Quantum Bit String Commitment

Adrian Kent
Trusted E-Services Laboratory
HP Laboratories Bristol
HPL-2001-317
December 11th , 2001*

quantum cryptography, protocol, bit commitment

A bit string commitment protocol securely commits N classical bits in such a way that the recipient can extract only $M<N$ bits of information about the string. Classical reasoning might suggest that bit string commitment implies bit commitment and hence, given the Mayers-Lo-Chau theorem, that non-relativistic quantum bit string commitment is impossible. But this classical argument is incorrect. There exist non-relativistic quantum bit string commitment protocols, with security parameters ε and M, that allow A to commit $N = N(M,\varepsilon)$ bits to B so that A's probability of successfully cheating when revealing any bit and B's probability of extracting more than $N' = N - M$ bits of information about the N bit string before revelation are both less than ε. With a slightly weakened but still restrictive definition of security against A, N can be taken to be $O(\exp(CN'))$ for a positive constant C. I briefly discuss possible applications.

* Internal Accession Date Only
Approved for External Publication

Quantum Bit String Commitment

Adrian Kent[1]
Hewlett-Packard Laboratories, Filton Road,
Stoke Gifford, Bristol BS34 8QZ, U.K.
(September 2001)

A bit string commitment protocol securely commits N classical bits in such a way that the recipient can extract only $M < N$ bits of information about the string. Classical reasoning might suggest that bit string commitment implies bit commitment and hence, given the Mayers-Lo-Chau theorem, that non-relativistic quantum bit string commitment is impossible. But this classical argument is incorrect. There exist non-relativistic quantum bit string commitment protocols, with security parameters ϵ and M, that allow A to commit $N = N(M, \epsilon)$ bits to B so that A's probability of successfully cheating when revealing any bit and B's probability of extracting more than $N' = N - M$ bits of information about the N bit string before revelation are both less than ϵ. With a slightly weakened but still restrictive definition of security against A, N can be taken to be $O(\exp(CN'))$ for a positive constant C. I briefly discuss possible applications.

[1] On leave from DAMTP, University of Cambridge, Silver Street, Cambridge CB3 9EW, U.K.

I. INTRODUCTION

As is by now well known, quantum information can guarantee classically unattainable security in a variety of important cryptographic tasks. Some no-go results have also been obtained, showing that quantum cryptography cannot guarantee perfect security for every task. We do not presently have a good characterisation of the tasks for which perfectly secure quantum protocols exist. In fact, we are not yet even able to characterise the range of cryptographic tasks for which perfectly secure quantum protocols *might possibly* exist. The main reason is that quantum cryptography involves more than devising quantum protocols for tasks known to be useful in classical cryptography. The properties of quantum information allow one to devise new and cryptographically useful tasks, which have no classical counterpart. Moreover, reductions and relations between classical cryptographic tasks need not necessarily apply to their quantum equivalents. This means that there is a wider range of tasks to consider, and that no-go theorems may not necessarily be quite as powerful as classical reasoning would suggest.

These remarks apply particularly to bit commitment, an important cryptographic protocol whose potential for physically secure implementation has been extensively investigated [2–8,10–14]. It is known that unconditionally secure quantum bit commitment is impossible for non-relativistic protocols [5–8,10]: that is, protocols in which the two parties are restricted to single pointlike sites, or more generally, in which the signalling constraints of special relativity are ignored. On the other hand, unconditionally secure bit commitment is thought to be possible between parties controlling appropriately separated pairs of sites, when the impossibility of superluminal signalling is taken into account. [12,13]

While sustaining a bit commitment indefinitely via relativistic protocols is practical with current technology [13], the constraints it imposes are not always desirable. Both parties have to maintain separated secure locations, and communications have to continue throughout the duration of the commitment. A further motivation for continued study of non-relativistic protocols is that it is theoretically interesting to characterise which secure quantum protocols can be implemented without relying on relativity. With these motivations in mind, we restrict attention to non-relativistic protocols in the rest of this paper. Rather than insert the word "non-relativistic" throughout, we generally take the restriction as understood below.

