New Journal of Physics
The open-access journal for physics

Controlling passively quenched single photon detectors by bright light

Vadim Makarov

Department of Electronics and Telecommunications, Norwegian University of Science and Technology (NTNU), NO-7491 Trondheim, Norway
and
Department of Physics, Pohang University of Science and Technology, Pohang 790-784, Korea
E-mail: makarov@vad1.com

New Journal of Physics **11** (2009) 065003 (18pp)
Received 13 January 2009
Published 12 June 2009
Online at http://www.njp.org/
doi:10.1088/1367-2630/11/6/065003

Abstract. Single photon detectors (SPDs) based on passively quenched avalanche photodiodes can be temporarily blinded by relatively bright light, of intensity less than 1 nW. A bright-light regime suitable for attacking a quantum key distribution system containing such detectors is described in this paper. In this regime, all SPDs in the receiver Bob are uniformly blinded by continuous illumination coming from the eavesdropper Eve. When Eve needs a certain detector in Bob to produce a click, she modifies the polarization (or other parameters used to encode quantum states) of the light she sends to Bob such that the target detector stops receiving light, while the other detector(s) continue to be illuminated. The target detector regains single photon sensitivity and, when Eve modifies the polarization again, produces a single click. Thus, Eve has full control of Bob and can perform a successful intercept–resend attack. To check the feasibility of the attack, three different models of passively quenched detectors have been tested. In the experiment, I have simulated the intensity diagrams the detectors would receive in a real QKD system under attack. Control parameters and side effects are considered. It appears that the attack could be practically possible.

1367-2630/09/065003+18$30.00
© IOP Publishing Ltd and Deutsche Physikalische Gesellschaft

Contents

1. Introduction **2**
2. Blinding and controlling a passively quenched SPD **3**
3. Proposed attack against the QKD system **6**
4. Detector tests **9**
4.1. Detector model 1 9
4.2. Detector model 2 12
4.3. Detector model 3 13
5. Possibly affected systems and countermeasures **15**
6. Conclusion **16**
Acknowledgments **16**
References **16**

1. Introduction

Quantum key distribution (QKD) is a technique that allows remote parties to grow shared secret random key material at a steady rate, using an insecure optical communication channel and an authenticated classical communication channel [1, 2]. From a tabletop demonstration 19 years ago [1], QKD has progressed to commercial devices working over tens of kilometers of optical fiber[1] and many long-distance experiments. Key transmission over more than 100 km of fiber [3, 4] and 23 and 144 km of free space [5]–[7] has been demonstrated. As QKD enters the commercial market, it becomes increasingly important to verify the actual level of security in its implementations, and search for possible loopholes.

QKD has been proved to be unconditionally secure for certain models of equipment that include most common imperfections of components [8]. However, it remains a challenge to build a system that is demonstrably in strict accordance with the model in the security proof. Discovering and patching loopholes and imperfections of components is an ongoing process [9]–[13]. Once found, such an imperfection affecting security can either be integrated into the unconditional proof, neutralized by a specific coutermeasure or avoided through a rational choice of components, optical scheme and QKD protocol.

When treating security of QKD, we follow Kerckhoffs' principle: 'The system must not be required to be secret, and it must be able to fall into enemy hands without causing inconvenience' [14]. This principle, embraced in classical cryptography since the nineteenth century, means Eve is assumed to know everything about Alice's and Bob's equipment. Thus, Eve can fully exploit every imperfection that exists in the legitimate parties' hardware and software. Although it is tempting to assume that Eve might not know the type of equipment or its exact parameters, the history of cryptography shows that she will eventually find this out. In QKD, practical ways of measuring unobtrusively equipment parameters of a running cryptosystem may exist as well [11].

[1] Commercial QKD systems are available, as of early 2009, from at least three companies: id Quantique (Switzerland), http://www.idquantique.com/; MagiQ Technologies (USA), http://www.magiqtech.com/; SmartQuantum (France), http://www.smartquantum.com/

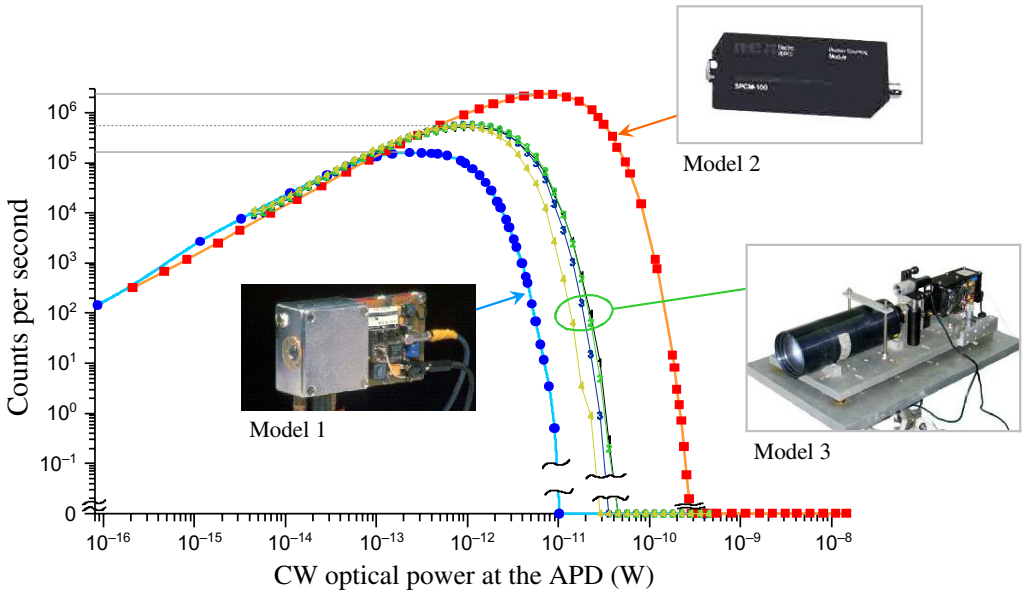

Figure 1. Detector saturation curves. Model 1: do-it-yourself design by Kurtsiefer *et al* (currently used in several laboratories; the sample tested was assembled at the Laboratory of Spontaneous Parametric Down-Conversion at Moscow State University). Model 2: EG&G SPCM-200-PQ (industrially produced in the 1990s). Model 3: four detectors used in Bob in a daylight free-space QKD system [17] (entire Bob is pictured in the inset; curves for model 3 reprinted from [18]). The dark count rate is around 100 counts per second (cps) for model 1, around 50 cps for model 2, and in the 900–2100 cps range for model 3.

In this paper, I report an imperfection found in single photon detectors (SPDs) of one particular type, namely those based on passively quenched avalanche photodiodes (APDs). This particular type of SPD is probably used in about 10% of all QKD implementations reported to date. Since the passive quenching is most suited for silicon APDs, the majority of the possibly affected systems are free-space QKD experiments doing optical transmission in the 500–900 nm wavelength range; they are listed in section 5. The current commercial devices working at longer telecommunication wavelengths[1] are *not* affected by this paticular vulnerability, because they use another type of SPD, a gated APD.

