Secure and authenticated quantum secret sharing

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

Noor Ul Ain  
Department of Computer Sciences,  
School of Electrical Engineering and Computer Science,  
National University of Sciences and Technology (NUST),  
H-12 Islamabad, Pakistan  
13msccsnaain@seecs.nust.edu.pk

We propose here a quantum secret sharing scheme that works for both quantum and classical secrets. The proposed scheme is based on both entanglement swapping and teleportation together. It allows sender to encrypt his/her secret and simultaneously distribute decryption information of the encrypted secret among distant parties where decryption shares are non-locally correlated with each other. Two-fold quantum non-local correlations, generated through entanglement swapping and then teleporting quantum states over swapped maximally entangled pairs, guarantee both authentication and secrecy of the secret from internal as well as external eavesdroppers. For classical secrets, we demonstrate a direct (2,2) quantum secret sharing scheme where neither pre-shared key nor physically secure quantum/classical channel are required. The same scheme turns out to be a (5,5) quantum secret sharing scheme for quantum secrets if sender and receivers have private quantum/classical channels among them.

Introduction

Secret sharing is a cryptographic procedure where a secret (or decryption function of secret) is divided among multiple parties such that each party gets a part of secret (or decryption function of secret) but cannot extract the secret on its own. However, the secret can only be reconstructed (extracted) when all the parties collaborate together and share their part. Such a secret sharing scheme is called \((n, n)\) threshold scheme. In general, the original secret can be reconstructed if and only if at least \(k \leq n\) parties collaborate called a \((k, n)\) secret sharing threshold scheme.

Secret sharing is an important cryptographic primitive that can be used as sub-protocol for implementing secure multiparty computation, multiparty key agreement, hardware security modules, PGP key recovery, and visual cryptography. The idea of classical secret sharing was given originally by Shamir and Blakely in 1979 [1,2] and was extended to the quantum regime by M. Hillery et al [3] in 1999. Quantum secret sharing scheme proposed by M. Hillery was based on three-particle GHZ states. Later on, Karlsson et al showed that quantum secret sharing protocol similar to that of M. Hillery can also be constructed by using two-particle quantum entangled states [4]. After generalization of secret sharing to quantum regime [3,4], a number of quantum secret sharing schemes are developed for both classical (bits) as well as quantum (qubits) secrets [5-27].

Here we show that, by using two-particle quantum entangled states, a secure and authenticated (2,2) quantum secret sharing can be constructed without having any pre-shared data or private quantum/classical channels between sender and receivers. The proposed scheme is based on two-fold quantum non-local correlations generated through fundamental and
important quantum information tasks namely entanglement swapping [28] and teleportation [29] together. By using at least two EPR pairs with receivers R₁ and R₂, two-fold quantum non-local correlations allow sender to encrypt his/her classical secret \(|\varphi\rangle\) (either \(|\varphi\rangle = |0\rangle\) or \(|\varphi\rangle = |1\rangle\)) and distribute non-locally correlated decryption information between receivers R₁ and R₂ such that either R₁ or R₂ cannot decrypt the secret alone but they can find original secret if and only if they meet and share distributed decryption information.

The proposed procedure for secret sharing guarantees secrecy from both internal (receivers R₁ and R₂) as well as external (third party) eavesdroppers. It allows sender as well as receivers to perform repetitive measurements in publically known basis and extract authentication token. Repetitive measurements allow both sender and receivers to store classical information and later extract encrypted secret after indefinite time. After verifying authentication tokens from both receivers with quantum non-local correlations, sender reveals his/her share of decryption information publically.

The proposed (2,2) secret sharing scheme for classical secret can be used as a (5,5) secret sharing scheme for quantum secrets. In that case, sender needs to have physically secure quantum/classical channels with receivers or they can establish secure channels through QKD or EPR based quantum channels.

Such a quantum procedure based on entanglement swapping and teleportation together can be used to achieve a number of cryptographic applications such as unconditionally secure bit commitment with arbitrarily long commitment time [30,31], two-sided two-party secure computation, asynchronous ideal coin tossing [32], and secure positioning [33-35].

