Quantum eavesdropping without interception: an attack exploiting the dead time of single-photon detectors

Henning Weier¹,²,⁴, Harald Krauss¹, Markus Rau¹, Martin Fürst¹,², Sebastian Nauerth¹,² and Harald Weinfurter¹,³

¹ Fakultät für Physik, Ludwig-Maximilians-Universität, 80799 Munich, Germany
² Qutools GmbH, 80539 Munich, Germany
³ Max-Planck-Institut für Quantenoptik, 85748 Garching, Germany
E-mail: henning.weier@lmu.de

New Journal of Physics 13 (2011) 073024 (10pp)
Received 27 January 2011
Published 15 July 2011
Online at http://www.njp.org/
doi:10.1088/1367-2630/13/7/073024

Abstract. The security of quantum key distribution (QKD) can easily be obscured if the eavesdropper can utilize technical imperfections in the actual implementation. Here, we describe and experimentally demonstrate a very simple but highly effective attack that does not need to intercept the quantum channel at all. Only by exploiting the dead time effect of single-photon detectors is the eavesdropper able to gain (asymptotically) full information about the generated keys without being detected by state-of-the-art QKD protocols. In our experiment, the eavesdropper inferred up to 98.8% of the key correctly, without increasing the bit error rate between Alice and Bob significantly. However, we find an even simpler and more effective countermeasure to inhibit this and similar attacks.

The communication of sensitive data has become part of our everyday life, resulting in a growing need for mechanisms that ensure secure transmissions of these data. The secrecy of the information transfer can be guaranteed using a classical cryptographic method called the one-time pad. This method enables unconditionally secure communication provided that the exchange of the cryptographic key has been perfectly secure. In 1984 Bennett and Brassard showed that this can indeed be achieved using quantum cryptography, or more
precisely quantum key distribution (QKD) [1, 2], an approach that employs non-orthogonal quantum states to encode information. In recent years there have been remarkable QKD experiments pushing the limits in distance and/or key rate [3–6], as well as the level of applicability, achieving network functionality [7–9] with the first systems for quantum-secured communication becoming commercially available.

However, what does ‘secure’ mean? Today, there exist security proofs [10, 11] showing that the ideal protocol is secure in the sense that any knowledge of an eavesdropper about the key can be quantified and consequently made negligibly small. However, these proofs rarely specify requirements for QKD hardware and, if they do, real implementations will usually not fully comply with these specifications. This can lead to new types of attack that are not covered by the proofs and hence will not be revealed by standard security tests. Recently, considerable effort has been made to reveal these potential threats [12–17] and to find countermeasures [18–24]. Many attacks are designed only for very specific systems and/or require sophisticated technology that is not yet (public) state-of-the-art.

In this paper, we introduce a novel type of attack that does not even need to intercept the qubits sent over the quantum channel. We show how to utilize an imperfection, which almost all QKD systems display, namely the fact that common single-photon detectors are rendered inactive for a period of time (called dead time) after a detection event. This enables the eavesdropper to uncover the full key without significantly changing the quantum bit error ratio (QBER) while using very simple equipment. On the one hand, we demonstrate that this new attack renders a conventional QKD system absolutely insecure, but, on the other, we also provide an effective countermeasure.

There are two characteristic features of nearly all QKD systems implemented so far. The first is the fact that when a single photon avalanche detector (SPAD) registers a photon, there usually follows a period of time during which it will not be able to detect a second event. This period (called dead time $\tau_D$) can range from less than a nanosecond to some tens of microseconds. The second feature is the periodic operation: the transmitter emits signals only at well-defined times $t_i = i \cdot T$, with period $T$. Consequently, in order to reduce noise originating from intermediate dark counts and scattering events, the receiver accepts a detection event only during a narrow time window ($\Delta_{tw} \ll T$) around $t_i$—all events outside these time windows are discarded.5

Several attacks have been proposed that make use of the dead time of SPADs to enable intercept–resend eavesdropping strategies [26–28]. Effectively, for these attacks the eavesdropper employs a sophisticated intercept–resend setup and uses bright light to gain full control over the SPADs of the receiver and to generate detection events equal to his own. The attack demonstrated here is technically much simpler and it does not intercept the quantum channel, and nor does it require bright light to control the receiver or to spy on the system via a Trojan horse attack. Rather, it utilizes the fact that dead times enable the eavesdropper to manipulate the detection efficiencies for a short time around $t_i$ by blinding some of the installed detectors. Although the eavesdropper does not need to intercept the qubits sent over the quantum channel, she can reveal the full key without being detected.

