Quantum Bit Commitment

Naya Nagy and Marius Nagy

College of Computer Engineering and Science
Prince Mohammad Bin Fahd University
Al Azeziya, Eastern Province, KSA
mnagy@pmu.edu.sa

School of Computing, Queen’s University
Kingston, Ontario, Canada
{nagy,marius}@cs.queensu.ca

Abstract. This paper is reversing the current belief on Quantum Bit Commitment. Several papers have claimed and given a formal proof that quantum bit commitment is impossible. Nevertheless, the hypotheses of the formal mathematical model are too restrictive and do not exhaustively reflect the original definition of the problem. They share the same unnecessary restriction that the responsibility of hiding information and committing to a bit value is attributed to the same communicating partner. The protocol described here fully abides to the original description of the bit commitment problem. The two communicating partners share responsibilities, one partner is mostly responsible for hiding information and the other one for committing to the bit value. The security of the protocol derives from quantum properties such as the unclonability of unknown states, the indistinguishability of non-orthogonal states and also from randomly discarding and permuting qubits. The protocol is safe from classical attacks and quantum attacks using entanglement. The level of security can be made arbitrarily large by using more qubits. This result opens the door for a whole set of cryptographic applications using bit commitment as a building block: remote coin tossing, zero-knowledge proofs and secure two-party computation.

Keywords: bit commitment, protocol, quantum, measurements, permutation, entanglement.

1 Introduction

The field of quantum cryptography is best known for its results in two major directions: key distribution and bit commitment. It is interesting to note that the foundations of both directions were laid in the same seminal paper by Bennett and Brassard in 1984 [1]. However, the destinies of the two results would prove to be far from similar. A variety of quantum key distribution protocols were proposed after the initial BB84, making key distribution the most successful practical application of quantum mechanics to information processing.

On the other hand, things were not so straightforward with quantum bit commitment. The classical problem of bit commitment can be described intuitively
as follows. Alice places a bit of her choice into a "safe" or "box" that she locks up, before handing it over to Bob (the commit step). By guarding the "box", Bob makes sure that Alice cannot change the bit she committed to. At a later time, when Bob wants to find out the value Alice has locked in the box, he asks Alice for the key (the decommit step). From the very beginning (BB84) it was realized that entanglement would offer the ideal attack strategy on any quantum bit commitment protocol, allowing someone to actually avoid commitment right until the decommit step. Researchers in the field have tried ever since to somehow circumvent this difficulty by resorting to a wide range of ideas, from some clever use of measurements and classical communication to combining quantum mechanics with other physical theories in order to achieve their goal.

Perhaps the best known exponent of the early efforts to achieve an unconditionally secure protocol for quantum bit commitment was the BCJL protocol, developed in 1993 [4]. The future was looking bright for quantum cryptography following this result, since many important applications could be realized based on bit commitment (see [6] for example). The bad news came in 1996, when Mayers [10] and, independently, Lo and Chau [8] discovered a flaw in the BCJL protocol. Even worse, Mayers proved a more general result, stating that an unconditionally secure quantum bit commitment protocol is impossible [11].

It may have been the importance of bit commitment for the general field of cryptography or the intuition that the success of quantum key distribution could be replicated for quantum bit commitment that still pushed people to look for a solution. Several protocols were proposed that try to restrict the behavior of the cheater in some way so as to obtain a secure bit commitment scheme [3, 5, 7]. It turned out that all these protocols were falling under the scope of Mayers’ impossibility result. This led to a general belief that the principles of quantum mechanics alone cannot be used to create an unconditionally secure bit commitment protocol. Therefore, recent advances on the topic either exploit realistic physical assumptions like the dishonest party being limited by “noisy storage” for quantum information [12] or combine the power of Einstein’s relativity with quantum theory [9]. Secure bit commitment using quantum theory alone is still believed to be impossible.

The difficulty of the problem stems from the lack of trust between the parties. Alice may want to defer commitment until the decommit phase and Bob may want to find out Alice’s commitment during the commit phase. First, Alice should be forced to commit during the commit phase, and Bob should be secure of the necessity of Alice’s commitment. Bob should be able to test Alice’s fairness. Secondly, Bob should not have enough information to allow him to find Alice’s commitment during the commit phase. Alice should be able to ensure that she is not revealing too much information to Bob.