### Teleportation and entanglement swapping

Suppose sender S and receiver R share one of the four EPR pairs

\[
\begin{align*}
|\Phi^+\rangle &= (|00\rangle + |11\rangle)/\sqrt{2} \\
|\Psi^+\rangle &= (|01\rangle + |10\rangle)/\sqrt{2} \\
|\Phi^-\rangle &= (|00\rangle - |11\rangle)/\sqrt{2} \\
|\Psi^-\rangle &= (|01\rangle - |10\rangle)/\sqrt{2}
\end{align*}
\]

and S wants to send an arbitrary quantum state \(|\varphi\rangle\) to R through teleportation [29]. He performs Bell state measurement (BSM) [36] on quantum state \(|\varphi\rangle\) and his half of EPR pair such that both quantum state and EPR pair collapsed and he gets classical 2-bit string ss’. On the other hand, entangled half in possession of R becomes \(|\varphi\rangle = \sigma_i |\varphi\rangle\) where teleportation encoding \(\sigma_i\) depends upon both classical string ss’ and identity of shared EPR pair. In other word, receiver R can decode quantum state \(|\varphi\rangle\) from \(|\varphi\rangle = \sigma_i |\varphi\rangle\) if and only if he knows both classical string ss’ and identity of shared EPR pair as shown in the table 1.

Entanglement swapping [28] is an interesting extension of teleportation [29], in fact, teleportation of entanglement, where two uncorrelated quantum systems gets entangled without having any interaction with each other. Let’s consider three distant parties S, R₁, and R₂ where R₁ shares EPR pairs \(|\sigma_i\rangle\) and \(|\sigma_j\rangle\) with S and R₂ respectively while S and R₂ are uncorrelated. Now if R₁ performs BSM on his/her halves, quantum systems in possession of S and R₂ gets
entangled into one of the four possible Bell states $\ket{sr_2}$. Exact identity if EPR pair $\ket{sr_2}$ swapped between S and R depends upon both initially shared EPR pairs $\ket{sr_1}$ as well as BSM result of $\ket{r_2}$. All possible transformations of initially shared quantum system $\ket{sr_1}$ to $\ket{r_2}$ are summarized in table 2.

| EPR   | $ss'$ | $|\varphi\rangle = \sigma_i|\varphi\rangle$ |
|-------|-------|----------------------------------------|
| $\Phi^+$ | 00 01 10 11 | $|\varphi\rangle$ $\sigma_x|\varphi\rangle$ $\sigma_z|\varphi\rangle$ $\sigma_x\sigma_z|\varphi\rangle$ |
| $\Psi^+$ | 00 01 10 11 | $\sigma_x|\varphi\rangle$ $|\varphi\rangle$ $\sigma_x\sigma_z|\varphi\rangle$ $\sigma_z|\varphi\rangle$ |
| $\Phi^-$ | 00 01 10 11 | $\sigma_z|\varphi\rangle$ $\sigma_x|\varphi\rangle$ $|\varphi\rangle$ $\sigma_x|\varphi\rangle$ |
| $\Psi^-$ | 00 01 10 11 | $\sigma_x\sigma_z|\varphi\rangle$ $\sigma_z|\varphi\rangle$ $\sigma_x|\varphi\rangle$ $|\varphi\rangle$ |

**Table 1:** Teleportation: If sender S and receiver R share entangled state $\ket{\Phi^-}$ and BSM result of S is $ss'=11$ then R will have state $|\varphi\rangle = \sigma_x|\varphi\rangle$ on his side.

| $\ket{sr_1}$ | $\ket{r_2}$ | $\ket{r_1}$ | $\ket{sr_2}$ |
|--------------|--------------|--------------|--------------|
| $\ket{\Phi^+}$ | $\ket{\Phi^+}$ | $\ket{\Phi^-}$ | $\ket{\Phi^-}$ |
| $\ket{\Phi^+}$ | $\ket{\Psi^+}$ | $\ket{\Phi^-}$ | $\ket{\Psi^-}$ |
| $\ket{\Phi^-}$ | $\ket{\Psi^+}$ | $\ket{\Phi^+}$ | $\ket{\Psi^-}$ |
| $\ket{\Phi^-}$ | $\ket{\Psi^-}$ | $\ket{\Phi^-}$ | $\ket{\Psi^+}$ |

**Table 2:** Entanglement swapping: After BSM of $\ket{r_1}$, initially shared quantum system $\ket{sr_1} \ket{r_2} = \ket{\Phi^+} \ket{\Psi^-}$, could be transformed to one of the four possibilities, $\ket{sr_1} \ket{r_2} = \ket{\Phi^+} \ket{\Psi^-}$, $\ket{sr_1} \ket{r_2} = \ket{\Phi^-} \ket{\Phi^-}$, or $\ket{sr_1} \ket{r_2} = \ket{\Psi^-} \ket{\Phi^+}$.

