Deterministic MDI QKD with two secret bits per shared entangled pair

Sofia Zebboudj, Mawloud Omar

Quantum Information Processing Journal manuscript No.
(will be inserted by the editor)

Deterministic MDI QKD with two secret bits per shared entangled pair

Sofia Zebboudj · Mawloud Omar

the date of receipt and acceptance should be inserted later

Abstract Although Quantum Key Distribution schemes have been proven theoretically secure, they are based on assumptions about the devices that are not yet satisfied with today's technology. The measurement-device-independent scheme has been proposed to shorten the gap between theory and practice by removing all detector side-channel attacks. On the other hand, two-way quantum key distribution schemes have been proposed to raise the secret key generation rate. In this paper, we propose a new quantum key distribution scheme able to achieve a relatively high secret key generation rate based on two-way quantum key distribution that also inherits the robustness of the measurement-device-independent scheme against detector side-channel attacks.

Keywords Quantum key distribution · Measurement-device-independent · Two-way quantum key distribution.

1 Introduction

Labelled as counterintuitive, quantum physics was one of the most debated theories during the last century. It is only recently that quantum conundrums

Sofia Zebboudj
Laboratoire d'Informatique Médicale, Faculté des Sciences Exactes
Université de Bejaia, 06000 Bejaia, Algérie.
E-mail: sofiazebboudj@gmail.com, sofia.zebboudj@univ-bejaia.dz

Mawloud Omar
Laboratoire d'Informatique Médicale, Faculté des Sciences Exactes
Université de Bejaia, 06000 Bejaia, Algérie.
E-mail: mawloud.omar@gmail.com, mawloud.omar@univ-bejaia.dz

have been used as the basis of many potentially positive applications in the domain of quantum information transmission (quantum dense coding, quantum key distribution, quantum teleportation, etc.) [1] [2]. Namely, Quantum Key Distribution (QKD) has known a rapid progress in both theory and practice. It allows two parties, commonly referred as Alice and Bob, to share a secret key via quantum channels [1]. The rapid evolution of QKD has been triggered by the conjunction of many other ones. In the classical key distribution algorithms, the security lies in the assumption of unproven mathematical difficulties of certain problems such as the integer factorization problem for RSA [3] and the discrete logarithm problem for the Diffie-Hellman protocol [4]. However, in 1997, Peter W. Shor has discovered algorithms able to perform integer factorization and find discrete logarithms in polynomial time on a quantum machine [5]. Such algorithms would make a large number of private and secret keys, already used in industry, obsolete. Therefore, private information would be no longer protected.

In contrast to the classical key distribution schemes, the security of QKD draws on laws of physics. Indeed, with Heisenberg's uncertainty principle [6] and the quantum no-cloning theorem [7], QKD has been proven information-theoretically secure i.e. no assumptions are made about the amount of resources available to an eavesdropper, Eve, for computing the secret key [8] [9]. Charles H. Bennett and Gilles Brassard were the first to propose a QKD scheme in 1984. In the BB84 scheme [10], Alice and Bob use two photon polarization bases (rectilinear and diagonal) to encode the binary secret key in four quantum states $\{|\uparrow\rangle, |\downarrow\rangle, |\nwarrow\rangle, |\nearrow\rangle\}$. The secret key is then sent by Alice to Bob and sifted through bases reconciliation, information reconciliation and privacy amplification phases. If Eve attempts to measure the photons before transmitting them to Bob she would disturb the photons' states and reveal her presence. Other schemes have also been proposed such as the Six-State Protocol (SSP) [11], as well as E91 [12] and BBM92 [13] schemes which use quantum entanglement.

