Insecurity of Detector-Device-Independent Quantum Key Distribution

Shihan Sajeed, Anqi Huang, Shihai Sun, Feihu Xu, Vadim Makarov, and Marcos Curty

Phys. Rev. Lett. **117**, 250505 — Published 16 December 2016

DOI: 10.1103/PhysRevLett.117.250505

Insecurity of detector-device-independent quantum key distribution

Shihan Sajeed[1,2,*] Anqi Huang[1,2], Shihai Sun[3], Feihu Xu[4], Vadim Makarov[1,2,5], and Marcos Curty[6]
[1]*Institute for Quantum Computing, University of Waterloo, Waterloo, ON, N2L 3G1 Canada*
[2]*Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, ON, N2L 3G1 Canada*
[3]*College of Science, National University of Defense Technology, Changsha 410073, China*
[4]*Research Laboratory of Electronics, Massachusetts Institute of Technology, 77 Massachusetts Avenue, Cambridge, MA 02139, USA*
[5]*Department of Physics and Astronomy, University of Waterloo, Waterloo, ON, N2L 3G1 Canada*
[6]*Escuela de Ingeniería de Telecomunicación, Department of Signal Theory and Communications, University of Vigo, Vigo E-36310, Spain*
(Dated: November 11, 2016)

Detector-device-independent quantum key distribution (ddiQKD) held the promise of being robust to detector side-channels, a major security loophole in QKD implementations. In contrast to what has been claimed, however, we demonstrate that the security of ddiQKD is not based on post-selected entanglement, and we introduce various eavesdropping strategies that show that ddiQKD is in fact insecure against detector side-channel attacks as well as against other attacks that exploit device's imperfections of the receiver. Our attacks are valid even when the QKD apparatuses are built by the legitimate users of the system themselves, and thus free of malicious modifications, which is a key assumption in ddiQKD.

Introduction.—Quantum key distribution (QKD), a technique to distribute a secret random bit string between two separated parties (Alice and Bob), needs to close the gap between theory and practice [1]. In theory, QKD provides information-theoretic security. In practice, however, it does not because QKD implementation devices do not typically conform to the theoretical models considered in the security proofs. As a result, any unaccounted device imperfection might constitute a side-channel which could be used by an eavesdropper (Eve) to learn the secret key without being detected [2–12].

To bridge this gap, various approaches have been proposed recently [13–17], with measurement-device-independent QKD (mdiQKD) [17] probably being the most promising one in terms of feasibility and performance. Its security is based on post-selected entanglement, and it can remove all detector side-channels from QKD implementations, which is arguably their major security loophole [3–10, 12]. Also, its practicality has been already confirmed both in laboratories and via field trials [18–24]. A drawback of mdiQKD is, however, that it requires high-visibility two-photon interference between independent sources, which makes its implementation more demanding than that of conventional QKD schemes. In addition, current finite-key security bounds against general attacks [25] require larger post-processing data block sizes than those of standard QKD, though recent proposals [26] significantly improve the performance of mdiQKD in the finite-key regime.

To overcome these limitations, a novel approach, so-called detector-device-independent QKD (ddiQKD), has been introduced recently [27–30]. It avoids the problem of interfering photons from independent light sources by using the concept of a single-photon Bell state measurement (BSM) [31]. As a result, its finite-key security bounds and classical post-processing data block sizes are expected to be similar to those of prepare-and-measure QKD schemes [32]. Despite this presumed promising performance, however, the robustness of ddiQKD against detector side-channel attacks has not been rigorously proven yet, and only partial security proofs have been introduced [27, 28].

In this Letter we show that, in contrast to what has been claimed [27–30], the security of ddiQKD *cannot* rely on the same principles as mdiQKD (*i.e.,* post-selected entanglement). More importantly, we demonstrate that ddiQKD is in fact vulnerable to detector side-channel attacks and to other attacks that exploit imperfections of the receiver's devices. These attacks are valid even when Alice's and Bob's state preparation processes are fully characterised and trusted, an essential assumption in ddiQKD. Moreover, they do not require that Eve substitutes Bob's detectors with a measurement apparatus prepared by herself to leak key information to the channel [33]. That is, our attacks apply as well to the scenario where Alice and Bob build the QKD devices themselves.

mdiQKD & ddiQKD.—Let us start by reviewing the basic principles behind mdiQKD and ddiQKD. To simplify the discussion, we shall assume that Alice and Bob have at their disposal perfect single-photon sources. Note, however, that both schemes can operate as well, for instance, with phase-randomised weak coherent pulses in combination with decoy states [34–36], which does not prevent the attacks considered here.

