ETSI White Paper No. 27

Implementation Security of Quantum Cryptography

Introduction, challenges, solutions

First edition – July 2018

ISBN No. 979-10-92620-21-4

Authors:
Marco Lucamarini, Andrew Shields, Romain Alléaume, Christopher Chunnilall, Ivo Pietro Degiovanni, Marco Gramegna, Atilla Hasekioglu, Bruno Huttner, Rupesh Kumar, Andrew Lord, Norbert Lütkenhaus, Vadim Makarov, Vicente Martin, Alan Mink, Momtchil Peev, Masahide Sasaki, Alastair Sinclair, Tim Spiller, Martin Ward, Catherine White, Zhiliang Yuan

ETSI
06921 Sophia Antipolis CEDEX, France
Tel +33 4 92 94 42 00
info@etsi.org
www.etsi.org

About the authors

Marco Lucamarini
Senior Researcher, Toshiba Research Europe Limited, Cambridge, UK

Marco Lucamarini works on the implementation security of real quantum key distribution (QKD) systems. He has authored more than 50 papers related to protocols, methods and systems for quantum communications. He is a regular contributor to the ETSI Industry Specification Group (ISG) on QKD.

Andrew Shields FREng, FInstP
Assistant Managing Director, Toshiba Research Europe Limited, Cambridge, UK

Andrew Shields leads R&D on quantum technologies at TREL. He was a co-founder of the ETSI ISG on QKD and serves currently as its Chair. He has published over 300 papers in the field of quantum photonics, which have been cited over 15000 times.

Romain Alléaume
Associate Professor, Telecom-ParisTech, Paris, France

Romain Alléaume works on quantum cryptography and quantum information. He co-founded the start-up company SeQureNet in 2008, that brought to market the first commercial CV-QKD system in 2013. He has authored more than 40 papers in the field and is a regular contributor to the ETSI ISG QKD.

Christopher Chunnilall
Senior Research Scientist, National Physical Laboratory, Teddington, UK

Christopher Chunnilall works on the development of metrological techniques for quantifying the optical performance of QKD hardware. He led the drafting of ETSI's Group Specification document entitled "Component characterization: characterizing optical components for QKD systems".

Ivo Pietro Degiovanni
Senior Researcher, Istituto Nazionale di Ricerca Metrologica (INRIM), Torino, Italy

Ivo Pietro Degiovanni works on metrology for quantum photonics technology and has coordinated EU funded projects on metrology for QKD. He has authored more than 80 papers in the field. He is a regular contributor to the ETSI ISG QKD.

Marco Gramegna
Research Scientist, Istituto Nazionale di Ricerca Metrologica (INRiM), Torino IT

Marco Gramegna works in quantum optics, quantum communication, quantum metrology and metrology for quantum technologies. In these fields he is author of more than 45 papers on JCR journals. He is a regular contributor to the ETSI Industry Specification Group (ISG) on QKD.

Atilla Hasekioglu
Consultant and Senior Researcher, Tubitak Bilgem, Kocaeli, Turkey

Atilla Hasekioglu works as a coordinator for quantum technology related projects. He worked on the theory and implementations of QKD systems. He was also involved in cryptography and cyber security areas. Currently, he is a vice-chair of ETSI ISG QKD.

Bruno Huttner
Director for Quantum Space Programs, ID Quantique, Geneva, Switzerland

Bruno Huttner joined ID Quantique in 2014, participating in business development and product management for the Quantum-Safe Security division, which develops next-generation encryption solutions, including quantum key distribution systems.

Andrew Lord
Head of Optical Research, BT PLC, Adastral Park, UK

Andrew currently leads BT's optical core and access research including optical access, high speed transmission, Software Defined Networking and Quantum Communications. He regularly speaks at conferences and was Technical Program Chair for OFC 2015 and General Chair for OFC 2017.

Rupesh Kumar
Research Associate, Quantum Comms Hub, Univ. York; Centre for Photonic Systems, Univ. Cambridge

Rupesh Kumar works on the experimental realisation of quantum key distribution, both in continuous variable and discrete variable systems and networks. He has more than 10 years' experience in quantum-related technology with publications and patents in this field.

Norbert Lütkenhaus, Fellow of the American Physical Society
Professor, Inst. for Quantum Computing and Dept. Physics & Astronomy, University of Waterloo, Canada

Norbert Lütkenhaus was project leader for one of the first commercial QKD implementations in 2000 and leads research groups in the area of QKD security since 2001. He published over 100 scientific articles, is a regular invited speaker at international conferences and is a Vice-Chair of the ETSI QKD ISG.

Vadim Makarov
Vadim Makarov is an expert in implementation security of quantum cryptography and a contributor to ETSI ISG QKD.

Vicente Martin
Professor of Computational Sciences, Universidad Politécnica de Madrid

Vicente Martin's main research interest is the integration of QKD in communications networks. He has published over 60 contributions and awarded 5 patents on quantum communications technologies. He has participated in ETSI ISG QKD since its foundation in 2008.

Alan Mink
Researcher, NIST, USA

Alan Mink works in the area of QKD and is a regular participant to the ETSI QKD ISG.

Momtchil Peev
Quantum Communication Project Leader, Huawei Technologies Düsseldorf GmbH, Munich, Germany

Momtchil Peev leads the group on quantum communication technologies at the Munich Research Centre of Huawei Technologies Düsseldorf GmbH. He was a co-founder of the ETSI ISG QKD and serves currently as a Vice-Chair. He has co-authored around 90 papers on QKD and related fields.

Masahide Sasaki
Distinguished Researcher, National Institute of Information and Communications Technology, Japan

Masahide Sasaki works on the development on QKD systems and the deployment of QKD networks. He has led Japanese national projects on QKD for more than 17 years and authored more than 250 papers on quantum communication.

Alastair Sinclair
Principal Research Scientist, National Physical Laboratory, Teddington, UK

Alastair Sinclair works on development of metrological techniques for quantifying the optical performance of QKD hardware. His research has contributed to ETSI's Group Specification document entitled "Component characterization: characterizing optical components for QKD systems".

Tim Spiller CPhys, FInstP
Professor, Department of Physics, University of York, UK

TS is Director of the York Centre for Quantum Technologies and the EPSRC Quantum Communications Hub, a major academia-industry collaboration of the UK National Quantum Technologies Programme. Previously he led the Quantum Technology programme at HP Laboratories Bristol.

Martin Ward
Senior Research Scientist, Toshiba Research Europe Ltd, Cambridge, UK

Martin Ward's research interests include quantum photonic sources, quantum optics and quantum key distribution and network security. He is Secretary of the ETSI ISG QKD.

Catherine White
Senior Researcher, BT PLC, Adastral Park, UK

Catherine White is a member of the optics research team at BT and has been involved in integration of QKD systems in field trials at BT since 2013. She is involved in coordinating BT's QKD activity, for example through engagement with ETSI QKD working group and UK Quantum Communications hub.

Zhiliang Yuan
Principal Research Scientist and Team Leader, Toshiba Research Europe Ltd, Cambridge, UK

Zhiliang Yuan leads a multi-disciplinary research team developing high bit rate quantum key distribution systems and their underlying component technologies. He has co-authored over 100 scientific papers.

Contents

About the authors 2
Contents 6
Executive Summary 7
Scope and Purpose 9
Overview 10
Theoretical security 10
Implementation security 12
Specific examples 14
Side channels 14
Trojan-horse attack 15
Multi-photon emission 15
Imperfect encoding 16
Phase correlation between signal pulses 16
Bright-light attack 17
Efficiency mismatch and time-shift attacks 17
Back-flash attack 18
Manipulation of local oscillator reference 18
Other attacks 18
Advanced countermeasures 19
Role of ETSI and National Agencies 20
Conclusion 21
Acronyms and abbreviations 22
Bibliography 22

Executive Summary

Quantum cryptography provides an ensemble of protocols, such as quantum key distribution [1-3], quantum random number generation [4], closed group digital signatures [5], long-term secure data storage [6] and multi-party secure computation [7], which are robust against future algorithmic and computational advances, including the emergence of quantum computers. This is because its security is information-theoretic, i.e., it can be proven based only on models of the local devices operated by legitimate users and does not require any assumptions on the resources available to an adversary [8-12].