QKD has been demonstrated through many tests out of the laboratories [14] and commercial QKD applications are currently available on the market, e.g., Cerberis, QPN-8505 and qOptica created respectively by IdQuantique, MagiQ and QuintessenceLabs. However, although QKD has been granted unconditional security by laws of physics, real-life implementations are still far

from reaching this level of security and various attacks have been demonstrated effective against commercial systems [15] [16]. This is due to the fact that the considered technology in the security proofs of QKD was overlooked and idealized, and therefore, do not reflect the current available technology. Indeed, non reliable equipments may produce signals containing more than one photon prepared in the same state, hence, allowing Eve to conduct a Photon-Number-Splitting attack (PNS) [17], where she blocks all single-photon signals and splits off multi-photon signals, keeping a copy of the quantum state and sending the others to Bob. Therefore, the no-cloning theorem is wasted and the security of QKD is compromised.

The sources that prepare the quantum signals may also be exploited to gain information about the secret key without being detected. However, the sources are typically less likely to be targeted since it is possible for Alice and Bob to prepare their quantum signals in a fully protected environment outside the influence of Eve. On the other hand, protecting the measurement devices is more challenging. In fact, many side-channel attacks targeting the measurement devices can be performed to completely learn about the secret key [16]. Other schemes have been proposed in order to cope with the practical issues of QKD. A relatively easy to implement scheme, named the decoy state scheme [18] [19], was proposed to detect a PNS attack by using decoy states in addition to the signal states. The Device-Independent (DI) QKD [20] was proposed to regain the security by removing side-channel attacks and prove it without knowing implementation details. The expected key rate is however too low even at short distances (10^{-10} bits per pulse) [20]. The Measurement-Device-Independent (MDI) QKD was then proposed to remove all detector side-channel attacks while the key generation rate appears to be more practical: (623 bits/s over 80 km [21], 0.018 bits/s over 200 km [22], 134 kbits/s at 0 km [23] and even a rate of 1.6 Mbits/s has been reached at 0 km with sources generating 10^9 pulses per second [24]). Another way to increase the distributed secret key rate was proposed in [25], where the secret key is distributed in a deterministic manner, thus, no qubits have to be discarded due to base mismatch, which theoretically occurs 50% of the time in One-Way (OW) QKD. In this class of schemes, named Two-Way (TW) QKD and based on the idea of Quantum Dense Coding (QDC) [2], Alice performs encoding operations on quantum states received from Bob without knowing the preparation

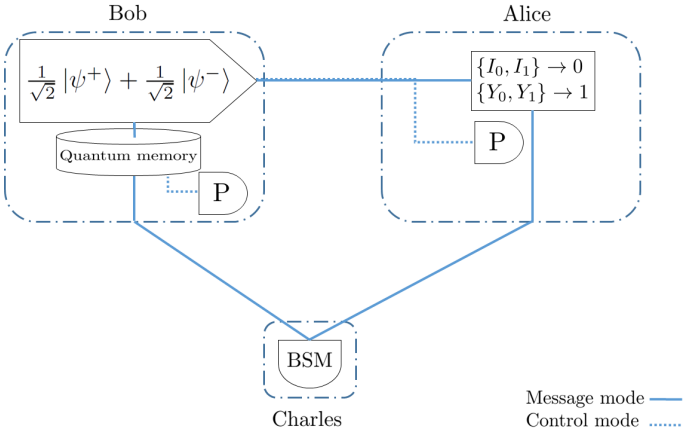
bases. She sends back these quantum states to Bob, who measures them in the same basis he has prepared them. According to the measurement outputs, Bob can then recover the secret key encoded by Alice. However, the security proofs of most TWQKD schemes do not consider the losses in the channels and the detectors [26]. A Modified Ping-Pong (MPP) scheme, however, has been proven secure even in lossy channels [26] and experimentally realized [27]. In this paper, we propose a new QKD scheme that combines the robustness of the MDI scheme against detector side-channel attacks and the bases reconciliation free MPP scheme to increase the secret key generation rate. Moreover, the proposed scheme doubles the generated final secret key compared to the MPP scheme and is more practical for today's massively exchanged data.