Some variants of bit commitment, for which non-relativistic protocols are not known to be impossible, have previously been studied. [18,19] This paper considers a different type of generalisation, bit string commitment, in which one party commits many bits to another in a single protocol. Two non-relativistic bit string commitment protocols, which offer classically unattainable levels of security against cheating, are described.

II. BIT STRING COMMITMENT

Consider the following classical cryptographic problem. Two mistrustful parties, A and B, need a protocol which will (i) allow A to commit a string $a_1 a_2 \ldots a_n$ of bits to B, and then, (ii) at any later time of her choice, reveal the committed bits. The protocol should prevent A from cheating, in the sense that she should have little or no chance of unveiling bits a_i' different from the a_i without B being able to detect the attempted detection. In other words, A should be genuinely committed after the first stage. The protocol should also prevent B from being able to completely determine the bit string. More precisely, it must guarantee that, before revelation, B has little or no chance of obtaining more than m bits of

information about the committed string, for some fixed integer $m < n$.

This (m, n) *bit string commitment* problem is a generalisation of the standard bit commitment problem, in which $n = 1$ and $m = 0$. Clearly, a protocol for bit commitment would solve this generalised problem, since the protocol could be repeated n times to commit each of the a_i, and B would be able to obtain no information about the committed string. Conversely, classical reasoning implies that a protocol for the generalised problem, for any integers m and n with $m < n$, could be used as a protocol for standard bit commitment. For A and B can use any coding of a single bit a by the n bit string such that none of the m bits available to B give information about a, and then use the protocol to commit A to a.

Classically, then, (m, n) bit string commitment is essentially equivalent to bit commitment. At first sight, allowing A and B to use quantum information may seem to make no difference. But there is a subtlety. Extracting information from a quantum state can generally be done in many different ways. Each of these generally disturbs the quantum state, so that different ways of information extraction are generally incompatible: after method one has been applied, method two may no longer give as much (or any) information. This leaves open the possibility of bit string commitment protocols in which B can obtain some m bits of information about the committed n bit string in many different ways. It might not be possible for A to predict or greatly constrain which m bits of information will be obtained. (It might not necessarily be possible for B to choose precisely which bits will be obtained either.) Any attempt to use such a protocol to commit a single bit, by a redundant coding, could then fail: it could be that B, knowing the coding, could choose measurements which reveal the relevant bit. Nonetheless, one could hope to guarantee that, although any single coded bit could be read by B, he has little or no chance of obtaining more than m bits of information, however he proceeds.

In other words, there is no obvious equivalence between quantum (m, n) bit string commitment and quantum bit commitment. The impossibility of unconditionally secure quantum bit commitment does not necessarily imply that, with an analogous definition of security, unconditionally secure quantum bit string commitment is impossible. In fact, the next sections show it can be achieved.

III. PROTOCOL 1

Define qubit states $\psi_0 = |0\rangle$ and $\psi_1 = \sin\theta|0\rangle + \cos\theta|1\rangle$, where $\sin^2\theta = \delta$. We take $\theta > 0$ and $r = n - m$ to be security parameters for the protocol.

Commitment: To commit a string $a_1 \ldots a_n$ of bits to B, A sends the qubits $\psi_{a_1}, \ldots, \psi_{a_n}$, sequentially.

Unveiling: To unveil, A simply declares the values of the string bits, and hence the qubits sent. Assuming that B has not disturbed the qubits, he can test the bit values a_i' claimed by A at unveiling 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. If he obtains eigenvalue 0 in any case, he concludes (assuming that noise is negligible) that A has cheated.

Security against A: Whatever strategy A follows, once she transmits the qubits to B, their respective density matrices ρ_i are fixed. Let $p_i^j = \langle\psi_j|\rho_i|\psi_j\rangle$ be the probability of B accepting a revelation of j for the i-th bit. We have

$$p_i^0 + p_i^1 \leq \cos^2((\pi/4) - (\theta/2)) + \sin((\pi/4) + (\theta/2))\,, \quad (1)$$

which is $\leq 1 + \theta$ for small θ. This is the standard definition of security against A for an individual bit commitment, with security parameter θ. In other words, A's scope for cheating on any bit of the string is limited to slightly increasing the probability of revealing a 0 or 1, by an amount $\leq \theta$, which can be made arbitrarily small by choosing the security parameters appropriately.

