Creation of backdoors in quantum communications via laser damage

Vadim Makarov, Jean-Philippe Bourgoin, Poompong Chaiwongkhot, Mathieu Gagné, Thomas Jennewein, Sarah Kaiser, Raman Kashyap, Matthieu Legré, Carter Minshull, and Shihan Sajeed

Phys. Rev. A **94**, 030302 — Published 15 September 2016

DOI: 10.1103/PhysRevA.94.030302

Laser damage creates backdoors in quantum communications

Vadim Makarov,[1, 2, 3, 4, *] Jean-Philippe Bourgoin,[2, 3] Poompong Chaiwongkhot,[2, 3] Mathieu Gagné,[5]
Thomas Jennewein,[2, 3, 6] Sarah Kaiser,[2, 3] Raman Kashyap,[5] Matthieu Legré,[7] Carter Minshull,[2] and Shihan Sajeed[2, 4]

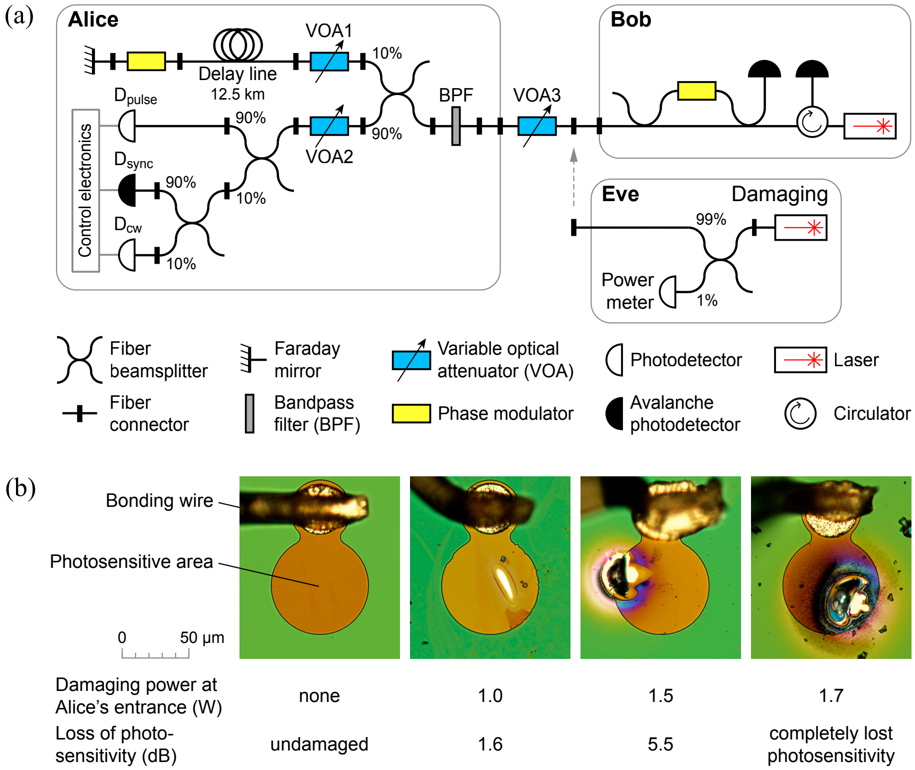
[1] *The rest of the authors are listed alphabetically.*
[2] *Institute for Quantum Computing, University of Waterloo, Waterloo, ON, N2L 3G1 Canada*
[3] *Department of Physics and Astronomy, University of Waterloo, Waterloo, ON, N2L 3G1 Canada*
[4] *Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, ON, N2L 3G1 Canada*
[5] *Department of Engineering Physics and Department of Electrical Engineering,*
École Polytechnique de Montréal, Montréal, QC, H3C 3A7 Canada
[6] *Quantum Information Science Program, Canadian Institute for Advanced Research, Toronto, ON, M5G 1Z8 Canada*
[7] *ID Quantique SA, Chemin de la Marbrerie 3, 1227 Carouge, Geneva, Switzerland*

Practical quantum communication (QC) protocols are assumed to be secure provided implemented devices are properly characterized and all known side channels are closed. We show that this is not always true. We demonstrate a laser-damage attack capable of modifying device behaviour on-demand. We test it on two practical QC systems for key distribution and coin-tossing, and show that newly created deviations lead to side channels. This reveals that laser damage is a potential security risk to existing QC systems, and necessitates their testing to guarantee security.