2. Blinding and controlling a passively quenched SPD

Passive quenching is the oldest and simplest possible circuit design in SPDs based on APDs [15, 16]. Beyond the useful photon counting rate range, passively quenched SPDs exhibit saturation and blinding behavior. Figure 1 illustrates this with the example of three different SPD models that I have tested. Up to a certain point different for each SPD model, their count rate increases approximately linearly with intensity of CW illumination. At higher input light intensities, the count rate saturates, reaches the peak value different for each model and begins to drop. It drops to *exactly* zero at 10 pW input power (at 820 nm wavelength) for model 1, at 280 pW (at 780 nm) for model 2 and at intermediate power values for the four tested detectors

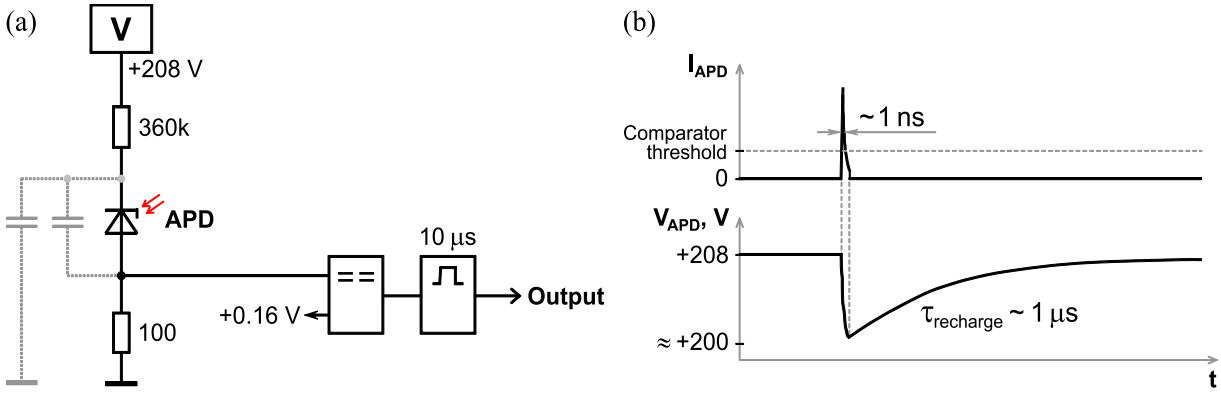

Figure 2. Detector model 1: (a) equivalent circuit diagram, (b) current through the APD and voltage at the APD during an avalanche and subsequent recharge.

of model 3. The shapes of the saturation curves are similar for all the tested detector models. This suggests that the saturation and blinding is generic to the passively quenched detector design. For the rest of this paper (except section 4.2), characteristics of model 1 are given in all examples, while models 2 and 3 are implied to exhibit the same behavior with different values of parameters.

To explain the blinding behavior, let us consider the circuit diagram of the detector model 1 (figure 2). The Si APD (PerkinElmer C30902S) is biased 6–10 V above its breakdown voltage from a high-voltage source via a 360 kΩ resistor. The circuit works thanks to the presence of two stray capacitances of the order of 1 pF each, shown in the circuit diagram. When there is no current flowing through the APD, both capacitances are charged to the bias voltage. During an avalanche, they quickly discharge through the APD, producing a short current pulse. The discharge current of the leftmost capacitance is converted into voltage at a 100 Ω resistor, and this voltage is sensed by a fast ECL comparator (MC100EL16). The short output pulse of the comparator is widened to about 10 μs by a non-retriggerable monostable multivibrator. The current pulse produced during the avalanche is of the order of 1 ns wide. When the voltage at the APD drops sufficiently close to the breakdown voltage, the avalanche quenches. The capacitances are subsequently slowly recharged through the bias resistor, with a recharge time constant of the order of 1 μs.

Until the capacitances recharge to a certain threshold voltage, which in our detector sample takes about 1 μs, the detector has no single photon sensitivity. (After 1 μs, it increases its quantum efficiency gradually as the voltage continues to rise.) However, a photon coming during the first microsecond may still cause an avalanche with a smaller peak current, not reaching the comparator threshold [16]. Such small avalanches reset the voltage and can keep the detector blinded indefinitely if they occur often enough. This is the primary blinding mechanism in the passively quenched detectors. Additionally, heating of the APD chip can contribute to the blinding. At 10 pW input optical power, the average electrical power dissipated in the APD is measured to be 5.7 mW. PerkinElmer C30902S APD is reported to have a high thermal resistance between the chip and the package [19]. The measured electrical power may raise the chip temperature by several degrees. This rise in temperature would increase the breakdown voltage by several volts, which could be a contributing factor to the blinding.

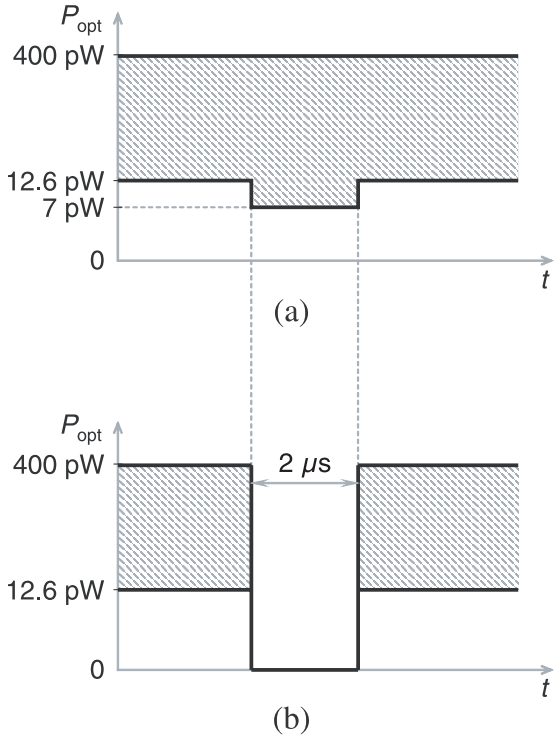

Figure 3. Control diagrams for detector model 1: (a) input intensity diagram that keeps the detector completely blinded at all times (no output pulses); (b) input intensity diagram that produces a single output pulse with probability greater than 0.8, right after the end of the 2 μs gap. The actual input intensity on both diagrams may take any shape within the hatched area.

In applications of SPDs, the nonlinearity of the response is undesirable [16]. Typically a detector is considered usable only in the mostly linear portion of its characteristic, located to the left of the saturation peak in figure 1. Detectors are never used beyond their saturation point. The following might be the first 'useful application' I have found for the beyond-saturation regime. In doing an attack against a QKD system, Eve may blind Bob's SPDs by delivering constant illumination higher than 10 pW to each of them. However, by introducing a gap in which the intensity of illumination drops to zero at one of Bob's SPDs, she may induce an output pulse at that SPD.

Let us first consider how Eve can control a single SPD. Experimental tests made on the detector model 1 have demonstrated that the control diagrams shown in figure 3 can be used. When the power of input illumination P_{opt} stays within the range depicted in figure 3(a), the SPD is kept blinded. However, in figure 3(b), after the light is switched off, the capacitances in the SPD have time to recharge and it becomes sensitive to single photons. When the light is switched on 2 μs later, the SPD produces a single photon count with probability greater than 0.8 (or no click in the remaining fraction of the cases), and after that becomes blinded again. I have only tested power values up to 400 pW with this detector model; however, the upper border of the power range could probably be extended much higher than 400 pW without causing any new effects. Experimental tests of the detectors are treated in more detail later on, in section 4.

3. Proposed attack against the QKD system

With the detector control method described above, Eve can attack a complete QKD system. In a QKD system, Bob has several detectors and/or makes a choice of detection basis. Eve needs a way to cause a click in a specific detector in a specific basis of her choice, without causing a click in the other detector(s) or in a different basis. I initially explain the attack with the example of a system with polarization coding and active basis choice at Bob that runs the Bennett–Brassard 1984 (BB84) protocol [1, 20]. In such a system, input light at Bob first passes through a modulator that, at Bob's random choice, either does nothing or rotates any input polarization state 45° clockwise, thus setting one of the two possible detection bases (figure 4(a)). After the modulator, light is split at a polarizing beam splitter (PBS). The vertical component of polarization goes to the detector D0 and the horizontal component goes to the detector D1.