These two major properties of any correct quantum bit commitment solution, namely, binding Alice to her choice and hiding this choice from Bob, are considered mutually exclusive by Mayers. He states that in any protocol that is hiding, the quantum states of the safe containing either 0 or 1 must be very similar (if not identical) since otherwise Bob would be able to discern the dif-
ference and gain knowledge about the committed bit prematurely. But the very fact that the two states are virtually the same gives Alice the possibility to keep her options open and postpone her *commitment* for later on.

In this paper, we show that quantum bit commitment is indeed possible if Alice and Bob share the responsibilities of ensuring binding and concealing: Alice is responsible to hide her choice, while Bob must make sure that Alice cannot change her mind in the decommit step. Both properties can be achieved by resorting to incomplete information. Thus, the quantum state of the "safe" does not have to be identical (or close to identical) for the two possible values of the committed bit, but they have to *appear* as such to Bob, because he does not have complete information about it. Similarly, incomplete information about the "structure" of the "safe" prevents Alice from cheating in the decommit step. Thus, the key to achieving bit commitment through quantum means lies in a protocol in which none of the two parties has complete information on the "safe" throughout the entire commit phase.

The remainder of this paper is organized as follows. The next section describes in detail the steps Alice and Bob should go through when they want to honestly execute our quantum bit commitment protocol. Section 3 analyzes the security of the protocol, proving that it is both binding and concealing. In particular, we show how Bob can enforce the binding property without compromising the concealing property. A discussion on why this protocol falls outside the scope of Mayers impossibility result is offered in section 4. The main ideas that made this result possible and its significance for the field of quantum cryptography are summarized in the concluding section.

## 2 Protocol Description

We choose to describe our protocol in general terms, without restricting to a particular physical embodiment for a qubit (such as photon polarization or particle spin). Consequently, in what follows we will refer to \( \{ |0\rangle, |1\rangle \} \) as the normal computational basis and to \( \{ H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), H|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \} \) as the Hadamard basis.

### 2.1 Commit Phase

The Commit Phase, depicted in Fig. 1, is comprised of the following steps:

1. Bob generates a sequence of \( N \) qubits in the state \( |0\rangle \otimes |0\rangle \otimes \cdots \otimes |0\rangle \otimes H|0\rangle \otimes H|0\rangle \otimes \cdots \otimes H|0\rangle \), where \( N \) is some positive even integer. The first \( N/2 \) qubits in the sequence are all in state \( |0\rangle \), while the qubits in the second half are all in state \( H|0\rangle \). Bob sends a random permutation of this sequence to Alice. This step is repeated \( M \) times (for some positive integer \( M \)), such that in the end Alice will have received from Bob \( M \) sequences, each sequence consisting of \( N/2 \) qubits in state \( |0\rangle \) and \( N/2 \) qubits in state \( H|0\rangle \), in random order. In an intuitive description of this step, Bob hands out to Alice a number of
$M$ "boxes", each different from the others (different permutation), yet all sharing the same characteristics (an equal number of qubits in each of the two possible states).

2. Alice verifies that the "boxes" she received correspond to the agreed specifications. In detail, one of the $M$ sequences ("boxes") received is saved for the actual commit step, while all remaining sequences are verified in order to determine if Bob executed the protocol honestly. For each of the $M-1$ sequences selected for verification, Alice asks Bob to disclose, qubit by qubit, whether it was prepared in state $|0\rangle$ or in state $H|0\rangle$. Then, she can proceed to measure each qubit in the proper basis: the normal computational basis for a $|0\rangle$ qubit and the Hadamard basis for a $H|0\rangle$ qubit. In the first place, in each group (or sequence), $N/2$ qubits must have been prepared in state $|0\rangle$ and $N/2$ in state $H|0\rangle$. Secondly, all measurements must yield a value of 0, otherwise Bob has not been honest in telling the states in which the qubits were prepared. If both conditions are satisfied, Alice is confident that Bob has abided by the protocol rules and as such, she concludes that the last ($M$-th box) also contains $N/2$ qubits in state $|0\rangle$ and $N/2$ qubits in state $H|0\rangle$ in a random order. Alice then proceeds to the next step. Otherwise, if Alice’s test fails, the protocol is abandoned as Bob has been proven dishonest.