Cryptography, an art of secure communication, has traditionally relied on either algorithmic or computational complexity [1]. Even the most state-of-the-art classical cryptographic schemes do not have a strict mathematical proof to ascertain their security. With the advance of quantum computing, it may be a matter of time before the security of the most widely used public-key cryptography protocols is broken [2]. Quantum communication (QC) protocols, on the other hand, have theoretical proofs of being unconditionally secure [3–9]. In theory, their security is based on the assumption of modeled behaviour of implemented equipment. In practice, the actual behaviour often deviates from the modeled one, leading to a compromise of security as has been seen so far in case of quantum key distribution (QKD) [10–16]. However, it is widely assumed that as long as these deviations are properly characterized and security proofs are updated accordingly [5, 17], implementations are unconditionally secure. In this work we show that satisfying this during the initial installation only is not enough to guarantee security. Even if a system is perfectly characterized and deviations are included into the security proofs, an adversary can still create a new deviation on-demand and make the system insecure.

Before going into details on how the adversary may do it, let's consider a few examples of deviations and their consequences. For example, a calibrated optical attenuator is required to set a precise value of the outgoing mean photon number μ in the implementations of ordinary QKD [18, 19], decoy-state QKD [20], coherent-one-way QKD [21], measurement-device-independent QKD [22], continuous-variable QKD [23], digital signature [7], relativistic bit commitment [8], coin-tossing [24] and secret-sharing [9] protocols. An unexpected increase of this optical component's attenuation may cause a denial-of-service. However, a reduction in attenuation will increase μ, leading to a compromise of security via attacks that rely on measurement of multi-photon pulses [25, 26]. E.g., in QKD and secret-sharing this will allow eavesdropping of the key, and in bit commitment cheating the committed bit value. Some implementations use a detector for time synchronization [8, 9, 18, 19, 21–24]. Desensitizing it may result in the denial-of-service. However, several implementations require a calibrated monitoring detector for security purposes [8, 9, 18, 19, 21, 23, 24]. A reduction in its sensitivity may lead to security vulnerabilities such as a Trojan-horse attack that reads the state preparation [27]. This leaks the key in QKD, increases the cheating probability in coin-tossing [26], leaks the program and client's data in quantum cloud computing [6] and allows forging of digital signatures [7]. Many implementations use beamsplitters and rely on their precharacterized splitting ratio (e.g., [8, 18–21, 23, 24]). A shift in the splitting ratio may lead to either the denial-of-service or security vulnerabilities (e.g., [28] or one of the above-mentioned attacks). A shift in characteristics of a phase modulator or a Faraday mirror may create imperfect qubits that will result in the denial-of-service or a breach in security [14, 15, 29]. If the dark count rate of single-photon detectors is increased, it may lead to the denial-of-service [30]. Even in device-independent QKD (DI-QKD) [31], the absence of information-leakage channels and memory is assumed [32]. Thus, there is a risk these assumptions may be compromised by deviations in device characteristics. To give a speculative illustration, let's suppose detectors in DI-QKD emit light on detection [33–35], and to prevent this leaking information about detection results, spectral filters and optical isolators are added to the devices. Then, unexpected deviations in characteristics of the latter components become important for security. In summary, quantum communication systems rely on multiple characteristics of many components for their correct operation, and a deviation might

[*] makarov@vad1.com



Damaging power at Alice's entrance (W)	none	1.0	1.5	1.7
Loss of photo-sensitivity (dB)	undamaged	1.6	5.5	completely lost photosensitivity