For our blinding attack, the eavesdropper (Eve) simply sends attenuated light pulses of one of the four polarizations used in the protocol (i.e. $H, V, +45^\circ$ or $-45^\circ$), into the quantum channel at time $t_{B,i}$, shortly (less than $\tau_D$) before $t_i$ and of course still outside of Bob’s time

5 This attack thus also applies to gated detector systems as long as $\Delta_{tw} < t_{act}$, the time during which the detector is activated.
window \((\Delta_{tw}/2 < t_i - t_{B,i} < \tau_D)\). Depending on the intensity and polarization of the pulse, Bob’s SPADs detect this light with a certain probability, except for the SPAD detecting the orthogonal polarization. Bob then is partially blinded (note that in QKD protocols the events caused by blinding pulses are not taken into account as they are outside of Bob’s time window) and if he agrees with Alice on using a particular event in the sifting phase, Eve will have significant information about the respective key bit as it could have been detected only by detectors that have not been blinded. Eve can easily tune the intensity of her blinding pulses and thus the information about the key. As it turns out, dim pulses containing only a few photons are sufficient to determine almost all of the key (appendices).

In the following, we describe a model QKD device that employs a BB84 protocol \([1]\) with the polarization of single photons or attenuated light pulses encoding the qubits. The general principle can easily be transferred to nearly all other QKD systems \([6, 29]\). We set up a copy of our free space QKD system \([7, 25]\) in the laboratory. There, Alice used a four-diode transmitter and was connected by a short free space quantum channel to Bob’s four-SPAD receiver module (figure 1(a)). Both transmitter and receiver units were fully computer controlled and ran a real-time BB84 protocol. Additionally, Eve coupled dim pulses from a transmitter module, similar to the Alice module, into the quantum channel. For easier synchronization with Alice and Bob, control signals for the Eve module were obtained from Alice’s controller.

The timing was set such that Alice’s signal pulses were sent with a period of \(T = 4\ \mu\text{s}\) (long enough to allow the SPADs to recover with a high probability between two consecutive signal pulses and to guarantee unbiased detections). In accordance with the timing conditions of our setup \((\tau_D \sim 0.5\ \mu\text{s}, \Delta_{tw} = 5\ \text{ns})\), the randomly polarized blinding pulses were sent 200 ns before the signal pulses. The mean photon number \(\mu_B^{\text{eff}} := \eta_B \mu_B\) of the blinding pulses was set by inserting different combinations of neutral density filters. Here, \(\mu_B^{\text{eff}}\) constitutes the mean photon number per pulse Eve would have to send into an ideal detector module (regarding transmission and detector efficiency), built as depicted in figure 1. \(\eta_B\) describes the transmission from Eve to Bob. Uniform, but non-unity transmission and detector efficiencies can be included here. For receiver modules with active basis switching (two detectors), only half of the blinding pulse intensity is necessary.

Eve’s key was deduced solely from the knowledge about the setting of her blinding pulses and from eavesdropping on the classical communication between Alice and Bob. To demonstrate the efficiency of this attack, Eve applied different blinding intensities during regular runs of the BB84 protocol between Alice and Bob. The calculated blinding pulse detection probabilities (figure 2(a)) are in good agreement with the experimental data, particularly for low blinding pulse intensities \(\mu_B^{\text{eff}}\). For higher values of \(\mu_B^{\text{eff}}\), the predictions differ mainly because of a higher number of background events due to increased spontaneous emissions from Eve’s laser diodes between the pulses. These, too, can render the detectors inactive and thus reduce the probability for multi-photon detection events due to blinding pulses. In our experiment, no hardware gating is used, i.e. the SPADs are in principle always active. However, as gate times are device information we can safely assume that the eavesdropper knows about the timing of the detector efficiency relative to the signal pulses and will act accordingly.

