Research Article Vol. 27, No. 22 / 28 October 2019 / *Optics Express* 32253

Optics EXPRESS

Controlling single-photon detector ID210 with bright light

VLADIMIR CHISTIAKOV,[1,*] ANQI HUANG,[2,3,4] VLADIMIR EGOROV,[1] AND VADIM MAKAROV[5,6,7,8]

[1] *Faculty of Photonics and Optical Information, ITMO University, St. Petersburg, Russia*
[2] *Institute for Quantum Information & State Key Laboratory of High Performance Computing, College of Computer, National University of Defense Technology, Changsha 410073, China*
[3] *Institute for Quantum Computing, University of Waterloo, Waterloo, ON N2L 3G1, Canada*
[4] *Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, ON N2L 3G1, Canada*
[5] *Russian Quantum Center, Skolkovo, Moscow 143025, Russia*
[6] *Shanghai Branch, National Laboratory for Physical Sciences at Microscale and CAS Center for Excellence in Quantum Information, University of Science and Technology of China, Shanghai 201315, China*
[7] *NTI Center for Quantum Communications, National University of Science and Technology MISiS, Moscow 119049, Russia*
[8] *Department of Physics and Astronomy, University of Waterloo, Waterloo, ON N2L 3G1, Canada*
[*] *v_chistyakov@itmo.ru*

Abstract: We experimentally demonstrate that a single-photon detector ID210 commercially available from ID Quantique is vulnerable to blinding and can be fully controlled by bright illumination. In quantum key distribution, this vulnerability can be exploited by an eavesdropper to perform a faked-state attack giving her full knowledge of the key without being noticed. We consider the attack on standard BB84 protocol and a subcarrier-wave scheme and outline a possible countermeasure.

1. Introduction

Quantum key distribution (QKD) technology allows to securely distribute symmetric keys between two parties by utilizing fundamental aspects of quantum physics [1]. In theory, legitimate users (Alice and Bob) are able to detect any eavesdropping in the quantum channel performed by Eve. Today security of several QKD protocols has been unconditionally proven [2]. However, in practice Eve is still able to obtain information about quantum keys without alarming Alice and Bob by exploiting loopholes in QKD hardware, which are not taken into consideration during the security analysis. This technique is referred to as "quantum hacking" and has been experimentally demonstrated with a variety of QKD components [3–14]. These results have helped to further solidify QKD security by patching the loopholes or extending security analysis. It is therefore important to continue testing other QKD devices in order to develop efficient hacking countermeasures.

A particular QKD component found to be vulnerable to quantum hacking is a single-photon detector [6,12,15–23]. For field applications in urban infrastructure, where the QKD nodes are located at medium distances (up to 100 km), it is most practical to use single-photon registration systems based on avalanche photodiodes (APDs) [24] because they provide sufficient efficiency without use of complex cooling systems required for superconducting detectors [25]. Several experiments demonstrated that Eve can take full control over the detector by blinding it by an intense continuous wave (c.w.) laser and then sending additional trigger pulses in order to achieve controllable clicks at desired times. Combining this method with measuring photon states send by Alice allows Eve to secretly obtain full knowledge about the quantum key [22]. This quantum

#375872 https://doi.org/10.1364/OE.27.032253
Journal © 2019 Received 27 Aug 2019; revised 6 Oct 2019; accepted 11 Oct 2019; published 22 Oct 2019

hacking technique is known as a faked-state attack [6,22,26]. It has been implemented on several commercially available APDs [6,12,16,21,27].

The purpose of this work is to investigate the vulnerability to the faked-state attack of another single-photon detector, ID Quantique ID210, which is currently commercially available [28] and has recently been used in several QKD setups [29–31]. Notably some of these experimental schemes are based on subcarrier-wave (SCW) QKD architecture where quantum states are formed at spectral sidebands of an intense light through phase modulation [32–34]. Notably, this practical QKD setup requires only one SPD for implementing a phase protocol. In SCW QKD systems a major fraction of the signal is filtered out before detection. Therefore another important task is to calculate realistic blinding parameters for SCW systems with ID Quantique ID210 detector. We have found that these setups are potentially susceptible to the faked-state attack.

2. Experimental setup

In our tests we have used ID210 single-photon detector by ID Quantique based on InGaAs/InP APD (unit serial number 1119019J010) [28]. To simulate realistic conditions for Eve's attack, we have treated the detector as a black box in the course of all experiments. We have not opened its housing nor manually interfered in operation of any internal circuits. All APD settings have been at the values normally used in SCW QKD operation [30]: quantum efficiency 10%, gating frequency 100 MHz, gate width 3 ns, deadtime 100 ns. For these settings, the dark count rate fluctuates around 200 Hz. All the parameters have been set using standard ID210 user interface from the front panel of the device.

