Oxford, 2000).
[50] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, U.K., 2000).
[51] A. Vakhitov, V. Makarov, and D. R. Hjelme, J. Mod. Opt. **48**, 2023 (2001).
[52] N. Gisin, S. Fasel, B. Kraus, H. Zbinden, and G. Ribordy, Phys. Rev. A **73**, 022320 (2006).

Faked states attack using detector efficiency mismatch on SARG04, phase-time, DPSK, and Ekert protocols

Vadim Makarov[1, 2, *] and Johannes Skaar[1]

[1] *Department of Electronics and Telecommunications, Norwegian University of Science and Technology, NO-7491 Trondheim, Norway*
[2] *Radiophysics Department, St. Petersburg State Polytechnic University, Politechnicheskaya street 29, 195251 St. Petersburg, Russia*

(Dated: February 27, 2007)

In quantum cryptosystems, variations in detector efficiency can be exploited to stage a successful attack. This happens when the efficiencies of Bob's two detectors are different functions of a control parameter accessible to Eve (e.g., timing of the incoming pulses). It has previously been shown that the Bennett-Brassard 1984 (BB84) protocol is vulnerable to this attack. In this paper, we show that several other protocols and encodings are also vulnerable. We consider a faked states attack in the case of a partial efficiency mismatch on the Scarani-Acin-Ribordy-Gisin 2004 (SARG04) protocol, and derive the quantum bit error rate as a function of detector efficiencies. Additionally, it is shown how faked states can in principle be constructed for quantum cryptosystems that use a phase-time encoding, the differential phase shift keying (DPSK) and the Ekert protocols.

PACS numbers: 03.67.Dd

I. INTRODUCTION

Quantum key distribution (QKD) is a technique that allows remote parties to grow shared secret random key material at a steady rate, given an insecure optical communication channel and an initially authenticated classical communication channel between them [1, 2]. Since the first experimental demonstration seventeen years ago [1], QKD systems have developed to commercial devices working over tens of kilometers of optical fiber [3, 4], as well as experiments over more than a hundred kilometers of fiber [5, 6, 7, 8] and 23 km of free space [9, 10]. Although the security of QKD has been unconditionally proven for a model of equipment that includes certain non-idealities [11, 12, 13, 14, 15], not all real properties of optical and electrooptical components have been included into the proof. Identifying the properties of components potentially dangerous for security and integrating them into the proof (or closing the issue in some other way) is an ongoing work [16, 17, 18, 19, 20, 21].

In this paper, we continue to analyse a common imperfection of Bob's single photon detectors: variation of their efficiency that can be controlled by Eve via a choice of an external parameter. It has been shown in Refs. 20 and 21 that even smallest variations of one detector efficiency relative to the other detector reduce the amount of secret information theoretically available to Alice and Bob in the case of the BB84 protocol. The amount of key compression during the privacy amplification must be adjusted based on an evaluation of the worst-case efficiency mismatch of Bob's detectors. We recap these results in Sec. II. In the following sections, we consider other protocols and encodings: SARG04 in Sec. III, a class of schemes using the phase-time encoding and the DPSK protocol in Sec. IV, and the Ekert protocol with a source of entangled photons in Sec. V. It is shown how to construct a faked states attack [19] against these protocols and encodings. For the SARG04, the upper bound on available secret key information is estimated, through calculating the quantum bit error rate (QBER) caused by this attack.

II. BB84 PROTOCOL

Variation of efficiency is a common and, indeed, unavoidable imperfection of single photon detectors. The efficiency may depend on the timing of incoming light pulse (e.g., in gated detectors based on avalanche photodiodes), wavelength of incoming light (e.g., in upconversion detectors [22, 23, 24]), polarization and other parameters conceivably controllable by Eve. In QKD schemes that employ two detectors (or a time-multiplexed detector), the variation will be different between the detectors (or detection windows), allowing Eve to control the relative probability of one detection outcome over the other. To illustrate how she can use this to construct a successful attack on the BB84 protocol [1], we assume first that the efficiency mismatch for some values of the control parameter is so large that Eve can practically blind either detector while the other remains sensitive, i.e., we have the case of a *total efficiency mismatch*. We call the value of the control parameter that blinds the 1 detector t_0, and the value that blinds the 0 detector t_1. Eve then proceeds with a faked states attack [19], which is an intercept-resend attack where she uses a replica of Bob's setup to detect every Alice's state, and resends specially formed faked states to Bob. The faked state she resends in this case would be a state normally used in the protocol but with the opposite bit value in

*Electronic address: makarov@vad1.com

the opposite basis comparing to what Eve has detected. Additionally, in the faked state she sets the value of the control parameter that blinds the detector for the opposite bit value from what she has detected. For example, suppose Eve has detected the 0 bit value in the X basis. She resends the 1 bit in the Z basis, with the control parameter t_0. If Bob tries to detect this faked state in the Z basis, he never detects anything, for his 1 detector is blinded by Eve's choice of the control parameter. If he tries to detect in the X basis, he with equal probability doesn't detect anything or detects the 0 bit. To run a successful intercept-resend attack, Eve needs either her detection basis always be the same as Alice's, or her detection basis always be the same as Bob's; here she achieves the latter.[1] The reader may notice that the attack reduces the detection probability at Bob, but this can be compensated by a proportionally increased brightness of the faked states. Thus, in the case of the total efficiency mismatch, Eve can run an attack that causes zero QBER and provides her full information on the key.

In the case of a *partial efficiency mismatch*, when either detector cannot be completely blinded, this attack causes some non-zero QBER. Eve can pick the values of the control parameter to minimize the ratios $\eta_0(t_1)/\eta_1(t_1)$ and $\eta_1(t_0)/\eta_0(t_0)$, where η_0 and η_1 are efficiencies of the 0 and 1 detectors. It has been shown in Ref. 20 that in this case the attack causes

$$(\text{QBER}) = \frac{2\eta_0(t_1) + 2\eta_1(t_0)}{\eta_0(t_0) + 3\eta_0(t_1) + 3\eta_1(t_0) + \eta_1(t_1)}. \quad (1)$$

In the special case of symmetric detector efficiency curves $\eta_0(t_1)/\eta_1(t_1) = \eta_1(t_0)/\eta_0(t_0) \equiv \eta$ and Eve adjusting the brightness of her faked states sent with t_0 and t_1 such that Bob's detection probability for both values of the control parameter remains equal, this simplifies to

$$(\text{QBER}) = \frac{2\eta}{1 + 3\eta}. \quad (2)$$

The QBER value of 0.11 (commonly regarded as the threshold value for the BB84 protocol, after which no secret key could be extracted) would be reached at $\eta \approx 1/15$.

The attack described above is not necessarily optimal. In Ref. 20 it is indicated that the BB84 protocol is secure provided $(\text{QBER}) \lesssim 0.11\eta$. However, note that Eq. 11 in Ref. 20 is incorrect; the available bit rate after privacy amplification is reduced even in the case $(\text{QBER}) = 0$ [21]. A rigorous treatment of the security for arbitrary attacks exploiting detector efficiency mismatch is still not available.

[1] Surely, in the latter case Eve detects half of Alice's bits in a wrong basis. However, when she forces Bob to detect in the same wrong basis, all her wrong detection results are later discarded by Alice and Bob during sifting.

III. SARG04 PROTOCOL

The purpose of the SARG04 protocol [25, 26, 27] is to increase the maximum trasmission distance and key yield in schemes that use a weak coherent source; the protocol has improved characteristics against the photon number splitting attack, comparing to the BB84. Here we consider the version of the SARG04 that uses states physically equivalent to those used in the BB84 (Fig. 1), and differs from the latter only at the sifting stage. The bit values 0 and 1 in the SARG04 are encoded by the choice of basis. Alice sends randomly one of the four states $|0_a\rangle$, $|0_b\rangle$, $|1_a\rangle$ or $|1_b\rangle$. Bob measures either in the 0 or 1 detection basis, and uses two detectors labeled a and b. At the sifting stage, Alice announces publicly a set of two states that contains the actual state sent and a random state from the opposite basis. For definiteness, suppose that Alice has sent $|0_a\rangle$ and that she has announced the set $\{|0_a\rangle, |1_a\rangle\}$. If Bob has measured in the 0 basis, he has certainly got the result 0_a; but since this result is possible for both states in the set $\{|0_a\rangle, |1_a\rangle\}$, he has to discard it. If he has measured in the 1 basis and got 1_a, he again cannot discriminate. But if he has measured in the 1 basis and got 1_b, he knows that Alice has sent $|0_a\rangle$, and adds 0 to his key.

Since this protocol uses the same states as the BB84, the faked states attack described in the previous section could be applied to it. In the case of the total efficiency mismatch, it obviously causes zero QBER. To calculate the QBER it causes in the case of the partial efficiency mismatch, we follow the approach of Ref. 20 and consider all the possible basis and detector combinations during the attack. The different events are shown in Table I for the special case where Alice sends the $|0_a\rangle$ state (the other three cases are symmetrical to this case). We disregard the probability of Eve's and Bob's detectors firing simultaneously due to the multiphoton fraction of the pulses, assume that Bob's detectors have no dark counts, assume that Eve's detectors and optical alignment are perfect, and that Eve generates faked states that match the optical alignment in Bob's setup perfectly. None of these assumptions is critical for the attack to work, but it is convenient to make them to simplify the calculation.

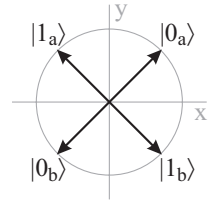
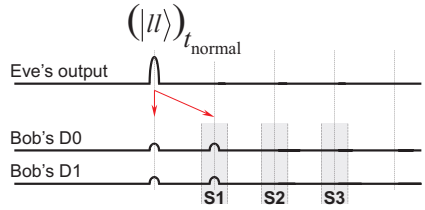
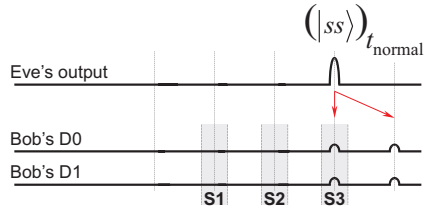
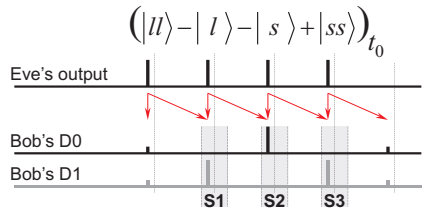
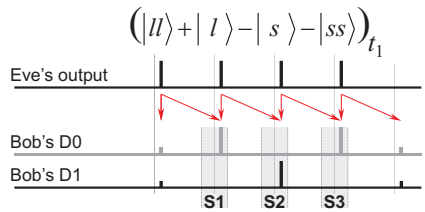


FIG. 1: States configuration for the SARG04 protocol in the case when the states used are physically equivalent to those in the BB84 protocol. The circle represents the equator of the Poincare sphere.

TABLE I: The intercept-resend attack on the SARG04 protocol when Alice sends the $|0_a\rangle$ state (as indicated in the first column; in the table, brackets around states are omitted for clarity). The second column contains the basis chosen by Eve and the measurement result; the third column shows the state and timing as resent by Eve. In the next columns Bob's basis choice and measurement results are given. For the case with the partial detector sensitivity mismatch, the probabilities for the different results are shown, given Eve's state and timing in addition to Bob's basis. In the last two columns, pairs of states announced by Alice during sifting (two possible pairs announced with equal probability of 1/2), and the sifting results, are shown. Note that, for ease of discussion, the first two rows are repeated so that each row in the table occurs with probability 1/8.

