# Standard quantum bit commitment – an indefinite commitment time

*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*

Currently, it is believed in the literature that unconditionally secure bit commitment is impossible in non-relativistic quantum cryptography while only a weaker notion of bit commitment with finite commitment time is achievable in relativistic quantum setting. Moreover, relativistic classical bit commitment protocols allow arbitrary long commitment time but such protocols are not practically feasible; either because of multiple rounds of communication that result in exponential increase in communication complexity or due to asymptotic nature of security argument. The impossibility of practically feasible standard bit commitment leaves an obvious skepticism on the completeness of Hilbert space quantum cryptography and its claims of unconditional security. Contrary to the previously proposed results, we demonstrate here that an information-theoretic standard bit commitment scheme can be devised by using rules of purely non-relativistic quantum mechanics only; neither additional resources from theory of relativity nor multiple rounds of communications are required. The proposed bit commitment scheme can be applied efficiently with existing quantum technologies without long term quantum memory; quantum entanglement is required only for time $t+\delta$ where $t$ is the communication time between the committer and receiver while $\delta << t$ is the processing time at laboratory.

Bit commitment is one of the most important cryptographic primitive which has a number of applications in modern cryptography, communication, or distributed computing in general. For example, bit commitment is an essential building block for implementing a wide range of other tasks such as zero-knowledge proofs, coin tossing[1], digital signature[2], oblivious transfer[3], and two-party secure computation[4,5].

A bit commitment is a task between two mistrustful parties, a committer and a receiver. In general, committer commits to a specific bit by giving some information to the receiver and then unveils his/her commitment at some time later. Standard bit commitment is said to be information-theoretically secure if it fulfils following three security requirements: (i) Hiding: receiver should not be able to extract the committed bit value during the scheme. (ii) Binding: when committer reveals, it must be possible for receiver to know the genuine bit value with absolute guarantee while committer should not be able to reveal a bit different from the committed one. (iii) Indefinite commitment time: the scheme should sustain information-theoretic security for arbitrarily long time after commitment made by committer.

In non-relativistic classical cryptography, secure bit commitment scheme based on unproven computational hardness is impossible against quantum technologies[6]. However, standard bit commitment is possible in relativistic classical cryptography[7,8] with assurance of hiding, binding, and indefinite commitment time. Unfortunately, such relativistic classical protocols are not practically feasible either because of multiple rounds with exponential increase in communication[7] or due to asymptotic nature of security argument[8]. Recently, Lunghi *et al* also proposed a relativistic classical multi-round bit commitment scheme[9] with assurance of both

hiding and binding and commitment time longer than communication time between the locations of the agents. However, maximum commitment time allowed by their scheme is 212ms only.

On the other hand, in non-relativistic quantum cryptography, currently it is believed in the literature that secure bit commitment is impossible against Mayers and Lo-Chau quantum attacks[10-13] if committer and receiver do not pre-share any data. However, in relativistic quantum cryptographic settings, a secure but weaker notion of bit commitment protocols [14-18] have been presented with commitment time equivalent to the communication time between committer and one of the receiver's agents. Moreover, relativistic quantum bit commitment protocol[15] has been experimentally demonstrated, using quantum communication and special relativity, with commitment times of 15ms[19] and 30μs[20], respectively.

Impossibility of standard bit commitment, with arbitrarily long commitment time, leaves an obvious question on the completeness of quantum information theory; Can quantum mechanics allow same standards for bit commitment while relying on Hilbert space formalism only as classical cryptography does with computational hardness or exponentially rise in communication complexity? Here we demonstrate that methods of purely non-relativistic quantum mechanics, EPR type quantum correlations[21] in the form of teleportation[22-24], are sufficient to guarantee unconditionally secure standard bit commitment. First we propose a non-relativistic quantum bit commitment protocol and then show that it assures hiding, binding and arbitrarily long commitment time without requiring extra powers from theory of relativity as relativistic quantum bit commitment protocols[14-18] do or multiple rounds of communications as relativistic classical bit commitment protocols[7-9] require. Proposed scheme supersedes our earlier bit commitment scheme where commitment time was equivalent to the communication time between committer and one of the receiver's agents[18].

