Results in Physics 2 (2012) 97–99

Contents lists available at SciVerse ScienceDirect

Results in Physics

journal homepage: www.journals.elsevier.com/results-in-physics

A practical quantum bit commitment protocol

S. Arash Sheikholeslam *, T. Aaron Gulliver

Department of Electrical and Computer Engineering, University of Victoria, P.O. Box 3055, STN CSC, Victoria, BC, Canada V8W 3P6

ARTICLE INFO

Article history:
Received 17 May 2012
Accepted 19 July 2012
Available online 27 July 2012

Keyword:
Quantum bit commitment
Quantum cryptography
EPR attack

ABSTRACT

In this paper, we introduce a new quantum bit commitment protocol which is secure against entanglement attacks. A general cheating strategy is examined and shown to be practically ineffective against the proposed approach.

1. Introduction

Quantum cryptography in the sense of key distribution was first introduced in [1] with the BB84 protocol. The authors also proposed a bit commitment scheme which they determined was not secure. Construction of an unconditionally secure quantum bit commitment technique has since become an important research problem. There have been many commitment schemes created, as well as a number of results on the impossibility of perfectly secure commitment [2,6,7]. Even teleportation has been considered to achieve unconditional security [3]. Recently, "practically" secure commitment schemes [4] have been examined, rather than asymptotically secure protocols. By practical it is simply meant that the security is very hard to break rather than impossible. This paper considers practically secure bit commitment, as is the case with classical commitment schemes.

Consider a two party (Alice and Bob) bit commitment. Alice chooses a bit $b \in \{0,1\}$, locks it and sends it to Bob (commitment phase). When it is the time to reveal b (opening phase), Bob locks the bit with his own lock (i.e., he locks the bit locked by Alice), and sends it back to Alice. She then opens her lock and sends the bit back to Bob and announces b. Bob then opens his lock and checks whether the locked bit b is the same as the one which was announced.

Here we propose a simple scheme using the principles of the well-known Diffie-Hellman key exchange protocol (details of this protocol can be found in [5]). However, we employ multiplication by a unitary transform instead of exponentiation in a multiplicative group modulo a prime. Although this commitment scheme also falls within the category for which entanglement cheating is a proof of insecurity, (since it satisfies the criteria based on the simplified Yao model [8] as described in [7]), it is practically very hard for Alice to cheat. This is due to the fact that constructing the unitary transform required to apply on her share of the entangled pair can be made infeasible, as will be shown.

Before presenting our bit-commitment protocol, we will first define practical security. For this, we need the following.

1.1. Binding experiment (BE)

- Alice and Bob share a system $H_A \otimes H_B$ and a protocol Π for which the final state before the opening phase is $\rho_{AB} \in H_A \otimes H_B$.
- A cheating Alice performs the operation $A \otimes I[\rho_{AB}]$ and reveals $b \leftarrow_R \{0,1\}$ to Bob (A is a trace preserving operation).
- Bob then performs the operation (actually a measurement) $I \otimes B[\rho_{AB}]$ to obtain b'.
- The outcome of the experiment is 1 (success) if $b = b'$ and 0 (fail) otherwise.

Definition 1.1. A protocol π is computationally binding (CB) if for all polynomial time quantum operations Alice can perform we have $\Pr\left[BE_{\pi}^{A}(1^n) = 1\right] \leqslant \frac{1}{2} + negl(n)$, where $negl(n)$ is a negligible function of the secrecy parameter n and 1^n denotes a string of n qubits.

Note that in the above definition, polynomial time is with respect to the dimension of the Hilbert space. Bob and Alice are using (i.e., n, which is the number of qubits in the strings used to represent 0 and 1).

Proposition 1.2. *If a protocol is CB then there is no collection of circuits $\{Q_x | x \in S\}$ (where S is any string), which can be generated in polynomial time that can closely approximate the operation A.*

* Corresponding author.
E-mail addresses: sasheikh@uvic.ca (S. Arash Sheikholeslam), agullive@ece.uvic.ca (T. Aaron Gulliver).