Alice	→Eve	Eve→	Bob	Result, Probability		Alice's announce	Sifting
0_a	0_a	$1_b t_a$	0	a,	$\frac{1}{2}\eta_a(t_a)$	$\{0_a, 1_a\}$	Discard
						$\{0_a, 1_b\}$	Discard
				b,	$\frac{1}{2}\eta_b(t_a)$	$\{0_a, 1_a\}$	1_a (error)
						$\{0_a, 1_b\}$	1_b (error)
0_a	0_a	$1_b t_a$	1	a,	0		
				b,	$\eta_b(t_a)$	$\{0_a, 1_a\}$	0_a (right)
						$\{0_a, 1_b\}$	Discard
0_a	0_a	$1_b t_a$	0	a,	$\frac{1}{2}\eta_a(t_a)$	$\{0_a, 1_a\}$	Discard
						$\{0_a, 1_b\}$	Discard
				b,	$\frac{1}{2}\eta_b(t_a)$	$\{0_a, 1_a\}$	1_a (error)
						$\{0_a, 1_b\}$	1_b (error)
0_a	0_a	$1_b t_a$	1	a,	0		
				b,	$\eta_b(t_a)$	$\{0_a, 1_a\}$	0_a (right)
						$\{0_a, 1_b\}$	Discard
0_a	1_a	$0_b t_a$	0	a,	0		
				b,	$\eta_b(t_a)$	$\{0_a, 1_a\}$	1_a (error)
						$\{0_a, 1_b\}$	1_b (error)
0_a	1_a	$0_b t_a$	1	a,	$\frac{1}{2}\eta_a(t_a)$	$\{0_a, 1_a\}$	Discard
						$\{0_a, 1_b\}$	0_a (right)
				b,	$\frac{1}{2}\eta_b(t_a)$	$\{0_a, 1_a\}$	0_a (right)
						$\{0_a, 1_b\}$	Discard
0_a	1_b	$0_a t_b$	0	a,	$\eta_a(t_b)$	$\{0_a, 1_a\}$	Discard
						$\{0_a, 1_b\}$	Discard
				b,	0		
0_a	1_b	$0_a t_b$	1	a,	$\frac{1}{2}\eta_a(t_b)$	$\{0_a, 1_a\}$	Discard
						$\{0_a, 1_b\}$	0_a (right)
				b,	$\frac{1}{2}\eta_b(t_b)$	$\{0_a, 1_a\}$	0_a (right)
						$\{0_a, 1_b\}$	Discard

TABLE II: Faked states for a QKD system utilizing the phase-time encoding. Each faked state is illustrated by a time diagram. The arrows indicate how every pulse coming to Bob is split into the two arms of his interferometer. The waveform for the intensity of light at Bob's detector that is blinded by Eve's choice of the control parameter t is printed in gray.

Eve's detection result	Faked state
S1	
S3	
$S2_0$	
$S2_1$	

Based on the probabilities in the table, we calculate the QBER caused by the attack. When Alice sends the $|0_a\rangle$ state, the probability that the qubit arrives at Bob and is *not* discarded as an inconclusive detection result during sifting is

$$P(\text{arrive}|A{=}0_a){=}\frac{1}{8}[\frac{1}{4}\eta_a(t_a){+}\frac{1}{4}\eta_a(t_b){+}\frac{13}{4}\eta_b(t_a){+}\frac{1}{4}\eta_b(t_b)]. \quad (3)$$

The probability of arrival averaged over Alice's four state choices is found by symmetrization of this equation, yielding

$$P(\text{arrive}) = \frac{1}{32}[\eta_a(t_a) + 7\eta_a(t_b) + 7\eta_b(t_a) + \eta_b(t_b)]. \quad (4)$$

Similarly, we find the QBER,

$$(\text{QBER}){=}\frac{P(\text{error})}{P(\text{arrive})}{=}\frac{4\eta_a(t_b) + 4\eta_b(t_a)}{\eta_a(t_a) + 7\eta_a(t_b) + 7\eta_b(t_a) + \eta_b(t_b)}, \quad (5)$$

where $P(\text{error})$ accounts for the cases when Bob keeps a bit value different from what Alice has sent.

In the special case of symmetric detector efficiency curves, we get

$$(\text{QBER}) = \frac{4\eta}{1 + 7\eta}. \quad (6)$$

The SARG04 protocol has security bounds different from the BB84 protocol [27, 28, 29]. While it is invalid to directly compare QBER between the protocols, we note that in SARG04 this attack causes QBER lower than 0.11 when $\eta \lesssim 1/30$, while in BB84 (see Eq. 2) the same happens when $\eta \lesssim 1/15$. Thus, the effect of the described attack on these two protocols appears to be quantitatively different, although of the same order of magnitude.

IV. PHASE-TIME ENCODING AND DPSK PROTOCOL

In a QKD system with the phase-time encoding [30], Alice prepares one of the four states: $|l\rangle$, $|s\rangle$, $|l\rangle + |s\rangle$ or $|l\rangle - |s\rangle$, where $|l\rangle$ and $|s\rangle$ denote states that have travelled via the long and short arm of Alice's AMZ (Fig. 2). Bob gates his detectors three times. The state $|l\rangle$ can cause a detection either in the S1 or S2 time slot. The state $|s\rangle$ can cause a detection either in the S2 or S3 time slot. The states $|l\rangle + |s\rangle$ and $|l\rangle - |s\rangle\}$ can cause a detection in any of the three time slots. The plus or minus sign determines which of the two detectors (D0 or D1) clicks when the detection happens in the S2 time slot where the pulses from the two arms of Bob's AMZ have interfered. Thus, pairs of states $\{|l\rangle, |s\rangle\}$ and $\{|l\rangle + |s\rangle, |l\rangle - |s\rangle\}$ form two bases. This system uses the BB84 protocol. (We note that the function of Bob's apparatus is similar to an earlier system that uses entangled photons in energy-time Bell states [31].)

Faked states for this QKD system are listed in Table II. Eve uses an apparatus that can form a single pulse (denoted $|ll\rangle$) in the time slot that follows the time slot of Alice's $|l\rangle$ state, a single pulse (denoted $|ss\rangle$) in the time slot that precedes the time slot of Alice's $|s\rangle$ state, or coherent states consisting of four pulses with certain phase shifts between them and a certain value of the control parameter t (which can be timing as shown on the diagrams, or some other parameter). The single pulse states are sent with the control parameter value t_{normal} that blinds neither detector. The coherent four pulse states are sent with the control parameter value t_0 or t_1 that blinds the detector D1 or D0. The faked states rely on the lack of detector gating in what would be Bob's time slots S0 and S4, or on Bob discarding detection results with these times. Additionally, in the last two faked states, Eve blinds one of Bob's detectors by the choice of the control parameter.

In a QKD system with the DPSK protocol [8], Alice randomly modulates the phase of a weak coherent pulse train by $\{0, \pi\}$ for each pulse, and sends it to Bob with an average photon number of less than 1 per pulse (Fig. 3). Bob measures the phase difference between adjacent pulses with a 1-bit delay interferometer followed by two detectors placed at the interferometer output ports. Detector D0 clicks when the phase difference is 0 and detector D1 clicks when the phase difference is π. Since the average photon number per pulse is less than 1, Bob observes clicks only occasionally and in a random time slot. Bob informs Alice of the time slots in which he has observed clicks. From her modulation data Alice knows which detector has clicked on Bob's side, so they share an identical bit string.

Faked states for this QKD system are constructed similarly to the previous one (Fig. 4). In the case of the DPSK, Eve can run two generators of faked states in parallel, so that states with the values of the control parameter t_0 and t_1 may overlap. When Eve has had identical detection results in two adjacent bit slots, she can use a single-pulse faked state. In all other cases she generates longer faked states that encompass two or more detection results with the same bit value. In these faked states, Bob's other detector is blocked by the choice of the control parameter, and unwanted bit slots are blocked by destructive interference. In the limit, Eve may just generate two consecutive trains of pulses with the control parameters t_0 and t_1, and modulate the phase of pulses in each train to produce the detections she wants at Bob.

The part of Eve's setup that generates faked states for both systems considered in this section may be similar to Alice's setup in Fig. 3. In the case of the DPSK, two such setups could possibly be used, with their outputs combined on an optical coupler.

Although we do not calculate it here, the faked states presented in this section would obviously work in the case of the partial efficiency mismatch, causing the more QBER the smaller the mismatch becomes. We note that schemes utilizing the DPSK protocol with limited-length states [32, 33] can also be attacked using the methods considered in this section.

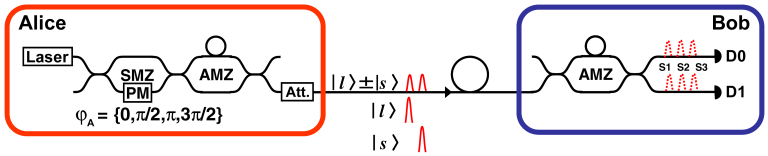


FIG. 2: Scheme of a QKD system utilizing the phase-time encoding [30]. SMZ, symmetric Mach-Zehnder interferometer; AMZ, asymmetric Mach-Zehnder interferometer; PM, phase modulator; Att., optical attenuator; D0 and D1, single photon detectors.

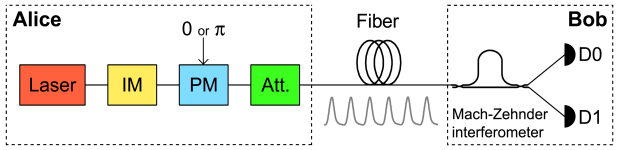


FIG. 3: Scheme of a QKD system utilizing the DPSK protocol [8]. IM, intensity modulator; PM, phase modulator; Att., optical attenuator; D0 and D1, single photon detectors.

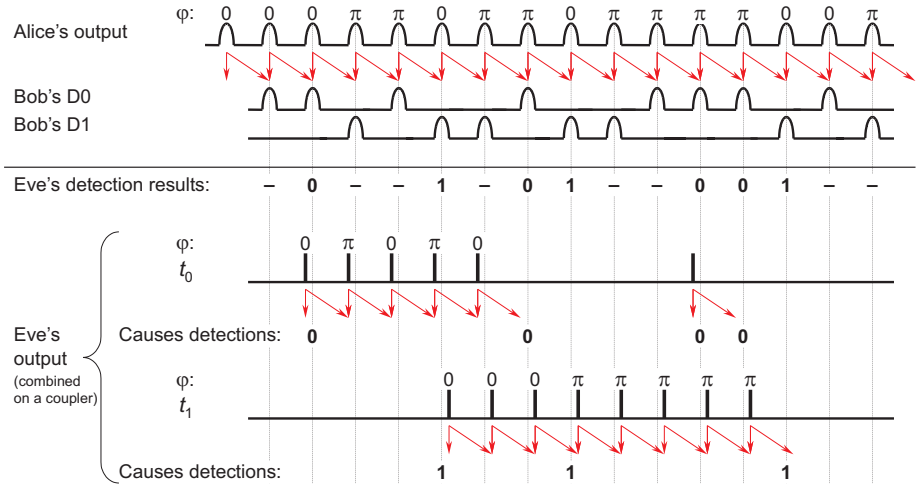


FIG. 4: Time diagram of a QKD system utilizing the DPSK ptotocol, and faked states for it. The three uppermost waveforms represent the intensity of light during normal system operation; the phase φ of each Alice's pulse is noted. The rest of the diagram shows examples of possible faked states. For the compactness of illustration, Alice's average photon number per pulse is increased greatly, which gives Eve more frequent detections than would be possible in a real system. The arrows indicate how every pulse coming to Bob is split into the two arms of his interferometer.

V. EKERT PROTOCOL

The Ekert protocol [34] uses an external source of entangled pairs of photons in a singlet state, from which one photon is routed to Alice and the other to Bob. Alice and Bob perform measurements on their photons in one of the possible bases (Fig. 5), choosing between the bases randomly and independently of one another for each pair of incoming photons. After a series of measurements has taken place, the choices of bases are publicly announced. For those pairs where Alice and Bob both have registered a count in their detectors, quantum mechanics guarantees certain degree of correlation between the measurement results, depending on the combination of the bases chosen. The quantity

$$E(\mathrm{a}_i,\mathrm{b}_j) = P_{++}(\mathrm{a}_i,\mathrm{b}_j) + P_{--}(\mathrm{a}_i,\mathrm{b}_j) - P_{+-}(\mathrm{a}_i,\mathrm{b}_j) - P_{-+}(\mathrm{a}_i,\mathrm{b}_j) \quad (7)$$

is the correlation coefficient of the measurements performed by Alice in the a_i basis and by Bob in the b_j basis. Here $P_{\pm\pm}(\mathrm{a}_i,\mathrm{b}_j)$ denotes the probability that the result ±1 has been obtained in the a_i basis and ±1 in the b_j basis. For two identical pairs of bases ($\mathrm{a}_2,\mathrm{b}_1$ and $\mathrm{a}_3,\mathrm{b}_2$) the measurement results are totally anticorrelated:

$$E(\mathrm{a}_2,\mathrm{b}_1) = E(\mathrm{a}_3,\mathrm{b}_2) = -1. \quad (8)$$

These measurement results are used in the protocol to form a secret key. Four other basis combinations are used to check for possible eavesdropping via computing the Clauser-Horne-Shimony-Holt quantity

$$S = E(\mathrm{a}_1,\mathrm{b}_1) - E(\mathrm{a}_1,\mathrm{b}_3) + E(\mathrm{a}_3,\mathrm{b}_1) + E(\mathrm{a}_3,\mathrm{b}_3), \quad (9)$$

which in the absence of eavesdropping should be equal to $-2\sqrt{2}$.