Our proposed scheme is a two-round bit commitment scheme where committer commits in the first round and then confirms his/her commitment in the second round. The scheme offers indefinite commitment time by allowing receiver to extract non-locally correlated measurement outcomes during the scheme which can be stored for arbitrarily long time. As a result, the bit commitment scheme can be applied efficiently with existing quantum technologies without long term quantum memory; committer and receiver have no pre-shared quantum/classical data and quantum entanglement is required only for time $t+\delta$ where $t$ is the communication time between the committer and receiver while $\delta << t$ is the processing time at laboratory.

However, apart from proposed standard bit commitment in this paper and possibilities of other unconditionally secure cryptographic tasks in purely Hilbert space quantum formalism[25-27], extra bounds from theory of relativity can be useful for multi-party tasks[28,29] and position-based quantum cryptography[30-39].

**Standard quantum bit commitment scheme**

Suppose committer Bob secretly prepares and shares an EPR pair $|\Phi_{\alpha\beta}\rangle \in H_\alpha \otimes H_\beta$ with receiver Alice where $H_{\alpha\beta} = H_\alpha \otimes H_\beta$ is four dimensional Hilbert space spanned by Bell basis $|\Phi_{\alpha\beta}\rangle \in \{|\Phi_{00}\rangle, |\Phi_{01}\rangle, |\Phi_{10}\rangle, |\Phi_{11}\rangle\}$ . Here $\alpha, \beta \in \{0,1\}$ and we write four Bell states as $|\Phi_{\alpha 0}\rangle = (|00\rangle \pm |11\rangle)/\sqrt{2}$ and $|\Phi_{\alpha 1}\rangle = (|01\rangle \pm |10\rangle)/\sqrt{2}$ . In other words, Bell states $|\Phi_{\alpha 0}\rangle$ correspond to classical bit $\beta = 0$ while those of $|\Phi_{\alpha 1}\rangle$ correspond to classical bit $\beta = 1$. That is, Bob commits him to the bit $\beta = 0$ or $\beta = 1$ by sharing EPR pair $|\Phi_{\alpha 0}\rangle$ or $|\Phi_{\alpha 1}\rangle$ with Alice.

At some later time that comes from the scheme, Bob applies unitary transformations $\sigma_z^{\alpha}\sigma_x^{\beta}$ on his retained qubit and confirms his commitment by sending retained qubit to Alice. Detailed protocol is outlined below:

1. *Pre-commitment:* Bob commits him to a bit $\beta \in \{0,1\}$ by sending entangled half of his secret EPR pair $\left|\Phi_{\alpha\beta}\right\rangle \in H_{\alpha} \otimes H_{\beta}$ to Alice. Alice prepares her secret EPR pair $\left|\Phi_{\alpha'\beta'}\right\rangle \in H_{\alpha'} \otimes H_{\beta'}$, applies Bell operator[24] on $H_{\alpha} \otimes H_{\alpha'}$, and stores classical result $a_1 a_2$. Simultaneously, Alice applies Bell operator on $H_0 \otimes H_{\beta'}$, here $\left|\psi\right\rangle \in H_0$ is her secret single qubit system, and stores another classical result $a_1' a_2'$.

2. *Confirmation:* Bob applies unitary operator $\sigma_z^{\alpha}\sigma_x^{\beta}$ on her retained half, now transformed to $\left|\psi'\right\rangle = \sigma^{\tau}\left|\psi\right\rangle$, and confirms his commitment by sending state $\left|\psi'\right\rangle = \sigma_z^{\alpha}\sigma_x^{\beta}\sigma^{\tau}\left|\psi\right\rangle$ back to Alice. Alice measures $\left|\psi'\right\rangle$, measurement basis are known only to her, and stores classical outcome.

3. *Opening:* After arbitrarily long commitment time, Bob reveals his commitment by announcing two classical bits $\alpha\beta$. Alice verifies whether Bob's announcement is consistent with non-locally correlated shares $a_1 a_2$, $a_1' a_2'$ and hence exact teleportation encoding $\sigma^{\tau}$ or not. If quantum non-local correlations are satisfied, Alice validates commitment genuine otherwise aborts.