Experimental setup for testing the detector for control by bright light is shown in Fig. 1. The APD is externally gated by an arbitrary waveform generator (AWG 1; Agilent 81110A) at frequency of 100 MHz. This value is typical for SCW QKD schemes [30,32]. Another generator (AWG 2; Highland Technology P400) is synchronized from AWG 1 and performs two functions. Firstly, it provides constant current to a continuous laser source (L1; Alcatel 1905 LMI) used for APD blinding. Secondly, it is driving the trigger pulse laser (L2; Gooch & Housego AA1401) at 10 MHz rate. This value is lower than the gating frequency, because in realistic conditions only a small fraction of pulses emitted by Alice (no more than 10%) reach Bob's single photon detector. L1 and L2 outputs are connected to variable optical attenuators (VOA 1; OZ Optics DA-100-3S-1550 and VOA 2; FOD 5418) that regulated output optical power. VOA outputs lead to fiber-optic beam splitter with a 50 : 50 ratio. One beamsplitter output arm is connected to an optical power meter (OPM; Joinwit JW3208), while the other leads to the ID210 detector (APD). The power meter monitors optical power applied to the APD from L1 and L2. We have taken into account a non-ideal beamsplitting ratio when calibrating this power. At the second

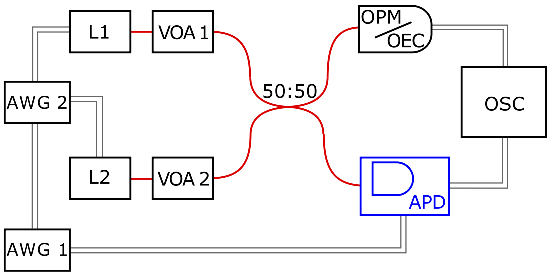

Fig. 1. Experimental setup for testing the detector. L, laser; AWG, arbitrary waveform generator; VOA, variable optical attenuator; OPM, optical power meter; OEC, optical-to-electrical converter; OSC, oscilloscope; APD, avalanche photodiode single-photon detector ID Quantique ID210.

stage of experiment, we have substituted OPM with an optical-to-electrical converter limited to roughly 2 GHz bandwidth (OEC; LeCroy OE555), in order to accurately determine an optical pulse shape of L2. The electrical signals from OEC and APD are measured by an oscilloscope (OSC; LeCroy 820Zi). Trigger pulse energy is calculated from average optical power registered by OPM divided by the pulse repetition rate.

3. Results

Our first task has been to find out if ID210 is susceptible to blinding. To do this, we have used L1 to generate c.w. laser radiation directed to APD optical input (with L2 switched off). L1 optical power has been regulated by VOA 1. When optical power at APD input has exceeded 24 nW, we have registered a complete absence of dark counts that indicates successful blinding of ID210 detector by c.w. radiation. The blinding does not harm the detector in any way, as its parameters return to normal each time L1 is turned off.

Blinding the APD implies switching it from Geiger to linear mode by bright illumination. After that Eve can take full control over detector clicks by exceeding a current threshold at a comparator in the linear mode by sending trigger pulses of sufficient energy along with c.w. blinding radiation [6]. Therefore our second step has been to determine the necessary trigger pulse parameters and synchronize these pulses with APD gates.

We have initiated trigger pulses by turning on L2 with 5 ns wide pulses at 10 MHz frequency. The latter value has been chosen as a maximum expected detector click frequency given 100 ns deadtime. The shape of the optical trigger pulse is important for accurately adjusting the delay between the "faked state" and the detector gate (Fig. 2). Its measured duration is less than 500 ps full-width at half-magnitude (FWHM). Meanwhile, FWHM of the gate pulse matches the preset gate width of 3 ns. We have then adjusted the timing of our optical trigger pulse to minimize its energy required to produce a click in the blinded regime, which presumably aligns it with the middle of the gate.

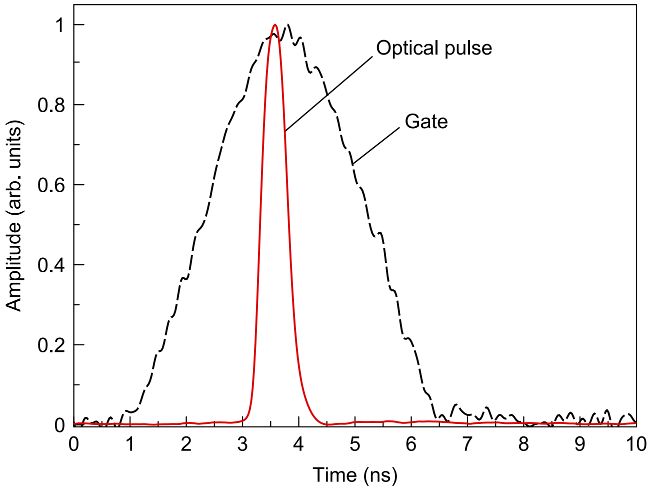

Fig. 2. Oscillograms of the APD gate signal (provided at ID210 front-panel output) and the optical trigger pulse. Their relative timing is shown here as an assumption. The optical pulse width shown is limited by the bandwidth of OEC, i.e., the actual pulse is shorter.

