Hacking the Quantum Key Distribution System by Exploiting the Avalanche-Transition Region of Single-Photon Detectors

Yong-Jun Qian,[1,2,3] De-Yong He,[1,2,3] Shuang Wang,[1,2,3,*] Wei Chen,[1,2,3] Zhen-Qiang Yin,[1,2,3]
Guang-Can Guo,[1,2,3] and Zheng-Fu Han[1,2,3]

[1] *CAS Key Laboratory of Quantum Information, University of Science and Technology of China, Hefei 230026, China*

[2] *CAS Center for Excellence in Quantum Information and Quantum Physics, University of Science and Technology of China, Hefei 230026, China*

[3] *State Key Laboratory of Cryptology, P.O. Box 5159, Beijing 100878, China*

(Received 7 August 2018; revised manuscript received 10 November 2018; published 28 December 2018)

Avalanche-photodiode-based single-photon detectors (SPDs), as crucial and practical components, are widely used in quantum key distribution (QKD) systems. For effective detection, most of these SPDs are operated in the gated mode, in which the gate is added to obtain high avalanche gain and is removed to quench the avalanche. The avalanche-transition region (ATR) is certain to exist in the process of adding and removing the gate. We first experimentally investigate the characteristic of the ATR, including in a commercial SPD and a high-speed SPD, and then propose an ATR attack to control the detector. In the experiment on hacking the plug-and-play QKD system, Eve introduces less than 0.5% quantum bit error rate and almost leaves no traces of her presence, including the photocurrent and afterpulse probability. We finally give possible countermeasures against this attack.

DOI: 10.1103/PhysRevApplied.10.064062

I. INTRODUCTION

Quantum key distribution (QKD) enables two remote parties, commonly known as Alice and Bob, to share a string of secure keys [1]. The eavesdropper, Eve, cannot obtain any information without introducing errors. As the first application of quantum information in wide fields, the unconditional security of the BB84 QKD protocol has been proven [2–5].

Generally, the source, modulators, and detectors are the main components in a QKD system. The models of these components are ideal in security proof, while these components have imperfections in real life. The gaps between ideal models and imperfect components would leave loopholes for Eve and threaten the practical security [6–28]. For instance, the original BB84 protocol requires a perfect single-photon source, but most practical QKD systems used a weak coherent source. The existence of multiphoton states gave Eve a chink to implement a photon-number-splitting attack until the decoy-state method was proposed [8,9,29,30].

A single-photon detector (SPD) is an indispensable component for a BB84 QKD system, but as a complex one at the receiver's side, there are many loopholes that Eve can exploit to hack the system [14–28]. Recently, a series of hacking types, named "detector-control attacks," have been proposed [20–28]. One of the most famous attacks is a detector-blinding attack [20–24], where the eavesdropper blinds the SPDs and then remotely controls them to steal all keys without increasing the quantum bit error rate (QBER), but it requires bright illumination. Moreover, faint trigger pulses can also be used to control SPDs without extra blinding light, but the increased QBER is relatively high (more than 12%) to be discovered [26].

Several strategies have been proposed to defend against these detector-control attacks. The most-attractive approach is a measurement-device-independent protocol [31] that can remove all detector-side channel attacks, but experimental challenges and relatively low secure-key rates need to be overcome before commercial application. Another approach is to improve existing systems, such as monitoring optical illumination [20,32], photocurrent [33–35], and afterpulse [36], or randomly removing gates to check the clicks [25]. The improvement approach minimizes changes to the original system. But some of these methods do not close all underlying loopholes or do not have a strictly theoretical proof, and new proposed attacks may defeat the QKD system.

Here we propose an avalanche-transition-region (ATR) attack on gated-mode avalanche-photodiode (APD) detectors, which are widely used in QKD systems [37]. When the gate is *on*, the detector is in the Geiger mode and sensitive to the single photon. When the gate is *off*, it is in the linear mode and cannot detect the single photon. The

[*] wshuang@ustc.edu.cn

ATR refers to the region from the Geiger mode to the linear mode. When weak multiphoton signals arrive at this region, the probability of being detected depends on the delay in the ATR and the incident flux at matching basis and mismatching basis. Eve can implement an ATR attack to steal all keys but introduce almost no errors (less than 0.5%). Moreover, since the incident flux is faint and the avalanche gain factor in the ATR is relatively small, the strategies of monitoring illumination, photocurrent, and afterpulse are inoperative.

II. ATR-ATTACK MODEL

For an APD detector operated in the Geiger mode, the reverse bias voltage should be above the breakdown voltage ($V_{\rm BD}$) when the gate is *on*. As shown in Fig. 1, in normal operation, a single-photon pulse arrives in the gate and creates a detectable macrosopic current signal. Then the gate should be removed to quench the avalanche [37]. In reality, there must be a voltage transition in the process of removing the gate. Since the avalanche gain factor decreases with reduction of the bias voltage on the APD [38–40], this voltage-transition region is also an ATR. In this region, a single-photon pulse cannot be detected, but a multiphoton pulse (hundreds to thousands of photons) would create a superimposed avalanche signal, whose amplitude is comparable with that of a single avalanche signal created by a single-photon pulse at the gate.