Eve runs an intercept–resend attack (faked-state attack [11]) against this system. In the faked-state attack, she blocks the light between Alice and Bob completely (figure 4(b)). Eve uses a replica of Bob's setup Bob′ to detect Alice's quantum state, choosing the detection basis at random. Then, Eve forces Bob to make a click in her basis only and with the same bit value as she has just detected. (This is the difference between the conventional intercept–resend attack [1] and the faked-state attack [11]: in the latter, the basis and bit value of Bob's detector click is always the same as Eve's, thus the attack does *not* cause errors in the sifted key and eavesdropping is not detected.) Eve forces a click in the selected basis with the specific bit value by sending to Bob a specially crafted light state called a *faked state*, using her faked state generator FS. The faked state exploits technological imperfections in Bob to achieve its goal. In the present study, it will exploit detector controllability.

Let us suppose for certainty that Eve has detected Alice's quantum state in the 0° basis and registered a click in her D0 detector. She now has to form and send to Bob a faked state. The faked state should cause a click in Bob's D0 detector in the case that Bob chooses the 0° basis (the same basis as Eve has used), and should cause no clicks in either of Bob's detectors in the case that Bob chooses the 45° basis (not the basis Eve has used). The faked state that reaches this goal consists of an incoherent mixture of vertical and horizontal polarization components, with an intensity diagram for each polarization component as shown in the upper half of figure 4(c). The lower half of figure 4(c) shows what happens to this faked state in Bob's setup. If Bob chooses the 0° basis, his modulator does nothing and the two polarization components of the faked state are split each to its own detector. The intensity diagram of the vertical polarization component causes a click in D0 with probability greater than 0.8 (for the gap width of 2 μs). The intensity diagram of the horizontal polarization component keeps D1 blinded. If Bob, however, chooses the 45° basis, each polarization component is rotated 45° and is split equally at the polarizing beam splitter. The halves of the two polarization components sum at each detector, resulting in identical intensity diagrams that keep both detectors blinded. Eve's three other possible bit-basis detection results are treated symmetrically. Thus, my faked-state attack succeeds.

The reader may notice that the probability of a faked state sent by Eve to cause a click at Bob is $\frac{0.8}{2} = 0.4$. Many realistic Bobs have an overall photon detection efficiency of less than 40%, mainly due to limited quantum efficiency of the APDs. For these Bobs, Eve can mimic their detection rate before the attack, provided she uses ideal SPDs with 100% quantum efficiency and zero-loss optics in Bob′. However, I want my attack to be not only possible *in principle*, but also implementable in practice, today. For that, Eve cannot use non-existent ideal

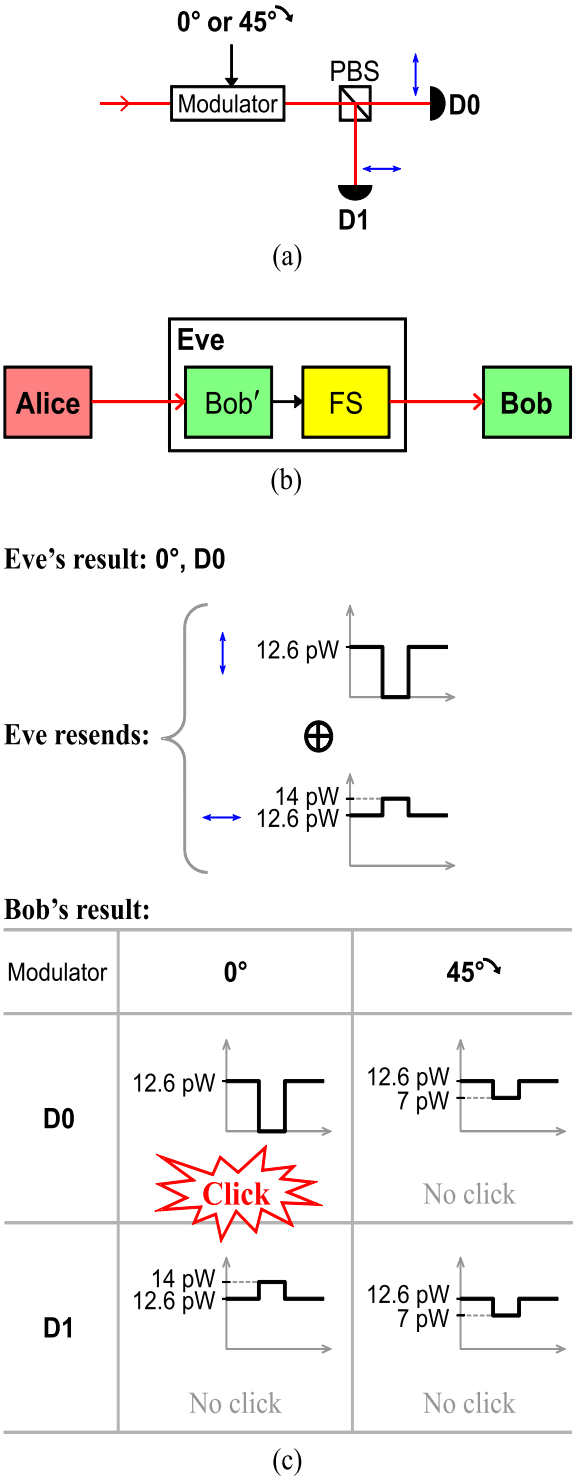

Figure 4. Proposed attack against a QKD system that uses two model 1 detectors: (a) equivalent optical scheme of Bob's setup; (b) scheme of the faked-state attack; (c) faked state sent by Eve in the case of her detection in the 0° basis with the result D0, and the intensity diagrams that result at Bob's detectors for his two possible basis choices. Optical losses in components are neglected; in the presence of losses, Eve should send a proportionally brighter faked state.

detectors. It would also be impractical for her to use exotic high-quantum-efficiency detectors working at cryogenic temperatures. Most practical for Eve would be to use a copy of Bob's actual setup for her Bob′, maybe with limited improvements. In this situation, Bob will observe loss of detection efficiency under attack, which equivalently appears to him as a sudden 4 dB additional loss in the line, and may trigger a security alarm. However, this would be a solvable problem for Eve in most of the real situations, because loss in the transmission line between Alice and Bob almost always exceeds 4 dB. Eve may place her detection unit closer to Alice. Thus, she excludes the loss in the length of the line between her detection unit and Bob. This compensates for the reduced 'detection efficiency' of her faked states at Bob. Eve could also try to improve the quantum efficiency of her detectors and reduce losses in Bob′ compared to those of Bob's setup. In free-space QKD, the losses Eve could try to reduce would include the coupling loss from Alice's free-space beam into the receiver telescope.

My attack is applicable to different protocols and schemes, when they use vulnerable detectors. The attack clearly applies to schemes with passive basis choice at Bob [5]–[7], [17], [21]–[30]. For these schemes, Eve should double the intensity of her faked states. The random basis choice by Bob is removed: Eve always gets to choose the basis for him. In the case of the BB84 protocol, the four cells in the table in figure 4(c) represent the intensity diagrams at Bob's four detectors. This is the case described in the abstract of this paper.