3. The only sequence left after the verification step is the box used by Alice to hide the committed bit inside. If Alice decides to commit to 0, she leaves the qubits in the sequence untouched, while in the case of a commitment
to 1, she applies a Hadamard gate to all $N$ qubits composing that last sequence. Finally, she randomly permutes the qubits before sending them to Bob. Applying the Hadamard gate or not corresponds to placing the committed bit inside the box, while the random permutation of the qubits amounts to "locking the box".

4. Bob measures each received qubit either in the normal computational basis or in the Hadamard basis. The choice is random for each measured qubit. Bob records the outcome of each measurement and awaits the Decommit phase.

2.2 Decommit Phase

When Alice wants to unveil the bit she committed to, she has to disclose to Bob, for each of the $N$ qubits sent, its index in the original sequence. In order to be satisfied that Alice executed the protocol honestly, Bob proceeds to the following verification.

Based on the index information provided by Alice, Bob can determine for each qubit if it was measured in the "correct" basis or not: for a qubit that was originally in state $|0\rangle$ the correct basis is the normal computational basis, while for a qubit whose state was originally $H|0\rangle$ the correct basis is the Hadamard basis. Now, if Alice committed to 0, all the qubits measured in the "correct" basis must yield a value of 0. The other measurements will yield a 0 or a 1 with equal probability. On the other hand, if Alice committed to 1, then the qubits measured "incorrectly" must all yield a value of 0 and the others have an equal chance to be observed as 0 or as 1. Any other scenario for the measurement outcomes (in the ideal case of an error-free environment) points to a dishonest participant to the protocol.

3 Correctness

The protocol described above is both binding and concealing. Let us start by showing the concealing property first.

3.1 Concealing Property

Since Bob is the one initiating the protocol, it appears that he is in the position to set things to his advantage. In theory, he could distinguish between a commitment to 0 and a commitment to 1, if the sequence selected as "the box" is not balanced between $|0\rangle$ and $H|0\rangle$ states. The closer we are to a constant sequence (all qubits $|0\rangle$ or all qubits $H|0\rangle$), the higher the chances for Bob to guess the committed bit correctly. Consider, for example, a sequence (box) made up of $N$ qubits, all in state $|0\rangle$. If Alice commits to 0, this exact sequence is sent to Bob, otherwise a sequence made up of $N$ qubits in state $H|0\rangle$ will be sent. Bob, when receiving the $N$ qubits, measures all of them in the normal computational basis. If all measurements yield a 0, Bob is highly confident that the committed bit is
0 because, for a commitment to 1, he expects a 50 – 50 probability distribution between 0 and 1 in the outcomes obtained.

In summary, Bob’s chances to correctly guess the committed bit are directly proportional to how unbalanced the sequence selected to act as the box is. Thus, the probability of a correct guess varies between 0.5 (completely random guess) and a value which can be brought as close to 1 as desired by increasing the number of qubits in the sequence. This is also reflected in how close the density matrix corresponding to a commitment to 0 is to the density matrix for the case where Alice commits to 1. For a balanced sequence, the two density matrices are identical:

$$\rho_0 = \frac{1}{2} |0\rangle\langle 0| + \frac{1}{2} |1\rangle\langle 1| = \frac{1}{2}(|0\rangle + |1\rangle)(\langle 0| + \langle 1|\sqrt{2} ) + \frac{1}{2}(|0\rangle - |1\rangle\sqrt{2} )\langle 0| = \rho_1. \quad (1)$$

On the other hand, the density matrices are at a maximum distance from one another when the sequence is constant.

