METRICA
METRology Institutional CAtalog

ISTITUTO NAZIONALE DI RICERCA METROLOGICA
Repository Istituzionale

Quantifying backflash radiation to prevent zero-error attacks in quantum key distribution

Original
Quantifying backflash radiation to prevent zero-error attacks in quantum key distribution / Meda, Alice; Degiovanni, Ivo Pietro; Tosi, Alberto; Yuan, Zhiliang; Brida, Giorgio; Genovese, Marco. - In: LIGHT, SCIENCE & APPLICATIONS. - ISSN 2047-7538. - 6:6(2017), p. e16261. [10.1038/lsa.2016.261]

Availability:
This version is available at: 11696/56885 since: 2018-01-29T08:17:51Z

Publisher:
Nature Publishing Group

Published
DOI:10.1038/lsa.2016.261

Terms of use:

This article is made available under terms and conditions as specified in the corresponding bibliographic description in the repository

Publisher copyright

(Article begins on next page)

09 November 2024

OPEN

Light: Science & Applications (2017) 6, e16261; doi:10.1038/lsa.2016.261
Official journal of the CIOMP 2047-7538/17
www.nature.com/lsa

ORIGINAL ARTICLE

Quantifying backflash radiation to prevent zero-error attacks in quantum key distribution

Alice Meda[1], Ivo Pietro Degiovanni[1], Alberto Tosi[2], Zhiliang Yuan[3], Giorgio Brida[1] and Marco Genovese[1]

Single-photon avalanche diodes (SPADs) are the most widespread commercial solution for single-photon counting in quantum key distribution applications. However, the secondary photon emission that arises from the avalanche of charge carriers that occurs during the detection of a photon may be exploited by an eavesdropper to gain information without inducing errors in the transmission key. In this paper, we characterize such backflash light in gated InGaAs/InP SPADs and discuss its spectral and temporal characterization for different detector models and different operating parameters. We qualitatively bound the maximum information leakage due to backflash light and propose solutions for preventing such leakage.
Light: Science & Applications (2017) **6,** e16261; doi:10.1038/lsa.2016.261; published online 16 June 2017

Keywords: backflash; quantum key distribution; single-photon avalanche diode; zero-error attack

INTRODUCTION

Quantum key distribution (QKD) is a method for sharing secret cryptographic keys between two parties (Alice and Bob) with an unprecedented level of security[1–7]. This level of security is ensured by the laws of quantum mechanics and does not depend on the technological resources available to an eavesdropper (Eve), provided that the QKD implementation does not deviate from the theoretical model. However, the security of a practical system (just as for any other cryptographic system) strongly depends on its device implementation. Any deviation of a QKD device from the theoretical model can be exploited as a side channel or back door [8–10].

In 2010, two zero-error attacks on commercial QKD systems were reported that exploited defects in quantum signal encoding[8] and detection[9]. Shortly after, a plethora of quantum hacking attacks were implemented using existing technologies to exploit device imperfections in a number of QKD designs (with different protocols, modules and systems)[10–16]. To guarantee security, each practical implementation must be carefully analyzed and tested for its robustness against zero-error attacks.

Single-photon avalanche diodes (SPADs) are the most widespread commercial solution for single-photon detection in practical QKD implementations[17–26]. They can also be the most vulnerable components because they are optically exposed to Eve through the open quantum channel. Eve can inject strong light to take control of these detectors, thereby compromising the security of an entire QKD system. Alternatively, Eve can also passively measure any backflash light arising from avalanching carriers[27] to learn the detected bit value (Figure 1). Backflashes have been shown to exist in both InGaAs/InP and Si SPADs[27–30]. However, these demonstrations are limited to free-space detectors, and no experiments have been performed on fiber-pigtailed SPADs, which are the detectors of choice in all existing commercial QKD systems because of their practicality.

Here, we present the first characterization of backflash light in fiber-pigtailed InGaAs SPADs from various manufacturers. We construct a reconfigurable optical time-domain reflectometer (OTDR) operating at the single-photon level[31–35] with exceptional sensitivity. This OTDR enables unambiguous identification of detector backflashes from conventional light back reflections and provides a practical way to bound the information leakage, i.e., a fundamental step toward QKD security. Furthermore, we show that information can be leaked through backflashes when two detectors produce temporally distinguishable secondary emissions.

