Quantum non-locality and information security

Muhammad Nadeem
Department of Basic Sciences,
School of Electrical Engineering and Computer Science
National University of Sciences and Technology (NUST)
H-12 Islamabad, Pakistan
muhammad.nadeem@seecs.edu.pk

We show that quantum non-locality, as discussed here, is sufficient to achieve unconditional information security without requiring advanced quantum technology, pre-shared secret keys or private quantum/classical channels between distant systems (users). Two-fold quantum non-local correlations imply two-way secret transmission in a single round with assurance of confidentiality, integrity and authenticity. Interestingly, the proposed scheme (quantum telephone or QPhone) provides resources for indefinite future secure communication and acts as *life-time* pad.

Information can be expressed in terms of physical systems (representations), processed through laws (rules) obeyed by these physical systems (representations) and is protected from unauthorized users through cryptographic techniques/algorithms. Objectives of these cryptographic techniques are to assure confidentiality, integrity, authenticity and availability of information to legitimate users.

These information security requirements are closely related with each other but each have well defined domain: Confidentiality assures that only a legitimate user can store, process, and transmit private information to a specific destination without disclosing to unauthorized users. Integrity assures that information can only be controlled by authorized users and processed in a specific manner and cannot be changed by unauthorized users. In other words, changes from malicious attacks or errors in functioning of systems should easily be detected. Authenticity verifies that information is valid and its originator is genuine. Finally, availability means systems timely response and information remains accessible to legitimate users.

Usually, cryptographic techniques need to handle following different situations regarding security concerns against malicious attacks: (C-1) Two-party communication where both parties are trusted and security is required against eavesdroppers. (C-2) Two-party communication where both parties are distrustful and security is concerned against these parties only such as oblivious transfer, two-party secure computation, coin tossing and bit commitment. (C-3) Multi-party communication where sender is individual but there are two (or more than two) parties at the receiving end. Sender is trusted but at least one out of two (or k out of n) receiver(s) is (are) not trusted such as secret sharing between two (or n) parties on the receiving end. (C-4) Multi-party communication where there is not complete trust between sender and receivers. That is, sender can deny from the message he/she has actually sent or one of the receivers can try to forge the original message. Security against such denial and forgery requires digital signatures.

Classical information theory relies on deterministic systems for encoding information and tries to achieve information security through following three main cryptographic techniques: (i) symmetric encryption, (ii) asymmetric encryption, and (iii) hashing along with message authentication code and digital signatures. However, widely used classical algorithms for distribution of symmetric keys secretly, generation of public-private key pairs and hashing are

only computationally secure – eavesdroppers with efficient technology (quantum computer) can easily break all these classical algorithms and hence spoil the security.

On the other hand, newly developed quantum information theory[1] encodes information over probabilistic microscopic systems called qubits; an atom, nuclear spins, or polarized photon. These encoded quantum systems, may be in superposition state represented by unit vectors in Hilbert space, are processed through unitary operators. This formulism of quantum information theory allows defining cryptographic tasks that are not possible in classical cryptography.

Quantum information theory gains this power in cryptography from laws/properties of quantum physics such as uncertainty, non-locality, interference, and no-cloning of unknown quantum states. For example, uncertainty principle allows two distant users to agree upon an unconditionally secure key[2]. Here no-cloning[3] and state reduction while measurement is performed prevents malicious attacks. Quantum non-locality, EPR type correlations[4], also offers secure QKD[5] where generalized Bell's theorem[6,7] is used to detect eavesdroppers. Using secret key obtained from QKD, a secret message of equal length can be transmitted securely over the classical channel. However, quantum cryptography based on QKD can only be used for one-way secret transmission and assures confidentiality but further requires key-based classical algorithms for ensuring integrity and authenticity.

We propose here a general quantum scheme for information security during the communication between two trusted users (C-1) based on quantum non-locality that implies secure and authenticated two-way secret transmission in a single round (QPhone). Two-fold quantum non-local correlations are used for assurance of confidentiality, integrity and authenticity while availability is achieved through repetitive measurements from both users. The proposed setup achieves these information security requirements without advanced quantum technology, prior secret key distribution and does not require private quantum/classical channels. All classical information can be communicated over public channels without compromising any of the security requirements. Interestingly, if no eavesdropping is detected, the scheme allows two-way secret transmission for indefinite future secure communication and acts as *life-time* pad.