Our next step has been to determine a maximum trigger pulse energy E_{never} at which the blinded detector still clicks with zero probability, and minimum energy E_{always} at which it clicks with unity probability. When the trigger pulse energy E_{trigger} is increased, the click probability undergoes a transition, shown in Fig. 3 for several blinding powers. For example, under 35 nW c.w. blinding, the detector never clicks when $E_{\text{trigger}} \leq E_{\text{never}} = 15.4$ fJ and always clicks when $E_{\text{trigger}} \geq E_{\text{always}} = 25.8$ fJ. At higher blinding powers, a click probability transition from 0 to 1 becomes more abrupt, which is apparent by comparing the plots for c.w. blinding of 35 and 2512 nW that have been measured with a higher resolution to illustrate this effect.

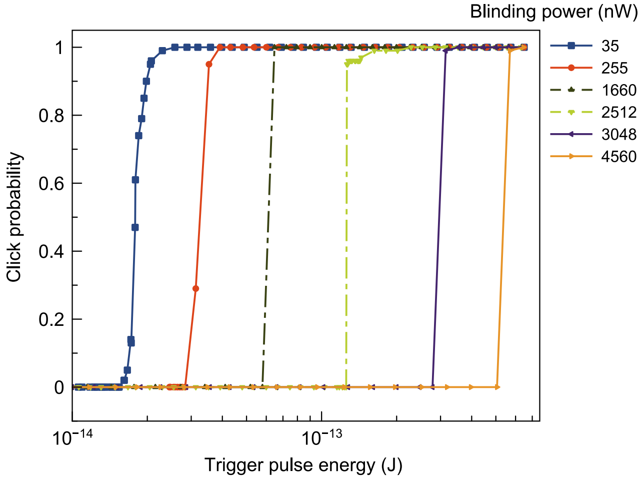

Fig. 3. Detector click probability in the blinded regime as a function of control pulse energy.

The last step of characterizing the APD is defining the boundary values for trigger pulse energies that Eve can use to carry out the most efficient faked-state attack. In [12], Huang et al. describes in detail the methodology we use here for estimating these values. Let us consider BB84 protocol with four states in two orthogonal bases [1]. When Eve performs the faked-state attack, there are two possible detection outcomes: either Eve and Bob choose the same bases, or not. Eve wants Bob's detector to always click in the first case, and never in the second. She can achieve it by imposing a limitation on her E_{trigger}, making it sufficient to induce a click only when Bob's basis choice is the same as hers [6]:

$$E_{\text{always}} \leq E_{\text{trigger}} \leq 2E_{\text{never}}. \tag{1}$$

Figure 4 illustrates these boundaries for the analyzed ID210 detector: any trigger pulse energy between E_{always} and $2E_{\text{never}}$, indicated by a shaded area, can be utilized for a successful attack. When Eve uses E_{trigger} values from this interval, and Bob chooses the same basis, the eavesdropper will fully control the APD response and possess information on every key bit. When their bases do not coincide, a click will never happen, and these instances will be discarded by Alice and Bob during sifting stage. Thanks to this approach, Eve imposes on Bob only the states that she knows, and acquires full information about the quantum key. Hence, we have shown that an eavesdropper can perform a successful faked-state attack on ID210 single-photon detector in a realistic scenario of BB84 protocol.

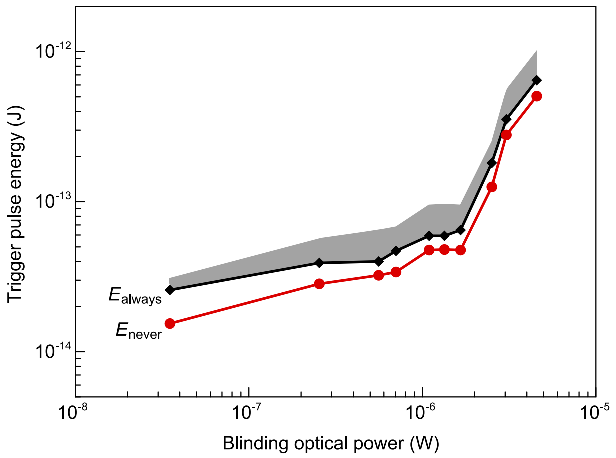

Fig. 4. Click thresholds of investigated ID210 detector under different blinding powers. E_{always} is a minimum pulse energy at which the detector always clicks and E_{never} is a maximum energy when it never clicks. Shaded area shows the range of trigger pulse energies E_{trigger} of the perfect attack (limited above by $2E_{\text{never}}$).