2 The proposed scheme

In its basic setup [28], the MDI QKD scheme allows Alice and Bob to share a secret key based on prepared phase randomized Weak Coherent Pulses (WCPs) in the different BB84 polarization states. Alice and Bob send their qubits to Charles, an untrusted measurement device, which performs a Bell State Measurement (BSM) on the received qubits. Alice and Bob then post-select the events where they use the same bases and Charles outputs a successful result, i.e., when Alice and Bob do not prepare the qubits in the same state when they both select the rectilinear basis. Depending on Charles output and their preparation bases, Alice and Bob decide to flip or not their bits. Just as in typical OWQKD schemes, the qubits are not all used to generate the final secret key and are simply discarded. In order to make a deterministic aspect out of the MDI QKD scheme and therefore, raise the secret key rate, we propose a scheme where the shared secret key bits are encoded according to the deterministic TWQKD scheme MPP [26]. Thus, our scheme inherits the immunity against detector side-channel attacks and no prepared qubit is discarded because of bases reconciliation.

Our scheme is illustrated in Figure 1 and proceeds as follows. First, Bob prepares N pairs of maximally entangled qubits in the states $|\psi^+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$ and $|\psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$, with equal probabilities. Bob sends to Alice one of the two qubits; "the travel qubit" and stores the "home qubit" in a quantum memory. Since the pairs are maximally entangled, the reduced

Fig. 1 Our scheme



state of the travel qubit is maximally mixed. Eve would not have any significant information about which state Bob has prepared. Alice and Bob both switch to either control mode or message mode. In control mode, Bob measures his reserved qubit and Alice measures the travel qubit using the projectors $P = \{|v\rangle\langle v|, |0\rangle\langle 0|, |1\rangle\langle 1|\}$, where $|v\rangle$ is the vacuum state. The measurement results are publicly announced and the probabilities p_{00}, p_{01}, p_{0v}, p_{10}, p_{11} and p_{1v} (where p_{ij} is the probability that Alice receives $|i\rangle$ when the travel qubit is $|j\rangle$) are shared in order to bound Eve's information on the secret key. In message mode, Alice performs one of the four unitary operations on the travel qubit $\{I_0, I_1, Y_0, Y_1\}$, where [26]: $I_0\{|v\rangle, |0\rangle, |1\rangle\} = \{|v\rangle, |0\rangle, |1\rangle\}$ and $I_1\{|v\rangle, |0\rangle, |1\rangle\} = \{|v\rangle, -|0\rangle, -|1\rangle\}$ are used to encode the classical bit 0, while $Y_0\{|v\rangle, |0\rangle, |1\rangle\} = \{|v\rangle, |0\rangle, -|1\rangle\}$ and $Y_1\{|v\rangle, |0\rangle, |1\rangle\} = \{|v\rangle, -|0\rangle, |1\rangle\}$ are used to encode the classical bit 1. Note that the vacuum state $|v\rangle$ will introduce a phase randomization to Eve's system and limit the information she can gain about the secret key, while the decoding in Bob's side is not affected. Also in message mode, Alice and Bob both send their part of the pair to Charles (untrusted measurement device), where he performs a Bell State Measurement (BSM) and projects the received qubits into either $|\psi^+\rangle$ or $|\psi^-\rangle$. The results are then publicly revealed. If Bob prepares the system in the state $|\psi^+\rangle$ (respectively $|\psi^-\rangle$), receiving the result $|\psi^+\rangle$ (respectively $|\psi^-\rangle$) from Charles means that Alice has encoded the classical bit 0, while receiving the result $|\psi^-\rangle$ (respectively $|\psi^+\rangle$) means that Alice has encoded the classical bit 1. Once all the travel qubits are sent, Bob and Alice estimate

the error rate e of the raw key through an authenticated channel and perform information reconciliation and privacy amplification to generate a correlated and secure final key.