Security against B: We assume that, prior to the commitment, B has no information about the bit string and regards every possible value as equiprobable. From B's perspective, then, he has to obtain information about a density matrix of the form

$$\rho = (1/2^n) \sum_{a_1 \ldots a_n} |\psi_{a_1} \ldots \psi_{a_n}\rangle\langle\psi_{a_1} \ldots \psi_{a_n}|\,. \quad (2)$$

Holevo's theorem [20] tells us that the accessible information available to B by any measurement on ρ is bounded by the entropy

$$S(\rho) = (((1 + \sin\theta)/2)\log_2((1 + \sin\theta)/2) + ((1 - \sin\theta)/2)\log_2((1 - \sin\theta)/2))^n\,. \quad (3)$$

Now, for any fixed $\theta > 0$, we have $S(\rho) < n$. For any fixed r, by taking n sufficiently large, we can ensure $n - S(\rho) > r$. In other words we can ensure that, however B proceeds, an average of at least r bits of information about the string will remain inaccessible to him. By choosing n suitably large, we can also ensure that the probability of his obtaining more than $n - r$ bits of information about the string is smaller than ϵ, for any given $\epsilon > 0$.

IV. PROTOCOL 2

Protocol 1 ensures bit-wise security against A, but uses a rather inefficient bit string coding which allows B to

obtain almost all of the bit string before revelation. For large n, more efficient codings allow the security against B to be greatly enhanced, though with a weakened notion of security against A.

We again take $\theta > 0$ to be a security parameter and write $\epsilon = \sin\theta$. Now, for any $\theta > 0$ and large n, explicit constructions are known for sets $v_1, \ldots, v_{f(n)}$ of vectors in H^n such that $|\langle v_i \,|\, v_j \rangle| < \sin\theta$ for all $i \neq j$, with the property that $f(n) = O(\exp(Cn))$, where C is a positive constant that depends on θ. [21,22] (The use of these constructions for efficient quantum coding of classical information has previously been noted by Buhrman et al. [23], who describe efficient quantum fingerprinting schemes which reduce communication complexity in the simultaneous message passing model.) A string of $O(Cn)$ bits can thus be encoded by vectors in H^n, such that the overlap between the code vectors for two distinct strings is always less than $\sin\theta$, suggesting the following bit string commitment protocol.

Commitment: Let N be the number of bits that can be encoded in H^n by the above construction. To commit a string $a_1 \ldots a_N$ of bits to B, A sends the state $v_{a_1 \ldots a_N}$, treating the index as a binary number.

Unveiling: To unveil, A simply declares the values of the string bits, and hence the state sent. Assuming that B has not disturbed the qubits, he can test A's claim at unveiling by measuring the projection onto $v_{a_1 \ldots a_N}$. If he obtains eigenvalue 1, he accepts the unveiling as an honest revelation of a genuine commitment. If he obtains eigenvalue 0, he concludes that A has cheated.

Security against A: As before, once A transmits a quantum state to B, its density matrix ρ is fixed. Consider some set $i_1, \ldots, i_r$ of bit strings which A might wish to maintain the option of revealing after commitment. Let P_i be the projection onto v_i, let $p_i = \mathrm{Tr}(\rho P_i)$ be the probability of A successfully revealing string i, and write

$$Q = P_{i_1} + \ldots + P_{i_r} \,. \tag{4}$$

It is easy to verify that

$$\mathrm{Tr}(\rho Q) \leq (1 + \epsilon + \epsilon^2 r)/(1 - \epsilon) \,. \tag{5}$$

In other words,

$$p_{i_1} + \ldots + p_{i_r} \leq 1 + f(\epsilon, r) \,, \tag{6}$$

where, for any fixed r, f can be made as small as desired by choosing θ suitably small.

So, given that A is determined to reveal a bit string from some finite set of size r, her scope for cheating is limited to increasing the probability of revealing any given element of the set by a fixed amount. For any fixed r, that amount can be made arbitrarily small by choosing the security parameters appropriately. If B's concern is to prevent cheating of this type, for some predetermined r, the protocol can guarantee him security.

Security against B: Holevo's theorem implies that the information about the $N \approx Cn$ bit string accessible to B is at most $\log n$ bits.