Now, Bob faces the following dilemma in his cheating strategy: the more counterfeited boxes he prepares (sequences that are not balanced between $|0\rangle$ and $H|0\rangle$), the more chances one of them will be used by Alice, but at the same time the more chances to be detected by Alice during the verification step. Formally, we can distinguish between the following two cases:

1. Bob chooses to play safely and from the $M$ sequences prepared, only a constant number, say $c$, do not correspond to the agreed specifications. Here, constant means that, always, only $c$ sequences are ”counterfeited”, regardless of what the value for $M$ is. In this situation, the probability $\varepsilon_1$ that Alice will choose one of the counterfeited boxes to place the committed bit inside can be made infinitesimally small by increasing $M$ (the number of boxes she chooses from):

$$\varepsilon_1 = \frac{c}{M} \quad (2)$$

Thus, for a maximum allowed probability of picking a counterfeited box $\varepsilon_1$, the total number of boxes must satisfy the inequality:

$$M \geq \left\lceil \frac{c}{\varepsilon_1} \right\rceil \quad (3)$$

For example, suppose that Bob always prepares $c=10$ counterfeited boxes and we would like to limit the probability of picking a counterfeited box to $\varepsilon_1 = 0.01$. Then the total number of boxes to choose from should be at least 1000.

2. Bob plays aggressively and from the $M$ boxes prepared, a certain fraction $f$ are counterfeited. In this case, even if one of the counterfeited boxes is set aside by Alice for the commit step, the other $f \cdot M - 1$ will undergo the verification step. By definition, a counterfeited box is a sequence in which
at least one qubit does not correspond to the agreed specifications. What is the actual state of such a qubit is irrelevant, as long as there is a certain non-zero probability $p$ that Alice will catch Bob when verifying that qubit. Again, by increasing the value of $M$, the probability of catching Bob can be brought as close to 1 as desired, or equivalently, the probability $\varepsilon_2$ of Bob escaping detection can be made arbitrarily small:

$$\varepsilon_2 = (1 - p)^{M^{-1}}$$

Therefore, if we want to keep the probability of Bob escaping detection to at most $\varepsilon_2$, then a lower bound on the total number of boxes used in the protocol is given by

$$M \geq \left\lceil \frac{1 + \log_2(1 - p) \varepsilon_2}{\varepsilon_2} \right\rceil$$

Note that the above formula assumes that there is just one "incorrect" qubit in each counterfeited box. If there are more, like, for example, the whole sequence is constant, then the lower bound is obviously smaller. Also, the number of counterfeited boxes does not have to vary linearly with $M$, the analysis remains valid for any increasing function of $M$. Going through a concrete example again, let us assume that 10% of the boxes prepared by Bob are counterfeited and there is a 25% chance of detecting a "forged" qubit when verified. Under these circumstances, in order to catch Bob with a probability of 99%, the total number of boxes to choose from should be at least 171.

Consequently, there is no winning strategy for Bob: with an arbitrarily high probability (controlled by the value of parameter $M$), either he will be detected as dishonest or none of his counterfeited boxes will be selected by Alice. This result can be formally expressed as the following theorem:

**Theorem 1** \( \lim_{M \to \infty} \varepsilon_1 \cdot \varepsilon_2 = 0 \)

**Proof.** The proof follows from the two cases discussed above. The more counterfeited boxes Bob prepares, the higher the chances he will be caught. In other words, in order to keep the probability of escaping detection above a certain threshold $\tau$

$$\lim_{M \to \infty} \varepsilon_2 \geq \tau,$$

Bob cannot create more than a certain number $\eta$ of counterfeited boxes (where $\eta$ is a function of $\tau$). But in that case, the chance to select one of the counterfeited boxes to place the bit inside drops to zero as $M$ grows unbounded:

$$\lim_{M \to \infty} \varepsilon_1 = \lim_{M \to \infty} \frac{\eta}{M} = 0.$$

$\square$
Note that in the above analysis, Bob is free to use any states he wants, with no restrictions. Even entangled states will do him no good, since all measurements performed by Alice must consistently yield a 0, with no exception. There is no entangled state that will always be observed as 0, no matter how it is measured.