4. Attack on subcarrier-wave QKD

The investigated detector has recently been employed in several QKD experiments [30,31] based on SCW principle [35]. This QKD scheme is promising as a backbone for large-scale quantum network thanks to its high capability for multiplexing [36,37] and robustness against environmental influence on the optical fiber [32,38,39]. In this type of systems the encoding photons are not directly generated by an attenuated laser source but rather appear on spectral sidebands during a phase modulation of light. As can be seen from a general scheme of SCW QKD setup (Fig. 5) excluding the red parts described in Section 5, the signal spectrum passes through a narrow filter (SF) before detection in order to remove the optical carrier that contains most of the optical power. It is therefore important to investigate if this filtering is an obstacle for Eve's detector control and faked-state attack on SCW QKD setups. In realistic conditions we should also consider insertion losses in Bob.

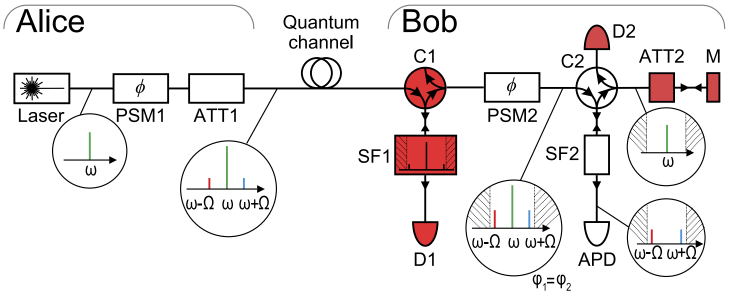

Fig. 5. Subcarrier-wave QKD scheme. Components shaded red (gray) are introduced as a countermeasure. PSM, electro-optical phase shift modulator; ATT, optical attenuator; C, circulator; SF, spectral filter; APD, avalanche photodiode; M, fiber-optic mirror; D, photodetector. Insets show optical spectra at different points.

For our analysis we have used SCW QKD experimental parameters from [32]: loss in Bob module 6.4 dB, SF extinction ratio 30 dB, and modulation index (the ratio between optical power in the carrier and the two sidebands) of 20. Let Eve prepare the signal states in a way similar to Alice: a spectrum with a strong carrier and two subcarriers. This spectrum will pass through the receiving unit undergoing the same modulation and filtering as the normal Alice's signal. Knowing the subcarrier power levels sufficient to blind the detector, we can estimate the total power that Eve should send into Bob module for successful blinding. For instance, let us consider the lowest blinding power of 35 nW confirmed experimentally in this work. In the SCW QKD scheme, before the pulse reaches the APD, it must undergo phase modulation at PSM2, where only $1/20$ of the initial optical carrier power is directed into the sidebands that will subsequently pass the SF. Therefore initial power at PSM2 input should be at least 700 nW. Likewise one must take into account loss in Bob module (6.4 dB in initial implementation [32] or 8 dB including the countermeasures described in Section 5). Therefore minimum power level used by Eve for a successful attack should be at least 4417 nW for the analyzed configuration. A similar logic works for the trigger pulse energy, as summarized in Table 1. As can be seen, although Eve must operate with higher blinding powers and trigger pulse energies in order to control the detector in SCW QKD scheme, the power levels needed are still sufficiently low not to damage any optical components [13]. These results suggest that SCW QKD setups do not have enough intrinsic loss to prevent detector control using the described method.

Table 1. Parameters for successful control of ID210 detector in SCW QKD scheme.

Eve's faked-state power in. . .	Blinding power (nW)	E_{always} (fJ)	E_{never} (fJ)	Countermeasure testing power (nW)
Subcarriers after filtering	35	25.8	15.4	114.8
Spectrum before modulation	700	516	308	2440
Spectrum entering Bob's module	4417	3256	1943	15395
Reflected carrier spectrum	320	–	–	1127
D2 input	2.2	–	–	7.8

We remark that the subcarrier-wave QKD is a fairly unusual scheme that uses only one detector in Bob. Most other QKD schemes use more than one detector. For them, Eve needs to consider unequal click thresholds of Bob's detectors, which nevertheless often allows her to attack [6,22,40,41].

5. Countermeasures

The faked-state attack is very general and has been successfully used for hacking different APDs. The most efficient countermeasure against it is implementing measurement-device-independent (MDI) QKD architecture [42], where the detection unit is moved from Alice and Bob to an untrusted party Charlie. MDI QKD protocol is based on Bell state measurements and ensures that Charlie (or Eve) is limited to openly announcing the measurement outcomes and is incapable of acquiring secure key information. Unfortunately, in practice MDI QKD architecture remains difficult to implement and yields much lower key rates.