The ATR of the APD detector is experimentally characterized by measurement of the detection probability at different positions and with different incident fluxes. The commercial SPD (ID201, ID Quantique) under test is based on an In-Ga-As APD with a gate width of 2.5 ns. With a gating rate of 1 MHz, this SPD is illuminated by a variable-intensity pulse with a repetition rate of 1 MHz and temporal width of 30 ps at 1550 nm. As shown in Fig. 2, the detection probability of this SPD changes greatly with the position and incident flux. When the incident flux is 0.1 photon/pulse [the black curve in Fig. 2(a)], the delay between the incident pulse and the gate signal is carefully tuned to get the maximum detection probability. The maximum detection probability is about 1.33% (corresponding to 13.4% detection efficiency) in the gate-signal region, and the corresponding delay time is set as the zero point. To show the characteristics of the ATR clearly, we display the data in the range only from the position of 1.06-ns delay to 1.26-ns delay in Fig. 2. When the incident flux increases to the level of hundreds of photons, the corresponding detection probability increases greatly even in the ATR, but reduces with the position away from the gate signal. In the region from 1.11 to 1.21 ns, the ranges for the reduction of the detection probability with different incident fluxes are different; for instance, the range is from 98.7% to 0.52% for a flux of 890 photons/pulse [red curve in Fig. 2(a)], is from 18.6% to 0.04% for a flux of 445 photons/pulse [blue curve in Fig. 2(a)], and remains at the dark-count probability level for a flux of 0.1 photon/pulse [black curve in Fig. 2(a)]. Furthermore, the detection probability is also investigated with increase of the incident flux for five given positions in the ATR (their delay values are 1.06, 1.11, 1.16, 1.21, and 1.26 ns, respectively). For each curve in Fig. 2(b), the detection probability starts rising gently, then increases steeply, and finally the increase

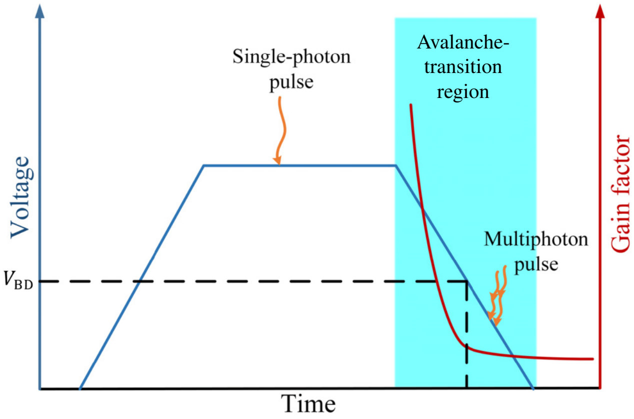

FIG. 1. Conceptual avalanche-transition region. $V_{\rm BD}$ denotes the breakdown voltage.

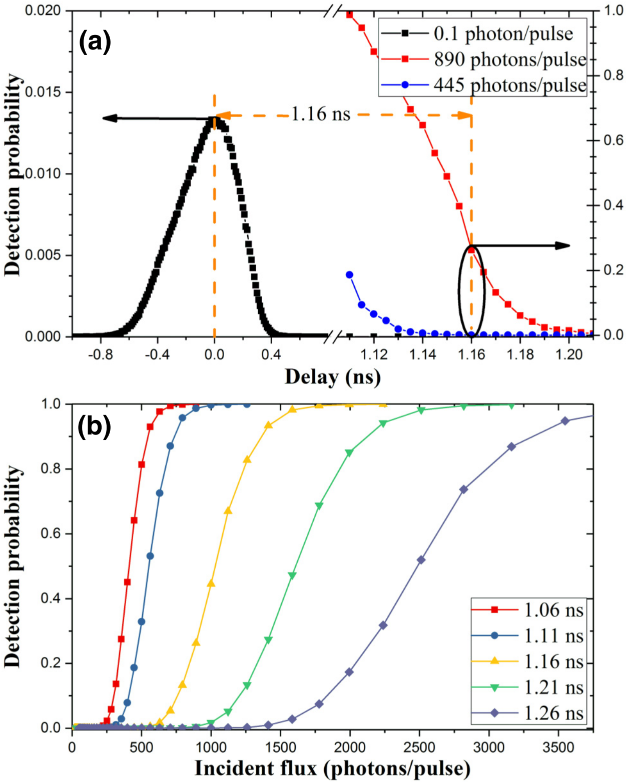

FIG. 2. Characteristic of the ATR. (a) The detection probability versus delay position with different incident fluxes. (b) The detection probability versus incident flux of the pulse at different delay positions.

slows down to saturation. It is obvious that the steepness of the increase of the detection probability is weakened as the position in the ATR is far from the gate signal. The farther in the ATR the position is, the lower the bias voltage on the APD is, the smaller the avalanche gain factor is, and then more incident photons are needed to create a superimposed signal with the same amplitude.

The property that the detection probability increases steeply with the incident flux in the ATR can be used by Eve to control the APD detector operated in the gated mode. With a position of 1.16-ns delay, for example, the detection probability is 26.2% when the incident flux is 890 photons/pulse, and reduces to 0.083% when the incident flux halves to 445 photons/pulse. Thus, to control Bob's detector, Eve could send encoded multiphoton pulses with a flux of 890 photons/pulse to Bob (assuming Bob's decoding components are lossless) and make these pulses arrive at the detector at the position of 1.16-ns delay. If Eve and Bob select matching bases, these encoded multiphoton pulses have a high probability of being detected. If Eve and Bob select opposite bases, half the flux of these encoded multiphoton pulses hits the detector and has a very low probability of being detected. After Bob publicly acknowledges his detected signals, Eve would have almost identical choices of bases and bit values as Bob. That means Eve could steal almost all information on the secure keys shared between Alice and Bob but leave almost no trace if she used such an attack, which is named an "ATR attack."