It is important to note that in the MPP scheme, Bob and Alice do not announce beforehand which trials are in control mode and which ones are in message mode because Eve would know when not to disturb the transmission. Therefore, Alice and Bob may not always be in the same mode. When Alice is in CM and Bob is in MM for instance, the trial will not serve to control the transmission in order to detect Eve because Bob will not measure its home qubit and compare his results with Alice's measurement; neither will the trial serve to generate the secret key since Alice will not encode anything in the travel qubit. Consequently, when they are not in the same mode, Alice and Bob have to discard the trial, similar to when the two pairs have to discard all the qubits they did not measure in the same basis in One-Way QKD. Thus, the bases reconciliation disadvantage of One-Way schemes would only become a mode reconciliation problem for MPP. Note also that without knowing the preparation of Bob, Eve cannot determine which bit has been encoded by Alice. Since the result of the BSM is also known by Alice, therefore, Alice knows the preparation of Bob. If Alice chooses to encode the classical bit 1 (respectively 0), she will (not) modify the state of the prepared entangled qubits. Then, according to the result of Charles, she will know whether Bob has prepared $|\psi^+\rangle$ or $|\psi^-\rangle$. We can make use of this "extra" knowledge to encode an additional bit per shared maximally entangled states. The first bit will be determined by which operation Alice uses to encode the travel qubit (I_i for 0 and Y_i for 1 where $i \in \{0, 1\}$) and the second bit will be determined by Bob's preparation. They will associate for example the classical bit 0 to $|\psi^+\rangle$ and the classical bit 1 to $|\psi^-\rangle$.

An example of our scheme's process is as follows. Suppose that Alice wants to send the classical bit 0 and Bob wants to send the classical bit 1. Alice would choose to use either I_0 or I_1 to encode the first bit 0 and Bob would prepare the qubits in the state $|\psi^-\rangle$. Once the result of the BSM is known, Alice would use it to know which state Bob has prepared, and therefore which bit he wants to share. Bob, on the other hand, would use it to know which bit Alice has encoded in the travel qubit. If the BSM result is $|\psi^-\rangle$, Bob would know that Alice has encoded the bit 0 and Alice would know that Bob has prepared the

state $|\psi^-\rangle$ which is associated with the classical bit 1. The first bit is encoded in the travel qubit while the second one is determined by Bob's preparation. This is illustrated in Table 1.

Table 1 Possible outcomes of the secret key bits

•	I_0	I_1	Y_0	Y_1
$\|\psi^+\rangle$	00	00	10	10
$\|\psi^-\rangle$	01	01	11	11

3 Security proofs

The secret key generated in our scheme depends on both Bob's preparation and Alice's encoding. The probabilities of Bob preparing $|\psi\rangle^+$ and $|\psi\rangle^-$ are $\frac{1}{2}$. Since the prepared pairs of qubits are maximally entangled, the reduced states of the travel and home qubits are maximally mixed and neither Eve nor Alice can gain any information on which state Bob has prepared given only the travel qubit. In our scheme, as in the MDI QKD scheme, the measurement device, Charles, can be untrusted; Eve can control the BSM results. Fortunately, that would not compromise the security; Alice and Bob can verify the honesty of Charles by comparing a random set of their data [28]. Moreover, in our scheme, Bob's preparation cannot be found given only the BSM results.

As for gaining information on Alice's encoding, we can describe the most general collective attack on the Bob-Alice channel as a unitary interaction between Eve's probe and the travel qubit [26]:

$$U|0\rangle|\epsilon\rangle = \sqrt{p_{0v}}\,|v\rangle|\epsilon_{0v}\rangle + \sqrt{p_{00}}\,|0\rangle|\epsilon_{00}\rangle + \sqrt{p_{01}}\,|1\rangle|\epsilon_{01}\rangle\,, \tag{1}$$

$$U|1\rangle|\epsilon\rangle = \sqrt{p_{1v}}\,|v\rangle|\epsilon_{1v}\rangle + \sqrt{p_{10}}\,|0\rangle|\epsilon_{10}\rangle + \sqrt{p_{11}}\,|1\rangle|\epsilon_{11}\rangle\,, \tag{2}$$

where U is the unitary operator and $|\epsilon_{ij}\rangle$ are Eve's possible quantum ancillary states after the interaction. p_{0v}, p_{01}, p_{1v} and p_{10} are the probabilities that Eve's operation has altered the travel qubit, while p_{00} and p_{11} are the probabilities that the travel qubit has not been altered.

