Quantum Bit Commitment from a Physical Assumption

Louis Salvail[1] *

BRICS, Basic Research in Computer Science of the Danish National Research Foundation, Department of Computer Science,University of Århus, Ny Munkegade, building 540,DK-8000 Århus C, Denmark.
salvail@daimi.aau.dk

Abstract. Mayers and independently Lo and Chau have shown that unconditionally secure quantum bit commitment is impossible. In this paper we show that under the assumption that the sender is not able to perform generalized measurements involving more than n qubits coherently (n-coherent measurements) then quantum bit commitment is possible. A commitment scheme is δ-binding if for each execution there is an $\tilde{x} \in \{0,1\}$ that cannot be unveiled with probability of success better than δ. Our bit commitment scheme requires the transmission of N qubits and is δ-binding, for any $\delta > 0$, if the committer can only carry out n-coherent measurements for some $n \in \Omega(N)$. For some $\alpha > 0$, the scheme is $2^{-\alpha N}$-binding against n-coherent measurements for some $n \in \Omega(\sqrt{N})$. The security against malicious receivers is unconditional.

1 Introduction

The first application of quantum mechanics in cryptography was proposed by Wiesner [34] in the late 1960's through what he called "quantum multiplexing". Classically, this primitive has been reinvented a decade later by Rabin [32] as one-out-of-two oblivious transfer. The power of oblivious transfer is known to provide the sufficient and necessary tool for solving the very general secure two-party computation problem[20, 15]. In its original paper [34], Wiesner describes an attack based on generalized quantum measurements against its own scheme. Although proven insecure, Wiesner's scheme requires a quantum attacker with technology far beyond what is achievable today. In 1984, Bennett and Brassard proposed two new cryptographic applications of quantum mechanics: secret-key exchange and coin flipping by telephone [3]. Whilst the former is still strongly believed to be secure [25, 7] the latter was already known to be breakable using EPR pairs [16, 3]. The proposed coin flipping protocol can be modified easily to implement a quantum bit commitment scheme that can indeed be defeated by the same EPR attack [9]. Unlike Wiesner protocol, the attack is conceivable using today's technology [1]. Some attempts to find a quantum bit commitment scheme not suffering the same weaknesses have then been made [9, 10]. In 1993, Brassard, Crépeau, Jozsa and Langlois [10] proposed a quantum commitment

* Part of this work has been done while the author was at CWI.

scheme (the BCJL scheme) that was claimed to be unconditionally secure until Mayers discovered a subtle flaw in 1995 [26]. This was bad news considering Yao [35] had provided a proof that, under the assumption that secure bit commitment scheme exists, the BBCS protocol [5] for quantum oblivious transfer(QOT) is secure. Despite BCJL was known to be insecure, it was still conceivable that a secure quantum quantum bit commitment scheme could be found.

The situation turned out to be a dead end when Mayers [29], and independently Lo and Chau [22], showed that no quantum bit commitment whatsoever exists. It was shown that the EPR attack can be generalized against any quantum bit commitment provided the committer can deal with large entangled quantum states. Different approaches have then been tried in order to escape the no-go theorem [13]. All these attempts aimed at taking advantage of subtle assumptions in the theorem statement. The common feature of most approaches is the use of a classical assumption that has to hold only temporarily. The goal being to build from such a *temporary assumption* a commitment scheme that is both concealing and binding even after the assumption is withdrawn. Unfortunately, none of these attempts has produced a scheme achieving more than what classical cryptography alone can provide. Quantum bit commitment is now known to be impossible in scenarios lying beyond the initial statement of the no-go theorem [11]. It naturally raises the question of what assumptions are needed in order for secure quantum bit commitment to exist and can these assumptions be made independent of the classical one whilst remaining meaningful? In other words, does quantum mechanics helps in providing secure two-party computation?

In this paper we consider a physical limitation upon which the security of quantum bit commitment, and QOT [35], can be based. The assumption does not restrict the computing power and therefore makes sense whether or not one-way functions exist in the classical world [19]. For, we restrict the ability of one party to carry out arbitrary quantum coherent measurements. We say that a measurement is n-coherent if it involves no more than n qubits coherently. We propose a variant of BCJL that is shown to be secure under this restriction. One reason for considering this assumption is that large coherent measurements are not known to be realizable by a reliable physical process. As an example, consider the simplest interesting case $n = 2$. Perhaps the most important 2-coherent measurement that is not 1-coherent is the Bell measurement which, together with the ability to produce EPR pairs, leads to quantum teleportation [6]. Interestingly, although quantum teleportation has been shown to work experimentally [8], the Bell measurements could only be approximated. It is in general more difficult to make several qubits interact in a measurement than producing entangled states [31, 24, 8]. Whereas EPR pairs can be *easily* produced experimentally, measuring in the Bell basis requires more work. Even though Bell measurements will probably be accomplished in the near future, large coherent measurements are very challenging even in a controlled environment. The complexity and reliability required for the physical process implementing large n-coherent measurements might well not be achievable in a foreseeable future. A coherent measurement can be seen as an unitary transformation acting on the observed system plus an ancilla, followed by a standard Von Neumann measurement. This process is exactly what is meant by a quantum algorithm. The ability to perform n-coherent measurements suggests that quantum computers working on n qubits can also be realized. However, it might be the case that n-qubits quantum computers exist but n-coherent measurements against quantum protocols don't. One reason could be that quantum cryptography, unlike quantum computation, can take place in an extremely hostile environment for the survival of large entangled quantum states [17]. Our result shows that large coherent measurements are necessary in order to apply Mayers' attack against our scheme. A commitment scheme is δ-binding if for each execution there is a bit $\tilde{x} \in \{0,1\}$ that cannot be unveiled with probability of success better than δ. Our bit commitment scheme requires the transmission of N qubits and is δ-binding, for any $\delta > 0$, provided the committer can only carry out n-coherent measurements for some $n \in \Omega(N)$. For some $\alpha > 0$, the scheme is $2^{-\alpha N}$-binding against n-coherent measurements for some $n \in \Omega(\sqrt{N})$. The commitment is also shown to conceal unconditionally the committed bit.

In section 2 we give the preliminary ingredients. Section 3 presents a variation of the BCJL protocol, called LJCB. In section 4 we introduce the definitions and tools about quantum measurements and outcomes. In section 5, we define the class of n-coherent strategies against the binding condition. We show that LJCB is *binding* against the class of n-coherent strategies for some $n \in \Omega(N)$ where N is the total number of qubits sent through the quantum channel. In section 6, LJCB is shown to be unconditionally concealing. We conclude in section 7.

2 Preliminaries

We write $x \in_R X$ for "the element x is picked uniformly and randomly from the set X". Notation $x \odot y$ for $x, y \in \{0,1\}^n$ means $\bigoplus_{i=1}^n x_i \cdot y_i$. For sets $X = \{x_0, x_1, \ldots, x_n\}$ and $s \in \{0, \ldots, n\}$ we write X_s for the s-th element x_s in X. If y represents the outcome of some random experiment then we write $\boldsymbol{y}$ as the random variable associate with the experiment. We denote the Shannon entropy and information functions by $\boldsymbol{H}(y)$ and $\boldsymbol{I}(y)$ respectively. For any strings $c, c' \in \{0,1\}^n$ we define $\Delta(c, c')$ as the Hamming distance between c and c'. When the context allows, we also write $\Delta(c, c')$ as the set of distinct positions. For $X \subseteq \{1, \ldots, n\}$ and $b \in \{0,1\}^n$ we denote by b_X the substring of b defines for positions in X. [1]

2.1 Bit Commitment

A bit commitment scheme allows Alice to send a piece of evidence to Bob that she has a bit $x \in \{0,1\}$ in mind. Given what he receives, Bob cannot tell what x is. This phase of the bit commitment scheme is called the committing phase. After a while, Bob can ask Alice to unveil x in such a way that it is not possible for her to unveil $1 - x$ without being detected. This phase is called the opening phase. The security of such a scheme is captured by the following definition:

Definition 1. *A bit commitment scheme is*

- statistically concealing *if the information $\mathcal{V}$ the receiver gets about the committed bit $x \in \{0,1\}$ after the committing phase (and before opening) is such that $\boldsymbol{I}(x|\mathcal{V}) \leq 2^{-\alpha N}$ for some $\alpha > 0$ and N a security parameter,*

[1] If $b, c, c' \in \{0,1\}^n$ are any n-bit string then $b_{\Delta(c,c')} \in \{0,1\}^{\Delta(c,c')}$ is the substring of b restricted to positions where c and c' differ.

