Deterministic secure quantum communication with and without entanglement

Tarek A. Elsayed$^1$\footnote{tarek.ahmed.elsayed@gmail.com}

$^1$Department of Physics and Astronomy, Hunter College of the City University of New York, New York 10065, USA

(Dated: April 15, 2019)

We present a quantum protocol for sending a deterministic message by encrypting each classical bit by two photons and using a quantum key. The protocol has two varieties where the two photons can be either entangled or non-entangled and requires a one-way quantum channel and a classical channel. The protocol requires also preprocessing the information before being encoded in the quantum state of photons in order to prevent an eavesdropper from deciphering parts of the message. The key to decrypt the message is sent with the same quantum encryption protocol only if no eavesdropper is detected.

1. INTRODUCTION

Quantum cryptography has become one of the most fruitful and versatile commercial applications of quantum information. While classical encryption can in principle be compromised with a powerful enough computer, quantum encryption provides a platform where any eavesdropping attempt can be detected with a very high probability. There are several major schemes where quantum encryption is employed such as quantum key distribution (QKD) where a random key is generated and securely shared between two parties and used later in classical encryption, quantum secure direct communication (QSDC) where a certain message is securely and directly transferred between two parties using a quantum algorithm without the need for sharing a secure key or sending data over the classical channel except for detecting an eavesdropper and deterministic secure quantum communication (DSQC) where the message is also sent deterministically over a quantum channel with the help of sending data over the classical channel [1]. There is also a wide variety of implementations of each of these schemes in terms of the states of the photons used (entangled photons or single photons) and the type of the quantum channel (one-way or two-way channel).

The oldest QKD protocol (BB84) was introduced by Bennett and Brassard in 1984 [2] and uses single photons. There are other protocols that use entangled pairs of photons such as the protocol introduced by Eckert [3]. Similarly, there are numerous QSDC schemes that use entangled photons, usually in one of Bell states $(|1\rangle - |6\rangle)$ and others which use single photons [7] and DSQC schemes which use entangled photons [8–10] and others that use single photons [9, 11–13]. Many QSDC/DSQC protocols require two-way quantum channels where photons are sent back and forth between Alice and Bob (the two famous parties who know the laws of quantum mechanics very well and use them in order to secure their communication). This requires storing the qubits for a long time which may be difficult to achieve due to their short coherence time and requires also controlling the timing of their manipulation using a quantum memory [14].

QKD can be implemented by sending single photons using only a single degree of freedom, i.e., using a two-dimensional Hilbert space, as in BB84 protocol. For sending data in a deterministic manner, we need at least a four-dimensional Hilbert space [11, 15]. For example, in the protocol proposed by A. Beige et. al. [11] both the spatial and polarization degrees of freedom of single photons are used. In DSQC/QSDC, we aim, as in QKD, to detect an eavesdropper (let us call him Evan) with a very high probability, and also to prevent Evan from discerning a good part of the message before being detected [7]. One of the main ideas in this paper is that fulfilling the first aim actually facilitates the fulfillment of the second one, by sending an encrypted message, and only sending the key to decrypt this message once the safety of the communication channel is verified. This can be done in several ways. For example, we can preprocess the message before sending it with a DSQC protocol using a symmetric cryptographic algorithm and send the crypto-key (using a similar DSQC protocol) only if the channel is safe. This way, we can ensure that even if Evan discerned part of the sent packet, he will not be able to decipher it since the key will not be available to him. Another simple way to do this is simply to shuffle the bits constituting the message in a random order and only send the information used to restore the order of each bit after ensuring the privacy of the channel.