An ATR attack is a general challenge for QKD systems with APD detectors operated in the gated mode, in which the ATR is necessary. In addition to the widely used commercial In-Ga-As SPD, two types of homemade SPD are tested to characterize the ATR. One is similar to the ID201 SPD, operating at 1 MHz, and the other uses the sine-wave filtering method, operating at 1 GHz [41]. As before, the delay with the maximum detection probability at 0.1 photon/pulse is set as the zero point. For the homemade 1-MHz SPD, at a delay of 1.09 ns, the detection probability is 21.5% when the incident flux is 890 photons/pulse, and reduces to 0.107% when the incident flux halves to 445 photons/pulse. The detection probability is 36.3% when the incident flux is 1000 photons/pulse and reduces to 0.29% when the incident flux halves to 500 photons/pulse. For the homemade 1-GHz SPD, at a delay of 300 ps, the detection probability is 40% when the incident flux is 1000 photons/pulse and reduces to 1.53% when the incident flux halves to 500 photons/pulse.

III. ATTACKING EXPERIMENT ON THE QKD SYSTEM

The ATR-attack experiment is demonstrated on the plug-and-play QKD system [42], similar to the commercial ID3110 Clavis2 QKD system. The upper part of Fig. 3 shows the schematic setup of the system working in normal operation, and the BB84 protocol is implemented. To be simple and precise, four phases (0, $\pi/2$, π, $3\pi/2$) are randomly modulated at Bob's site, and thus only one SPD is needed to implement the whole BB84 protocol. An ID201 SPD is used to detect the output signal of the 50:50 beam splitter at Bob's site.

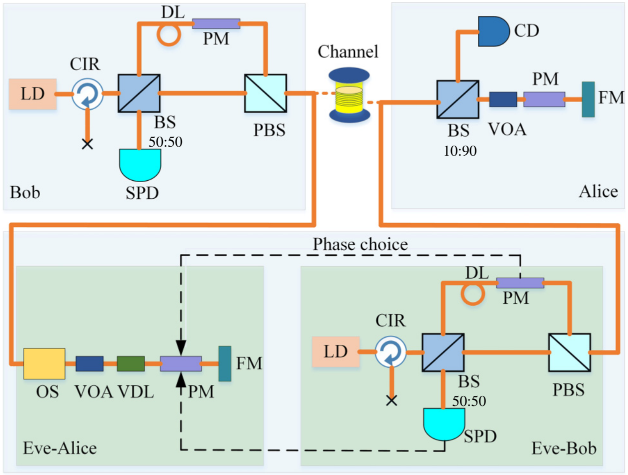

FIG. 3. Experimental demonstration of an ATR attack on the plug-and-play QKD system. The original system is composed of Alice and Bob (upper part). Eve's setup consists of Eve-Alice and Eve-Bob (bottom part). BS, beam splitter; CD, classical detector; CIR, circulator; DL, delay line; FM, Faraday mirror; LD, laser diode; OS, optical switch; PBS, polarization beam splitter; PM, phase modulator; VDL, variable delay line; VOA, variable optical attenuator.

Combined with an intercept-resend strategy, Eve can steal Alice's and Bob's secret keys without being discovered. Eve's setup is shown in the bottom part of Fig. 3, which consists of Eve-Bob and Eve-Alice. First, Eve-Bob sends strong pulses to Alice, and randomly chooses one of the phases (0, $\pi/2$, π, $3\pi/2$) after receiving the coding signals from Alice. From the responses of the SPD and the phase chosen, Eve can guess the phases that Alice encodes on the pulses, although the possibility of a correct guess is 50%. Then Eve-Alice intercepts the strong pulses from Bob, modulates the guessed phases on these pulses, and resends these multiphoton pulses to Bob. The key of the ATR attack is that Eve-Alice should carefully control the delay of these coding pulses to make them arrive in the ATR of Bob's SPD and should also carefully control the incident flux of these pulses on the basis of the characteristic of the ATR of the SPD. The variable delay line and the variable optical attenuator in Fig. 3 are used to tune the delay and incident flux of the coding pulses. The optical switch is used to control the resending number of multiphoton pulses. As shown in the detection tree of the ATR attack (see Fig. 4), the pulses intercepted by Eve-Alice have very high (or zero) probability of being detected by