- δ-binding *for* $0 < \delta < 1$, *if after the execution of the committing phase there exists* $\tilde{x} \in \{0,1\}$ *such that the probability to unveil* $\tilde{x}$ *with success is less than* δ*,*
- δ-secure *if it is both concealing and* δ*-binding.*

In this paper we are concerned with a slightly weaker form of the binding property than what is usually considered. Namely, we allow the sender to change her mind with some bounded probability of success δ. Nevertheless, a δ–secure bit commitment scheme is sufficient for secure quantum oblivious transfer[35, 5]. Mayers' theorem shows how to break any concealing commitment by constructing an attack allowing to reveal any bit with probability of success almost 1. The attack also applies for concealing but δ-binding commitment schemes whenever $\delta < 1$ [28, 29].

2.2 Quantum Coding

The essential quantum ingredient is the BB84 coding scheme [3]. In order to transmit the bit $b = 0$ one of the two non-orthogonal quantum states $|0\rangle_+ = \binom{1}{0}$ and $|0\rangle_\times = \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix}$ is chosen and sent through the quantum channel [2]. For the transmission of $b = 1$, the two non-orthogonal quantum states are $|1\rangle_+ = \binom{0}{1}$ and $|1\rangle_\times = \begin{pmatrix} \frac{-1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix}$. If for transmitting $b \in \{0,1\}$ the quantum state $|b\rangle_+$ is chosen then we say that b is transmitted in rectilinear basis "+". If b is encoded in $|b\rangle_\times$ we say that b is transmitted in diagonal basis "×". Let ρ_b be the quantum mixture associates with the transmission of bit b in a random basis $\theta \in_R \{+, \times\}$. Let $\{\gamma_0, \gamma_1\}$ be the unit vectors of the Breidbart basis (i.e. $\gamma_0 = (\cos\frac{\pi}{8}, \sin\frac{\pi}{8})$ and $\gamma_1 = (-\sin\frac{\pi}{8}, \cos\frac{\pi}{8})$). We have, for any $b \in \{0,1\}$, that (see [10] for more information)

$$\rho_b = \cos^2\frac{\pi}{8}|\gamma_b\rangle\langle\gamma_b| + \sin^2\frac{\pi}{8}|\gamma_{1-b}\rangle\langle\gamma_{1-b}|. \tag{1}$$

Equation 1 stands as long as the coding basis θ is random and independent. One interpretation of equation 1 is that the BB84 coding scheme is inherently ambiguous. Given any outcome of any quantum measurement, the transmitted bit b cannot be known with probability better than $\cos^2(\frac{\pi}{8})$. The intrinsic entropy $\boldsymbol{H}_{VN}(\rho_b)$ (Von Neumann entropy) about $b \in \{0,1\}$ is

$$\boldsymbol{H}_{VN}(\rho_b) = \boldsymbol{H}(\cos^2\frac{\pi}{8}, \sin^2\frac{\pi}{8}) \geq 0.4157611883. \tag{2}$$

No possible outcome of any measurement can give more information about b than $1 - \boldsymbol{H}_{VN}(\rho_b)$ simply because the quantum state does not carry more information than that. For any $X \subseteq \{1, \ldots, n\}$ and $b \in \{0,1\}^n$ we define $\rho^X(b) = \otimes_{i \in X}\rho_{b_i}$ as the density matrix associates with b_X when b is transmitted according to the BB84 coding scheme. As for equation 2 we have that

$$\boldsymbol{H}_{VN}(\rho_b^X) = \#X \cdot \boldsymbol{H}(\cos^2\frac{\pi}{8}, \sin^2\frac{\pi}{8}) \geq 0.4157611883 \cdot \#X. \tag{3}$$

[2] Notation $|b\rangle$ for $b \in \{0,1\}$ means $|b\rangle_+$ which is the computational basis.

In addition, since $\rho_+ = \rho_\times$ it follows that for all measurements no outcome gives information about the transmission basis.

2.3 Generalized Measurements

It is shown in [27] (see also section 2.2 of [33]) that any possible measurement can be represented by a single IPP (Inner Product Preserving Operator) transformation from the initial space of states to a larger space of states followed by an ordinary von Neumann measurement on the latter. An m-outcome generalized measurement on a space V is described by m operators $M_k : V \to W_k, k = 1, \ldots, m$, such that if the initial state is $|\phi\rangle$ and the observed classical outcome is k then the state after the measurement, up to normalization, is $M_k|\phi\rangle$. The probability to observe k when $|\phi\rangle$ is transmitted is $||M_k|\phi\rangle||^2$. The operator M_k is IPP if it is represented as a matrix of orthonormal columns. An IPP operator M_k for the measurement of an n qubits system has 2^n columns. The value $\langle k\rangle$ is called the classical outcome for M_k. From M_k, we define the column vector $\Phi^\theta(\langle k\rangle|b) = M_k|b\rangle_\theta$ containing the transition amplitudes from state $|b\rangle_\theta$ to any of the final state in M_k. The probability of observing $\langle k\rangle$ when $|b\rangle_\theta$ is the initial state is $||\Phi^\theta(\langle k\rangle|b)||^2$. If the measurement is complete then M_k is one-dimensional and $\Phi^\theta(\langle k\rangle|b)$ is not a vector but a complex number. We use the IPP representation because, as in [30], we want to analyze measurements acting on a fixed number n of qubits independently of the degree of freedom provided by appending an ancilla to the system (unlike the POVM model). When we say that a measurement is n-coherent, we mean that it measures a quantum state of dimension 2^n regardless the dimension of the ancilla.

3 The Protocol

The protocol we describe works on the same principles than BCJL [10]. The main difference is the direction of the quantum transmission allowing Alice to commit. For this reason our scheme is called LJCB. Unlike the BCJL scheme, the commitment is made by choosing how to measure the received qubits. The commitment is initiated by Bob who sends to Alice N qubits in state $|b\rangle_\theta$ for $b \in_R \{0,1\}^N$ and $\theta \in_R \{+, \times\}^N$. For each qubits she receives, one of the two incompatible Von Neumann measurements $+$ and $\times$ is chosen and the result is announced to Bob. Since the two measurements are incompatible, even knowing the outcome does not reveal all the information about which one has actually been done. Let C be an error-correcting code of length N, dimension k and minimum distance d. The code C does not need to have an efficient decoding algorithm. In order to commit (see protocol 1), Alice picks $c \in_R C$, measures the i–th photon π_i with the Von Neumann measurement $\{+, \times\}_{c_i}$ and announces the classical outcome $\beta_i \in \{0,1\}$. Alice also chooses and announces a random $r \in \{0,1\}^n$ subject to $r \odot c = x$. This completes the committing phase. In order to open x (see protocol 2), Alice simply announces c and x allowing Bob to verify (for each π_i) that when she measured in the basis he had chosen then the announced outcome corresponds to the bit originally sent. In this paper, we assume a noiseless quantum channel allowing Bob to reject Alice's commitment as soon as one position i is found such that $\theta_i = c_i$ but $b_i \neq \beta_i$. The case of a noisy quantum channel will be addressed in the final version.