MATERIALS AND METHODS

The experimental setup used to analyze backflash light is depicted in Figure 2. A strongly attenuated pulsed laser sends photons at 1550 nm to the InGaAs/InP SPAD under test (DUT). The back-reflected light is analyzed using our photon-counting OTDR to quantify the amount of secondary emission photons that could serve as an information side channel to Eve. The source is a commercial 1550-nm pulsed diode laser with pulse width of 300 ps and an energy per pulse lower than 1 fJ. The laser output is sent to a single-mode optical fiber and attenuated to the single-photon level by exploiting a fiber-coupled variable optical attenuator (with a maximum attenuation of 60 dB) combined with an additional 20-dB attenuation from a 99:1 fiber coupler.

We analyzed the back-reflected and backflash light of two different InGaAs/InP detectors. The first one, DUT1, is a prototype single-photon detection module[36]; the second one, DUT2, is the commercial IdQuantique ID201, widely used in research laboratories. Both

[1]INRIM, 10135 Torino, Italy; [2]Dipartimento di Elettronica, Informazione e Bioingegneria, Politecnico di Milano, 20133 Milano, Italy and [3]Toshiba Research Europe Ltd, Cambridge CB4 0GZ, UK
Correspondence: A Meda, Email: a.meda@inrim.it
Received 19 June 2016; revised 18 November 2016; accepted 30 November 2016; accepted article preview online 5 December 2016

detectors are pigtailed and operate in gated mode. These devices are highly configurable in terms of detection efficiency, gate duration, and dead time. They also exploit active quenching and allow long avalanche durations (~10 ns). Their configurability and long avalanche durations make them ideal for studying backflashes. The repetition rate of the laser pulses and of the trigger rate of the DUTs were set to $f_{pg} = 50$ kHz using an external pulse generator. Both back reflections and the DUT backflashes were directed by the circulator to the measuring detector, a free-running single-photon InGaAs/InP SPAD (IdQuantique ID220). The detector was operated with a low dark count rate (5 kHz), a nominal quantum efficiency of 10% and a timing resolution of 130 ps. The output electrical signals from the OTDR detector and the DUT were sent to time-correlated single photon-counting (TCSPC) electronics. Figure 3a and 3b shows traces corresponding to the OTDR signals triggered by the laser pulses, with an acquisition time of 60 min, for DUT1 and DUT2, respectively. The histogram represents the returned photons (due to either backflashes or back reflections) as a function of the time delay between the emission of a laser pulse and its detection by the OTDR detector. The horizontal axis represents the time for which a detected photon has traveled. In Figure 3, the sharp peaks arise from backreflection at the connections between different slices of fiber or between the fiber and other optical elements in the path (e.g., the circulator). There is also a rectangular or trapezoidal feature that appears only when the DUT is switched on. We attribute this feature to the backflash light emitted by the DUT during avalanches.

Each type of DUT has a unique, identifiable temporal profile, which reveals the type of detector and its manufacturer. We confirmed this finding by testing four additional devices of the DUT1 type and two of the DUT2 type. Such identifiable backflash profiles can be exploited by Eve to launch attacks tailored to a specific detector type.

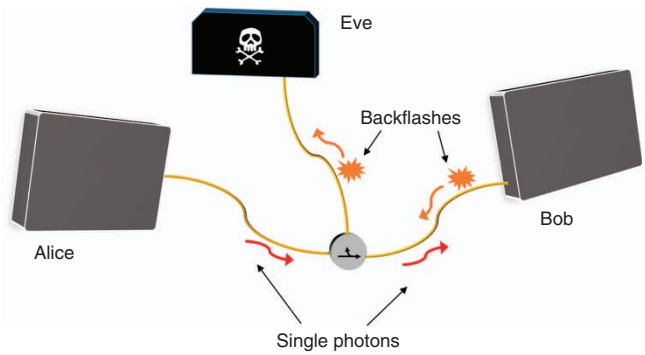

Figure 1 Representation of an eavesdropper attack exploiting backflash light. Alice sends the photons of the key to Bob; when the photons are detected by Bob using a SPAD, a flash of light, the backflash, is emitted back to the channel. Eve can use a circulator to intercept this spot of light to acquire information about the detector that has clicked.

RESULTS AND DISCUSSION

Here, we evaluate the maximum possible information leakage P_L due to backflash light for QKD systems implemented with detectors of either the DUT1 type or the DUT2 type. We consider a poorly designed QKD system that allows complete temporal discrimination of backflashes between different detectors. P_L is estimated starting from the ratio between the number of detected backflashes, N_B, and the corresponding total number of valid counts, N_P, of the DUT. N_B refers only to backflash events, i.e., after background subtraction. We consider the worst-case scenario in which Eve has ideal equipment, i.e., equipment that is lossless and with an ideal (unit) photon detection efficiency. Thus P_L is evaluated as

$$P_L = \frac{N_B}{N_P \eta_{det} \eta_{ch}} \quad (1)$$

where corrections for losses and inefficiencies of the OTDR system are applied, i.e., for the detection efficiency of the OTDR detector, η_{det}, and for the losses in the optical channel connecting the DUT and the OTDR detector due to the circulator and the fiber connections, η_{ch}. To be conservative, we slightly overestimate these losses and inefficiencies by assuming $\eta_{ch}\eta_{det} = 0.05$ based on their approximate evaluations. We obtain an information leakage P_L of 9.8% for DUT1 and a P_L of 6% for DUT2. These results suggest that the information that Eve can obtain by observing backflash light is not negligible and that countermeasures must be put in place.

