Analysis of one quantum bit string commitment

Zhengjun Cao

Département d'informatique, Université Libre de Bruxelles. zhencao@ulb.ac.be

Abstract A. Kent proposed a quantum bit string commitment protocol in 2003. Not using the standard two conjugate states $|0\rangle$, $|1\rangle$, $|+\rangle$ and $|-\rangle$, the protocol uses $\psi_0 = |0\rangle$ and $\psi_1 = \sin\theta|0\rangle + \cos\theta|1\rangle$, where $\theta \neq 0$. In this paper, we show that the protocol can not guarantee security to the receiver. $(1 - \frac{\sin^2\theta}{2})n$ bits are definitely exposed to the receiver, where n is the length of the committed string.

Keywords. bit string commitment, conjugate states

1 Introduction

In cryptography, a commitment scheme allows one to commit to a value while keeping it hidden, with the ability to reveal the committed value later. It is important to a variety of cryptographic protocols including secure coin flipping [2, 7], zero-knowledge proofs [3], and secure computation.

A bit string commitment protocol securely commits n classical bits so that the recipient can retrieve only m bits of information about the string. From a practical point of view, $m < \frac{n}{2}$. Otherwise, the content of the committed string may be easily recovered. To ensure a comparatively strong level security, it is usually required that $m \ll \frac{n}{2}$. In other words, $\frac{m}{n}$ is negligible.

In 2001, A. Kent proposed a quantum bit string commitment protocol in the manuscript [5]. A refined version was published as [6] in 2003. Not using the standard two conjugate states $|0\rangle$, $|1\rangle$, $|+\rangle$ and $|-\rangle$, the protocol uses $\psi_0 = |0\rangle$ and $\psi_1 = \sin\theta|0\rangle + \cos\theta|1\rangle$, where $\theta \neq 0$. With the introduced parameter θ, the author tried to show that the protocol can guarantee strong levels of security to both the committer and receiver.

In this paper, we point out that some parameters in Kent's protocol are not specified, and show that the protocol can not guarantee security to the receiver. $(1 - \frac{\sin^2\theta}{2})n$ bits are definitely exposed to the receiver, where n is the length of the committed string.

2 Review of Kent's commitment protocol

Consider the following cryptographic problem. Two mistrustful parties, Alice and Bob, need a protocol which will (i) allow Alice to commit a string $a_1a_2\cdots a_n$ of bits to Bob, and then, (ii) at any later time of her choice, reveal the committed bits. The protocol should prevent

Alice from cheating, in the sense that she should have a negligible chance of unveiling bits a'_i different from the a_i without Bob being able to detect the attempted detection. In other words, Alice should be genuinely committed after the first stage. The protocol should also prevent Bob from being able to completely determine the bit string. More precisely, it must guarantee that, before revelation, Bob has little or no chance of obtaining more than m bits of information about the committed string, for some fixed integer $m < n$. In 2003, A. Kent proposed such a (m, n) quantum bit string commitment protocol. We now describe it as follows.

Setup. Define qubit states $\psi_0 = |0\rangle$ and $\psi_1 = \sin\theta|0\rangle + \cos\theta|1\rangle$. Take $\theta > 0$ to be small; θ and $r = n - m$ are security parameters for the protocol. (We here emphasize that at least a state of ψ_0 and ψ_1 must be known to Bob in advance, otherwise Alice can flip each bit in her committed string.)

Commitment. To commit a string $a_1, \cdots, a_n$ of bits to Bob, Alice sends the qubits $\psi_{a_1}, \cdots, \psi_{a_n}$, sequentially.

Unveiling. Alice simply declares the values of the string bits, and hence the qubits sent. Assuming that Bob has not disturbed the qubits, he can test the bit values by measuring the projection onto $\psi_{a'_i}$ on qubit i, for each i. If he obtains eigenvalue 1 in each case, he accepts the unveiling as an honest revelation of a genuine commitment; otherwise he concludes Alice cheated.

To elaborate the protocol, we now investigate the following example, where the committed string is of length 6.