Protocol 1 (commit(x))

```
1: Bob picks and announces a random boolean generating matrix $G$ for a linear $[N,k,d]$-code $C$ with $N$ and $k$ chosen according to theorem 3,
2: Alice picks $m \in_R \{0,1\}^k$, sets $c \in_R G \cdot m$ and picks $r \in_R \{0,1\}^N$ subject to $c \odot r = x$. Alice announces $r$ to Bob,
3: Bob chooses randomly $b \in_R \{0,1\}^N$ and $\theta \in_R \{+,\times\}^N$,
4: $\mathop{\mathrm{DO}}_{i=1}^{N}$
   – Bob sends a photon $\pi_i$ in polarization state $|b_i\rangle_{\theta_i}$,
   – Alice measures $\pi_i$ in basis $\{+,\times\}_{c_i}$ and obtains the classical outcome $\beta_i \in \{0,1\}$,
5: Alice announces $\beta = \beta_1, \ldots, \beta_N$ to Bob.
```

Protocol 2 (open(r,β,θ,b)(c,x))

```
1: Alice announces $c$ and $x$ to Bob,
2: Bob accepts if and only if
   1. $c \in C$,
   2. $(\forall i \in \{1,\ldots,N\})[\theta_i = c_i \Rightarrow b_i = \beta_i]$ and
   3. $x = c \odot r$.
```

4 Tools

In this section, we give general properties applicable to any quantum measurement Alice may apply when she commits and opens the bit x. These properties are tools that will be used to deal with Alice general strategy against the binding condition.

When Alice commits, she measures the initial state $|b\rangle_\theta$ in order to get the classical outcome $\langle r, \beta\rangle$. When she opens x, she refines her measurement and gets the final classical outcome $\langle r,\beta,c\rangle$. The bit x needs not to appear in the final outcome description since it is uniquely defined as $c \odot r$. It is convenient to write $\langle r,\beta,v\rangle$ to represent a partial outcome with an extra piece of information $v \in \mathcal{V}$ for an arbitrary set $\mathcal{V}$. The extra outcome v will be used in section 5 to model successive steps in Alice opening strategy. The final outcome $\langle r,\beta,c\rangle$ is accepted by Bob if and only if $c \in C$ and the string $b \in \{0,1\}^N$ is in the set $S(\beta,c,\theta) = \{b \in \{0,1\}^n | (\forall i \in \{1,\ldots,n\})[\theta_i = c_i \Rightarrow b_i = \beta_i]\}$.

The following definition characterizes partial outcomes $\langle r,\beta,v\rangle$ allowing to announce safely the codeword c.

Definition 2. *A partial result with classical outcome $\langle r,\beta,v\rangle$ is (θ,c,p)-*safe *if for $\frac{1}{2} < p < 1, \theta \in \{+,\times\}^n$ and $c \in \{+,\times\}^n$ we have*

$$\mathrm{P}\left(\boldsymbol{b} \in S(\beta,c,\theta) | \boldsymbol{\beta} = \beta \wedge \boldsymbol{\theta} = \theta \wedge \boldsymbol{v} = v\right) \geq p. \tag{4}$$

We also say that $\langle r,\beta,v\rangle$ is (c,p,q)-safe if there exists a subset $\Theta \subseteq \{+,\times\}^n$ such that $\frac{\#\Theta}{2^n} \geq q$ and for each $\theta \in \Theta$ the partial outcome $\langle r,\beta,v\rangle$ is (θ,c,p)-safe.

Suppose the result $\langle r,\beta,v\rangle$ is (θ,c,p)-safe. The IPP operator implementing the measurement that produces $\langle r,\beta,v\rangle$ can be written in terms of transition amplitudes given the following identity (see section 2.3):

$$\mathrm{P}\left(b \in S(\beta,c,\theta) | \langle r,\beta,v\rangle \wedge \boldsymbol{\theta}=\theta\right) = \frac{\sum_{b\in S(\beta,c,\theta)} \|\Phi^\theta(\langle r,\beta,v\rangle|b\rangle)\|^2}{\sum_{b\in\{0,1\}^n} \|\Phi^\theta(\langle r,\beta,v\rangle|b\rangle)\|^2}.$$

This allows to rewrite equation 4 as

$$\sum_{b\in S(\beta,c,\theta)} \|\Phi^\theta(\langle r,\beta,v\rangle|b\rangle)\|^2 \geq p \sum_{b\in\{0,1\}^n} \|\Phi^\theta(\langle r,\beta,v\rangle|b\rangle)\|^2. \tag{5}$$

If $\langle r,\beta,v\rangle$ is (c,p,q)-safe then there exists $\Theta \subseteq \{+,\times\}^n$ such that $\frac{\#\Theta}{2^n} \geq q$ and equation 5 holds for all $\theta \in \Theta$. In section 5, we shall see that next definition characterizes the partial outcomes of n-coherent measurements Alice needs in order to attack the binding condition of LJCB. Lemma 1 will then put restrictions on what Alice can physically achieve.

Definition 3. *Let $\theta \in \{+,\times\}^n, r,\beta,c,c' \in \{0,1\}^n$. A partial result with classical outcome $\langle r,\beta,v\rangle$ is (θ,c,c',p)-*promising *if $\langle r,\beta,v\rangle$ is (θ,c,p)-safe and (θ,c',p)-safe. We also say that $\langle r,\beta,v\rangle$ is (c,c',p,q)-promising if there exists a subset $\Theta \subseteq \{+,\times\}^n$ such that $\frac{\#\Theta}{2^n} \geq q$ and for each $\theta \in \Theta$ the partial outcome $\langle r,\beta,v\rangle$ is (θ,c,c',p)-promising.*

Let $S(\beta,c,c',\theta) = S(\beta,c,\theta) \cap S(\beta,c',\theta)$ be the set of initial strings $b \in \{0,1\}^n$ such that from $\langle r,\beta\rangle$ both c and c' can be announced without error. Using equation 5, we easily get that $\langle r,\beta,v\rangle$ is (θ,c,c',p)-promising implies

$$\sum_{b\in S(\beta,c,c',\theta)} \|\Phi^\theta(\langle r,\beta,v\rangle|b\rangle)\|^2 \geq (2p-1) \sum_{b\in\{0,1\}^n} \|\Phi^\theta(\langle r,\beta,v\rangle|b\rangle)\|^2. \tag{6}$$

Next lemma shows that promising partial results don't always exist.

Lemma 1. *Let $c,c' \in \{0,1\}^n$ be such that $\Delta(c,c') \in \Omega(n)$ and let $r,\beta \in \{0,1\}^n$. Then, there exists no (c,c',p,q)-promising partial result with classical outcome $\langle r,\beta,v\rangle$ whenever $q(2p-1) \geq p_{max} = 0.586$.*

Proof. Let $\Theta \subseteq \{+,\times\}^n$ be a set of basis such that $\frac{\#\Theta}{2^n} \geq q$ and for all $\theta \in \Theta$ the partial outcome $\langle r,\beta,v\rangle$ is (θ,c,c',p)-promising. ¿From equation 6, for all $\theta \in \Theta$,

$$\mathrm{P}\left(b \in S(\beta,c,c',\theta) | \langle r,\beta,v\rangle \text{ is } (\theta,c,c',p)\text{-promising}\right) \geq 2p-1.$$

By construction we also have that $\mathrm{P}\left(b_{\Delta(c,c')} = \beta_{\Delta(c,c')} | b \in S(\beta,c,c',\theta)\right) = 1$. It follows that

$$\mathrm{P}\left(b_{\Delta(c,c')} = \beta_{\Delta(c,c')} | \langle r,\beta,v\rangle \text{ is } (\theta,c,c',p)\text{-promising}\right) \geq 2p-1. \tag{7}$$

Since no measurement outcome gives information about the transmission basis θ, we have that $\mathrm{P}\left(\boldsymbol{\theta} \in \Theta | \langle r,\beta\rangle\right) \geq q$. It follows from Bayes' law that

$$\mathrm{P}\left(b_{\Delta(c,c')} = \beta_{\Delta(c,c')} | \langle r,\beta,v\rangle \text{ is } (c,c',p,q)\text{-promising}\right) \geq q(2p-1).$$