**Two-fold quantum non-local correlations and information splitting**

Here we show that when entanglement swapping and teleportation, as discussed above, are performed together on a single quantum system consisting of at least two EPR pairs, it results in perfect encryption of a secret (quantum/classical) with non-locally correlated classical shares of decryption function. Both these cryptographic requirements, perfect encryption along with set of decryption pieces, directly lead to secure and authenticated quantum secret sharing schemes.

Suppose sender S secretly prepares two maximally entangled quantum systems $H_{r_1} = H_{r_1} \otimes H_{r_1}$ and $H_{r_2} = H_{r_2} \otimes H_{r_2}$ in one of the Bell basis $\ket{\Phi^+}$, $\ket{\Psi^+}$, $\ket{\Phi^-}$, or $\ket{\Psi^-}$ corresponding to 2-bit strings $r_{r_1} = 0$, $r_{r_1} = 01$, $r_{r_1} = 10$, or $r_{r_1} = 11$ respectively. He then sends second half of each system to receiver $R_1$ while first half of second system to receiver $R_2$. As a
result, sender S shares quantum system $H_{\eta_1} \otimes H_{\eta_2} \otimes H_{\eta_2'} \otimes H_{r_2}$ with two receivers R$_1$ and R$_2$ where $H_{\eta_1}$ is kept by S while $H_{\eta_1} \otimes H_{\eta_2}$ and $H_{r_2}$ are in possession of R$_1$ and R$_2$ respectively.

If R$_1$ applies Bell operator [36] on $H_{\eta_1'}$ and $H_{\eta_2'}$ while S applies Bell operator on his secret $H$ and retained half $H_{\eta_1'}$, then R$_2$’s half $H_{r_2}$ becomes $H_{r_2} = U(H)$ where $U$ is a 2×2 unitary operator. The unitary encoding $U$ is non-locally correlated with classical Bell state measurement (BSM) results $R_1R'_1 \in \{00,01,10,11\}$ and $ss' \in \{00,01,10,11\}$ of receiver R$_1$ and sender S respectively as well as identity of initially shared systems $r_1r'_1 \in \{00,01,10,11\}$ and $r_2r'_2 \in \{00,01,10,11\}$.

In other words, decoding information of secret $H$ is divided into five pieces; four equal shares of classical 2-bit strings $r_1r'_1$, $r_2r'_2$, $R_1R'_1$ and $ss'$, and one encrypted secret $H_{r_2} = U(H)$. We would like to highlight here that for each value of R$_1$’s BSM result $R_1R'_1$ obtained through Bell measurement on $H_{\eta_1'} \otimes H_{\eta_2'}$, there will be a unique Bell system $H_{\eta_1} \otimes H_{r_2}$ swapped between S and R$_2$ and hence unique teleportation encoding of quantum system $H$ corresponding to BSM result of Bob. As a result, secret $H$ can be decoded from $H_{r_2} = U(H)$ if and only if someone has four shares of decrypting information $r_1r'_1$, $r_2r'_2$, $R_1R'_1$ and $ss'$ at same location [18].

Quantum secret sharing - classical information

Let’s consider first a more general situation where sender S and two receivers R$_1$ and R$_2$ are distant parties and they have no pre-shared secret data among them. Our scheme guarantees secure and authenticated sharing of classical secret information between two receivers under standard quantum cryptographic requirements [37-39]: (i) Quantum transmissions can be actively intercepted. (ii) Classical channels can be monitored passively. (iii) However, classical communication cannot be altered or suppressed. Detailed (2,2) quantum secret sharing scheme for classical information is described below.