If the pairs of detectors on both Alice's and Bob's sides have a total efficiency mismatch, Eve can successfully mount a faked states attack that provides $S = -2\sqrt{2}$. She substitutes the source of entangled photons with one that generates, with certain probabilities, pairs of faked states listed below. We have assumed that, at Alice and at Bob, one detector is used to get the $+1$ measurement result in all three bases, and the other to get the -1 result. We have also assumed that Alice and Bob normalize detection probabilities separately for each combination of a_i and b_j before computing $E(\mathrm{a}_i,\mathrm{b}_j)$ correlation coefficients.

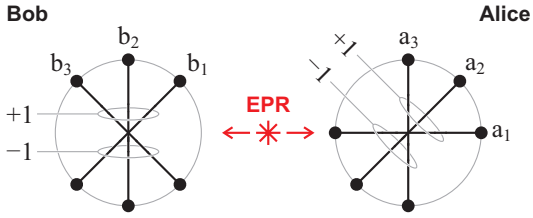


FIG. 5: Possible measurements by Alice and Bob in the Ekert protocol. The circles represent the equator of the Poincare sphere. Measurement bases are denoted by letters with indices; each measurement can yield $+1$ or -1 result as labeled on the diagram. EPR, source of entangled photon pairs.

The simplest set of faked states consists of two pairs; however, to make it symmetric, we expand it to four pairs grouped in two combinations. The purpose of one combination named $\boldsymbol{\alpha}$ is to be detected with equal probability and always produce total anticorrelation regardless of Alice's and Bob's choice of basis. It can, for example, consist of a pair of states conjugate to every other state used in the protocol and sent to Alice and Bob with opposite values of the control parameter t_{+1} and t_{-1}, which blind the -1 and $+1$ detectors. If linear polarizations are used in the protocol, Eve randomly sends to Alice and Bob either a pair of circular polarizations $[(\mathrm{circular})_{t_{+1}},(\mathrm{circular})_{t_{-1}}]$ or a pair $[(\mathrm{circular})_{t_{-1}},(\mathrm{circular})_{t_{+1}}]$.[2] In the other combination named $\boldsymbol{\beta}$, Eve sends either a pair $[(|-\mathrm{a}_3\rangle)_{t_{+1}},(|-\mathrm{b}_1\rangle)_{t_{+1}}]$ or a pair $[(|\mathrm{a}_3\rangle)_{t_{-1}},(|\mathrm{b}_1\rangle)_{t_{-1}}]$. It produces total correlation for the pair of bases $\mathrm{a}_1,\mathrm{b}_3$ used in computing S, and for three other pairs of bases ($\mathrm{a}_1,\mathrm{b}_2$; $\mathrm{a}_2,\mathrm{b}_2$; $\mathrm{a}_2,\mathrm{b}_3$) which are not used in the protocol. The combinations $\boldsymbol{\alpha}$ and $\boldsymbol{\beta}$ are generated by Eve with probabilities $P_{\boldsymbol{\alpha}} = 0.586$, $P_{\boldsymbol{\beta}} = 0.414$. It is easy to check that this will result in the desired value of the quantity S:

$$S = -1 - (-0.172) - 1 - 1 = -2\sqrt{2}. \quad (10)$$

If we add a third combination to the set, it would be possible for all four terms in the equation for S to have an equal absolute value, just as in the absence of the attack. In the third combination $\boldsymbol{\gamma}$, Eve sends either a pair $[(|-\mathrm{a}_2\rangle)_{t_{+1}},(|-\mathrm{b}_2\rangle)_{t_{+1}}]$ or a pair $[(|\mathrm{a}_2\rangle)_{t_{-1}},(|\mathrm{b}_2\rangle)_{t_{-1}}]$, and the combinations are now generated by Eve with probabilities $P_{\boldsymbol{\alpha}} = 0.116$, $P_{\boldsymbol{\beta}} = 0.653$, $P_{\boldsymbol{\gamma}} = 0.231$. This gives

$$S = -0.707 - 0.707 - 0.707 - 0.707 = -2\sqrt{2}. \quad (11)$$

Although our attack reproduces the expected value of S, it has side effects. Detection probabilities for different combinations of bases become substantially unequal, and the three unused correlation coefficients are not reproduced properly. Thus, the attack relies on the absence of additional consistency checks on the data by the legitimate users. We have not been able to come up with a

[2] Alternatively, in the combination $\boldsymbol{\alpha}$, instead of a circular polarization Eve can send a statistical mixture of two states from a single basis used in the protocol. In particular, she can send either a pair $[(|\mathrm{a}_3\rangle \text{ or } |-\mathrm{a}_3\rangle)_{t_{+1}},(|\mathrm{b}_1\rangle \text{ or } |-\mathrm{b}_1\rangle)_{t_{-1}}]$ or a pair $[(|\mathrm{a}_3\rangle \text{ or } |-\mathrm{a}_3\rangle)_{t_{-1}},(|\mathrm{b}_1\rangle \text{ or } |-\mathrm{b}_1\rangle)_{t_{+1}}]$. This would simplify Eve's apparatus, because here she needs to generate the same states as in the following combination $\boldsymbol{\beta}$.

set of faked states that does not produce any side effects. Also, the attack relies on the source of entangled photons being *outside* of Alice and Bob. If the source is placed inside one of their setups and only one of the two photons is accessible to Eve, it seems to us that with protocols that use more than two bases (the Ekert protocol and the six-state protocol [35, 36, 37]), a zero-QBER attack using the approach described in this section cannot be constructed. However, the six-state protocol implemented on a setup that uses an external source of entangled photons could be successfully attacked using a faked pair source similar to the one described in this section.

VI. CONCLUSION

We have shown that detector efficiency mismatch can be exploited to attack the SARG04 and Ekert protocols, as well as schemes that use the phase-time encoding and the DPSK protocol. The faked states attacks considered here might not be the optimal ones; however, they certainly set upper bounds on the secret information. We emphasize the necessity of characterizing the detector setup thoroughly and establishing security proofs with partial detector efficiency mismatch integrated into the equipment model.

[1] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, J. Cryptology **5**, 3 (1992).
[2] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002).
[3] http://www.idquantique.com/ .
[4] http://www.magiqtech.com/ .
[5] P. A. Hiskett, D. Rosenberg, C. G. Peterson, R. J. Hughes, S. Nam, A. E. Lita, A. J. Miller, and J. E. Nordholt, New J. Phys. **8**, 193 (2006).
[6] T. Kimura, Y. Nambu, T. Hatanaka, A. Tomita, H. Kosaka, and K. Nakamura, Jpn. J. Appl. Phys. **43**, L1217 (2004).
[7] C. Gobby, Z. Yuan, and A. Shields, Appl. Phys. Lett. **84**, 3762 (2004).
[8] H. Takesue, E. Diamanti, T. Honjo, C. Langrock, M. M. Fejer, K. Inoue, and Y. Yamamoto, New J. Phys. **7**, 232 (2005).
[9] C. Kurtsiefer, P. Zarda, M. Halder, H. Weinfurter, P. M. Gorman, P. R. Tapster, and J. G. Rarity, Nature **419**, 450 (2002).
[10] C. Kurtsiefer, P. Zarda, M. Halder, P. M. Gorman, P. R. Tapster, J. G. Rarity, and H. Weinfurter, Proc. SPIE **4917**, 25 (2002).
[11] D. Gottesman, H.-K. Lo, N. Lütkenhaus, and J. Preskill, Quant. Inf. Comput. **4**, 325 (2004).
[12] P. W. Shor and J. Preskill, Phys. Rev. Lett. **85**, 441 (2000).
[13] M. Koashi and J. Preskill, Phys. Rev. Lett. **90**, 057902 (2003).
[14] E. Biham, M. Boyer, P. O. Boykin, T. Mor, and V. Roychowdhury, in Proceedings of the 32nd Annual ACM Symposium on Theory of Computation (ACM Press, New York, 2000), pp. 715–724.
[15] H. Inamori, N. Lütkenhaus, and D. Mayers, e-print quant-ph/0107017.
[16] C. Kurtsiefer, P. Zarda, S. Mayer, and H. Weinfurter, J. Mod. Opt. **48**, 2039 (2001).
[17] A. Vakhitov, V. Makarov, and D. R. Hjelme, J. Mod. Opt. **48**, 2023 (2001).
[18] N. Gisin, S. Fasel, B. Kraus, H. Zbinden, and G. Ribordy, Phys. Rev. A **73**, 022320 (2006).
[19] V. Makarov and D. R. Hjelme, J. Mod. Opt. **52**, 691 (2005).
[20] V. Makarov, A. Anisimov, and J. Skaar, Phys. Rev. A **74**, 022313 (2006).
[21] B. Qi, C.-H. F. Fung, H.-K. Lo, and F.-X. Ma, Quant. Inf. Comp. **7**, 73 (2007).
[22] R. T. Thew, S. Tanzilli, L. Krainer, S. C. Zeller, A. Rochas, I. Rech, S. Cova, H. Zbinden, and N. Gisin, New J. Phys. **8**, 32 (2006).
[23] C. Langrock, E. Diamanti, R. V. Roussev, Y. Yamamoto, M. M. Fejer, and H. Takesue, Opt. Lett. **30**, 1725 (2005).
[24] E. Diamanti, H. Takesue, T. Honjo, K. Inoue, and Y. Yamamoto, Phys. Rev. A **72**, 052311 (2005).
[25] V. Scarani, A. Acin, G. Ribordy, and N. Gisin, Phys. Rev. Lett. **92**, 057901 (2004).
[26] A. Acin, N. Gisin, and V. Scarani, Phys. Rev. A **69**, 012309 (2004).
[27] C. Branciard, N. Gisin, B. Kraus, and V. Scarani, Phys. Rev. A **72**, 032301 (2005).
[28] K. Tamaki and H.-K. Lo, Phys. Rev. A **73**, 010302(R) (2006).
[29] M. Koashi, e-print quant-ph/0507154.
[30] Y. Nambu, T. Hatanaka, and K. Nakamura, Jpn. J. Appl. Phys. Part 2 **43**, L1109 (2004).
[31] W. Tittel, J. Brendel, H. Zbinden, and N. Gisin, Phys. Rev. Lett. **84**, 4737 (2000).
[32] K. Inoue, E. Waks, and Y. Yamamoto, Phys. Rev. Lett. **89**, 037902 (2002).
[33] W. T. Buttler, J. R. Torgerson, and S. K. Lamoreaux, Phys. Lett. A **299**, 38 (2002).
[34] A. K. Ekert, Phys. Rev. Lett **67**, 661 (1991).
[35] D. Bruß, Phys. Rev. Lett. **81**, 3018 (1998).
[36] H. Bechmann-Pasquinucci and N. Gisin, Phys. Rev. A **59**, 4238 (1999).
[37] C. H. Bennett, G. Brassard, S. Breidbart, and S. Wiesner, IBM Tech. Discl. Bull. **26**, 4363 (1984).

4.4. Conclusion

The last chapter has been about the one most important issue in quantum cryptography: its security. We have been specializing in the area of security studies dealing with component imperfections and optical loopholes.

We have considered several practical attacks on QKD systems, and proposed protection measures for each of the discussed vulnerabilities. We have studied the large pulse attack, introduced a new class of attacks — faked states attacks, discovered and studied effects of a common detector imperfection on security — the efficiency mismatch between the 0 and 1 detectors. Also, two possibilities of attacks have been pointed out: detecting light emitted by APDs, and using controlled high-power damage to assist in eavesdropping.