3.2 Binding Property

The only chance for Alice to postpone commitment until the decommit phase is to know the "structure" of the "box" she has used, that is, to know exactly what the quantum state of each qubit is in the sequence received from Bob. That way, when Bob asks for the index of each qubit received and measured, she can always pick a convenient index in the sequence, corresponding to a qubit that matches her late commitment. Unfortunately for Alice, there is no reliable way of distinguishing between $|0\rangle$ and $H|0\rangle$, as they are non-orthogonal quantum states. Without this knowledge, if she tries to be dishonest, there is always a probability of being revealed as a cheater for each qubit verified by Bob. Therefore, by increasing the value of $N$ (number of qubits composing each sequence), the probability of catching a dishonest Alice can be made arbitrarily high:

$$\lim_{N \to \infty} (1 - p^N) = 1,$$

where $p = 0.75$ is the probability per qubit that Alice passes Bob’s verification.

Again, note that entanglement is of no use to Alice, since no entangled state will consistently collapse (when measured) to the outcome expected by Bob.

4 Discussion

Since we have just shown that bit commitment through quantum means alone is still possible, despite a contrary belief that has lasted for almost 20 years, the obvious question is: How can this result be reconciled with Mayers’ impossibility result? The answer can be found in the framework in which that result was obtained, a framework that is not general enough to encompass all possible protocols. To be more explicit, Mayers shows that in any protocol that is concealing, Alice can cheat in a modified procedure $\text{commit}'$ by keeping everything at the quantum level and "never sending a register away to the environment except when this register contains a classical bit that she must transmit to Bob via the environment, using the phone for instance" [11]. The same is assumed for Bob in a modified procedure $\text{commit}". Under these assumptions, the fact that the expected value of the fidelity between the reduced density matrices on Bob’s side is arbitrarily close to 1 implies that Alice can apply a unitary transformation to steer the quantum state of her subsystem towards 0 or 1 in the decommit phase.

Our protocol does not fit this framework, because a key ingredient in it is the fact that both Alice and Bob have to keep classical information (in the commit phase) that is not to be sent to the other party. This classical information is the
missing information that prevents the other party from cheating. At the end of
the Commit Phase, all information in the system is actually classical, and Alice
cannot transform the state of the system from 0 to 1 without the information in
Bob’s custody (that is, the original quantum states of the qubits composing the
box chosen). Similarly, Bob cannot distinguish between a box containing a 0 and
a box containing a 1 without knowing the permutation applied by Alice. Because
no reduction exists that transforms our protocol into an equivalent one in which
no classical information is required (except for what needs to be communicated
classically), this protocol falls outside the scope of Mayers impossibility result.

5 Conclusion

We showed in this paper how a secure quantum bit commitment protocol can be
realized. The key idea that made this result possible was that at any time during
the protocol before the decommit phase, none of the two parties has complete
information on the box used to hide the committed bit. Although the box is
quantum in nature, the ”description” of the box is distributed to both Alice and
Bob, as classical information. Without knowledge of the information stored by
the other party, none of them is capable of mounting an effective cheating strat-
egy. The quantum nature of the box is essential because quantum mechanical
properties, like unclonability and indistinguishability of non-orthogonal quantum
states, are essential to ensuring the security of the protocol. Our scheme comes
with two security parameters, each controlling one of the two critical properties
of the protocol. The number \(M\) of boxes (or sequences) created initially by Bob
controls the concealing property: the higher the value of \(M\), the lower the proba-
bility of Bob being able to cheat and identify the committed bit prematurely.
The number of qubits in a sequence (or the size of the box), on the other hand,
controls the binding property: the larger the value for \(N\), the lower the proba-
bility that Alice will guess correctly the ”structure” of the box and thus, be able
to pick the value of the bit in the decommit phase. A secure bit commitment
protocol realizable through quantum means alone has huge implications for the
field of quantum cryptography. Remote coin tossing, which might be used for
long-distance gambling, is immediately realizable based on bit commitment (see
[2] for example). Quantum oblivious mutual identification [6], another important
result built on secure quantum bit commitment can be exploited to avoid frauds
from typing PIN codes to dishonest teller machines. Other applications may
range from ensuring the security of remote voting to global financial trading.
The future looks bright again for the field of quantum cryptography.

References

1. Charles H. Bennett and Gilles Brassard. Quantum cryptography: Public key dis-
tribution and coin tossing. In Proceedings of IEEE International Conference on
Bangalore, India, December 1984.