In traditional two-party QKD, attempts to produce a countermeasure of a similar quality integrated with a security proof have led to stringent requirements on components [43,44], which have not yet been implemented. Simpler countermeasures that utilize photon counting statistics have been proposed but none yet battle-tested [45–49]. A more practical countermeasure may imply redesigning an avalanche quenching circuit of the APD and introducing precise photocurrent sensors into it [50–55].

Here we propose a simple solution for the SCW QKD scheme analyzed in this Article. As explained above, in SCW QKD intense optical radiation acts as a carrier for the phase-modulated quantum signal on its sidebands. Even though the carrier contains no information about the key, in practical QKD it is necessary to detect it as a countermeasure against a photon-number-splitting attack [56]. We propose to reveal APD blinding by monitoring this signal. Our system contains a circulator C2 used to measure the carrier and sideband signals individually (Fig. 5). Since the faked-state attack requires significantly elevated carrier optical power (see Table 1), a watchdog detector D2 can be installed for monitoring its abnormally high values. We presume that one cannot put an unprotected detector into a third port of the circulator, as it could be potentially blinded by Eve there. We therefore suggest to place it into the fourth port and protect it by an attenuator and a mirror in the third port, as shown in Fig. 5. The attenuation value should be carefully chosen to be high enough to prevent blinding of D2 but sufficiently low to allow carrier detection by a regular photodiode.

In order to assess the feasibility of our idea, we have performed experimental testing of the countermeasure by adding several components (shaded red in Fig. 5) to the SCW QKD device designed at ITMO University. We employed FOD 1204 optical power meter as D2, a fiber-optic Faraday mirror (AC Photonics PMFRDMR13211) as M and a 10 dB fixed attenuator as ATT2. For now let us consider that Eve uses the same wavelength as Alice (an alternative strategy is discussed below, explaining the roles of SF1 and D1 in Fig. 5). Insertion loss in C2 arms was around 1.6 dB. The experimental results are given in the fifth column of Table 1. We managed to blind the APD using the technique described above, and the required faked-state power level (114.8 nW) resulted in registering a signal on D2 (7.8 nW) that was a clear indication of the attack in progress. We have therefore confirmed that our countermeasure can be efficiently used for monitoring the faked-states attack.

From Table 1 one can see that blinding power used in countermeasure testing was slightly higher (but of the same order of magnitude) than one defined during initial experiments with APD described in Section 3. The reason for this is that the experiment with realistic SCW QKD setup was affected by fluctuations of optical parameters, such as insertion losses and SF2 extinction ratio. In order to estimate countermeasure efficiency for the blinding power's lower boundary (35 nW), we have calculated carrier power reflected from SF2 and passing through C2 into D2. It is found to be 2.2 nW, which is still way above D2 sensitivity lower limit (50 pW). Therefore these differences do not affect our conclusions. However, it may be beneficial to experimentally optimize ATT2 loss for any particular setup.

Finally, let us analyze the case when Eve uses a wavelength outside SF2 reflection spectrum. Indeed, since in SCW QKD the quantum signals are registered in SF2 transmission band, while the carrier, which is used for monitoring purposes, is located in the reflection band, Eve could bypass our countermeasure by simply tuning the faked-state signal wavelength outside the SF2 reflection window. In that case the APD could be successfully controlled without alarming D2. To prevent this situation we suggest placing another narrow spectral filter SF1 at Bob's module input. Its reflection spectrum should be centered around the carrier wavelength ω and the bandwidth must be close to 2Ω (in our case, about 10 GHz), where Ω is the subcarrier frequency shift. In such setup full signal spectrum reflects from SF1 and propagates into Bob's module, but radiation on any other frequency passes thorough the filter (as shown by hatched spectral ranges in Fig. 5). An additional monitoring detector D1 could be placed after SF1 for reference. Eve would therefore be restricted to using frequencies in SF1 passband. Notably, she could try using bright light at the sideband frequency (instead of the carrier), but then this signal would be modulated at PSM2, its fraction would reflect from SF2 and get detected by D2.

6. Conclusion

We have demonstrated experimentally that ID Quantique ID210 single-photon detector based on avalanche photodiode is vulnerable to blinding and can be controlled by bright light. We have performed all the tests treating ID210 as a black box, without any knowledge of its internal structure or circuit diagram. Also, the vulnerability of a subcarrier-wave QKD system to the faked-state attack has been experimentally proven. We have shown that the faked-state attack will work in SCW QKD systems despite a major signal fraction being filtered out before the detection. We have also introduced and experimentally tested a simple optical scheme that could act as a countermeasure in SCW QKD.