FIG. 1. **Attack on fiber-optic system Clavis2.** (a) Experimental setup. The system consists of Alice and Bob connected by a lossy fiber communication channel (simulated by variable optical attenuator VOA3). Bob sends to Alice pairs of bright coherent optical pulses, produced by his laser and two fiber arms of unequal length [18, 19]. Alice uses fiber beamsplitters to divert parts of incoming pulse energy to monitoring detector D_{pulse}, synchronization detector D_{sync} and line-loss measurement detector D_{cw}. She prepares quantum states by phase-modulating the pulses, reflecting them at a Faraday mirror and attenuating to single-photon level with VOA1. Bob measures the quantum states by applying his basis choice via phase modulator and detecting outcome of quantum interference with single-photon avalanche photodetectors. Eve's damaging laser is connected to the channel manually. BPF, bandpass filter. (b) Pulse-energy-monitoring photodiode before and after damage. Brightfield microphotographs show top-view of decapsulated photodiode chips. The last two samples have holes melted through their photosensitive area. Scattered dark specks are debris from decapsulation.

lead to severe security consequences.

In classical communications, there is no real concern about the possibility of a shift in device characteristics. Classical devices' security-critical parts can be physically separated from the communication channel and isolated from physical access by the adversary [37]. However the front-end of a quantum communication system is essentially an analog optical system connected to the channel (at least, at our present level of the technology), and is easily accessible by the adversary. The latter can shoot a high-power laser from the communication channel to alter system component characteristics via laser damage [30]. The question is what will this achieve? Will the adversary break some component needed for operation and cause the denial-of-service (which is not a useful outcome for her), or will she change some component in such a way as to facilitate a compromise of security? Further, will the security compromise be only possible in theory or be practical with today's technology? This cannot be predicted in advance, because system implementations contain many components and their laser damage thresholds and failure behavior are generally not precisely known. To assess the risk for quantum communications, we have performed tests on two extensively characterized, completely different and widely used implementations: a commercial fiber-optic system for QKD and coin-tossing with phase-encoded qubits [18, 19], and a free-space system for QKD with polarization-encoded qubits [20]. In both systems, we have unfortunately observed the best possible outcome for the adversary. After the laser damage, the systems' security has become compromisable with today's technology.

Laser damage in fiber-optic system. As a representative of a fiber-optic quantum communication implementation, we chose a plug-and-play QKD [18] and loss-tolerant quantum coin tossing (QCT) [24]. Both were implemented using a commercial system Clavis2 from ID Quantique [19]. In both cases, Bob sends bright light pulses to Alice. Alice randomly encodes her secret bits by applying one out of four phases $(0, \frac{\pi}{2}, \pi, \frac{3\pi}{2})$, attenuates the pulses and reflects them back to Bob [Fig. 1(a)]. The security of both protocols requires an upper bound on the

