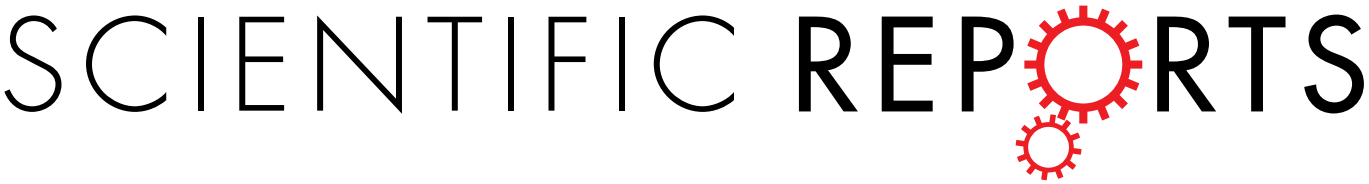

OPEN

Feasible attack on detector-device-independent quantum key distribution

Received: 23 September 2016
Accepted: 1 March 2017
Published online: 27 March 2017

Kejin Wei[1,2], Hongwei Liu[1], Haiqiang Ma[1], Xiuqing Yang[3], Yong Zhang[1], Yongmei Sun[1], Jinghua Xiao[1] & Yuefeng Ji[1]

Recently, to bridge the gap between security of Measurement-device-independent quantum key distribution (MDI-QKD) and a high key rate, a novel protocol, the so-called detector-device-independent QKD (DDI-QKD), has been independently proposed by several groups and has attracted great interest. A higher key rate is obtained, since a single photon bell state measurement (BSM) setup is applied to DDI-QKD. Subsequently, Qi has proposed two attacks for this protocol. However, the first attack, in which Bob's BSM setup is assumed to be completely a "black box", is easily prevented by using some additional monitoring devices or by specifically characterizing the BSM. The second attack, which combines the blinding attack and the detector wavelength-dependent efficiency, is not explicitly discussed, and its feasibility is not experimentally confirmed. Here, we show that the second attack is not technically viable because of an intrinsically wavelength-dependent property of a realistic beam splitter, which is an essential component in DDI-QKD. Moreover, we propose a feasible attack that combines a well-known attack—detector blinding attack with intrinsic imperfections of single-photon detectors. The experimental measurement and proof-of-principle test results confirm that our attack can allow Eve to get a copy of quantum keys without being detected and that it is feasible with current technology.

Quantum key distribution (QKD) enables two legitimate parties, usually called Alice and Bob, to share a private key through a quantum channel, which is possible in the presence of an eavesdropper, Eve[1,2]. Ideal QKD protocols, guaranteed by the laws of quantum mechanics, have been proved to be unconditionally secure without imposing any restrictions on the computational power of Eve[3,4]. However, real-life implementations of QKD inevitably contain certain imperfections leaving some vulnerable loopholes (the so-called side channels). Indeed, such loopholes have been exploited by Eve and have led to various subtle attacks for real-life QKD systems[5–16]. For example, in the security proof of QKD, a key assumption is that two legitimate parties encode their signals without errors, which is violated in a real QKD system. Xu *et al*. have experimentally shown that Eve can exploit such loopholes to launch a phase-remapping attack to steal secure keys without being detected[10]. See ref. 17 for a recent review.

To build loophole-free QKD systems, the one crucial solution is to develop device-independent QKD protocols[18–20], which can remove all loopholes due to imperfect devices. Among them, the measurement-device-independent (MDI) QKD protocol, which is more practical in comparison to other device-independent protocols, has received great attention. MDI-QKD can automatically remove all side channels from measurement apparatus, which are undoubtedly the most critical part of QKD systems. Several groups have experimentally demonstrated the practicality of MDI-QKD with current technology[21–27]. Ref. 28 is a recent review on this topic. However, setups of MDI-QKD, which require a two-photon interference from two individual lasers, are rather complicated and lead to a lower key rate comparing to conventional QKD, such as decoy-state BB84 QKD[29,30].

Recently, to bridge the gap between security of MDI-QKD and a high key rate, a novel protocol, the so-called detector-device-independent QKD (DDI-QKD)[31], has been independently proposed by several groups and has

[1]School of Science and State Key Laboratory of Information Photonics and Optical Communications, Beijing University of Posts and Telecommunications, Beijing, 100876, China. [2]Guangxi Key Laboratory for Relativistic Astrophysics, School of Physics Science and Technology, Guangxi University, Nanning, 530004, China. [3]School of Science, Beijing Jiaotong University, Beijing, 100044, China. Kejin Wei and Hongwei Liu contributed equally to this work. Correspondence and requests for materials should be addressed to H.M. (email: hqma@bupt.edu.cn)