As expected, for low blinding pulse intensities Eve’s attack has only a low probability of success and her key is hardly correlated with the sifted key between Alice and Bob. However, by slightly increasing the power of her pulses, the match between the keys rises rapidly. The maximum observed overlap between Bob’s and Eve’s sifted keys was as high as 98.83% at a blinding pulse mean photon number of only \(\mu_B^{\text{eff}} = 16.52\), corresponding to a mutual information
Figure 1. (a) Schematic drawing of the setup: the transmitter (Alice) on the left, her pulses marked blue, the eavesdropper (Eve) in the center, her pulses marked red, and the receiver (Bob) on the right. The latter performs a state analysis with four detectors and passive optical components. The module utilizes a first non-polarizing 50/50 beam splitter (BS), which effectively serves as a (quantum) random basis switch, such that if the incident photon is reflected and detected behind a polarizing beam splitter (PBS) it is analyzed in the $H/V$ basis, whereas if it is transmitted by the BS and a half-wave plate at $22.5^\circ$ and detected behind a second PBS, it is analyzed in the $\pm 45^\circ$ basis. In this example, when Eve sent a light pulse polarized in one of the four polarizations (here $-45^\circ$), up to three of Bob’s detectors (in this example $H$, $-45^\circ$ and $V$, red) become inactive with a certain probability. Eve thus knows that Alice’s signal pulse can only be detected in the remaining detector (here $+45^\circ$) and can infer the respective key bit. (b) Relative efficiency for a second detection event after a detection at $t=0$ (appendices), together with the timing of Eve’s blinding pulses at $t_{B,i}$ and Alice’s signal pulses at $t_i$. (Pulse and gate widths are not to scale, typically $\sim 1$ ns.)

$I_{EB} = 0.908$ bit (figure 2(b), table 1). Figure 3 visualizes the success of Eve’s attack; she easily recovers the emblem of the University of Munich from the one-time pad encrypted cipher. We note that the attack decreases the signal rate (and hence the sifted key rate) to 25\%, depending
Figure 2. Experimental results for the eavesdropping attack. (a) The probability of detecting blinding pulse photons in zero, one, two, three or four detectors, depending on the effective mean photon number per blinding pulse (appendices). (b) The QBER of Alice’s and Bob’s key and the information about this key gained by Eve. By using different combinations of neutral density filters, the mean photon number per blinding pulse was changed, while keeping the signal pulse intensity constant. With increasing the number of photons per blinding pulse, the probability that three detectors are blinded increases rapidly, resulting in information of >0.9 bit for about 17 photons, while the QBER is not affected and leaves Alice and Bob ignorant about the attack.

In conclusion, we have demonstrated a powerful and successful attack that threatens many state-of-the-art QKD systems. By inserting blinding pulses into the quantum channel and eavesdropping on the classical communication only, an adversary is able to gain almost full information about the sifted key without being detected. The potential of this attack is especially high because of its simplicity. In contrast to previous attacks, for the first time the eavesdropper does not need to intercept the quantum channel and does not need to measure the low-light-level photonic signals emitted by Alice.

New Journal of Physics 13 (2011) 073024 (http://www.njp.org/)
Table 1. QBERs and Eve’s information for the different blinding pulse intensities used in the experiment. The three datasets marked with an asterisk are the ones used to decrypt the secret message shown in figure 3. Note that there is only a minor change in the QBER between Alice and Bob, making it impossible for them to discover the attack. The sifted key files were each longer than 20 kbytes, resulting in a statistical error in the QBER of <3%.

| $\mu_{\text{eff}}^B$ | QBER Alice–Bob (%) | QBER Bob–Eve (%) | $l_{\text{EB}}$ |
|----------------------|----------------------|------------------|----------------|
| 0.37                 | 1.10                 | 48.17            | 0.001          |
| 0.49                 | 1.12                 | 47.54            | 0.002          |
| 0.83*                | 1.09                 | 45.24            | 0.007          |
| 1.88                 | 1.01                 | 38.43            | 0.039          |
| 5.29*                | 1.11                 | 21.00            | 0.259          |
| 9.75                 | 1.12                 | 6.91             | 0.638          |
| 16.52*               | 1.25                 | 1.17             | 0.908          |