In this paper, we present a scheme where both the key and the encrypted message are sent over a quantum channel using pairs of single photons or entangled photons. The two protocols require a one-way quantum channel in addition to the classical channel and use a similar pre- and postprocessing of the transmitted bits (Fig. 1) but differ in the quantum encryption part (Fig. 2). In section 2, we present the first protocol using unentangled photons and describe the classical preprocessing common in the two protocols. In section 3, we present the second protocol using entangled photons. We present the two protocols using generic quantum circuits. Finally, in section 4, we analyze the error rates caused by a simple eavesdropping scheme for the two protocols.
2. DSQC PROTOCOL WITHOUT ENTANGLEMENT

In this protocol, Alice encodes each bit by two photons (we will refer to photons as qubits henceforth) encoded in two different bases assigned to the two qubits randomly. For general qubits, a Hadamard gate can be inserted to one of the two qubits selected randomly after being encoded in the computational basis with the state of the classical bit. In the case for photons, these two bases can be the rectilinear and diagonal polarization. Bob, on the other hand, measures the two qubits always in the same basis which can be either one of them randomly for each pair (see Fig. 2-a, b). By doing this, and assuming a noiseless channel, he ensures that at least one of the two qubits will be measured in the correct basis. The measurement outcome of the other qubit will be completely random. In cases where his measurements of the two qubits agree, he knows for sure which bit was encoded by Alice without the need for classical communication. For the other cases, Bob will send to Alice over the classical channel the locations of the pairs where his measurement outcomes are different. Alice, in turn, will send him over the classical channel her choices for these cases.

So far, we have introduced only the quantum encryption part of our DSQC protocol. In order to detect eavesdropping and ensure that Evan cannot decode any part of the message before he is detected, more layers of complexity should be added at each level (see Fig. 1). For example, Alice can insert a random subset of bits (redundancy check bits) into the main message at random locations and communicate with Bob in public at the end of transmission her choices for these bits together with their locations. An eavesdropper intervening in the middle by doing any kind of measurements will spoil the encoding of the redundant qubit pairs. Moreover, in order to prevent Evan from detecting any sequence of bits before being detected, the packet is encrypted with some sort of symmetric-key encryption algorithms before being sent to Bob. The key is generated at Alice’s side and sent to Bob in the same manner at the end of the encrypted packet transmission only if no eavesdropping is detected. Consequently, even if Evan could intercept a few bits of the encrypted message by posing as Bob, he would not be able to get any useful information from them without the key used by Alice to encrypt the message. In other words, in order for Evan to get any part of the packet he needs to know both the exact key and the exact encrypted message without being detected which is very improbable to happen.

Let us now outline the complete algorithm in detail.

1. Alice divides the full message into small packets \( M \), and computes a hash value \( S \) for each packet, such as a cyclic redundancy check (CRC) [16] or a checksum to detect errors in the transmission. Let us denote each of the new packets resulting after appending \( S \) to \( M \) as \( C \).

2. Alice generates a random key \( K \) and use it to encrypt \( C \) by a symmetric key algorithm [17] to obtain a new packet \( P \). We recommend an error correcting code such as [18] in order to overcome errors due to noisy channels or imperfect photon detectors. Nevertheless, let us assume for the sake of simplicity that \( P = K \times C \).

3. Alice adds a small number of random bits at random locations of \( P \) as a redundancy check to obtain a new packet \( T \).

4. Inside the quantum encoder, Alice encodes each bit of \( T \) by two qubits in the \(|0\rangle \) or \(|1\rangle \) according to the classical bit before applying a Hadamard gate to one of the two qubits selected randomly (see Fig. 2-a).

5. Bob receives each pair of qubits and either applies a Hadamard gate to the two qubits or not randomly and records his measurements for each pair, as in Fig. 2-b.

6. Bob sends to Alice over the classical channel the locations of the pair where his measurements outcomes agree. These are the bits of \( T \) which Bob could decode independently of Alice.

7. Alice sends to Bob over the classical channel her choices of the basis for the other pairs. Bob uses this information to decode the rest of \( T \).

8. Alice sends to Bob the indices of the redundant bits added to \( P \) and they compare their values of these bits. If the number of discrepancies between them is higher than a certain threshold determined by the noise of the channel, they conclude that an eavesdropper is intercepting the transmission and the transmission is aborted. Otherwise, they proceed with the transmission of the key and steps 4-7 are repeated for \( K \).

9. Bob uses \( K \) to decrypt \( T \) in order to obtain \( C \). He computes the hash value \( S \) and compares it with the received one. In case of discrepancies, they conclude that either the channel is too noisy and the errors have corrupted the message/key or the whole transmission is compromised.