**Security analysis**

The proposed scheme attains unconditional security through combination of quantum non-local correlations generated by repetitive action of Bell operators by Alice. In the pre-commitment phase, distributed quantum system can be expressed as

$$\left|\Phi_{\alpha\beta}\right\rangle \otimes \left|\Phi_{\alpha'\beta'}\right\rangle = \frac{1}{2}\sum_{i=1}^{4}\left|\Phi_{\alpha\alpha'}\right\rangle_i \otimes \left|\Phi_{\beta\beta'}\right\rangle_i \tag{1}$$

where $\left|\Phi_{\alpha\alpha'}\right\rangle$, and $\left|\Phi_{\beta\beta'}\right\rangle$ are local unitary equivalent to Bell basis depending on $\left|\Phi_{\alpha\beta}\right\rangle \otimes \left|\Phi_{\alpha'\beta'}\right\rangle$. Bell operator by Alice on $\left|\Phi_{\alpha\alpha'}\right\rangle$, shares an EPR channel $\left|\Phi_{\beta\beta'}\right\rangle$ between Alice and Bob whose exact identity remains unknown to both parties. Now the shared system among Alice and Bob reduces to and can be expressed as

$$\left|\psi\right\rangle \otimes \left|\Phi_{\beta\beta'}\right\rangle = \frac{1}{2}\sum_{i=1}^{4}\left|\Phi_{\alpha''\beta''}\right\rangle_i \otimes \sigma_i^{\tau}\left|\psi\right\rangle \tag{2}$$

where $\left|\Phi_{\alpha''\beta''}\right\rangle$ is local unitary equivalent to Bell basis depending on $\left|\Phi_{\beta\beta'}\right\rangle$. After Bell operator on $\left|\Phi_{\alpha''\beta''}\right\rangle$ again, Alice gets another classical 2-bit string $a_1' a_2'$ while Bob's half transforms to $\left|\psi'\right\rangle = \sigma^{\tau}\left|\psi\right\rangle$. Here Pauli encoding $\sigma^{\tau}$ is non-locally correlated with classical strings $a_1 a_2$ and $a_1' a_2'$ in possession of Alice as well as initial EPR system $\left|\Phi_{\alpha\beta}\right\rangle \otimes \left|\Phi_{\alpha'\beta'}\right\rangle$. We show here that hiding is guaranteed to Bob by following theorem 1 while binding is assured by Alice through theorem 2 and 3 respectively.

**Hiding:** Suppose Alice tries to cheat by exploiting Mayers and Lo-Chau quantum attacks[10-13] and delays her actions until Bob confirms his commitment. In that case, Bob will be sending

$\sigma_z^\alpha \sigma_x^\beta \left|\Phi_{\alpha\beta}\right\rangle$ to Alice straightforward. Can Alice find exact identity of $\beta \in \{0,1\}$ prior to Bob's opening? Interestingly answer is No by following theorem 1.

**Theorem 1:** *Suppose two distant parties Alice and Bob share a bipartite quantum system* $\left|\Phi_{\alpha\beta}\right\rangle \in H_A \otimes H_B$ *;* $\alpha\beta \in \{0,1\}$ *whose exact identity is known only to Bob. If Bob applies Pauli encoding* $\sigma_z^\alpha \sigma_x^\beta \in \{I, \sigma_x, \sigma_z, \sigma_x\sigma_z\}$ *on retained half* $H_B$ *and sends to Alice, the set* $\{\sigma_z^\alpha \sigma_x^\beta, \left|\Phi_{\alpha\beta}\right\rangle\}$ *remains arbitrary to Alice unless Bob reveals identity of* $\alpha\beta$.

*Proof:* Both Bell states $\left|\Phi_{\alpha\beta}\right\rangle \in \{\left|\Phi_{00}\right\rangle, \left|\Phi_{01}\right\rangle, \left|\Phi_{10}\right\rangle, \left|\Phi_{11}\right\rangle\}$ and Pauli transformations $\sigma_z^\alpha \sigma_x^\beta \in \{I, \sigma_x, \sigma_z, \sigma_x\sigma_z\}$ form complete orthonormal basis set for Hilbert space $H_A \otimes H_B$ and some canonical inner product space with inner product $Tr(\sigma_i \sigma_j^\dagger)$ respectively. If one-to-one mapping of these two sets is followed, the transformation $\sigma_z^\alpha \sigma_x^\beta \left|\Phi_{\alpha\beta}\right\rangle$ always maps to a unique Bell state $\left|\Phi_{00}\right\rangle$;

$$\sigma_z^\alpha \sigma_x^\beta \left|\Phi_{\alpha\beta}\right\rangle = \left|\Phi_{00}\right\rangle \tag{3}$$