Figure 3. Application of the keys obtained in the experiment. Alice uses her sifted key to encrypt the original image with a one-time pad (top left corner) and sends the ciphertext (top center) to Bob, who uses his error-corrected key to decrypt the image (top right corner). The three images below are decrypted using Eve’s educated guess of the sifted key, for blinding pulses with a mean photon number of $\mu_{\text{eff}}^B = 0.83$, $\mu_{\text{eff}}^B = 5.29$ and $\mu_{\text{eff}}^B = 16.52$, respectively.

Fortunately, the defence against this blinding attack is correspondingly simple. Evidence could be obtained if Bob analyzed the detection events outside of the short time windows. However, by cleverly employing (several) blinding pulses at random times during this interval, Eve would simulate background noise and her attack could remain unnoticed. A better strategy would be to monitor the status of the SPADs. This can
be deduced from the bias voltage at the SPADs such that it is guaranteed that the detection efficiency is at a nominal level. Now, if we use only those detection events for the key generation where all detectors are active, the blinding attack and all other currently proposed dead time attacks [26–28] become ineffective. This scheme also avoids possible problems due to saturation effects in ultra-high-rate QKD setups [30–32], thereby establishing significant confidence in this quantum secure photonic communication method.

Acknowledgments

This work was funded by the Elite Network of Bavaria program QCCC and the BMBF project QPENS.

Appendix A. Dead time analysis

SPADs exhibit a detection efficiency that depends on the overbias voltage applied. After detection, depending on the electronics, it takes some time until the detector regains full efficiency. For the characterization of the detector’s dead time, we illuminated it by two consecutive faint laser pulses. The delay between the first and second pulses has been varied and the corresponding relative detection efficiency (normalized to the value after 3.5 µs) was recorded (see figure 1(b)). The line is a fit using the function \( E(t') = \frac{1}{2}(1 + \text{erf}(t' - \tau_D)) \cdot (1 - e^{-t'/\tau_2}) \), with \( t' \) being time after detection and fit parameters \( \tau_D \), \( \tau_2 \) (jitter due to pulse discrimination) and \( \tau_3 \) (charging time of SPAD capacity). For passive quenching electronics, the dead time \( \tau_D \) is particularly long (≈ 400 ns), whereas it is about 50 ns when using active quenching. Nevertheless, the eavesdropping scheme can be applied equally well.

Appendix B. Detection probabilities

B.1. Blinding pulse detection probabilities

To estimate Eve’s information (figure 2), we assume that the delay between two of Bob’s signal time slots and between Eve’s blinding pulse and the preceding signal pulse is greater than the average dead time of the SPADs, which itself is longer than a signal time slot. We will further assume the recovery process to be binary (on or off) with a certain dead time and a passive basis choice setup with four detectors (see figure 1). Active switching systems with two detectors can be analyzed accordingly.

We first calculate the detection probabilities of blinding pulses (coming from Eve) and signal pulses (emitted by Alice). We start with the blinding pulses. Let \( P_p(\mu_{\text{eff}}^B) \) and \( P_d(\mu_{\text{eff}}^B) \) be the probability that a blinding pulse is recognized in the detector analyzing parallel and diagonal polarizations relative to the blinding pulse polarization, respectively. The corresponding detection probability in the orthogonal orientation is negligible. Detection probabilities depend on the blinding pulse intensity expressed as the mean photon number per pulse \( \mu_{\text{eff}}^B \) coupled into the (ideal) quantum channel. Here we include the coupling efficiency from Eve to Bob.
The probabilities of registering detections in one, two or three of the respective detectors at the same time then are