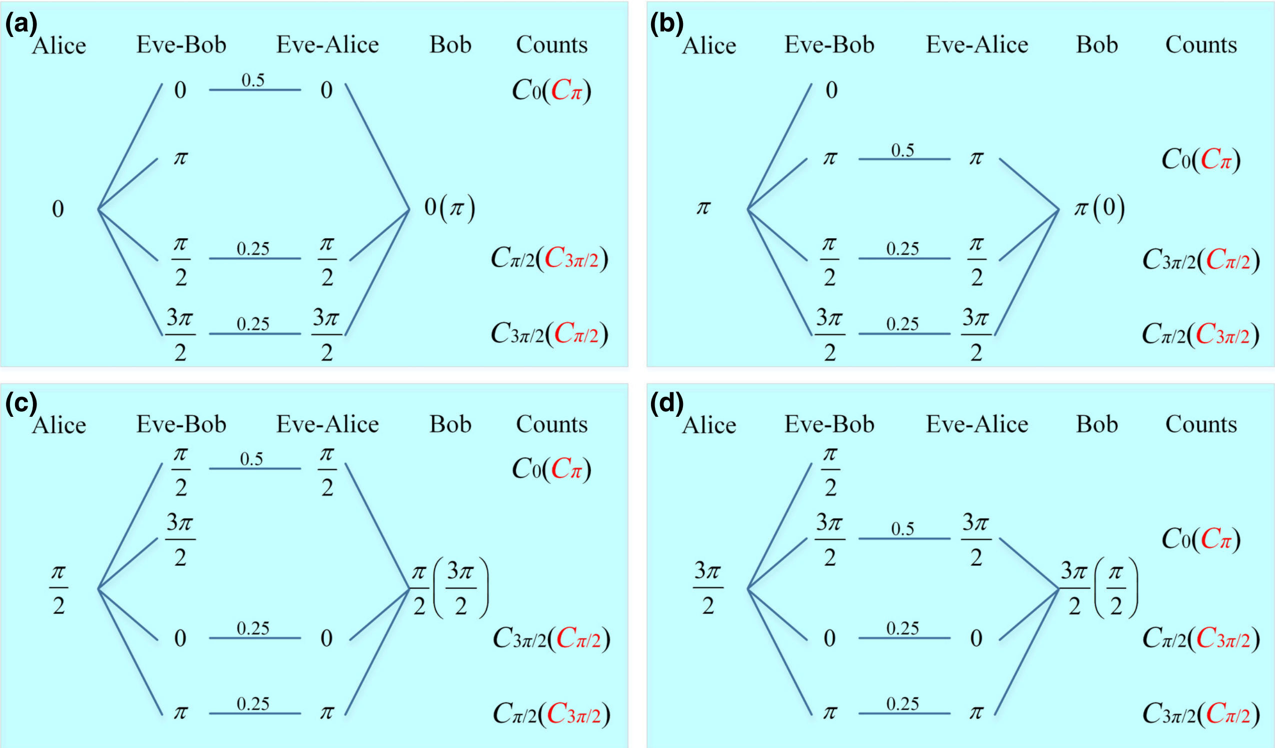

FIG. 4. Detection tree of ATR attack combined with an intercept-resend strategy. In (a)–(d), each column indicates the phase one chooses. The detection counts marked in red indicate error counts introduced by Eve.

Bob's SPD if the phase difference between Eve-Alice and Bob is 0 (or π), and the counts of Bob's SPD are denoted as C_0 (C_π) when Eve and Bob choose matching bases. The pulses intercepted by Eve-Alice have very low probability of being detected by Bob's SPD if the phase difference between Eve-Alice and Bob is $\pi/2$ or $3\pi/2$, and these counts are denoted as $C_{\pi/2}$ and $C_{3\pi/2}$, respectively, when Eve and Bob choose opposite bases. Thus, the QBER of the attacked QKD system can be given as

$$e_{\text{QBER}} = \frac{C_{3\pi/2} + C_{\pi/2} + 2C_\pi}{2(C_0 + C_{\pi/2} + C_\pi + C_{3\pi/2})}. \tag{1}$$

Since the four phases are randomly modulated and only one SPD is used at Bob's site, and similar processes are also used at Eve's site, C_π corresponds to the error counts coming from apparatus imperfections [43]. When Eve-Alice and Bob choose matching bases and their phase difference is π, a very small portion of the multiphoton pulses will hit the SPD, and the detection probability of this small flux in the ATR is very close to 0, so C_π is almost equal to 0. When Eve-Alice and Bob choose opposite bases, we have $C_{\pi/2} = C_{3\pi/2}$. If Eve-Alice resends M multiphoton pulses per second and the detection probability of Bob's SPD is denoted as P_f with full incident flux and P_h with half incident flux, the counts can be expressed as $C_0 = \frac{1}{4}M \cdot P_f$ and $C_{\pi/2} = C_{3\pi/2} = \frac{1}{4}M \cdot P_h$. Then Eq. (1) can be simplified as

$$e_{\text{QBER}} \simeq \frac{C_{\pi/2}}{C_0 + 2C_{\pi/2}} = \frac{P_h}{P_f + 2P_h}. \tag{2}$$

In the ATR-attack experiment, Eve-Alice carefully tunes her variable delay line to make the resending multiphoton pulses arrive at the position of 1.16-ns delay, and tunes her variable optical attenuator to make the flux hitting Bob's SPD be close to 890 photons/pulse if the phase difference between Eve-Alice and Bob is 0, and also controls her optical switch to ensure the counts of Bob's SPD are nearly unchanged. The experimental results are shown in Fig. 5, which presents Bob's detection counts versus the phase difference for different cases. The first bar (blue one) for each phase difference corresponds to normal operation without Eve, and the phase difference is between Alice and Bob. The second and third bars correspond to the case with an ATR attack: the phase difference for the second bar (orange one) is between Eve (Eve-Alice) and Bob and for the third bar (red one) is between Alice and Bob. It is obvious that Eve has totally controlled Bob's SPD, and the statistical counts between Bob and Alice are almost identical before and after the ATR attack. More importantly, the QBER of the QKD system is nearly unchanged after the attack. According to the second bar (orange one) at each phase difference and Eq. (1), the QBER under the

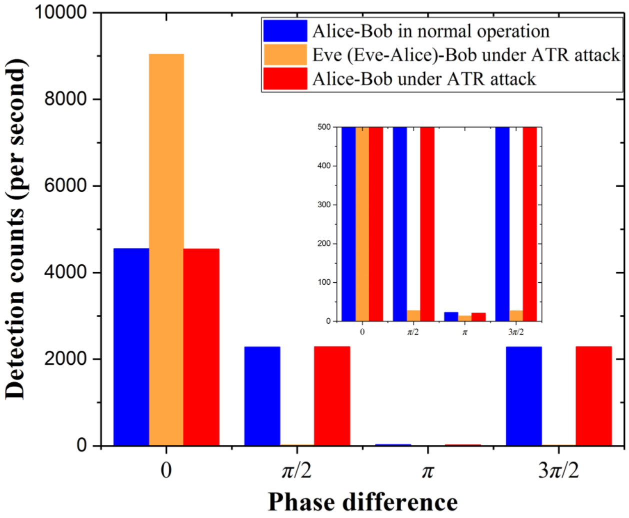

FIG. 5. Bob's detection counts versus the phase difference in different cases.