That is, regardless of the initially shared Bell state $\left|\Phi_{\alpha\beta}\right\rangle$ or committed bit $\beta$, Bell state measurement outcome on Alice's site is always $\left|\Phi_{00}\right\rangle$. Hence, the exact identity of $\left|\Phi_{\alpha\beta}\right\rangle$ can only be known to Alice if and only if Bob reveals identity of $\alpha\beta$.

**Binding:** Can Bob change his commitment after confirmation of his commitment? No. We would like to highlight here that even though Bob shares an EPR pair $\left|\Phi_{\alpha\beta}\right\rangle$ with Alice to make his initial commitment, his commitment gets mature only when Bob replies $\left|\psi'\right\rangle = \sigma_z^\alpha \sigma_x^\beta \sigma^\tau \left|\psi\right\rangle$; Alice teleports $\left|\psi\right\rangle$ to Bob, Bob applies $\sigma_z^\alpha \sigma_x^\beta$ on his retained half and returns to Alice. That is, Bob have a choice and can change his commitment (EPR pair) during the time laps of pre-commitment phase by applying specific Pauli transformations on retained half and it cannot be considered as successful cheating. However, after confirmation by returning $\left|\psi'\right\rangle = \sigma_z^\alpha \sigma_x^\beta \sigma^\tau \left|\psi\right\rangle$ to Alice, it is impossible for Bob to alter her commitment by following theorems 2 and 3.

**Theorem 2:** *Suppose two distant parties Alice and Bob secretly prepare bipartite quantum systems* $H_{A',B'} = H_{A'} \otimes H_{B'}$ *and* $H_{A,B} = H_A \otimes H_B$ *respectively and Bob sends his entangled half* $H_A$ *to Alice. If Alice applies Bell operator* $U_A$ *on* $H_{A,A'} = H_A \otimes H_{A'}$, initial system $H_{A',B'} \otimes H_{A,B}$ transforms to $H_{A,A'} \otimes H_{B,B'}$. *Exact identity of entangled system* $H_{B,B'} = H_B \otimes H_{B'}$ *remains unknown to both Alice and Bob unless they communicate and reveal their secret information.*

*Proof:* To restrict for binary measurement outcomes, we take both systems $H_{A',B'} = H_{A'} \otimes H_{B'}$ and $H_{A,B} = H_A \otimes H_B$ of Alice and Bob respectively as 2-qubit maximally entangled states

$|\Phi_{\alpha'\beta'}\rangle \in C^2 \otimes C^2$ and $|\Phi_{\alpha\beta}\rangle \in C^2 \otimes C^2$ with Bell basis $|\Phi_{00}\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$, $|\Phi_{01}\rangle = (|01\rangle + |10\rangle)/\sqrt{2}$, $|\Phi_{10}\rangle = (|00\rangle - |11\rangle)/\sqrt{2}$, and $|\Phi_{11}\rangle = (|01\rangle - |10\rangle)/\sqrt{2}$.

From equation (1), it can be seen that regardless of the initially shared EPR system $|\Phi_{\alpha\beta}\rangle \otimes |\Phi_{\alpha'\beta'}\rangle$, four classical outcomes $a_1a_2 \in \{00,01,10,11\}$ of Alice's Bell operator on $|\Phi_{\alpha\alpha'}\rangle$ and hence one of the four Bell states $|\Phi_{\beta\beta'}\rangle \in \{|\Phi_{00}\rangle, |\Phi_{01}\rangle, |\Phi_{10}\rangle, |\Phi_{11}\rangle\}$ swapped between Alice and Bob are equally likely, each with probability of ¼. Hence, the exact identity of $|\Phi_{\beta\beta'}\rangle$ can only be known to someone who knows all three shares $a_1a_2$ and Bell states $|\Phi_{\alpha\beta}\rangle$ and $|\Phi_{\alpha'\beta'}\rangle$. In other words, exact identity of entangled system $|\Phi_{\beta\beta'}\rangle \in H_B \otimes H_{B'}$ remains unknown to both Alice and Bob unless they communicate and reveal their secret information.