Information-theoretic security will be important for data confidentiality in the future when we expect more powerful computers and new algorithms to be at the fingertips of our digital foes. Of particular concern is the advent of quantum computers that can be used to launch efficient attacks on conventional techniques, such as the widely-used forms of public key cryptography.

Well before more powerful conventional and quantum computers become available, quantum cryptography will be important to protect against a generic vulnerability inherent to current cryptographic techniques based on computational complexity: encrypted data can be stored today and decrypted in the future, when suitable technology becomes available. This leads to the possibility of retrospectively breaking encryption keys established with computational techniques, such as the Diffie-Hellman key exchange algorithm. This becomes a serious threat if data confidentiality must be maintained for several years, especially as it is now feasible to store large volumes of information.

Although the quantum cryptographic *protocols* are information-theoretic secure, *real systems* may still possess side channels, i.e. security vulnerabilities, if their implementation deviates significantly from the idealised models used in the security analysis [12-15]. This is a common threat to any cryptosystem, irrespective of whether it is based on quantum theory [16-23] or computational complexity [24-28]. For example, timing attacks can threaten implementations of both quantum [16] and non-quantum [24] systems. Therefore, the security analysis of a cryptosystem's implementation, for simplicity called "implementation security", is a natural and important development in the evolution of all cryptographic technologies, including quantum cryptography.

Since the security of quantum cryptography depends only on the legitimate users' local equipment, the fundamental task in quantum cryptography implementation security is to estimate how much information such equipment leaks to a potential adversary. When this information leakage can be bounded below a certain value, security can be restored [29, 30] using a technique called *privacy amplification* [31, 32, 33]. This compresses a partially secret bit sequence into a highly secure key, with the amount of compression depending upon the estimated information leakage. Thus, by adequately characterising a real system, it is possible to restore the security promise of the theoretical protocol against technology available at the time that secret key is being created. It is a specific feature of quantum cryptography that this security statement does not change with future technological advances.

Privacy amplification is not the only resource available to enforce the implementation security of quantum cryptography. Modifications to hardware and protocols can dramatically reduce the information leakage and the potential occurrence of side-channels and active attacks [34-38]. Moreover, quantum correlations can be used to test the hardware of a real system [39-40]. Such tests can be quite demanding to implement but have the advantage of immunity against a large class of implementation issues.

The importance of analysing the implementation security of quantum cryptography is widely recognised and is a very active area of research. National metrology institutes, government organisations, universities and private companies fully acknowledge the importance of this subject and are supporting its effective development. ETSI has established an Industry Specification Group (ISG) to coordinate these efforts and to set forward-looking standards in quantum cryptography implementation security [41]. These will guide security evaluation by qualified third parties, as part of a security certification of quantum cryptographic products.

Scope and Purpose

The main purpose of this White Paper is to summarise for a general audience the current status of quantum cryptography implementation security and to outline the current understanding of the best practice related to it. We will illustrate the discussion with Quantum Key Distribution (QKD), although many of the arguments also apply to the other quantum cryptographic primitives. It is beyond the scope of this paper to analyse the security of all QKD protocols. To maintain readability, we will outline how the physical implementation may impact security but will not provide a detailed theoretical analysis. For the latter, we refer the reader to the references cited in the paper.

The information-theoretic security of a QKD system can be established based on an idealised model of that system. Therefore, the only way to attack a QKD system is to challenge the sole trust assumption that is made in QKD, namely that the system faithfully implements the underlying protocols and does not unintentionally leak information about the key to the attacker. All of the attacks against QKD reported so far, including those reported in the news as “quantum hacking” (see e.g. [42-44]), exploit (actively or passively) real system imperfections, i.e., deviations of the implementation from an idealised model, to break the trust assumption mentioned above. This White Paper summarises the work that has been conducted recently and which may be unfamiliar to readers outside this field, to enable the development of QKD systems with high implementation security assurance.

We shall consider the typical cryptographic scenario, where two distant parties use their QKD systems to obtain a string of bits R, the raw key, through an insecure communication channel. An eavesdropper, Eve, attempts to gain information about R by measuring the quantum signals travelling along the channel. This inevitably adds noise to the transmission due to the quantum properties of the signals. By measuring the noise, the QKD system can estimate the maximum amount of information gained by Eve on R. Privacy amplification (PA) can then be used to compress the string R into a new string S, the secret (final) key, on which Eve has no information. A convenient way to perform PA is by applying a two-universal hash function f, chosen by conventional communication, to R. The final length of S depends through f on the estimated leaked information.

A typical quantum hacking strategy exploits a deviation of the implementation from the idealised model to access information about the secure key. It is intuitively obvious that the larger the gap between the implementation and the idealised model, the greater the amount of leaked information. It is less intuitive that the impact is a shorter, but equally secure, final key. In QKD, the security level is a prerequisite of the system, fixed beforehand by the users. However, the length of the final key S depends upon the amount of potentially leaked information, which determines the PA compression ratio. This means that, provided it can be accurately characterised, an implementation deviation can reduce the amount of key material, but leaves the overall security of a QKD system unchanged. Of course, if the deviation exceeds a certain threshold, it may no longer be possible to generate a secure key. We note that although PA can limit information loss, it cannot prevent a denial of service (DoS) attack. Indeed, just as for any point-to-point communication system, a DoS attack can always be made by “cutting” the communication channel. As in a conventional communication system, DoS attacks can be prevented by introducing alternatives channels (e.g., in a quantum network) to route the key material.

Overview

Theoretical security

Sending messages that can be kept secret from adversaries has always been important for human society and many ingenious methods have been devised over the centuries. Up until the first half of the 20th century, cryptography has been more art than science, relying on intuition rather than provable arguments. This changed when Claude Shannon introduced the concept of perfect secrecy, or "information theoretic secrecy" and proved that this property applies for the "one-time-pad" cipher [45]. For the one-time pad cipher the key ought to be random, have as many bits as the message and be used only once. For perfectly secret communication the problem is thus shifted to the distribution of the *key* used to encrypt and decrypt messages. We should note that communication using the one-time pad, although secret, is not guaranteed to be authentic and authenticity has to be ensured by other means.

Although the one-time-pad has been used in espionage, the manual distribution of long keys has proven to be extremely cumbersome and dangerous should key material be used more than once. For this reason, encryption has more practically resorted to "block ciphers" that require only a short secret key, for example of 256 bits for the widely used AES algorithm. If implemented correctly, block ciphers can be practically unbreakable through a brute force attack, due to the very large number of possible key combinations (e.g. $>10^{77}$ for a 256-bit key!). Thus, breaking the cypher through a systematic search of the key space is regarded as virtually impossible for the foreseeable future. Although block ciphers have practical advantages over the one-time pad, they still require the distribution of a secret key, albeit a much shorter one.

A solution to the key distribution problem arrived with Diffie and Hellman's (DH) 1976 paper [46], which heralded the era of public-key cryptography. There a method is presented on how to distribute keys between authenticated remote parties without using trusted couriers. The central idea is the "one-way function with a trapdoor" [46], i.e., functions that the legitimate users can easily calculate, but which are extremely difficult for Eve to invert. This idea is also exploited in the RSA algorithm [47], where the users are assigned the task of multiplying two large prime numbers (easy), whereas Eve has to factorise the result of the multiplication (difficult).

In public-key cryptography there are two strings, a "public key" that should be open but uniquely bound to the identity of a legitimate party and another "private key" that should be secret, i.e. known only to the legitimate party. The two "keys" (strings) are mathematically related. Anyone can use the public key, for example to encrypt a message, but only the person owning the private key can employ it, in this case, to decrypt the message.