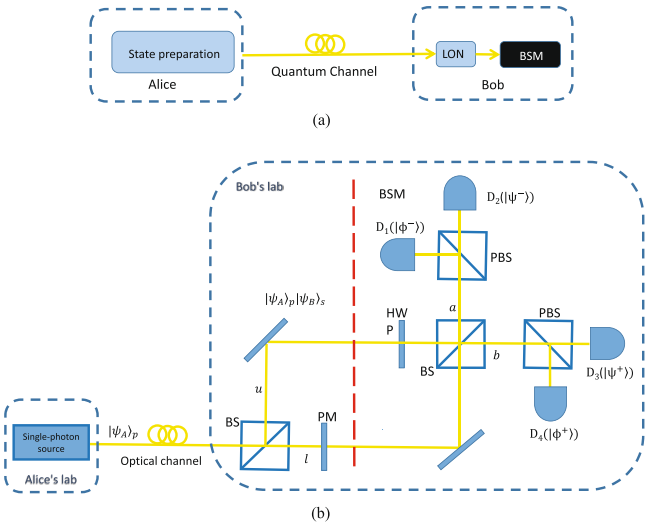

Figure 1. (**a**) Schematic diagram of DDI-QKD. LON is the linear optical network, and BSM is the Bell state measurement. (**b**) Schematic diagram of a specified example of DDI-QKD proposed in ref. 33. BS: 50:50 beam splitter, BSM: Bell state measurement, HWP: half-wave plate, PM: phase modulator, PBS: polarizing beam splitter, and D_i, with $i \in \{1, 2, 3, 4\}$: single-photon detectors in the BSM setup. In Bob's laboratory, the areas before and after the red dashed line denote the LON and the BSM setup, respectively. For the ideal case, a click on each detector D_i corresponds to the projection on one of the four Bell states. $|\psi_A\rangle_p$ is one of the four BB84 polarization states prepared by Alice, and $|\psi_B\rangle_s$ are Bob's encoding bit in spatial mode. Symbols u, l and a, b denote two paths of the first and second BS, respectively. In practice, Alice prepares $|\psi_A\rangle_p$ by generating phase-randomized weak coherent pulses which can be modelled as Poissonian (with parameter u) mixture of photon number states in different BB84 polarization states[1,2,29].

attracted great interest[32–34]. Instead of exploiting two-photon interference in MDI-QKD, this protocol utilizes an untrusted single-photon Bell state measurement (BSM) setup[35]. Consequently, as declared in DDI-QKD, it can still be immune to all detector side-channel attacks, which is the major advantage of MDI-QKD, with a comparable performance of conventional QKD. Subsequently, Qi reported two attacks for this protocol and showed that additional assumptions on the BSM setup are required to reach the claimed DDI-QKD security level[36]. To launch the first attack, the BSM located inside Bob's laboratory is assumed to be completely a "black box" (as the security assumption claimed in refs 32–34), which led to leak of "unwanted" information to Eve. Nevertheless, this attack is easily removed by either introducing additional apparatus to monitor Bob's input signals[32] or specifically characterizing the BSM[34]. The second attack (we call it the *wavelength-dependent attack* since it exploits the detector wavelength-dependent efficiency), combining a well-known detector blinding attack and the detector wavelength-dependent efficiency, allows Eve to learn the total key string without introducing any errors. In the attack, Eve employs bright light to blind Bob's detectors and then controls which detector clicks by carefully tailoring the wavelength of a superimposed bright pulse into the bright light. If detectors in the BSM have different wavelength-dependent efficiencies, Eve exploits such an imperfection to cover unusual double-click rate s caused by her attack. However, ref. 36 does not explicitly discuss the second attack. For example, how can Eve blind four detectors? More importantly, it is unknown whether the attack employing the detector wavelength-dependent efficiency is experimentally feasible. We note that, more recently, a simple implementation of DDI-QKD has been experimentally reported[37].

Here, we show that the wavelength-dependent attack in ref. 36 is not technically viable because of the harm caused by an intrinsically wavelength-dependent property of a realistic beam splitter, which is an essential component in DDI-QKD. Moreover, we propose a feasible attack, the same as the wavelength-dependent attack that is based on the well-known detector-blinding attack. We explain how Eve blind four detectors in detail. To avoid an unusual double-click rate, different from the wavelength-dependent attack, we utilize another imperfection that two practically blinded detectors respond differently to the same blinding power. Our experimental measurement and proof-of-principle test results confirm that our attack can allow Eve to get a copy of a quantum key without being detected and that it is feasible with current technology. We remark that our attack is not against the wavelength-dependent attack; strictly speaking, we propose an alternative solution to the problem of double clicks in the wavelength-dependent attack and experimentally confirm its feasibility.

Results

DDI-QKD. In DDI-QKD (as shown in Fig. 1(a)), Alice generates a single photon in one of the four BB84 polarization states $|\psi_A\rangle_p$ and then sends it to Bob over an insecure quantum channel. Once Bob receives the photon, he exploits a trusted linear optical network (LON), which includes some linear optical components for manipulating the state of an incoming photon, to encode his random bit $|\psi_B\rangle_s$ in a different degree (say spatial) of freedom of the photon. Afterwards, the photon is detected by an untrusted single-photon BSM setup, which is considered to be a "black box" (this means that the BSM, for the worst case, is controlled by Eve), and the

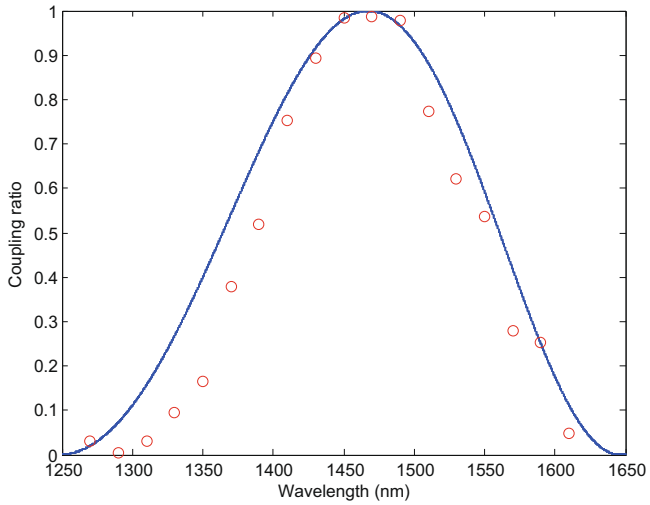

Figure 2. Relationship between the wavelength of the source and the coupling ratio. The coupling ratio of the BS is defined as $r = \frac{I_{port1}}{I_{port1} + I_{port2}}$, where I_{port1} (I_{port2}) is the output intensity of BS output 1(2). The theoretical relationships are based on the coupling model $r = F^2 \sin^2(C\omega/F)$ given in ref. 11, where F^2 is the maximal coupled power, C is the coupling coefficient, and ω is the heat source width. The red dot is the experimental measurement result, and the curve is the theoretical result. The coupling ratio changes from 0.003 to 0.968 with the wavelength changing from 1290 nm and 1470 nm. (The figure is reproduced with permission from ref. 11).