2211-3797 © 2012 Elsevier B.V. Open access under CC BY-NC-ND license.
http://dx.doi.org/10.1016/j.rinp.2012.07.002

Proof. The proof follows from the definition of a binding experiment. □

Achieving CB security is a general task and Alice may employ different approaches in an attempt to compromise the security of a protocol. One important case is an EPR attack by Alice. EPR attacks [7] have been proven to make all quantum bit commitment schemes theoretically insecure. Therefore we introduce the notion of EPR-Computationally Binding (EPR-CB).

Definition 1.3. A protocol π is EPR-Computationally Binding (EPR-CB) if for all polynomial time quantum operations by Alice, $\Pr\left[BE_{\pi}^{A}(1^n) = 1\right] \leqslant \frac{1}{2} + negl(n)$, where $negl(n)$ is a negligible function of the secrecy parameter n. Note that Alice is only capable of entangling an ancillary system in the corresponding Hilbert space, and can perform unitary transforms and POVM (Positive Operator Valued Measure) measurements on her system before the opening phase.

Proposition 1.4. *CB is equivalent to EPR-CB if a cheating Alice can extend any system to a larger system in polynomial time.*

Proof. Obviously, any EPR-CB protocol is also CB. It is known that all trace preserving quantum operations on a Hilbert space can be extended to a higher dimensional system in which these operations can be reduced to a unitary transform. Therefore, a cheating Alice can extend a system and then perform a unitary transform. A general CB experiment on a Hilbert space H^n is equivalent to a (unitary and POVM) CB experiment on a Hilbert space H^m where $m \geqslant n$. Therefore EPR-CB security is equivalent to CB security. □

This proposition is important as it connects the concept of binding to EPR security.

Definition 1.5. An ensemble of protocols $\Pi = \{\pi_1, \cdots, \pi_n\}$ is computationally binding (CB) if all $\pi_i \in \Pi$ are CB.

An ensemble of protocols is required because if there is only one protocol for which the bit commitment is CB, a cheating Alice can prepare the necessary circuit for changing the qubit in advance and use it at the time of commitment.

2. The proposed bit commitment protocol

In this section, we present the proposed method of bit commitment. With this protocol, each party first prepares a secret unitary operator. It is assumed that a quantum channel as well as a classical side-channel is available, as with other bit commitment schemes. The qubits are exchanged through the quantum channel, while the side-channel is used to exchange the secret unitary operators in the opening phase. The proposal can then be described as follows.

- Commitment phase:
  - Bob prepares two previously agreed upon orthogonal states $|\phi_0\rangle$, $|\phi_1\rangle$, and applies his secret transform U_B on them. He sends these to Alice and tells her which to use if she wants to commit 0 or 1.
  - Alice prepares $U_A \cdot U_B|\phi_0\rangle$ or $U_A \cdot U_B|\phi_1\rangle$ and sends $|\phi\rangle \in \{U_A \cdot U_B|\phi_0\rangle, U_A \cdot U_B|\phi_1\rangle\}$ back to Bob depending on the bit she wants to share.
- Opening phase:
  - Alice reveals her unitary transform U_A to Bob through the classical channel.
  - Bob computes $|\psi\rangle = U_B \cdot U_A|\phi\rangle$ and checks if it agrees with the committed qubit.

Note that the secret unitary transforms can be chosen at random from a continuous subset of the unitary group. As an example, we can assume that $|\phi_0\rangle = |0\rangle$ and $|\phi_1\rangle = |1\rangle$, and $U_A, U_B \in \{R_x(\theta), R_y(\theta), R_z(\theta)\}$ where $R_x(\theta)$ is a rotation about the x axis with an angle θ.

3. Security and cheating strategies

One approach for Alice to attempt to cheat is to apply a unitary transform U_A during the committing phase but then send $V \cdot U_A$ during the opening phase (where V is another unitary transform), such that when Bob tries to open the commitment he receives a bit other than the one which was committed (say Alice has committed $|\phi_0\rangle$ but now wants Bob to open $|\phi_1\rangle$). For Alice to be successful in cheating, the following must be true for the last step of the opening phase

$$|\psi\rangle = U_B \cdot V \cdot U_A \cdot U_A \cdot U_B|\phi_0\rangle = |\phi_1\rangle \Rightarrow U_B \cdot V \cdot U_B = |\phi_1\rangle\langle\phi_0|.$$

This shows that Alice can construct such a transform V only if she knows the secret transform of Bob. By a similar analysis, Bob cannot determine the state $|\phi_i\rangle$ if he only knows $U_A \cdot U_B|\ \phi_i\rangle$.