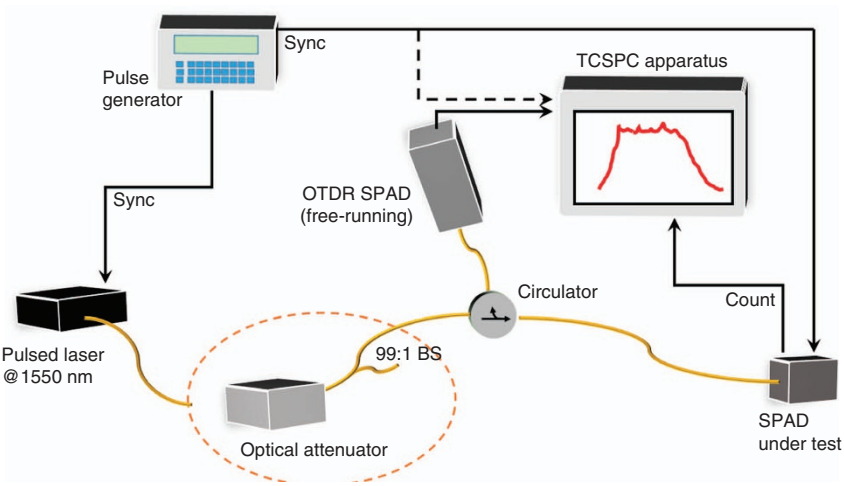

Figure 2 A schematic representation of our experimental setup. A photon-counting OTDR observes backflash light from the SPAD under test. The source is an attenuated pulsed laser emitting at 1550 nm. The backflash light is detected by a free-running InGaAs/InP detector. Time stamping of detected light is obtained by means of a time-correlated single-photon counting (TCSPC) apparatus.

doi:10.1038/lsa.2016.261

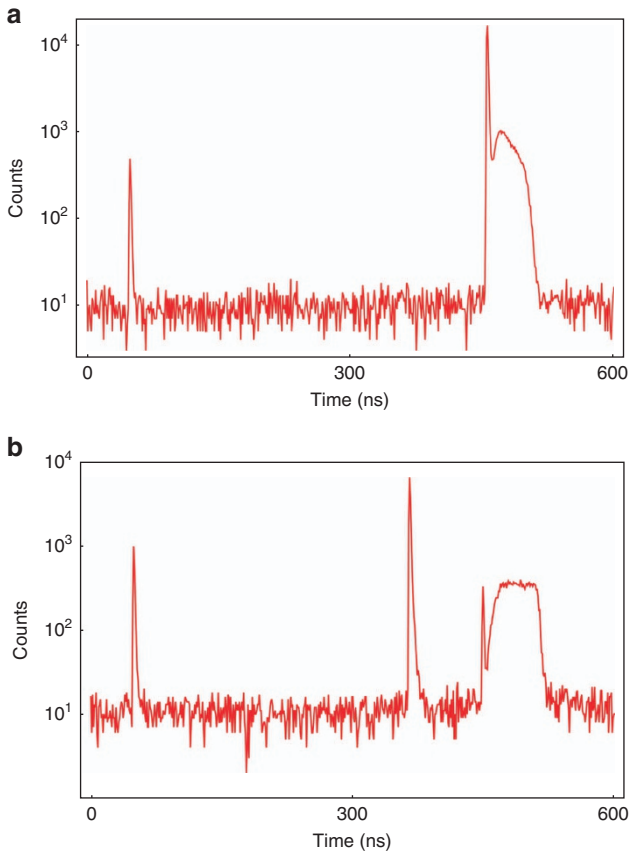

Figure 3 (**a**, **b**) The traces of the optical correlator after 60 min of acquisition for DUT1 and DUT2, respectively. A backflash peak that is unique to the particular DUT type is visible when an avalanche is triggered. For DUT1, we set an excess bias voltage of 7 V, corresponding to a detection efficiency higher than 35% and a gate width of 20 ns, whereas for DUT2, the efficiency is 10% and the gate width is 100 ns. On observing zoomed views of the backflash peaks for DUT1 and for DUT2, different peak shapes are evident.