measurement result is reported to Bob. Finally, through an authenticated classical channel, Bob broadcasts, which photons have a successful BSM click together with the corresponding Bell state gained and the basis information. Then, Alice and Bob estimate the quantum bit error rate (QBER) for the data where they choose the same basis. If the QBER is below the secure threshold, they perform error correction and privacy amplification to distill the secure key. To clearly describe our attack, we use the proposed protocol in ref. 33 as an example. The implementation of the protocol is shown in Fig. 1(b). To encode the information in the spatial mode, Bob sends the receiving photon to a 50/50 beam slitter (BS) and applies a phase φ_B on the lower arm (represented by l) by a phase modulator (PM). A single-photon BSM setup contains a half-wave plate (HWP) on the upper arm (represented by u), followed by a 50/50 BS to combine the two arms, and two polarizing beam splitters (PBSs) followed by four single-photon detectors (SPDs). With this structure shown in Fig. 1(b), a click on each SPD denotes the projection on one of the Bell states. In practice, Alice prepares $|\psi_A\rangle_p$ by generating phase-randomized weak coherent pulses which can be modelled as Poissonian (with parameter μ) mixture of photon number states in different BB84 polarization states[1,2,29]. The density matrix of the state can be written as $\rho_A = \sum_{i=0}^{\infty} \frac{\mu^i}{i!} e^{-\mu} |i\rangle\langle i|$, where $|i\rangle\langle i|$ is the density matrix of the i–photon state for $i = 0, 1, \ldots$. When μ is small, the contribution of the $n = 1$ state to a mixture of the photon number states dominates that of the $n > 2$ multiphoton states. Although the possible implementations of the DDI protocol in refs 32–34 are somewhat different, our attack is feasible on all of them since they all employ four SPDs to perform the BSM.

Wavelength-dependent attack. To highlight the feasibility of our proposed attack, first, we show that the wavelength attack is failed because of its applied strategy (the detector wavelength-dependent efficiency) to remove an unusual double-click rate. As discussed in the wavelength-dependent attack[36] or a similar analysis in the following subsection 2, Eve could use the imperfection-detector wavelength-dependent efficiency in the BSM to deal with an unusual double-click rate resulted by detector controlling, i. e., Eve could reduce the double-click rate by carefully tailoring the wavelength of the superimposed light. This solution will work well if all fiber-optic components in Bob's laboratory are wavelength-independent. Unfortunately, in practice, a part of the fiber-optic components, such as BSs and PMs, are wavelength-dependent and affect which detector clicks with the varying wavelength of the superimposed light. For instance, a realistic BS is generally manufactured using fused biconical taper technology, and the coupling ratio is commonly wavelength-dependent. Figure 2 shows the relationship between the wavelength of a source and the coupling ratio of a fused biconical taper 50/50 BS. The coupling ratio can be easily checked to vary nonlinearly with the wavelength, and the optimal coupling ratio is reached at the central wavelength of 1550 nm. For simplicity, in the wavelength-dependent attack, to reduce the unusual double-click rate, the imperfection should satisfy that the detector $D_2(D_3)$ clicks at the central wavelength and detector $D_1(D_4)$ clicks at a different wavelengths λ with an unbalanced coupling ratio r. Here, we define $r = P_i/(P_i + P_j)$, where $i \in \{u, a\}$ and $j \in \{l, b\}$ represent the paths of BS in Fig. 1b. Suppose that the superimposed light that Eve resends to Bob are in the form $|2\alpha_e\rangle$, according to DDI-QKD (a similar and detailed procedure is shown in following subsection 2), the intensities arriving at different detectors in the wavelength-dependent attack can be expressed as

$$
\begin{aligned}
-|[r+(1-r)e^{i(\varphi_e+\varphi_B)}]\alpha_e\rangle_{D_1} \otimes & -|[re^{i\varphi_e}+(1-r)e^{i\varphi_B}]\alpha_e\rangle_{D_2} \\
\otimes & \; i|\sqrt{r(1-r)}(e^{i\varphi_e}-e^{i\varphi_B})\alpha_e\rangle_{D_3} \\
\otimes & \; i|\sqrt{r(1-r)}(1-e^{i(\varphi_e+\varphi_B)})\alpha_e\rangle_{D_4},
\end{aligned} \tag{1}
$$

where φ_e and φ_B represent the phase choices of Eve and Bob, respectively, and D_i, with $i \in \{1, 2, 3, 4\}$, denote Bob's detectors. From Eq. (1), we know that the intensities arriving at each detector are extremely dependent on the coupling ratio r. With random phase modulations, the counts of the four detectors are distributed evenly only if the coupling ratio r equals 0.5. For a sharp comparison, we suppose that $r=1$ corresponds to the wavelength $\lambda=1260\,nm$ in Fig. 2. Eq. (1) converts into

$$
-|\alpha_e\rangle_{D_1} \otimes -|e^{i\varphi_e}\alpha_e\rangle_{D_2}. \tag{2}
$$

The light only arrives at the two detectors at the output a regardless of the basis choice of Bob and Alice. Consequently, Bob can easily detect the wavelength-dependent attack by checking whether the four detectors respond equally to the four Bell states.