3. DSQC PROTOCOL WITH ENTANGLEMENT

Here, we introduce a second protocol which is similar to the one presented in the previous section in terms of the classical preprocessing, but differs in the quantum encoding stage. In this protocol, we encode every classical bit by two entangled qubits which are divided among Alice and Bob. In particular, we encode ‘1’ by the state \( \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) \) and ‘0’ by the state \( \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) \). These two states can be generated by the circuit shown in Fig. 2-c with the information bit controlling a Z-gate [19]. The two states
are verified to be entangled using the Peres–Horodecki criterion [20, 21].

Alice sends one of the two qubits to Bob and keeps the other one. Bob applies a Hadamard gate to his qubit before measuring it in the computational basis (see Fig. 2-d). The state of the two qubits just before the measurements become the Bell states $\frac{1}{\sqrt{2}}(|10\rangle - |01\rangle)$ for ‘1’ and $\frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$ for ‘0’. When Alice announces in public the result of her measurement, Bob knows from his own measurement whether the Z-gate was inserted or not, i.e., whether ‘1’ or ‘0’ was encoded. An eavesdropper tampering with the communication channel will alter the state of the two qubits and eventually introduce errors that can be detected using the redundancy check bits.

4. SECURITY ANALYSIS AND DISCUSSION

Let us imagine a typical eavesdropping scenario and analyze the bit error rate (BER) caused by it, assuming that perfect photon detectors are used by all sides. Let us consider first the quantum encoder without entanglement. A typical strategy Evan can follow is to behave as Bob by measuring the two qubits in the same basis, re-encode them, as Alice would do, and send them forward to Bob. This is called intercept-resend-attack. In this strategy, one of the two qubits (the one corresponding to disagreement between Alice’s and Evan’s choices) will be certainly disturbed by Evan. Bob, on the other hand, will measure the two qubits in some basis, which may be different than Evans’. If their choices agree, their measurement outcomes will also agree. In this case, regardless whether the measurement outcomes of the two qubits are the same or not, Evan will be able to know the classical bit that was encoded after Alice communicates her choices over the classical channel and it will also cause no errors in the transmitted bit. This scenario will occur 50% of the time. On the other hand, if the choices of Evan and Bob disagree (this occurs 50% of the time as well), the measurement outcomes at Bob’s side will be completely random, and therefore errors will occur with a probability 50%, given this scenario. Therefore, the bit error rate, assuming a noiseless channel, caused by the intervention of Evan is 25%, similar to the BER of BB84 protocol for the same kind of attack. More complex attack scenarios may result in lower BER.

Let us now consider the same intercept-resend attack for quantum encoder with entanglement. Evan, while posing as Bob, will insert a Hadamard gate before he measures in the computational basis. In doing so, he will project the qubit into $|1\rangle$ or $|0\rangle$, thus disentangling it from the other qubit. When Bob performs his measurement after inserting a Hadamard gate, he will get a completely random outcome, therefore the bit error rate will be as high as 50%. While Evan acquires most or all of the transmitted bits after the public exchange between Alice and Bob with these two encoders, the high bit error rate, especially with using entangled qubits, increases the probability of detecting the eavesdropper before sending the key and thus prevents Evan from deciphering the original message.

In conclusion, it was shown that by combining the methods of classical cryptography and quantum encryption we can find new protocols for deterministic secure quantum communication that encodes both the key and the message with the same quantum algorithm and can detect an eavesdropper with a high probability. Conventional methods of DSQC do not require sharing a private key between Alice and Bob. In our case, we use a special key to encrypt each packet and send it on the quantum channel. While for the quantum one-time pad protocol [7] a security check is performed before the message is sent, here, we perform the check concurrently while sending an encrypted message. The proposed scheme does not require a two-way quantum channel and thus demands less stringent requirements on the photon storage than other schemes which require two-way quantum channels. A full security proof and an analysis of more complex attack strategies are required to ensure the security of this protocol.