Public key cryptography is currently a cornerstone of internet security, where it provides functionalities such as key distribution (for subsequent encryption of data using block ciphers), public-key encryption and public-key verifiable digital signatures. Public-key cryptography is however facing challenges, as its security relies on assumption about Eve's computing power and cryptanalytic capability, assumptions that may not hold in the future and thus do not guarantee long-term security. Although one-way-ness does not necessarily assume lack of limitless computing, the existence of such one-way functions is still open conjecture, and the algorithms employed in public key cryptography can be inverted with a sufficiently powerful computer. This differs from "information-theoretic security", which is independent of all future algorithmic advances or the availability of unlimited computational power.

Along these lines present-day public-key cryptography is believed to offer security against an eavesdropper equipped with a powerful conventional computer. However, the length of the keys must be continuously increased to keep up with advancing technology, leading to inefficiency in the execution of the algorithms. For example, RSA encryption and decryption times scale with the n^2 and n^3 of the string (key) length n, respectively (see, e.g., [48]), entailing a much longer execution time whenever the key length is even slightly increased.

The discovery of quantum algorithms speeding up the solution of complex problems [49, 50] has prompted recent work to redefine the security assumptions of public key cryptography. Shor's algorithm [49], in particular, can factorise integers and compute discrete logarithms (the mathematical problem on which the DH algorithm is based) in polynomial time, thus threatening the main security advantage of traditional public-key cryptography.

To react to these developments, there is ongoing research on new methods that are more resistant to attacks by a quantum computer [51, 52]. The target for these quantum-computer resistant (or "post-quantum (computer)" as they are often known) ciphers is often resilience to Shor's algorithm [53]. (We note in passing that block ciphers are Shor resilient in contrast to DH and RSA.) However, proving security against any possible attack utilising quantum computers, even unknown ones, is non-feasible and regarded to be beyond the scope of these new methods. Furthermore, as large-scale quantum computers do not exist yet, it is difficult to test the resilience of the new public key algorithms. As an alternative to public key cryptography, it has also been suggested that signature schemes could be constructed using block ciphers and hash functions [54].

QKD is an alternative approach to cryptographic key establishment, first suggested by Wiesner [55], Bennett and Brassard [1] and Ekert [2]. It relies on sending and detecting quantum (light) signals, as well as conventional data about the measurements and settings, to distil a secure key. The conventional communications channel must be authentic, something that can be achieved using an information-theoretical protocol such as 2-universal hashing.

The novel and unique feature of QKD is that the protocol security can be guaranteed without setting any assumptions on Eve's resources, including her computational power. Indeed, an eavesdropper can be assumed to use unlimited computational power, unlimited storage memory and any conceivable device. Despite these assumptions the transmission of the cryptographic keys through an open channel, even one that is entirely under Eve's control, can be guaranteed perfectly secure.

The security proofs for QKD allow a failure probability to be defined for each individual key [56-59]. This arises in part because the number of quantum signals used to form each key is necessarily finite and their measurement will thus have errors associated with random statistical fluctuations. A "failure" in QKD means any leakage of the final key, even only a partial one, to the eavesdropper [59]. The failure probability provides a convenient parameter to quantify the security of a QKD protocol. It can be made arbitrarily small, although this will also reduce the secure key rate. Current QKD systems implementing one of the variants of the BB84 protocol can provide keys with failure probabilities smaller than 10^{-10} [60-62]. For typically used key sizes this would amount to a single failure in 30,000 years.

We note that quantum cryptography does not replicate all the functionalities of public key cryptography. In particular, although there is ongoing research on quantum digital signature schemes, they are not yet as efficient or flexible as public key schemes. It is very likely therefore that QKD, quantum random

number generation and other quantum-based primitives, will be used in conjunction with quantum resistant algorithms in future quantum-safe infrastructures.

The security of many QKD protocols have been proven to be universally composable [63], which means that QKD keys can be used in conjunction with other cryptographic techniques [56, 58]. Used in combination with the one-time pad cipher and information-theoretically secure authentication, the resulting data communication protocol satisfies Shannon's definition of perfect secrecy and the security of the communications is unbreakable from a theoretical point of view. Note that, although QKD used together with block ciphers is no longer information theoretically secure, it is resilient to attack by a quantum computer.

Another important consequence of QKD security, is the fact that it is "everlasting", in the sense that keys, established via QKD, cannot be broken retrospectively. In contrast this vulnerability is generic when one uses computational techniques. Interestingly, everlasting security of QKD holds even when the initial authentication relies on computational techniques [7, 64] so long as the authentication is not compromised during the key transfer itself. This offers a practical solution for the initial authentication of QKD devices in large-scale networks.

Implementation security

Given that the theoretical security of a cryptographic protocol is known, we consider how it can be transferred into a real cryptosystem. This question defines the "implementation security" of a protocol, which markedly depends on the assumptions made about the QKD devices. Such devices are often assumed to be "flawless" (i.e., to behave exactly as described in the model used to prove QKD security), but in practice they display imperfections, i.e. deviations from the idealised model, which might weaken security. Assessing the magnitude of the deviations between the system and the ideal and reducing them sufficiently is the main goal of implementation security.

The analysis of a system's implementation security is usually far from trivial, as it depends on the physical components employed to build it. Such components have to be characterised and then included in a physical model. The model has to be refined until it captures all the relevant features of a real system and has to tolerate deviations in each different system. The good news, however, is that although non-trivial, the implementation security problem is well-founded. In a cryptographic scenario, it is crucial to allot the security assumptions unevenly between eavesdropper and users, so that most of them fall onto the users and only the smallest part onto the eavesdropper. The reason is that *the assumptions on an adversary cannot be verified whereas those on the QKD system hardware can*, at least in principle. For QKD, in particular, there is no assumption on Eve's resources. Therefore, if we could guarantee the "correct" (i.e., model-consistent) behaviour of the QKD devices, we would immediately gain the highest level of security for the system.

Before moving on to discuss the implementation security of QKD systems, we notice that computational cryptographic systems are not immune to attacks based on imperfect implementation [24-28]. One example is described in [27]. Here, a timing attack was performed from a machine in a campus network against a web server via three routers located in the same network running an OpenSSL implementation of the RSA algorithm. Dummy queries were sent to the server and the response time from the server was recorded and analysed. This way, the attacker managed to reconstruct bit after bit the private key stored on the server.

Irrespective of the quantum or non-quantum nature of the cryptosystem, Eve can often gain more information by probing a non-ideal part of the physical implementation than attacking the cryptographic algorithm.

The implementation security of a QKD system depends on the specific setup considered, its components and their physical description. A brute-force approach would then be to develop an ad-hoc treatment for each and every part of a system until all parts have been scrutinised. Fortunately, there have been recent advances [29, 11] allowing information leaks common to different QKD systems to be identified, irrespective of their specific implementation. A prominent example is the decoy-state technique to overcome photon number splitting attacks [35-37], which is now a standard tool in most QKD systems.

If the information leak resulting from an attack based on a model-deviation can be accurately estimated and if it is not too large, PA may be used to suppress any residual information available to Eve after such an attack. The process is conceptually simple. The information leakage is identified and quantified by a careful characterisation of the QKD apparatus. Then, PA is performed to exclude from the key any potentially leaked information. As long as the leaked information is below a given threshold, QKD will still provide a positive key rate. The amount of PA necessary is calculated using the limiting theorems of quantum mechanics (see, e.g., [65, 66]). For larger deviations, it may be advantageous to introduce an appropriate countermeasure to detect an attack or reduce the amount of information that it can leak, to a level that can be mitigated by PA.

Incidentally we note here that PA is essentially a software routine with a parameter describing how much the key has to be compressed. This parameter can be updated securely at distance by a manufacturer. Therefore, if a QKD setup's implementation security analysis changes because a new vulnerability is discovered, we may expect that the customer will usually not need to return the QKD system to the vendor, contrary to what is suggested in [67]. An exception will be if the information leakage is too large to be compensated by PA, in which case a physical countermeasure may be required to reduce the information leaked to an adversary.