Two-fold quantum non-local correlations

Two-fold non-local quantum correlations can be achieved as follows: Suppose Alice share EPR systems $H_\alpha \otimes H_\beta$ and $H_{\alpha'} \otimes H_\gamma$ with Bob and Charlie respectively. Both of these systems can be publically known. Now if Alice performs Bell state measurement (BSM)[8] $(B \otimes I)(H_\alpha \otimes H_{\alpha'}) \otimes (H_\beta \otimes H_\gamma)$, systems H_β and H_γ non-locally correlate with each other in one of the four possible EPR states corresponding to BSM result of Alice[9]. In second phase, if Bob teleportes[10] an unknown quantum state $|\varphi\rangle$ over swapped entangled system $(H_\beta \otimes H_\gamma)$, Charlie's half H_γ can be decoded to exact quantum state $|\varphi\rangle$ only if both Alice and Bob share their classical BSM results with Charlie. We would like to highlight here that for each value of Alice's BSM result, there will be a unique Bell system $H_\beta \otimes H_\gamma$ and hence unique Pauli encoding of quantum state $|\varphi\rangle$ corresponding to BSM result of Bob[11].

This simple multiplicity of quantum non-locality directly leads to unconditional information security and will be discussed in detail here. In a related work[11], we showed that combination of such two-fold non-local correlations with causality proves to be useful for important mistrustful cryptographic tasks (C-2) such as oblivious transfer, two-sided two-party secure computation, asynchronous ideal quantum coin tossing with zero bias, and

unconditionally secure bit commitment. In a related work, we have shown that multi-fold quantum non-local correlations are also useful for multi-party quantum secret sharing (C-3) and quantum signatures (C-4) which are more powerful than existing classical/quantum digital signature schemes.

Security criteria

The proposed scheme guarantees secure and authenticated two-way secret transmission in a single round under standard quantum cryptographic requirements[2,5,12]: eavesdroppers have efficient quantum technologies and are allowed to interact with quantum transmission and can monitor but cannot alter or suppress the classical communication.

That is, if Alice and Bob can establish publically known EPR pairs through classical communication not altered by eavesdroppers, then the proposed scheme allows them to send secret information to each other securely even in the presence of eavesdroppers/noise. Fortunately, maximally entangled pairs can be generated from Werner states or any supply of other entangled mixed states with entanglement purification procedure[13-15].

One-way secret transmission

We describe here one-way secret transmission from Bob to Alice first and later show that it can easily be generalized to two-way secret transmission between Alice and Bob in a single round by sharing one more EPR pair. Suppose Alice and Bob share a publically known quantum system $H_s = H_1 \otimes H_2 \otimes H_3$ where $H_i = H_\alpha \otimes H_\beta$ is a two-qubit EPR pair

$$\left|\alpha_a \beta_b\right\rangle = \frac{\left|0\right\rangle\left|\beta_b\right\rangle + (-1)^{\alpha_a}\left|1\right\rangle\left|1 \oplus \beta_b\right\rangle}{\sqrt{2}} \tag{1}$$

where $\alpha_a, \beta_b \in \{0,1\}$, $a, b \in \{1,2,3\}$ and $\oplus$ denotes addition with mod 2. Detailed one-way secret transmission is described below and shown in figure 1.

Phase-1: Secure distribution of EPR pairs

(1). Alice and Bob share three EPR pairs $\left|\alpha_a \beta_b\right\rangle$ where first qubit of each pair belongs to Alice while second to Bob. These pairs can be publically known.

(2). Alice (and Bob) performs BSM on qubits $\left|\alpha_2\right\rangle$ and $\left|\alpha_3\right\rangle$ ($\left|\beta_2\right\rangle$ and $\left|\beta_3\right\rangle$). This BSM results in two EPR pairs $\left|\alpha_2 \alpha_3\right\rangle$ and $\left|\beta_2 \beta_3\right\rangle$ in possession of Alice and Bob respectively. These swapped EPR pairs will be known only to Alice and Bob but unknown to eavesdroppers.

Phase-II: Direct encoding

(3). Now Alice performs BSM on qubits $\left|\alpha_1\right\rangle$ and $\left|\alpha_2\right\rangle$ and gets classical information $\alpha_1 \alpha_2 \in \{00,01,10,11\}$. This measurement projects the qubits $\left|\alpha_3\right\rangle$ and $\left|\beta_1\right\rangle$ into one of the four possible Bell states $\left|\alpha_3 \beta_1\right\rangle$. The swapped ERP pair will be known to Alice and can only be known to Bob if Alice reveals her BSM result $\alpha_1 \alpha_2$. However, even after public announcement of Alice's BSM result, eavesdroppers will remain ignorant about exact identity of $\left|\alpha_3 \beta_1\right\rangle$.