The amount of uncertainty about $b_{\Delta(c,c')}$ can therefore be upper bounded as follows:

$$\begin{aligned} &\boldsymbol{H}(b_{\Delta(c,c')}|\langle r,\beta,v\rangle \text{ is } (c,c',p,q)\text{–promising }) \\ &\qquad\le \boldsymbol{H}(q(2p-1),\overbrace{\frac{1-q(2p-1)}{2^{\Delta(c,c')}-1},\ldots,\frac{1-q(2p-1)}{2^{\Delta(c,c')}-1}}^{2^{\Delta(c,c')}-1 \text{ times}}) \\ &\qquad\le \boldsymbol{H}(q(2p-1),1-q(2p-1)) + (1-q(2p-1))\Delta(c,c'). \end{aligned}$$

The above equation contradicts the lower bound expressed equation 3 since $q(1-2p) > p_{\max}$ implies

$$\begin{aligned} \boldsymbol{H}(b_{\Delta(c,c')}|\langle r,\beta,v\rangle \text{ is } (c,c',p,q)\text{–promising }) &\le \boldsymbol{H}(0.586,0.414) + 0.414\Delta(c,c') \\ &\le \boldsymbol{H}_{VN}(\rho_b^{\Delta(c,c')}) \end{aligned}$$

when $\Delta(c,c') \in \Omega(n)$ is large enough. □

In other words, any outcome $\langle r,\beta,v\rangle$ that is (c,c',p,q)-promising for p and q such that $q(2p-1) \ge p_{\max}$, conveys more information about $b_{\Delta(c,c')}$ than what is allowed by equation 3. This holds regardless of the extra outcome v.

5 The Binding Condition

5.1 n-coherent Opening Strategies

Alice's opening strategies are of the following form:

- During the committing phase, Alice incompletely measures the N qubits in order to get the partial outcome $\langle r,\beta\rangle$ for $r \in \{0,1\}^N$ and $\beta \in \{0,1\}^N$. She announces r and β to Bob.
- During the opening phase, Alice completes her previous measurement according to the bit x she wants to unveil. The outcome of the refinement is a codeword $c \in C$ and the unveiled bit $x \in \{0,1\}$ is $c \odot r = x$. The final and complete outcome $\langle r,\beta,c\rangle$ allows Bob to learn x.

An opening strategy is n-coherent if all measurements performed by Alice during both phases are n-coherent. Unlike fully coherent strategies, a n–coherent strategy is made out of $t \ge \lceil \frac{N}{n} \rceil$ measurements depending only classically upon each others. Each possible measurement must be expressible as an IPP operator with no more than 2^n columns. However, the description of each IPP operator may depend upon some partial outcomes obtained from previous measurements and therefore can change dynamically as the opening strategy evolves. In order to model arbitrary n-coherent opening strategies, it is convenient to use a tree structure T_N^n. Each node in T_N^n represents the current state and the next measurement to be applied. The relevant operations are quantum measurements and classical announcements. For the sake of simplicity, we only represent in T_N^n the opening part of Alice's strategy. In other words, the root of T_N^n represents the first refinement Alice applies from the partial outcome $\langle r,\beta\rangle$ when the opening phase is initiated. We require that each measurement along any path P of T_N^n can be expressed as a set of measurements $\mathcal{M}_P = \{M_1, \ldots, M_t\}$ where each $M \in \mathcal{M}_P$, is an IPP operator of at most 2^n columns acting on a subset $B \subseteq \{1, \ldots, N\}$ of the received qubits. Without loss of generality we assume that all announcements are made at the very end of the measurement process i.e. they are leafs of T_N^n. We also assume each internal node to define a binary outcome refinement. The outgoing edges are labelled according to the possible outcomes and lead to the next node. At the end of each path, a final announcement $c \in C$ is made. Each path P in T_N^n defines a complete final outcome $\langle r, \beta, c\rangle$ which is the concatenation of all t measurement outcomes defined along P. Since each measurement $M_i \in \mathcal{M}_P$ is applied to a block $B_i \subseteq \{1, \ldots, N\}$ of at most n qubits, P defines a partition $\mathcal{B} = \{B_1, \ldots, B_t\}$ such that for all $i \in \{1, \ldots, t\}$, $\#B_i \leq n$. Each measurement M_i may act coherently on photons $\{\pi_j\}_{j \in B_i}$. We call $\mathcal{B}$ the ***block decomposition*** of P and each $B \in \mathcal{B}$ is called a ***block***. The partial and final outcomes for a measurement $M \in \mathcal{M}_P$ acting on block $B \in \mathcal{B}$ are denoted by $\langle r, \beta\rangle_B = \langle r_B, \beta_B\rangle$ and $\langle r, \beta, c\rangle_B = \langle r_B, \beta_B, c_B\rangle$ respectively. It is also convenient to define the block decomposition $\mathcal{B}(d)$ at node d which is the block decomposition for measurements along the path from the root to node d.

Once the measurement in node d is completed during the execution of T_N^n with root $\langle r, \beta\rangle$, Alice gets the partial outcome $\langle r, \beta, v(d)\rangle$ where $v(d)$ represents the composite partial outcome (or view) for refinements down to d. We denote the final outcome by $\langle r, \beta, c\rangle$ with $c \in C$ dropping the irrelevant auxiliary view $v(d)$. Let d' be a node in T_N^n reachable from d. We write $\langle r, \beta, v(d)\rangle \xrightarrow{u} \langle r, \beta, v(d')\rangle$ if the probability to go from d to d' in T_N^n is at least u. We write $\langle r, \beta, v(d)\rangle \rightarrow \langle r, \beta, v(d')\rangle$ to indicate that the probability of transition from d to d' is nonzero. We denote $L(T_N^n, s)$ the set of nodes at level s in T_N^n.

Definition 4. *Let T_N^n be a n-coherent opening strategy from partial outcome $\langle r, \beta\rangle$. We say that T_N^n is (u, γ)*-successful *if there exists $C^* \subseteq C$ such that $\mathrm{P}\left(c \in C^* | \langle r, \beta\rangle \wedge T_N^n\right) \geq u$ and for all $c \in C^*, \mathrm{P}\left(\boldsymbol{b} \in S(\boldsymbol{\theta}, \beta, c) | \langle r, \beta\rangle \wedge T_N^n\right) \geq \gamma$. Similarly, a node d in T_N^n is said to be (u, γ)*-successful *if the subtree $T_N^n(d)$ of T_N^n is (u, γ)-successful.*

Next lemma gives some simple properties any n-coherent opening strategy T_N^n must have. The proof is omitted but follows easily from the definition 4 and the above discussion.

Lemma 2. *Let T_N^n be an n-coherent opening strategy with root $\langle r, \beta\rangle$. Let $\gamma = 1 - (1 - \varrho)(1 - q)$ for $0 < \varrho, q < 1$ and let $l > 0$ be an integer. Let $d \in T_N^n$ and $t = \lceil \frac{n}{N} \rceil$. The following holds:*

1. *If d' is a son of d in T_N^n then $\#(\mathcal{B}(d') \cap \mathcal{B}(d)) \geq t - 1$,*
2. *If $\langle r, \beta, v(d)\rangle$ is both (c, ϱ, q)-safe and (c', ϱ, q)-safe then $\langle r, \beta, v(d)\rangle$ is $(c, c', \varrho, 2q - 1)$-promising,*
3. *If for $B \in \mathcal{B}(d)$, $\langle r, \beta, v(d)\rangle_B \xrightarrow{u} \langle r, \beta, c\rangle_B$ and $\langle r, \beta, c\rangle_B$ is (c, ϱ, q)-safe then $\langle r, \beta, v(d)\rangle_B$ is $(c, \varrho u, q)$-safe,*
4. *if $\langle r, \beta, v(d)\rangle \xrightarrow{\varrho^l} \langle r, \beta, c\rangle$ then*
   $(\exists \widehat{\mathcal{B}}(d) \subseteq \mathcal{B}(d))(\forall B \in \widehat{\mathcal{B}}(d))[\langle r, \beta, v(d)\rangle_B \xrightarrow{\varrho} \langle r, \beta, c\rangle \wedge \#\widehat{\mathcal{B}}(d) \geq t - l]$,
5. *if $\mathrm{P}\left(\boldsymbol{b} \in S(\boldsymbol{\theta}, \beta, c) | \langle r, \beta, c\rangle\right) \geq \gamma^l$ then*
   $(\exists \widehat{\mathcal{D}}(d) \subseteq \mathcal{B}(d))(\forall B \in \widehat{\mathcal{D}}(d))[\langle r, \beta, c\rangle_B$ *is* (c, ϱ, q)*-safe* $\wedge \ \#\widehat{\mathcal{D}}(d) \geq t - l]$.