\[ p_p(\mu_B^{\text{eff}}) = \frac{P_p(\mu_B^{\text{eff}})}{P_d(\mu_B^{\text{eff}})} \cdot (1 - P_d(\mu_B^{\text{eff}}))(1 - P_d(\mu_B^{\text{eff}})) \]  \hspace{1cm} \text{(B.1)}

parallel detector clicks \hspace{1cm} \text{both diagonal detectors do not click}

\[ P_d(\mu_B^{\text{eff}}) = P_d(\mu_B^{\text{eff}}) \cdot (1 - P_p(\mu_B^{\text{eff}}))(1 - P_d(\mu_B^{\text{eff}})) \]  \hspace{1cm} \text{(B.2)}

\[ p_{pd}(\mu_B^{\text{eff}}) = P_p(\mu_B^{\text{eff}}) \cdot P_d(\mu_B^{\text{eff}}) \cdot (1 - P_d(\mu_B^{\text{eff}})) \]  \hspace{1cm} \text{(B.3)}

\[ p_{dd}(\mu_B^{\text{eff}}) = P^2_d(\mu_B^{\text{eff}}) \cdot (1 - P_p(\mu_B^{\text{eff}})) \]  \hspace{1cm} \text{(B.4)}

\[ p_{pdd}(\mu_B^{\text{eff}}) = P_p(\mu_B^{\text{eff}}) \cdot P^2_d(\mu_B^{\text{eff}}). \]  \hspace{1cm} \text{(B.5)}

So the probabilities that none, one, two or three detectors fire due to a blinding pulse are (figure 2)

\[ p(0)(\mu_B^{\text{eff}}) = (1 - P_p(\mu_B^{\text{eff}})) \cdot (1 - P_d(\mu_B^{\text{eff}}))^2, \]  \hspace{1cm} \text{(B.6)}

\[ p(1)(\mu_B^{\text{eff}}) = P_p(\mu_B^{\text{eff}}) + 2P_d(\mu_B^{\text{eff}}), \]  \hspace{1cm} \text{(B.7)}

\[ p(2)(\mu_B^{\text{eff}}) = 2p_{pd}(\mu_B^{\text{eff}}) + p_{dd}(\mu_B^{\text{eff}}), \]  \hspace{1cm} \text{(B.8)}

\[ p(3)(\mu_B^{\text{eff}}) = p_{pdd}(\mu_B^{\text{eff}}). \]  \hspace{1cm} \text{(B.9)}

B.2. Signal pulse detection probabilities

Using the previous results, the probability that a detector registers a signal pulse, depending on the detector’s polarization \( \phi \) and the signal pulse’s polarization \( \theta \) with respect to the blinding pulse, can be calculated, giving

\[ P_{\theta,\phi}(\mu_B^{\text{eff}}, \mu_S^{\text{eff}}) = (1 - P_{\phi}(\mu_S^{\text{eff}}))P_{\theta}(\mu_S^{\text{eff}}), \]  \hspace{1cm} \text{(B.10)}

with \( \phi, \theta \in \{p, d, o\} \) meaning parallel, diagonal and orthogonal and \( P_{o}(\mu_B^{\text{eff}}) = 0 \) and the signal pulse mean photon number at the receiver \( \mu_S^{\text{eff}} := \eta_S\mu_S \) with mean photon number at the (signal) source \( \mu_S \) and coupling efficiency from Alice to Bob \( \eta_S \).

From this, the amount of information an adversary can gain from such an attack can be estimated: the difference between the maximum (= 1) and the current value of the binary entropy is used as the information gain a potential eavesdropper would have:

\[ I = 1 - H_2(p(x_{Eve} = x_{Bob})) \]  \hspace{1cm} \text{(B.11)}

\[ = 1 + \Pr(x_{Eve} = x_{Bob}) \log(\Pr(x_{Eve} = x_{Bob})) + \Pr(x_{Eve} \neq x_{Bob}) \log(\Pr(x_{Eve} \neq x_{Bob})). \]  \hspace{1cm} \text{(B.12)}