An example of a possible implementation of mdiQKD is illustrated in Fig. 1(a) [17]. Both Alice and Bob generate BB84 states [37] and send them to an untrusted relay Charles. If Charles is honest, he performs a two-photon BSM that projects the incoming signals into a Bell state. In any case, Charles has to declare which of his measure-

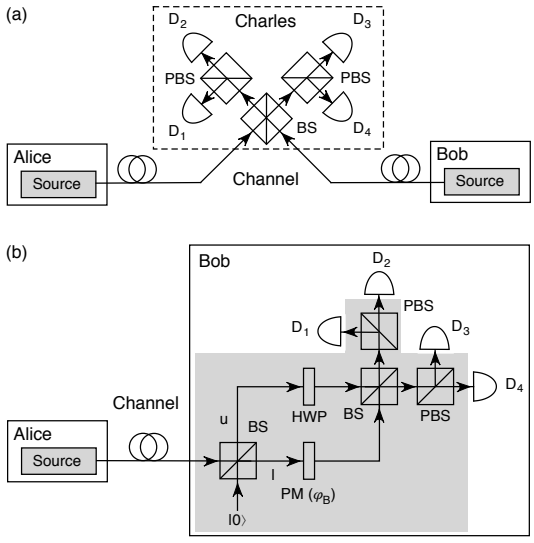

FIG. 1: Possible implementations of partially-device-independent QKD with linear optics. (a) mdiQKD [17]. PBS, polarising beamsplitter; BS, 50 : 50 beamsplitter; and D_i, with $i \in \{1, 2, 3, 4\}$, Charles' single-photon detectors. (b) ddiQKD [28]. HWP, half-wave plate; and PM, phase modulator. One single click in the detector D_1, D_2, D_3, or D_4 corresponds to a projection into the Bell state $|\Psi^+\rangle$, $|\Phi^+\rangle$, $|\Psi^-\rangle$, or $|\Phi^-\rangle$ respectively (see main text for further details). In both schemes, the grey areas denote devices that need to be characterised and trusted. Also, Alice's and Bob's laboratories need to be protected from any information leakage to the outside.

ments are successful together with the Bell states obtained. Alice and Bob then extract a secret key from those successful events where they used the same basis. Importantly, if Charles is honest, his BSM measurement post-selects entanglement between Alice and Bob, and, therefore, he is not able to learn any information about their bit values. To test whether or not Charles is honest, Alice and Bob can simply compare a randomly chosen subset of their data to see if it satisfies the expected correlations associated to the Bell states announced. That is, mdiQKD can be seen as a time-reversed Einstein-Podolsky-Rosen QKD protocol [38]. Therefore, its security can be proven without any assumption on the behaviour of Charles' measurement unit.

ddiQKD [27–30] aims to follow the same spirit of mdiQKD. The key idea is to replace the two-photon BSM with a two-qubit single-photon BSM [31]. This requires that Alice and Bob use two different degrees of freedom of the single-photons to encode their bit information. In so doing, one avoids the need for interfering photons from independent light sources. An example of a possible implementation is illustrated in Fig. 1(b) [28] (see also [27, 29, 30] for similar proposals). Here, Alice sends Bob BB84 polarisation states: $(|\mathrm{H}\rangle + e^{i\theta_\mathrm{A}} |\mathrm{V}\rangle)/\sqrt{2}$, where $|\mathrm{H}\rangle$ ($|\mathrm{V}\rangle$) denotes the Fock state of a single-photon prepared in horizontal (vertical) polarisation, and the phase $\theta_\mathrm{A} \in \{0, \pi/2, \pi, 3\pi/2\}$. Bob then encodes his bit information by using the spatial degree of freedom of the incoming photons. This is done with a 50 : 50 beamsplitter (BS) together with a phase modulator (PM) that applies a random phase $\varphi_\mathrm{B} \in \{0, \pi/2, \pi, 3\pi/2\}$ to each input signal. Finally, Bob performs a BSM that projects each input photon into a Bell state: $|\Phi^\pm\rangle = (|\mathrm{H}\rangle |\mathrm{u}\rangle \pm |\mathrm{V}\rangle |\mathrm{l}\rangle)/\sqrt{2}$ and $|\Psi^\pm\rangle = (|\mathrm{H}\rangle |\mathrm{l}\rangle \pm |\mathrm{V}\rangle |\mathrm{u}\rangle)/\sqrt{2}$, where $|\mathrm{u}\rangle$ ($|\mathrm{l}\rangle$) represents the state of a photon that goes through the upper (lower) arm of the interferometer (see Fig. 1(b)). A photon detection event ("click") in only one detector D_i corresponds to a projection on a particular Bell state.