Specific examples

In the following, we will go through the main implementation security aspects affecting various QKD systems. In most cases, we will implicitly refer predominantly to the BB84 [1] protocol, which is the most widely implemented and tested QKD protocol. However, other protocols share the same rationale in tackling implementation issues and some of these are addressed.

In Table 1, we report a representative sample of the main attacks against a QKD setup as well as the countermeasures to avert them. In the following we will give a more detailed description of each item. It should be noted that many of these attacks are conceptually similar and often addressed by the same countermeasure.

Table 1 – List of attacks against a typical QKD system and respective countermeasures. The acronyms in the table are listed at the end of the paper.

SECURITY ISSUE	DESCRIPTION	COUNTERMEASURES
Trojan-horse attack	Eve probes the QKD equipment with light to gain information about the device settings	privacy amplification (PA), isolators, filters
Multi-photon emission	When more than one photon is emitted in a pulse, information is redundantly encoded on multiple photons	PA, characterisation, decoy states, SARG04 and other protocols
Imperfect encoding	Initial states do not conform to the protocol	PA, characterisation
Phase correlation between signal pulses	Non-phase-randomised pulses leak more info to Eve, decoy states fail	phase randomisation, PA
Bright-light attack	Eve manipulates the photon detectors by sending bright-light to them	active monitoring, measurement device independent QKD (MDI-QKD)
Efficiency mismatch and time-shift attack	Eve can control, at least partially, which detector is to click, gaining information on the encoded bit	MDI-QKD, detector symmetrisation
Back-flash attack	Eve can learn which detector clicked and hence knows the bit	isolators, MDI-QKD, detector symmetrisation
Manipulation of Local Oscillator reference	In continuous variable QKD (CV-QKD), the local oscillator (LO) can be tampered with by Eve if it is sent on a communications channel	Generate LO at the receiver. Phase reloading, i.e. only synchronise the phase of LO

Side channels

As a start, let us consider the so-called “side-channels”, which are present both in quantum and non-quantum cryptography. A naïve example of a side-channel is a group of soldiers using encrypted smoke signals to communicate their supposedly secret position to their allies. Clearly their enemies have an easy life in finding out the secret information here, because they just need to look at the physical origin of the smoke to know the position of the soldiers, without even thinking about decrypting the code in the smoke signals. In this case, it is not the encryption method that fails, but rather its physical implementation, which clearly contains a side-channel leaking sensitive information.

In modern cryptography, side-channels represent “any attack based on information gained from the physical implementation of a cryptosystem, rather than brute force or theoretical weaknesses in the algorithm or protocol” [68]. For example, the timing of the signals exchanged between sender and receiver and the power consumption of the CPU performing encryption and decryption are common side channels [24-28], where Eve gains information from the information leakage, not from decoding the encryption algorithm.

In QKD, side-channels have a similar meaning, representing the encoding of redundant information that differ from the intended encoding. This might involve correlations in degrees of freedom that are different from the intended ones. This can occur due to an unintentional flaw in the implementation or be triggered by the eavesdropper.

It might happen, for instance, that the sending unit unintentionally emits light over multiple frequencies. If information were redundantly encoded in the additional frequencies Eve could capture this without disturbing the intended encoding and leaving a trace through increased error. A simple way to avoid this problem is to filter the emission spectrum of the source, characterise its spectral components and remove any residual leaked information from the key using PA.

Trojan-horse attack

In some cases, Eve can actively attack a QKD system. For example, she can inject light into the sending module to probe and retrieve information about the encoding devices, thus realizing a quantum version of the “Trojan-horse attack” [69, 70]. Light injected by Eve passes through the same devices encoding information on the quantum signals and some of this light is then reflected back to Eve due to the non-zero reflectivity of the electro-optic components. Viewed naively this may seem a difficult problem to overcome, as it is impossible to perfectly shield a real physical system from Eve’s probing light, or to stop it from emitting undesired radiation correlated with the information encoded by the QKD system. This has brought researchers to question the very physical foundation of QKD [71] and to suggest that a “black-hole lab” would be necessary to guarantee the necessary isolation of the QKD modules [72].

Fortunately, PA is a far simpler method to overcome inevitable deviations from the idealised model. With PA, it suffices to first minimise the leakage (e.g., using isolators) and then upper bound the small remaining information leakage and remove it from the final key using, e.g., 2-universal hashing, to restore security. The information leak can be upper bounded using physical mechanisms, such as the ISO-defined laser-induced damage threshold of an optical fibre [38].

Multi-photon emission

Another type of implementation issue is related to a QKD system’s light source. Ideally a QKD system would use a true single photon source, which never generates more than one photon in each output pulse. However, as these are not yet available commercially, an attenuated laser diode is often used instead. The pulses from an attenuated laser can of course contain more than one photon. For these, the same information is redundantly encoded on all the photons in the pulse, thus creating the conditions for Eve to attack the system through a photon-number-splitting attack [15]. Eve can block all the pulses emitted by the QKD system containing less than two photons. From all the others, Eve can subtract one photon and keep it for herself, while forwarding the remaining photons to the QKD receiver. During the public discussion, Eve will learn the encoding basis and will then be able to reliably measure the photons she captured. This way, Eve gains full information whereas the QKD receiver interprets the undetected photons as a normal loss due to the communication channel, leaving Eve undetected.

This problem was identified very early and solutions proposed [29, 73, 74]. The main countermeasure is similar to the previous case. By properly characterizing and modelling the light source, we can estimate the rate of multi-photon pulses emitted and therefore the information leakage. However, the leaked information can be removed from the key by executing PA. In a sense, therefore multi-photon emission is no longer an issue in QKD implementation security, as we can do a complete security analysis with the correct PA setting just by modelling the signal sources as weak coherent light pulses. The resulting key, after the PA discussed above, is information-theoretically secure.

Although this solution works fine, it usually entails a severe PA compression, thus reducing the key rate and also the transmission distance of QKD. A drastic improvement of the performance can be obtained by modifying the BB84 protocol to include weaker intensity "decoy states" [35-37]. By varying the intensity of the weak light pulses in a predetermined, random sequence, the system can detect the actual occurrence of a photon-number-splitting attack on the quantum channel and precisely estimate the information loss. This usually allows a high secure key rate to be maintained.

Another solution is the so-called "SARG04 protocol" [75]. This is a variant of the BB84 protocol [1] that improves its performance and its tolerance to multi-photon emission by a simple modification of the software-based post-processing routine.

Imperfect encoding

Every QKD protocol has to specify how to prepare the quantum states to be transmitted over the insecure public channel. This is to a certain extent analogous to the initial selection of good prime numbers in the RSA algorithm, where a weak choice can compromise the overall security.

In QKD, the prepared states can deviate from those specified by the protocol due to imperfections of the physical equipment. This suggests that it should have only a small impact on security. However, if standard security proofs are applied [15, 55], the result is not robust against the typical losses of a communication channel, leading to a higher-than expected reduction in the key rate.

This impairment was resolved by recently developed security proofs [76, 77], available not only for asymptotically infinite key blocks but also in the finite-size scenario [78]. Such proofs can be applied to the measured deviation from the ideal model to restore the security of a QKD system and obtain nearly the same key generation rate as with a flawless encoding.

Phase correlation between signal pulses

As already discussed regarding multi-photon emission, it is quite common in QKD to replace the ideal single-photon light source with an attenuated laser. One of the consequences of this replacement is that the electromagnetic phase of each emitted light pulse may be partially related to the phase of the other pulses due to the laser coherence.

In principle, this is not a security problem and indeed some protocols [72, 73] even make use of this coherence to distil a secure key, as this can be accounted for in the corresponding security proofs. Even the commonly used BB84 protocol can be run with signals that are not phase randomised [79]. However, this has been shown to severely limit its performance and setting a random phase between adjacent pulses provides better results [79, 80]. Moreover, when decoy states are used in combination with the BB84 protocol, the pulses' random phase is a fundamental assumption that has to be fulfilled in the practical implementation [35-37].