Proposed attack. Our proposed attack can be summarized with the following three steps:

Step 1 - Detector blinding. In DDI-QKD, Alice prepares randomly quantum signals in the X or Y basis at a single-photon level. However, in our attack, Eve employs bright light $|2\beta_e\rangle_\alpha$ in the Z basis to force Bob's detectors into the so-called linear mode[8], where the subscript α denotes an eigenstate in the Z basis. In detail, Eve intercepts Alice's signals and then sends bright light $|2\beta_e\rangle_H$ (for simplicity, we assume the polarization of Eve's light horizontal) to Bob. By using the LON, Bob can yield the BB84 states $|\psi_B\rangle_s = (i|u\rangle + e^{i\varphi_B}|l\rangle)/\sqrt{2}$ in spatial modes, where $\varphi_B \in \{0, \pi/2, \pi, 3\pi/2\}$. Therefore, after passing the LON, $|2\beta_e\rangle_H$ becomes $|2\beta_e\rangle_H \otimes |\psi_B\rangle_s$. When the light enters the BSM setup, it first is made unitary transformations $|Hu\rangle \rightarrow |Vu\rangle$ and $|Vu\rangle \rightarrow |Hu\rangle$ on the upper arm by the HWP. Hence, the state transforms into $i|\sqrt{2}\beta_e u\rangle_V \otimes e^{i\varphi_B}|\sqrt{2}\beta_e l\rangle_H$. After transmitting through the second BS, according to the unitary transformation $|u\rangle \rightarrow (i|a\rangle + |b\rangle)/\sqrt{2}$ and $|l\rangle \rightarrow (|a\rangle + i|b\rangle)\sqrt{2}$, the state can be written as

$$
i|\beta_e\rangle_{D_1} \otimes i|e^{i\varphi_B}\beta_e\rangle_{D_2} \otimes |e^{i\varphi_B}\beta_e\rangle_{D_3} \otimes |\beta_e\rangle_{D_4}, \tag{3}
$$

In Eq. (3), it does not matter which modulated phase is chosen by Bob as the intensities entering the four SPDs are always the same. Thus, by elaborately tailoring the light, Eve can successfully blind Bob's detectors, forcing the four detectors to work in the so-called linear operation mode. In this mode, the SPDs do not respond to a receiving single photon, but remain sensitive to bright light with a classical optical power threshold P_{th}. We remark that this is not the only way to blind the detectors; alternative schemes, such as thermal blinding, have been reported[38–40].

Step 2 - Detector controlling. After the blinding process in step 1, Eve performs an intercept-resend attack on the signals transmitted from Alice. That is, she intercepts the transmitted signals and measures each of them in one randomly chosen basis from the BB84 bases, and then she prepares a new signal according to her measurement result and sends it to Bob. Bob will get a detection event only if his active basis choice coincides with that of Eve. Here, without any loss of generality, we suppose that Eve resends a superimposed light pulse $|2\alpha_e\rangle_R$ to control Bob's detectors, where the subscript R represents the BB84 states $(|H\rangle + e^{i\varphi_e}|V\rangle)/\sqrt{2}$ re-prepared by Eve. With a similar analysis in step 1, after passing the LON and the second BS, the state becomes

$$
\begin{aligned}
\frac{1}{\sqrt{2}}i|[1+e^{i(\varphi_e+\varphi_B)}]\alpha_e\rangle_{D_1} \otimes & \; \frac{1}{\sqrt{2}}i|(e^{i\varphi_e}+e^{i\varphi_B})\alpha_e\rangle_{D_2} \\
\otimes & \; \frac{1}{\sqrt{2}}|(e^{i\varphi_e}-e^{i\varphi_B})\alpha_e\rangle_{D_3} \\
\otimes & \; \frac{1}{\sqrt{2}}|(1-e^{i(\varphi_e+\varphi_B)})\alpha_e\rangle_{D_4}.
\end{aligned} \tag{4}
$$

According to the Eq. (4) above, we can obtain the observed intensity arriving at each of Bob's four detectors. If Bob and Eve use the same basis, only two out of the four detectors have the same arriving intensity (one-half of the total intensity). When they have an incompatible basis choice, all the four detectors share the intensity evenly (a quarter of the total intensity). To highlight it, as an example, Table 1 lists the observed intensities arriving at each of Bob's four detectors when Eve sends $|+\rangle$ and Bob measures it with different bases. Here, we suppose that the classical optical power threshold of Bob's blinded detectors P_{th} meets $|\alpha|^2/2 < P_{th} < |\alpha|^2$. From this table, we easily find that when Bob chooses $|\pm i\rangle$, which is a different basis from Eve, his blinded SPDs cannot have any detection events; when Bob chooses the same basis as Eve, two of his four SPDs may have clicks. However, it will cause an unusual double-click rate that ensures Bob is vigilantly aware of the presence of Eve and easily prevents our attack with random bit assignments for double clicks[41]. Consequently, to successfully perform the attack, it is necessary to find a solution to ensure that only one detector has a click.

Eve	Bob	$D_1(\|\psi^-\rangle)$	$D_2(\|\phi^-\rangle)$	$D_3(\|\phi^+\rangle)$	$D_4(\|\psi^+\rangle)$
+	+	1	1	0	0
	−	0	0	1	1
	$+i$	0.5	0.5	0.5	0.5
	$-i$	0.5	0.5	0.5	0.5

Table 1. Observed intensity arriving at each of Bob's four detectors when Eve sends $|+\rangle$. Here, we suppose that the classical optical power threshold of Bob's blinded detectors P_{th} meets $|\alpha|^2/2 < P_{th} < |\alpha|^2$. The intensities are normalized by $|\alpha|^2$.