Table 1: An example for Kent's quantum bit string commitment

committed string	$a_1 = 0$	$a_2 = 1$	$a_3 = 1$	$a_4 = 0$	$a_5 = 0$	$a_6 = 1$
states sent	ψ_0	ψ_1	ψ_1	ψ_0	ψ_0	ψ_1
opened string	0	1	1	0	0	1
honest measurement	ψ_0	ψ_1	ψ_1	ψ_0	ψ_0	ψ_1
eigenvalue	1	1	1	1	1	1

3 The commitment is not secure against the receiver

3.1 The false security argument against Bob

In the argument for security against Bob, the author claimed:

> We assume that prior to commitment Bob has no information about the bit string: to Bob, all string values are equiprobable. He thus has to obtain information about

a density matrix of the form

$$\rho = 2^{-n} \sum_{a_1,\cdots,a_n} |\psi_{a_1},\cdots,\psi_{a_n}\rangle\langle\psi_{a_1},\cdots,\psi_{a_n}|$$

Hence, the accessible information available to Bob by any measurement on ρ is bounded by the entropy

$$S(\rho) = \left[H\left(\frac{1+\sin\theta}{2}\right)\right]^n$$

For any fixed $\theta > 0$, we have $S(\rho) < n$. For any fixed r, by taking n sufficiently large, we can ensure $n - S(\rho) > r$. So we can ensure that, however Bob proceeds, on average at least r bits of information about the string will remain inaccessible to him.

We now point out that:

1. The security parameter r is not specified. Furthermore, recall that $r = n - m$. By the inequality $n - S(\rho) > r$, we have $m > S(\rho)$, which is not indicating the upper bound to the number of exposed bits. The original claim that at least r bits of information about the string will remain inaccessible to Bob is not sound.

2. The formula for Von Neumann entropy $S(\rho)$ is incorrect. Since all qubits are mutually independent, the entropy is linear with the string length, n, not exponential with n, namely

$$S(\rho) = -n\left[\left(\frac{1+\sin\theta}{2}\right)\log_2\left(\frac{1+\sin\theta}{2}\right) + \left(\frac{1-\sin\theta}{2}\right)\log_2\left(\frac{1-\sin\theta}{2}\right)\right]$$

(The author has acknowledged this “typo” in a recent communication.)

3.2 Bob’s trick

Dishonest Bob can measure the projection onto $\psi_0 = |0\rangle$ for all qubits before Alice declares the committed string. In such case, for the previous example we have the following result.

Table 2: Bob prior measures the projection onto $\psi_0 = |0\rangle$ for all qubits

committed string	$a_1 = 0$	$a_2 = 1$	$a_3 = 1$	$a_4 = 0$	$a_5 = 0$	$a_6 = 1$
states sent	ψ_0	ψ_1	ψ_1	ψ_0	ψ_0	ψ_1
prior measurement	ψ_0	ψ_0	ψ_0	ψ_0	ψ_0	ψ_0
eigenvalue	1	t_1	t_2	1	1	t_3

Notice that each t_i $(i = 1, 2, 3)$ is of the eigenvalue 1 with the probability $\sin^2\theta$, where θ is a parameter settled in the *Setup*. Since θ is taken small, Bob can assert that $a_2 = 1, a_3 = 1, a_6 = 1$ pretty well.

Suppose that the committed string is balanced, namely, each bit is equiprobably 0 or 1. Theoretically, by the such attack Bob can retrieve $(1-\frac{\sin^2\theta}{2})n$ bits when the committed string is of n bits. Thus, the commitment protocol is not secure against Bob since $(1-\frac{\sin^2\theta}{2})n \approx n$ if θ is taken small. That is to say, almost committed bits are exposed to Bob.

4 Conclusion

One might argue that using the standard two conjugate states $|0\rangle, |1\rangle, |+\rangle, |-\rangle$, like BB84 protocol [1], for a quantum bit string commitment. Such a protocol (DMS00) has been proposed [4] in 2000. Notice that the committed bits $0, 1$ are encoded respectively to two measurements $+, \times$, instead of four quantum states. Moreover, a family of one-way permutations is involved.

Acknowledgement Cryptasc Project (Institute for the encouragement of Scientific Research and Innovation of Brussels), CNNSF Project 60873227.

References

[1] C. H. Bennett, G. Brassard, Quantum Cryptography: Public Key Distribution and Coin Tossing, Proc. of the IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, India, December 1984, pp. 175-179 (1984)

[2] M. Blum, Coin flipping by telephone a protocol for solving impossible problems, ACM SIGACT News, Vol.15, Issue 1, 23-27 (1983)

[3] M. Blum, P. Feldman, and S. Micali, Non-Interactive Zero-Knowledge and Its Applications. Proceedings of the twentieth annual ACM symposium on Theory of computing (STOC 1988). 103-112 (1988)

[4] P. Dumais, D. Mayers, L. Salvail, Perfectly Concealing Quantum Bit Commitment from any Quantum One-Way Permutation, EUROCRYPT 2000, LNCS 1807, pp. 300-315 (2000)

[5] A. Kent, www.hpl.hp.com/techreports/2001/HPL-2001-317.pdf

[6] A. Kent, PhysRevLett.90.237901 (2003)

[7] Vladimir Z. Vulovic and Richard E. Prange, Randomness of a true coin toss. Phys.RevA 33: 576-582 (1986)