Guaranteeing a random phase in a real QKD setup can be achieved in a few different ways. If the pulses are carved from a continuous-wave (CW) laser beam using an intensity modulator, an additional phase modulator can be used to apply a random phase value. Imparting phases distributed over all the possible arbitrary values is not very practical to implement. Recently, however, a protocol was proposed using a discrete number of phase values between 0 and 2π. If the total number of discrete values is of order 8 or 16, the approximation to the ideal case is excellent and the resulting key rates do not suffer a significant reduction [81].

The most common, and simple, approach involves using a gain switched laser diode to generate the pulses [82]. As the cavity of the laser diode is devoid of light between pulses, each light pulse is initiated by a random spontaneous emission event and thus has a random phase. Recently this was shown to result in minimal phase correlation between pulses for a 1GHz repetition rate and indeed can even be used to generate random numbers at high rates [83, 84].

Bright-light attack

A crucial part of most QKD systems are the single-photon detectors, used in the QKD receiver to detect the weak optical signals sent by the transmitter through the communication channel. The most common single-photon detectors are avalanche photodiodes (APDs) operated in Geiger mode. The APD is reverse-biased above the breakdown voltage so that a single photon can trigger a self-sustained avalanche easily detectable by a sudden increase in the output current. However, any detector necessarily spends part of its time below the breakdown voltage, because at some point the detection avalanche has to be quenched to reset the detector to the initial conditions. When this happens, the detector enters the linear mode, where it is not sensitive to single-photon light anymore.

It has been shown that the linear regime can be exploited by Eve to control the output of the detectors and determine, unnoticed, bits of the final key [18-20]. In some cases, Eve can even push a single-photon detector into the linear mode by sending bright-light into the receiver module, to then exploit her controlling abilities and steal key bits.

This group of attacks needs to be carefully analysed and efforts must be made to distinguish between incorrect operation of a detector and genuine loopholes. For example, it has been shown that bright illumination from a continuous-wave (CW) laser in the 1fW – 10mW range is easily detected when gated APDs are operated in a specific mode [85]. Alternatively, the QKD system could monitor in real time the APD parameters like its photocurrent, the bias voltage, the temperature, the after-pulsing rate or its quantum efficiency [18, 85-87]. These countermeasures greatly reduce the information Eve can gain about the key and current work is ongoing to precisely quantify their impact on the secure key rate. Finally, it is worth mentioning that measurement-device-independent (MDI)-QKD [39, 40], described below, makes this and all the other attacks directed at single-photon detectors irrelevant.

Efficiency mismatch and time-shift attacks

A typical QKD setup includes two detectors, each of which is associated with a different value of the key bit, either 0 or 1. Clearly, if Eve can learn which of the detectors has responded to the input light, she can learn the key bit. Therefore, it is necessary to make the two detectors indistinguishable from Eve's point of view. This is challenging because two complex objects like photodetectors are unlikely to be identical. In general, whenever the response curves of the detectors are different, Eve has room to attack the QKD setup. More specifically, if the wavelength dependence of the detector efficiencies differ, Eve can attempt the so-called "efficiency-mismatch" attack [88], whereas if the time responses are different, Eve can run

the “time-shift” attack [89]. Recently another attack to actively induce a detector mismatch has been described [90].

This kind of attack can be avoided using a combination of PA and characterisation of the differences in the parameters of the two detectors. The security proof in [34] takes into account the difference between the response curves of the detectors and removes the extra information leaked to Eve through PA. This attack may also be negated by symmetrisation of the detectors with respect to a particular single photon signal state. By randomly switching the bit assignment between the two detectors, the two detectors are rendered virtually identical, thus preventing Eve from assigning bit values to the information she retrieves.

Back-flash attack

A passive way allowing Eve to learn the bit values associated with detection events is the so-called back-flash attack. The secondary photons emitted by an APD during the avalanche of charge carriers due to a detection event can travel from the detectors back to Eve through the communication channel to the transmitter [91]. This effect has been shown to occur also in gated InGaAs/InP detectors routinely employed in QKD systems operating at telecom wavelengths [92].

Proper design and testing of QKD systems should be implemented in order to avoid the back-flash attack. Solutions are low-loss passive optical devices such as isolators, circulators or spectral filters to bound the probability of a back-flash photon leaking out of the QKD system to a low level to enable the use of PA to recover security. Furthermore, the use of a short gate is expected to considerably reduce the intensity of the emitted light in fast-gated detectors [93, 94].

It should be pointed out that the detector symmetrisation technique mentioned in the preceding section can prove effective also against the back-flash attack, provided that the bit label of the light retrieved by Eve is not leaked by the QKD receiver module. Finally, the users could resort to MDI-QKD, discussed later, to remove this attack as well as all other attacks targeting the detectors.

Manipulation of local oscillator reference

In QKD systems that require the transmission of an intense phase reference, such as continuous variable QKD, Eve can manipulate the amplitude, shape and wavelength of the reference as well as the signal pulse. By doing so, Eve can control homodyne or heterodyne detectors in the receiver, to bias the noise estimation and hide her presence in the noise. In some attacks [95, 96], Eve changes the amplitude of the local oscillator (LO) while in others [97] the LO pulse shape is modified, to control the clock signals.

Real time monitoring of the LO [97] has been proposed as a feasible countermeasure. Alternatives are phase reloading, where the transmitted reference pulse only synchronises the phase of a local oscillator [98], as well as other techniques for local regeneration of the LO at the receiver [99, 100], thus removing the need for sharing the LO and preventing all attacks related to a malicious LO manipulation.

Other attacks

Recently it was proposed to use very bright laser light to damage components within the QKD system [101, 102]. These can be considered second-generation quantum attacks, as they target the countermeasures used to prevent more basic implementation bugs. The merit of these new attacks is to bring attention to parts and procedures that should be failsafe. However, they do not appear to be intrinsically more threatening than the issues discussed in this paper.

Clearly, in order to guarantee the full security of a given QKD setup, all the implementation issues of that setup should be tackled simultaneously rather than individually. In some cases, the countermeasure is broad enough to encompass more than one issue. In other cases, a promising approach has been recently proposed in [103], where a numerical routine directly outputs the privacy amplification compression rate of a system with multiple deviations from a standard model.

Advanced countermeasures

In addition to the countermeasures discussed such as PA, characterisation, symmetrisation and hardware modifications, it is important to stress that there are already conceptual methods capable of closing the vast majority of the QKD implementation issues. Examples are the teleportation gate [104], which can act as a perfect filter-isolator pair, shielding a private location from the outside world and so-called "device-independent" QKD [105-109], which can guarantee the security of communications between two isolated locations irrespective of the actual, even faulty, implementation of the protocol. These solutions are not widely adopted as they usually provide poor key rates, insufficient for modern-day applications.

In this respect, the recently introduced measurement device independent QKD (MDI-QKD) [39, 40] represents an interesting compromise between conceptual security and practicality. In fact, several MDI-QKD experiments have been performed already [110-118], with some of them showing the suitability of MDI-QKD for quantum networks [115], long distance [116, 117] and high-rate [118] communications.

MDI-QKD allows the assumptions about the security of the measuring devices to be relaxed. For MDI-QKD, neither end point is configured as an optical receiver, as in conventional send-and-measure QKD, but rather both ends are optical transmitters. The two optical transmitters send light pulses to an intermediate station, which couples and measures them. The users can distil a secret key from the measurement results disclosed by the mid-station.

The MDI-QKD protocol is protected against a malicious attempt by someone compromising the mid-station to gain information about the key. The legitimate users can always detect any attempt to alter the correct operation of the mid-station, as this would manifest as a form of regular eavesdropping.

In MDI-QKD it is no longer necessary to take special measures to protect the detection system from attack. Thus, the focus shifts to safeguarding the optical transmitters, which is easier conceptually than protecting optical receivers. In the former case, the optical pulses are prepared locally by a trusted user, whereas in the latter they are received from the outside, prepared by someone who is potentially untrusted and possibly interested in breaking the security of the system.

When combined with the other solutions presented in previous sections, the advanced methods discussed here make QKD implementation security a tractable problem, with large parts of it already resolved by design.