5.2 LJCB is Binding

In this section we prove that whenever n is *small* with respect to C's minimum distance d, Alice cannot change her mind with arbitrary good probability of success. The smaller n is, compared to d, the better the probability is for Bob to detect Alice changing her mind. Next lemma shows that any successful strategy allows to unveil only one $c \in C$ with good probability of success. The binding condition will then follow.

Lemma 3. *Let $\varrho = 0.93$,$\gamma = 0.9937$ and $n \leq \frac{d}{4l+5}$. If T_N^n is a (ϱ^l, γ^l)-successful n-coherent opening strategy from partial outcome $\langle r, \beta\rangle$ then the following predicate holds,*

$$
\begin{aligned}
H(s) \equiv {} & [(\forall d \in L(T_N^n, s))(\exists! c^* \in C) \\
& [\langle r,\beta,v(d)\rangle \rightarrow \langle r,\beta,c^*\rangle \wedge \mathrm{P}\,(b \in S(\theta,c^*,\beta)|\langle r,\beta,c^*\rangle) \geq \gamma^l]].
\end{aligned}
$$

Proof. Let $q = 0.91$ be such that $\gamma = 1-(1-\varrho)(1-q)$. Let $t = \lceil\frac{N}{n}\rceil$ be a lower bound on the number of n-coherent measurements. The proof proceeds by mathematical induction. In the first place, it is easy to see that $H(0)$ holds since all nodes at level 0 are announcements. Second, assume $H(s)$ holds, we show that $H(s+1)$ also holds. Let $d \in L(T_N^n, s+1)$. Let d^0 and d^1 be the left and right son of d respectively. If $T_N^n(d^0)$ or $T_N^n(d^1)$ is not (ϱ^l,γ^l)-successful then $H(s+1)$ followed directly from $H(s)$. Now suppose both $T_N^n(d^0)$ and $T_N^n(d^1)$ are (ϱ^l,γ^l)-successful. By induction hypothesis, $T_N^n(d^0)$ and $T_N^n(d^1)$ are such that $\langle r,\beta,v(d^0)\rangle \xrightarrow{\varrho^l} \langle r,\beta,c^0\rangle$ and $\langle r,\beta,v(d^1)\rangle \xrightarrow{\varrho^l} \langle r,\beta,c^1\rangle$ respectively, for $c^0, c^1 \in C$. If $c^0 = c^1$ then $H(s+1)$ follows from $H(s)$. Assume for a contradiction that $c^0 \neq c^1$. Let $\widehat{\mathcal{B}}(d^0)$ and $\widehat{\mathcal{B}}(d^1)$ be defined according to lemma 2-4). We have that for all $w \in \{0,1\}$, $\#\widehat{\mathcal{B}}(d^w) \geq t-l$. Let $\widehat{\mathcal{D}}(d^0)$ and $\widehat{\mathcal{D}}(d^1)$ be defined as in lemma 2-5) ensuring that for all $w \in \{0,1\}$,$\#\widehat{\mathcal{D}}(d^w) \geq t-l$. Let $\Gamma^w = \widehat{\mathcal{B}}(d^w) \cap \widehat{\mathcal{D}}(d^w) \cap \mathcal{B}(d)$ be the set of blocks $B \in \mathcal{B}(d)$ such that $\langle r,\beta,v(d^w)\rangle_B \xrightarrow{\varrho} \langle r,\beta,c^w\rangle_B$ and $\langle r,\beta,c^w\rangle_B$ are (c_B^w,ϱ,q)-safe. From property 2-1), we get that $\#\Gamma^w \geq t-2(l+1)$ and from lemma 2-3), all $B \in \Gamma^w$ are such that $\langle r,\beta,v(d^w)\rangle_B$ is (c_B^w,ϱ^2,q)-safe. Let $\Gamma^{0,1} = \Gamma^0 \cap \Gamma^1$ be the set of blocks $B \in \mathcal{B}(d)$ such that $\langle r,\beta,v(d)\rangle_B$ is $(c_B^0,c_B^1,\varrho^2,2q-1)$-promising. Since both $\#\Gamma^0$ and $\#\Gamma^1$ are greater than $t-2(l+1)$ it follows that $\#\Gamma^{0,1} \geq t-4(l+1)$. Let $\mathcal{B}_\Delta = \{B \in \mathcal{B}(d) | \Delta(c_B^0,c_B^1) \in \Omega(n)\}$ be such that $\#\mathcal{B}_\Delta \geq 4l+5$ from the fact that $n \leq \frac{d}{4l+5}$. From lemma 2-2), all $B \in \Gamma_\Delta = (\Gamma^0 \cap \Gamma^1) \cap \mathcal{B}_\Delta$ are such that $\langle r,\beta,v(d)\rangle_B$ is $(c_B^0,c_B^1,\varrho^2,2q-1)$-promising in addition to $\Delta(c_B^0,c_B^1) \in \Omega(n)$. To get a contradiction, it suffices to show that Γ_Δ is not empty since any $B \in \Gamma_\Delta$ is such that $\langle r,\beta,v(d)\rangle_B$ is $(c_B^0,c_B^1,\varrho^2,2q-1)$-promising contradicting lemma 1 since $(2\varrho^2-1)(2q-1) > p_{\max}$. By the pigeonhole principle, since $\#(\mathcal{B}(d) \setminus \Gamma^{0,1}) \leq 4l+4$ and $\#\mathcal{B}_\Delta \geq 4l+5$, it must exist a block $B \in \mathcal{B}_\Delta$ that is also in $\Gamma^{0,1}$ and therefore $\#\Gamma_\Delta \geq 1$. We must conclude that $c^0 \neq c^1$ is impossible and $H(s+1)$ follows. □

Next theorem uses lemma 3 in order to conclude that LJCB is δ-binding for any $\delta > 0$ and against all n-coherent opening strategies for some $n \in \Omega(N)$.