ATR attack is approximately 0.48%, which originates from imperfections of Eve's apparatus and the characteristic of the ATR of Bob's SPD. At the position of 1.16-ns delay with full incident flux of 890 photons/pulse, $P_f = 26.2\%$ and $P_h = 0.083\%$. If Eve's apparatus is perfect, the QBER introduced by the ATR attack is approximately 0.31% according to Eq. (2). On the basis of the ATR attack, Eve can obtain all information on the secure keys by hiding her presence in the QBER of the QKD system, since the QBER introduced by this attack is small enough.

We emphasize that the goal of research on quantum hacking is to enhance the practical security of QKD through openly discovering and closing security loopholes [20]. The ATR-attack experiment is demonstrated in a proof-in-principle manner with only one SPD. Since the ATR attack is time sensitive, the effectiveness of this attack would be reduced if two or more SPDs were used in the QKD system and they had different properties in the ATR. For example, with an incident flux of 890 photons/pulse and the hacking position chosen for the commercial SPD corresponding to a delay of 1.16 ns, the QBER introduced by Eve is approximately 0.31%; for the hacking position chosen for the homemade SPD corresponding to a delay of 1.09 ns, the QBER introduced by Eve is approximately 0.49%. For these two SPDs, the hacking positions have a time mismatch of 0.07 ns. However, this mismatch could be compensated by exploitation of the weakness of the calibration routine [44], which was proposed by Jain *et al.* [44]. In Ref. [44], Eve causes a temporal separation of up to 0.45 ns between two SPDs in a commercial QKD system.

IV. COUNTERMEASURES

In the ATR attack, Eve resends the attacking pulses to the ATR of Bob's SPD and totally controls the detector. Several countermeasures have been proposed to defeat detector-control attacks. We first discuss some existing possible countermeasures against an ATR attack.

Monitoring the photocurrent of the APD is an effective way to detect most detector-control attacks [33,35], since these attacks would leave an obvious fingerprint of high photocurrent (more than 40 times stronger than the photocurrent under normal operation). But in an ATR attack, the photocurrent could be equal to or even less than the photocurrent under normal operation. Suppose the photocurrents per detection count with full and half incident flux are i_f and i_h, respectively, which can be obtained when we measure the detection probability of Bob's SPD under full and half incident flux. If Eve-Alice resends M attacking pulses per second and Bob gets C detection counts, then $C = C_0 + C_{\pi/2} + C_\pi + C_{3\pi/2} \simeq \frac{1}{4}M(P_f + 2P_h)$. If Bob monitors the photocurrent of his SPD, the average photocurrent will be

$$I_{\text{avg}} = \frac{C(P_f i_f + 2P_h i_h)}{P_f + 2P_h}, \tag{3}$$

where the background photocurrent of the SPD has been ignored. To measure the photocurrent characteristic under an ATR attack, the ID201 SPD is replaced by the similar homemade SPD, and the attacking position is changed from 1.16- to 1.09-ns delay. For different incident fluxes, the corresponding detection probability (black points), the average photocurrent (red points), and the QBER (blue points) are shown in Fig. 6. The dashed red line denotes

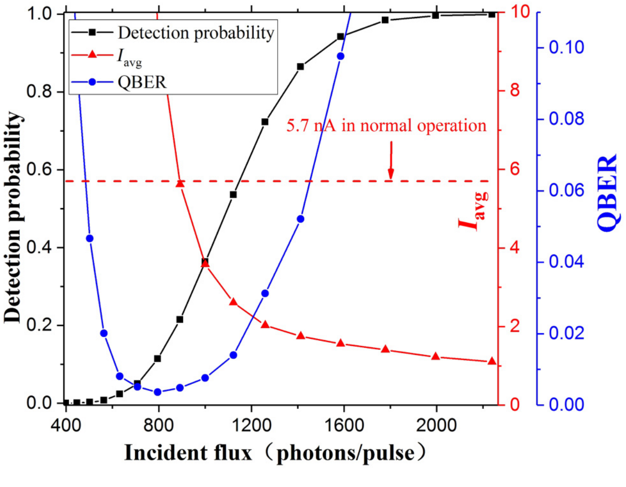

FIG. 6. The detection probability, average photocurrent (I_{avg}), and QBER versus incident flux. The detection probability is measured in the experiment. The average photocurrent is calculated with Eq. (3) on the basis of the measured photocurrents per detection i_f and i_h and detection probabilities P_f and P_h, under the condition that Bob's detection count remains the same as that in normal operation. The QBER introduced by the ATR attack is calculated according to Eq. (2) on the basis of the measured detection probabilities P_f and P_h.

the average photocurrent under normal operation with a value of 5.7 nA, and the corresponding detection count is approximately 9.11×10^3 per second. When the incident flux is 890 photons/pulse, the photocurrents per detection count with full and half flux are 0.287 and 33.832 pA per count, respectively. The average photocurrent is about 5.6 nA, and the QBER is less than 0.5%. From the point of view of the average photocurrent and QBER, it is hard to detect the ATR attack. When the incident flux is further increased, the average photocurrent will decrease if the detection count remains unchanged. Thus, monitoring the average photocurrent is ineffective to detect the ATR attack.