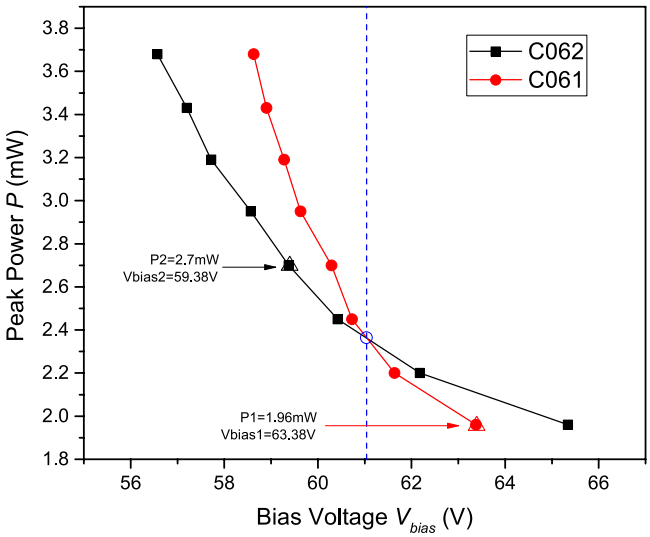

Figure 3. Click thresholds versus biased voltage of the APDs in two different SPDs C062 and C061. Here, for a particular biased voltage of APD Vbias, each point in the red (black) curves represents the minimum value of the peak power of SPD C061 (C062). The blue circle is the cross point of the two curves. The triangles are two different combinations in the feasibility test.

Step 3 - Reducing the double-click rate. To reduce the usual double-click rate, in our attack, we apply an intrinsic imperfection of SPDs that real single-photon detectors respond differently to the same blinding power. As shown in Fig. 3 (see Methods section for the detailed measurement setup), for a particular biased voltage of avalanche photodiodes (APDs) Vbias in two different SPDs, the click thresholds are different. In the original blinding attack, the blinding is caused by the drop of the bias voltage such that the APD operates in the linear mode. Hence, in our measurement, we directly change the bias voltage of the APDs in the two SPDs and record corresponding click thresholds. Especially, with the increase in Vbias, the click threshold curves for the two detectors cross (see the dashed line in Fig. 3). Before the dashed line, the threshold of detector C062 is less than that of detector C061; however, after the dashed line, the threshold of detector C062 is larger than that of detector C061. Hence, Eve can simply choose a combination of P and Vbias before (after) the dashed line, such that a click occurs only on detector C062 (C061) and no click occurs on detector C061 (C062). By doing this, Eve can easily reduce the usual double-click rate. To demonstrate the feasibility of our attack, we control the two detectors with two different combinations of P and Vbias. The results are shown in Fig. 4. The values $P1 = 1.96\,mW$ and $V\,bias1 = 63.38\,V$ cause a detection event in detector C061, however, never cause it in detector C062. In contrast, the values $P2 = 2.7\,mW$ and $V\,bias2 = 59.38\,V$ cause a detection event in detector C062, however, never cause it in detector C061.

It seems that Eve can use another independent imperfection of detectors—detector efficiency mismatch—to reduce an unusual double-click rate. However, there is no concrete proof that the detector still has the efficiency mismatch when it works in the linear mode. It is worth noting that DDI-QKD is naturally secure against a time-shift attack[7], which is based on the fact that two practical SPDs have detection-efficiency mismatch in time domain and each SPD denotes respectively one of bits 0 and 1. However, such criterion are not suitable in DDI-QKD, in which the bits each SPD denotes is varying with Alice's and Bob's chosen bases. A related scheme[42], in which Alice and Bob will get conclusive bits only when they used the different basis for measurement, is strongly similar to DDIQKD and is also immune to the time-shift attack. However, our attack is still working for this scheme, that is, detector will keep silence when Bob's active basis choice did not coincide with that of Eve.

Schematics of hacking scheme. Figure 5 shows the proposed hacking scheme. Eve consists of copies of Alice (Alice') and Bob (Bob'), which share bit and basis settings and a blinding laser. To perform our attack, Eve intercepts the state of Alice and randomly measures it in one of the two bases X and Y using the same devices as Bob. Eve then prepares new signals with detection results and the chosen basis from Bob', overlaps them to a continuous-wave blinding laser which keeps Bob blind via an optical coupler C. Such detector blinding procedure and detector