Both mdiQKD and ddiQKD require that Alice's and Bob's state preparation processes are characterised and trusted. This is indicated by the grey areas shown in Fig. 1. In ddiQKD, the elements inside Bob's grey area can be regarded as his trusted transmitter (when compared to mdiQKD). Among the trusted components there are elements which belong to the BSM, but, importantly, the detectors D_i do not need to be trusted.

The security of ddiQKD is not based on post-selected entanglement.—At a first sight, it seems that the security of ddiQKD follows directly from that of mdiQKD, given, of course, that the assumptions on Alice's and Bob's state preparation processes are fulfilled [27–30]. That is, it relies on the fact that the BSM post-selects entanglement between Alice and Bob. A first indication that confronts this idea was given recently in [33]. There, it was shown that, in contrast to mdiQKD, ddiQKD is actually insecure if Eve is able to replace Bob's detectors with a measurement apparatus that leaks information to the channel [33]. Although this result is important from a conceptual point of view, it violates one of the security assumptions of ddiQKD: Bob's detectors have to be built by a trusted party (but do not need to be characterised) to avoid that they intentionally leak key information to the outside [27]. Below we show that even in this scenario, the security of ddiQKD cannot be based on post-selected entanglement alone, unlike mdiQKD.

For this, we will consider a slightly simplified version of the ddiQKD scheme illustrated in Fig. 1(b). In particular, we will assume that Bob's receiver has only one active detector, say for instance the detector D_1, while the other detectors are disabled. That is, now Bob's BSM projects the incoming photons only into the Bell state $|\Psi^+\rangle$. If the security of ddiQKD is based on post-selected entanglement, this modification should not affect its security (only its secret key rate is reduced by a factor of four), as a projection into a single Bell state should be sufficient to guarantee security [17]. Next we show that a blinding attack [6, 8] renders ddiQKD insecure in this situation.

In particular, suppose that Eve shines bright light onto Bob's detector D_1 to make it enter linear-mode oper-

TABLE I: Mean photon number of the input light to Bob's detectors as a function of the phases $\phi_{\rm E}$ and $\varphi_{\rm B}$.

(a) $\phi_{\rm E} = 0$

$\varphi_{\rm B}$	D_1	D_2	D_3	D_4
0	μ	μ	0	0
$\frac{\pi}{2}$	$\frac{\mu}{2}$	$\frac{\mu}{2}$	$\frac{\mu}{2}$	$\frac{\mu}{2}$
π	0	0	μ	μ
$\frac{3\pi}{2}$	$\frac{\mu}{2}$	$\frac{\mu}{2}$	$\frac{\mu}{2}$	$\frac{\mu}{2}$

(c) $\phi_{\rm E} = \pi$

$\varphi_{\rm B}$	D_1	D_2	D_3	D_4
0	0	0	μ	μ
$\frac{\pi}{2}$	$\frac{\mu}{2}$	$\frac{\mu}{2}$	$\frac{\mu}{2}$	$\frac{\mu}{2}$
π	μ	μ	0	0
$\frac{3\pi}{2}$	$\frac{\mu}{2}$	$\frac{\mu}{2}$	$\frac{\mu}{2}$	$\frac{\mu}{2}$

(b) $\phi_{\rm E} = \frac{\pi}{2}$

$\varphi_{\rm B}$	D_1	D_2	D_3	D_4
0	$\frac{\mu}{2}$	$\frac{\mu}{2}$	$\frac{\mu}{2}$	$\frac{\mu}{2}$
$\frac{\pi}{2}$	μ	0	0	μ
π	$\frac{\mu}{2}$	$\frac{\mu}{2}$	$\frac{\mu}{2}$	$\frac{\mu}{2}$
$\frac{3\pi}{2}$	0	μ	μ	0