(4). Bob teleports his secret message $\left|\varphi_b\right\rangle \in \{0,1\}$ to Alice using $\left|\alpha_3 \beta_1\right\rangle$. If BSM result of Bob is $\beta\beta' \in \{00,01,10,11\}$ while teleporting the state, then Alice's half $\left|\alpha_3\right\rangle$ becomes one of the corresponding four possible states $\left|\psi_b\right\rangle = \sigma_z^l \sigma_x^m \left|\varphi_b\right\rangle$ ($l, m \in \{0,1\}$) totally random to Alice.

Phase-III: Secure decoding and authentication

(5). Alice measures qubit $|\alpha_3\rangle$ in the agreed basis and gets result ψ_b. Simultaneously, she sends result ψ_b and her BSM result $\alpha_1\alpha_2$ to Bob over public classical channels. Bob verifies the non-local correlations generated through entanglement swapping and teleportation. That is, if $|\alpha_3\beta_1\rangle$ and ψ_b are consistent with BSM results $\alpha_1\alpha_2$ and $\beta\beta'$ of Alice and Bob respectively, Bob verifies that transmission is secure against eavesdroppers/noise and announces $\beta\beta'$. Now Alice can extract encoded message $|\varphi_b\rangle$ from $|\psi_b\rangle = \sigma_z^l \sigma_x^m |\varphi_b\rangle$ securely with assurance of confidentiality, integrity and authenticity of secret information $|\varphi_b\rangle$.

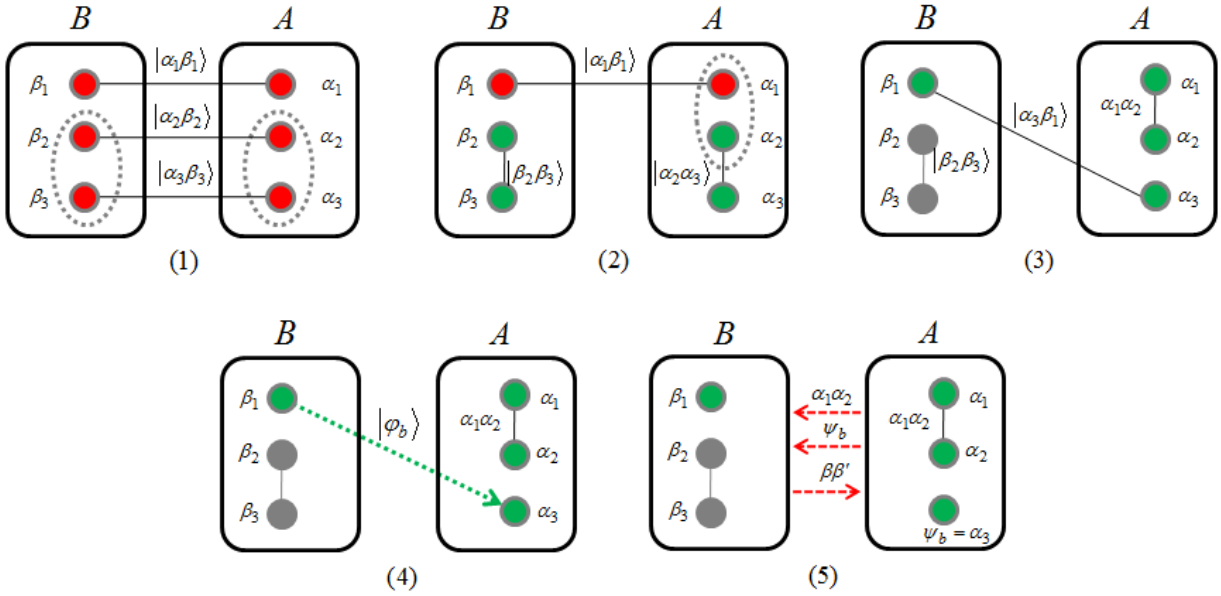

Figure 1: One-way secret transmission from Bob to Alice. Dotted arrow (green) represents teleportation while dashed arrows (red) show classical communication over public channels. Red color shows public information while green represents information kept by Alice and Bob secret.

Two-way secret transmission (QPhone)

Now if Alice and Bob start the scheme with four EPR pairs, the scheme allows both Alice and Bob for two-way secret and authenticated transmission simultaneously in a single round. That is, both Alice and Bob can send secret messages to each other simultaneously.