Overall, even though the faked-state attack was introduced a decade ago, no universal industrial-scale solution for prepare-and-measure QKD has been found yet. Today MDI QKD remains the only strictly proven countermeasure against detector hacking. All alternative solutions are still to be meticulously tested and incorporated into existing security proofs. Our results emphasize that known vulnerabilities should be addressed at the system design stage, and any countermeasures thoroughly tested experimentally.

Funding

Natural Sciences and Engineering Research Council of Canada (CryptoWorks21, Discovery); Ministry of Education and Science of the Russian Federation (5-in-100, NTI center for quantum communications); China Scholarship Council; Canada Foundation for Innovation; Ontario Ministry of Research, Innovation and Science; National Natural Science Foundation of China (grant 61901483); Government Council on Grants, Russian Federation (08-08).

Acknowledgments

This manuscript has been reviewed by ID Quantique prior to its publication. V.C. conducted the experiment, analyzed data, proposed the countermeasure, and wrote the manuscript with input from all authors. A.H. guided the experiment. V.M. and V.E. supervised the study.

Disclosures

The authors declare no conflicts of interest.

References

1. C. H. Bennett and G. Brassard, “Quantum cryptography: Public key distribution and coin tossing,” in *Proc. IEEE International Conference on Computers, Systems, and Signal Processing (Bangalore, India)*, (New York, 1984), pp. 175–179.
2. R. Renner, “Security of quantum key distribution,” Int. J. Quantum Inform. **06**(01), 1–127 (2008).
3. A. Lamas-Linares and C. Kurtsiefer, “Breaking a quantum key distribution system through a timing side channel,” Opt. Express **15**(15), 9388–9393 (2007).
4. S. Nauerth, M. Fürst, T. Schmitt-Manderbach, H. Weier, and H. Weinfurter, “Information leakage via side channels in freespace BB84 quantum cryptography,” New J. Phys. **11**(6), 065001 (2009).
5. F. Xu, B. Qi, and H.-K. Lo, “Experimental demonstration of phase-remapping attack in a practical quantum key distribution system,” New J. Phys. **12**(11), 113026 (2010).
6. 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**(10), 686–689 (2010).
7. S.-H. Sun, M.-S. Jiang, and L.-M. Liang, “Passive Faraday-mirror attack in a practical two-way quantum-key-distribution system,” Phys. Rev. A **83**(6), 062331 (2011).
8. 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**(11), 110501 (2011).
9. Y.-L. Tang, H.-L. Yin, X. Ma, C.-H. F. Fung, Y. Liu, H.-L. Yong, T.-Y. Chen, C.-Z. Peng, Z.-B. Chen, and J.-W. Pan, “Source attack of decoy-state quantum key distribution using phase information,” Phys. Rev. A **88**(2), 022308 (2013).
10. 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**(7), 070503 (2014).
11. S. Sajeed, I. Radchenko, S. Kaiser, J.-P. Bourgoin, A. Pappa, L. Monat, M. Legré, and V. Makarov, “Attacks exploiting deviation of mean photon number in quantum key distribution and coin tossing,” Phys. Rev. A **91**(3), 032326 (2015).
12. A. Huang, S. Sajeed, P. Chaiwongkhot, M. Soucarros, M. Legré, and V. Makarov, “Testing random-detector-efficiency countermeasure in a commercial system reveals a breakable unrealistic assumption,” IEEE J. Quantum Electron. **52**(11), 1–11 (2016).
13. V. Makarov, J.-P. Bourgoin, P. Chaiwongkhot, M. Gagné, T. Jennewein, S. Kaiser, R. Kashyap, M. Legré, C. Minshull, and S. Sajeed, “Creation of backdoors in quantum communications via laser damage,” Phys. Rev. A **94**(3), 030302 (2016).