(d) $\phi_{\rm E} = \frac{3\pi}{2}$

$\varphi_{\rm B}$	D_1	D_2	D_3	D_4
0	$\frac{\mu}{2}$	$\frac{\mu}{2}$	$\frac{\mu}{2}$	$\frac{\mu}{2}$
$\frac{\pi}{2}$	0	μ	μ	0
π	$\frac{\mu}{2}$	$\frac{\mu}{2}$	$\frac{\mu}{2}$	$\frac{\mu}{2}$
$\frac{3\pi}{2}$	μ	0	0	μ

ation [6, 8]. In this mode the detector is no longer sensitive to single-photon pulses, but it can only detect strong light. We assume that when D_1 receives a bright pulse of mean photon number μ it always produces a click, while if the pulse's mean photon number is $\mu/2$, it never produces a click. This behaviour has been experimentally confirmed in many detector types [6, 8, 39–44]. Once D_1 is blinded, Eve performs an intercept-resend attack on every signal sent by Alice. That is, she measures Alice's signals in one of the two BB84 bases (which Eve selects at random for each pulse), and she prepares a new signal, depending on the result obtained, that is sent to Bob. Intercept-resend attacks correspond to entanglement-breaking channels and, therefore, they cannot lead to a secure key [45]. Suppose, for instance, that the signals that Eve sends to Bob are coherent states of the form $\left|\sqrt{2\mu}\right\rangle$ with creation operator $a^\dagger = (a_{\rm H}^\dagger + e^{i\phi_{\rm E}} a_{\rm V}^\dagger)/\sqrt{2}$. Here, $a_{\rm H}^\dagger$ ($a_{\rm V}^\dagger$) denotes the creation operator for horizontally (vertically) polarised photons, and the phase $\phi_{\rm E} \in \{0, \pi/2, \pi, 3\pi/2\}$ depends on Eve's measurement result. More precisely, for each measured signal, Eve sends Bob a coherent state prepared in the BB84 polarisation state identified by her measurement. Then, it can be shown that the state at the input ports of Bob's detectors $D_{\rm i}$ is a coherent state of the form (see Supplemental Material Sec. I [46] for details)

$$|\psi\rangle = \left|\frac{\sqrt{\mu}}{2}\left(e^{i\phi_{\rm E}} + e^{i\varphi_{\rm B}}\right)\right\rangle_{D_1} \otimes \left|\frac{\sqrt{\mu}}{2}\left(1 + e^{i(\phi_{\rm E}+\varphi_{\rm B})}\right)\right\rangle_{D_2} \otimes \left|\frac{\sqrt{\mu}}{2}\left(e^{i\phi_{\rm E}} - e^{i\varphi_{\rm B}}\right)\right\rangle_{D_3} \otimes \left|\frac{\sqrt{\mu}}{2}\left(1 - e^{i(\phi_{\rm E}+\varphi_{\rm B})}\right)\right\rangle_{D_4}. \tag{1}$$

This situation is illustrated in Table I, where we show the mean photon number of the incoming light to Bob's detectors for all combinations of $\phi_{\rm E}$ and $\varphi_{\rm B}$. Most importantly, from this table we can see that if D_1 is the only active detector, then Bob only obtains a click when he uses the same measurement basis as Eve (*i.e.,* when $\varphi_{\rm B}, \phi_{\rm E} \in \{0, \pi\}$ or $\varphi_{\rm B}, \phi_{\rm E} \in \{\pi/2, 3\pi/2\}$), and $\varphi_{\rm B} = \phi_{\rm E}$. That is, this attack does not introduce any error. Moreover, we have that Bob and Eve select the same basis with at least 1/2 probability. This means that the ddiQKD scheme illustrated in Fig. 1(b) (with only one active detector) is actually insecure against the detector blinding attack for a total system loss beyond only 3 dB, just like standard QKD schemes. This confirms that the security of ddiQKD cannot be based on post-selected entanglement. The same conclusion applies as well to the ddiQKD schemes introduced in Refs. [27], [29], and [30].