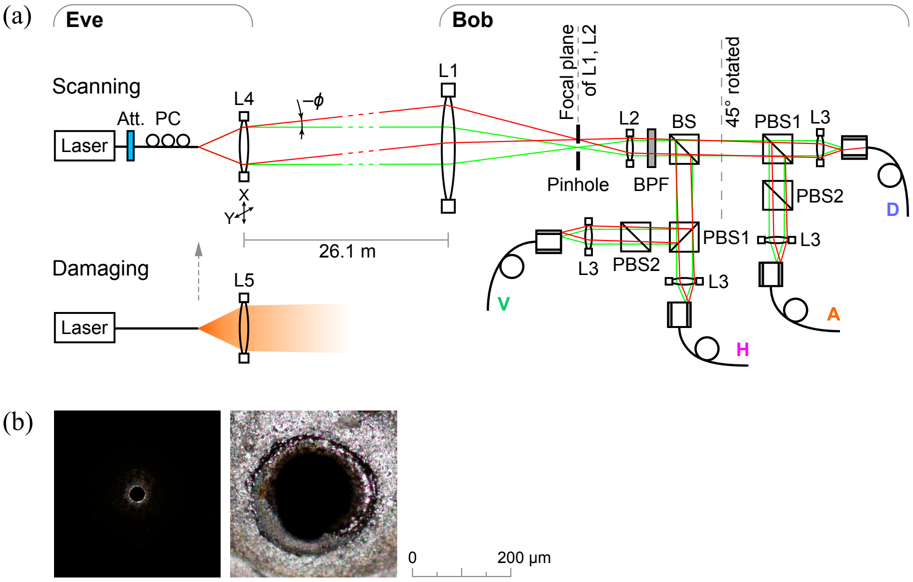


FIG. 2. **Attack on free-space QKD system.** (a) Experimental setup. QKD receiver Bob consists of two lenses L1, L2 reducing input beam diameter, 50:50 beamsplitter BS, and two arms measuring photons in HV and DA polarizations using polarizing beamsplitters PBS [16, 20]. Photons are focused by lenses L3 into multimode fibers leading to single-photon detectors. Setup drawing is not to scale. Eve's apparatus contains a scanning laser source that tilts the beam angle (ϕ, θ) by laterally shifting lens L4. Green marginal rays denote initial Eve's alignment, replicating the alignment Alice–Bob at $\phi = \theta = 0$. Red marginal rays show a tilted scanning beam missing fiber cores V, H, A, but coupling into D. Eve's damaging laser source can be manually inserted in place of the scanning source. Att., attenuator; PC, polarization controller. (b) Spatial filter before and after damage. Darkfield microphotographs show front view of the pinhole. See Supplemental Section IV [36] for real-time video recording of laser damage to the pinhole inside Bob.

mean photon number μ coming out of Alice. Otherwise, an eavesdropper Eve can perform a Trojan-horse attack [27] by superimposing extra light to the bright pulses on their way to Alice from Bob. If Alice is unaware of this and applies the same attenuation, then light coming out of her has a higher μ than allowed by the security proofs [5], making the implementations insecure. It is thus crucial for the security of both protocols that Alice monitors the incoming pulse energy. This is achieved by employing a pulse-energy-monitoring detector [D_{pulse} in Fig. 1(a)]. A portion of the incoming light is fed to D_{pulse} such that whenever extra energy is injected, an alarm is produced [26]. The sensitivity of D_{pulse} is factory-calibrated, thus closing the side-channel associated with the Trojan-horse attack.

Our testing showed that this countermeasure is vulnerable to laser damage. During normal QKD operation, we disconnected the fiber channel Alice–Bob temporarily and connected Eve [Fig. 1(a)]. She then injected 1550 nm laser light from an erbium-doped fiber amplifier for 20–30 s, delivering continuous-wave (c.w.) high power into Alice's entrance. 44% of this power reached the fiber-pigtailed InGaAs p-i-n photodiode D_{pulse} (JDSU EPM 605LL), and damaged it partially or fully. It became either less sensitive to incoming light (by 1–6 dB after 0.5–1.5 W illumination at Alice's entrance) or completely insensitive (after ≥ 1.7 W). The physical damage is shown in Fig. 1(b). No other optical component was damaged at this power level. We repeated the experiment with 6 photodiode samples. In half of these trials, QKD continued uninterrupted and kept producing more key after we reconnected the channel back to Bob, as if nothing has happened. In the other half, a manual software restart was needed. However, in all the trials the damage was sufficient to permanently open the system up to the Trojan-horse attack. As modeled in Ref. 26, in the QKD protocol, Eve can eavesdrop partial or full key using today's best technology if the sensitivity of D_{pulse} drops by more than 5.6 dB. In the QCT implementation, a sensitivity reduction by 2.6 dB can increase Bob's cheating probability above a classical level, removing any quantum advantage of coin-tossing. Laser damage thus compromises both the QKD and QCT implementations. See Supplemental Section I [36] for details.

Laser damage in free-space system. As a representative of free-space quantum communication, we chose a long-distance satellite QKD prototype operating at 532 nm wavelength [20] employing Bennett-Brassard 1984 (BB84) protocol [3]. At each time slot, Alice randomly sends one out of four polarizations: horizontal (H), vertical (V), +45° (D), or −45° (A) using a phase-randomized attenuated laser. Bob randomly measures in either horizontal-vertical (HV) or diagonal-antidiagonal (DA) basis, using a polarization-beamsplitter receiver [Fig. 2(a)]. It has been shown in Ref. 16 that an eavesdropper can, in practice, tilt the beam going towards Bob

