Possibility, Impossibility, and cheat sensitivity of quantum-bit string commitment

Buhrman, H.; Christandl, M.; Hayden, P.; Lo, H.-K.; Wehner, S.

Published in: Physical Review A

DOI: 10.1103/PhysRevA.78.022316

Citation for published version (APA):
Commitments play an important role in modern day cryptography. Informally, a commitment allows one party to prove that she has made up her mind and cannot change it, while hiding the actual decision until later. Imagine two mutually distrustful parties Alice and Bob at distant locations. They can only communicate over a channel, but want to play the following game: Alice secretly chooses a bit $x$. Bob wants to be sure that Alice indeed has made her choice. At the same time, Alice wants to keep $x$ hidden from Bob until she decides to reveal it. To convince Bob that she made up her mind, Alice sends Bob a commitment. From the commitment alone, Bob cannot deduce what Alice sent. At a later time, Alice reveals $x$ and enables Bob to open the commitment. Bob can now check if Alice is telling the truth. This scenario is known as bit commitment.

Bit commitment is a very powerful cryptographic primitive with a wide range of applications. It has been shown that quantum oblivious transfer (QOT) [1] can be achieved provided there exists a secure bit commitment scheme [2, 3]. In turn, oblivious transfer is known to be sufficient for solving the general problem of secure two-party computation [4, 5]. Commitments are also useful for constructing zero-knowledge proofs [6]. Furthermore, a bit commitment protocol can be used to implement secure coin tossing [7]. Classically, unconditionally secure bit commitment is known to be impossible. Unfortunately after several quantum schemes were suggested [8, 9, 10], non-relativistic quantum bit commitment has also been shown to be impossible [11, 12, 13, 14, 15, 16]. Only very limited degrees of concealment and binding can be achieved [17]. In the face of these negative statements, what can we still hope to achieve?

### A. String Commitment

Here we take a different approach and look at the task of committing to a string of $n$ bits at once in the setting where Alice and Bob have unbounded resources. Since perfect bit commitment is impossible, perfect string commitment is impossible, too. However, is it possible to design meaningful string commitment schemes when we allow for a small ability to cheat on both Alice’s and Bob’s side? To make this question precise, we introduce a framework for the classification of string commitments in terms of the length $n$ of the string, Alice’s ability to cheat on $a$ bits and Bob’s ability to acquire $b$ bits of information before the reveal phase. Instead of asking for a perfectly binding commitment, we allow Alice to reveal up to $2^a$ strings successfully: Bob will accept any such string as a valid opening of the commitment. Formally, we demand that $\sum_{x \in \{0,1\}^n} p_x^A \leq 2^a$, where $p_x^A$ is the probability that Alice successfully reveals string $x$ during the reveal phase. Contrary to classical computing, Alice can always choose to perform a superposition of string commitments without Bob’s knowledge. Thus even for a perfectly binding string commitment we would only demand $\sum_{x \in \{0,1\}^n} p_x^A \leq 1$, since a strategy based on superpositions is indistinguishable from the “classical” honest behaviour of choosing a string beforehand and then committing to it. At the same time, we relax Bob’s security condition, and allow him to acquire at most $b$ bits of information before the reveal phase. The nature of his security definition is crucial to our investigation: If $b$ determines a bound on his probability to guess Alice’s string, then we prove that $a + b$ is at least $n$ (up to a
been introduced into the model. Salvail [19] showed that, with probability less than \( \varepsilon \) and honest Alice accepts.

Our proof makes use of privacy amplification with two-universal hash functions. If the protocol is executed multiple times in parallel, we prove that any quantum bit string commitment protocol with \( a + b < n \) is insecure. We refer to these results as “impossibilities”, as they show that QBSC schemes offer almost no advantage over the trivial classical protocol: Alice first sends \( b \) bits of the \( n \) bit string to Bob during the commit phase, and then supplies him with the remaining \( n - b \) bits in the reveal phase.