Insecurity of ddiQKD against detector side-channel attacks.—If Bob uses four active detectors, the detector blinding attack has one main drawback: it produces double-clicks [33]. From Table I one can already see that whenever Bob uses the same measurement basis as Eve there is always two detectors that click. For instance, when $\varphi_{\rm B} = \phi_{\rm E} = 0$ the detectors D_1 and D_2 always click, and similar for the other cases. This means that Alice and Bob could, in principle, try to monitor double-clicks to detect the presence of Eve. So, the question is whether or not four active detectors can make ddiQKD secure again. As we show below, the answer is "no". For this, we introduce two possible eavesdropping strategies that exploit practical imperfections of Bob's detectors to avoid double-clicks. See also Supplemental Material Sec. II [46] for two alternative attacks that achieve the same goal by exploiting other imperfections of Bob's linear optics network.

The first eavesdropping strategy uses the fact that single-photon detectors respond differently to the same blinding power $P_{\rm B}$. This has been recently analysed in Ref. [44]. There, the authors compare the response of two single-photon detectors in a commercial QKD system Clavis2 [47] to varying blinding power. They first illuminate the detectors with continuous-wave bright light of power $P_{\rm B}$ to force them enter linear-mode operation. Then they record the maximum and minimum value of the trigger pulse energy $E_{\rm T}$ for which the click probabilities are 0 and 1 respectively. The results are shown in Fig. 2(a) [44]. For a particular blinding power $P_{\rm B}$, each point in the solid (dashed) curves shown in the figure represents the maximum (minimum) value of trigger pulse energy $E_{\rm T}$ for which the detection efficiency $\eta_{\rm det}$ is 0 (1). The blue and green colours identify the two detectors. (Note that if the energies $E_{\rm T}$ corresponding to the dashed curves are halved, the result is always below the solid curves, thus satisfying the assumption made in the previous section that pulses with mean photon number $\mu/2$ result in zero click probability.) Next, we show how these detector characteristics could be used to avoid double-clicks.

For this, we return to the blinding attack described

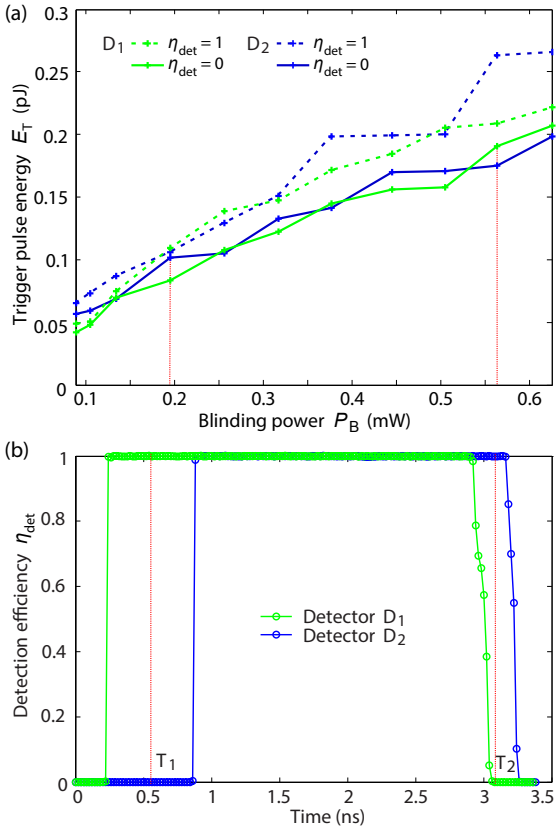

FIG. 2: Detector click probability in bright-light blinded regime in commercial QKD system Clavis2. (a) Click trigger thresholds versus blinding power $P_{\rm B}$ for two different single-photon detectors $\rm D_1$ and $\rm D_2$. Here, for a particular blinding power $P_{\rm B}$, each point in the solid (dashed) curves represents the maximum (minimum) value of trigger pulse energy $E_{\rm T}$ for which the detection efficiency $\eta_{\rm det}$ is 0 (1). The experimental data has been reprinted from Ref. [44]. (b) Measured detection efficiency mismatch in the time domain between two blinded single-photon detectors at $P_{\rm B} = 0.32\,\rm mW$, $E_{\rm T} = 0.24\,\rm pJ$, and 0.7 ns wide trigger pulse (see main text for further details).