Suppose Alice and Bob share four EPR pairs $|\alpha_a\beta_b\rangle$ and Alice performs BSM on qubits $|\alpha_3\rangle$ and $|\alpha_4\rangle$ while Bob on $|\beta_3\rangle$ and $|\beta_4\rangle$ respectively. This BSM results in two EPR pairs $|\alpha_3\alpha_4\rangle$ and $|\beta_3\beta_4\rangle$ in possession of Alice and Bob respectively. In second phase, Alice performs BSM on qubits $|\alpha_1\rangle$ and $|\alpha_3\rangle$ and projects qubits $|\beta_1\rangle$ and $|\alpha_4\rangle$ into one of the four possible Bell states $|\alpha_4\beta_1\rangle$. Similarly Bob performs BSM on qubits $|\beta_2\rangle$ and $|\beta_3\rangle$ and projects the qubits $|\alpha_2\rangle$ and $|\beta_4\rangle$ into one of the four possible Bell states $|\alpha_2\beta_4\rangle$. Now both Alice and Bob can teleport their secret messages $|\varphi_a\rangle$ and $|\varphi_b\rangle$ to each other. Finally, they can decode and authenticate

secret transmissions by communicating their classical results over public channels. Detailed two-way secret transmission scheme is shown in figure 2.

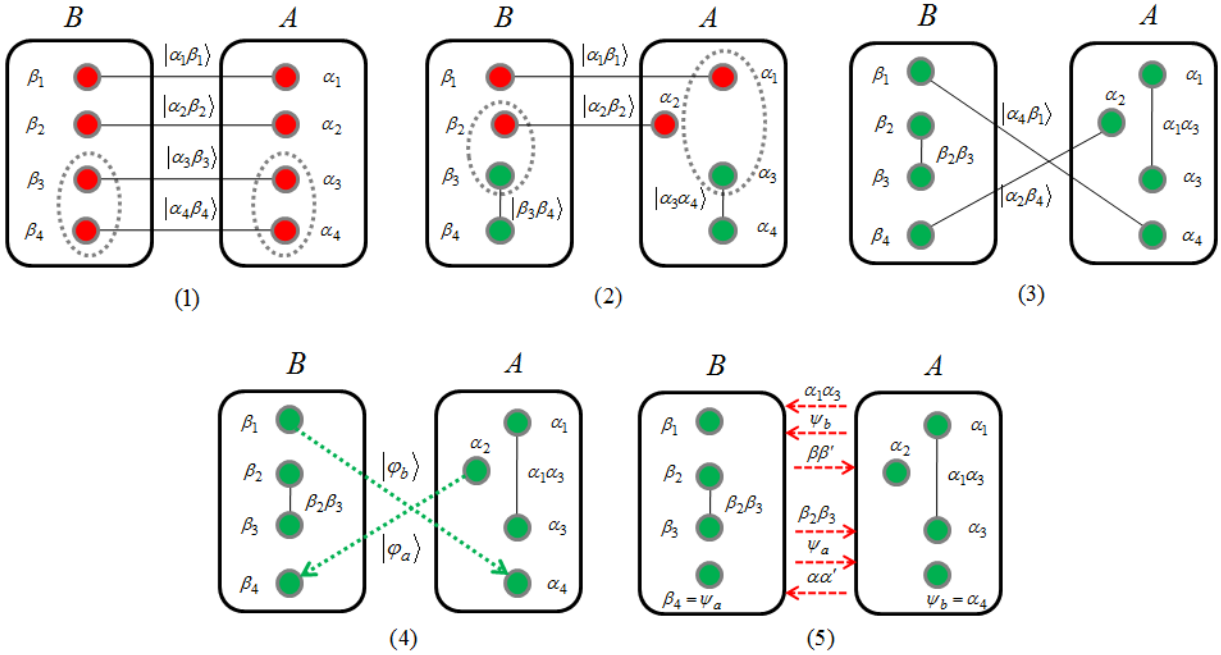

Figure 2: Two-way secret transmission from Alice to Bob and vice versa. Dotted arrow (green) represents teleportation while dashed arrows (red) show classical communication over public channels. Red color shows public information while green represents information kept by Alice and Bob secret.