Theorem 3.1. *The proposed protocol is practically secure against an EPR (entanglement) attack by Alice.*

Proof. Let $|A\rangle$ and $|B\rangle$ denote the uniform superposition of all possible U_A and U_B on $|\phi_i\rangle$. In other words, assuming U_A and U_B are controlled gates and $|\ A\rangle$ and $|B\rangle$ are the corresponding control registers, we have a register ($|A\rangle$ or $|B\rangle$) which is a superposition of all possible choices of the unitary transformations by Alice and Bob (i.e., $|A\rangle = \sum U_A^i|\phi_0\rangle$ where $\left\{U_A^i\right\}$ is the set of all possible U_A). Considering these registers at the end of the commitment phase, we have

$$|\psi_0\rangle = \sum_A\sum_B |B\rangle U_A U_B|\phi_0\rangle \otimes U_A U_B|\phi_1\rangle|A\rangle;$$
$$|\psi_1\rangle = \sum_A\sum_B |B\rangle U_A U_B|\phi_1\rangle \otimes U_A U_B|\phi_0\rangle|A\rangle,$$

where $|\psi_0\rangle$ denotes 0 and $|\psi_1\rangle$ denotes 1. In each state, the component on the right side of the tensor product is possessed by Alice. Now, if the protocol is secure against Bob then the local trace over the system components of Alice must be equal for both $|\psi_0\rangle$ and $|\psi_1\rangle$. As a result, considering the Schmidt decomposition [9], we have a unitary transform V on Alice's side which can take values from $|\psi_0\rangle$ to $|\psi_1\rangle$. In order for Alice to produce V, she must know all possible choices for U_B (but she does not need to know a particular choice of U_B). The existence of V shows that the protocol is not theoretically secure, but the two parties can hide their sets of unitary transforms and make the protocol practically secure against an entanglement attack. This protocol is practically secure because in order to construct $|B\rangle$, one has to construct an arbitrary unitary operation on n qubits to take a state (say $|0\rangle$) to $|B\rangle$. It has been shown that this requires $O\left(n^2 4^n \log^c\left(\frac{n^2 4^n}{\epsilon}\right)\right)$ gates in order to approximate such a transformation within distance ϵ [9]. □

Note that there is a trade off between the security and time complexity of this protocol, as is the case for other security protocols.

4. Conclusions

In this paper, we proposed a simple but secure bit commitment protocol which is based on the application of secret unitary transforms by each party (Alice and Bob) in succession. Cheating strategies, including entanglement cheating, were examined and the system was shown to be effective against these attacks.

References

[1] Bennett CH, Brassard G. Quantum cryptography: public key distribution and coin tossing. In: Proc IEEE int conf on computers systems and signal process. Bangalore, India; 1984. p. 175–179.

[2] Mayers D. Unconditionally secure quantum bit commitment is impossible. Phys Rev Lett 1997;78(17):3414–7.

[3] Yuen HP. A simple unconditionally secure quantum bit commitment protocol via quantum teleportation; 2004. arXiv:quant-ph/0305142v3.

[4] Danan A, Vaidman L. Practical quantum bit commitment protocol. Quantum Information Processing. 2012;11(3):769–75.

[5] Menezes AJ, van Oorschot PC, Vanstone SA. Handbook of applied cryptography. Boca Raton, FL: CRC Press; 1996.

[6] Mayers D. The trouble with quantum bit commitment. Los Alamos. Preprint archive quant-ph/9603015, March; 1996.

[7] Lo H-K, Chau HF. Why quantum bit commitment and ideal quantum coin tossing are impossible. Physica D: Nonlinear Phenom 1998;120(12):177–87.

[8] Yao AC-C. Security of quantum protocols against coherent measurements. In Proc ACM symp on theory of computing. Las Vegas NV; May 1995. p. 67–75.

[9] Nielsen MA, Chuang IL. Quantum computation and quantum information, section 4.5.4. New York: Cambridge University Press; 2000.