Besides polarization, another coding widely used in QKD is phase coding [31, 32]. If a scheme with phase coding employs vulnerable detectors, this attack can be run against it. For phase coding Eve shall, instead of the polarization components shown in figure 4(c), use components of faked state with 0 and π phase differences between the arms of the interferometer. The attack will also work on systems using the Scarani–Acin–Ribordy–Gisin 2004 (SARG04) protocol [33] and most of the decoy-state protocols [4, 5, 34, 35], as long as Bob is using passively quenched detectors. The decoy-state protocols referenced above do not help the legitimate users against this attack, because Eve does not measure photon number. She detects Alice's states with a faithful replica of Bob's setup and then simply forces her detection results onto Bob as transparently as she can. Finally, this attack is also applicable to the Bennett 1992 (B92) protocol [31], [36]–[42], to the Ekert protocol [43, 44], to the six-state protocol [45] and, under certain conditions, to secret sharing schemes [46].

For a practical implementation of the attack, it is important to consider all side effects it causes, and how to mask them so that Alice and Bob are not alarmed. One side effect, the less-than-unity 'detection efficiency' of the faked states at Bob, has been discussed above. Another side effect is the replacement of dark counts of Bob's detectors with dark counts of Eve's detectors. During the attack, Eve keeps Bob's detectors blinded when she is not sending faked states. Thus, they do not produce spontaneous counts. Instead, Eve has dark counts in her detectors and she cannot distinguish these from Alice's photons. She passes them on to Bob as faked states. Eve's detectors may have a lower ratio of dark counts to photon counts than Bob's. Eve is certainly allowed to achieve this in practice, either by using better detectors or by placing them closer to Alice (which she may have to do anyway). This may cause an overall reduction in the quantum bit error rate (QBER) experienced by Alice and Bob, and be noticed by them. If this becomes a problem, Eve can emulate additional dark counts by sending random faked states to Bob at random times. Similarly, optical imperfections at Bob that originally contributed to the QBER get replaced by the optical imperfections in Eve's copy of Bob's setup. (However, the optical imperfections at Bob may still make some contribution to the QBER through timing side effects during the attack, as will be shown in the next section.)

Side effects may arise when Eve begins and ends the attack. When she goes into the control mode by switching on the constant illumination, Bob's detectors will each produce a single click. These initial clicks at the beginning of the attack may register as one or more error bits in the key. However, this should not be a problem as long as Eve does not switch in and out of the attack mode too frequently. At the end of the attack, when Eve switches off the illumination, no extra clicks are produced except for, maybe, afterpulses with slightly increased probability than normal. Thus, at least in principle, Eve can begin and end this attack on a running quantum cryptolink.

Another side effect is the additional delay in the quantum channel caused by Eve. The major component of this delay is the gap width in the faked state. Eve begins forming the faked state immediately after detecting Alice's quantum state. However, the actual click at Bob occurs at the end of the gap, which comes 2 μs later. Thankfully, the time on Alice's and Bob's clocks is not authenticated in the QKD protocol. Many of the possibly affected QKD systems (listed in section 5) measure the time difference by the time of arrival of quantum states to Bob. In these systems, the additional 2 μs delay will easily be absorbed by the time synchronization algorithm. In case the delay ever becomes a problem for Eve, she may try a slightly different tactic. Eve could begin sending to Bob a faked state for a particular bit-basis combination before she actually detects it. Then, when she detects Alice's quantum state in this bit-basis combination, she instantly ends the gap and finishes the faked state. As will be shown in the next section, the gap in the faked state can be of variable width, so this tactic might work.

Finally, Eve must take into account two practical limitations of the hardware. One limitation is a finite extinction ratio of Bob's PBS, as well as Eve's finite precision in forming polarized light with exact parameters of polarization. The resulting imperfect splitting of the two faked state components at Bob's PBS leads to nonzero optical power in the gap on the control intensity diagram of the target detector. Another limitation is the time distribution of detector counts induced immediately after the end of the gap. This time distributon has a non-negligible width. These two limitations and their effects on the attack are considered in the next section.

4. Detector tests

In this section, I mainly consider time distribution of clicks induced by faked states. Many of the possibly affected QKD systems register the timing of detector output pulses with sub-nanosecond precision. The width of Bob's time bin in which clicks are accepted as belonging to a particular Alice's qubit can be of the order of 1 ns. Ideally, Eve's faked state should induce a click with sub-nanosecond time precision, to target the qubit time bin. However, as the tests show, the actual time distribution of the induced clicks is much wider.

The experimental tests of three different detector models are reported below.

4.1. Detector model 1

This detector model is based on a solder-it-yourself printed circuit board developed by Kurtsiefer *et al*. Being a low-cost, simple and compact design, it is used in several laboratories around the world. The equivalent diagram of the signal part of the circuit is shown in figure 2(a). The particular sample I have tested features a multivibrator pulse duration of about 10 μs, while it is usually made orders of magnitude shorter in this circuit.

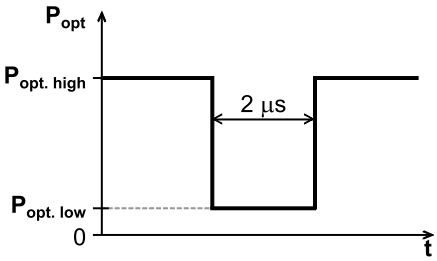

Figure 5. Detector model 1: control intensity diagram during testing. It was applied at 1 kHz repetition rate.

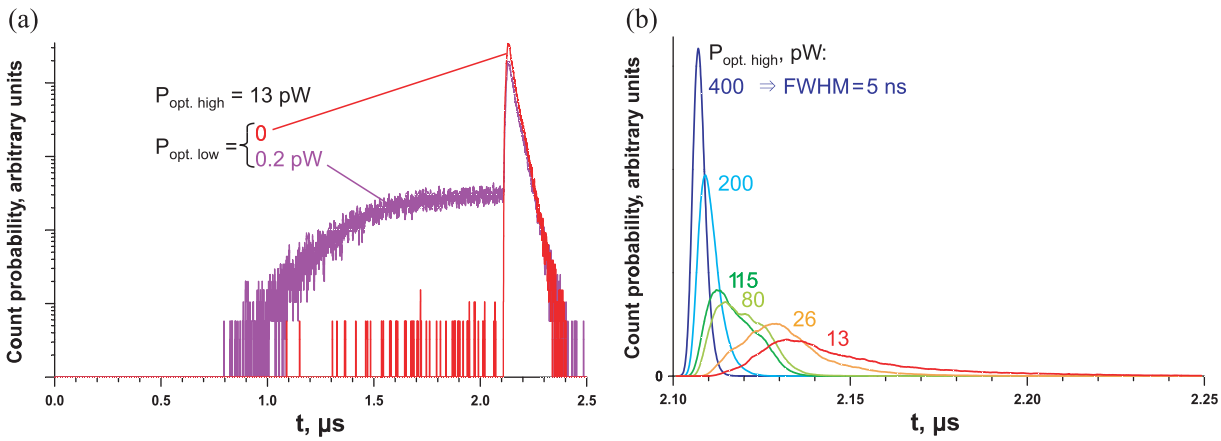

Figure 6. Detector model 1: time distributions of pulse's leading edge at the detector output, when Eve controls it by constant illumination with an approximately 2 μs wide gap: (a) time distributions for zero and nonzero $P_{\text{opt. low}}$ (at $P_{\text{opt. high}} = 13$ pW); (b) time distributions in the main response peak for a range of $P_{\text{opt. high}}$ values (at $P_{\text{opt. low}} = 0$). On the charts, $t = 0$ approximately corresponds to the start of the gap in illumination; the main response peak begins just after the end of the gap.