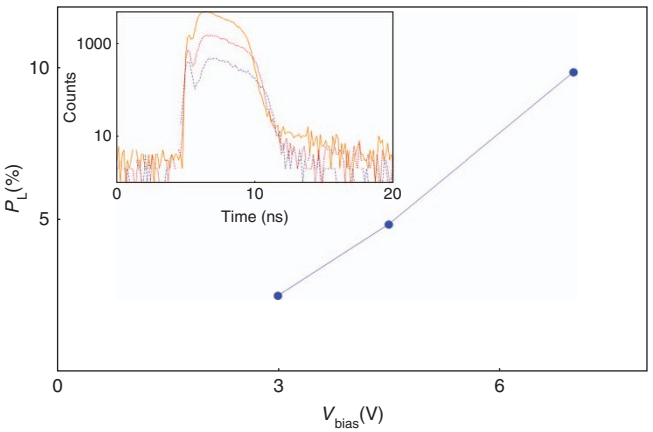

Figure 4 Information leakage P_L as a function of the excess bias voltage for the prototype detector DUT1. The peaks of the back-reflected light is presented in the inset (the continuous, dashed and dot-dashed lines represent the cases of 7, 4.5 and 3 V, respectively); the smaller peak due to the reflection of the laser light from the diode surface is relatively more evident at low excess bias voltages.

The backflash light is a consequence of the carrier avalanches that are triggered by an absorbed photon when the device is biased beyond its breakdown voltage. This light is quenched, together with the avalanche itself, when the detector bias is lowered below the breakdown voltage. Thus, the backflash intensity strongly depends on the parameter settings of the quenching electronics. We investigated the information leakage percentage in DUT1 for different detector operating conditions by varying the detection efficiency, gate width, and so on. The results are summarized in Figures 4 and 5. In Figure 4, the information leakage of DUT1 is presented as a function of the excess bias voltage. We used three different excess bias voltage settings, namely, 3, 4.5 and 7 V, corresponding to nominal detection efficiencies of 15%, 22% and 35%, respectively. As shown, the backflash intensity increases as the excess bias of the detector increases because the number of carriers also increases.

Figure 5 shows the information leakage as a function of the DUT gate delay relative to the incident laser pulse (measured for delays of 2, 10 and 18 ns after the beginning of the gating window). The two sets of data were collected for DUT1 operating at different bias voltages of 7 and 3 V. A decrease in the information leakage is observed when the laser photons arrive at the end of the gating window. This is because late avalanches are quenched by the falling edge of the gate window rather than by the active quenching circuit. The same effect explains the behavior observed when the laser peak is centered with respect to the gating window but different gating window widths are used. The information leakage is reduced when the width of the gating window is comparable to the width of the temporal profile of the backflash emission in DUT1 (i.e., 5 ns or less). To study the spectral distribution of the backflash emission, we integrated a fiber-optic tunable optical filter (Santec OTF-970) into our OTDR system before the OTDR measuring detector. The spectral range of the filter was from 1530 to 1600 nm, and we set a passband bandwidth of 10 nm. The results are presented in Figure 6a; the four presented profiles are the temporal distributions of the backflash counts centered at 1530, 1550, 1570 and 1600 nm. The temporal emission profile is similar to the one obtained without spectral filtering (Figure 3a) for all wavelengths. When the filter is centered at 1550 nm, the reflection peak dominates.

Figure 6b presents the total backflash counts as a function of the center wavelength of the filter. The subtraction of the back-reflected light was performed by measuring the laser light back reflected by DUT1 with a bias voltage applied but in the absence of a gate signal. The backflash emission is broadband, or at least it extends beyond the spectral range of our tunable filter, because it originates from the relaxation of hot carriers generated in the multiplication region[28–30]. In the spectral region of our tunable filter, it is reasonably uniform, except in the region around 1550 nm (1545–1555 nm), where a peak is observed even after the subtraction of the laser light back reflected by the DUT (see the sharp peak in Figure 6a). It is reasonable to suppose that the sharp peak that is present even after background subtraction is due to back-reflected laser light, since we observed that the reflectivity of the diode varies with the applied bias (in particular, a relative in reflectivity increase of almost one order of magnitude of the SPAD surface was observed in the case of non-polarized versus polarized, but non-gated, detector) and we attribute this to the refractive index change in the semiconductor material[37].