It is too early to see what effect our work would have on the field of quantum cryptography. However, the author is glad to see at least some of the latest QKD systems designed to avoid the vulnerabilities we have pointed out and studied (e.g., [73, 159, 213]). Perhaps the most enthusiastic readers of our publications have been researchers at MaqiQ Technologies, who have applied for several U.S. patents describing protection measures against our attacks ([226, 227]; also [214] with an optical filter “to block photons generated by the SPD”).

Conclusion and future plans

In our research at NTNU, we have tackled several aspects of the interdisciplinary field known as quantum cryptography. We have attempted to construct a fiber optic QKD system and demonstrated its operation in a laboratory setting, developed an optimal phase tracking algorithm for an interferometer working in the photon counting mode, developed an APD-based single photon detector with an afterpulse blocking technique allowing it to run at a higher gating rate than other similar detectors.

A special attention has been paid to the security of QKD, which is a difficult and intricate problem requiring a large amount of scrutiny. Our niche and our contribution to the security field have been the study of vulnerabilities not yet accounted for in theoretical proofs. A large pulse attack, faked states attack, detector efficiency mismatch have been evaluated in detail and protection measures proposed. We think that our group has built a unique expertise in the practical security of QKD, or *quantum cryptanalysis* as we like to call it.

Will the QKD technology succeed and be adopted for wide use? Will it lead to new discoveries beyond what we foresee now? It's perhaps still too early to tell for sure. Right now, QKD has to compete with classical security solutions that are superior in convenience and price, and there seemingly is no pressing need to replace them. When and whether such a pressing need arises, depends on the progress in cryptanalysis (classical cryptanalysis, development of quantum computers), on the one hand, and progress in mathematical encryption (asymmetric ciphers, complexity theory), on the other hand. Then, the market for hi-tech stuff follows its own logic. Sometimes, in the security field, more convenient solutions with weaknesses are chosen over strong but more demanding ones. Sometimes an unforeseen alternative appears. Sometimes, even, a technology is suppressed due to political reasons; though so far, quantum cryptography has enjoyed a strong government support both in the USA and in the European Union, through centralized research and collaboration programs. QKD has a large room for improvement that will be achieved through research in the coming years. Let's not miss our chance to be a part of this development.

Future directions of research at NTNU

Despite the nascent commercialization [47], the bulk of research in quantum cryptography remains at the academia, and continues to grow in volume worldwide. As we see it, possible future directions of this research at NTNU are the following.

- Continuing security studies. Further investigations *beyond those presented in the thesis* are already being made. An experimental investigation has been done of a blinding mode in a passively quenched Si APD that can be used for a successful faked states attack on a cryptosystem that employs this type of APDs. Also, we are attempting to further improve the general security bound for the BB84 protocol that includes the detector efficiency mismatch into the equipment model.
- Repairing the existing QKD setup and doing experiments demonstrating key distribution and characterizing detector performance. Since we already have the setup and necessary equipment, all this can be done relatively cheap. The ex-

periments might include characterizing performance of QKD over various lengths of spooled and installed optical fiber, further assessing the performance of phase tracking, assessing the performance of afterpulse blocking, and measuring various characteristics of APDs in our detector.

If a sufficient funding is obtained, security studies could be expanded in directions that require setting up new experiments, e.g., eavesdropping assisted by high-power damage as outlined in Section 4.3.2. Experimental investigation of some of the numerous novel ideas in QKD would also be actual, e.g., the decoy state protocol (see Section 4.2.1.), differential phase shift keying [32, 74, 75], upconversion detectors (see Section 3.1.), gigahertz modulation rates.

A wider national support for quantum cryptography and quantum information research in Norway is needed. Let me refer to a map that shows locations of research groups in the area of quantum information (Fig. 50). While most other European and Scandinavian countries have multiple groups, we in Trondheim are a lone dot in Norway, and even we are underfunded at the moment.

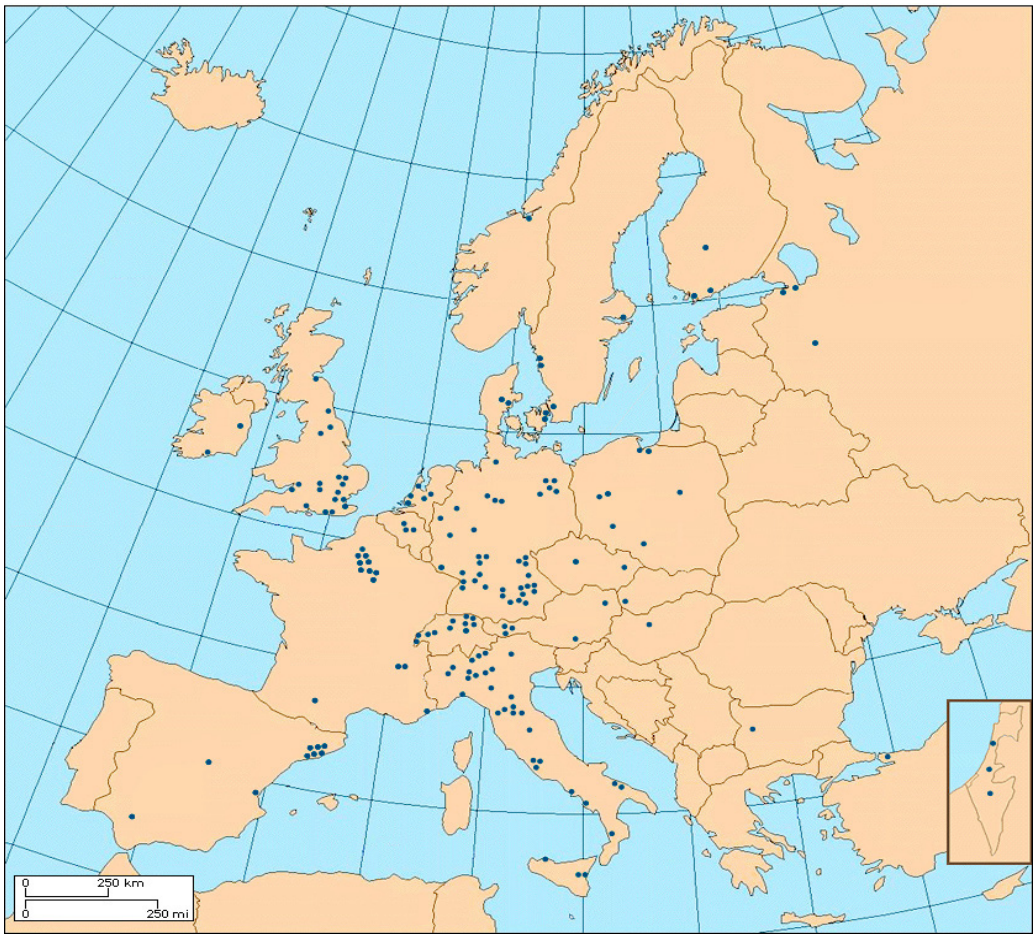


Fig. 50. Cartography of European research groups in quantum information processing and communication, as of August 2006. Each dot represents a registered research group (map taken from member's area of the ERA-Pilot website, http://qist.ect.it/).

Appendix A. Breakdown in lithium niobate phase modulator

As we were finishing the eavesdropping experiment described in Section 4.3.1. ,an electrical breakdown in one of the phase modulators happened.

The breakdown occurred between planar electrodes separated by 8 μm gap in JDS Uniphase UTP PM-130-080 travelling-wave 8 GHz phase modulator (Fig. 51).

While not being of any scientific significance, this mishap stalled the experiments for a long time, because phase modulators for 1300 nm were no longer manufactured. We had to place an order with a different company (Alenia Marconi / Crisel Instruments) for custom-made ones, which cost us a lot and took a long time to deliver.

When we were discussing the replacement order, an Alenia Marconi engineer informed us that they were factory-testing all their phase modulators (which had the electrode gap of a similar width) at over 40 V, and that the breakdown that occurred in our modulator at a lower voltage was probably due to contamination (dust) left inside the package. Indeed, we had to open the hermetically sealed package of the ill-fated modulator previously to "surgically" remove the built-in 50 Ohm terminating resistor. The resistor, as we found out well after the modulator purchase, would have overheated and burned up at our modulation voltages. It was a bad idea anyway to leave the heat-producing resistor inside the modulator package even if it withstood the voltage, because the heat generated would cause a large phase drift in the interferometer.

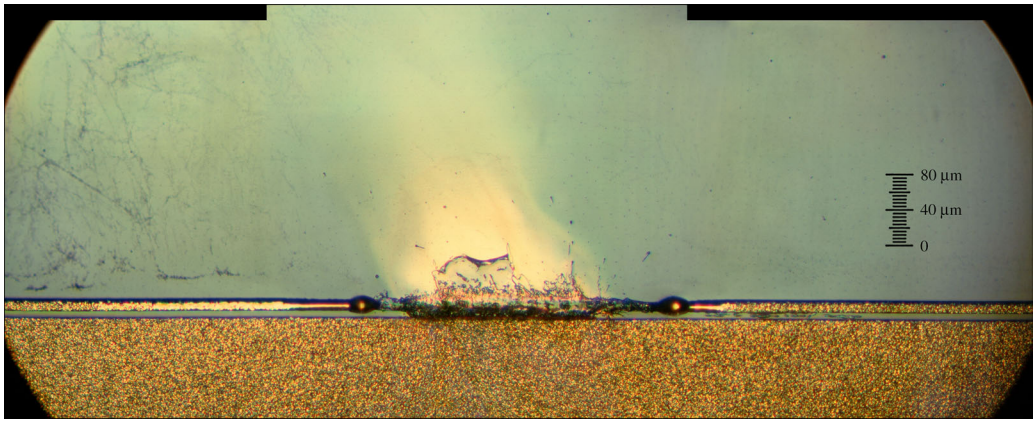


Fig. 51. Microphotograph of the damaged area of the waveguide. The gold electrodes and lithium niobate substrate melted and probably partially evaporated in the arc (the "smoke plume" seen on the photograph is static debris deposited on the crystal surface). Voltage was supplied to the left side of the thin electrode; breakdown occurred at 20 to 30 V, probably assisted by contamination left in the modulator after we had to open its hermetic package. The surface optical waveguide (invisible on this image) made in the crystal somewhere near the electrode gap was also damaged by the discharge: the optical attenuation rose by 10 dB comparing to the normal value.

Appendix B. List of publications

This work has led to five journal publications:

- Vadim Makarov and Johannes Skaar, "Faked states attack using detector efficiency mismatch on SARG04, phase-time, DPSK, and Ekert protocols," quant-ph/0702262; submitted to the Journal of Modern Optics. — reprinted in Section 4.3.3.2.
- Vadim Makarov, Andrey Anisimov, and Johannes Skaar, "Effects of detector efficiency mismatch on security of quantum cryptosystems," Physical Review A **74**, 022313 (2006). — reprinted in Section 4.3.3.2.
- Vadim Makarov and Dag R. Hjelme, "Faked states attack on quantum cryptosystems," Journal of Modern Optics **52**, 691–705 (2005). — reprinted in Section 4.3.3.1.
- Vadim Makarov, Alexei Brylevski, and Dag. R. Hjelme, "Real-time phase tracking in single-photon interferometers," Applied Optics **43**, 4385–4392 (2004). — reprinted in Section 2.3.
- Artem Vakhitov, Vadim Makarov, and Dag R. Hjelme, "Large pulse attack as a method of conventional optical eavesdropping in quantum cryptography," Journal of Modern Optics **48**, 2023–2038 (2001). — reprinted in Section 4.3.1.