The detector has been tested under an input illumination time diagram shown in figure 5. Laser illumination at 820 nm wavelength was applied uniformly over the entire photosensitive area of the APD 0.5 mm in diameter[2]. The optical power values P_{opt} are calculated as the total power impinging on the photosensitive area. I have tested the detector at both zero and nonzero power levels in the gap $P_{\text{opt. low}}$.

Figure 6(a) shows a typical time distribution of the SPD output pulses and what effects the nonzero power in the gap has on this time distribution. During approximately the first 1 μs of the gap, the SPD does not produce output pulses at all. After 1 μs, some premature output pulses appear. When there is no illumination in the gap ($P_{\text{opt. low}} = 0$), the average rate of these pulses is, at the parameters for which the chart is plotted, between three and four times the normal dark count rate (of about 100 cps). After the end of the gap, there is a major response peak of a certain width. Nonzero illumination in the gap causes two effects. Firstly, the probability of premature

[2] A detailed description of the testing setup can be found in the first version of this paper, arXiv:0707.3987v1 [quant-ph].

output pulses greatly increases, as can be seen on the $P_{\text{opt. low}} = 0.2\,\text{pW}$ curve. Secondly, the probability of output pulses in the main response peak decreases.

The width of the main response peak can be reduced by increasing $P_{\text{opt. high}}$, as shown in figure 6(b). 5 ns full-width at half-maximum (FWHM), or 10 ns width as measured near the base of the peak at the 2% magnitude level, has been achieved at $P_{\text{opt. high}} = 400\,\text{pW}$. The width could likely be decreased further at higher levels of $P_{\text{opt. high}}$; however, I did not test beyond 400 pW with this detector model. The detector response in the main peak is a single-photon click, as suggested by the exponentially decaying tail of the time distribution and by an estimate of the number of photons impinging on the APD in a unit of time. It is possible that multi-photon effects influence the time distribution at higher levels of $P_{\text{opt. high}}$; however, there was no practical way of testing this. I have not investigated which effect is responsible for the gradual rising edge of the main response peak in this test.

As you see, the total width of the time distribution, including the premature clicks, is more than 1 μs. The practical significance of this wide time distribution varies a lot depending on how Bob treats clicks falling outside his qubit time bin (which is always much narrower than 1 μs). If all or most of these clicks are simply disregarded by him, this is not much of a problem for Eve. In this case, she only faces an additional reduction in the 'detection efficiency' of her faked states at Bob, which could be compensated as discussed in the previous section. If, however, clicks registered by Bob outside the proper qubit time bin contribute to the QBER (by falling into adjacent qubit time bins) or trigger an alarm condition, then Eve faces more stringent requirements. How these clicks are actually treated depends on implementation details and algorithms in each particular QKD system under attack, which I do not consider here. The relevant implementation details are usually not reported in papers to the required extent, so experimenting with each QKD system will be necessary.

We can still estimate how bad this problem can be by considering one of the worst possible cases for Eve. While the width of the main response peak can be reduced by increasing $P_{\text{opt. high}}$, the premature counts in the gap are always distributed over a wide time span. I assume that all these premature counts fall into wrong qubit time bins at Bob. This can happen in a high-speed QKD system with qubit time bins following each other with no gaps between them, and passive basis choice at Bob. In the BB84 protocol, a count falling into a wrong qubit bin has 25% chance of causing an error in the sifted key (a combination of 50% chance of being in a compatible basis and 50% chance of having a wrong bit value). At the same time, I assume that all counts in the main peak fall into the proper time bin and register as error-free key bits. To avoid being discovered, Eve needs to maintain the QBER at approximately the same level as before her attack. The premature counts are caused by nonzero optical power in the gap, which is caused in part by imperfect optical alignment between Eve and Bob. To estimate the required quality of optical alignment, I have measured time distributions at several values of $P_{\text{opt. low}}$ (at $P_{\text{opt. high}} = 13\,\text{pW}$ and gap width of 2 μs). From the obtained data, I have calculated the probability ratio of having a premature click to having a click in the main response peak, for each used value of $P_{\text{opt. low}}$. The measurement has shown that this probability ratio rises approximately linearly with $P_{\text{opt. low}}$. If we additionally assume that this effect is the main contribution to the QBER and that Eve uses the intensity diagrams with power levels as given in figure 4(c), then the measurement data suggest

$$\text{QBER} \approx \frac{4.2}{r_{\text{e}}}, \tag{1}$$

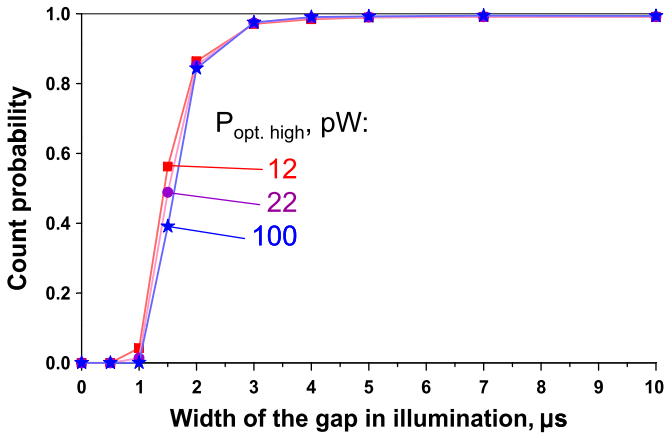

Figure 7. Detector model 1: Eve's probability of producing a pulse at the detector output versus width of the gap in illumination (at $P_{\text{opt. low}} = 0$).

where r_e is an extinction ratio between Bob's two detectors in the target basis achieved by Eve. Thus, to match values of the QBER in the 2–5% range typically observed in QKD systems, Eve may need to achieve r_e in the 19–23 dB range (or higher if other sources of errors are significant). This would be possible if the native extinction ratio of Bob's PBS exceeds r_e; this depends on the type of PBS used. Then, Eve would face a rather strong but probably realistic requirement on the precision of her polarization alignment. To narrow down the assumptions made in this assessment one would need to analyze and attack a concrete QKD implementation. This could be a task for the future.

Finally, figure 7 shows how the probability of inducing the output pulse depends on the gap width. I have chosen the gap width of 2 μs for all the other measurements with this detector, to achieve the count probability reasonably close to 1 without making the gap unnecessarily wide. As you can see, the count probability for a 2 μs or wider gap almost does not depend on $P_{\text{opt.high}}$. Interestingly, although the count probability exceeds 0.99 at gap widths larger than 5 μs, it never becomes exactly 1.

In these measurements, the gap repetition rate was 1 kHz. However, I have verified that, if necessary, the gap repetition rate can be increased to the limit. When the gaps follow each other in close succession (with less than 2 μs between them), they still cause clicks at the SPD output.