Role of ETSI and National Agencies

An important aspect of QKD implementation security is related to the standardisation process currently ongoing for QKD. In this case the task is to define best practices to operate QKD systems so as to minimise the risk of inadvertently opening a door for attacks. Furthermore, it is important to define and standardise those countermeasures that have been recognised to be effective in guaranteeing the security of a QKD setup.

The existence of a set of standards would reduce the risk that new systems are produced without effective protection measures to address known implementation issues. It will also help to ensure designs follow best practice to reduce the risk of systems being found vulnerable to newly identified implementation issues. These standards could also be used by certification authorities, to assess the security level of QKD products.

This process has already started, with ETSI establishing an Industry Specification Group for QKD. The group brings together important actors from science, industry and commerce to address standardisation issues in quantum cryptography and associated quantum technologies. A key role in this process is played by National Metrology Institutes, which are impartial bodies capable of supporting the process of characterising QKD components and assessing the security level of a QKD system by performing high-precision measurements. Their contribution to standards will improve the available solutions and promote the commercial availability of optical components for QKD that are specifically designed to ensure security.

Finally, we mention that national certification and information security agencies are likely to play an important role by overseeing a security certification process based on appropriate processes, e.g., certification by Common Criteria. This should provide an assessment of the adequacy of the QKD proof provided, model assumptions and implementation of quantum products from a security perspective. The ETSI ISG QKD will provide expert knowledge to help develop a suitable certification process.

Conclusion

The extraordinary benefit offered by QKD is that it is secure against all future algorithmic and computational advances. The security of its protocols does not rely on any assumptions about the resources available to the adversary, which are impossible to test. However, it is important to test the legitimate users' devices. An appropriately designed implementation should limit the information available through side channels. By determining an upper bound on the residual leaked information and using privacy amplification, it is possible to derive secure keys. The challenge of implementation security also exists for conventional cryptography and many of the digital end-point issues are common between conventional and quantum cryptography. Modelling of the implementation in quantum cryptography often enables deviations from an idealised model to be quantified.

Extensive theoretical and experimental work over the past 15 years has greatly improved our understanding of the implementation security of QKD. Methods for closing the most readily exploitable loopholes have been developed, such that attention has shifted to analysing the less significant ones. As a result, the gap between the theoretical description and a practical implementation of QKD has been reduced remarkably and a number of crucial "weaknesses" have been completely eliminated. These achievements have demonstrated the potential to mitigate all significant vulnerabilities, thus making QKD a robust solution to protect next-generation telecommunications.

Acronyms and abbreviations

Qubit: quantum bit

QKD: quantum key distribution

CV-QKD: continuous variable QKD

PA: privacy amplification

MDI: measurement-device-independent

APD: avalanche photodiode

ISG: Industry Specification Group

CW: continuous wave

LO: local oscillator

Bibliography

1. C. H. Bennett and G. Brassard, “Quantum cryptography: public key distribution and coin tossing”, Theor. Comput. Sci. 560, 7 (2014).
2. A. Ekert, “Quantum cryptography based on Bell's theorem”, Phys. Rev. Lett. 67, 661 (1991).
3. N. Gisin, G. Ribordy, W. Tittel and H. Zbinden, “Quantum cryptography”, Rev. Mod. Phys. 74, 145 (2002).
4. X. Ma, X. Yuan, Z. Cao, B. Qi. and Z. Zhang, “Quantum random number generators”, Npj Quantum Information 2, 16021 (2016).
5. P.J. Clarke et al., "Experimental demonstration of quantum digital signatures using phase-encoded coherent states of light", Nat. Commun. 3, 1174 (2012).
6. J. Braun, J. A. Buchmann, D. Demirel, M. Geihs, M. Fujiwara, S. Moriai, M. Sasaki and A. Waseda, “LINCOS: A Storage System Providing Long-Term Integrity, Authenticity and Confidentiality”, AsiaCCS 461-468 (2017).
7. D. Unruh, “Universally composable quantum multi-party computation”, In Advances in Cryptology—EUROCRYPT 2010, 486 (2010).
8. D. Mayers, “Quantum key distribution and string oblivious transfer in noisy channels”, Lecture Notes Comput. Sci. 1109, 343 (1996).
9. H.-K. Lo and H. F. Chau, “Unconditional security of quantum key distribution over arbitrarily long distances”, Science 283, 2050 (1999).
10. P. W. Shor and J. Preskill, “Simple proof of security of the BB84 quantum key distribution protocol”, Phys. Rev. Lett. 85, 441 (2000).
11. M. Koashi, “Simple security proof of quantum key distribution based on complementarity”, New J. Phys. 11, 045018 (2009).
12. V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus and M. Peev, “The security of practical quantum key distribution”, Rev. Mod. Phys. 81, 1301 (2009).
13. C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, J. Smolin, “Experimental quantum cryptography”, Journal of Cryptology 5, 3 (1992).

14. V. Scarani and C. Kurtsiefer, “The black paper of quantum cryptography: real implementation problems”, Theor. Comput. Sci. 560, 27 (2014).
15. G. Brassard, N. Lütkenhaus, T. Mor and B. C. Sanders, “Limitations on Practical Quantum Cryptography”, Phys. Rev. Lett. 85, 1330 (2000).
16. B. Qi, C.-H. F. Fung, H.-K. Lo and X. Ma, “Time-shift attack in practical quantum cryptosystems”, Quantum Inf. Comput. 7, 73 (2007).
17. Y. Zhao, C.-H. F. Fung, B. Qi, C. Chen, H.-K. Lo, “Quantum hacking: Experimental demonstration of time-shift attack against practical quantum-key-distribution systems”, Phys. Rev. A 78, 042333 (2008).
18. V. Makarov, “Controlling passively quenched single photon detectors by bright light”, New J. Phys. 11, 065003 (2009).
19. L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar and V. Makarov, “Hacking commercial quantum cryptography systems by tailored bright illumination”, Nat. Photonics 4, 686 (2010).
20. I. Gerhardt, Q. Liu, A. Lamas-Linares, J. Skaar, C. Kurtsiefer and V. Makarov, “Full-field implementation of a perfect eavesdropper on a quantum cryptography system”, Nat. Commun. 2, 349 (2011).
21. N. Jain, E. Anisimova, I. Khan, V. Makarov, Ch. Marquardt and G. Leuchs, “Trojan-horse attacks threaten the security of practical quantum cryptography”, New J. Phys. 16, 123030 (2014).
22. J.-Z. Huang, S. Kunz-Jacques, P. Jouguet, Ch. Weedbrook, Z.-Q. Yin, S. Wang, W. Chen, G.-C. Guo and Z.-F. Han, “Quantum hacking on quantum key distribution using homodyne detection”, Phys. Rev. A 89, 032304 (2014).
23. H. Qin, R. Kumar and R. Alleaume, “Quantum hacking: saturation attack on practical continuous-variable quantum key distribution”, Phys. Rev. A. 94, 012325 (2016).
24. P. Kocher, “Timing attacks on implementations of Diffie-Hellman, RSA, DSS and other systems”. CRYPTO’96, LNCS, vol. 1109, pp. 104–113 (1996).
25. P. Kocher, J. Jae and B. Jun, “Differential power analysis,” CYRPTO’99, LNCS, vol. 1666, pp. 388–397 (1999).
26. W. Schindler, “A timing attack against RSA with the Chinese remainder theorem” CHES’2000, LNCS, vol. 1965, pp. 110–125 (2000).
27. D. Brumley and D. Boneh, “Remote timing attacks are practical”, in Proc. of the 12th Usenix Security Symposium, pp. 1-14 (2003).
28. T. Finke, M. Gebhardt and W. Schindler, “New side-channel attack on RSA prime generation”, CHES’09, LNCS, vol. 5747, pp. 141–155 (2009).
29. D. Gottesman, H.-K. Lo, N. Lütkenhaus and J. Preskill, “Security of quantum key distribution with imperfect devices”, Quantum Inf. Comput. 4, 325 (2004).
30. H. Inamori, N. Lütkenhaus and D. Mayers, “Unconditional security of practical quantum key distribution”, Eur. Phys. J. D 41, 599 (2007).
31. C. H. Bennett, G. Brassard and J.-M. Robert, “Privacy amplification by public discussion”, SIAM J. on Comp. 17, 210–229 (1988).
32. C. H. Bennett, G. Brassard, C. Crépeau and U. M. Maurer, “Generalised privacy amplification”, IEEE Trans. On Information Theory 41, 1915 (1995).
33. T. Horvath, L.B. Kish and J. Scheuer, “Effective privacy amplification for secure classical communications”, EPL 94 (2011), 28002
34. C.-H. F. Fung, K. Tamaki, B. Qi, H.-K. Lo and X. Ma, “Security proof of quantum key distribution with detection efficiency mismatch”, Quant. Inf. and Comput. 9, 131-165 (2009).
35. W.-Y. Hwang, “Quantum key distribution with high loss: toward global secure communication”, Phys. Rev. Lett. 91, 057901 (2003).
36. X.-B. Wang, “Beating the photon-number-splitting attack in practical quantum cryptography”, Phys. Rev. Lett. 94, 230503 (2005).