This was confirmed by measurements of the backflash spectrum performed with a pulsed laser operating at 1570 nm as source of our spectrally filtered OTDR. In this configuration, we expected to observe

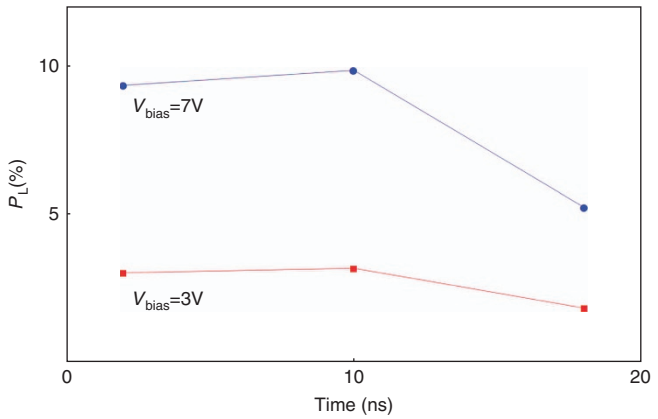

Figure 5 Information leakage as a function of the arrival time of laser photons with respect to the gate window that triggers the DUT. The data were collected for DUT1 operating at different bias voltages of 7 and 3 V.

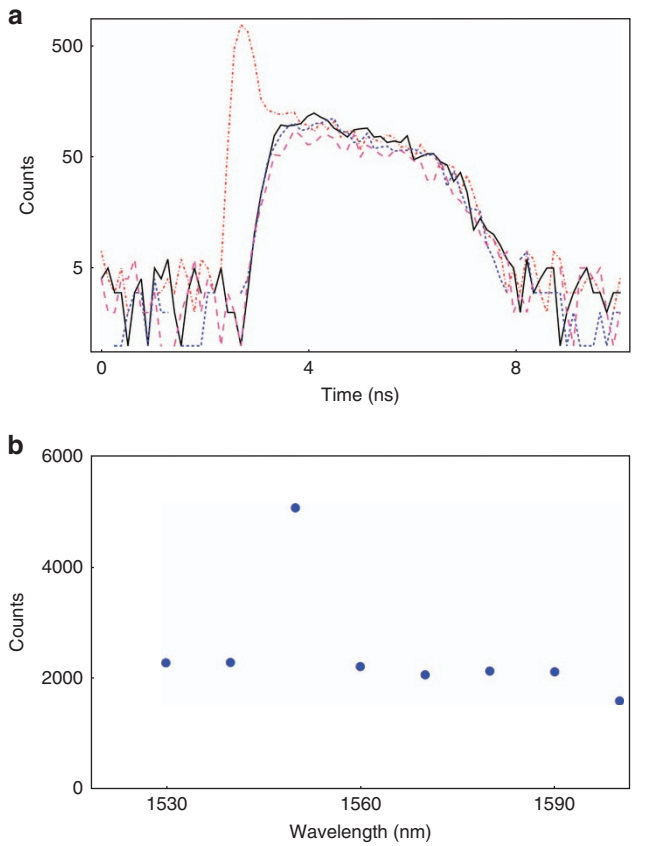

Figure 6 (**a**) Temporal distributions of the backflash counts after spectral filtering, with the filter centered at 1530, 1550, 1570 and 1600 nm. (**b**) Total counts of backflash light in the observed spectral range (from 1530 to 1600 nm). All measurements were performed using filters with a 10-nm bandwidth.

the sharp peak disappearing at 1550 nm and appearing at 1570 nm, and indeed, this was exactly what occurred, confirming that the sharp peak was just due to the change in the reflectivity of the SPAD surface caused by the change in its bias voltage.

CONCLUSIONS

We proved that significant backflash emission occurs in commercial InGaAs/InP single-photon detectors operating at telecom wavelengths. These backflashes could potentially allow a severe security breach in a poorly designed QKD system. Proper design and testing of QKD systems should be implemented to avoid attacks based on backflashes. Possible solutions can be based on passive optical devices[38] such as isolators, circulators or spectral filters to prevent backflashes leaking out of a QKD system. We emphasize that these countermeasures should consider the wide bandwidth of backflash light emission. For example, the use of a 1-nm-wide spectral filter centered at 1550 nm can reduce the information leakage of a DUT1-type device from 9.8% to 0.12%, under the assumption that the intensity of the backflash light is uniformly distributed throughout the spectral range under investigation (1530–1600 nm). Adding an isolator will result in a further attenuation of the backflash signal by ~30 dB.

Careful characterization of the spectral behavior of these optical components is necessary to ensure their operation as countermeasures.