The probabilities of encoding key bit 0 or 1 are $\frac{1}{2}$ and Eve cannot obtain any information from the vacuum state. Following the same line sketched in [26], we obtain the Von Neumann entropy on Alice's part of the key bit A' given the system AE:

$$S(A'|AE) = 1 - H(p'_{01}), \tag{3}$$

where $p'_{01} = p_{01}/(p_{00} + p_{01})$.

Later, Alice and Bob send their qubits to Charles, Eve's total entropy on Alice becomes:

$$S(A'|AE) \geq -\frac{H(p'_{01}) + H(p'_{10})}{2\eta}, \tag{4}$$

where η is the channel efficiency.

Finally, they can estimate the error rate e by comparing a set of their shared bits to perform information reconciliation and privacy amplification to finally generate the secret key.

Since Bob's preparation is also taken into account, the final key bits in our proposal are doubled in comparison with MPP [26] and much higher than MDI [28] because of the possible base mismatch, so is the rate. The secret key generation rate R is given by:

$$R = 2 \cdot R_{MPP} \geq 2 \cdot \left(1 - \frac{H(p'_{01}) + H(p'_{10})}{2\eta} - H(e)\right). \tag{5}$$

4 Simulation

Numerical simulation is given in this section to evaluate the performance of our proposal. For the sake of comparison, we use off-the-shelf experimental parameters and the same assumptions as MPP [26]: optical fiber is used to transmit the polarized photons and its transmission efficiency η is the same in the Bob-Alice, Alice-Charles and Bob-Charles channels. The optical fiber loss coefficient is 0.2 dB/km, detection efficiency is $\eta_d = 10\%$, its dark count rate is $p_d = 10^{-5}$ and the misalignment of detector is $d_e = 1\%$. The polarization errors corresponding to p'_{01} come from the dark count of single photon detector:

$$p'01 = \frac{\eta\eta_d d_e + (1 - \eta\eta_d)p_d}{\eta\eta_d + 2(1 - \eta\eta_d)p_d}, \tag{6}$$

and the error rate e only comes from dark count:

$$e = \frac{(1-\eta^2)\eta^2\eta_d p_d}{\eta^4\eta_d^2 + 2(1-\eta^2)\eta^2\eta_d p_d}. \tag{7}$$

The key generation rate is:

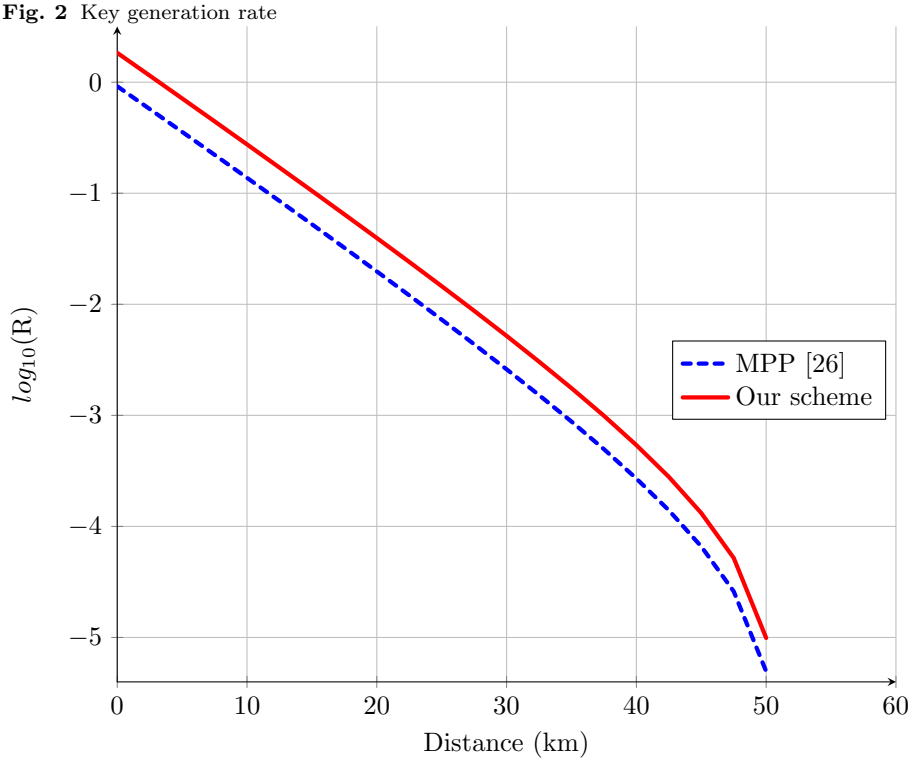
$$R = 2 \cdot \eta^4 \left(1 - \frac{H(p'_{01}) + H(p'_{10})}{2\eta} - H(e)\right). \tag{8}$$

To calculate the key generation rate as a function of the distance d, we use the relation between the transmission efficiency and the distance, such as

$$\eta = 10^{-0.02 \cdot d}, \tag{9}$$

which we replace in Eq. 8.