**Authentication tokens:** Sender S shares two publically known EPR pairs with each of receivers R$_1$ and R$_2$, say $|\Phi^+\rangle$ and $|\Phi^-\rangle$ with receiver R$_1$ while $|\Psi^+\rangle$ and $|\Psi^-\rangle$ with receiver R$_2$. Both R$_1$ and R$_2$ perform BSM on their halves and keep their respective BSM results $r_1r'_1$ and $r_2r'_2$ secret from each other. However, their BSM results are known to sender S; S stores 2-bit strings $\eta_1r'_1$ and $r_2r'_2$ corresponding to his BSM on retained pairs.

**Information splitting between R$_1$ and R$_2$:** In the second round, S prepares two EPR pairs $H_{\eta_1r'_1} = H_{\eta_1} \otimes H_{r'_1}$ and $H_{r_2r'_2} = H_{r_2} \otimes H_{r'_2}$ corresponding to BSM results of R$_1$ and R$_2$ respectively. He then sends $H_{\eta_1'}$ and $H_{r_2'}$ to receiver R$_1$ while $H_{r_2}$ to receiver R$_2$. Receiver R$_1$ performs BSM on $H_{\eta_1'}$ and $H_{r_2'}$ and gets classical 2-bit string $R_1R'_1$ while sender S and receiver R$_2$ shares entangled system $H_{\eta_1} \otimes H_{r_2}$. The sender S teleports his secret $|\varphi\rangle \in \{0,1\}$ to R$_2$ over EPR channel $H_{\eta_1} \otimes H_{r_2}$ and keeps his BSM result $ss' \in \{00,01,10,11\}$ secret. R$_2$ measures his half, that has been transformed to $|\varphi'\rangle = \sigma_i|\varphi\rangle$ now where $\sigma_i$ is teleportation encoding, and gets an arbitrary outcome $\varphi' \in \{0,1\}$.

**Authentication:** R$_1$ bit-wise XOR his BSM results $\eta_1r'_1$ and $R_1R'_1$ and sends $(\eta \oplus R_1)(\eta'_1 \oplus R'_1)$ to S over classical channel. Similarly, R$_2$ XOR measurement outcome $\varphi' \in \{0,1\}$ with $r_2 \oplus r'_2$ and
The sender S extracts $R_t R'_t$ through bit-wise XOR of $(r_t \oplus R_t)(r'_t \oplus R'_t)$ and $r_t$ while $\varphi'$ through XOR of $\varphi' \oplus r_2 \oplus r'_2$ and $r_2 \oplus r'_2$. If sender S finds $R_t R'_t$ and $\varphi'$ consistent with his secret $|\varphi\rangle$, he sends his BSM result $ss'$ to both $R_1$ and $R_2$ over public channels.

**Combining secret shares:** Receivers $R_1$ and $R_2$ can extract encoded message $|\varphi\rangle$ from $|\varphi'\rangle = \sigma_i |\varphi\rangle$ only if they meet and share their secrets: $r_t$ and $R_t R'_t$ kept by $R_1$ while $\varphi'$ and $r'_2$ kept by $R_2$ respectively.

**Quantum secret sharing - quantum information**

Now let’s consider sender S has five distant agents $R_1, R_2, ..., R_5$ such that sender S can securely communicate both quantum and classical information with his agents; either they have physically secure quantum/classical channels between them or they can establish secure quantum channel through QKD or EPR based quantum channels. In this situation, our proposed (2,2) quantum secret sharing scheme can be used as (5,5) quantum secret sharing scheme for quantum information $|\varphi\rangle = \alpha |0\rangle + \beta |1\rangle$ without requiring authentication.