V. DISCUSSION

The bit string commitment protocols above use the properties of quantum information to guarantee strong levels of security to both the committer and receiver. They highlight another cryptographic application of quantum information: no (non-relativistic) classical protocol can guarantee such security. They also highlight the fact that quantum cryptography can introduce distinctions between tasks which are classically equivalent, such as bit commitment and bit string commitment.

As a metaphor for the cryptographic uses of bit string commitment, consider a situation in which A knows the combination to a lock, wants to be able to prove to B in future that she knows it now, but does not want to give B the ability to open the lock now. If she sends a bit string commitment of the combination now, she can prove her present knowledge later by opening the commitment. However, B, who can only get partial information about the committed string, will not be able to deduce the combination from it. If the combination is sufficiently long, the security parameters for the bit string commitment are appropriately chosen, and A knows how fast B can try possible combinations, she can ensure that B remains sufficiently ignorant about the combination to be almost certainly unable to break the lock during some fixed interval of her choice. More generally, bit string commitment allows a sort of "partial knowledge proof", in which A can establish to B her possession of some information (for instance, the proof of a theorem) while restricting the amount of information B can obtain.

VI. ACKNOWLEDGEMENTS

This work was supported by the European collaboration EQUIP.

[1] S. Wiesner, SIGACT News **15** (1983) 78.

[2] C.H. Bennett and G. Brassard, in *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing* (IEEE, New York, 1984), p. 175.

[3] G. Brassard, C. Crépeau, R. Jozsa and D. Langlois, in *Proceedings of the 34th Annual IEEE Symposium on the Foundation of Computer Science* (IEEE Comp. Soc., Los Alamitos, California, 1993), p. 362.
[4] G. Brassard and C. Crépeau, in *Advances in Cryptology: Proceedings of Crypto'90*, Lecture Notes in Computer Science Vol 537 (Springer-Verlag, Berlin, 1991), p. 49.
[5] H.-K. Lo and H. Chau, Phys. Rev. Lett. **78** (1997) 3410.
[6] D. Mayers, Phys. Rev. Lett. **78** (1997) 3414.
[7] D. Mayers, quant-ph/9603015.
[8] H.-K. Lo and H. Chau, Physica D **120** (1998) 177.
[9] H.-K. Lo, Phys. Rev. A **56** (1997) 1154.
[10] D. Mayers, in *Proceedings of the Fourth Workshop on Physics and Computation* (New England Complex System Inst., Boston, 1996), p. 226.
[11] G. Brassard, C. Crépeau, D. Mayers and L. Salvail, quant-ph/9806031.
[12] A. Kent, Phys. Rev. Lett. 83 (1999) 1447-1450.
[13] A. Kent, quant-ph/9906103, submitted to J. Cryptology.
[14] A. Kent, Phys. Rev. A 61, 042301 (2000).
[15] A. Kent, Phys. Rev. Lett. 83 (1999) 5382-5384.
[16] A. Yao, in *Proceedings to the 26th Symposium on the Theory of Computing*, June 1995, pp. 67-75.
[17] L. Salvail, in *Proceedings of Crypto'98*, Lecture Notes in Computer Science Vol 1462 (Springer-Verlag, Santa-Barbara, 1998) pp. 338-353.
[18] L. Hardy and A. Kent, quant-ph/9911043
[19] D. Aharonov, A. Ta-Shma, U. Vazirani and A. Yao, "Quantum Bit Escrow", in *Proceedings of the 32nd Annual ACM Symposium on the Theory Of Computing* (2000).
[20] A. Holevo, "Statistical problems in quantum physics", in *Proceedings of the Second Japan-USSR Symposium on Probability Theory*, ed. by G. Maruyama and J. Prokhorov (Springer-Verlag, Berlin, 1973).
[21] J. Conway and N. Sloane, *Sphere Packings, Lattices and Groups*, 2nd edition, (Springer-Verlag, New York, 1993)
[22] J. Justesen, IEEE Trans. Info. Th. **18** 652 (1972).
[23] H. Buhrman, R. Cleve, J. Watrous and R. de Wolf, "Quantum Fingerprinting", quant-ph/0102001.