Results of this work were timely reported at the following international and national conferences (without publication in proceedings):

- XI International Conference on Quantum Optics in Minsk, Belarus, May 26–31, 2006.
- 1st Quantum Information Theory (QIT) workshop of SECOQC project in Erlangen, Germany, September 13–17, 2004.
- Norwegian Electro-Optics Meeting 2004 in Tønsberg, Norway, May 2–4, 2004 (talk given by B. Vignes).
- Norwegian Cryptographic Seminar 2002 in Trondheim, Norway, October 17–18, 2002.
- Norwegian Electro-Optics Meeting 2002 in Flåm, Norway, May 2–5, 2002, on which the author claimed the *Best poster presentation by a young scientist* award.
- 2nd QIPC Workshop in Turin, Italy, October 28–31, 2001.
- QUICK: Quantum interference and cryptographic keys: novel physics and advancing technologies in Cargese, Corsica, France, April 7–13, 2001.
- 1st QIPC Workshop in Potsdam, September 27–29, 2000.
- Norwegian Electro-Optics Meeting 1999 in Balestrand, Norway, May 6–9, 1999.

Also, the five master theses done by students under the Quantum Cryptography project, this doctoral thesis, our papers and additional materials have been published on the project Web site at http://www.iet.ntnu.no/groups/optics/qcr/

We take the liberty to include group pictures from three of the conferences listed above that the author had the pleasure not only to present his work at, but also to photograph :)


1st QIPC Workshop
Potsdam, September 27-29, 2000

Participants of the QUICK conference. Cargese, Corsica, April 7–13, 2001.

Participants of the XI International Conference on Quantum Optics in Minsk, Belarus, May 26–31, 2006.

References

1. S. Singh, *The Code Book* (Fourth Estate, London, 2000).
2. "History of cryptography," article in Wikipedia (retrieved on 2006-10-27), http://en.wikipedia.org/w/index.php?title=History_of_cryptography&oldid=83652220
3. G. Vernam, "Secret signaling system," U.S. patent No. 1310719 (applied in 1918, granted in 1919).
4. G. Vernam, "Cipher printing telegraph system for secret wire and radio telegraphic communications," J. Am. Institute of Electrical Engineers Vol. XLV, 109–115 (1926).
5. C. Shannon, "Communication theory of secrecy systems," Bell System Technical J. **28**, 656–715 (1949).
6. W. Stallings, *Cryptography and network security: principles and practice* (Prentice Hall, 3rd edition, 2003).
7. R.L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," Comm. ACM **21**, 120–126 (1978).
8. P.W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," SIAM J. Comput. **26**, 1484–1509 (1997); the first version of this paper appeared in *Proceedings of the 35th Symposium on Foundations of Computer Science* (IEEE Computer Society Press, 1994), pp. 124–134.
9. L.M.K. Vandersypen, M. Steffen, G. Breyta, C.S. Yannoni, M.H. Sherwood, and I.L. Chuang, "Experimental realization of Shor's quantum factoring algorithm using nuclear magnetic resonance," Nature **414**, 883–887 (2001).
10. W.K. Wootters and W.H. Zurek, "A single quantum cannot be cloned," Nature **299**, 802–803 (1982).
11. S. Wiesner, "Conjugate coding," Sigact News **15,** 78–88 (1983). Manuscript written circa 1970 but unpublished until 1983.
12. A. Peres, "How the no-cloning theorem got its name," quant-ph/0205076.
13. C. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," in *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing* (Institute of Electrical and Electronics Engineers, New York, 1984), pp. 175–179.
14. C. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, "Experimental quantum cryptography," J. Cryptology **5,** 3–28 (1992).
15. M. Wegman and J. Carter, "New hash functions and their use in authentication and set equality," J. Comp. Syst. Sci. **22**, 265–279 (1981).
16. N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," Rev. Mod. Phys. **74,** 145–195 (2002).
17. A. Muller, J. Breguet, and N. Gisin, "Experimental demonstration of quantum cryptography using polarized photons in optical fiber over more than 1 km," Europhysics Lett. **23**, 383–388 (1993).
18. A. Muller, H. Zbinden, and N. Gisin, "Quantum cryptography over 23 km in installed under-lake telecom fibre," Europhysics Lett. **33**, 335–339 (1996).

19. C.H. Bennett, G. Brassard, and A.K. Ekert, “Quantum cryptography,” Scientific American (October 1992), pp. 26–33.
20. W. Tittel, G. Ribordy, and N. Gisin, “Quantum cryptography,” Physics World, March 1998, pp. 41–45.
21. G.P. Collins, “Quantum cryptography defies eavesdropping,” Physics Today (November 1992), pp. 21–23.
22. J. Breguet, A. Muller, and N. Gisin, “Quantum cryptography with polarized photons in optical fibers: experimental and practical limits,” J. Mod. Opt. **41**, 2405–2412 (1994).
23. A. Muller, H. Zbinden, and N. Gisin, “Underwater quantum coding,” Nature **378**, 449–449 (1995).
24. C. Marand and P. Townsend, “Quantum key distribution over distances as long as 30 km,” Opt. Lett., **20,** 1695–1697 (1995).
25. P.D. Townsend, “Simultaneous quantum cryptographic key distribution and conventional data transmission over installed fibre using wavelength-division multiplexing,” Electronics Lett. **33**, 188–190 (1997).
26. P.D. Townsend, “Quantum cryptography on multiuser optical fibre networks,” Nature **385**, 47–49 (1997).
27. P.D. Townsend, “Quantum cryptography on optical fiber networks,” Opt. Fiber Tech. **4**, 345–370 (1998).
28. R. Hughes, G. Morgan, and C. Peterson, “Practical quantum key distribution over a 48-km optical fiber network,” J. Mod. Opt. **47,** 533–547 (2000).
29. P.A. Hiskett, G. Bonfrate, G.S. Buller, and P.D. Townsend, “Eighty kilometre transmission experiment using an InGaAs/InP SPAD-based quantum cryptography receiver operating at 1.55 μm,” J. Mod. Opt. **48**, 1957–1966 (2001).
30. T. Kimura, Y. Nambu, T. Hatanaka, A. Tomita, H. Kosaka, and K. Nakamura, “Single-photon interference over 150km transmission using silica-based integrated-optic interferometers for quantum cryptography,” Jpn. J. Appl. Phys. **43**, L1217–L1219 (2004).
31. C. Gobby, Z. Yuan, and A. Shields, “Quantum key distribution over 122 km of standard telecom fiber,” Appl. Phys. Lett. **84**, 3762–3764 (2004).
32. H. Takesue, E. Diamanti, T. Honjo, C. Langrock, M.M. Fejer, K. Inoue, and Y. Yamamoto, “Differential phase shift quantum key distribution experiment over 105km fibre,” New J. Phys. **7**, 232 (2005).
33. P.A. Hiskett, D. Rosenberg, C.G. Peterson, R.J. Hughes, S. Nam, A.E. Lita, A.J. Miller, and J.E. Nordholt, “Long-distance quantum key distribution in optical fibre,” New J. Phys. **8**, 193 (2006).
34. B.C. Jakobs and J.D. Franson, “Quantum cryptography in free space,” Opt. Lett. **21**, 1854–1856 (1996).
35. W.T. Buttler, R.J. Hughes, P.G. Kwiat, S.K. Lamoreaux, G.G. Luther, G.L. Morgan, J.E. Nordholt, C.G. Peterson, and C.M. Simmons, “Practical free-space quantum key distribution over 1 km,” Phys. Rev. Lett. **81**, 3283–3286 (1998).
36. W.T. Buttler, R.J. Hughes, S.K. Lamoreaux, G.L. Morgan, J.E. Nordholt, and C.G. Peterson, “Daylight quantum key distribution over 1.6 km,” Phys. Rev. Lett. **84**, 5652–5655 (2000).

37. R.J. Hughes, W.T. Buttler, P.G. Kwiat, S.K. Lamoreaux, G.L. Morgan, J.E. Nordholt, and C.G. Peterson, "Free-space quantum key distribution in daylight," J. Mod. Opt. **47**, 549–562 (2000).
38. J.G. Rarity, P.M. Gorman, and P.R. Tapster, "Secure key exchange over 1.9 km free-space range using quantum cryptography," Electronics Lett. **37**, 512–514 (2001).
39. R.J. Hughes, J.E. Nordholt, D. Derkacs, and C.G. Peterson, "Practical free-space quantum key distribution over 10 km in daylight and at night," New J. Phys. **4**, 43 (2002).
40. C. Kurtsiefer, P. Zarda, M. Halder, H. Weinfurter, P.M. Gorman, P.R. Tapster, and J.G. Rarity, "A step towards global key distribution," Nature **419**, 450–450 (2002).
41. C. Kurtsiefer, P. Zarda, M. Halder, P.M. Gorman, P.R. Tapster, J.G. Rarity, and H. Weinfurter, "Long distance free space quantum cryptography," Proc. SPIE **4917**, 25–31 (2002).
42. J.G. Rarity, P.R. Tapster, P.M. Gorman, and P. Knight, "Ground to satellite secure key exchange using quantum cryptography," New J. Phys. **4**, 82 (2002).
43. J.L. Duligall, M.S. Godfrey, K.A. Harrison, W.J. Munro, and J.G. Rarity, "Low cost and compact quantum key distribution," New J. Phys. **8**, 249 (2006).
44. H.-J. Briegel, W. Dür, J.I. Cirac, and P. Zoller, "Quantum repeaters: the role of imperfect local operations in quantum communication," Phys. Rev. Lett. **81**, 5932–5935 (1998).
45. L.-M. Duan, M.D. Lukin, J.I. Cirac, and P. Zoller, "Long-distance quantum communication with atomic ensembles and linear optics," Nature **414**, 413–418 (2001).
46. C. Elliott, "Building the quantum network," New J. Phys. **4**, 46 (2002).
47. As of December 2006, one could place an order for a complete quantum cryptosystem with a plug-and-play type optical scheme for QKD paired with VPN classical encryption equipment, with two companies: id Quantique (Geneva, Switzerland, http://www.idquantique.com/) and MagiQ Technologies (Boston, USA, http://www.magiqtech.com/).
48. M. Hack, "Quantum cryptography, it's some kind of MagiQ," interview with Bob Gelfond, CEO of MagiQ Technologies Inc. (retrieved on 2006-12-14), http://hackreport.net/2006/12/13/quantum-cryptography-its-some-kind-of-magiq/
49. http://www.smartquantum.com/
50. G. Ribordy, J. Brendel, J.-D. Gautier, N. Gisin, and H. Zbinden, "Long-distance entanglement-based quantum key distribution," Phys. Rev. A **63,** 012309 (2001).
51. T. Hasegawa, K. Inoue, K. Oda, "Polarization independent frequency conversion by fiber four-wave mixing with a polarization diversity technique," Photonics Technol. Lett. **5**, 947–949 (1993).
52. T. Morioka, K. Mori, and M. Saruwatari, "Ultrafast polarisation-independent optical demultiplexer using optical carrier frequency shift through crossphase modulation," Electronics Lett. **28**, 1070–1072 (1992).
53. Y. Nambu, K. Yoshino, A. Tomita, "One-way quantum key distribution system based on planar lightwave circuits," quant-ph/0603041.
54. G. Bonfrate, "Integrated optics for practical quantum cryptography systems," presented at the 2nd QIPC Workshop in Turin, Italy, 28–31 Oct. 2001.