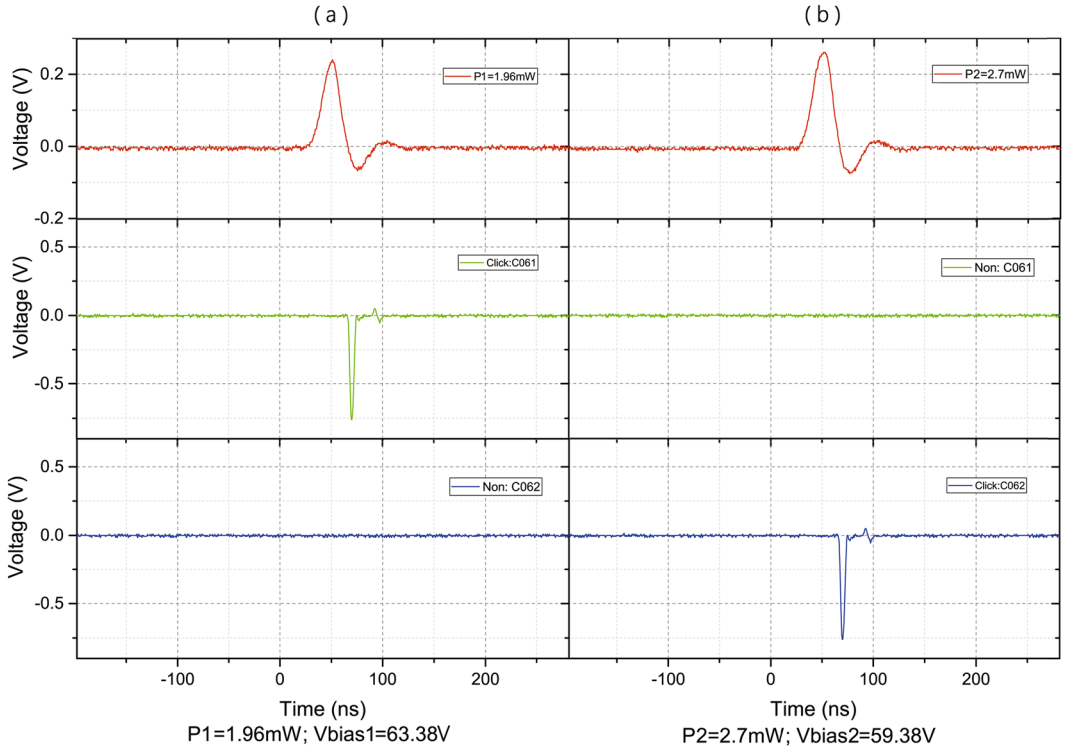

Figure 4. Electrical signal oscillograms when the APDs in SPDs Co62 and C061 are controlled by the trigger pulse peak power with a corresponding biased voltage. (**a**) The values $P = 1.96\,mW$ and $V\,bias = 63.38\,V$ cause a detection event in detector C061, however, never cause it in detector C062. (**b**) In contrast, the values $P = 2.7\,mW$ and $V\,bias = 59.38\,V$ cause a detection event in detector C062, however, never cause it in detector C061.

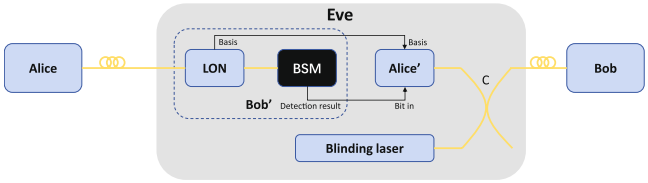

Figure 5. Schematics of hacking scheme. Eve consists of copies of Alice (Alice') and Bob (Bob'), which share bit and basis settings and a blinding laser. C: optical coupler.

controlling have been successfully tested in QKD systems under laboratory or realistic condition[9,43]. The critically implemented part of our attack is whether Eve can prepare the new signals to make only one of detectors in Bob have clicks. As we analyse in *step 3*, the answer is "yes". For simplicity, suppose that Eve wants to force a click only on detector D_1 and no click on detector D_2 illustrated in Fig. 1(b). If the behaviour of the detector D_1 (D_2) coincides with the red (black) curves illustrated in Fig. 3, the values $P = 1.96\,mW$ and $V\,bias = 63.38\,V$ are an combination that meet the requirements. Similarly, if $P = 2.7\,mW$ and $V\,bias = 59.38\,V$, Eve can cause a detection event in detector D_2, however, never cause it in detector D_1. The corresponding experimental tests for these examples are shown in Fig. 4. In our experiment, a full demonstration of the proposed hacking scheme has not been performed. The detector blinding procedure, which had been successfully tested in previous works, has not been repeated. The detector controlling, proofing that Eve can reduce usual double-click rates, has been performed. It worth mentioning that, although the results shown in Fig. 3 are gained by measuring a home-made detector circuit, we note that, in a recent work, Huang *et al.*[44] show that SPDs in commercial QKD system Clavis2 have similar behaviours. Futhermore, our attack is valid for the scheme proposed in ref. 34. It is easy to check that the intensities arriving at Bob's four detectors are the same if the initial polarization of the bright light of Eve is $|R\rangle = (|H\rangle + |V\rangle)/\sqrt{2}$. By careful tailoring the intensities of the bright light and superimposed light pulse according to steps 2 and 3, Eve can successfully hack the scheme without being detected.

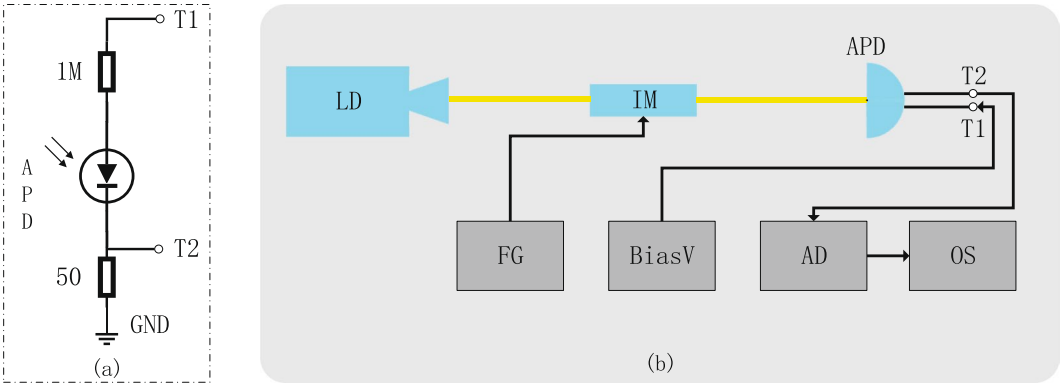

Figure 6. (**a**) Detector circuit diagram. Tap T1: analog tap of the APD bias voltage with a biased resistance of 1 MΩ. T2: analog tap of avalanche signals with a load resistance of 50 Ω. (**b**) LD: laser diode, IM: intensity modulator, FG: function generator, BiasV: home-made DC power, AD: amplifier discriminator, and OS: oscilloscope.