In the second approach, afterpulses caused by macroscopic APD current are non-negligible [35]. For instance, the afterpulse probability increased from 1.79% to 76.6% after an after-gate attack [36]. For the ID201 SPD in the QKD system under an ATR attack in Sec. III, the incident fluxes at the position of 1.16-ns delay are 890, 445, 0, and 445 photons/pulse with equal probability, corresponding to the four phase differences 0, $\pi/2$, π, and $3\pi/2$, respectively, between Eve-Alice and Bob. Following the method proposed by Yuan *et al.* [45], the afterpulse probability is measured as 0.57%, which is consistent with the low QBER under an ATR attack. So the second approach is also ineffective to find the ATR attack.

A third possible countermeasure is to randomly remove gates and check clicks at the positions without gates [25], which is based on the property that clicks still occur under attacks. The effectiveness of this countermeasure against an ATR attack is checked by the following experiment: the ID201 SPD is triggered with a repetition rate of 1 MHz and is illuminated by a pulse train with a rate of 2 MHz. This is equivalent to removing half of the 2-MHz gates. In the normal case, the pulse train with a flux of 0.1 photon/pulse arrives at the zero point (with maximum detection probability). The temporal distribution of the normalized detection counts is shown in Fig. 7(a). Clicks occur only with gates, and there are no clicks at the removed gates. In the ATR-attack case, the pulse train with a flux of 890 photons/pulse arrives at the position of 1.16-ns delay. The corresponding temporal distribution of the normalized detection counts is shown in Fig. 7(b), which is similar to the normal case, and there are still no clicks at the removed gates. Since the output of the ATR-attacking pulse mainly depends on the avalanche gain factor of the APD, if the gate were removed, the gain factor would be very small and no clicks would occur. Hence, removing the gate is also invalid to detect the ATR attack.

The three existing countermeasures cannot effectively detect the proposed ATR attack. However, we find that the temporal distribution of detection counts under an ATR attack is different from that under normal operation. The temporal distribution of detection counts of the ID201 SPD is measured with 1-ps timing resolution, as shown in Fig. 8. Under normal operation (blue points in Fig. 8), the detector is illuminated by an incident flux of 0.1 photon/pulse at the zero point. Under the ATR attack (red points in Fig. 8), the detector is illuminated by an incident flux of 890 photons/pulse at the 1.16-ns-delay position. The temporal distribution of detection counts under normal operation is relatively concentrated in a small range (from −0.05 to 0.05 ns), while the temporal distribution under the ATR attack is relatively wide (from −0.05 to 0.15 ns) and its center is delayed by about 0.043 ns. These differences might be an approach to find an ATR attack.

Additionally, since the avalanche gain factor in the ATR of the APD is time sensitive, the QBER of the QKD system introduced by the ATR attack would increase if the time jitter of the gate becomes large. For instance, when

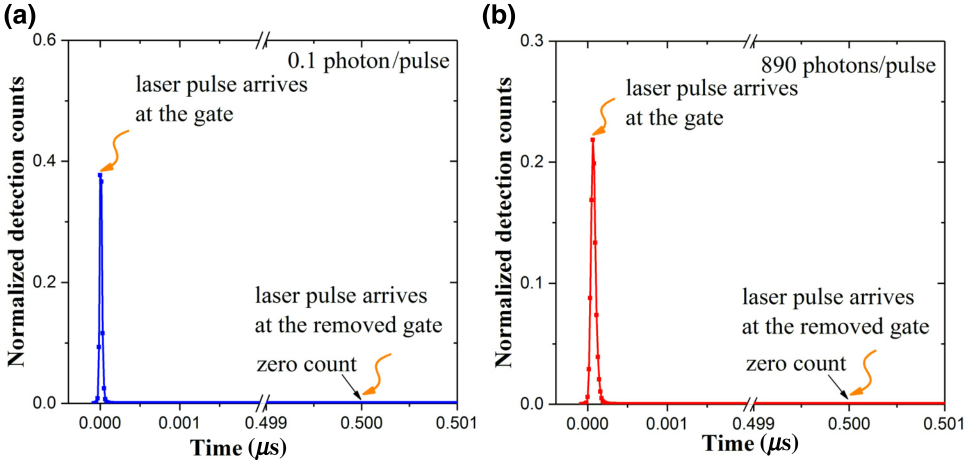

FIG. 7. Checking of detection counts at the gate and at the removed gate. The SPD is triggered a rate of 1 MHz and illuminated by a laser pulse train with a rate of 2 MHz. (a) The laser pulse train arrives at the zero point in the gate with 0.1 photon/pulse. (b) The laser pulse train arrives with 1.16-ns delay with 890 photons/pulse. The timing resolution is 16 ps.