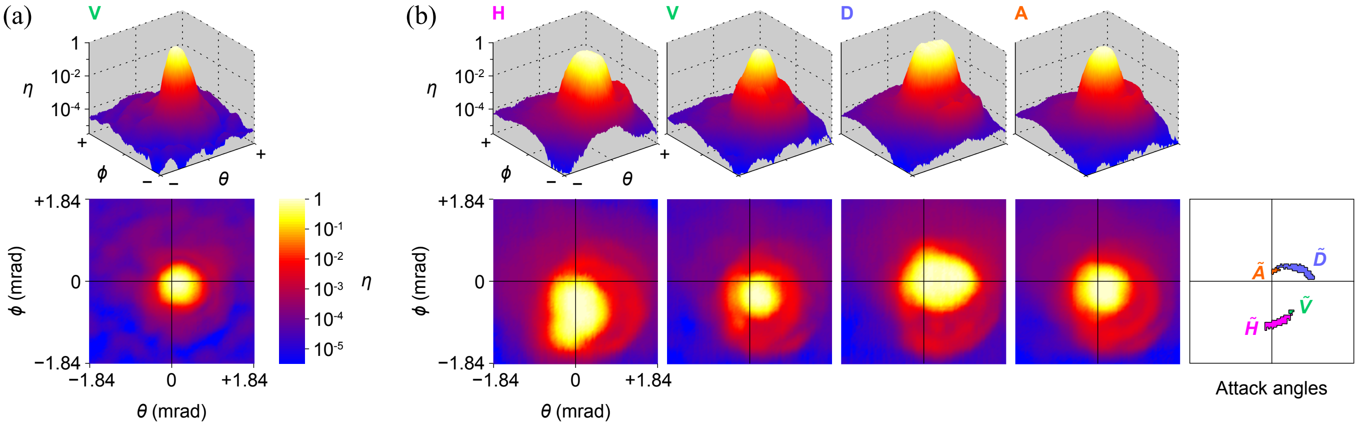


FIG. 3. **Efficiency-mismatch side-channel opened after laser damage in free-space QKD system**. Each pair of 3D–2D plots shows normalised photon detection efficiency η in a receiver channel versus illuminating beam angles ϕ and θ. (a) Before laser damage, the angular dependence is essentially identical between the four channels [16]. Plot for one channel (V) before damage is shown. (b) After the laser damage, the four receiver channels H, V, D, A exhibit unequal sensitivity to photons outside the middle area around $\phi = \theta = 0$. The last plot shows angular ranges for targeting the four detectors that satisfy conditions for the faked-state attack.

by an angle (ϕ, θ) such that the beam misses, partially or fully, the cores of fibers leading to three detectors while being relatively well coupled into the core leading to the fourth detector, as illustrated in Fig. 2(a). This happens because real-world optical alignments are inherently imperfect and manufacturing precision is finite. By sending light at different spatial angles, the eavesdropper can have control over Bob's basis and measurement outcome and steal the key unnoticed [13, 16, 38]. This attack can be prevented by placing a spatial filter or 'pinhole' at the focal plane of lenses L1 and L2, as shown in Fig. 2(a) [16]. Since the pinhole limits the field of view, any light entering at a higher spatial angle is blocked and Eve no longer has access to the target angles required to have control over Bob. As was demonstrated in Ref. 16, a pinhole of 25 µm diameter eliminates this side-channel by making the angular efficiency dependence identical between the four detectors [Fig. 3(a)].

Our testing showed that this countermeasure is destroyed by laser damage. From a distance of 26.1 m, we shot an 810 nm collimated laser beam delivering a 10 s pulse of 3.6 W c.w. power at the pinhole inside Bob's setup. The intensity there was sufficient to melt the material (13 µm thick stainless steel) and enlarge the hole diameter to ≈ 150 µm. The state of the pinhole before and after damage is shown in Fig. 2(b), and a real-time video of the damage process is shown in Supplemental Section IV [36]. Although Bob was up and running in photon counting mode during the test, none of his other components were damaged. With this larger pinhole opening, it was again possible to send light at angles that had relatively higher mismatches in efficiency, as shown in Fig. 3(b). This enabled a faked-state attack under realistic conditions of channel loss in 1–15 dB range with quantum bit error ratio (QBER) < 6.6%. Thus laser damage completely neutralizes this countermeasure, and makes this free-space QKD system insecure. See Supplemental Section II [36] for details.