With

\[ p_{||}(\mu_B^{\text{eff}}, \mu_S^{\text{eff}}) := p_{p,p}(\mu_B^{\text{eff}}, \mu_S^{\text{eff}}) + p_{d,d}(\mu_B^{\text{eff}}, \mu_S^{\text{eff}}) \]  \hspace{1cm} \text{(B.13)}

\[ p_{\perp}(\mu_B^{\text{eff}}, \mu_S^{\text{eff}}) := p_{o,o}(\mu_B^{\text{eff}}, \mu_S^{\text{eff}}) + p_{d,d}(\mu_B^{\text{eff}}, \mu_S^{\text{eff}}) \]  \hspace{1cm} \text{(B.14)}

it is intuitively clear that for large \( \mu_B^{\text{eff}} \), i.e. high blinding intensities, all the terms with \( p_{d,d} \) and \( p_{p,p} \) will become small, because, most of the time, all detectors except the one orthogonal to the blinding pulse will be inactive.
Now the information gain (appendix B.12) can be calculated to give:

$$I(\mu_B^{\text{eff}}, \mu_S^{\text{eff}}) = 1 + \frac{p_\parallel}{p_\parallel + p_\perp} \log_2 \left( \frac{p_\parallel}{p_\parallel + p_\perp} \right) + \frac{p_\perp}{p_\parallel + p_\perp} \log_2 \left( \frac{p_\perp}{p_\parallel + p_\perp} \right).$$

(B.15)

The signal rate $R(\mu_B^{\text{eff}})$ that Bob detects from Alice can be calculated like this:

$$R(\mu_B^{\text{eff}}) = R_0(\mu_S^{\text{eff}}) \left( 1 - 0.25 \cdot p(1) (\mu_B^{\text{eff}}) - 0.5 \cdot p(2) (\mu_B^{\text{eff}}) - 0.75 \cdot p(3) (\mu_B^{\text{eff}}) \right),$$

(B.16)

with the undisturbed signal rate $R_0(\mu_S^{\text{eff}})$ between Alice and Bob when no blinding attack is launched. It is easy to see that with high mean number, the photon number per blinding pulse, $p(3) (\mu_B^{\text{eff}})$, will approach unity, so that the rate will approach 25% of its original value.

In the simulation (figure 2) it is assumed that the photon statistics of signal and blinding pulses in a four-SPAD receiver (figure 1) are Poissonian and thus $P_p(\mu_B^{\text{eff}}) = 1 - e^{-\mu_B^{\text{eff}}/2}$, $P_d(\mu_B^{\text{eff}}) = 1 - e^{-\mu_B^{\text{eff}}/4}$, $P_p^S(\mu_S^{\text{eff}}) = 1 - e^{-\mu_S^{\text{eff}}/2}$ and $P_d^S(\mu_S^{\text{eff}}) = 1 - e^{-\mu_S^{\text{eff}}/4}$.