The second part of the paper is devoted to the “possibility” of QBSC. If we weaken our standard of security and measure Bob’s information gain in terms of the accessible information, it becomes possible to construct meaningful QBSC protocols with \( a = 2 \log_2 n + O(1) \) and \( b = 4 \). Our protocols are based on the effect of locking classical information in quantum states [18]. This surprising effect shows that given an initial shared quantum state, the transmission of \( \ell \) classical bits can increase the total amount of correlation by more than \( \ell \) bits. In Section III we show

**Possibility of \((n,a,b)\)-QBSC:**

For \( n \geq 3 \), there exist \((n,4\log_2 n + O(1),4)\)-QBSC protocols.

We then consider cheat-sensitive protocols: Even though Bob is in principle able to gain a large amount of information on Alice’s committed string, honest Alice has a decent probability of detecting such an attempt to cheat the protocol. We give an explicit tradeoff between Bob’s information gain, and Alice’s ability to catch him cheating. In Section IV we show

**Possibility of cheat-sensitive \((n,1,n/2)\)-QBSC:**

There exist a \((n,1,n/2)\)-QBSC that is cheat-sensitive against Bob. If Bob is detected cheating with probability less than \( \varepsilon \), then his classical information gain is less than \( 4\sqrt{\varepsilon} \log_2 d + 2\mu(2\sqrt{\varepsilon}) \) with \( \mu(x) = \min \{-x \log_2 x, 1/e\} \).

### I. PRELIMINARIES

#### A. Framework

We first formalize the notion of quantum string commitments in a quantum setting.

**Definition 1** An \((n,a,b)\)-Quantum Bit String Commitment (QBSC) is a quantum communication protocol between two parties, Alice (the committer) and Bob (the receiver), which consists of two phases and two security requirements.

- **(Commit Phase)** Assume that both parties are honest. Alice chooses a string \( x \in \{0,1\}^n \) with probability \( p_x \). Alice and Bob communicate and at the end Bob holds state \( \rho_x \).
- **(Reveal Phase)** If both parties are honest, Alice and Bob communicate and at the end Bob learns \( x \). Bob accepts.
- **(Concealing)** If Alice is honest, \( \sum_{x \in \{0,1\}^n} p_x^B \leq 2^k \), where \( p_x^B \) is the probability that Bob correctly guesses \( x \) before the reveal phase.
We say that Alice successfully reveals a string $x$ if Bob accepts the opening of $x$, i.e., he performs a test depending on the individual protocol to check Alice’s honesty and concludes that she was indeed honest. Note that quantumly, Alice can always commit to a superposition of different strings without being detected. Thus even for a perfectly binding bit string commitment (i.e., $a = 0$) we only demand that $\sum_{x \in \{0,1\}^n} p_x^A \leq 2^n$, whereas classically one wants that $p_x^B = \delta_{x,x'}$. Note that our concealing definition reflects Bob’s a priori knowledge about $x$. We choose an a priori uniform distribution (i.e., $p_x = 2^{-n}$) for $(n,a,b)$-QBSCs, which naturally comes from the fact that we consider $n$-bit strings. A generalization to any $(P_X,a,b)$-QBSC where $P_X$ is an arbitrary distribution is possible but omitted in order not to obscure our main line of argument. Instead of Bob’s guessing probability, one can take any information measure concealing definition reflects Bob’s a priori knowledge about $x$, pending on the individual protocol to check Alice’s honesty and concludes that she was indeed honest. Note from the fact that we consider $n$-bit strings. A generalization to any $(P_X,a,b)$-QBSCs, which naturally comes from the fact that we consider $n$-bit strings. A generalization to any $(P_X,a,b)$-QBSC where $P_X$ is an arbitrary distribution is possible but omitted in order not to obscure our main line of argument. Instead of Bob’s guessing probability, one can take any information measure.

\begin{align}
\xi(\mathcal{E}) &\equiv n - H_2(\rho_{AB}|\rho), \quad (1)
\end{align}

where $\rho_{AB} = \sum_x p_x|x\rangle\langle x| \otimes \rho_x$ and $\rho = \sum_x p_x \rho_x$ are only dependent on the ensemble $\mathcal{E} = \{p_x, \rho_x\}$. $H_2(\cdot|\cdot)$ is an entropic quantity defined in $\mathbb{H}$ $H_2(\rho_{AB}|\rho) \equiv -\log \text{Tr}((\mathbb{I} \otimes \rho^{-\frac{1}{2}})\rho_{AB})^2$. This quantity is directly connected to Bob’s maximal average probability of successful guessing the string:

**Lemma 1** Bob’s maximal average probability of successfully guessing the committed string, i.e., $\sup_M \sum_x p_x p_{y|x}^{B,M}$ where $M$ ranges over all measurements and $p_{y|x}^{B,M}$ is the conditional probability of guessing $y$ given $p_x$, obeys

$$\sup_M \sum_x p_x p_{y|x}^{B,M} \geq 2^{-H_2(\rho_{AB}|\rho)}.$$

**Proof.** By definition the maximum average guessing probability is lower bounded by the average guessing probability for a particular measurement strategy. We choose the square-root measurement which has operators $M_x = p_x^{-\frac{1}{2}} \rho_x^{-\frac{1}{2}} \rho_{AB}^{-\frac{1}{2}}$. $p_{y|x}^{B,x} = \text{Tr}(M_y \rho_x)$ is the probability that Bob guesses $x$ given $p_x$, hence

$$(1) \quad \log_2 \sum_x p_x p_{x,x,x}^{\max} \geq \log_2 \sum_x p_x^2 \text{Tr}(\rho^{-\frac{1}{2}} \rho_x \rho^{-\frac{1}{2}} \rho_x) = \log \text{Tr} \left( \left(\mathbb{I} \otimes \rho^{-\frac{1}{2}}\right)\rho_{AB} \right)^2 = -H_2(\rho_{AB}|\rho) \quad \square$$

Related estimates were derived in $\cite{35}$. For the uniform distribution $p_x = 2^{-n}$ we have from the concealing condition that $\sum_x p_x^B \leq 2^b$ which by Lemma 1 implies $\xi(\mathcal{E}) \leq b$ and hence the following lemma.

**Lemma 2** Every $(n,a,b)$-QBSC is an $(n,a,b)$-QBSC.$\xi$.

C. Tools

We now gather the essential ingredients for our proof. First, we show that every $(n,a,b)$-QBSC is an $(n,a,b)$-QBSC.$\xi$. The security measure $\xi(\mathcal{E})$ is defined by

$$\xi(\mathcal{E}) = n - H_2(\rho_{AB}|\rho), \quad (1)$$

where $\rho_{AB} = \sum_x p_x|x\rangle\langle x| \otimes \rho_x$ and $\rho = \sum_x p_x \rho_x$ are only dependent on the ensemble $\mathcal{E} = \{p_x, \rho_x\}$. $H_2(\cdot|\cdot)$ is an entropic quantity defined in $\mathbb{H}$ $H_2(\rho_{AB}|\rho) \equiv -\log \text{Tr}((\mathbb{I} \otimes \rho^{-\frac{1}{2}})\rho_{AB})^2$. This quantity is directly connected to Bob’s maximal average probability of successful guessing the string:

**Lemma 1** Bob’s maximal average probability of successfully guessing the committed string, i.e., $\sup_M \sum_x p_x p_{y|x}^{B,M}$ where $M$ ranges over all measurements and $p_{y|x}^{B,M}$ is the conditional probability of guessing $y$ given $p_x$, obeys

$$\sup_M \sum_x p_x p_{y|x}^{B,M} \geq 2^{-H_2(\rho_{AB}|\rho)}.$$

**Proof.** By definition the maximum average guessing probability is lower bounded by the average guessing probability for a particular measurement strategy. We choose the square-root measurement which has operators $M_x = p_x^{-\frac{1}{2}} \rho_x^{-\frac{1}{2}} \rho_{AB}^{-\frac{1}{2}}$. $p_{y|x}^{B,x} = \text{Tr}(M_y \rho_x)$ is the probability that Bob guesses $x$ given $p_x$, hence

$$\log_2 \sum_x p_x p_{x,x,x}^{\max} \geq \log_2 \sum_x p_x^2 \text{Tr}(\rho^{-\frac{1}{2}} \rho_x \rho^{-\frac{1}{2}} \rho_x) = \log \text{Tr} \left( \left(\mathbb{I} \otimes \rho^{-\frac{1}{2}}\right)\rho_{AB} \right)^2 = -H_2(\rho_{AB}|\rho) \quad \square$$

Related estimates were derived in $\cite{35}$. For the uniform distribution $p_x = 2^{-n}$ we have from the concealing condition that $\sum_x p_x^B \leq 2^b$ which by Lemma 1 implies $\xi(\mathcal{E}) \leq b$ and hence the following lemma.