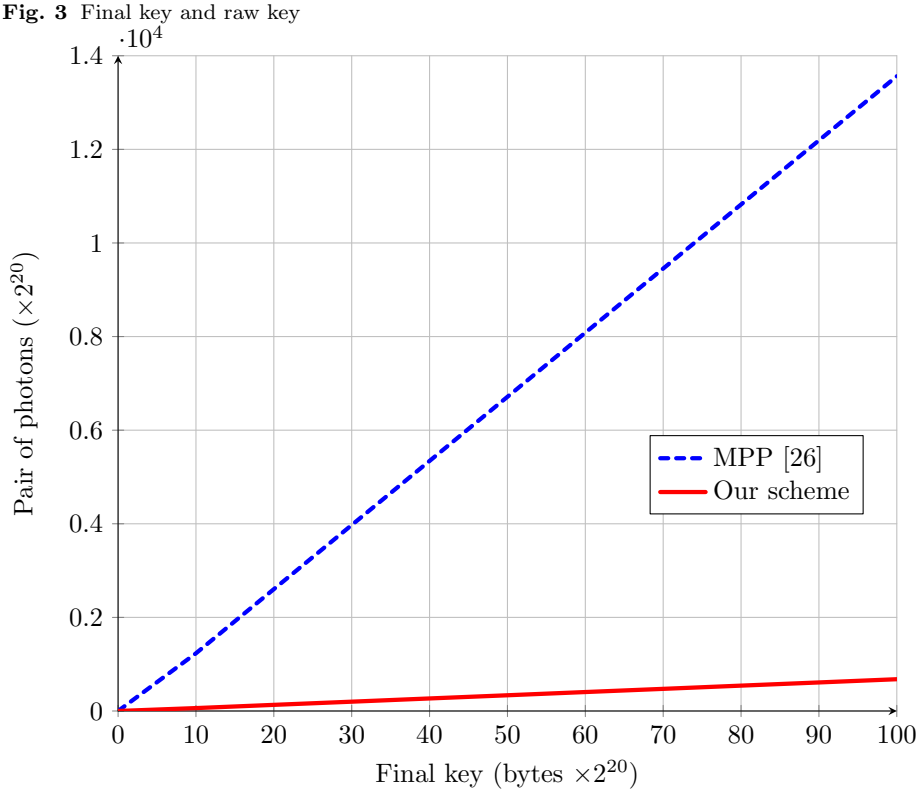
Fig. 2 Key generation rate



Simulation results, illustrated in Figure 2, show that the secret key generation rate of our scheme at slightly more than 0 km is $R = 1.8$ and for a distance of 50 km, the rate is $R = 10^{-5}$ (10 dB loss). With light sources generating pulses at 4 MHz effective clock rate, our scheme would produce secret key rates ranging from about 40 bits/s at 50 km to more than 7 Mbits/s at 0 km. This results show that our scheme can distribute keys at relatively high rates.

To show more about the advantage of our proposal, we have calculated the number of pairs of photons N needed to be prepared in order to generate a secret key over 25 km for both our proposal and the MPP scheme. This is illustrated in Figure 3.

Fig. 3 Final key and raw key



It is clearly observable that our scheme is better for establishing the long secret keys needed nowadays for encrypting massive data. In fact, our scheme

does not need as many pairs of photons as MPP to establish secret keys of a certain length. For instance, less than $N = 3.5 \times 10^8$ pairs of photons are needed to establish a secret key of 50 Mbytes with our scheme, while about $N = 7.2 \times 10^9$ pairs are needed for the MPP scheme.

5 Conclusion

The implementation of QKD schemes has been challenged by loopholes in the devices, which have lowered the security level of those schemes. The MDI QKD have been proposed to remove all detector side-channel attacks, arguably the most critical part of QKD implementation [28]. Because of the base mismatch in MDI QKD, only 50% of the shared qubits are used to estimate errors and generate the final key. TWQDK has been proposed to avoid bases reconciliation and therefore, make use of every prepared and encoded bit. In this paper, we have proposed a new QKD scheme which allows two pairs, Alice and Bob, to share a secret key used for encryption. The proposed scheme is designed similarly to the MDI QKD scheme in order to gain its robustness against detector side-channel attacks. In order to overcome the base mismatch problem, TWQKD principle is applied and Alice's key bits are encoded with the same unitary operators as the MPP scheme. Bob's preparation is also included in the process of our scheme allowing us to obtain a higher and more practical final secret key generation rate.

Acknowledgements The authors would like to thank H. GHARBI for helpful discussions. We also thank M. AZNI for helping us clarify some of the issues treated in this paper. This work was carried out as part of research activities of the LIMED laboratory affiliated to the Faculty of Exact Sciences of the University of Bejaia.

References

1. Gisin, N., Ribordy, G., Tittel, W., Zbinden, H., Quantum Cryptography, Rev. Mod. Phys., 74, 145 (2002).
2. Bennett, C. H. Wiesner, S. J., Communication via one- and two-particle operators on Einstein-Podolsky-Rosen states, Phys. Rev. Lett., 69, 2881 (1992).
3. Rivest, R., Shamir, A., Adleman, L., A method for obtaining digital signatures and public-key cryptosystems, Commun. ACM, vol. 21, no. 2 (1978).
4. Diffie, W. Hellman, M., New directions in cryptography, IEEE Trans. Inform. Theory IT-22, 644-654 (1976).