Following this line of thought, a combination of circulators or isolators with interference optical filters at the input of the QKD system should essentially nullify the information leakage due to backflash light at the cost of some additional optical loss (the insertion losses of the optical filter and of the circulator) in the QKD signal. Eve may also attempt to intercept the backflash light just at the output of Bob's QKD box (or Bob's security perimeter). Thus, QKD engineers should also prevent the possibility of backflash light propagating in the cladding modes by implementing cladding-mode suppression solutions when necessary (in our case, the bending of our long single-mode fiber and the FC connectors essentially nullify the possibility of detecting backflash light propagating in the cladding). Furthermore, as discussed in connection with Figure 3, the use of gates that are as short as possible and small avalanches will reduce the emitted backflash light. In this sense, fast-gated detectors[39–44] represent an interesting solution for QKD systems, not only in terms of speed but also because of their much lower avalanche charges (as much as 100 times lower). In fact, it is expected that they should produce significantly lower backflash light emission. In addition, the use of short gates makes it more difficult for Eve to temporally discriminate the backflash light. Thus, testing the backflash behavior of fast-gated detectors would be an interesting research direction.

For QKD applications, superconducting-nanowire single-photon detectors are an excellent option. Indeed, in addition to their high detection efficiency, their low dark count rate, and their short recovery time[45–47], it is expected that they should not produce any backflash light (and thus should not allow any related information leakage). Unfortunately, they require cryogenic temperatures for operation, and because of the high cost of cryogenic equipment, they currently appear unsuitable for the practical deployment of QKD systems in the real world.

In a complete analysis of the security of a realistic QKD system design, other sources of information leakage must be considered in addition to backflashes. Eve can obtain information about the key by, for example, measuring the spatial, spectral or temporal properties of the transmitted qubits, exploiting the detector dependence of the signal basis and channel losses, or manipulating the detectors[9,48,49]. Once information leakage has been reduced as much as possible with dedicated hardware-based countermeasures, the residual information leakage can be overcome by applying privacy amplification protocols[49–52].

doi:10.1038/lsa.2016.261

CONFLICT OF INTEREST

The authors declare no conflict of interest.

AUTHOR CONTRIBUTIONS

IPD, AT and ZY conceived the idea of the experiment, which was discussed and designed with input from all authors. AM, IPD and GB realized the experimental setup and collected the data in the INRIM Quantum Optics Labs, coordinated by MG. All authors discussed the results and contributed to the writing of the paper.

ACKNOWLEDGEMENTS

This work has received funding from the European Union's Horizon 2020 and the EMPIR and EMRP Participating States in the contexts of the projects EXL02 SIQUTE and 14IND05 MIQC2, respectively. We also acknowledge funding support from FIRB Project No. D11J11000450001 funded by MIUR and from the NATO SPS Project 984397.