**Theorem 3:** *Suppose two distant parties Alice and Bob share an EPR pair $|\Phi_{\beta\beta'}\rangle$ whose exact identity is unknown to both Alice and Bob. If Alice teleports a quantum state $|\psi\rangle$ to Bob, he gets two classical bits $a_1'a_2' \in \{00,01,10,11\}$ while Bob's entangled half becomes $|\psi'\rangle = \sigma^\tau|\psi\rangle$. The Pauli encoding $\sigma^\tau \in \{I, \sigma_x, \sigma_z, \sigma_z\sigma_x\}$ remains unknown to Bob unless he knows both $a_1'a_2'$ and exact Bell state $|\Phi_{\beta\beta'}\rangle$.* Similarly, *Pauli encoding $\sigma^\tau \in \{I, \sigma_x, \sigma_z, \sigma_z\sigma_x\}$ remains unknown to Alice unless she knows exact Bell state $|\Phi_{\beta\beta'}\rangle$.*

*Proof:* From equation (2), it can be seen that regardless of the initially shared EPR system $|\psi\rangle \otimes |\Phi_{\beta\beta'}\rangle$, four classical outcomes $a_1'a_2' \in \{00,01,10,11\}$ of Alice's Bell operator on $|\Phi_{\alpha''\beta''}\rangle$ and hence one of the four possible states $\sigma^\tau|\psi\rangle$ at Bob's side are equally likely, each with probability of ¼. Hence, Pauli encoding $\sigma^\tau$ can only be known to someone who knows both $a_1'a_2'$ and Bell state $|\Phi_{\beta\beta'}\rangle$.

From theorems 2 and 3, it can be concluded that for each value of Alice's Bell state measurement result $a_1a_2$, there is a unique swapped Bell state $|\Phi_{\beta\beta'}\rangle$ and hence unique teleportation encoding $\sigma^\tau$ corresponding to Bell state measurement result of Alice $a_1'a_2'$. Hence, by giving $|\psi'\rangle = \sigma_z^\alpha \sigma_x^\beta \sigma^\tau|\psi\rangle$ back to Alice, Bob cannot simulate with $|\psi'\rangle$ by change identity of $\alpha\beta$ on his will; a perfect binding for committed bit $\beta \in \{0,1\}$.

**Quantum bit commitment over noisy channels**

Quantum information is very fragile to noisy channels in nature. To avoid loses and hence dispute between committer and receiver, in the pre-commitment phase, maximally entangled pair for Bob's commitment can be generated from Werner states or any supply of other entangled mixed states with entanglement purification procedure[40-42] while keeping the identity of EPR pair secret from receiver Alice. For example, Bob generates secretly two copies of same EPR pair and sends entangled half of each pair to Alice. Both Alice and Bob use entanglement purification procedure[40-42] but only Alice announces her measurement result. Bob verifies whether remaining

pair is pure or not without opening his measurement result. If remaining EPR pair is pure and verified, he announces Alice to proceed bit commitment scheme otherwise repeats the purification.

**Discussion:**

We propose here a two-round quantum commitment scheme where committer commits to a specific bit by sharing an EPR pair with receiver in the first round. In the second round, committer applies unitary transformations, depending upon the identity of committed EPR pair, on his/her retained half and confirms his/her commitment by sending retained qubit to the receiver. We showed that proposed scheme guarantees perfect hiding to committer, perfect binding to receiver, and arbitrarily long commitment time without quantum memory.

Proposed scheme is purely non-relativistic quantum mechanical, built over Hibert space unitary transformations and fulfills promises of unconditional security relying on methods of quantum mechanics only. (i) The scheme does not require any classical communication; Alice and Bob use only quantum channels for communication between them. (ii) The scheme does not require extra powers from relativity such as no-communication theorem; there is no constraint on time and space and neither party requires distributed agents at different points of Minkowski space time. (iii) Unlike previously proposed relativistic bit commitment schemes where commitment time is tried to enhance either through multiple rounds of communications or by enhancing communication time by taking large distance between committer and receiver, our scheme gives arbitrarily long commitment time by using only two round of communication while distance between committer and receiver can be as small as possible.