Discussion. The crucial step of the attack, creating the deviation in device characteristics, has thus been experimentally demonstrated for both systems tested. We repeated this step several times and confirmed that laser power above a certain value (1.7 W in fiber-optic system and 3.6 W in free-space one) always destroys the security-critical component, without inflicting any collateral damage that could result in the denial-of-service. After this, building a complete eavesdropper would be a realistic if time-consuming task [39].

In our testing, we haven't done anything that Eve could not do in the real world. She could buy a copy of each system, rehearse her attacks, then attack an installed system of the same model. By Kerckhoffs' principle [40], Eve is assumed to know the system characteristics and results of damage precisely. In practice when attacking installed devices, if she needs to measure their characteristics, she may probe them remotely by imaging, reflectometry [27], and watching public communication Alice–Bob [38, 39].

At present, no quantum communication system has countermeasures specifically designed to stop laser-damage attack, neither do they have a mechanism to check all possible deviations in device characteristics from the modeled values. Countermeasures to other attacks do not prevent this attack, in fact they become weak points as our experimental study shows. Development of necessary countermeasures is complicated by the fact that Eve can use a laser with different characteristics: power, timing (e.g., short-pulsed laser induces different damage mechanisms than c.w. thermal damage we have observed [41]), wavelength, polarization. Eve can attack the systems in different phases of their operation including powered-off state, which can control what component is damaged. We have experimentally observed dependence of damage on the laser timing profile, as detailed in Supplemental Section III [36], where we show that some profiles have resulted in the denial-of-service but some in a successful attack. We stress that Eve will select the illumination regime that results in the successful attack, if such regime exists at all. Any countermeasure must thus be tested in all possible illumination regimes. Possible directions of development include a passive optical power limiter [42], a single-use 'fuse' that permanently breaks the optical connection if a certain power is exceeded, battery-powered active monitoring supplemented with wavelength filtering, or an optical isolator (for Alice that uses one-way light propagation [6, 7, 20–23, 31, 39]). Hardware self-characterization may be promising [43], however to protect from an arbitrary damage it must monitor a potentially large number of hardware parameters.

It is an interesting question if risk for untested system designs can be estimated. As we have discussed, any given system design contains many optical components with unknown damage characteristics. The outcome of damage (denial-of-service or successful attack) is thus impossible to predict prior to testing. Then, if some of the system designs chosen at random were tested, the risk for the remaining untested designs could be calculated by Bayesian statistics [44]. Unfortunately, truly random choice is impractical to implement with the current state of quantum communications research and limited sample availability. We have instead tested the two system designs that were available in our lab. This biased the choice towards more mature and older designs. Although this unknown bias makes the Bayesian analysis inapplicable, we find it illustrative to consider the risk figure that would have applied if the choice were random. With zero systems tested, the Bayesian probability that at least 20% of the untested system designs (assuming at least 50 of them exist) are vulnerable to this attack is 70.4% (80%), assuming a Jeffreys (uniform) prior. If two randomly chosen system designs were tested with two positive outcomes, this probability would have increased greatly to 98.9% (98.6%). Note that the security risk is generally high, which is in stark contrast with the very low expected theoretical risk [4, 5, 17].

We have experimentally demonstrated laser damage as a new eavesdropping tool that alters parameters of a well-characterized quantum communication system. Any modification of system characteristics might compromise the security either directly by leading to an attack as we have demonstrated, or indirectly by shifting some parameter in the security proof so it would no longer apply. Existing security proofs do not accommodate this, neither do existing systems have any countermeasure implemented against this. Our results thus reveal the potential security risk for other existing systems, which should be tested against this attack.