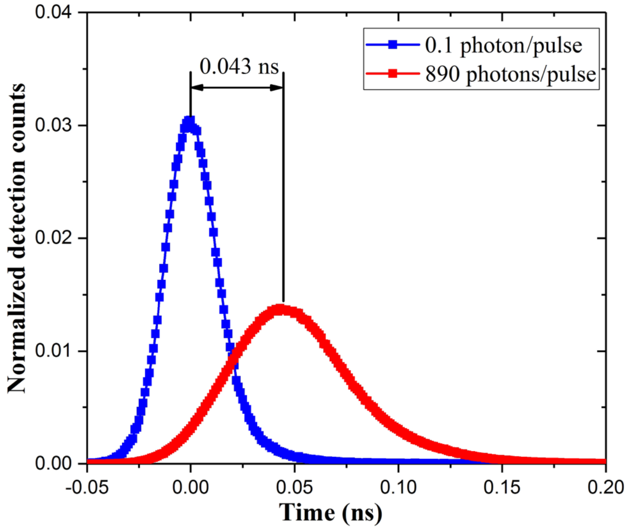

FIG. 8. Temporal distribution of normalized detection counts. The timing resolution is 1 ps.

the setting of the ID201 SPD "trigger delay" is changed from "bypass" to "set 15 ns," the full width at half maximum of the time jitter of the gate (through measurement of the "gate out" signal) increases from 19 to 65 ps. Then at the position of 1.16-ns delay, the detection probability with an incident flux of 890 photons/pulse increases from 26.2% to 97.6%, that with half flux (445 photons/pulse) increases from 0.083% to 44.9%, and the QBER introduced by the ATR attack increases to 24%. Still, Eve could change the incident flux to reduce her introduced QBER. If the full incident flux is changed to 400 photons/pulse, the detection probability is 31.3% for full flux and 0.56% for half flux, and the QBER introduced by the ATR attack is about 1.7%.

V. CONCLUSION

In this paper, we propose and demonstrate an attack strategy exploiting the characteristic of the ATR of the gated-mode SPD. The proposed ATR attack is a general challenge for QKD systems using APD-based detectors operated in the gated mode. Through choice of the proper attacking position in the ATR and incident flux of attacking pulses, Eve could almost completely control Bob's detector. In the attacking experiment on the plug-and-play QKD system, the detection counts with different phase differences and QBER are identical before and after the ATR attack. Since the QBER introduced by Eve is less than 0.5%, Eve could hide her presence in the original error under normal operation. Also, three existing countermeasures against detector-control attacks are invalid to detect the proposed ATR attack. However, on the basis of the experimental observations, we propose possible countermeasures to reveal the attack. The ATR attack highlights the importance of detection signals in practical QKD systems.

ACKNOWLEDGMENTS

This work was supported by the National Natural Science Foundation of China (Grants No. 61622506, No. 61575183, No. 61627820, No. 61475148, and No. 61675189), the National Key Research and Development Program of China (Grants No. 2018YFA0306400 and No. 2016YFA0302600), and Anhui Initiative in Quantum Information Technologies.

Y-J.Q. and D-Y.H. contributed equally to this work.

[1] C. H. Bennet and G. Brassard, in *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India, 1984* (IEEE, New York, 1984), p. 175.

[2] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Quantum cryptography, Rev. Mod. Phys. **74**, 145 (2002).

[3] H.-K. Lo and H. F. Chau, Unconditional security of quantum key distribution over arbitrarily long distances, Science **283**, 2050 (1999).

[4] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, The security of practical quantum key distribution, Rev. Mod. Phys. **81**, 1301 (2009).

[5] D. Gottesman, H.-K. Lo, N. Lütkenhaus, and J. Preskill, Security of quantum key distribution with imperfect devices, Quantum Inf. Comput. **4**, 325 (2004).

[6] G. Brassard, N. Lütkenhaus, T. Mor, and B. C. Sanders, Limitations on Practical Quantum Cryptography, Phys. Rev. Lett. **85**, 1330 (2000).

[7] X. B. Wang, Decoy-state quantum key distribution with large random errors of light intensity, Phys. Rev. A **75**, 052301 (2007).

[8] B. Huttner, N. Imoto, N. Gisin, and T. Mor, Quantum cryptography with coherent states, Phys. Rev. A **51**, 1863 (1995).

[9] N. Lütkenhaus and M. Jahma, Quantum key distribution with realistic states: Photon-number statistics in the photon-number splitting attack, New J. Phys. **4**, 44 (2002).

[10] C. H. F. Fung, B. Qi, K. Tamaki, and H. K. Lo, Phase-remapping attack in practical quantum-key-distribution systems, Phys. Rev. A **75**, 032314 (2007).

[11] 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**, 113026 (2010).

[12] 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**, 062331 (2011).

[13] H. W. Li, S. Wang, J. Z. Huang, W. Chen, Z. Q. Yin, F. Y. Li, Z. Zhou, D. Liu, Y. Zhang, G. C. Guo, W. S. Bao, and Z. F. Han, Attacking a practical quantum-key-distribution system with wavelength-dependent beam-splitter and multiwavelength sources, Phys. Rev. A **84**, 062308 (2011).

[14] Y. Zhao, C. H. F. Fung, B. Qi, C. Chen, and H. K. Lo, Quantum hacking: Experimental demonstration of time-shift attack against practical quantum-key-distribution systems, Phys. Rev. A **78**, 042333 (2008).

[15] V. Makarov, A. Anisimov, and J. Skaar, Effects of detector efficiency mismatch on security of quantum cryptosystems, Phys. Rev. A **74**, 022313 (2006).

[16] 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**, 030302 (2016).

[17] N. Jain, C. Wittmann, L. Lydersen, C. Wiechers, D. Elser, C. Marquardt, V. Makarov, and G. Leuchs, Device Calibration Impacts Security of Quantum Key Distribution, Phys. Rev. Lett. **107**, 110501 (2011).

[18] A. Lamas-Linares and C. Kurtsiefer, Breaking a quantum key distribution system through a timing side channel, Opt. Express **15**, 9388 (2007).