above against the ddiQKD implementation illustrated in Fig. 1(b). For simplicity, let us consider again the case where $\varphi_{\rm B} = \phi_{\rm E} = 0$. In particular, suppose for instance that Eve wants to force a click only on detector say $\rm D_1$, and no click on detector $\rm D_2$. Then, in order to achieve this goal, she can simply choose a combination of $P_{\rm B}$ and $E_{\rm T}$ such that the detector $\rm D_1$ ($\rm D_2$) has a non-zero (zero) click probability. If the behaviour of the detector $\rm D_1$ ($\rm D_2$) corresponds to the green (blue) curves shown in Fig. 2(a), then the values $P_{\rm B} \approx 0.2$ mW and $E_{\rm T} \approx 0.1$ pJ constitute an example that satisfies this criterion. Similarly, if $P_{\rm B} \approx 0.56$ mW and $E_{\rm T} \approx 0.19$ pJ, then Eve could make the detector $\rm D_2$ ($\rm D_1$) to have a non-zero (zero) click probability. Importantly, note that when Bob's basis matches that of Eve, only two out of the four detectors $\rm D_{\it i}$ might produce a click (see Table I). Hence, in these instances Eve only needs to avoid double-clicks between two detectors in order to remain undetected. A similar argument can be applied as well to any other value of $\varphi_{\rm B}$ and $\phi_{\rm E}$.

This attack demonstrates that if Bob's detectors are uncharacterised, as assumed in ddiQKD, this type of schemes are indeed insecure against detector side-channel attacks. That is, Eve could learn the whole secret key without producing any error nor a double-click.

A second eavesdropping strategy that also allows Eve to avoid double-clicks is based on a time-shift attack [3, 4] that exploits the detection efficiency mismatch between Bob's detectors. In this type of attack, Eve shifts the arrival time of each signal that she sends to Bob such that only one detector can produce a click each given time. Here, we have confirmed experimentally that this type of attack is also possible with blinded detectors. For this, we blinded two single-photon detectors from the commercial QKD system Clavis2 [47] and we measured their detection efficiency mismatch. The experimental results are shown in Fig. 2(b). We find, for instance, that whenever Bob receives a trigger pulse at the time instance T_1 (T_2), only the detector $\rm D_1$ ($\rm D_2$) can produce a click because this instance is outside of the response region of the detector $\rm D_2$ ($\rm D_1$). That is, by combining the time-shift attack with the blinding attack introduced in the previous section, Eve could again break the security of ddiQKD without introducing errors nor double-clicks.

Conclusion.—We have analysed the security of detector-device-independent QKD (ddiQKD), a novel scheme that promised to be robust against detector side-channel attacks. We have shown that its security is not based on post-selected entanglement, as originally claimed. Most importantly, we have presented various eavesdropping attacks that demonstrate that ddiQKD is actually vulnerable to detector side-channel attacks as well as to other side-channel attacks that exploit imperfections of Bob's receiver. These attacks are valid even when Alice's and Bob's state preparation processes are fully characterised and trusted, and Bob's detectors are built by a trusted party and cannot be replaced with a measurement device manufactured by Eve. Alice and Bob might try to prevent these attacks by designing proper countermeasures at the detector side, just like in standard QKD schemes. In such scenario, however, it is unclear what would be the real advantage (in terms of complexity and performance) of using ddiQKD instead of standard QKD systems. As a final remark, let us say that the main reason for the insecurity of ddiQKD seems to be Bob's state preparation process; while in mdiQKD it is assumed to be protected, in ddiQKD it can be influenced by Eve via the signals she sends him.

Acknowledgments.—This work was supported by Industry Canada, CFI, NSERC (programs Discovery, PDF,

CryptoWorks21), Ontario MRI, US Office of Naval Research, National Natural Science Foundation of China (grant No. 11304391 and 11674397), Spain MINECO, FEDER (grant No. TEC2014-54898-R), and Galician Regional Government (programs EM2014/033, AtlantTIC). The authors thank ID Quantique for cooperation, technical assistance, and providing the QKD hardware.

S.S. and A.H. contributed equally to this work.