**Information splitting:** S prepares two EPR pairs $H_{s_1 s'_1} = H_{s_1} \otimes H_{s'_1}$ and $H_{s_2 s'_2} = H_{s_2} \otimes H_{s'_2}$ and sends $H_{s_1}$ and $H_{s_2}$ to receiver $R_1$ while $H_{s'_2}$ to receiver $R_2$. Simultaneously, he sends 2-bit strings $s_1 s'_1$ and $s_2 s'_2$ to receivers $R_3$ and $R_4$ respectively. Receiver $R_1$ performs BSM on $H_{s_1}$ and $H_{s_2}$ and gets classical 2-bit string $R_t R'_t$ while sender S and receiver R$_2$ shares entangled system $H_{s_1} \otimes H_{s_2}$. The sender S teleports his secret $|\varphi\rangle = \alpha |0\rangle + \beta |1\rangle$ to $R_2$ and sends his BSM result $ss' \in \{00, 01, 10, 11\}$ to receiver $R_5$. At the end of this phase, $R_5$’s half has been transformed to $|\varphi'\rangle = \sigma_i |\varphi\rangle$ where $\sigma_i$ is teleportation encoding non-locally correlated with four equal shares of classical information $s_1 s'_1$, $s_2 s'_2$, $ss'$, and $R_t R'_t$.

**Decoding secret:** Receivers $R_1, R_2, ..., R_5$ can extract encoded message $|\varphi\rangle$ from $|\varphi'\rangle = \sigma_i |\varphi\rangle$ only if they meet and share their secrets $R_t R'_t$, $|\varphi'\rangle = \sigma_i |\varphi\rangle$, $s_1 s'_1$, $s_2 s'_2$ and $ss'$ respectively.

**Discussion**

We proposed here a quantum secret sharing scheme based on two-fold quantum non-local correlations that assure authentication and secrecy of secret from internal as well as external eavesdropping simultaneously. The proposed quantum secret sharing scheme can be used as (2,2) threshold scheme for classical secret where both authenticity and secrecy is guaranteed without relying on advanced quantum technology, pre-shared secret keys or private quantum/classical channels between distant users. Repetitive measurements and classical communication over public channels assures availability of secret information and result in secure and authenticated quantum secret sharing scheme. Only requirement for security/availability of secret information against eavesdroppers/noise is unsuppressed classical communication over public channels between distant users. 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 key or trusted source for secure distribution of EPR pairs.

Finally, our proposed (2,2) quantum secret sharing scheme for classical secrets can be used as (5,5) quantum secret sharing scheme for quantum secret (qubit). For (5,5) threshold scheme, sender needs to have either physically secure quantum/classical channels with the receivers or they can establish secure quantum channel through QKD or EPR based quantum channels. Since quantum information, in the form of an arbitrary qubit $|\psi\rangle = \alpha |0\rangle + \beta |1\rangle$, is destroyed after measurement in computational basis, a similar approach for authentication as discussed for classical secret is not possible.