**Lemma 2** Every $(n,a,b)$-QBSC is an $(n,a,b)$-QBSC.$\xi$.

Furthermore, we make use of the following theorem, known as privacy amplification against a quantum adversary. In our case, Bob holds the quantum memory and privacy amplification is used to find Alice’s attack.
Theorem 1 (Th. 5.5.1 in [34] (see also [36])) Let \( G \) be a class of two-universal hash functions from \( \{0,1\}^n \) to \( \{0,1\}^s \). Application of \( g \in G \) to the random variable \( X \) maps the ensemble \( \mathcal{E} = \{p_x, \rho_x\} \) to \( \mathcal{E}_g = \{q^g_x, \sigma^g_x\} \) with probabilities \( q^g_x = \sum_{x \in G^{-1}(y)} p_x \) and quantum states \( \sigma^g_x = \sum_{x \in G^{-1}(y)} p_x \rho_x \). Then

\[
\frac{1}{|G|} \sum_{g \in G} d(\mathcal{E}_g) \leq 1 - 2^{-\frac{1}{2} \|H_2(\rho_{AB}|\rho) - s\}},
\]

where \( d(\mathcal{E}) \equiv \sum_{x \in G} p_x |x(x) \otimes \rho_x, \mathbb{I}/2^n \otimes \rho\) (and similarly for \( d(\mathcal{E}_g) \)) and \( \delta(\alpha, \beta) \equiv \frac{1}{2}||\alpha - \beta||_1 \) with \( ||A||_1 = \text{Tr} \sqrt{A^\dagger A} \).

Finally, the following reasoning, previously used to prove the impossibility of quantum bit commitment [11], will be essential: Suppose \( \rho_0 \) and \( \rho_1 \) are density operators that correspond to a commitment of a “0” or a “1” respectively. Let \( |\phi_0\rangle \) and \( |\phi_1\rangle \) be the corresponding purifications on the joint system of Alice and Bob. If \( \rho_0 \) equals \( \rho_1 \) then Alice can find a local unitary transformation \( U \) that she can apply to her part of the system and satisfying \( |\phi_1\rangle = U \otimes \mathbb{I} |\phi_0\rangle \). This enables Alice to change the total state from \( |\phi_0\rangle \) to \( |\phi_1\rangle \) and thus cheat. This also holds in an approximate sense [11], used here in the following form:

**Lemma 3** Let \( \delta(\rho_0, \rho_1) \leq \epsilon \) and assume that the bit-commitment protocol is error-free if both parties are honest. Then there is a method for Alice to cheat such that the probability of successfully revealing a 0 given that she committed to a 1 is greater or equal to \( 1 - \sqrt{2\epsilon} \).

**Proof.** \( \delta(\rho_0, \rho_1) \leq \epsilon \) implies \( F(\rho_0, \rho_1) \geq 1 - \epsilon \). \( F(\cdot, \cdot) \) is the fidelity of two quantum states, which equals \( \max_{\alpha, \beta} \langle \alpha | \rho | \beta \rangle \) by Uhlmann’s theorem. Here, \( |\phi_0\rangle \) and \( |\phi_1\rangle \) are the joint states after the commit phase and the maximization ranges over all unitaries \( U \) on Alice’s (i.e. the purification) side. Let \( |\psi_0\rangle = U \otimes \mathbb{I} |\phi_1\rangle \) for a \( U \) achieving the maximization. Then

\[
\delta(|\phi_0\rangle \langle \phi_0|, |\psi_0\rangle \langle \psi_0|) = 1 - \frac{1}{2} |\langle \phi_0 | \psi_0 \rangle| \leq 1 - (1 - \epsilon)^2 \leq \sqrt{2\epsilon}.
\]