55. A. Trifonov, A. Zavriyev, D. Subacius, R. Alléaume, J.-F. Roch, “Practical quantum cryptography,” in *Quantum Information and Computation II Orlando, Florida, USA, 2004,* E. Donkor, A.R. Pirich, and H.E. Brandt, eds., Proc. SPIE **5436** (SPIE, Bellingham, WA, 2004), pp. 1–11.
56. P. Townsend, J. Rarity, and P. Tapster “Single photon interference in 10 km long optical fibre interferometer,” Electronics Lett. **29**, 634–635 (1993).
57. C. Elliott, D. Pearson, and G. Troxel, “Quantum cryptography in practice,” in *Proceedings of the 2003 conference on Applications, technologies, architectures, and protocols for computer communications* (ACM Press, New York, NY, USA, 2003), pp. 227–238; quant-ph/0307049.
58. A. Muller, T. Herzog, B. Huttner, W. Tittel, H. Zbinden, and N. Gisin, “"Plug and play" systems for quantum cryptography,” Appl. Phys. Lett. **70**, 793–795 (1997).
59. M. Martinelli, “A universal compensator for polarization changes induced by birefringence on a retracting beam,” Opt. Commun. **72,** 341–344 (1989).
60. M. Martinelli, “Time reversal for the polarization state in optical systems,” J. Mod. Opt. **39,** 451–455 (1992).
61. C.H. Bennett, “Quantum cryptography using any two nonorthogonal states,” Phys. Rev. Lett. **68**, 3121–3124 (1992).
62. G. Ribordy, J.-D. Gautier, N. Gisin, O. Guinnard, and H. Zbinden, “Fast and user-friendly quantum key distribution,” J. Mod. Opt. **47**, 517–531 (2000).
63. D. Stucki, N. Gisin, O. Guinnard, G. Ribordy, and H. Zbinden, “Quantum key distribution over 67 km with a plug&play system,” New J. Phys. **4,** 41.1–41.8 (2002).
64. V. Scarani, A. Acin, G. Ribordy, and N. Gisin, “Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulses implementations,” Phys. Rev. Lett. **92**, 057901 (2004); quant-ph/0211131 v4.
65. A. Acin, N. Gisin, and V. Scarani, “Coherent-pulse implementations of quantum cryptography protocols resistant to photon-number-splitting attacks,” Phys. Rev. A **69**, 012309 (2004); quant-ph/0302037.
66. C. Branciard, N. Gisin, B. Kraus, and V. Scarani, “Security of two quantum cryptography protocols using the same four qubit states,” Phys. Rev. A **72**, 032301 (2005).
67. M. Bourennane, F. Gibson, A. Karlsson, A. Hening, P. Jonsson, T. Tsegaye, D. Ljunggren, and E. Sundberg, “Experiments on long wavelength (1550 nm) "plug and play" quantum cryptography systems,” Opt. Express **4**, 383–387 (1999).
68. M. Bourennane, D. Ljunggren, A. Karlsson, P. Jonsson, A. Hening, and J.P. Ciscar, “Experimental long wavelength quantum cryptography: from single-photon transmission to key extraction protocols,” J. Mod. Opt. **47**, 563–579 (2000).
69. P.M. Nielsen, C. Schori, J.L. Sørensen, L. Salvail, I. Damgård, and E. Polzik, “Experimental quantum key distribution with proven security against realistic attacks,” J. Mod. Opt. **48**, 1921–1942 (2001).

70. V. Kurochkin, A. Zverev, Y. Kurochkin, I. Ryabtsev, I. Neizvestny, S. Moon, B. Bae, H. Shin, J. Park, and C. Park, "Experimental quantum cryptography for standard telecom fibers and free space," unpublished (talk presented at the XI International Conference on Quantum Optics in Minsk, Belarus, May 26–31, 2006).
71. A. Trifonov, "Secure quantum communication for optical networking," unpublished (talk presented at the XI International Conference on Quantum Optics in Minsk, Belarus, May 26–31, 2006).
72. J.-M. Mérolla, Yu. Mazurenko, J.-P. Goedgebuer, and W.T. Rhodes, "Single-photon interference in sidebands of phase-modulated light for quantum cryptography," Phys. Rev. Lett. **82**, 1656–1659 (1999).
73. Y. Nambu, T. Hatanaka, and K. Nakamura, "BB84 quantum key distribution system based on silica-based planar lightwave circuits," Jpn. J. Appl. Phys. **43**, L1109–L1110 (2004).
74. K. Inoue, E. Waks, and Y. Yamamoto, "Differential phase shift quantum key distribution," Phys. Rev. Lett. **89**, 037902 (2002).
75. W.T. Buttler, J.R. Torgerson, and S.K. Lamoreaux, "New, efficient and robust, fiber-based quantum key distribution schemes," Phys. Lett. A **299**, 38–42 (2002).
76. W. Tittel, J. Brendel, H. Zbinden, and N. Gisin, "Quantum cryptography using entangled photons in energy-time Bell states," Phys. Rev. Lett. **84,** 4737–4740 (2000).
77. T. Jennewein, C. Simon, G. Weihs, H. Weinfurter, and A. Zeilinger, "Quantum cryptography with entangled photons," Phys. Rev. Lett. **84,** 4729–4732 (2000).
78. D.S. Naik, C.G. Peterson, A.G. White, A.J. Berglund, and P.G. Kwiat, "Entangled state quantum cryptography: eavesdropping on the Ekert protocol," Phys. Rev. Lett. **84,** 4733–4736 (2000).
79. H.-K. Lo and J. Preskill, "Phase randomization improves the security of quantum key distribution," quant-ph/0504209.
80. C. Poole, R. Tkach, A. Chraplyvy, and D. Fishman, "Fading in lightwave systems due to polarization-mode dispersion," IEEE Photon. Tech. Lett. **3**, 68–70 (1991).
81. S. Bjørnstad, M. Nord, and D.R. Hjelme, "Transparent optical protection switching scheme based on detection of polarisation fluctuations," in *Proceedings of the Optical Fiber Communication conference OFC2002,* 433–434 (2002).
82. T. Okoshi, "Polarization-state control schemes for heterodyne or homodyne optical fiber communications," J. Lightwave Tech. **LT-3**, 1232–1237 (1985).
83. A. Brylevski, "Quantum key distribution: Real-time compensation of interferometer phase drift," master thesis (done at Department of Physical Electronics, Norwegian University of Science and Technology, and defended at Radiophysics Department, St. Petersburg State Technical University, 2002), http://www.iet.ntnu.no/groups/optics/qcr/alexey/
84. M. Chizhov, "Quantum cryptography systems," master thesis (done at Department of Electronics and Telecommunications, Norwegian University of Science and Technology, and defended at Radiophysics Department, St. Petersburg State Polytechnic University, 2004), http://www.iet.ntnu.no/groups/optics/qcr/chizhov-2004/

85. A. Yoshizawa, R. Kaji, and H. Tsuchida, “A method of discarding after-pulses in single-photon detection for quantum key distribution,” Jpn. J. Appl. Phys. **41**, 6016–6017 (2002).
86. The threshold value of QBER is still being discussed. Most of the recent strict security analyses, however, put it at 11%. For review, see for example [16, 87] and references thereof.
87. M. Bourenanne, A. Karlsson, G. Bjork, N. Gisin, and N. J Cerf, “Quantum key distribution using multilevel encoding: security analysis,” J. Phys. A: Math. Gen. **35,** 10065–10076 (2002).
88. H. Zbinden, J. D. Gautier, N. Gisin, B. Huttner, A. Muller, and W. Tittel, “Interferometry with Faraday mirrors for quantum cryptography,” Electr. Letters **33,** 586–588 (1997).
89. A. Vakhitov, V. Makarov, and D. R. Hjelme, “Large pulse attack as a method of conventional optical eavesdropping in quantum cryptography,” J. Mod. Opt. **48,** 2023–2038 (2001); reprinted in Section 4.3.1.
90. G. Ribordy, J-D. Gautier, N. Gisin, O. Guinnard, and H. Zbinden, “Automated “plug & play” quantum key distribution,” Electr. Letters **34,** 2116–2117 (1998).
91. W. Tittel, J. Brendel, N. Gisin, and H. Zbinden, “Long-distance Bell-type tests using energy-time entangled photons,” Phys. Rev. A **59,** 4150–4163 (1999).
92. Hugo Zbinden, Université de Genève, Group of Applied Physics (GAP)-Optique, Rue de l’École-de-Médecine 20, CH-1211 Genève 4, Suisse / Switzerland (personal communication, 2001).
93. S. Pellegrini, “EQUIS Project” (retrieved on 2005-09-01), http://www.phy.hw.ac.uk/resrev/EQUIS/, see page “WP4 — Integrated Mach-Zehnder / Michelson interferometer”.
94. P. Townsend, J. Rarity, and P. Tapster, “Enhanced single photon fringe visibility in a 10 km-long prototype quantum cryptography channel,” Electronics Lett. **29,** 1291–1293 (1993).
95. K. Vylegjanine, “ High-speed single photon detector for quantum cryptosystems,” master thesis (done at Department of Physical Electronics, Norwegian University of Science and Technology, and defended at Radiophysics Department, St. Petersburg State Technical University, 2000), http://www.iet.ntnu.no/groups/optics/qcr/kirill/
96. S. Hecht, S. Shlaer, and M.H. Pirenne, “Energy, quanta, and vision,” J. Gen. Physiol. **25**, 819–840 (1942).
97. W. Bialek, lecture notes for Biophysics course (2006) (retrieved in August 2006), http://www.princeton.edu/~wbialek/PHY562/PHY562_home.html
98. A.-C. Aho, K. Donner, C. Hydén, L.O. Larsen, and T. Reuter, “Low retinal noise in animals with low body temperature allows high visual sensitivity,” Nature **334**, 348–350 (1988).
99. D.A. Baylor, G. Matthews, and K.-W. Yau, “Two components of electrical dark noise in toad retinal rod outer segments,” J. Physiol. **309**, 591–621 (1980).
100. F. Rieke and D.A. Baylor, “Molecular origin of continuous dark noise in rod photoreceptors,” Biophys. J. **71**, 2553–2572 (1996).
101. D.A. Baylor, B.J. Nunn, and J.F. Schnapf, “The photocurrent, noise and spectral sensitivity of rods of the monkey *Macaca fascicularis*,” J. Physiol. **357**, 575–607 (1984).

102. M.C. Teich, P.R. Prucnal, G. Vannucci, M.E. Breton, and W.J. McGill, "Multiplication noise in the human visual system at threshold. 3: The role of non-Poisson quantum fluctuations," Biol. Cybern. **44**, 157–165 (1982).
103. G.L. Locher, "Photoelectric quantum counters for visible and ultraviolet light. Part I," Phys. Rev. **42**, 525–546 (1932).
104. A.T. Krebs, "Early history of the scintillation counter," Science **122**, 17–18 (1955).
105. *Photomultiplier handbook* (Burle Technologies, Inc., 1980), available as of 2006 at http://www.burle.com/cgi-bin/byteserver.pl/pdf/Photo.pdf
106. *Photomultiplier tubes: Basics and applications* (Hamamatsu Photonics K. K., 2006), http://sales.hamamatsu.com/assets/applications/ETD/pmt_handbook/pmt_handbook_complete.pdf
107. Hamamatsu near infrared photomultiplier tube R5509-73 data sheet (2006), http://jp.hamamatsu.com/products/node.do?dir=/division/etd/pd001/pd002/pd394/R5509-73&lang=en&ext=html
108. S. Cova, M. Ghioni, A. Lotito, I. Rech, and F. Zappa, "Evolution and prospects for single-photon avalanche diodes and quenching circuits," J. Mod. Opt. **51**, 1267–1288 (2004).
109. A. Goetzberger, B. McDonald, R.H. Haitz, and R.M. Scarlett, "Avalanche effects in silicon p–n junctions. II. Structurally perfect junctions," J. Appl. Phys. **34**, 1591–1600 (1963).
110. R.H. Haitz, "Mechanisms contributing to the noise pulse rate of avalanche diodes," J. Appl. Phys. **36**, 3123–3131 (1965).
111. R.J. McIntyre, "The distribution of gains in uniformly multiplying avalanche photodiodes: Theory," IEEE Trans. Electron Devices **Ed-19**, 703–713 (1972).
112. A. Lacaita, P.A. Francese, F. Zappa, and S. Cova, "Single-photon detection beyond 1 μm: performance of commercially available germanium photodiodes," Appl. Opt. **33**, 6902–6918 (1994).
113. S. Cova, M. Ghioni, A. Lacaita, C. Samori, and F. Zappa, "Avalanche photodiodes and quenching circuits for single-photon detection," Appl. Opt. **35**, 1956–1976 (1996).
114. H. Dautet, P. Deschamps, B. Dion, A.D. MacGregor, D. MacSween, R.J. McIntyre, C. Trottier, and P.P. Webb, "Photon counting techniques with silicon avalanche photodiodes," Appl. Opt. **32**, 3894–3900 (1993).
115. M. Akiba, M. Fujiwara, and M. Sasaki, "Ultrahigh-sensitivity high-linearity photodetection system using a low-gain avalanche photodiode with an ultralow-noise readout circuit," Opt. Lett. **30**, 123–125 (2005).
116. M. Akiba and M. Fujiwara, "Ultralow-noise near-infrared detection system with a Si p–i–n photodiode," Opt. Lett. **28**, 1010–1012 (2003).
117. P.G. Kwiat, A.M. Steinberg, R.Y. Chiao, P.H. Eberhard, and M.D. Petroff, "High-efficiency single-photon detectors," Phys. Rev. A **48**, R867–R870 (1993).
118. SPCM-AQR single photon counting module data sheet, PerkinElmer Optoelectronics (2006), http://optoelectronics.perkinelmer.com/content/Datasheets/SPCM-AQR.pdf
119. P.C.M. Owens, J.G. Rarity, P.R Tapster, D. Knight, and P.D. Townsend, "Photon counting with passively quenched germanium avalanche," Appl. Opt. **33**, 6895–6901 (1994).