* shihan.sajeed@gmail.com

[1] H.-K. Lo, M. Curty, and K. Tamaki, Nat. Photonics **8**, 595 (2014).
[2] A. Vakhitov, V. Makarov, and D. R. Hjelme, J. Mod. Opt. **48**, 2023 (2001).
[3] V. Makarov, A. Anisimov, and J. Skaar, Phys. Rev. A **74**, 022313 (2006), erratum ibid. **78**, 019905 (2008).
[4] B. Qi, C.-H. F. Fung, H.-K. Lo, and X. Ma, Quantum Inf. Comput. **7**, 73 (2007).
[5] A. Lamas-Linares and C. Kurtsiefer, Opt. Express **15**, 9388 (2007).
[6] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, Nat. Photonics **4**, 686 (2010).
[7] F. Xu, B. Qi, and H.-K. Lo, New J. Phys. **12**, 113026 (2010).
[8] I. Gerhardt, Q. Liu, A. Lamas-Linares, J. Skaar, C. Kurtsiefer, and V. Makarov, Nat. Commun. **2**, 349 (2011).
[9] H. Weier, H. Krauss, M. Rau, M. Fürst, S. Nauerth, and H. Weinfurter, New J. Phys. **13**, 073024 (2011).
[10] P. Jouguet, S. Kunz-Jacques, and E. Diamanti, Phys. Rev. A **87**, 062313 (2013).
[11] S. Sajeed, I. Radchenko, S. Kaiser, J.-P. Bourgoin, A. Pappa, L. Monat, M. Legré, and V. Makarov, Phys. Rev. A **91**, 032326 (2015).
[12] S. Sajeed, P. Chaiwongkhot, J.-P. Bourgoin, T. Jennewein, N. Lütkenhaus, and V. Makarov, Phys. Rev. A **91**, 062301 (2015).
[13] D. Mayers and A. Yao, in *Proc. 39th Annual Symposium on Foundations of Computer Science* (IEEE, 1998) pp. 503–509.
[14] A. Acín, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani, Phys. Rev. Lett. **98**, 230501 (2007).
[15] U. Vazirani and T. Vidick, Phys. Rev. Lett. **113**, 140501 (2014).
[16] C. A. Miller and Y. Shi, in *Proc. 46th Annual ACM Symposium on Theory of Computing (STOC'14)* (ACM, New York, NY, USA, 2014) pp. 417–426.
[17] H.-K. Lo, M. Curty, and B. Qi, Phys. Rev. Lett. **108**, 130503 (2012).
[18] A. Rubenok, J. A. Slater, P. Chan, I. Lucio-Martinez, and W. Tittel, Phys. Rev. Lett. **111**, 130501 (2013).
[19] T. F. da Silva, D. Vitoreti, G. B. Xavier, G. C. do Amaral, G. P. Temporão, and J. P. von der Weid, Phys. Rev. A **88**, 052303 (2013).
[20] Y. Liu, T.-Y. Chen, L.-J. Wang, H. Liang, G.-L. Shentu, J. Wang, K. Cui, H.-L. Yin, N.-L. Liu, L. Li, X. Ma, J. S. Pelc, M. M. Fejer, C.-Z. Peng, Q. Zhang, and J.-W. Pan, Phys. Rev. Lett. **111**, 130502 (2013).
[21] Z. Tang, Z. Liao, F. Xu, B. Qi, L. Qian, and H.-K. Lo, Phys. Rev. Lett. **112**, 190503 (2014).
[22] L. C. Comandar, M. Lucamarini, B. Fröhlich, J. F. Dynes, A. W. Sharpe, S. W.-B. Tam, Z. L. Yuan, R. V. Penty, and A. J. Shields, Nat. Photonics **10**, 312 (2016).
[23] Y.-L. Tang, H.-L. Yin, Q. Zhao, H. Liu, X.-X. Sun, M.-Q. Huang, W.-J. Zhang, S.-J. Chen, L. Zhang, L.-X. You, Z. Wang, Y. Liu, C.-Y. Lu, X. Jiang, X. Ma, Q. Zhang, T.-Y. Chen, and J.-W. Pan, Phys. Rev. X **6**, 011024 (2016).
[24] H.-L. Yin, T.-Y. Chen, Z.-W. Yu, H. Liu, L.-X. You, Y.-H. Zhou, S.-J. Chen, Y. Mao, M.-Q. Huang, W.-J. Zhang, H. Chen, M. J. Li, D. Nolan, F. Zhou, X. Jiang, Z. Wang, Q. Zhang, X.-B. Wang, and J.-W. Pan, Phys. Rev. Lett. (in press), arXiv:1606.06821 [quant-ph].