References:
1. Shamir, A.: How to share a secret. Commun. ACM 22(11), 612–613 (1979)
2. Blakley, G.R.: Safeguarding cryptographic keys. In: Proceedings of National Computer Conference, vol. 48, pp. 313–317. AFIP-PS Press, Montvale, NJ (1979)
3. Hillery, M., Buzek, V., Berthiaume, A.: Quantum secret sharing. Phys. Rev. A. 59(3), 1829–1834 (1999)
4. Karlsson, A., Koashi, M., Imoto, N.: Quantum entanglement for secret sharing and secret splitting. Phys. Rev. A. 59, 162 (1999).
5. Cleve, R., Gottesman, D., Lo, H.K.: How to share a quantum secret. Phys. Rev. Lett. 83(3), 648–651 (1999)
6. Gottesman, D.: Theory of quantum secret sharing. Phys. Rev. A. 61, 042311–042318 (2000)
7. Bandyopadhyay, S.: Teleportation and secret sharing with pure entangled states. Phys. Rev. A. 62, 012308 (2000).
8. Tittel, W., Zbinden, H., Gisin, N.: Experimental demonstration of quantum secret sharing. Phys. Rev. A 63, 042301 (2001).
9. Anderson, C.A.N., Joern, M.Q., Hideki, I.: Improving quantum secret sharing schemes. Phys. Rev. A. 64, 042311–042315 (2001)
10. Karimipour, V., Bahraminasab, A.: Entanglement swapping of generalized cat states and secret sharing. Phys. Rev. A 65, 042320 (2002).
11. Chau, H. F.: Practical scheme to share a secret key through a quantum channel with a 27.6% bit error rate. Phys. Rev. A. 66, 060302 (2002).
12. Bagherinezhad, S., Karimipour, V.: Quantum secret sharing based on reusable Greenberger-Horne-Zeilinger states as secure carriers. Phys. Rev. A. 67, 044302 (2003).
13. Hsu, L. Y.: Quantum secret-sharing protocol based on Grover’s algorithm. Phys. Rev. A. 68, 022306 (2003).
14. Lance, A. M., Symul, T., Bowen, W. P., Sanders, B. C., Lam, P. K.: Tripartite Quantum State Sharing. Phys. Rev. Lett. 92, 177903 (2004).
15. Xiao, L., Long, G.L., Deng, F.G., Pan, J.W.: Efficient multiparty quantum-secret-sharing schemes. Phys.Rev.A.69, 052307 (2004)
16. Zhang, Z.J., Man, Z.X.: Multiparty quantum secret sharing of classical messages based on entanglement swapping. Phys. Rev. A. 72, 022303–022306 (2005)
17. Zhang, Z.J., Li, Y., Man, Z.X.: Multiparty quantum secret sharing. Phys. Rev. A. 71, 044301–044306 (2005)
18. Zhang, Z.J.: Multiparty quantum secret sharing scheme of classical messages by swapping qudit-state entanglement. Int. J. Mod. Phys. C. 18, 1885–1901 (2007)
19. Lin, Q., Chan, W.H., Long, D.Y.: Semiquantum secret sharing using entangled states. Phys.
20. Gheorghiu, V.: Generalized semiquantum secret sharing schemes. Phys. Rev. A. 85, 052309–052319 (2012)
21. Yang, Y.G., Jia, X., Wang, H.Y., Zhang, H.: Verifiable quantum (k, n) threshold secret sharing. Quantum Inf. Process. 11, 1619–1625 (2012)
22. Nie, Y.Y., Li, Y.H., Wang, Z.S.: Semi-quantum information splitting using GHZ-type states. Quantum Inf. Process. 12, 437–448 (2013)
23. Rupert, U., Richard, H.: Quantum information: Sharing quantum secrets. Nature. 501, 37 (2013)
24. Lin, J., Hwang, T.: New circular quantum secret sharing for remote agents. Quantum Inf. Process. 12, 685–697 (2013)
25. Dehkordi, M.H., Fattahi, E.: Threshold quantum secret sharing between multiparty and multiparty using Greenberger-Horne-Zeilinger. Quantum Inf. Process. 12, 1299–1306 (2013)
26. Gao, G.: Secure multiparty quantum secret sharing with the collective eavesdropping-check character. Quantum Inf. Process. 12, 55–68 (2013)
27. Lai, H., Xiao, J., Orgun, M. A., Xue, L., Pieprzyk, J.: Quantum direct secret sharing with efficient eavesdropping-check and authentication based on distributed fountain codes. Quantum Inf. Process. 13, 895–907 (2014)
28. Braunstein, S., Mann, A., Revzen, M.: Maximal violation of Bell inequalities for mixed states. Phys. Rev. Lett. 68, 3259 (1992).
29. 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).
30. Nadeem, M.: Delayed choice relativistic quantum bit commitment with arbitrarily long commitment time. arXiv:1504.03316 (2015).
31. Nadeem, M.: Unconditionally secure commitment in position-based quantum cryptography. Sci. Rep. 4, 6774; DOI:10.1038/srep06774 (2014).
32. Nadeem, M.: Quantum non-locality, causality and mistrustful cryptography. arXiv:1407.7025 (2014).
33. Nadeem, M.: The causal structure of Minkowski space time - possibilities and impossibilities of secure positioning. arXiv: 1505.01839 (2015).
34. Nadeem, M.: Secure positioning and non-local correlations. arXiv:1406.3013 (2014).
35. Nadeem, M.: Position-based quantum cryptography over untrusted networks. Laser Phys. 24, 085202 (2014).
36. Zukowski, M., Zeilinger, A., Horne, M., Ekert, A.: Event-ready-detectors” Bell experiment via entanglement swapping. Phys. Rev. Lett. 71, 4287 (1993).
37. 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).
38. Ekert, A.: Quantum Cryptography Based on Bell's Theorem. Phys. Rev. Lett. 67, 661 (1991).
39. Bennett, C.: Quantum cryptography using any two nonorthogonal states. Phys. Rev. Lett. 68, 3121 (1992).