Theorem 1. *Let N be the number of BB84 qubits transmitted. Let $l > 0$ be an integer. Let $d \in \Omega(N)$ be C's minimum distance. Protocol LJCB is $\delta(l)$-binding* *against any n-coherent opening strategy for $\delta(l) = \gamma^l + \varrho^l$ provided $n \leq \frac{d}{4l+5}$ and γ, ϱ are defined as in lemma 3.*

Proof. Assume Alice can open any $x \in \{0,1\}$ with an appropriate n-coherent opening strategy $T_N^n(x)$. The trees $T_N^n(0)$ and $T_N^n(1)$ cannot be both (ϱ^l, γ^l)-successful since otherwise the tree T_N^n with $T_N^n(0)$ and $T_N^n(1)$ as left and right subtree respectively will also be (ϱ^l, γ^l)-successful. By construction, T_N^n has two codewords $c^0 \neq c^1$ such that for all $x \in \{0,1\}$ $\langle r, \beta \rangle \rightarrow \langle r, \beta, c^x \rangle$ and $\mathrm{P}\left(\boldsymbol{b} \in S(\boldsymbol{\theta}, c^x, \beta) | \langle r, \beta, c^x \rangle\right) \geq \gamma^l$ contradicting lemma 3. It follows that there exists $\tilde{x} \in \{0,1\}$ having probability less than $\delta(l) \leq (1-\varrho^l)\gamma^l + \varrho^l \leq \gamma^l + \varrho^l$ of being unveiled with success. □

6 The Concealing Condition

In this section we show how to choose the code C such that Bob gets almost no Shannon information about the committed bit x. The technique is similar to the one introduced in [10] to deal with the concealing condition of BCJL. Here, we sketch the proof that LJCB is concealing along the same lines. We first define the density matrix ρ_c that characterizes Bob's view about $c \in C$ given the announcement $\langle r, \beta \rangle$. We then show that Bob's view about c is equivalent to receiving c through a noisy channel. This is done by introducing a fictitious protocol used by Alice to send $c \in C$ in such a way that Bob gets the same view than after the committing phase of LJCB. We finally show, using privacy amplification techniques [4, 12], that the fictitious protocol conceals x and therefore so it is for LJCB.

The most general attack for Bob is to prepare a quantum system initially in pure state $|\psi\rangle \in H_{2^N} \otimes H_B$ where H_{2^N} is the Hilbert space of N qubits and H_B is an auxiliary Hilbert space helping Bob in its quest for x. The quantum state $|\psi\rangle$ can be written, for some $I \in \mathbb{N}$, as $|\psi\rangle = \sum_{1 \leq i \leq I} a_i |\psi_i^A\rangle \otimes |\psi_i^B\rangle$ where $|\psi_i^A\rangle \in H_{2^N}$, $|\psi_i^B\rangle \in H_B$ and the a_i's are complex numbers such that $\sum_i |a_i|^2 = 1$. We do not require $|\psi_i^A\rangle$'s (resp. $|\psi_i^B\rangle$) to be orthogonal. Bob then sends $\rho_A = \mathrm{Tr}_{H_B}(|\psi\rangle\langle\psi|)$ to Alice and keeps the remaining part $\rho_B = \mathrm{Tr}_{H_{2^N}}(|\psi\rangle\langle\psi|)$ for later use. Once $\beta, r \in \{0,1\}^N$ have been announced, Bob determines an unitary transformation $U(r, \beta)$ which he applies to ρ_B. The strategy is completed after a standard measurement $\boldsymbol{M}$ is finally applied to the final state $U(r,\beta)\rho_B U(r,\beta)^\dagger$. First, we show that Bob has no advantage in preparing ρ_A in a mixed state. Consider that, instead of preparing state $|\psi\rangle$ as described above, Bob follows the procedure **Simulate**(ψ) defined as:

1. Bob picks $i \in \{1, \ldots, I\}$ with probability $|a_i|^2$,
2. Bob sends to Alice the quantum state $|\psi_i^A\rangle$ and keeps $|\psi_i^B\rangle$ for later,
3. Bob waits for $r, \beta \in \{0,1\}^N$ and applies $|\widehat{\psi}_i^B\rangle = U(r,\beta)|\psi_i^B\rangle$,
4. Bob measures $|\widehat{\psi}_i^B\rangle$ with measurement $\boldsymbol{M}$.

The above procedure gives exactly the same view than what Bob would get if he had prepared the entangled state $|\psi\rangle$ since $|\psi\rangle$ is a purification of **Simulate**(ψ) [18]. The density matrices, for Alice's and Bob's systems, before $\boldsymbol{M}$ is applied are identical in both cases. It follows that $\boldsymbol{M}$ behaves the same way in both scenarios and therefore, if the initial preparation $|\psi\rangle$ helps Bob in cheating then so it is for **Simulate**(ψ). By the same argument, each qubit π_i can be assumed in pure state $|\phi_i\rangle \in H_2$ allowing us to restrict the analysis to Bob's strategy consisting of sending N qubits in state $\otimes_{i=1}^{N}|\phi_i\rangle$.

Let Bob's qubits π_i, for $i \in \{1,\ldots,N\}$, be in quantum state $|\phi_i\rangle = \cos\alpha_i|0\rangle + \sin\alpha_i|1\rangle$ where α_i is an arbitrary angle. For $\mathtt{m},\mathtt{w} \in \{0,1\}$, let $p_{\mathtt{wm}}(\alpha_i)$ be the probability that Alice observes the classical outcome $\mathtt{m}$ whenever $|\phi_i\rangle$ is measured in basis $\{+,\times\}_{\mathtt{w}}$. We have that $p_{00}(\alpha_i) = \cos^2\alpha_i, p_{01}(\alpha_i) = \sin^2\alpha_i, p_{10}(\alpha_i) = (\cos\alpha_i + \sin\alpha_i)^2/2$ and $p_{11}(\alpha_i) = (\sin\alpha_i - \cos\alpha_i)^2/2$. Let $\rho^i_{c_i}$ be the density matrix describing what Bob gets when Alice chooses to measure π_i in basis $\{+,\times\}_{c_i}$:

$$\rho^i_{c_i}(\alpha_i) = p_{c_i0}(\alpha_i)|0\rangle\langle 0| + p_{c_i1}(\alpha_i)|1\rangle\langle 1|. \tag{8}$$

The density matrix $\rho_x(\alpha)$ associates with the commitment of bit x and given the polarization angles $\alpha = \alpha_1,\alpha_2,\ldots,\alpha_N$ is such that (see [10] for details)

$$\rho_x(\alpha) = \sum_{\{c\in C | c\odot r = x\}} 2^{-k+1} \bigotimes_{i=1}^{N} \rho^i_{c_i}(\alpha_i).$$

Consider the following fictitious protocol for transmitting $c \in_R C$ from Alice to Bob. It is easy to verify that the density matrix $\widehat{\rho}_x(\alpha)$ corresponding to the transmission of a random codeword from C in **fictitious**(x), satisfies $\widehat{\rho}_x(\alpha) = \rho_x(\alpha)$.

Protocol 3 (fictitious(x))

```
1: Alice chooses $c \in_R C$,
2: For each $i \in \{1,\ldots,N\}$, Alice sends to Bob a photon $\pi_i$ in state:
   – If $c_i = 0$ then she sends $|0\rangle$ with probability $p_{00}(\alpha_i)$ and sends $|1\rangle$ with
     probability $p_{01}(\alpha_i)$,
   – If $c_i = 1$ then she sends $|0\rangle$ with probability $p_{10}(\alpha_i)$ and sends $|1\rangle$ with
     probability $p_{11}(\alpha_i)$.
3: Alice announces a random $r \in \{0,1\}^N$ such that $c \odot r = x$.
```

Protocol **fictitious**(x) does not require the transmission of qubits. Classical communication is enough since only orthogonal states are sent. Given α, Bob's view about c in LJCB is the same as if c was sent through a classical noisy channel. Let ω_i be the bit received by Bob in the i-th transmission. In general, for any $\mathtt{c},\mathtt{w} \in \{0,1\}$ and any actual view $\mathcal{V}_i$ up to the i-th transmission , we have

$$\mathrm{P}\left(c_i = \mathtt{c} | \omega_i = \mathtt{w} \wedge \alpha_i \wedge \mathcal{V}_i\right) = \frac{\mathrm{P}\left(c_i = \mathtt{c}|\mathcal{V}_i\right) p_{\mathtt{cw}}(\alpha_i)}{\mathrm{P}\left(c_i = 0|\mathcal{V}_i\right) p_{0\mathtt{w}}(\alpha_i) + \mathrm{P}\left(c_i = 1|\mathcal{V}_i\right) p_{1\mathtt{w}}(\alpha_i)}. \tag{9}$$

An easy calculation shows that for any actual view $\mathcal{V}_i$, the best choice for α_i is $\alpha_i = \frac{v\pi}{4}$ for some $v \in \mathbb{N}$. Whenever $\mathrm{P}\left(c_i = \mathtt{c}|\mathcal{V}_i\right) = \frac{1}{2}$ any $\alpha_i = \frac{v\pi}{4}$ for $v \in \mathbb{N}$ works equally good. In order to simplify the analysis, we assume that C is a $[N,k]$-systematic random code. This ensures that for all $i \in \{1,\ldots,k\}$, $\mathrm{P}\left(c_i = \mathtt{c}|\mathcal{V}_i\right) = \frac{1}{2}$ allowing us to set $\alpha_i = 0$ without loss of generality. In addition, we also assume that the redundancy part $\tilde{c} \in \{0,1\}^{N-k}$ of $c \in C$ is sent perfectly to Bob. This new procedure is called **fictitious***(x) and is identical to protocol 3 except that C is systematic and only the message part $m \in \{0,1\}^k$ of a codeword c is sent imperfectly. Obviously if Bob does not get much information when c is sent according to **fictitious***(x) then he gets no more information whenever c is received according to **fictitious**(x).