Acknowledgments. We thank Q. Liu, E. Anisimova and O. Di Matteo for early experimental efforts, S. Todoroki, N. Lütkenhaus, M. Mosca, Y. Zhang, L. Lydersen and S. Lydersen for discussions. This work was supported by the US Office of Naval Research, Industry Canada, CFI, Ontario MRI, NSERC, Canadian Space Agency, ID Quantique, European Commission's FET QICT SIQS project, EMPIR 14IND05 MIQC2 project, and CryptoWorks21. We acknowledge using University of Waterloo's Quantum NanoFab. P.C. was supported from Thai DPST scholarship. J.-P.B. was supported by FED DEV.

Conflicts of interest. A part of this study was supported and M.L. was employed by ID Quantique. The company has been informed prior to this publication, and is developing countermeasures for their affected QKD system. The other authors declare no competing financial interests.

Author contributions. V.M. conceived and led the study. S.K. implemented the fiber-optic experiment. S.S. implemented the free-space experiment and contributed to the fiber-optic experiment. P.C. contributed to the free-space experiment. M.G. contributed to the fiber-optic experiment. C.M. made minor contributions to the free-space experiment. M.L. provided and supported the fiber-optic QKD system under test. T.J. and J.-P.B. provided the free-space QKD receiver under test and contributed to the free-space experiment. R.K. provided the fiber laser facility and co-supervised the fiber-optic experiment. S.S. and V.M. wrote the article, with contributions from all authors.

[1] S. Singh, *The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography* (Fourth Estate, London, 1999).

[2] P. W. Shor, SIAM J. Comput. **26**, 1484 (1997).

[3] 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.

[4] H.-K. Lo and H. F. Chau, Science **283**, 2050 (1999).

[5] D. Gottesman, H.-K. Lo, N. Lütkenhaus, and J. Preskill, Quant. Inf. Comp. **4**, 325 (2004).

[6] S. Barz, E. Kashefi, A. Broadbent, J. F. Fitzsimons, A. Zeilinger, and P. Walther, Science **335**, 303 (2012).

[7] R. J. Collins, R. J. Donaldson, V. Dunjko, P. Wallden, P. J. Clarke, E. Andersson, J. Jeffers, and G. S. Buller, Phys. Rev. Lett. **113**, 040502 (2014).

[8] T. Lunghi, J. Kaniewski, F. Bussières, R. Houlmann, M. Tomamichel, A. Kent, N. Gisin, S. Wehner, and H. Zbinden, Phys. Rev. Lett. **111**, 180504 (2013).

[9] W. P. Grice, P. G. Evans, B. Lawrie, M. Legré, P. Lougovski, W. Ray, B. P. Williams, B. Qi, and A. M. Smith, Opt. Express **23**, 7300 (2015).

[10] C. H. Bennett, F. Bessette, L. Salvail, G. Brassard, and J. Smolin, J. Cryptology **5**, 3 (1992).

[11] V. Makarov, A. Anisimov, and J. Skaar, Phys. Rev. A **74**, 022313 (2006), erratum ibid. **78**, 019905 (2008).

[12] B. Qi, C.-H. F. Fung, H.-K. Lo, and X. Ma, Quant. Inf. Comp. **7**, 73 (2007).

[13] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, Nat. Photonics **4**, 686 (2010).

[14] F. Xu, B. Qi, and H.-K. Lo, New J. Phys. **12**, 113026 (2010).

[15] S.-H. Sun, M.-S. Jiang, and L.-M. Liang, Phys. Rev. A **83**, 062331 (2011).

[16] S. Sajeed, P. Chaiwongkhot, J.-P. Bourgoin, T. Jennewein, N. Lütkenhaus, and V. Makarov, Phys. Rev. A **91**, 062301 (2015).

[17] C.-H. F. Fung, K. Tamaki, B. Qi, H.-K. Lo, and X. Ma, Quant. Inf. Comp. **9**, 131 (2009).

[18] D. Stucki, N. Gisin, O. Guinnard, G. Ribordy, and H. Zbinden, New J. Phys. **4**, 41 (2002).

[19] Clavis2 specification sheet, `http://www.idquantique.com/images/stories/PDF/clavis2-quantum-key-distribution/clavis2-specs.pdf`, visited 20 March 2016.

[20] J.-P. Bourgoin, N. Gigov, B. L. Higgins, Z. Yan, E. Meyer-Scott, A. K. Khandani, N. Lütkenhaus, and T. Jennewein, Phys. Rev. A **92**, 052339 (2015).