References

[1] Bennett C H and Brassard G 1984 Quantum cryptography: public key distribution and coin tossing Proc. IEEE Int. Conf. on Computers, Systems and Signal Processing (Bangalore, India) pp 175–9
[2] Gisin N, Ribordy G, Tittel W and Zbinden H 2002 Quantum cryptography Rev. Mod. Phys. 74 145–95
[3] Bienfang J et al 2004 Quantum key distribution with 1.25 Gbps clock synchronization Opt. Express 12 2011–6
[4] Rosenberg D, Harrington J, Rice P, Hiskett P, Petersen C, Hughes R, Lita A, Nam S and Nordholt J 2007 Long-distance decoy-state quantum key distribution in optical fiber Phys. Rev. Lett. 98 010503
[5] Schmitt-Manderbach T et al 2007 Experimental demonstration of free-space decoy-state quantum key distribution over 144 km Phys. Rev. Lett. 98 010504
[6] Dixon A R, Yuan Z L, Dynes J F, Sharpe A W and Shields A J 2010 Continuous operation of high bit rate quantum key distribution Appl. Phys. Lett. 96 161102
[7] Peev M et al 2009 The SECOQC quantum key distribution network in Vienna New J. Phys. 11 075001
[8] Elliot C, Colvin A, Pearson D, Pikalo O, Schafer J and Yeh H 2005 Quantum Information and Computation III (Proc. SPIE) vol 5815 ed E J Donkor, A R Pirich and H E Brandt (Bellingham, WA: SPIE) pp 138–49 arXiv:0503058
[9] Sasaki M et al 2011 Field test of quantum key distribution in the Tokyo QKD Network Opt. Express 19 10387
[10] Lo H-K and Chau H F 1999 Unconditional security of quantum key distribution over arbitrarily long distances Science 283 2050–6
[11] Shor P W and Preskill J 2000 Simple proof of security of the BB84 quantum key distribution protocol Phys. Rev. Lett. 85 441–4
[12] Lamas-Linares A and Kurtsiefer C 2007 Breaking a quantum key distribution system through a timing side channel Opt. Express 15 9388–93
[13] Gelles R and Mor T 2008 Quantum-space attacks arXiv:0711.3019v2
[14] Zhao Y, Fung C-H, Qi B, Chen C and Lo H-K 2008 Quantum hacking: Experimental demonstration of time-shift attack against practical quantum-key-distribution systems Phys. Rev. A 78 042333
[15] Nauerth S, Först M, Schmitt-Manderbach T, Weier H and Weinfurter H 2009 Information leakage via side channels in freespaced BB84 quantum cryptography New J. Phys. 11 065001
[16] Xu F, Qi B and Lo H-K 2010 Experimental demonstration of phase-remapping attack in a practical quantum key distribution system New J. Phys. 12 113026
[17] Wiechers C et al 2011 After-gate attack on a quantum cryptosystem New J. Phys. 13 013043
[18] Inamori H, Lütkenhaus N and Mayers D 2007 Unconditional security of practical quantum key distribution Eur. Phys. J. D 41 599
Gottesman D, Lo H-K, Lütkenhaus N and Preskill J 2004 Security of quantum key distribution with imperfect devices Quantum Inf. Comput. 4 325

Hwang W-Y 2003 Quantum key distribution with high loss: toward global secure communication Phys. Rev. Lett. 91 057901

Wang X-B 2005 Beating the photon-number-splitting attack in practical quantum cryptography Phys. Rev. Lett. 94 230503

Lo H-K, Ma X and Chen K 2005 Decoy state quantum key distribution Phys. Rev. Lett. 94 230504

Ma X, Qi B, Zhao Y and Lo H-K 2005 Practical decoy state for quantum key distribution. Phys. Rev. A 72 012326

Fung C-H F, Tamaki K, Qi B, Lo H-K and Ma X 2009 Security proof of quantum key distribution with detection efficiency mismatch Quantum Inf. Comput. 9 0131

Weier H, Schmitt-Manderbach T, Regner N, Kurtsiefer C and Weinfurter H 2006 Free space quantum key distribution: towards a real life application Fortschr. Phys. 54 840

Makarov V, Anisimov A and Sauge S 2009 Quantum hacking: adding a commercial actively-quenched module to the list of single-photon detectors controllable by Eve arXiv:0809.3408v2

Makarov V 2009 Controlling passively quenched single photon detectors by bright light New J. Phys. 11 065003

Lydersen L, Wiechers C, Wittmann C, Elser D, Skaar J and Makarov V 2010 Hacking commercial quantum cryptography systems by tailored bright illumination Nat. Photonics 4 686–9

Yuan Z L, Dynes J F and Shields A J 2010 Avoiding the detector blinding attack on quantum cryptography Nat. Photonics 4 800–1

Rogers D J, Bienfang J C, Nakassis A, Xu H and Clark C W 2007 Detector dead-time effects and paralyzability in high-speed quantum key distribution New J. Phys. 9 319

Burenkov V, Qi B, Fortescue B and Lo H-K 2007 Security of high speed quantum key distribution with finite detector dead time arXiv:1005.0272

Xu H, Ma L, Bienfang J C and Tang X 2006 Influence of avalanche-photodiode dead time on the security of high-speed quantum-key distribution systems Conf. on Lasers and Electro-Optics/Quantum Electronics and Laser Science Conference and Photonic Applications Systems Technologies (Long Beach, CA, May 2006) JTuH3