37. H.-K. Lo, X. Ma and K. Chen, “Decoy state quantum key distribution”, Phys. Rev. Lett. 94, 230504 (2005).
38. M. Lucamarini, I. Choi, M. B. Ward, J. F. Dynes, Z. L. Yuan and A. J. Shields, “Practical security bounds against the Trojan-horse attack in quantum key distribution”, Phys. Rev. X 5, 031030 (2015).
39. S. Pirandola and S. Braunstein, “Side-channel-free quantum key distribution”, Phys. Rev. Lett. 108, 130502 (2012).
40. H.-K. Lo, M. Curty and B. Qi, “Measurement-device-independent quantum key distribution”, Phys. Rev. Lett. 108, 130503 (2012).
41. http://www.etsi.org/technologies-clusters/technologies/quantum-key-distribution
42. Z. Merali, “Quantum crack in cryptographic armour”, Nature News (20 May 2010).
43. Z. Merali, “Hackers blind quantum cryptographers”, Nature News (29 Aug 2010).
44. S. McGann, “Tricking the perfect code machine”, BBC News (13 Aug 2011).
45. C. E. Shannon, “Communication theory of secrecy systems,” Bell Syst. Tech. I., vol. 28, pp. 656-715, Oct. 1949.
46. W. Diffie and M. E. Hellman, “New directions in cryptography”, IEEE Trans. Informat. Theory, vol. IT-22, pp. 644-654 (1976).
47. R. L. Rivest, A. Shamir and L. Adleman, “A method for obtaining digital signatures and public-key cryptosystems”, Comm. ACM, vol. 21, pp. 120-126 (1978).
48. A. K. Lenstra and E. R. Verheul, “Selecting cryptographic key sizes”, Journal of Cryptology 14, 255 (2001).
49. P. Shor, “Polynomial-time algorithms for prime factorization and discrete logarithm problems”, SIAM J. Computing 26 (1997), 1484-1509.
50. L. Grover, “A fast quantum mechanical algorithm for database search”, Proc. 28th Annual ACM Symp. Theory of Computing, 212 (1996).
51. PQCrypto 2006. Katholieke Universiteit Leuven, Belgium, May 23-26 (2006).
52. D. J. Bernstein, J. Buchmann and E. Dahmen, Post-Quantum Cryptography, Springer, NewYork (2009).
53. P. Rebentrost, A. Steffens and S. Lloyd, “Quantum singular value decomposition of non-sparse low-rank matrices”, Phys. Rev. A 97, 012327 (2018).
54. K. Paterson, “Threats to Modern Cryptography and State-ofthe-Art Solutions”, https://web-tgm.newton.cam.ac.uk/presentation/2014-05-08/19435
55. S. Wiesner, Sigact News 15, 78 (1983).
56. R. Renner and R. Koenig, “Universally composable privacy amplification against quantum adversaries”, Proc. of TCC 2005, LNCS, Springer, vol. 3378 (2005).
57. M. Hayashi, “Practical evaluation of security for quantum key distribution”, Phys. Rev. A 74, 022307 (2006).
58. M. Hayashi, “Upper bounds of eavesdropper’s performances in finite-length code with the decoy method”, Phys. Rev. A 76, 012329 (2007).
59. V. Scarani and R. Renner, “Quantum cryptography with finite resources: unconditional security bound for discrete-variable protocols with one-way postprocessing”, Phys. Rev. Lett. 100, 200501 (2008).
60. S. Kunz-Jacques and P. Jouguet, “Robust shot-noise measurement for continuous-variable quantum key distribution”, Phys. Rev. A. 91, 022307(2015).
61. M. Lucamarini, K. A. Patel, J. F. Dynes, B. Fröhlich, A. W. Sharpe, A. R. Dixon, Z. L. Yuan, R. V. Penty and A. J. Shields, "Efficient decoy-state quantum key distribution with quantified security", Opt. Express 21, 24550 (2013).
62. A. R. Dixon, J. F. Dynes, M. Lucamarini, B. Fröhlich, A. W. Sharpe, A. Plews, S. Tam, Z. L. Yuan, Y. Tanizawa, H. Sato, S. Kawamura, M. Fujiwara, M. Sasaki and A. J. Shields, “High speed prototype quantum key distribution system and long-term field trial”, Opt. Express 23, 7583 (2015).

63. R. Canetti, “Universally Composable Security: A New Paradigm for Cryptographic Protocols,” in Proceedings of the 42Nd IEEE Symposium on Foundations of Computer Science, Washington, DC, USA, p136 (2001).
64. M. Mosca, D. Stebila and B. Ustaoglu, „Quantum key distribution in the classical authenticated key exchange framework”, in Philippe Gaborit, editor, *Proc. 5th International Conference on Post-Quantum Cryptography (PQCrypto) 2013*, *LNCS*, vol. 7932, pp. 136-154. Springer (2013).
65. W. K. Wootters and W. H. Zurek, “A single quantum cannot be cloned”, Nature 299, 802-803 (1982).
66. W. Heisenberg, “Über den anschaulichen Inhalt der quantentheoretischen Kinematik und Mechanik”, Zeitschrift für Physik (in German) 43, 172 (1927).
67. “Quantum key distribution: A CESG White Paper” (2016).
68. https://en.wikipedia.org/wiki/Side-channel_attack
69. 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 (2001).
70. 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).
71. D.J. Bernstein, “Is the security of quantum cryptography guaranteed by the laws of physics?”, Arxiv 1803.04520 (2018).
72. T. Rudolph, “The laws of physics and cryptographic security”, Arxiv: quant-ph/0202143 (2002).
73. K. Inoue, E. Waks and Y. Yamamoto, “Differential-phase-shift quantum key distribution,” Phys. Rev. Lett. 89, 037902 (2002).
74. D. Stucki, N. Brunner, N. Gisin, V. Scarani and H. Zbinden, “Fast and simple one-way quantum key distribution”, Appl. Phys. Lett. 87, 194108 (2005).
75. V. Scarani, A. Acín, G. Ribordy and N. Gisin, “Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations”, Phys. Rev. Lett. 92, 057901 (2004).
76. K. Tamaki, M. Curty and M. Lucamarini, “Decoy-state quantum key distribution with a leaky source”, New J. Phys. 18, 065008 (2016).
77. K. Tamaki, M. Curty, G. Kato, H.-K. Lo and K. Azuma, “Loss-tolerant quantum cryptography with imperfect sources”, Phys. Rev. A 90, 052314 (2014).
78. A. Mizutani, M. Curty, C. C. W. Lim, N. Imoto and K. Tamaki, “Finite-key security analysis of quantum key distribution with imperfect light sources”, New J. Phys. 17, 093011 (2015).
79. H.-K. Lo and J. Preskill, “Security of quantum key distribution using weak coherent states with non-random phases”, Quant. Inf. Comput. 8, 431-458 (2007).
80. H.-K. Lo and J. Preskill, “Phase randomization improves the security of quantum key distribution”, preprint quant-ph/0504209 (2005).
81. Z. Cao, Z. Zhang, H.-K. Lo and X. Ma, “Discrete-phase-randomised coherent state source and its application in quantum key distribution”, New J. Phys. 17, 053014 (2015).
82. P. Hiskett, G. Bonfrate, G. Buller and J. Townsend, “Eightly kilometre transmission experiment using InGaAs/InP SPAD-based quantum cryptography receiver operating at 1.55 km”, Mod. Opt. 48, 1957 (2001).
83. M. Jofre, M. Curty, F. Steinlechner, G. Anzolin, J. P. Torres, M. W. Mitchell and V. Pruneri, “True random numbers from amplified quantum vacuum”, Opt. Express 19, 20665 (2011).
84. Z. L. Yuan, M. Lucamarini, J. F. Dynes, B. Fröhlich, A. Plews and A. J. Shields, “Robust random number generation using steady-state emission of gain-switched laser diodes”, Appl. Phys. Lett. 104, 261112 (2014).
85. Z. L. Yuan, J. F. Dynes and A. J. Shields, “Resilience of gated avalanche photodiodes against bright illumination attacks in quantum cryptography”, Appl. Phys. Lett. 98, 231104 (2011).