14. A. Huang, S.-H. Sun, Z. Liu, and V. Makarov, "Quantum key distribution with distinguishable decoy states," Phys. Rev. A **98**(1), 012330 (2018).
15. V. Makarov, A. Anisimov, and J. Skaar, "Effects of detector efficiency mismatch on security of quantum cryptosystems," Phys. Rev. A **74**(2), 022313 (2006). Erratum ibid. **78**, 019905 (2008).
16. L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, "Thermal blinding of gated detectors in quantum cryptography," Opt. Express **18**(26), 27938–27954 (2010).
17. C. Wiechers, L. Lydersen, C. Wittmann, D. Elser, J. Skaar, C. Marquardt, V. Makarov, and G. Leuchs, "After-gate attack on a quantum cryptosystem," New J. Phys. **13**(1), 013043 (2011).
18. H. Weier, H. Krauss, M. Rau, M. Fürst, S. Nauerth, and H. Weinfurter, "Quantum eavesdropping without interception: an attack exploiting the dead time of single-photon detectors," New J. Phys. **13**(7), 073024 (2011).
19. L. Lydersen, N. Jain, C. Wittmann, Ø. Marøy, J. Skaar, C. Marquardt, V. Makarov, and G. Leuchs, "Superlinear threshold detectors in quantum cryptography," Phys. Rev. A **84**(3), 032320 (2011).
20. L. Lydersen, M. K. Akhlaghi, A. H. Majedi, J. Skaar, and V. Makarov, "Controlling a superconducting nanowire single-photon detector using tailored bright illumination," New J. Phys. **13**(11), 113042 (2011).
21. S. Sauge, L. Lydersen, A. Anisimov, J. Skaar, and V. Makarov, "Controlling an actively-quenched single photon detector with bright light," Opt. Express **19**(23), 23590–23600 (2011).
22. 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**(1), 349 (2011).
23. S. Sajeed, P. Chaiwongkhot, J.-P. Bourgoin, T. Jennewein, N. Lütkenhaus, and V. Makarov, "Security loophole in free-space quantum key distribution due to spatial-mode detector-efficiency mismatch," Phys. Rev. A **91**(6), 062301 (2015).
24. R. H. Hadfield, "Single-photon detectors for optical quantum information applications," Nat. Photonics **3**(12), 696–705 (2009).
25. C. M. Natarajan, M. G. Tanner, and R. H. Hadfield, "Superconducting nanowire single-photon detectors: physics and applications," Supercond. Sci. Technol. **25**(6), 063001 (2012).
26. V. Makarov and D. R. Hjelme, "Faked states attack on quantum cryptosystems," J. Mod. Opt. **52**(5), 691–705 (2005).
27. J. Jogenfors, A. M. Elhassan, J. Ahrens, M. Bourennane, and J.-Å. Larsson, "Hacking the Bell test using classical light in energy-time entanglement-based quantum key distribution," Sci. Adv. **1**(11), e1500793 (2015).
28. ID210 infrared single-photon detector datasheet, https://marketing.idquantique.com/acton/attachment/11868/f-0239/1/-/-/-/-/ID210_Brochure.pdf, visited 11 Oct 2019.
29. G. Cañas, N. Vera, J. Cariñe, P. González, J. Cardenas, P. W. R. Connolly, A. Przysiezna, E. S. Gómez, M. Figueroa, G. Vallone, P. Villoresi, T. F. da Silva, G. B. Xavier, and G. Lima, "High-dimensional decoy-state quantum key distribution over multicore telecommunication fibers," Phys. Rev. A **96**(2), 022317 (2017).
30. O. Bannik, V. Chistyakov, L. Gilyazov, K. Melnik, A. Vasiliev, N. Arslanov, A. Gaidash, A. Kozubov, V. Egorov, S. Kozlov, A. Gleim, and S. Moiseev, "Multinode subcarrier wave quantum communication network," (2017). *presentation at International conference on quantum cryptography QCrypt 2017, Cambridge, UK, 18–22 September 2017*.
31. G. P. Miroshnichenko, A. V. Kozubov, A. A. Gaidash, A. V. Gleim, and D. B. Horoshko, "Security of subcarrier wave quantum key distribution against the collective beam-splitting attack," Opt. Express **26**(9), 11292–11308 (2018).
32. A. V. Gleim, V. V. Chistyakov, O. I. Bannik, V. I. Egorov, N. V. Buldakov, A. B. Vasilev, A. A. Gaĭdash, A. V. Kozubov, S. V. Smirnov, S. M. Kynev, S. É. Khoruzhnikov, S. A. Kozlov, and V. N. Vasil'ev, "Sideband quantum communication at 1 Mbit/s on a metropolitan area network," J. Opt. Technol. **84**(6), 362–367 (2017).
33. A. Gaidash, A. Kozubov, and G. Miroshnichenko, "Methods of decreasing the unambiguous state discrimination probability for subcarrier wave quantum key distribution systems," J. Opt. Soc. Am. B **36**(3), B16–B19 (2019).
34. A. Gaidash, A. Kozubov, and G. Miroshnichenko, "Countermeasures for advanced unambiguous state discrimination attack on quantum key distribution protocol based on weak coherent states," Phys. Scr. **94**(12), 125102 (2019).
35. J.-M. Mérolla, Y. Mazurenko, J.-P. Goedgebuer, and W. T. Rhodes, "Phase-modulation transmission system for quantum cryptography," Opt. Lett. **24**(2), 104–106 (1999).
36. J. Mora, A. Ruiz-Alba, W. Amaya, A. Martínez, V. García-Muñoz, D. Calvo, and J. Capmany, "Experimental demonstration of subcarrier multiplexed quantum key distribution system," Opt. Lett. **37**(11), 2031–2033 (2012).
37. V. V. Chistyakov, A. V. Gleim, V. I. Egorov, and Y. V. Nazarov, "Implementation of multiplexing in a subcarrier-wave quantum cryptography system," J. Phys.: Conf. Ser. **541**, 012078 (2014).
38. A. V. Gleim, V. I. Egorov, Y. V. Nazarov, S. V. Smirnov, V. V. Chistyakov, O. I. Bannik, A. A. Anisimov, S. M. Kynev, A. E. Ivanova, R. J. Collins, S. A. Kozlov, and G. S. Buller, "Secure polarization-independent subcarrier quantum key distribution in optical fiber channel using BB84 protocol with a strong reference," Opt. Express **24**(3), 2619 (2016).
39. S. Kynev, V. Chistyakov, S. Smirnov, K. Volkova, V. Egorov, and A. Gleim, "Free-space subcarrier wave quantum communication," J. Phys.: Conf. Ser. **917**, 052003 (2017).
40. L. Lydersen, J. Skaar, and V. Makarov, "Tailored bright illumination attack on distributed-phase-reference protocols," J. Mod. Opt. **58**(8), 680–685 (2011).
41. Q. Liu, A. Lamas-Linares, C. Kurtsiefer, and J. Skaar, "A universal setup for active control of a single-photon detector," Rev. Sci. Instrum. **85**(1), 013108 (2014).
42. H.-K. Lo, M. Curty, and B. Qi, "Measurement-device-independent quantum key distribution," Phys. Rev. Lett. **108**(13), 130503 (2012).