Discussion

In summary, we show that the wavelength-dependent attack in ref. 36 is not technically viable because of an intrinsically wavelength-dependent property of a realistic beam splitter, which is an essential component in DDI-QKD. Moreover, we propose a feasible attack, the same as the wavelength-dependent attack that is based on the well-known detector-blinding attack. We explain how Eve blinds four detectors in detail. To avoid an abnormal double-click rate, different from the wavelength-dependent attack, we utilize another imperfection in real single-photon detectors. An experimental measurement and a proof-of-principle test are performed, and their results confirm that our attack is feasible with current technology. To prevent our attack as well as the wavelength-dependent attack, one specific countermeasure is that Bob introduces additional filtering and monitoring devices with the same idea of QKD with an untrusted source for plug & play system[45]. Another countermeasure is the so-called random-detector efficiency, in which the efficiency of SPDs is randomly varied[46]. We remark that while DDI-QKD is not strictly secure as MDI-QKD, it is more secure than traditional QKD protocols, such as BB84, and is the best for certain practical applications.

Methods

Measurement method. Figure 6(a) shows the detector circuit diagram in our experiment. The APD is biased by a high voltage from analog tap T1 with a biased resistance of 1 MΩ. Tap T2 is an analog tap of avalanche signals with a load resistance of 50 Ω. We do not re-engineer exact detector circuit in commercial SPDs, which contain filter circuits and a fast comparator. Figure 5(b) shows the measurement setup used to measure intrinsic imperfections of APDs. To produce trigger pulses, a laser diode sends light pulses, and then they are attenuated by an intensity modulator controlled by directly applying the pulsed voltage from a function generator (Tektronix AFG3022C). The detector blinding is simulated by directly applying a high voltage for tap T1 from a home-made DC power. An amplifier discriminator (ORTEC 9302) and an oscilloscope (Tektronix TDS 2024B) are used to monitor the avalanche signals. The two APDs are both from Princeton Lightwave. The breakdown voltage of the first APD (Serial number 1444C061), denoted as C061 in Fig. 3, is 72.41 V at 25 °C, and that of the second APD (Serial number 1444C062), denoted as C062, is 71.25 V at 25 °C. In the imperfection measurement, we record the click threshold in the biased voltage range from 56 V to 66 V, at which the APD works in the linear mode. The measurement results are shown in Fig. 3. In the feasibility test, we choose two points beside the dashed line and record whether the APDs have a click event as shown in Fig. 4.

References

1. Bennett, C. H. & Brassard, G. Quantum cryptography: Public key distribution and coin tossing. In *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, vol. 175 (New York, 1984).
2. Gisin, N., Ribordy, G., Tittel, W. & Zbinden, H. Quantum cryptography. *Rev. Mod. Phys.* **74**, 145 (2002).
3. Lo, H.-K. & Chau, H. F. Unconditional security of quantum key distribution over arbitrarily long distances. *Science* **283**, 2050–2056 (1999).
4. Shor, P. W. & Preskill, J. Simple proof of security of the bb84 quantum key distribution protocol. *Phys. Rev. Lett.* **85**, 441–444 (2000).
5. Makarov, V. & Hjelme, D. R. Faked states attack on quantum cryptosystems. *J. Mod. Optic.* **52**, 691–705 (2005).
6. Makarov, V., Anisimov, A. & Skaar, J. Effects of detector efficiency mismatch on security of quantum cryptosystems. *Phys. Rev. A* **74**, 022313 (2006).
7. Zhao, Y., Fung, C.-H. F., Qi, B., Chen, C. & Lo, H.-K. Quantum hacking: Experimental demonstration of time-shift attack against practical quantum-key-distribution systems. *Phys. Rev. A* **78**, 042333 (2008).
8. Lydersen, L. *et al.* Hacking commercial quantum cryptography systems by tailored bright illumination. *Nat. Photon.* **4**, 686–689 (2010).
9. Xu, F., Qi, B. & Lo, H.-K. Experimental demonstration of phase-remapping attack in a practical quantum key distribution system. *New J. Phys.* **12**, 113026 (2010).
10. Jain, N. *et al.* Device calibration impacts security of quantum key distribution. *Phys. Rev. Lett.* **107**, 110501 (2011).
11. Li, H.-W. *et al.* Attacking a practical quantum-key-distribution system with wavelength-dependent beam-splitter and multiwavelength sources. *Phys. Rev. A* **84**, 062308 (2011).
12. Sun, S.-H., Jiang, M.-S. & Liang, L.-M. Passive faraday-mirror attack in a practical two-way quantum-key-distribution system. *Phys. Rev. A* **83**, 062331 (2011).