1 Bennett CH, Brassard G. Quantum cryptography: public key distribution and coin tossing. In: Proceedings IEEE International Conference on Computers, Systems and Signal Processing. IEEE: Bangalore, India, 1984, pp175–179.
2 Gisin N, Ribordy G, Tittel W, Zbindenr H. Quantum cryptography. *Rev Mod Phys* 2002; **74**: 145–195.
3 Scarani V, Bechmann-Pasquinucci H, Cerf NJ, Dusek M, Lukenhaus N *et al.* The security of practical quantum key distribution. *Rev Mod Phys* 2009; **81**: 1301–1350.
4 Lim CCW, Curty M, Walenta N, Xu FH, Zbinden H. Concise security bounds for practical decoy-state quantum key distribution. *Phys Rev A* 2014; **89**: 022307.
5 Zheng C, Long GF. Quantum secure direct dialogue using Einstein–Podolsky–Rosen pairs. *Sci China-Phys Mech Astron* 2014; **57**: 1238–1243.
6 Zhang CM, Li M, Yin ZQ, Li HW, Chen W *et al.* Decoy-state measurement-device-independent quantum key distribution with mismatched-basis statistics. *Sci China-Phys Mech Astron* 2015; **58**: 590301.
7 Cao DY, Liu BH, Wang Z, Huang YF, Li CF *et al.* Multiuser-to-multiuser entanglement distribution based on 1550 nm polarization-entangled photons. *Sci Bull* 2015; **60**: 1128–1132.
8 Xu FH, Qi B, Lo HK. Experimental demonstration of phase-remapping attack in a practical quantum key distribution system. *New J Phys* 2010; **12**: 113026.
9 Lydersen L, Wiechers C, Wittmann C, Elser D, Skaar J *et al.* Hacking commercial quantum cryptography systems by tailored bright illumination. *Nat Photonics* 2010; **4**: 686–689.
10 Huang AQ, Sajeed S, Chaiwongkhot P, Soucarros M, Legré M *et al.* Testing random-detector-efficiency countermeasure in a commercial system reveals a breakable unrealistic assumption. *IEEE J Quantum Electron* 2016; **52**: 8000211.
11 Gerhardt I, Liu Q, Lamas-Linares A, Skaar J, Scarani V *et al.* Experimentally faking the violation of Bell's inequalities. *Phys Rev Lett* 2011; **107**: 170404.
12 Jain N, Wittmann C, Lydersen L, Wiechers C, Elser D *et al.* Device calibration impacts security of quantum key distribution. *Phys Rev Lett* 2011; **107**: 110501.
13 Gerhardt I, Liu Q, Lamas-Linares A, Skaar J, Kurtsiefer C *et al.* Full-field implementation of a perfect eavesdropper on a quantum cryptography system. *Nat Commun* 2011; **2**: 349.
14 Weier H, Krauss H, Rau M, Furst M, Nauerth S *et al.* Quantum eavesdropping without interception: an attack exploiting the dead time of single-photon detectors. *New J Phys* 2011; **13**: 073024.
15 Li HW, Wang S, Huang JZ, Chen W, Yin ZQ *et al.* Attacking a practical quantum-key-distribution system with wavelength-dependent beam-splitter and multiwavelength sources. *Phys Rev A* 2011; **84**: 062308.
16 Jiang MS, Sun SH, Li CY, Liang LM. Wavelength-selected photon-number-splitting attack against plug-and-play quantum key distribution systems with decoy states. *Phys Rev A* 2012; **86**: 032310.
17 Peev M, Pacher C, Alléaume R, Barreiro C, Bouda J *et al.* The SECOQC quantum key distribution network in Vienna. *New J Phys* 2009; **11**: 075001.
18 Chen TY, Wang J, Liang H, Liu HY, Liu Y *et al.* Metropolitan all-pass and inter-city quantum communication network. *Opt Express* 2010; **18**: 27217–27225.
19 Wang S, Chen W, Yin ZQ, Zhang Y, Zhang T *et al.* Field test of wavelength-saving quantum key distribution network. *Opt Lett* 2010; **35**: 2454–2456.
20 Stucki D, Legré M, Buntschu F, Clausen B, Felber N *et al.* Long-term performance of the SwissQuantum quantum key distribution network in a field environment. *New J Phys* 2011; **13**: 123001.
21 Sasaki M, Fujiwara M, Ishizuka H, Klaus W, Wakui K *et al.* Field test of quantum key distribution in the Tokyo QKD Network. *Opt Express* 2011; **19**: 10387–10409.
22 Yoshino K, Ochi T, Fujiwara M, Sasaki M, Tajima A. Maintenance-free operation of WDM quantum key distribution system through a field fiber over 30 days. *Opt Express* 2013; **21**: 31395–31401.
23 Patel KA, Dynes JF, Lucamarini M, Choi I, Sharpe AW *et al.* Quantum key distribution for 10 Gb/s dense wavelength division multiplexing networks. *Appl Phys Lett* 2014; **104**: 051123.
24 Korzh B, Lim CCW, Houlmann R, Gisin N, Li MJ *et al.* Provably secure and practical quantum key distribution over 307 km of optical fibre. *Nat Photonics* 2015; **9**: 163–168.
25 Zhang J, Itzler MA, Zbinden H, Pan JW. Advances in InGaAs/InP single-photon detector systems for quantum communication. *Light: Sci Appl* 2015; **4**: e286, doi:10.1038/lsa.2015.59.
26 Liang Y, Zeng HP. Single-photon detection and its applications. *Sci China-Phys Mech Astron* 2014; **57**: 1218–1232.
27 Kurtsiefer C, Zarda P, Mayer S, Weinfurter H. The breakdown flash of silicon avalanche photodiodes-back door for eavesdropper attacks? *J Mod Opt* 2001; **48**: 2039–2047.