120. B.F. Levine and C.G. Bethea, “Single photon detection at 1.3 μm using a gated avalanche photodiode,” Appl. Phys. Lett. **44**, 553–555 (1984).
121. A. Lacaita, F. Zappa, S. Cova, and P. Lovati, “Single-photon detection beyond 1 μm: performance of commercially available InGaAs/InP detectors,” Appl. Opt. **35**, 2986–2996 (1996).
122. B.F. Levine, C.G. Bethea, and J.C. Campbell, “Near room temperature 1.3 μm single photon counting with a InGaAs avalanche photodiode,” Electronics Lett. **20**, 596–598 (1984).
123. G. Ribordy, J.-D. Gautier, H. Zbinden, and N. Gisin, “Performance of InGaAs/InP avalanche photodiodes as gated-mode photon counters,” Appl. Opt. **37**, 2272–2277 (1998).
124. D. Stucki, G. Ribordy, A. Stefanov, H. Zbinden, J.G. Rarity, and T. Wall, “Photon counting for quantum key distribution with Peltier cooled InGaAs/InP APDs,” J. Mod. Opt. **48**, 1967–1981 (2001).
125. M. Bourennane, A. Karlsson, J.P. Ciscar, and M. Mathés, “Single-photon counters in the telecom wavelength region of 1550 nm for quantum information processing,” J. Mod. Opt. **48**, 1983–1995 (2001).
126. D.S. Bethune, W.P. Risk, and G.W. Pabst, “A high-performance integrated single-photon detector for telecom wavelengths,” J. Mod. Opt. **51**, 1359–1368 (2004).
127. G. Ribordy, N. Gisin, O. Guinnard, D. Stucky, M. Wegmuller, and H. Zbinden, “Photon counting at telecom wavelengths with commercial InGaAs/InP avalanche photodiodes: current performance,” J. Mod. Opt. **51**, 1381–1398 (2004).
128. A. Trifonov, D. Subacius, A. Berzanskis, and A. Zavriyev, “Single photon counting at telecom wavelength and quantum key distribution,” J. Mod. Opt. **51**, 1399–1415 (2004).
129. M.A. Albota and E. Dauler, “Single photon detection of degenerate photon pairs at 1.55 μm from a periodically poled lithium niobate parametric downconverter,” J. Mod. Opt. **51**, 1417–1432 (2004).
130. id200 single photon detection module (2006), http://www.idquantique.com/
131. S. Pellegrini, R.E. Warburton, L.J.J. Tan, J.S. Ng, A.B. Krysa, K. Groom, J.P.R. David, S. Cova, M.J. Robertson, and G.S. Buller, “Design and performance of an InGaAs–InP single-photon avalanche diode detector,” IEEE J. Quantum Electron. **42**, 397–403 (2006).
132. M.D. Petroff, M.G. Stapelbroek, and W.A. Kleinhans, “Detection of individual 0.4–28 μm wavelength photons via impurity-impact ionization in a solid-state photomultiplier,” Appl. Phys. Lett. **51**, 406–408 (1987).
133. E. Waks, K. Inoue, W.D. Oliver, E. Diamanti, and Y. Yamamoto, “High-efficiency photon-number detection for quantum information processing,” IEEE J. Sel. Top. Quantum Electron. **9**, 1502–1511 (2003).
134. J. Kim, Y. Yamamoto, and H.H. Hogue, “Noise-free avalanche multiplication in Si solid state photomultipliers,” Appl. Phys. Lett. **70**, 2852–2854 (1997).
135. J. Kim, S. Takeuchi, Y. Yamamoto, and H.H. Hogue, “Multiphoton detection using visible light photon counter,” Appl. Phys. Lett. **74**, 902–904 (1999).
136. S. Takeuchi, J. Kim, Y. Yamamoto, and H.H. Hogue, “Development of a high-quantum-efficiency single-photon counting system,” Appl. Phys. Lett. **74**, 1063–1065 (1999).

137. 16PT-ADR cryogen free two stage adiabatic demagnetization refrigerator system, Janis Research Company, Inc. (2006), http://www.janis.com/p-adr3.html; this cooling equipment weighs slightly over 200 kg.
138. A. Peacock, P. Verhoeve, N. Rando, A. van Dordrecht, B.G. Taylor, C. Erd, M.A.C. Perryman, R. Venn, J. Howlett, D.J. Goldie, J. Lumley, and M. Wallis, "Single optical photon detection with a superconducting tunnel junction," Nature **381**, 135–137 (1996).
139. P. Verhoeve, N. Rando, A. Peacock, A. van Dordrecht, and A. Poelaert, "Superconducting tunnel junctions as photon counting detectors in the infrared to the ultraviolet," IEEE Trans. Appl. Supercond. **7**, 3359–3362 (1997).
140. C.A. Mears, S.E. Labov, and A.T. Batfknecht, "Energy-resolving superconducting x-ray detectors with charge amplification due to multiple quasiparticle tunneling," Appl. Phys. Lett. **63**, 2961–2963 (1993).
141. R.J. Schoelkopf, S.H. Moseley, C.M. Stahle, P. Wahlgren, and P. Delsing, "A concept for a submillimeter-wave single-photon counter," IEEE Trans. Appl. Supercond. **9**, 2935–2939 (1999).
142. O. Astafiev, S. Komiyama, T. Kutsuwa, V. Antonov, Y. Kawaguchi, and K. Hirakawa, "Single-photon detector in the microwave range," Appl. Phys. Lett. **80**, 4250–4252 (2002).
143. J.H.J. de Bruijne, A.P. Reynolds, M.A.C. Perryman, F. Favata, and A. Peacock, "Analysis of astronomical data from optical superconducting tunnel junctions," Opt. Eng. **41**, 1158–1169 (2002).
144. B. Cabrera, R.M. Clarke, P. Colling, A.J. Miller, S. Nam, and R.W. Romani, "Detection of single infrared, optical, and ultraviolet photons using superconducting transition edge sensors," Appl. Phys. Lett. **73**, 735–737 (1998).
145. A.J. Miller, S.W. Nam, J.M. Martinis, and A.V. Sergienko, "Demonstration of a low-noise near-infrared photon counter with multiphoton discrimination," Appl. Phys. Lett. **83**, 791–793 (2003).
146. D. Rosenberg, A.E. Lita, A.J. Miller, S. Nam, and R.E. Schwall, "Performance of photon-number resolving transition-edge sensors with integrated 1550 nm resonant cavities," IEEE Trans. Appl. Supercond. **15**, 575–578 (2005).
147. D. Rosenberg, A.E. Lita, A.J. Miller, and S.W. Nam, "Noise-free high-efficiency photon-number-resolving detectors," Phys. Rev. A **71**, 061803(R) (2005).
148. A.D. Semenov, G.N. Gol'tsman, and A.A. Korneev, "Quantum detection by current carrying superconducting film," Physica C **351**, 349–356 (2001).
149. G.N. Gol'tsman, O. Okunev, G. Chulkova, A. Lipatov, A. Semenov, K. Smirnov, B. Voronov, A. Dzardanov, C. Williams, and R. Sobolewski, "Picosecond superconducting single-photon optical detector," Appl. Phys. Lett. **79**, 705–707 (2001).
150. A. Verevkin, A. Pearlman, W. Słysz, J. Zhang, M. Currie, A. Korneev, G. Chulkova, O. Okunev, P. Kouminov, K. Smirnov, B. Voronov, G.N. Gol'tsman, and R. Sobolewski, "Ultrafast superconducting single-photon detectors for near-infrared-wavelength quantum communications," J. Mod. Opt. **51**, 1447–1458 (2004).
151. R. Sobolewski, A. Verevkin, G.N. Gol'tsman, A. Lipatov, and K. Wilsher, "Ultrafast superconducting single-photon optical detectors and their applications," IEEE Trans. Appl. Supercond. **13**, 1151–1157 (2003).

152. A. Korneev, P. Kouminov, V. Matvienko, G. Chulkova, K. Smirnov, B. Voronov, G.N. Gol'tsman, M. Currie, W. Lo, K. Wilsher, J. Zhang, W. Słysz, A. Pearlman, A. Verevkin, and R. Sobolewski, "Sensitivity and gigahertz counting performance of NbN superconducting single-photon detectors," Appl. Phys. Lett. **84**, 5338–5340 (2004).
153. K.M. Rosfjord, J.K.W. Yang, E.A. Dauler, A.J. Kerman, V. Anant, B.M. Voronov, G.N. Gol'tsman, and K.K. Berggren, "Nanowire single-photon detector with an integrated optical cavity and anti-reflection coating," Opt. Express **14**, 527–534 (2006).
154. R.H. Hadfield, M.J. Stevens, S.S. Gruber, A.J. Miller, R.E. Schwall, R.P. Mirin, and S.W. Nam, "Single photon source characterization with a superconducting single photon detector," Opt. Express **13**, 10846–10853 (2005).
155. A. Engel, A. Semenov, H.-W. Hübers, K. Il'in, and M. Siegel, "Superconducting single-photon detector for the visible and infrared spectral range," J. Mod. Opt. **51**, 1459–1466 (2004).
156. J.E. Midwinter and J. Warner, "Up-conversion of near infrared to visible radiation in lithium-meta-niobate," J. Appl. Phys. **38**, 519–523 (1967).
157. C. Langrock, E. Diamanti, R.V. Roussev, Y. Yamamoto, and M.M. Fejer, "Highly efficient single-photon detection at communication wavelengths by use of upconversion in reverse-proton-exchanged periodically poled $LiNbO_3$ waveguides," Opt. Lett. **30**, 1725–1727 (2005).
158. E. Diamanti, H. Takesue, T. Honjo, K. Inoue, and Y. Yamamoto, "Performance of various quantum-key-distribution systems using 1.55-μm up-conversion single-photon detectors," Phys. Rev. A **72**, 052311 (2005).
159. R.T. Thew, S. Tanzilli, L. Krainer, S.C. Zeller, A. Rochas, I. Rech, S. Cova, H. Zbinden, and N. Gisin, "Low jitter up-conversion detectors for telecom wavelength GHz QKD," New J. Phys. **8**, 32 (2006).
160. S. Tanzilli, W. Tittel, M. Halder, O. Alibart, P. Baldi, N. Gisin, and H. Zbinden, "A photonic quantum information interface," Nature **437**, 116–120 (2005).
161. A.P. Vandevender and P.G. Kwiat, "High efficiency single photon detection via frequency up-conversion," J. Mod. Opt. **51**, 1433–1445 (2004).
162. Y.-H. Kim, S.P. Kulik, and Y. Shih, "Quantum teleportation of a polarization state with a complete Bell state measurement," Phys. Rev. Lett. **86**, 1370–1373 (2001).
163. D. Achilles, C. Silberhorn, C. Śliwa, K. Banaszek, I.A. Walmsley, M.J. Fitch, B.C. Jakobs, T.B. Pittman, and J.D. Franson, "Photon-number-resolving detection using time-multiplexing," J. Mod. Opt. **51**, 1499–1515 (2004).
164. H. Kosaka, A. Tomita, Y. Nambu, T. Kimura, and K. Nakamura, "Single-photon interference experiment over 100 km for quantum cryptography system using balanced gated-mode photon detector," Electronics Lett. **39**, 1199–1201 (2003).
165. A. Tomita and K. Nakamura, "A balanced gated-mode photon detector for qubit discrimination in 1550 nm," quant-ph/0206150.
166. D. Rosenberg, S.W. Nam, P.A. Hiskett, C.G. Peterson, R.J. Hughes, J.E. Nordholt, A.E. Lita, and A.J. Miller, "Quantum key distribution at telecom wavelengths with noise-free detectors," Appl. Phys. Lett. **88**, 021108 (2006).