[25] M. Curty, F. Xu, W. Cui, C. C. W. Lim, K. Tamaki, and H.-K. Lo, Nat. Commun. **5**, 3732 (2014).
[26] Y.-H. Zhou, Z.-W. Yu, and X.-B. Wang, Phys. Rev. A **93**, 042324 (2016).
[27] P. González, L. Rebón, T. Ferreira da Silva, M. Figueroa, C. Saavedra, M. Curty, G. Lima, G. B. Xavier, and W. A. T. Nogueira, Phys. Rev. A **92**, 022337 (2015).
[28] C. C. W. Lim, B. Korzh, A. Martin, F. Bussières, R. Thew, and H. Zbinden, Appl. Phys. Lett. **105**, 221112 (2014).
[29] W.-F. Cao, Y.-Z. Zhen, Y.-L. Zheng, Z.-B. Chen, N.-L. Liu, K. Chen, and J.-W. Pan, manuscript withdrawn by authors on 23 Aug 2016 owing to the insecurity of the proposed scheme, arXiv:1410.2928v1 [quant-ph].
[30] W.-Y. Liang, M. Li, Z.-Q. Yin, W. Chen, S. Wang, X.-B. An, G.-C. Guo, and Z.-F. Han, Phys. Rev. A **92**, 012319 (2015).
[31] Y.-H. Kim, Phys. Rev. A **67**, 040301 (2003).
[32] C. C. W. Lim, M. Curty, N. Walenta, F. Xu, and H. Zbinden, Phys. Rev. A **89**, 022307 (2014).
[33] B. Qi, Phys. Rev. A **91**, 020303 (2015).
[34] W.-Y. Hwang, Phys. Rev. Lett. **91**, 057901 (2003).
[35] H.-K. Lo, X. Ma, and K. Chen, Phys. Rev. Lett. **94**, 230504 (2005).
[36] X.-B. Wang, Phys. Rev. Lett. **94**, 230503 (2005).
[37] C. H. Bennett and G. Brassard, in *Proc. IEEE International Conference on Computers, Systems, and Signal Processing (Bangalore, India)* (IEEE Press, New York, 1984) pp. 175–179.
[38] E. Biham, B. Huttner, and T. Mor, Phys. Rev. A **54**, 2651 (1996).
[39] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, Opt. Express **18**, 27938 (2010).
[40] C. Wiechers, L. Lydersen, C. Wittmann, D. Elser, J. Skaar, C. Marquardt, V. Makarov, and G. Leuchs, New J. Phys. **13**, 013043 (2011).
[41] L. Lydersen, M. K. Akhlaghi, A. H. Majedi, J. Skaar, and V. Makarov, New J. Phys. **13**, 113042 (2011).
[42] S. Sauge, L. Lydersen, A. Anisimov, J. Skaar, and V. Makarov, Opt. Express **19**, 23590 (2011).
[43] J. Jogenfors, A. M. Elhassan, J. Ahrens, M. Bourennane, and J.-Å. Larsson, Sci. Adv. **1**, e1500793 (2015).
[44] A. Huang, S. Sajeed, P. Chaiwongkhot, M. Soucarros, M. Legré, and V. Makarov, IEEE J. Quantum Electron. **52**, 8000211 (2016).
[45] M. Curty, M. Lewenstein, and N. Lütkenhaus, Phys. Rev. Lett. **92**, 217903 (2004).
[46] See Supplemental Material at [URL will be inserted by publisher] (which also contains Refs. [28, 48, 49]) for more details about the quantum states arriving at Bob's detec-

tors and for side-channel attacks that exploit imperfections of Bob's linear optics network.

[47] Clavis2 specification sheet, http://www.idquantique.com/images/stories/PDF/clavis2-quantum-key-distribution/clavis2-specs.pdf, visited 23 Oct 2016.

[48] F. Xu, K. Wei, S. Sajeed, S. Kaiser, S. Sun, Z. Tang, L. Qian, V. Makarov, and H.-K. Lo, Phys. Rev. A **92**, 032305 (2015).

[49] 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, Phys. Rev. A **84**, 062308 (2011).