The first step consists of finding a lower bound on Bob's Rényi (or collision) entropy about c before Alice announces the redundancy part $\tilde{c}$ and $r \in \{0,1\}^N$ in **fictitious***(x). Setting $\alpha_i = 0$ in equation 9 gives that for all $\mathrm{c} \in \{0,1\}$:

$$\mathrm{P}\left(c_i = \mathrm{c} | w_i = 0 \wedge \mathcal{V}_i\right) \geq \frac{1}{3}. \tag{10}$$

The subset of positions $J \subseteq \{i | \omega_i = 0\}$ is, except with negligible probability $2^{-\lambda^2 k}$, such that $\#J \geq \mathrm{P}\left(\omega_i = 0 | \mathcal{V}_i\right) k - \lambda k = (\frac{3}{4} - \lambda)k$. Bob's Rényi entropy $R(c|\mathcal{V})$ given the view $\mathcal{V} = \cup_{1 \leq i \leq k} \mathcal{V}_i$ after the transmission of the k bits of message in c is such that,

$$R(c|\mathcal{V}) \geq -k(\frac{3}{4} - \lambda)\lg\frac{5}{9} = 0.848(\frac{3}{4} - \lambda)k. \tag{11}$$

Next, Bob learns perfectly $N-k$ parity bits about c_J. The situation is identical to receiving the bits in c_J over a binary symmetric channel with error probability $\frac{1}{3}$ plus $u = N-k$ parity bits. This situation has been analyzed extensively in [12]. It is shown that, except with probability $2^{-\lambda k}$, the Rényi entropy $R(\boldsymbol{c}|\mathcal{V} \wedge \boldsymbol{U} = U)$ given the complete view $\mathcal{V}$ and the parity bits U satisfies:

$$R(\boldsymbol{c}|\mathcal{V} \wedge \boldsymbol{U} = U) \geq R(\boldsymbol{c}|\mathcal{V}) - 2u - 2\lambda k \geq 2.63k - 2N - 3\lambda k. \tag{12}$$

Equation 12 and the privacy amplification theorem (PAT) of [4] allows to conclude that the committed bit $x = c \odot r$ is statistically hidden to Bob.

Theorem 2. *There exists $\widehat{\lambda} > 0$ such that except with negligible probability, the information Bob gets about x after the commit phase of LJCB is less than $2^{-\widehat{\lambda} N}$ provided $\frac{k}{N} \geq 0.77$.*

Proof sketch. According to the PAT [4], the amount of Shannon information $\boldsymbol{I}(\boldsymbol{x}|\mathcal{V} \wedge \boldsymbol{U} = U \wedge \boldsymbol{r} = r)$ about x after the execution of **fictitious***(x) is such that $\boldsymbol{I}(\boldsymbol{x}|\mathcal{V} \wedge \boldsymbol{U} = U \wedge \boldsymbol{r} = r) \leq 2^{-R(\mathrm{c}|\boldsymbol{U}=U \wedge \mathcal{V})+1} / \ln 2$. Plugging $\frac{k}{N} \geq 0.77$ and setting λ small enough in equation 12 gives $\boldsymbol{I}(\boldsymbol{x}|\mathcal{V} \wedge \boldsymbol{U} = U \wedge \boldsymbol{r} = r) \leq 2^{-\widehat{\lambda} N}$ for some $\widehat{\lambda} > 0$. This also holds for LJCB since **fictitious***(x) gives always more information about x. □

7 Conclusion

Theorem 1 and 2 ensure that LJCB can be tuned to provide both the binding and the concealing conditions. Using Gilbert-Varshamov bound (GVB) on random binary codes allows to conclude that the same tuning can satisfy both conditions simultaneously. According to GVB [23], a random $N \times k$ matrix with $\frac{k}{N} > 0.77$ defines a $[N, 0.77N, 0.035N]$–code except with negligible probability. Theorems 1, 2 and GVB allow to conclude with our main result:

Theorem 3. *Let C be a $[N, 0.77N]$ random binary code. Let $l > 0$ be an integer and let $n \leq \frac{0.035N}{4l+5}$. Protocol LJCB is $\delta(l)$-secure against all n-coherent opening strategies for $\gamma = 0.9937, \varrho = 0.93$ and $\delta(l) = \gamma^l + \varrho^l$.*

The binding condition, which is the target of Mayers' attack, holds because if Alice could succeed in changing her mind, it would imply that some measurement outcomes have given more information than what is physically achievable. Even though our analysis gives $n \in \Omega(N)$ for any $\delta(l) > 0$, the constant $\frac{n}{N} \approx \frac{0.035N}{4l+5}$ is small even for relatively large values of $\delta(l)$. It is important for practical applications to improve the constants appearing in the statement of theorem 3.

Bootstrapping the BBCS protocol with LJCB leads to secure QOT provided the receiver cannot carry out n-coherent opening strategies against the commitments [35]. In BBCS, the receiver must commit on measurement outcomes. Two commitments are produced for each of the N qubits received. ¿From theorem 3 and assuming each commitment requires the transmission of N qubits, we get that BBCS is secure against n-coherent measurements for some $n \in \Omega(\sqrt{N})$. Moreover, one call to BBCS is sufficient to get a $2^{-\alpha N}$-secure commitment scheme for some $\alpha > 0$. The resulting commitment is therefore $2^{-\alpha N}$-secure for some $n \in \Omega(\sqrt{N})$ as well. This leads to our main open question: Is LJCB $2^{-\alpha N}$-binding against any n-coherent opening strategy for some $n \in \Omega(N)$?

When used in BBCS, LJCB allows to realize QOT using only unidirectional quantum transmission. If QOT is used for quantum identification [14] then the scheme achieves unconditional security for the client and conditional security for the server. All quantum transmissions taking place are from the client to the server. This is interesting in practice because only the technology for sending photons (which is simpler than the one for receiving) is required for the client. However, in other scenarios it might be better to have a commitment scheme where the committer is sending the qubits. In such a case BCJL would be a better choice. Theorem 3 should also hold for BCJL but with different constants. It would be interesting to prove theorem 3 for BCJL as well.

Different experiments in quantum information theory (see [17, 24, 8, 31]) have given strong evidences that our assumption is realistic. It appears that the physical complexity of implementing n-coherent measurements grows very quickly as n increases. Today's technology only allows to deal imperfectly with the simple case $n = 2$. Future experiments will be important in order to capture more precisely what is the inherent difficulty of implementing arbitrary large coherent measurements. Despite the fact that quantum cryptography does not provide unconditional secure two-party computation, it allows to base cryptography upon physical, realistic and well-defined assumptions. In this paper, we have shown how quantum mechanics can help in providing an alternative framework to complexity-based cryptography.