Proposed scheme is unconditionally secure from both classical and quantum attacks. Since scheme does not require any classical communication between committer and receiver, hence is secure from classical attacks by definition. As for as quantum attacks are concerned, EPR type quantum non-local correlations guarantee that the scheme is perfectly concealed and receiver cannot predict/extract committed bit before the opening from committer. Similarly, multiple actions of Bell operator guarantee perfect binding to receiver that committer cannot change her committed bit after his/her confirmation.

The proposed scheme is practical and can be efficiently employed for arbitrarily long commitment time with existing quantum technologies without requiring long term quantum memories or maintaining coherence over distant quantum channels. Repetitive measurements by Alice allow her to store measurement outcomes that are non-locally correlated with initially prepared entangled states. Entanglement is required only for time $t+\delta$ where $t$ is the communication time between the committer and receiver while $\delta << t$ is the processing time at their laboratories.

In conclusion, possibilities of unconditionally secure standard bit commitment in purely Hilbert space quantum formalism would also allow implementing oblivious transfer, ideal coin tossing, quantum digital signatures, and two-sided two-party secure computations in general. These possibilities of pioneering tasks in cryptography, communication, and distributed computing would then reflect that methods of Hilbert space quantum mechanics are sufficient for unconditional security without requiring bounds of Minkowski space time and communication complexity.

1. Blum, M. **C**oin flipping by telephone a protocol for solving impossible problems. *SIGACT News* **15**, 23-27; DOI: 10.1145/1008908.1008911 (1983)
2. Rivest, R. L., Shamir, A., and Adleman, L. A method of obtaining digital signatures and public-key cryptosystems. *Comm. Assoc. Comput. Mach*. **21**, 120–126 (1978).
3. Wiesner, S. Conjugate coding. *Sigact News* **15**, 78 (1983)
4. Yao, A. C. Some complexity questions related to distributive computing. In *Proceedings of the 11th Annual ACM Symposium on Theory of Computing (STOC '79)*, pp. 209–213, Atlanta, Georgia, USA. ACM, New York, USA (April 30-May 02, 1979); DOI: 10.1145/800135.804414.
5. Kilian, J. Founding cryptography on oblivious transfer. *In Proceedings of the 20th Annual ACM Symposium on Theory of Computing (STOC '88),* pp. 20-31, Chicago, Illinois, USA. ACM, New York, USA (May 02-04, 1988); DOI: 10.1145/62212.62215.
6. Shor, P. W. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM J. Sci. Statist. Comput*. **26**, 1484 (1997).
7. Kent, A. Unconditionally secure bit commitment. *Phys. Rev. Lett.* **83,** 1447-1450 (1999).
8. Kent, A. Secure Classical Bit Commitment using Fixed Capacity Communication Channels. *J. Cryptology* **18,** 313-335 (2005).
9. Lunghi, T. *et al*. Practical relativistic bit commitment. *Phys. Rev. Lett*. **115,** 030502 (2015).
10. Mayers, D. Unconditionally secure quantum bit commitment is impossible. *Phys. Rev. Lett*. **78,** 3414-3417 (1997).
11. Lo, H. K. & Chau, H. F. Is quantum bit commitment really possible? *Phys. Rev. Lett.* **78,** 3410- 3413 (1997).
12. Lo, H. K. & Chau, H. F. Why quantum bit commitment and ideal quantum coin tossing are impossible. *Physica D,* **120,** 177-187 (1998).
13. Mayers, D., Kitaev, A. & Preskill, J. Superselection rules and quantum protocols. *Phys. Rev. A* **69,** 052326 (2004).
14. Kent, A. Unconditionally secure bit commitment with flying qudits. *New J. Phys*. **13**, 113015 (2011).
15. Kent, A. Unconditionally secure bit commitment by transmitting measurement outcomes. *Phys. Rev. Lett.* **109**, 130501 (2012).
16. Croke, S. & Kent, A. Security Details for Bit Commitment by Transmitting Measurement Outcomes. *Phys. Rev. A* **86**, 052309 (2012)
17. Kaniewski, J., Tomamichel, M., H¨anggi, E. & Wehner, S. Secure bit commitment from relativistic constraints. *IEEE Trans. Inf. Theo*. **59**, 4678–4699 (2013).
18. Nadeem, M**.** Unconditionally secure commitment in position-based quantum cryptography. *Sci. Rep*. **4**, 6774; DOI:10.1038/srep06774 (2014).
19. Lunghi, T. *et al*. Experimental bit commitment based on quantum communication and special relativity. *Phys. Rev. Lett.* **111**, 180504 (2013).
20. Liu, Y. *et al*. Experimental unconditionally secure bit commitment. *Phys. Rev. Lett.* **112**, 010504 (2014).
21. Einstein, A., Podolsky, B. & Rosen, N. Can quantum-mechanical description of physical reality be considered complete? *Phys. Rev.* **47**, 777 (1935).
22. Bennett, C. *et al*. Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. *Phys. Rev. Lett*. **70**, 1895 (1993).
23. Zukowski, M., Zeilinger, A., Horne, M. & Ekert, A. Event-ready-detectors'' Bell experiment via entanglement swapping. *Phys. Rev. Lett.* **71**, 4287 (1993).