Discussion

We proposed here a general quantum scheme based on two-fold quantum non-local correlations that assure confidentiality, integrity and authenticity of information transferred among trusted users. Repetitive measurements from both users and classical communication over public channels assure availability and result in QPhone; secure and authenticated two-way secret transmission in a single round. The proposed setup achieves these information security requirements without relying on advanced quantum technology, pre-shared secret keys or private quantum/classical channels between distant users.

Only requirement for security/availability of secret information against eavesdroppers/noise is unsuppressed classical communication between distant users over public channels. The proposed procedure then remains secure against passive monitoring of classical information as well as active quantum attacks. It does not use batches of encoded qubits and then statistical tests after measurements in agreed basis and hence does not allow eavesdroppers to successfully use quantum attacks such as entangling a quantum ancilla with the encrypted message and later performing a specific measurement on it according to public communication of legitimate users. However, if eavesdroppers can interrupt classical communication actively then distant users need to have some pre-agreed secret information or trusted source for secure distribution of EPR pairs $|\alpha_a\beta_b\rangle$.

Remarkably, even pre-sharing of secret information or use of trusted source for entanglement distribution is not as costly in our scheme as it is in other cryptographic schemes. The proposed setup allows distant users to communicate securely and indefinitely if first round is

successful; it allows distant users to generate secret and agreed entangled pairs for future secure transmission from previous communication. For example, Alice and Bob do not publically announce the identities of EPR pairs obtained from BSM in step 2; $|\alpha_2\alpha_3\rangle$ and $|\beta_2\beta_3\rangle$ in one-way and $|\alpha_3\alpha_4\rangle$ and $|\beta_3\beta_4\rangle$ in two-way secret transmission. These EPR states remain secret between them and if Alice (Bob) receives secret message $|\varphi_b\rangle$ ($|\varphi_a\rangle$) from Bob (Alice) successfully, they can store 2-bit strings $\alpha_a\beta_b$ as shared secret information and can start next round in future with corresponding EPR pairs. In conclusion, proposed procedure acts as *life-time* pad.

1. Wiesner, S. Conjugate coding. *Sigact News* **15**, 78 (1983)
2. Bennett, C. H. & Brassard, G. Quantum cryptography. *In Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing*, Bangalore, India, pp. 175-179 (Dec. 10-12,1984).
3. Wootters, W. & Zurek, W. A single quantum cannot be cloned. *Nature* **299**, 802-803; DOI:10.1038/299802a0 (1982).
4. Einstein, A., Podolsky, B. & Rosen, N. Can quantum-mechanical description of physical reality be considered complete? *Phys. Rev.* **47**, 777 (1935).
5. Ekert, A. Quantum Cryptography Based on Bell's Theorem. *Phys. Rev. Lett.* **67**, 661 (1991).
6. Bell, J. On the Einstein Podolsky Rosen paradox. *Physics* **1**, 195 (1965).
7. Clauser, J., Horne, M., Shimony, A. & Holt, R. Proposed Experiment to Test Local Hidden-Variable Theories. *Phys. Rev. Lett.* **23**, 880 (1969).
8. Braunstein, S., Mann, A. & Revzen, M. Maximal violation of Bell inequalities for mixed states. *Phys. Rev. Lett*. **68**, 3259 (1992).
9. Zukowski, M., Zeilinger, A., Horne, M. & Ekert, A. Event-ready-detectors'' Bell experiment via entanglement swapping. *Phys. Rev. Lett.* **71**, 4287 (1993).
10. Bennett, C., Brassard, G., Crepeau, C., Jozsa, R., Peres, A. & Wooters, W. Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. *Phys. Rev. Lett*. **70**, 1895 (1993).
11. Nadeem, M. Quantum non-locality, causality and mistrustful cryptography. *arXiv*: 1407.7025v5 (2014)
12. Bennett, C. Quantum cryptography using any two nonorthogonal states. *Phys. Rev. Lett*. **68**, 3121 (1992).
13. Bennett, C., Brassard, G., Popescu, S., Schumacher,B., Smolin, J. & Wooters, W. Purification of noisy entanglement and faithful teleportation via noisy channels *Phys. Rev. Lett.* **76**, 722 (1996).
14. Bennett, C., DiVincenzo, D., Smolin, J. & Wooters, W. *Phys. Rev. A* **54**, 3824 (1996).
15. Deutsch, D., Ekert, A., Jozsa, R., Macchiavello, C., S. Popescu, S. & Sanpera, A. Quantum privacy amplification and the security of quantum cryptography over noisy channels. *Phys. Rev. Lett*. **77**, 2818 (1996). Erratum: *Phys. Rev. Lett*. **80**, 2022 (1998).