4.2. Detector model 2

This detector model is SPCM-200-PQ, industrially produced by EG&G in the 1990s. While testing this model, I have focused on reducing the width of the main response peak. To achieve this goal, an improved control intensity diagram, shown in figure 8, has been used. A 780 nm illumination formed by mixing signals from two semiconductor lasers was applied uniformly over the entire photosensitive area of the APD 0.15–0.2 mm in diameter. The optical power at the APD is kept at the minimum blinding level $P_{\text{blind}} = 280$ pW most of the time. In the beginning of the gap, a short brighter pulse **A** is applied. The purpose of this pulse is to discharge the capacitances in the SPD to about the same level every time in the beginning of the gap. Then the recharging process always starts at the same voltage and time, which leads to a certain voltage being applied to the APD at the end of the gap. If the pulse **A** is absent, the recharge process

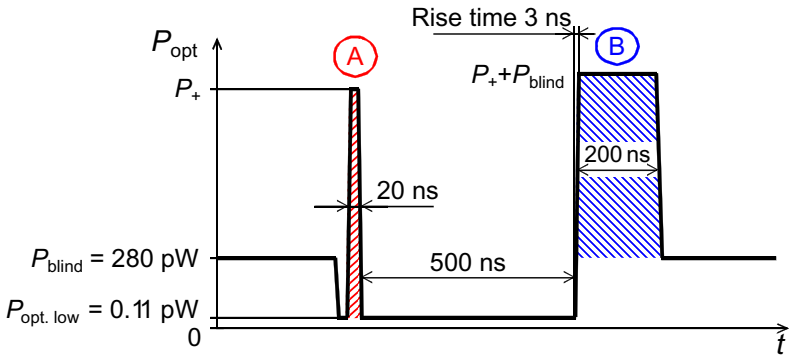

Figure 8. Detector model 2: control intensity diagram during testing. It was applied at 10 kHz repetition rate.

starts at a random time of the last occurrence of avalanche before the gap. In this case, the APD voltage at the end of the gap varies, which leads to increased jitter in the single photon response [16]. The gap ends with another brighter pulse **B**, which guarantees the arrival of the first few photons at the APD within a very short time. To fulfill this purpose, the pulse **B** does not have to be long. However, the tested detector sample tended to produce double output pulses when P_{blind} was applied near the end of its first output pulse. Extending the length of the bright pulse **B** to 200 ns reduced the probability of another output pulse appearing after the first one from 8 to 0.5%. In the 500 ns wide gap, illumination at the power level 34 dB below P_{blind} was applied to the detector, to simulate imperfect polarization splitting at Bob's PBS.

The resulting time distribution of the SPD output pulses is shown in figure 9. At 0.22 μW peak power in the optical pulses **A** and **B**, the main response peak on the time distribution is 0.92 ns wide. The familiar premature counts in the gap are present on this time distribution, as well as delayed counts after the main peak. The latter can probably be attributed to small avalanches occurring early in the gap, resulting in delayed detector response after the end of the gap. The total probability, including the premature and delayed counts, of the detector producing a click in response to the control diagram is very close to 1.

The presence of both brighter optical pulses **A** and **B** on the control diagram is necessary to achieve the narrowest width of the main response peak. Figure 10 shows how the width depends on the presence of each of these pulses and on the peak power in them.

4.3. Detector model 3

This detector model is used in a compact passive polarization analyzer module in Bob in a daylight free-space QKD system [17]. The system has been developed at the Centre for Quantum Technologies in Singapore. We have tested all four detector channels. Unlike the previous two experiments, in this one we did not have physical access to measure absolute power impinging on the APDs. The saturation curves for model 3 in figure 1 are scaled based on a guess that the detector quantum efficiency in the linear part of the curves was around 50%.

On this QKD system, Q Liu and I have demonstrated that the Bob control method proposed in section 3 works and that the detectors are individually addressable with sub-nanosecond jitter.

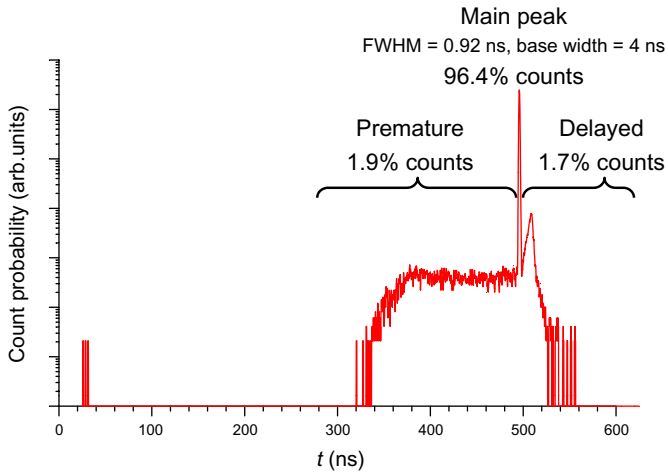

Figure 9. Detector model 2: time distribution of pulse's leading edge at the detector output, when Eve controls it by an intensity diagram in which both parts **A** and **B** are present, at $P_+ = 784 P_{\text{blind}} = 0.22\,\mu\text{W}$.

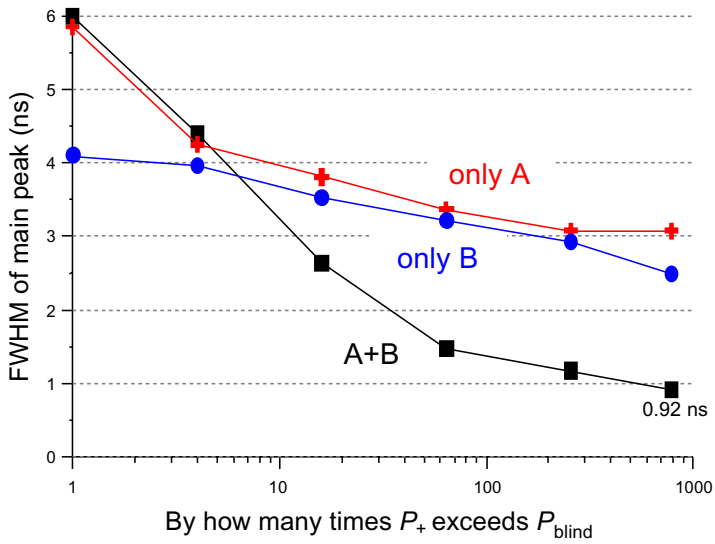

Figure 10. Detector model 2: width of the main response peak versus excess optical power P_+ in the parts **A** and **B** of the control intensity diagram. Three cases are charted: only part **A** is present on the control diagram (while **B** is not), only part **B** is present (while **A** is not), and both parts **A** and **B** are present simultaneously. Note that the leftmost point on the 'only **A**' curve corresponds to roughly the same shape of the control diagram as was used for testing the detector model 1: a gap in constant illumination at the minimum blinding intensity.

We used polarization faked states that resulted in a control intensity diagram at the APDs similar to the one in figure 8. This will be reported in a separate paper [18].

From the experiments reported above, it appears that Eve might in practice be able to control passively quenched detectors well enough to attack a real QKD system.

5. Possibly affected systems and countermeasures

Currently, there are at least 28 papers reporting different QKD experiments that employ non-gated Si APDs. The breakdown of these papers is as follows. Eight of them reported the use of passively quenched APDs [5, 17, 22, 25, 29, 44, 47, 48], ten reported the use of non-gated, actively quenched APDs [26, 30, 36, 37], [39]–[42], [49, 50], and another ten did not specify the type of quenching, only saying that Si APDs or 'detectors' (which I assume were Si APDs) were used [6, 7, 21, 23, 24, 27, 28, 38, 51, 52]. I have since learned that three of the latter ten experiments [6, 7, 28] did in fact use passively quenched detectors of a design very similar to the models 1 and 3 studied in this paper. Thus, it appears that passively quenched and actively quenched Si APDs are equally frequently used in QKD experiments. I remark that at least one model of actively quenched Si SPD has been shown to be vulnerable to a somewhat similar attack also involving bright illumination [13].