24. Braunstein, S., Mann, A. & Revzen, M. Maximal violation of Bell inequalities for mixed states. *Phys. Rev. Lett*. **68**, 3259 (1992).
25. Nadeem, M. Quantum cryptography – an information theoretic security. *arXiv:* 1507.07918 (2015).
26. Nadeem, M. Quantum digital signature scheme. *arXiv:* 1507.03581 (2015).
27. Nadeem, M. & Noor Ul Ain. Secure and authenticated quantum secret sharing. *arXiv*: 1506.08558 (2015).
28. Nadeem**,** M**.** Delayed choice relativistic quantum bit commitment with arbitrarily long commitment time*. arXiv:*1504.03316 (2014).
29. Nadeem, M. Quantum non-locality, causality and mistrustful cryptography**.** *arXiv:*1407.7025 (2014).
30. Nadeem, M. The causal structure of Minkowski space time - possibilities and impossibilities of secure positioning. *arXiv*: 1505.01839 (2015).
31. Nadeem, M. Secure positioning and non-local correlations. *arXiv:*1406.3013 (2014).
32. Nadeem, M. Position-based quantum cryptography over untrusted networks. *Laser Phys.* **24** 085202 (2014).
33. Kent, A., Munro, W. & Spiller, T. Quantum tagging: authenticating location via quantum information and relativistic signalling constraints. *Phys. Rev. A*. **84**, 012326 (2011).
34. Malaney, R. Location-dependent communications using quantum entanglement. *Phys. Rev. A*. **81**, 042319 (2010).
35. Lau, H. & Lo, H. Insecurity of position-based quantum-cryptography protocols against entanglement attacks. *Phys. Rev. A*. **83**, 012322 (2011).
36. Buhman, H. *et al.* Position-based cryptography: impossibility and constructions. *In proceedings of Advances in Cryptology — CRYPTO 2011*, pages 429–446, Santa Barbara, CA, USA (*Lect. Notes Comput. Sci.* Vol. **6841**, Springer, Heidelberg) (Aug. 14-18, 2011); DOI: 10.1007/978-3-642-22792-9.
37. Chandran, N., Goyal, V., Moriarty, R. & Ostrovsky, R. Position based cryptography. *In proceedings of Advances in Cryptology — CRYPTO* 2009, pages 391–407, Santa Barbara, CA, USA (*Lect. Notes Comput. Sci.* Vol. **5677**, Springer, Heidelberg) (Aug. 16-20, 2009): DOI:10.1007/978-3-642-03356-8_23.
38. Brassard, G. The conundrum of secure positioning. *Nature* **479**, 307-308; DOI:10.1038/479307a (2011).
39. Kent, A. Quantum tagging for tags containing secret classical data. *Phys. Rev. A*. **84**, 022335 (2011).
40. Bennett, C. *et al*. Purification of noisy entanglement and faithful teleportation via noisy channels *Phys. Rev. Lett.* **76**, 722 (1996).
41. Bennett, C., DiVincenzo, D., Smolin, J. & Wooters, W. Mixed-state entanglement and quantum error correction. *Phys. Rev. A* **54**, 3824 (1996).
42. Deutsch, D. *et al*. Quantum privacy amplification and the security of quantum cryptography over noisy channels. *Phys. Rev. Lett.* **77**, 2818 (1996).