167. A. Gulian, K. Wood, G. Fritz, A. Gyulamiryan, V. Nikogosyan, N. Giordano, T. Jacobs, and D. Van Vechten, "X-ray/UV single photon detectors with isotropic Seebeck sensors," NIMA **444**, 232–236 (2000).
168. A. Gulian, K. Wood, D. Van Vechten, and G. Fritz, "Cryogenic thermoelectric (QVD) detectors: Emerging technique for fast single-photon counting and non-dispersive energy characterization," J. Mod. Opt. **51**, 1467–1490 (2004).
169. A.J. Shields, M.P. O'Sullivan, I. Farrer, D.A. Ritchie, R.A. Hogg, M.L. Leadbeater, C.E. Norman, and M. Pepper, "Detection of single photons using a field-effect transistor gated by a layer of quantum dots," Appl. Phys. Lett. **76**, 3673–3675 (2000).
170. A. Yoshizawa, R. Kaji, and H. Tsuchida, "Gated-mode single-photon detection at 1550 nm by discharge pulse counting," Appl. Phys. Lett. **84**, 3606–3608 (2004).
171. S. Cova, A. Longoni, and A. Andreoni, "Towards picosecond resolution with single-photon avalanche diodes," Rev. Sci. Instrum. **52**, 408–412 (1981).
172. N.S. Nightingale, "A new silicon avalanche photodiode photon counting detector module for astronomy," Exp. Astron. **1**, 407–422 (1991).
173. D.S. Bethune, R.G. Devoe, C. Kurtsiefer, C.T. Rettner, and W.P. Risk, "System for gated detection of optical pulses containing a small number of photons using an avalanche photodiode," U.S. Patent No. 6,218,657 (filed in 1998, granted in 2001).
174. D.S. Bethune and W.P. Risk, "An autocompensating fiber-optic quantum cryptography system based on polarization splitting of light," IEEE J. Quantum Electron. **36**, 340–347 (2000).
175. A. Yoshizawa, R. Kaji, and H. Tsuchida, "10.5 km fiber-optic quantum key distribution at 1550 nm with a key rate of 45 kHz," Jap. J. Appl. Phys. **43**, L735–L737 (2004).
176. P.L. Voss, K.G. Köprülü, S.-K. Choi, S. Dugan, and P. Kumar, "14 MHz rate photon counting with room temperature InGaAs/InP avalanche photodiodes," J. Mod. Opt. **51**, 1369–1379 (2004).
177. T. Nesheim, "Single photon detection using avalanche photodiode," master thesis (Department of Physical Electronics, Norwegian University of Science and Technology, 1999), http://www.iet.ntnu.no/groups/optics/qcr/torbjoern/
178. S. Cova, A. Lacaita, and G. Ripamonti, "Trapping phenomena in avalanche photodiodes on nanosecond scale," IEEE Electron Dev. Lett. **12**, 685–687 (1991).
179. A. Anisimov, "Avalanche photodiode-based single photon detectors for infrared radiation," PhD thesis (Radiophysics Department, St. Petersburg State Polytechnic University, 2005).
180. A. Yoshizawa, R. Kaji, and H. Tsuchida, "After-pulse-discarding in single-photon detection to reduce bit errors in quantum key distribution," Opt. Express **11**, 1303–1309 (2003).
181. J.M. Smith, P.A. Hiskett, I. Gontijo, L. Purves, and G.S. Buller, "A picosecond time-resolved photoluminescence microscope with detection at wavelengths greater than 1500 nm," Rev. Sci. Instr. **72**, 2325–2329 (2001).
182. Jason M. Smith, Department of Materials, University of Oxford, Parks Road, Oxford OX1 3PH, UK (personal communication, 2004).
183. N. Lutkenhaus, "Estimates for practical quantum cryptography," Phys. Rev. A **59,** 3301–3319 (1999).

184. MagiQ Technologies, http://www.magiqtech.com/, see information on the QPN Security Gateway (as of May 2006). Their commercial quantum cryptography system was first introduced in November 2003 under the name "Navajo".
185. G. Zeng, "Trojan horse attacking strategy on quantum cryptography," Quantum Computers and Computing **4,** 15–23 (2003).
186. J. Larsson, "A practical Trojan horse for Bell-inequality-based quantum cryptography," Quant. Inf. Comput. **2,** 434–442 (2002).
187. A. Ekert, "Quantum cryptography based on Bell's theorem," Phys. Rev. Lett. **67**, 661–663 (1991).
188. B. Schneier, "Crypto-Gram newsletter" from December 15, 2003, http://www.schneier.com/crypto-gram-0312.html
189. D. Mayers, "Quantum key distribution and string oblivious transfer in noisy channels," in *Advances in Cryptology—Proc. Crypto'96* (Springer-Verlag, New York, 1996); D. Mayers, "Unconditional security in quantum cryptography," J. Assoc. Comput. Mach. **48**, 351–406 (2001).
190. P. Shor and J. Preskill, "Simple proof of security of the BB84 quantum key distribution protocol," Phys. Rev. Lett. **85**, 441–444 (2000).
191. M. Koashi and J. Preskill, "Secure quantum key distribution with an uncharacterized source," Phys. Rev. Lett. **90**, 057902 (2003).
192. E. Biham, M. Boyer, P.O. Boykin, T. Mor, and V. Roychowdhury, "A proof of the security of quantum key distribution," in *Proceedings of the 32nd Annual ACM Symposium on Theory of Computation* (ACM Press, New York, 2000), pp. 715–724.
193. H. Inamori, N. Lutkenhaus, and D. Mayers, "Unconditional security of practical quantum key distribution," quant-ph/0107017.
194. D. Gottesman, H.-K. Lo, N. Lutkenhaus, and J. Preskill, "Security of quantum key distribution with imperfect devices," Quant. Inf. Comput. **4**, 325–360 (2004); quant-ph/0212066.
195. D. Bruβ, "Optimal eavesdropping in quantum cryptography with six states," Phys. Rev. Lett. **81**, 3018–3021 (1998).
196. H. Bechmann-Pasquinucci and N. Gisin, "Incoherent and coherent eavesdropping in the six-state protocol of quantum cryptography," Phys. Rev. A **59**, 4238–4248 (1999).
197. X.-B. Wang, "Decoy-state protocol for quantum cryptography with four different intensities of coherent light," Phys. Rev. A **72**, 012322 (2005).
198. S.J. van Enk and C.A. Fuchs, "The quantum state of a propagating laser field," quant-ph/0111157.
199. B. Huttner, N. Imoto, N. Gisin, and T. Mor, "Quantum cryptography with coherent states," Phys. Rev. A **51**, 1863–1869 (1995).
200. S. Felix, N. Gisin, A. Stefanov, and H. Zbinden, "Faint laser quantum key distribution: eavesdropping exploiting multiphoton pulses," J. Mod. Opt. **48,** 2009–2021 (2001).
201. G. Brassard, N. Lutkenhaus, T. Mor, and B.C. Sanders, "Limitations on Practical Quantum Cryptography," Phys. Rev. Lett. **85,** 1330–1333 (2000).
202. N. Lutkenhaus, "Security against individual attacks for realistic quantum key distribution," Phys. Rev. A **61,** 052304 (2000).

203. N. Lutkenhaus and M. Jahma, "Quantum key distribution with realistic states: photon-number statistics in the photon-number splitting attack," New J. Phys. **4**, 44 (2002).
204. A. Beveratos, R. Brouri, T. Gacoin, A. Villing, J.-P. Poizat, and P. Grangier, "Single photon quantum cryptography," Phys. Rev. Lett. **89**, 187901 (2002).
205. E. Waks, K. Inoue, C. Santori, D. Fattal, J. Vuckovic, G.S. Solomon, and Y. Yamamoto, "Secure communication: Quantum cryptography with a photon turnstile," Nature **420**, 762 (2002).
206. W.-Y. Hwang, "Quantum key distribution with high loss: toward global secure communication," Phys. Rev. Lett. **91**, 057901 (2003).
207. H.-K. Lo, "Quantum key distribution with vacua or dim pulses as decoy states," Proc. of IEEE International Symposium on Information Theory (ISIT) 2004 (2004), p. 137.
208. H.-K. Lo, X. Ma, and K. Chen, "Decoy state quantum key distribution," Phys. Rev. Lett. **94**, 230504 (2005).
209. X.-B. Wang, "Beating the photon-number-splitting attack in practical quantum cryptography," Phys. Rev. Lett. **94**, 230503 (2005).
210. X. Ma, B. Qi, Y. Zhao, and H.-K. Lo, "Practical decoy state for quantum key distribution," Phys. Rev. A **72**, 012326 (2005).
211. Y. Zhao, B. Qi, X. Ma, H.-K. Lo, and L. Qian, "Experimental quantum key distribution with decoy states," quant-ph/0503192.
212. "Trojan horse," article in Wikipedia (retrieved on 2006-04-20), http://en.wikipedia.org/w/index.php?title=Trojan_Horse&oldid=49066323
213. N. Gisin, S. Fasel, B. Kraus, H. Zbinden, and G. Ribordy, "Trojan-horse attacks on quantum-key-distribution systems," Phys. Rev. A **73,** 022320 (2006).
214. M. LaGasse, "Secure use of a single single-photon detector in a QKD system," U.S. patent application No. 20050190922 (applied in 2005). Note: M. LaGasse was with MagiQ Technologies at the time of applying for this patent.
215. W.-H. Kye, C.-M. Kim, M.S. Kim, and Y.-J. Park, "Quantum key distribution with blind polarization bases," Phys. Rev. Lett. **95**, 040501 (2005).
216. M. Lucamarini and S. Mancini, "Secure deterministic communication without entanglement," Phys. Rev. Lett. **94**, 140501 (2005).
217. C.-M. Kim, Y.J. Choi, and Y.-J. Park, "Eavesdropping attack with Hong-Ou-Mandel interferometer and random basis shuffling in quantum key distribution," quant-ph/0603013.
218. S. Kak, "A three-stage quantum cryptography protocol," quant-ph/0503027.
219. See proceedings of the annual Boulder damage symposium, e.g., *Laser-induced damage in optical materials: 2001,* G. Exarhos, A. Guenther, K. Lewis, M. Soileau, C. Stolz, eds., Proc. SPIE **4679** (2002).
220. C. Kurtsiefer, P. Zarda, S. Mayer, and H. Weinfurter, "The breakdown flash of silicon avalanche photodiodes — back door for eavesdropper attacks?" J. Mod. Opt. **48,** 2039–2047 (2001).
221. According to *Corning® SMF-28™ CPC6 single-mode optical fiber,* a product information sheet PL1036 (Corning Incorporated, 1999), the effective group index of refraction (N_{eff}) is 1.4675 at 1310 nm and 1.4681 at 1550 nm, which makes for 0.04% difference in group speed between these wavelengths.
222. Phoenix Photonics, http://www.phoenix-photonics.com/, see Products section.

223. Canadian Instrumentation & Research Ltd., http://www.cirl.com/, see Products section.
224. A. Stefanov, N. Gisin, O. Guinnard, L. Guinnard, and H. Zbinden, "Optical quantum random number generator," quant-ph/9907006.
The generator described in the above paper is commercially available from id Quantique, http://www.idquantique.com/
See also more recent (introduced in March 2004) 'Quantis' quantum random number generator.
225. *Melles Griot product catalog* (Melles Griot, 1999).
226. A. Trifonov, "Single-photon watch dog detector for folded quantum key distribution system," U.S. patent application No. 20040161109 (applied in 2004). Note: A. Trifonov was with MagiQ Technologies at the time of applying for this patent.
227. J.H. Mitchell, H. Vig, J. Young, and A. Trifonov, "Constant modulation for enhancing QKD security," U.S. patent application No. 20060088159 (applied in 2006). Note: A. Trifonov was with MagiQ Technologies at the time of applying for this patent.
228. V. Makarov, J. Skaar, and A. Anisimov. "Faked states attack exploiting detector efficiency mismatch on BB84, phase-time, DPSK, and Ekert protocols" (unpublished), http://www.iet.ntnu.no/groups/optics/qcr/poster-minsk-200605/