Continued frequent use of passive quenching can be explained by its practical properties. It is well known that an actively quenched APD delivers superior count rate and timing characteristics [16, 53]. However, a passively quenched circuit is simpler, cheaper and more versatile; the biasing parameters are easy to adjust; a larger photosensitive area APD can be used than those embedded in commercially available actively quenched detector modules. At the same time, the performance of the passively quenched SPD is often adequate for the task. For example, in the 144 km QKD experiments [5, 6], laboratory-made passively quenched detectors were used because the average count rate at Bob was low [54].

Unfortunately, none of the 28 experiments in my sampling of the literature seemed to implement any countermeasure against bright-light attacks (with the possible exception of [37] where Eve's illumination might accidentally cause Bob's separate timing detector to work incorrectly). Nor do I know of any SPD module with a specified guaranteed behavior under bright-light illumination or equipped with an extra output that signals saturation or blinding.

It may appear that introducing authenticated timing into the QKD protocol can prevent my attack. However, Eve can try a slightly different tactic discussed in section 3, by starting to form a faked state before the actual detection occurs in Bob′. This tactic may in practice allow her to mimic the timing of Bob's clicks with just a few ns extra delay. Additionally, when the QKD system uses an optical fiber [25], Eve can gain time by routing her classical communication from Bob′ to the FS (see figure 4(b)) via a radio link in which signals propagate faster than in the fiber. Authenticated timing does not prevent the detector controllability, and thus is not a complete solution.

Other researchers have proposed to equip each SPD with a 'detector ready' signal that is only present when the voltage at the APD guarantees certain minimum quantum efficiency [55]. I think this is a promising idea. These 'detector ready' signals from all of Bob's SPDs can be combined on an AND-gate and used to disable/enable click recording from all SPDs simultaneously by Bob's electronic registration system. Besides preventing the bright-light attacks, this would also be useful to thwart subtler exploits. This circuit introduces registration blanking time for all detectors simultaneously whenever at least one of them is insensitive to photons after an avalanche. Rejecting clicks that occur whenever at least one detector is having a deadtime seems to be a necessary security measure in any QKD system [55]. Additionally, this photon registration system can guarantee a certain quantified minimum quantum efficiency of each detector whenever the system is recording clicks. This guarantee may be required by a general security proof that takes into account equipment imperfections [56].

Once a hack-proofed system is built, it would have to be tested thoroughly under bright-light illumination with various temporal diagrams over a wide input intensity range. Ideally, the testing should include higher input power levels up to and above the damage threshold of Bob's optics.

6. Conclusion

In this paper, I have shown how the saturation and blinding behavior of the passively quenched APD can be used to gain control over detectors and stage an attack against a QKD system. Passively quenched detectors of three different models have been experimentally tested and their control demonstrated by the same method, under realistic conditions. It would now be interesting to demonstrate a complete attack against a running QKD system.

Acknowledgments

The author is grateful for hospitality, assistance, useful discussions and a loan of equipment to Sergei Kulik and his colleagues at the Laboratory of Spontaneous Parametric Down-Conversion at Moscow State University; to Oleg Kotov and his colleagues at the Fiber Optics Laboratory at St Petersburg State Polytechnical University; to Alexander Ushakov; to Christian Kurtsiefer, Ilja Gerhardt and colleagues at the Centre for Quantum Technologies in Singapore. The author thanks the anonymous reviewer for a valuable critique of the first version of this paper. Johannes Skaar and Lars Lydersen are thanked for comments on the manuscript. Financial support from NTNU, the Research Council of Norway (grant no. 180439/V30) and the Korea Science and Engineering Foundation (grant no. R01-2006-000-10354-0) is acknowledged. This work was also partially supported by the National Research Foundation and the Ministry of Education, Singapore.

References

[1] Bennett C H, Bessette F, Brassard G, Salvail L and Smolin J 1992 *J. Cryptol.* **5** 3

[2] Scarani V, Bechmann-Pasquinucci H, Cerf N J, Dušek M, Lütkenhaus N and Peev M 2008 arXiv:0802.4155 [quant-ph]

Gisin N, Ribordy G, Tittel W and Zbinden H 2002 *Rev. Mod. Phys.* **74** 145

[3] Takesue H, Nam S W, Zhang Q, Hadfield R H, Honjo T, Tamaki K and Yamamoto Y 2007 *Nat. Photonics* **1** 343

Hiskett P A, Rosenberg D, Peterson C G, Hughes R J, Nam S, Lita A E, Miller A J and Nordholt J E 2006 *New J. Phys.* **8** 193

Kimura T, Nambu Y, Hatanaka T, Tomita A, Kosaka H and Nakamura K 2004 *Japan. J. Appl. Phys.* **43** L1217

Gobby C, Yuan Z and Shields A 2004 *Appl. Phys. Lett.* **84** 3762

Takesue H, Diamanti E, Honjo T, Langrock C, Fejer M M, Inoue K and Yamamoto Y 2005 *New J. Phys.* **7** 232

[4] Rosenberg D, Harrington J W, Rice P R, Hiskett P A, Peterson C G, Hughes R J, Lita A E, Nam S W and Nordholt J E 2007 *Phys. Rev. Lett.* **98** 010503

Peng C-Z, Zhang J, Yang D, Gao W-B, Ma H-X, Yin H, Zeng H-P, Yang T, Wang X-B and Pan J-W 2007 *Phys. Rev. Lett.* **98** 010505

Yin Z-Q, Han Z-F, Chen W, Xu F-X, Wu Q-L and Guo G-C 2008 *Chin. Phys. Lett.* **25** 3547