Acknowledgements

The author is very grateful to Peter Høyer for indispensable help. I would like to thank Ivan Damgård, Jeroen van de Graaf and Claude Crépeau for helpful discussions and comments. I am also indebted to Gilles Brassard for having proposed the problem in the first place. Finally, thanks to the anonymous referees for valuable remarks.

References

1. ASPECT, A, P. GRANGIER and G. ROGER, "Experimental realization of the Einstein-Podolsky-Rosen-Bohm gedankenexperiment: A new violation of Bell's inequalities", *Physical Review Letters*, vol. 49, no. 2, 1982, pp. 91 - 94.
2. BELL, J.S.,"On the Einstein Podolsky Rosen Paradox", Physics, vol. 1, no. 1, 1964, p. 195.
3. BENNETT, C.H. and G. BRASSARD, "Quantum cryptography: Public key distribution and coin tossing", *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, Bangalore, India, December 1984, pp. 175 - 179.
4. BENNETT, C.H., G. BRASSARD, C. CRÉPEAU and U. MAURER, "Generalized Privacy Amplification", IEEE Transaction on Information Theory, vol. 41, 1995, pp. 1915 - 1923.
5. BENNETT, C.H., G. BRASSARD, C. CRÉPEAU and M.-H. SKUBISZEWSKA, "Practical quantum oblivious transfer", *Advances in Cryptology — Proceedings of Crypto '91*, August 1991, Springer - Verlag, pp. 351 - 366.
6. BENNETT, C.H., G. BRASSARD, C. CRÉPEAU, R. JOZSA, A. PERES and W.K. WOOTTERS, "Teleporting an Unknown Quantum State via Dual Classical and EPR Channels",*Physical Review Letters*, vol.70, no. 13, 1993, pp. 1895 - 1899.
7. BIHAM, E, G. BRASSARD,M. BOYER,J. VAN DE GRAAF and T. MOR, "Security of Quantum Key Distribution Against All Collective Attacks", Los Alamos preprint archive quant-ph/9801022, January 1998.
8. BOUWMEESTER, D, J.W. PAN, K. MATTLE,M. EIBL,H. WEINFURTER and A. ZEILINGER, "Experimental Quantum Teleportation",Nature, vol.390, 1997,p.575.
9. BRASSARD, G.and C. CRÉPEAU, "Quantum bit commitment and coin tossing protocols", *Advances in Cryptology — Proceedings of Crypto '90*, August 1990, Springer - Verlag, pp. 49 - 61.
10. BRASSARD, G., C. CRÉPEAU, R. JOZSA and D. LANGLOIS, "A quantum bit commitment scheme provably unbreakable by both parties", *Proceedings of 34th Annual IEEE Symposium on the Foundations of Computer Science*, November 1993, pp. 362 - 371.
11. BRASSARD, G., C. CRÉPEAU, D. MAYERS and L. SALVAIL, "A Brief Review on the Impossibility of Quantum Bit Commitment", Los Alamos preprint archive quant-ph/9712023, December 1997.
12. CACHIN, C.and U. MAURER,"Linking Information Reconciliation and Privacy Amplification",*Journal of Cryptology*, vol. 10, no. 2, 1997,pp. 97 - 110.
13. CRÉPEAU, C., "What is going on with quantum bit commitment?", *Proceedings of Pragocrypt '96: 1st International Conference on the Theory and Applications of Cryptology*, Prague, October 1996.
14. CRÉPEAU, C. and L. SALVAIL, "Quantum oblivious mutual identification", *Advances in Cryptology — Proceedings of Eurocrypt '95*, May 1995, Springer - Verlag, pp. 133 - 146.
15. CRÉPEAU, C., J. VAN DE GRAAF AND A. TAPP, "Committed Oblivious Transfer and Private Multi-Party Computation", in *Advances in Cryptology: Proceedings of Crypto '95* (Springer - Verlag, Berlin, 1995), Vol. 963, pp. 110 - 123.
16. EINSTEIN A., B. PODOLSKI and N. ROSEN, "Can Quantum-Mechanical Description of Physical Reality be Considered Complete?", *Physical Review*, no. 47, 1935, pp. 777 - 780.

17. HUGHES, R.J.,D.F.V. JAMES,J.J. GOMEZ,M.S. GULLEY,M.H. HOLZSCHEITES, P.G. KWIAT,S.K. LAMOREAUX,C.G. PETERSON,V.D. SANDBERG,M.M. SCHAUER,C.M. SIMMONS, C.E. THORBURN, D. TUPA, P.Z. WANG and A.G. WHITE, "The Los Alamos Trapped Ion Quantum Computer Experiment",Los Alamos preprint archive quant-ph/9708050, August 1997.
18. HUGHSTON, L. P., R. JOZSA, and W.K. WOOTTERS, "A complete classification of quantum ensembles having a given density matrix", *Physics Letters A*, vol. 183, 1993, pp. 14 - 18.
19. IMPAGLIAZZO, R. and M. LUBY,"One-way Functions are Essential for Complexity Based Cryptography", *Proceedings of 21th Annual IEEE Symposium on the Foundations of Computer Science*, 1989,pp. 230 - 235.
20. KILIAN, J., *Founding Cryptography on Oblivious Transfer*, in the proceeding of *20th Symposium on Theory of Computation*, Chicago, 1988, pp. 20 - 31.
21. KRANAKIS,E.,"Primality and Cryptography",John Wiley and Sons, 1986.
22. LO, H.-K. and H. F. CHAU, "Is quantum bit commitment really possible?", preprint archive http://xxx.lanl.gov/ps/quant-ph/9603004, March 1996.
23. MACWILLIAMS, F.J.and N.J.A. SLOANE,"The Theory of Error-Correcting Codes", North-Holland, 1977.
24. MATTLE, K.,H. WEINFURTER, P.G. KWIAT and A. ZEILINGER, "Dense coding in experimental quantum communication", *Physical Review Letters*, vol. 76, 1996, pp. 4656 - 4659.
25. MAYERS, D., On the security of the quantum oblivious transfer and key distribution protocols, *Advances in Cryptology: Proceeding of Crypto '95*, Lecture Notes in Computer Science, 1995.
26. MAYERS, D., "The trouble with quantum bit commitment", Presented at a workshop on quantum information theory, Montréal, October 1995. Available at http://xxx.lanl.gov/ps/quant-ph/9603015, March 1996.
27. MAYERS, D., "La sécurité des protocoles de la cryptographie quantique", PhD dissertation, Université de Montréal, 1996.
28. MAYERS, D., "Unconditionally secure quantum bit commitment is impossible", presented in the *Fourth Workshop on Physics and Computation — PhysComp '96*, Boston, November 1996.
29. MAYERS, D., "Unconditionally secure quantum bit commitment is impossible", *Physical Review Letters*, vol 78, 1997, pp. 3414 - 3417.
30. MAYERS, D. and L. SALVAIL, "Quantum oblivious transfer is secure against all individual measurements", *Proceedings of the Third Workshop on Physics and Computation — PhysComp '94*, Dallas, November 1994, IEEE Computer Society Press, pp. 69 - 77.
31. MICHLER, M., K. MATTLE, H. WEINFURTER and A. ZEILINGER, "Interferometric Bell-state analysis",*Physical Review Letters*,vol. 53, 1996,pp. 1209 - 1212.
32. RABIN, M. O., "How to exchange secrets by oblivious transfer", Technical Memo TR-81, Aiken Computation Laboratory, Harvard University, 1981.
33. SCHUMACHER, B.,"Sending quantum entanglement through noisy channels", Los Alamos preprint archive http://xxx.lanl.gov/ps/quant-ph/9604023, April 1996.
34. WIESNER, S., "Conjugate coding", *Sigact News*, Vol. 15, no. 1, 1983, pp. 78 - 88; original manuscript written *circa* 1969.
35. YAO, A. C.-C., "Security of quantum protocols against coherent measurements", *Proceedings of 26th Annual ACM Symposium on the Theory of Computing*, 1995, pp. 67 - 75.