[21] N. Walenta, A. Burg, D. Caselunghe, J. Constantin, N. Gisin, O. Guinnard, R. Houlmann, P. Junod, B. Korzh, N. Kulesza, M. Legré, C. W. Lim, T. Lunghi, L. Monat, C. Portmann, M. Soucarros, R. T. Thew, P. Trinkler, G. Trolliet, F. Vannel, and H. Zbinden, New J. Phys. **16**, 013047 (2014).

[22] Y.-L. Tang, H.-L. Yin, S.-J. Chen, Y. Liu, W.-J. Zhang, X. Jiang, L. Zhang, J. Wang, L.-X. You, J.-Y. Guan, D.-X. Yang, Z. Wang, H. Liang, Z. Zhang, N. Zhou, X. Ma, T.-Y. Chen, Q. Zhang, and J.-W. Pan, Phys. Rev. Lett. **113**, 190501 (2014).

[23] P. Jouguet, S. Kunz-Jacques, A. Leverrier, P. Grangier, and E. Diamanti, Nat. Photonics **7**, 378 (2013).

[24] A. Pappa, P. Jouguet, T. Lawson, A. Chailloux, M. Legré, P. Trinkler, I. Kerenidis, and E. Diamanti, Nat. Commun. **5**, 3717 (2014).

[25] S. Félix, N. Gisin, A. Stefanov, and H. Zbinden, J. Mod. Opt. **48**, 2009 (2001).

[26] S. Sajeed, I. Radchenko, S. Kaiser, J.-P. Bourgoin, A. Pappa, L. Monat, M. Legré, and V. Makarov, Phys. Rev. A **91**, 032326 (2015).

[27] A. Vakhitov, V. Makarov, and D. R. Hjelme, J. Mod. Opt. **48**, 2023 (2001).

[28] 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).

[29] 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).

[30] A. N. Bugge, S. Sauge, A. M. M. Ghazali, J. Skaar, L. Lydersen, and V. Makarov, Phys. Rev. Lett. **112**, 070503 (2014).

[31] A. Acín, N. Gisin, and L. Masanes, Phys. Rev. Lett. **97**, 120405 (2006).

[32] J. Barrett, R. Colbeck, and A. Kent, Phys. Rev. Lett. **110**, 010503 (2013).

[33] C. Kurtsiefer, P. Zarda, S. Mayer, and H. Weinfurter, J. Mod. Opt. **48**, 2039 (2001).

[34] P. V. P. Pinheiro *et al.,* poster presented at *QCrypt 2015, Tokyo, Japan, September 28 – October 2, 2015;* P. V. P. Pinheiro *et al.,* manuscript in preparation.

[35] A. Meda, I. P. Degiovanni, A. Tosi, Z. L. Yuan, G. Brida, and M. Genovese, arXiv:1605.05562 [quant-ph].

[36] See Supplemental Material at [URL will be inserted by publisher].

[37] *National security telecommunications and information systems security advisory memorandum (NSTISSAM) TEMPEST/2-95, red/black installation guidance* (US National Security Agency, 1995) declassified in 2000. `http://cryptome.org/tempest-2-95.htm`.

[38] V. Makarov and D. R. Hjelme, J. Mod. Opt. **52**, 691 (2005).

[39] I. Gerhardt, Q. Liu, A. Lamas-Linares, J. Skaar, C. Kurtsiefer, and V. Makarov, Nat. Commun. **2**, 349 (2011).

[40] A. Kerckhoffs, J. des Sciences Militaires **IX**, 5 (1883).

[41] R. M. Wood, *Laser-Induced Damage of Optical Materials* (CRC Press, 2003).

[42] L. W. Tutt and T. F. Boggess, Prog. Quant. Electr. **17**, 299 (1993).

[43] L. Lydersen, V. Makarov, and J. Skaar, Phys. Rev. A **83**, 032306 (2011).

[44] A. Gelman, J. B. Carlin, H. S. Stern, and D. B. Rubin, *Bayesian Data Analysis*, 2nd ed. (Chapman and Hall, 2004).