# Quantum Bit Commitment

Essay for the lecture "Introduction to Quantum Computing",
University of Edinburgh, 3 November 2016

Lukas Convent

This essay forms the coursework of the "Introduction to Quantum Computing" lecture taught by Petros Wallden at the University of Edinburgh in 2016. We give a short overview of bit commitment and its field of application and then focus on how quantum computing can be harnessed for its implementation. After describing why this cannot be done in an unconditionally secure way, we describe how quantum bit string commitment can be used as an approximation.

## 1 Bit Commitment

Bit commitment refers to the concept of committing to a bit, best explained at the example of Alice and Bob. Alice wants to commit to a bit, i.e. Bob gets the guarantee (commitment) that she has decided on a bit without initially learning its value. At a later point, Alice reveals the value she has committed to and Bob should be able to verify that she tells him the true value, using the commitment.

In a simple (but typical) formal setting, we can describe the procedure by a function $f(p, b)$, which takes a parameter $p$ (generated by Alice) and the bit $b$ to be committed and generates the commitment. We can then identify two phases of bit commitment:

- **Commit phase**. Alice produces a parameter $p$ (this could be a random value) and chooses her bit $b$. She then sends her commitment $f(p, b)$ to Bob.
- **Opening phase**. Alice send her bit $b$ to Bob. Bob verifies that $f(p, b)$ is the same as the commitment.

Two properties are important to make a bit commitment procedure useful:

- **Hiding property**. Bob should not be able to infer the bit value $b$ from $f(p, b)$.
- **Binding property**. Alice should not be able to find another parameter $p'$ and choose the opposite bit $b \oplus 1$ to generate the same commitment, obtaining $f(p, b) = f(p', b \oplus 1)$.

These two properties can now be implemented on different security levels. One labels a property **computationally** secure if it is not expected to be efficiently violable. One labels a property **perfectly** secure if the procedure intrinsically respects it, i.e. no computation at all could help violating it. A trivial example of a perfectly hiding procedure is the constant commitment function $f(p, b) = c$ (at the same time lacking the binding property), a trivial example of a perfectly binding procedure is the identity function $f(p, b) = b$ (at the same time lacking the hiding property).

It turns out that in a classical setting, i.e. without making use of quantum mechanics, finding a protocol which is both perfectly hiding and perfectly binding is not possible. We describe in the next section why this impossibility theorem extends also to settings in which quantum computation is admitted. Before that, in the next paragraph, we emphasize the general importance of bit commitment as a building block for different cryptographic applications.

### 1.1 Applications

Bit commitment can be generalized to commitment procedures for strings of arbitrary size, which are then referred to as **commitment schemes**. They are used in many domains where trust is an issue. A classical example is the coin flipping protocol, where Alice and Bob have to guess the result of a single coin flip, with only one of them having access to the physical coin. By being able to commit to a guess, trust can be established. Another common application is that of committing to a secret, but only revealing parts of it. This way, the verifier can check that the committing party knows the secret, but does not gain knowledge of its whole content. This scenario is used in zero-knowledge proofs and verifiable secret sharing [2].

## 2 Impossibility of Quantum Bit Commitment

Quantum bit commitment refers to protocols which rely on the quantum effects of unitary operations/measurements on qubits and in some sense also on the phenomenon of entanglement. Only in 1997 by Mayers [7] and independently in 1998 by Lo and Chau [6] it was shown that perfect quantum bit commitment is not possible. In the following, we first give an example of a quantum bit commitment protocol, using a protocol introduced by Kent [4]. We present how this protocol was meant to be invulnerable against EPR attacks and how an attacker nevertheless can outperform the defense mechanism and still succeed by an EPR attack. Finally, we describe how this pattern can be applied to any quantum bit commitment protocol.

### 2.1 Kent's Protocol

Alice wants to commit to a bit in front of Bob. The protocol makes use of two different bases $b_0 := \{|0\rangle, |1\rangle\}$ and $b_1 := \{|+\rangle, |-\rangle\}$ which allows harnessing quantum mechanics in the following way: If a qubit is in one of these four basis states and we measure it in the wrong basis, it destroys the state (leading to an unpredictable outcome). On the other hand, measuring in the right basis can be used to verify the value it represents. We first present a simpler version of the protocol (as it is described by Bennett and Brassard [1]) and then refine it to the version which is described by Kent [4]:

**Commit phase.** Alice sends Bob a number of qubits $x_1, ..., x_n$ which are each randomly selected from the four basis states $|0\rangle, |1\rangle, |+\rangle, |-\rangle$. Alice commits her bit $b$ by first tagging each qubit $x_i$ with its corresponding basis (i.e. 0 if its state belongs to $b_0$ and 1 if its state belongs to $b_1$), resulting in a bit string $\langle t_1, ..., t_n\rangle$ of length $n$. The commitment $c$ is then this bit string or its flipped version, depending on Alice's chosen bit: $c = \langle t_1 \oplus b, ..., t_n \oplus b\rangle$. Having received $c$ from Alice, Bob cannot infer any information about $b$, as in either case (i.e. either chosen base), the density matrices are the same. This guarantees a perfect hiding property.

**Opening phase.** Alice announces the following to Bob: First, her chosen bit $b$, which tells Bob in which base he can measure each qubit $x_1, ..., x_n$: If $b = 0$, he can measure $x_i$ in the base $b_{c_i}$. If $b = 1$, he can measure $x_i$ in the base $b_{c_i \oplus 1}$. Second, she announces the encoded states, i.e. whether a qubit was in state $|0\rangle$ or $|1\rangle$ (resp. $|+\rangle$ or $|-\rangle$). Bob can now verify that his measurements coincide with the opening information he received. If Alice had cheated and changed her bit $b$, she would have to guess the outcomes of the qubits when measured in the "wrong" bases by Bob, which is nearly impossible if $n$ is sufficiently large. Assuming that the states sent by Alice in the commit phase were really only out of the four basis states, this guarantees a perfect binding property.