86. Z. L. Yuan, J. F. Dynes and A. J. Shields, “Avoiding the blinding attack in QKD”, Nat. Photonics 4, 800 (2010).
87. L. Lydersen, V. Makarov and J. Skaar, “Secure gated detection scheme for quantum cryptography”, Phys. Rev. A 83, 032306 (2011).
88. V. Makarov, A. Anisimov and J. Skaar, “Effects of detector efficiency mismatch on security of quantum cryptosystems”, Phys. Rev. A 74, 022313 (2006).
89. B. Qi, C.-H. F. Fung, H.-K. Lo and X. Ma, “Time-shift attack in practical quantum cryptosystems”, Quant. Inf. Comput. 7, 73-82 (2007).
90. N. Jain, C. Wittmann, L. Lydersen, C. Wiechers, D. Elser, C. Marquardt, V. Makarov and G. Leuchs, “Device Calibration Impacts Security of Quantum Key Distribution”, Phys. Rev. Lett. 107, 110501 (2011).
91. C. Kurtsiefer, P. Zarda, S. Mayer and H. Weinfurter, “The breakdown flash of silicon avalanche photo-diodes –back door for eavesdropper attacks?”, J. Mod. Opt. 48. 2039 (2001).
92. A. Meda, I. P. Degiovanni, A. Tosi, Z. L. Yuan, G. Brida, M. Genovese, “Quantifying backflash radiation to prevent zero-error attacks in quantum key distribution”, Light: Science & Applications 6, e16261 (2017).
93. N. Namekata, S. Sasamori and S. Inoue, “800 MHz single-photon detection at 1550-nm using an InGaAs/InP avalanche photodiode operated with a sine wave gating”, Opt. Express 14, 10043 (2006).
94. Z. L. Yuan, B.E. Kardynal, A.W. Sharpe and A. J. Shields, “High speed single photon detection in the near infrared”, App. Phys. Lett. 91, 041114 (2007).
95. H. Haseler, T. Moroder and N. Lutkenhaus, “Testing quantum devices: practical entanglement verification in bipartite optical systems”, Phys. Rev. A. 77, 032303 (2008).
96. X. -C. Ma, S. -H. Sun, M.- S. Jiang and L. -M. Liang, “Local oscillator fluctuation opens a loophole for Eve in practical continuous-variable quantum-key-distribution systems”, Phys. Rev. A. 88, 022339 (2013).
97. P. Jouguet, S. Kunz-Jacques and E. Diamanti, “Preventing calibration attacks on the local oscillator in continuous-variable quantum key distribution”, Phys. Rev. A. 87, 062313 (2013).
98. M. Koashi, “Unconditional Security of Coherent-State Quantum Key Distribution with a Strong Phase-Reference Pulse,” Phys. Rev. Lett. 93, 120501 (2004).
99. B. Qi, P. Lougovski, R. Pooser, W. Grice and M. Bobrek, “Generating the local oscillator “locally” in continuous-variable quantum key distribution based on coherent detection”, Phys. Rev. X 5, 041009 (2015).
100. D. B. S. Soh, C. Brif, P. J. Coles, N. Lütkenhaus, R. M. Camacho, J. Urayama and M. Sarovar, “Self-referenced continuous-variable quantum key distribution protocol”, Phys. Rev. X 5, 041010 (2015).
101. A. N. Bugge, S. Sauge, A. M. M. Ghazali, J. Skaar, L. Lydersen and V. Makarov, “Laser damage helps the eavesdropper in quantum cryptography”, Phys. Rev. Lett. 112, 070503 (2014);
102. V Makarov et al, “Creation of backdoors in quantum communications via laser damage”, Phys. Rev. A 94, 030302 (2016).
103. P. J. Coles, E. M. Metodiev and N. Lütkenhaus, “Numerical approach for unstructured quantum key distribution”, Nat. Commun. 7, 11712 (2016).
104. C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres and W. K. Wootters, “Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels”, Phys. Rev. Lett. 70, 1895 (1993).
105. D. Mayers and A. Yao, “Self testing quantum apparatus”, Quantum Inform. Comput. 4, 273 (2004).
106. J. Barrett, L. Hardy and A. Kent, “No signalling and quantum key distribution”, Phys. Rev. Lett. 95, 010503 (2005).
107. A. Acín, N. Gisin and L. Masanes, “From Bell’s theorem to secure quantum key distribution”, Phys. Rev. Lett. 97, 120405 (2006).

108. A. Acín, N. Brunner, N. Gisin, S. Massar, S. Pironio and V. Scarani, “Device-independent security of quantum cryptography against collective attacks”, Phys. Rev. Lett. 98, 230501 (2007).
109. S. Pironio, A. Acín, N. Brunner, N. Gisin, S. Massar and V. Scarani, “Device-independent quantum key distribution secure against collective attacks”, New J. Phys. 11, 045021 (2009).
110. A. Rubenok, J. A. Slater, P. Chan, I. Lucio-Martinez and W. Tittel, “Real-world two-photon interference and proof-of-principle quantum key distribution immune to detector attacks”, Phys. Rev. Lett. 111, 130501 (2013).
111. Y. Liu et al., “Experimental measurement-device-independent quantum key distribution”, Phys. Rev. Lett. 111, 130502 (2013).
112. T. Ferreira da Silva et al., “Proof-of-principle demonstration of measurement-device-independent quantum key distribution using polarization qubits”, Phys. Rev. A 88, 052303 (2013).
113. Z. Tang et al., “Experimental demonstration of polarization encoding measurement-device-independent quantum key distribution”, Phys. Rev. Lett. 112, 190503 (2014).
114. R. Valivarthi et al., “Measurement-device-independent quantum key distribution: from idea towards application”, J. Mod. Optics 62, 1141 (2015).
115. Y.-L. Tang et al, “Measurement-device-independent quantum key distribution over untrustful metropolitan network”, Phys. Rev. X 6, 011024 (2016).
116. Y.-L. Tang et al., “Measurement-device-independent quantum key distribution over 200 km”, Phys. Rev. Lett. 113, 190501 (2014).
117. H.-L. Yin et al., “Measurement-device-independent quantum key distribution over a 404 km optical fiber”, Phys. Rev. Lett. 117, 190501 (2016).
118. L. C. Comandar, M. Lucamarini, B. Fröhlich, J. F. Dynes, A. W. Sharpe, S. W.-B. Tam, Z. L. Yuan, R. V. Penty and A. J. Shields, “Quantum key distribution without detector vulnerabilities using optically seeded lasers”, Nat. Photonics 10, 312 (2016).

ETSI
06921 Sophia Antipolis CEDEX, France
Tel +33 4 92 94 42 00
info@etsi.org
www.etsi.org