If both parties are honest, the reveal phase can be regarded as a measurement resulting in a distribution \( P_Y (P_Z) \) if \( |\phi_0\rangle \langle \phi_0| \) was the state before the reveal phase. The random variables \( Y \) and \( Z \) carry the opened bit or the value ‘reject (r)’. Since the trace distance does not increase under measurements, \( \delta(P_Y, P_Z) \leq \delta(|\phi_0\rangle \langle \phi_0|, |\psi_0\rangle \langle \psi_0|) \leq \sqrt{2\epsilon} \). Hence \( \frac{1}{2} |\langle P_Y (0) - P_Z (0) \rangle| + |\langle P_Y (1) - P_Z (1) \rangle| + |\langle P_Y (r) - P_Z (r) \rangle| \leq \sqrt{2\epsilon} \). Since \( |\phi_0\rangle \) corresponds to Alice’s honest commitment to 0 we have \( P_Y (0) = 1, P_Y (1) = P_Y (r) = 0 \) and hence \( P_Z (0) \geq 1 - \sqrt{2\epsilon} \).

**II. IMPOSSIBILITY**

The proof of our impossibility result consists of three steps: in the previous section, we saw that any \((n, a, b)\)-QBSC is also an \((n, a, b)\)-QBSC\( \xi \) with the security measure \( \xi(\mathcal{E}) \) defined eq. [1]. Below, we prove that an \((n, a, b)\)-QBSC\( \xi \) can only exist for values \( a, b \) and \( n \) obeying \( a + b + c \geq n \), where \( c \) is a constant independent of \( a, b \) and \( n \). This in turn implies the impossibility of an \((n, a, b)\)-QBSC for such parameters. At the end of this section we show that many executions of the protocol can only be secure if \( a + b \geq n \).

The intuition behind our main argument is simple: To cheat, Alice first chooses a two-universal hash function \( g \). She then commits to a superposition of all strings of which \( g(x) = y \) for a specific \( y \). We know from the privacy amplification theorem above, however, that even though Bob may gain some knowledge about \( x \), he is entirely ignorant about \( y \). But then Alice can change her mind and move to a different set of strings for which \( g(y) = y' \) with \( y \neq y' \) as we saw above! The following figure illustrates this idea.

![FIG. 1: Moving from y to y′.](image-url)
state of Alice and Bob at the end of the commit phase is thus \(|\psi_{y}^{g}⟩ = \left(\sum_{x \in g^{-1}(y)} |x⟩|\sigma_{x}\rangle\right) / \sqrt{|g^{-1}(y)|}\). The reduced states on Bob’s side are \(σ_{y} = \frac{1}{|g|} \sum_{x \in g^{-1}(y)} P_{x} \rho_{x}\) with probability \(q_{y}^{g} = \frac{1}{|g|} \sum_{x \in g^{-1}(y)} P_{x}\). We denote this ensemble by \(E_{y}\). Let \(σ = σ_{y} = \sum_{y} q_{y}^{g} |ψ_{y}^{g}⟩\) for all \(g\).

We now apply Theorem 1 with \(s = n - m\) and \(ξ(E) < b\) to obtain \(\frac{1}{|g|} \sum_{g \in d(E_{y})} d(E_{y}) \leq ε\) where \(ε = \frac{1}{2} \left(1 - \frac{1}{2}\right)^{(m - b)}\). Hence, there is at least one \(g\) such that \(d(E_{y}) \leq ε\); intuitively, this means that Bob knows only very little about the value of \(g(x)\). This \(g\) defines Alice’s cheating strategy. It is straightforward to verify that \(d(E_{y}) \leq ε\) implies

\[
2^{-(n-m)} \sum_{y} δ(σ, σ_{y}) \leq 2ε. \tag{3}
\]

Let us therefore assume without loss of generality that Alice chooses \(y_{0} ∈ Y\) with \(δ(σ, σ_{y_{0}}) ≤ 2ε\).