As hinted at, by sending entangled states instead of the basis states, Alice can break the binding property of the protocol. This attack is called Einstein-Podolsky-Rosen attack, because by generating EPR pairs that are maximally entangled, Alice can send over one half of the pairs and keep the other half as a local copy. She only needs to decide on her bit value in the opening phase. Measuring all her local qubits in the suitable bases, she determines and discovers the outcome of Bob's measurements and can therefore predict the right values. Kent's protocol was meant to defeat this attack by the following defense mechanism (which is insufficient as will be described):

**Verification during the commit phase.** The following modification is made to the commit phase: Instead of merely sending over basis states, Alice classically commits to the base and the encoded value of every one of them. The crucial point here is that the classical commitment only needs to be secure during the commit phase, i.e. for a short period of time. Of all the transmitted qubits, Bob can now choose a subset of them to verify that Alice is not cheating: He asks Alice to reveal the base and value of the chosen qubits, measures them on his own and checks if his measurements coincide with Alice's claims.

## 2.2 Breaking Kent's Protocol

We describe now how Alice can break the protocol described above. The description follows a detailed explanation given by Brassard et al. [3].

The central idea is that Alice prepares quantum states which allow the classical commitment to be carried out on a quantum level. This requires to entangle the qubits needed for the classical commitment with the qubit that is sent over to Bob. Let $f_{\theta v}$ be the four classical commit functions, with $\theta \in \{0, 1\}$ denoting the base $b_\theta$ and $v \in \{0, 1\}$ denoting the encoded value. Because Alice wants to bypass committing to a value $v$, she prepares three more qubits for every qubit she sends over to Bob. This results in four registers $r_w$, $r_f$, $r_z^A$ and $r_z^B$, whose qubits she entangles in the following way:

$$|\gamma(\theta)\rangle = \frac{1}{\sqrt{2^{n+1}}} \sum_{w \in \{0,1\}^n} |w\rangle \; |f_{\theta 0}(w)\rangle \; |0\rangle_\theta \; |0\rangle_\theta \;\; + \;\; |w\rangle \; |f_{\theta 1}(w)\rangle \; |1\rangle_\theta \; |1\rangle_\theta$$

The last two registers $r_z^A$ and $r_z^B$ serve the same purpose as it is the case for an ordinary EPR pair. To generate the classical commitment, Alice measures the register $r_f$. She does so without determining her value, i.e. the sum keeping $|0\rangle_\theta |0\rangle_\theta$ and $|1\rangle_\theta \; |1\rangle_\theta$ in superposition does not collapse. During the verification phase, when Bob asks Alice to unveil her commitment, Alice measures the $r_w$ register and the $r_z^A$ register in the basis $\theta$. Only at this point the "sum" collapses and Alice's measurement of register $r_z^A$ will be the same as Bob's measurement of $r_z^B$.

In the opening phase, she can disentangle two of the four registers and then measure the same outcomes as Bob does. Since the $r_f$ register is already measured, she only needs to disentangle the qubit representing the $r_w$ register. She can erase the value by an appropriate unitary operation, but since $r_w$ stores the input of the commitment function, she needs to invert the function $f_{\theta 0}$ (resp. $f_{\theta 1}$) for the measured commitment value of $r_f$. This inversion is a computationally hard problem, and because it is not performed during the short time of commitment only, the protocol cannot be seen as perfect.

### 2.3 General impossibility

The no-go theorem of Mayers [7] and Lo and Chau [6] generalize this result for any quantum bit protocol. The argument is based on the fact that every classical computation (like the commitment for the verification phase in Kent's protocol) can also be done on a quantum level through unitary operations. This way, by finding the right unitary operation (this could be a hard problem like in Kent's protocol) Alice obtains an EPR pair, making Bob's measurements totally transparent.

## 3 Generalization: Quantum Bit String Committment

There are some ways of how to approximate quantum bit commitment. One possibility is described by Kent's "Quantum Bit String Commitment"[5]. The idea is a generalization of bit commitment to bit string commitment, i.e. the task of committing to $n$ qubits $a_1, ..., a_n$. The security level is defined through another number $m < n$, the number of bits that Bob can extract from the commitment. For the single bit commitment, we have $n = 1$ and $m = 0$. As Kent argues in his paper, classically there is no real difference between the two since one can be simulated through the other (by repetition or by suitable encoding).

In the quantum analogue though, there is a difference between the two. First of all, committing to a single bit is impossible, as it was described [7]. When committing to several bits though, one can ensure a perfect binding property and a certain degree of hiding. The reason for guaranteeing that only some information will leak lies in the fact that quantum measurements disturb the state, limiting the number of sensible measurements for Bob [5].

## References

[1] Charles H. Bennett and Gilles Brassard. Quantum cryptography: Public key distribution and coin tossing. 560:7–11.

[2] Gilles Brassard, David Chaum, and Claude Crpeau. Minimum disclosure proofs of knowledge. 37(2):156–189.

[3] Gilles Brassard, Claude Crpeau, Dominic Mayers, and Louis Salvail. A brief review on the impossibility of quantum bit commitment.

[4] Adrian Kent. Permanently secure quantum bit commitment from a temporary computation bound.

[5] Adrian Kent. Quantum bit string commitment. 90(23):237901.

[6] Hoi-Kwong Lo and Hoi Fung Chau. Why quantum bit commitment and ideal quantum coin tossing are impossible. 120(1):177–187.

[7] Dominic Mayers. Unconditionally secure quantum bit commitment is impossible. 78(17):3414.