43. L. Lydersen, V. Makarov, and J. Skaar, “Secure gated detection scheme for quantum cryptography,” Phys. Rev. A **83**(3), 032306 (2011).
44. Ø Marøy, V. Makarov, and J. Skaar, “Secure detection in quantum key distribution by real-time calibration of receiver,” Quantum Sci. Technol. **2**(4), 044013 (2017).
45. T. Honjo, M. Fujiwara, K. Shimizu, K. Tamaki, S. Miki, T. Yamashita, H. Terai, Z. Wang, and M. Sasaki, “Countermeasure against tailored bright illumination attack for DPS-QKD,” Opt. Express **21**(3), 2667–2673 (2013).
46. A. Koehler-Sidki, M. Lucamarini, J. F. Dynes, G. L. Roberts, A. W. Sharpe, Z. Yuan, and A. J. Shields, “Intensity modulation as a preemptive measure against blinding of single-photon detectors based on self-differencing cancellation,” Phys. Rev. A **98**(2), 022327 (2018).
47. A. Fedorov, I. Gerhardt, A. Huang, J. Jogenfors, Y. Kurochkin, A. Lamas-Linares, J.-Å. Larsson, G. Leuchs, L. Lydersen, V. Makarov, and J. Skaar, “Comment on ‘Inherent security of phase coding quantum key distribution systems against detector blinding attacks’ (2018 Laser Phys. Lett. 15 095203),” Laser Phys. Lett. **16**(1), 019401 (2019).
48. J. Wang, H. Wang, X. Qin, Z. Wei, and Z. Zhang, “The countermeasures against the blinding attack in quantum key distribution,” Eur. Phys. J. D **70**(1), 5 (2016).
49. A. Gaidash, V. Egorov, and A. Gleim, “Revealing beam-splitting attack in a quantum cryptography system with a photon-number-resolving detector,” J. Opt. Soc. Am. B **33**(7), 1451–1455 (2016).
50. Z. L. Yuan, J. F. Dynes, and A. J. Shields, “Avoiding the blinding attack in QKD,” Nat. Photonics **4**(12), 800–801 (2010).
51. L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, “Reply to ‘Avoiding the blinding attack in QKD’,” Nat. Photonics **4**(12), 801 (2010).
52. 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**(23), 231104 (2011).
53. L. Lydersen, V. Makarov, and J. Skaar, “Comment on ‘Resilience of gated avalanche photodiodes against bright illumination attacks in quantum cryptography’,” Appl. Phys. Lett. **99**(19), 196101 (2011).
54. Z. L. Yuan, J. F. Dynes, and A. J. Shields, “Reply to "comment on ’resilience of gated avalanche photodiodes against bright illumination attacks in quantum cryptography’",” Appl. Phys. Lett. **99**(19), 196102 (2011).
55. A. Koehler-Sidki, J. F. Dynes, M. Lucamarini, G. L. Roberts, A. W. Sharpe, Z. L. Yuan, and A. J. Shields, “Best-practice criteria for practical security of self-differencing avalanche photodiode detectors in quantum key distribution,” Phys. Rev. Appl. **9**(4), 044027 (2018).
56. O. L. Guerreau, F. J. Malassenet, S. W. McLaughlin, and J.-M. Merolla, “Quantum key distribution without a single-photon source using a strong reference,” IEEE Photonics Technol. Lett. **17**(8), 1755–1757 (2005).