[19] 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**, 073024 (2011).

[20] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, Hacking commercial quantum cryptography systems by tailored bright illumination, Nat. Photonics **4**, 686 (2010).

[21] Z. L. Yuan, J. F. Dynes, and A. J. Shields, Avoiding the blinding attack in QKD, Nat. Photonics **4**, 800 (2010).

[22] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, Avoiding the blinding attack in QKD, Nat. Photonics **4**, 801 (2010).

[23] I. Gerhardt, Q. Liu, A. A. Lamas-Linares, J. Skaar, C. Kurtsiefer, and V. Makarov, Full-field implementation of a perfect eavesdropper on a quantum cryptography system, Nat. Commun. **2**, 349 (2011).

[24] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, and J. Skaar, Thermal blinding of gated detectors in quantum cryptography, Opt. Express **18**, 27938 (2010).

[25] 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**, 013043 (2011).

[26] 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**, 032320 (2011).

[27] A. N. Bugge, S. Sauge, A. M. M. Ghazali, J. Skaar, L. Lydersen, and V. Makarov, Laser Damage Helps the Eavesdropper in Quantum Cryptography, Phys. Rev. Lett. **112**, 070503 (2014).

[28] M. S. Jiang, S. H. Sun, G. Z. Tang, X. C. Ma, C. Y. Li, and L. M. Liang, Intrinsic imperfection of self-differencing single-photon detectors harms the security of high-speed quantum cryptography systems, Phys. Rev. A **88**, 062335 (2013).

[29] W.-Y. Hwang, Quantum Key Distribution with High Loss: Toward Global Secure Communication, Phys. Rev. Lett. **91**, 057901 (2003).

[30] H.-K. Lo, X. Ma, and K. Chen, Decoy State Quantum Key Distribution, Phys. Rev. Lett. **94**, 230504 (2005).

[31] H.-K. Lo, M. Curty, and B. Qi, Measurement-Device-Independent Quantum Key Distribution, Phys. Rev. Lett. **108**, 130503 (2012).

[32] S. Wang, W. Chen, Z.-Q. Yin, H.-W. Li, D.-Y. He, Y.-H. Li, Z. Zhou, X.-T. Song, F.-Y. Li, D. Wang, H. Chen, Y.-G. Han, J.-Z. Huang, J.-F. Guo, P.-L. Hao, M. Li, C.-M. Zhang, D. Liu, W.-Y. Liang, C.-H. Miao, P. Wu, G.-C. Guo, and Z.-F. Han, Field and long-term demonstration of a wide area quantum key distribution network, Opt. Express **22**, 21739 (2014).

[33] Z. L. Yuan, J. F. Dynes, and A. J. Shields, Resilience of gated avalanche photodiodes against bright illumination attacks in quantum cryptography, Appl. Phys. Lett. **98**, 231104 (2011).

[34] 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**, 196101 (2011).

[35] Z. L. Yuan, J. F. Dynes, and A. J. Shields, Response to “Comment on ‘Resilience of gated avalanche photodiodes against bright illumination attacks in quantum cryptography’ ”, Appl. Phys. Lett. **99**, 196101 (2011).

[36] T. F. da Silva, G. B. Xavier, G. P. Temporão, and J. P. von der Weid, Real-time monitoring of single-photon detectors against eavesdropping in quantum key distribution systems, Opt. Express **20**, 18911 (2012).

[37] M. D. Eisaman, J. Fan, A. Migdall, and S. V. Polyakov, Invited review article: Single-photon sources and detectors, Rev. Sci. Instrum. **82**, 071101 (2011).

[38] S. Cova, M. Ghioni, A. Lotito, I. Rech, and F. Zappa, Evolution and prospects for single-photon avalanche diodes and quenching circuits, J. Mod. Opt. **51**, 1267 (2004).

[39] K. S. Hyun and C. Y. Park, Breakdown characteristics in InP/InGaAs avalanche photodiode with pin multiplication layer structure, J. Appl. Phys. **81**, 974 (1997).

[40] J. S. Ng, C. H. Tan, J. P. R. David, and G. J. Rees, Effect of impact ionization in the InGaAs absorber on excess noise of avalanche photodiodes, IEEE J. Quantum Electron. **41**, 1092 (2005).

[41] D.-Y. He, S. Wang, W. Chen, Z.-Q. Yin, Y.-J. Qian, Z. Zhou, G.-C. Guo, and Z.-F. Han, Sine-wave gating InGaAs/InP single photon detector with ultralow afterpulse, Appl. Phys. Lett. **110**, 111104 (2017).

[42] D. Stucki, N. Gisin, O. Guinnard, G. Robordy, and H. Zbinden, Quantum key distribution over 67 km with a plug&play system, New J. Phys. **4**, 41 (2002).

[43] Z. L. Yuan, A. R. Dixon, J. F. Dynes, A. W. Sharpe, and A. J. Shields, Gigahertz quantum key distribution with InGaAs avalanche photodiodes, Appl. Phys. Lett. **92**, 201104 (2008).

[44] N. Jain, C. Wittmann, L. Lydersen, C. Wiechers, D. Elser, C. Marquardt, V. Makarov, and G. Leuchs, Device Calibration Impacts Security of Quantum Key Distribution, Phys. Rev. Lett. **107**, 110501 (2011).

[45] Z. L. Yuan, B. E. Kardynal, A. W. Sharpe, and A. J. Shields, High speed single photon detection in the near infrared, Appl. Phys. Lett. **91**, 041114 (2007).