28 Goetzberger A, McDonald B, Haitz RH, Scarlett RM. Avalanche effects in silicon *p–n* junctions. II. structurally perfect junctions. *J Appl Phys* 1963; **34**: 1591–1600.
29 Lacaita AL, Zappa F, Bigliardi S, Manfredi M. On the bremsstrahlung origin of hot-carrier-induced photons in silicon devices. *IEEE Trans Electron Devices* 1993; **40**: 577–582.
30 Acerbi F, Tosi A, Zappa F. Avalanche current waveform estimated from electroluminescence in InGaAs/InP SPADs. *IEEE Photonics Technol Lett* 2013; **25**: 1778–1780.
31 Healey P. Optical time domain reflectometry—a performance comparison of the analogue and photon counting techniques. *Opt Quantum Electron* 1984; **16**: 267–276.
32 Warburton R, Itzler M, Buller GS. Free-running, room temperature operation of an InGaAs/InP single-photon avalanche diode. *Appl Phys Lett* 2009; **94**: 071116.
33 Eraerds P, Legré M, Zhang J, Zbinden H, Gisin N. Photon counting OTDR: advantages and limitations. *J Light Technol* 2010; **28**: 952–964.
34 Rastello ML, Degiovanni IP, Sinclair AG, Kuck S, Chunnilall CJ *et al.* Metrology for industrial quantum communications: the MIQC project. *Metrologia* 2014; **51**: S267–S275.
35 Piacentini F, Meda A, Traina P, Suk HK, Degiovanni IP *et al.* Measurement facility for the evaluation of the backscattering in fiber: realization of an OTDR operating at single photon level. *Int J Quantum Inform* 2014; **12**: 1461014.
36 Tosi A, Della Frera A, Bahgat Shehata A, Scarcella C. Fully programmable single-photon detection module for InGaAs/InP single-photon avalanche diodes with clean and sub-nanosecond gating transitions. *Rev Sci Instrum* 2012; **83**: 013104.
37 Bennett BR, Soref RA, Del Alamo JA. Carrier-induced change in refractive index of InP, GaAs and InGaAsP. *IEEE J Quantum Electron* 1990; **26**: 113–122.
38 Lucamarini M, Choi I, Ward MB, Dynes JF, Yuan ZL *et al.* Practical security bounds against the Trojan-horse attack in quantum key distribution. *Phys Rev X* 2015; **5**: 031030.
39 Namekata N, Sasamori S, Inoue S. 800 MHz Single-photon detection at 1550-nm using an InGaAs/InP avalanche photodiode operated with a sine wave gating. *Opt Express* 2006; **14**: 10043–10049.
40 Yuan ZL, Kardynal BE, Sharpe AW, Shields AJ. High speed single photon detection in the near infrared. *Appl Phys Lett* 2007; **91**: 041114.
41 Dixon AR, Dynes JF, Yuan ZL, Sharpe AW, Bennett AJ *et al.* Ultrashort dead time of photon-counting InGaAs avalanche photodiodes. *Appl Phys Lett* 2009; **94**: 231113.
42 Liang XL, Liu JH, Wang Q, Du DB, Ma J *et al.* Fully integrated InGaAs/InP single-photon detector module with gigahertz sine wave gating. *Rev Sci Instrum* 2012; **83**: 083111.
43 Restelli A, Bienfang JC, Migdall AL. Single-photon detection efficiency up to 50% at 1310 nm with an InGaAs/InP avalanche diode gated at 1.25 GHz. *Appl Phys Lett* 2013; **102**: 141104.
44 Scarcella C, Boso G, Ruggeri A, Tosi A. InGaAs/InP single-photon detector gated at 1.3 GHz With 1.5% afterpulsing. *IEEE J Sel Topics Quantum Electron* 2015; **21**: 3800306.
45 Marsili F, Verma VB, Stern JA, Harrington SA, Lita AE *et al.* Detecting single infrared photons with 93% system efficiency. *Nat Photonics* 2013; **7**: 210–214.
46 Hu XL, Cheng YH, Gu C, Zhu XT, Liu HY. Superconducting nanowire single-photon detectors: recent progress. *Sci Bull* 2015; **60**: 1980–1983.
47 Zhang LB, Wan C, Gu M, Xu RY, Zhang S *et al.* Dual-lens beam compression for optical coupling in superconducting nanowire single-photon detectors. *Sci Bull* 2015; **60**: 1434–1438.
48 Nauerth S, Furst M, Schmitt-Manderbach T, Weier H, Weinfurter H. Information leakage via side channels in freespace BB84 quantum cryptography. *New J Phys* 2009; **11**: 065001.
49 Brassard G, Lutkenhaus N, Mor T, Sanders BC. Limitations on practical quantum cryptography. *Phys Rev Lett* 2000; **85**: 1330–1333.
50 Bennett CH, Brassard G, Crepeau C, Maurer UM. Generalized privacy amplification. *IEEE Trans Inf Theory* 1995; **41**: 1915–1923.
51 Bennett CH, Bessette F, Brassard G, Salvail L, Smolin J. Experimental quantum cryptography. *J Cryptol* 1992; **5**: 3–28.
52 Dusek QM, Lutkenhaus N, Hendrych M. Quantum cryptography. In: Wolf E, editor. *Progress in Optics*. Amsterdam: Elsevier; 2006. p381–454.

This work is licensed under a Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License. The images or other third party material in this article are included in the article's Creative Commons license, unless indicated otherwise in the credit line; if the material is not included under the Creative Commons license, users will need to obtain permission from the license holder to reproduce the material. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-sa/4.0/

© The Author(s) 2017