[5] Schmitt-Manderbach T *et al* 2007 *Phys. Rev. Lett.* **98** 010504
[6] Ursin R *et al* 2007 *Nat. Phys.* **3** 481
[7] Kurtsiefer C, Zarda P, Halder M, Weinfurter H, Gorman P M, Tapster P R and Rarity J G 2002 *Nature* **419** 450
Kurtsiefer C, Zarda P, Halder M, Gorman P M, Tapster P R, Rarity J G and Weinfurter H 2002 *Proc. SPIE* **4917** 25
[8] Lydersen L and Skaar J 2008 arXiv:0807.0767 [quant-ph]
Fung C-H F, Tamaki K, Qi B, Lo H-K and Ma X 2009 *Quantum Inf. Comput.* **9** 0131
Gottesman D, Lo H-K, Lütkenhaus N and Preskill J 2004 *Quantum Inf. Comput.* **4** 325
Shor P W and Preskill J 2000 *Phys. Rev. Lett.* **85** 441
Koashi M and Preskill J 2003 *Phys. Rev. Lett.* **90** 057902
Biham E, Boyer M, Boykin P O, Mor T and Roychowdhury V 2000 *Proc. 32nd Annu. ACM Symp. on Theory of Computation* (New York: ACM Press) pp 715–24
Inamori H, Lütkenhaus N and Mayers D 2007 *Eur. Phys. J.* D **41** 599
[9] Kurtsiefer C, Zarda P, Mayer S and Weinfurter H 2001 *J. Mod. Opt.* **48** 2039
[10] Vakhitov A, Makarov V and Hjelme D R 2001 *J. Mod. Opt.* **48** 2023
Gisin N, Fasel S, Kraus B, Zbinden H and Ribordy G 2006 *Phys. Rev.* A **73** 022320
[11] Makarov V and Hjelme D R 2005 *J. Mod. Opt.* **52** 691
[12] Makarov V, Anisimov A and Skaar J 2006 *Phys. Rev.* A **74** 022313
Qi B, Fung C-H F, Lo H-K and Ma F-X 2007 *Quantum Inf. Comput.* **7** 73
Zhao Y, Fung C-H F, Qi B, Chen C and Lo H-K 2008 *Phys. Rev.* A **78** 042333
Makarov V and Skaar J 2008 *Quantum Inf. Comput.* **8** 0622
Lamas-Linares A and Kurtsiefer C 2007 *Opt. Express* **15** 9388
[13] Makarov V, Anisimov A and Sauge S 2008 arXiv:0809.3408 [quant-ph]
[14] Kerckhoffs A 1883 *J. Sci. Militaires* **IX** 5–38
[15] Haitz R H 1964 *J. Appl. Phys.* **35** 1370
Haitz R H 1965 *J. Appl. Phys.* **36** 3123
[16] Cova S, Ghioni M, Lacaita A, Samori C and Zappa F 1996 *Appl. Opt.* **35** 1956
[17] Peloso M P, Gerhardt I, Ho C, Lamas-Linares A and Kurtsiefer C 2009 *New J. Phys.* **11** 045007
[18] Liu Q *et al* in preparation
[19] Dautet H, Deschamps P, Dion B, MacGregor A D, MacSween D, McIntyre R J, Trottier C and Webb P P 1993 *Appl. Opt.* **32** 3894
[20] Bennett C H and Brassard G 1984 *Proc. IEEE Int. Conf. on Computers, Systems and Signal Processing* (New York: IEEE Press) pp 175–9
[21] Rarity J G, Gorman P M and Tapster P R 2001 *Electron. Lett.* **37** 512
[22] Hughes R J, Nordholt J E, Derkacs D and Peterson C G 2002 *New J. Phys.* **4** 43
[23] Beveratos A, Brouri R, Gacoin T, Villing A, Poizat J-P and Grangier P 2002 *Phys. Rev. Lett.* **89** 187901
[24] Alléaume R, Treussart F, Messin G, Dumeige Y, Roch J-F, Beveratos A, Brouri-Tualle R, Poizat J-P and Grangier P 2004 *New J. Phys.* **6** 92
[25] Poppe A *et al* 2004 *Opt. Express* **12** 3865
[26] Resch K J *et al* 2005 *Opt. Express* **13** 202
[27] Peng C-Z *et al* 2005 *Phys. Rev. Lett.* **94** 150501
[28] Schmitt-Manderbach T, Weier H, Regner N, Kurtsiefer C and Weinfurter H 2005 *Proc. Quantum Electronics Conf. EQEC'05* p 305
Weier H, Schmitt-Manderbach T, Regner N, Kurtsiefer C and Weinfurter H 2006 *Fortschr. Phys.* **54** 840
[29] Marcikic I, Lamas-Linares A and Kurtsiefer C 2006 *Appl. Phys. Lett.* **89** 101122
[30] Erven C, Couteau C, Laflamme R and Weihs G 2008 *Opt. Express* **16** 16840
[31] Bennett C H 1992 *Phys. Rev. Lett.* **68** 3121

[32] Townsend P D, Rarity J G and Tapster P R 1993 *Electron. Lett.* **29** 634
Marand C and Townsend P D 1995 *Opt. Lett.* **20** 1695
[33] Scarani V, Acin A, Ribordy G and Gisin N 2004 *Phys. Rev. Lett.* **92** 057901
Acin A, Gisin N and Scarani V 2004 *Phys. Rev.* A **69** 012309
Branciard C, Gisin N, Kraus B and Scarani V 2005 *Phys. Rev.* A **72** 032301
[34] Hwang W-Y 2003 *Phys. Rev. Lett.* **91** 057901
Zhao Y, Qi B, Ma X, Lo H-K and Qian L 2006 *Phys. Rev. Lett.* **96** 070502
Hasegawa J, Hayashi M, Hiroshima T, Tanaka A and Tomita A 2007 arXiv:0705.3081v1 [quant-ph]
[35] Mauerer W and Silberhorn C 2007 *Phys. Rev.* A **75** 050305
[36] Buttler W T, Hughes R J, Kwiat P G, Lamoreaux S K, Luther G G, Morgan G L, Nordholt J E, Peterson C G and Simmons C M 1998 *Phys. Rev. Lett.* **81** 3283
[37] Buttler W T, Hughes R J, Lamoreaux S K, Morgan G L, Nordholt J E and Peterson C G 2000 *Phys. Rev. Lett.* **84** 5652
[38] Bienfang J C, Gross A J, Mink A, Hershman B J, Nakassis A, Tang X, Lu R, Su D H, Clark C W and Williams C J 2004 *Opt. Express* **12** 2011
[39] Shan X, Sun X, Luo J, Tan Z and Zhan M 2006 *Appl. Phys. Lett.* **89** 191121
[40] Gordon K J, Fernandez V, Townsend P D and Buller G S 2004 *IEEE J. Quantum Electron.* **40** 900
[41] Gordon K J, Fernandez V, Buller G S, Rech I, Cova S D and Townsend P D 2005 *Opt. Express* **13** 3015
[42] Fernandez V, Collins R J, Gordon K J, Townsend P D and Buller G S 2007 *IEEE J. Quantum Electron.* **43** 130
[43] Ekert A K 1991 *Phys. Rev. Lett.* **67** 661
[44] Ling A, Peloso M P, Marcikic I, Scarani V, Lamas-Linares A and Kurtsiefer C 2008 *Phys. Rev.* A **78** 020301
[45] Bruß D 1998 *Phys. Rev. Lett.* **81** 3018
Bechmann-Pasquinucci H and Gisin N 1999 *Phys. Rev.* A **59** 4238
Bennett C H, Brassard G, Breidbart S and Wiesner S 1984 *IBM Tech. Discl. Bull.* **26** 4363
[46] Gaertner S, Kurtsiefer C, Bourennane M and Weinfurter H 2007 *Phys. Rev. Lett.* **98** 020503
Schmid C, Trojek P, Gaertner S, Bourennane M, Kurtsiefer C, Zukowski M and Weinfurter H 2006 *Fortschr. Phys.* **54** 831
Schmid C, Trojek P, Bourennane M, Kurtsiefer C, Żukowski M and Weinfurter H 2005 *Phys. Rev. Lett.* **95** 230505
[47] Kurochkin V L, Ryabtsev I I and Neizvestny I G 2005 *Tech. Phys.* **50** 727
[48] Duligall J L, Godfrey M S, Harrison K A, Munro W J and Rarity J G 2006 *New J. Phys.* **8** 249
[49] Buttler W T, Hughes R J, Kwiat P G, Luther G G, Morgan G L, Nordholt J E, Peterson C G and Simmons C M 1998 *Phys. Rev.* A **57** 2379
[50] Thew R T, Tanzilli S, Krainer L, Zeller S C, Rochas A, Rech I, Cova S, Zbinden H and Gisin N 2006 *New J. Phys.* **8** 32
[51] Jacobs B C and Franson J D 1996 *Opt. Lett.* **21** 1854
[52] Waks E, Inoue K, Santori C, Fattal D, Vuckovic J, Solomon G S and Yamamoto Y 2002 *Nature* **420** 762
[53] Cova S, Ghioni M, Lotito A, Rech I and Zappa F 2004 *J. Mod. Opt.* **51** 1267
[54] Ursin R 2007 private communication
[55] Experimental Quantum Physics Group at Ludwig-Maximilians-Universität Munich 2008 private communication
[56] Skaar J 2009 private communication