13. Liu, W.-T., Sun, S.-H., Liang, L.-M. & Yuan, J.-M. Proof-of-principle experiment of a modified photon-number-splitting attack against quantum key distribution. *Phys. Rev. A* **83**, 042326 (2011).
14. Sun, S.-H., Gao, M., Jiang, M.-S., Li, C.-Y. & Liang, L.-M. Partially random phase attack to the practical two-way quantum-key-distribution system. *Phys. Rev. A* **85**, 032304 (2012).
15. Tang, Y.-L. *et al.* Source attack of decoy-state quantum key distribution using phase information. *Phys. Rev. A* **88**, 022308 (2013).
16. Bugge, A. N. *et al.* Laser damage helps the eavesdropper in quantum cryptography. *Phys. Rev. Lett.* **112**, 070503 (2014).
17. Lo, H.-K., Curty, M. & Tamaki, K. Secure quantum key distribution. *Nat. Photon.* **8**, 595–604 (2014).
18. Acn, A. *et al.* Device-independent security of quantum cryptography against collective attacks. *Phys. Rev. Lett.* **98**, 230501 (2007).
19. Lo, H.-K., Curty, M. & Qi, B. Measurement-device-independent quantum key distribution. *Phys. Rev. Lett.* **108**, 130503 (2012).
20. Braunstein, S. L. & Pirandola, S. Side-channel-free quantum key distribution. *Phys. Rev. Lett.* **108**, 130502 (2012).
21. Ferreira da Silva, T. *et al.* Proof-of-principle demonstration of measurement-device-independent quantum key distribution using polarization qubits. *Phys. Rev. A* **88**, 052303 (2013).
22. Liu, Y. *et al.* Experimental measurement-device-independent quantum key distribution. *Phys. Rev. Lett.* **111**, 130502 (2013).
23. Rubenok, A., Slater, J. A., Chan, P., Lucio-Martinez, I. & Tittel, W. Real-world two-photon interference and proof-of-principle quantum key distribution immune to detector attacks. *Phys. Rev. Lett.* **111**, 130501 (2013).
24. Tang, Z. *et al.* Experimental demonstration of polarization encoding measurement-device-independent quantum key distribution. *Phys. Rev. Lett.* **112**, 190503 (2014).
25. Tang, Y.-L. *et al.* Measurement-device-independent quantum key distribution over 200 km. *Phys. Rev. Lett.* **113**, 190501 (2014).
26. Tang, Z., Wei, K., Bedroya, O., Qian, L. & Lo, H.-K. Experimental measurement-device-independent quantum key distribution with imperfect sources. *Phys. Rev. A* **93**, 042308 (2016).
27. Valivarthi, R. *et al.* Measurement-device-independent quantum key distribution: from idea towards application. *Journal of Modern Optics* **62**, 1141–1150 (2015).
28. Feihu, X., Curty, M., Bing, Q. & Hoi-Kwong, L. Measurement-device-independent quantum cryptography. *IEEE. J. Sel. Top. Quant* **21**, 148–158 (2015).
29. Lo, H.-K., Ma, X. & Chen, K. Decoy state quantum key distribution. *Phys. Rev. Lett.* **94**, 230504 (2005).
30. Wang, X.-B. Beating the photon-number-splitting attack in practical quantum cryptography. *Phys. Rev. Lett.* **94**, 230503 (2005).
31. Ma, X. & Lütkenhaus, N. Improved data post-processing in quantum key distribution and application to loss thresholds in device independent qkd. *Quant. Inf. Comput.* **12**, 203–214, URL http://www.rintonpress.com/xxqic12/qic-12-34/0203-0214.pdf (2012).
32. Cao, W.-F. *et al.* Highly efficient quantum key distribution immune to all detector attacks. *arXiv:1410.2928* (2014).
33. Lim, C. C. W. *et al.* Detector-device-independent quantum key distribution. *Appl. Phys. Lett.* **105**, 221112 (2014).
34. González, P. *et al.* Quantum key distribution with untrusted detectors. *Phys. Rev. A* **92**, 022337 (2015).
35. Walborn, S. P., Pádua, S. & Monken, C. H. Hyperentanglement-assisted bell-state analysis. *Phys. Rev. A* **68**, 042313 (2003).
36. Qi, B. Trustworthiness of detectors in quantum key distribution with untrusted detectors. *Phys. Rev. A* **91**, 020303 (2015).
37. Liang, W.-Y. *et al.* Simple implementation of quantum key distribution based on single-photon bell-state measurement. *Phys. Rev. A* **92**, 012319 (2015).
38. Lydersen, L. *et al.* Thermal blinding of gated detectors in quantum cryptography. *Opt. Express* **18**, 27938–27954 (2010).
39. Wiechers, C. *et al.* After-gate attack on a quantum cryptosystem. *New J. Phys.* **13**, 013043 (2011).
40. Jiang, M.-S. *et al.* Intrinsic imperfection of self-differencing single-photon detectors harms the security of high-speed quantum cryptography systems. *Phys. Rev. A* **88**, 062335 (2013).
41. Beaudry, N. J., Moroder, T. & Lutkenhaus, N. Squashing models for optical measurements in quantum communication. *Phys. Rev. Lett.* **101**, 093601 (2008).
42. Ma, X. Quantum key distribution with key extracted from basis information. *arXiv:1410.5260* (2014).
43. Gerhardt, I. *et al.* Full-field implementation of a perfect eavesdropper on a quantum cryptography system. *Nat. Commum.* **2**, 349, URL http://dx.doi.org/10.1038/ncomms1348 (2011).
44. Huang, A. *et al.* Testing random-detector-efficiency countermeasure in a commercial system reveals a breakable unrealistic assumption. *IEEE. J. Quantum. Elect* **52**, 1–11 (2016).
45. Zhao, Y., Qi, B. & Lo, H.-K. Quantum key distribution with an unknown and untrusted source. *Phys. Rev. A* **77**, 052327 (2008).
46. Lim, C. C. W., Walenta, N., Legre, M., Gisin, N. & Zbinden, H. Random variation of detector efficiency: A countermeasure against detector blinding attacks for quantum key distribution. *IEEE. J. Sel. Top. Quant* **21**, 192–196 (2015).

Acknowledgements

The authors would like to thank Shihai Sun for helpful discussions. This work was supported by the Fund of State Key Laboratory of Information Photonics and Optical Communications (Beijing University of Posts and Telecommunications) No. IPOC2016ZT09, the National Natural Science Foundation of China Grants No. 61178010 and No. 11374042, and the Fundamental Research Funds for the Central Universities No. bupt2014TS01.

Author Contributions

K.W. and H.M. conceived the idea; K.W., H.L., and Y.S. conducted the experiment; K.W., H.L., X.Y., and Y.Z. performed the theoretical analysis. H.M., J.X., and Y.J. supervised the project. K.W. wrote the manuscript with input from all the authors. All the authors reviewed the manuscript.

Additional Information

Competing Interests: The authors declare that they have no competing interests.

Publisher's note: Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.