5. Shor, P. W., Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer, SIAM J. Sci. Statist. Comp., 26, 1484 (1997).
6. Barnett, S. M. Phoenix, S. J., Information-theoric limits to quantum cryptography, Phys. Rev. A, 48, R5-R8 (1993).
7. Wootters, W. K. Zurek, W. H., A single quantum cannot be cloned, Nature, 299, 802-803 (1982).
8. Mayers, D., Unconditional security in quantum cryptography, J. ACM, vol. 48, no. 3, 351-406 (2001).
9. Bruss, D., Erdélyi, G., Meyer, T., Riege, T., Rothe, J., Quantum cryptography: A survey, ACM Comp. Surv., vol. 39, no. 2, Article 6 (2007).
10. Bennett, C. H. Brassard, G., Quantum cryptography: Public key distribution and coin tossing, International Conference on Computers, Systems Signal Processing, Bangalore, India, 175-179 (1984).
11. Bechmann-Pasquinucci, H. Gisin, N., Incoherent and coherent eavesdropping in the six-state protocol of quantum cryptography, Phys. Rev. A, 59, 4238 (1999).
12. Ekert, A. K., Quantum cryptography based on Bell's theorem, Phys. Rev. Lett., vol.67, no. 6, 661 (1991).
13. Bennett, C. H., Brassard, G., Mermin, N. D., Quantum cryptography without Bell's theorem, Phys. Rev. Lett., 68:557 (1992).
14. Qiu, J., Quantum communications leap out of the lab. Nature, 508, 441-442 (2014).
15. Diamanti, A., Lo, H.-K., Qi, B., Yuan, Z., Practical challenges in quantum key distribution, npj Quantum Information, 2, 16025 (2016).
16. Lo, H.-K., Curty, M., Tamaki, K., Secure quantum key distribution. Nat. Photon., 8, 595-604 (2014).
17. Mailloux, L. O., Hodson, D. D., Grimaila, M. R., Engle, R., McLaughlin, C., Baumgartner, G., Using modeling and simulation to study photon number splitting attacks. IEEE Access, 4, 2188-2197 (2016).
18. Lo, H.-K., Ma, X., Chen, K., Decoy state quantum key distribution. Phys. Rev. Lett., 92, 230504 (2005).
19. Mailloux, L. O., Grimaila, M. R., Hodson, D. D., Engle, R., McLaughlin, C., Baumgartner, G., Modeling, simulation, and performance analysis of decoy state enabled quantum key distribution systems. Appl. Sci., 7, 212 (2017).
20. Mayers, D. Yao, A., A quantum cryptography with imperfect apparatus. in Proceeding of the 39th Annual Symposium on Foundations of Computer Science, 503-509 (1998).
21. Valivarthi, R. et al. Measurement-device-independent quantum key distribution: from idea towards application, J. Mod. Optic., 62, 1141-1150 (2015).
22. Tang, Y.-L. et al. Measurement-device-independent quantum key distribution over 200 km, Phys. Rev. Lett., 113, 190501 (2014).
23. Roberts, G. L., Lucamarini, M., Yuan, Z. L., Dynes, J. F., Comandar, L. C., Sharpe, A. W., Shields, A. J., Experimental measurement-device-independent quantum digital signatures, Nat. Commun., 8, Article 1098 (2017).
24. Comandar , L. C., Lucamarini, M., Fröhlich, B., Dynes, J. F., Sharpe, A. W., Tam, S. W.-B., Yuan, Z. L., Penty, R. V. Shields, A. J., Quantum key distribution without detector vulnerabilities using optically seeded lasers, Nat. Photonics, 10, 312-315 (2016).

25. Bostroem, K., Felbinger, T., Deterministic secure direct communication using entanglement. Phys. Rev. Lett, 89, 187902 (2002).
26. Han, Y.-G., Yin, Z.-Q., Li, H.-W., Chen, W., Wang, S., Guo, G.- C., Han, Z.-F., Security of modified Ping-Pong protocol in noisy and lossy channel, Sci. Rep., 4, 4936 (2014).
27. Chen, H., Zhou, Z.-Y., Zangana, A. J. J., Yin, Z.-Q., Wu, J., Han, Y.-G., Wang, S., Li, H.-W., He. D.-Y., Tawfeeq, A. K., Shi, B.-S., Guo, G.-C., Chen, W., Han, Z.-F., Experimental demonstration on the deterministic quantum key distribution based on entangled photons, Sci. Rep., 6, 20962 (2016).
28. Lo, H.-K., Curty, M., Qi, B., Measurement-device-independent quantum key distribution, Phys. Rev. Lett., 108, 130503 (2012).