The author thanks Prof. Mark Hillery for the hospitality of Hunter College of CUNY where this work was initiated.

[1] G.-l. Long, F.-g. Deng, C. Wang, X.-h. Li, K. Wen, and W.-y. Wang, Frontiers of Physics in China 2, 251 (2007).
[2] C. H. Bennett and G. Brassard, in Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, India (IEEE, 1984) pp. 175–179.
[3] A. K. Ekert, Physical Review Letters 67, 661 (1991).
[4] A.-D. Zhu, Y. Xia, Q.-B. Fan, and S. Zhang, Physical Review A 73, 022338 (2006).
[5] K. Boström and T. Felbinger, Physical Review Letters 89, 187902 (2002).
[6] Q.-Y. Cai and B.-W. Li, Physical Review A 69, 054301 (2004).
[7] F.-G. Deng and G. L. Long, Physical Review A 69, 052319 (2004).
[8] K. Shimizu and N. Imoto, Physical Review A 60, 157 (1999).
[9] X.-H. Li, F.-G. Deng, C.-Y. Li, Y.-J. Liang, P. Zhou, and H.-Y. Zhou, J. Korean Phy. Soc. 49, 1354 (2006).
[10] D. Joy, S. P. Surendran, and M. Sabir, Quantum Information Processing 16, 157 (2017).
[11] A. Beige, B.-G. Englert, C. Kurtsiefer, and H. Weinfurter, Acta Physica Polonica Series a 101, 357 (2001).
[12] W. Huang, Q.-Y. Wen, B. Liu, F. Gao, and H. Chen,
International Journal of Theoretical Physics 51, 2787 (2012).

[13] D. Jiang, Y. Chen, X. Gu, L. Xie, and L. Chen, Scientific Reports 7 (2017), 10.1038/srep44934.

[14] W. Zhang, D.-S. Ding, Y.-B. Sheng, L. Zhou, B.-S. Shi, and G.-C. Guo, Physical Review Letters 118, 220501 (2017).

[15] A. Beige, B.-G. Englert, C. Kurtsiefer, and H. Weinfurter, Journal of Physics A: Mathematical and General 35, L407 (2002).

[16] W. Peterson and D. Brown, Proceedings of the IRE 49, 228 (1961).

[17] H. Delfs and H. Knebl, Introduction to cryptography: principles and applications, 2nd ed. (Springer, Berlin ; New York, 2007).

[18] N. Moldovyan, A. Levina, and S. Taranov, in 2017 20th Conference of Open Innovations Association (FRUCT) (IEEE, St-Petersburg, Russia, 2017) pp. 290–295.

[19] T. Elsayed, Manuscript submitted for publication (2019).

[20] J. M. Leinaas, J. Myrheim, and E. Ovrum, Physical Review A 74 (2006), 10.1103/PhysRevA.74.012313.

[21] The implementation of Peres–Horodecki criterion that was used is available at http://physics.technion.ac.il/stateseparator/index.html/.
FIG. 1. The preprocessing block diagram of a classical message before it is fed into a quantum encoder. A hash value (checksum) is added to the message before it is being encrypted with a random key. Random redundancy check bits are inserted into the encrypted message at random locations.
FIG. 2. (a, b) The circuit diagram of the quantum encoder and decoder for the DSQC protocol that does not use entanglement. Every bit is encoded by two qubits. One random qubit is encoded in the computational basis $\{|0\rangle, |1\rangle\}$ and the other one in the Hadamard basis $\{\frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)\}$. The receiver, on the other hand, measures the two qubits in either the computational basis or the Hadamard basis in a random manner. The random choices are determined by a random number generator (RNG).

(c, d) The circuit diagram of the quantum encoder and decoder for the DSQC protocol that uses entangled qubits. ‘1’ and ‘0’ are encoded by two qubits in the states $\frac{1}{2}(|00\rangle - |01\rangle - |10\rangle - |11\rangle)$ and $\frac{1}{2}(|00\rangle - |01\rangle + |10\rangle + |11\rangle)$ respectively. The first qubit is measured by the sender, while the second one is measured by the receiver in the Hadamard basis.