Clearly, the probability to successfully reveal some \(x\) in \(g^{-1}(y)\) given \(|ψ_{y_{0}}^{g}⟩\) is one. Note that Alice learns \(x\), but can’t pick it; she committed to a superposition and is chosen randomly by measurement. Thus the probability to reveal \(y\) (i.e. to reveal an \(x\) such that \(y = g(x)\)) given \(|ψ_{y_{0}}^{g}⟩\) is one. Let \(\overline{p}_{x}\) and \(\overline{q}_{y}^{g}\) denote the probabilities to successfully reveal \(x\) and \(y\) respectively and \(\overline{p}_{x|y}^{g}\) be the conditional probability to successfully reveal \(x\), given \(y\). We have

\[
\sum_{x} \overline{p}_{x} = \sum_{y} \overline{q}_{y}^{g} \sum_{x \in g^{-1}(y)} \overline{p}_{x|y}^{g} \geq \sum_{y} \overline{q}_{y}^{g}.
\]

Recall that Alice can transform \(|ψ_{y_{0}}^{g}⟩\) approximately into \(|ψ_{y}^{g}⟩\) if \(σ_{y_{0}} \approx σ_{y}\) by applying local transformations to her part alone. It follows from Lemma 3 that we can estimate the probability of revealing \(y\), given that the state was really \(|ψ_{y_{0}}⟩\). Since this reasoning applies to all \(y\), on average, we have

\[
\sum_{y} \overline{q}_{y}^{g} \geq \sum_{y} \left(1 - 2^{\frac{1}{2}} δ(σ_{y_{0}}, σ_{y})^{\frac{1}{2}}\right) \geq 2^{n-m} - 2^{\frac{1}{2}} 2^{n-m} (2^{m-n} \sum_{y} δ(σ_{y_{0}}, σ_{y})^{\frac{1}{2}}) \geq 2^{n-m}[1 - 2^{\frac{1}{2}} (2^{m-n} \sum_{y} δ(σ_{y_{0}}, σ) + δ(σ, σ_{y}))^{\frac{1}{2}}] \geq 2^{n-m}(1 - 2(2ε)^{\frac{1}{2}}),
\]

where the first inequality follows from Lemma 3, the second from Jenson’s inequality and the concavity of the square root function, the third from the triangle inequality and the fourth from eq. (3) and \(δ(σ_{y_{0}}, σ) ≤ 2ε\). Recall that to be secure against Alice, we require \(2m ≥ 2^{n-m}(1 - 2(2ε)^{\frac{1}{2}})\). We insert \(ε = \frac{1}{2} \left(1 - \frac{1}{2}\right)^{(m - b)}\), define \(m = b + γ\) and take the logarithm on both sides to get

\[
a + b + δ \geq n, \tag{4}
\]

where \(δ = γ - \log_{2}(1 - 2^{-\gamma/4+1})\). Keeping in mind that \(1 - 2^{-\gamma/4+1} > 0\) (equivalently \(γ > 4\)), we find that the minimum value of \(δ\) for which eq. (4) is satisfied is \(δ = 5 \log_{2}5 - 4\) and arises from \(γ = 4(\log_{2}5 - 1)\). Thus, no \((n, a, b)\)-QBSC\(_{ξ}\) with \(a + b + 5 \log_{2}5 - 4 < n\) exists.

Since the constant \(c\) does not depend on \(a\), \(b\) and \(n\), multiple parallel executions of the protocol in the form of multiple simultaneous commit phases followed by the corresponding opening phases, can only be secure if \(a + b ≥ n:\)

**Proposition 1** Let \(P\) be an \((n, a, b)\)-QBSC\(_{ξ}\) or \((n, a, b)\)-QBSC. The \(m\)-fold parallel execution of \(P\) will be insecure if \(a + b < n - c/m\). In particular, no \((n, a, b)\)-QBSC\(_{ξ}\) or \((n, a, b)\)-QBSC with \(a + b < n\) can be executed securely an arbitrary number of times in parallel. Furthermore, no \((n, a, b)\)-QBSC\(_{ξ}\) with \(a + b < n\) and \(ξ\) the Holevo information can be executed securely an arbitrary number of times in parallel.

**Proof.** In the following, we assume wlog that \(a\) and \(b\) are the smallest cheat parameters for \(P\). Let \(Q\) denote the \((nm, am, bm)\)-QBSC\(_{ξ}\) or \((nm, am, bm)\)-QBSC protocol obtained by executing \(P\) \(m\) times in parallel. By Theorem 2 \(Q\) is insecure if \(am + bm < nm - c\). Since \(a\) and \(b\) were assumed to be the smallest cheat parameters for \(P\), the product cheating attack by Alice and Bob lead to the estimates \(am ≥ am\) and \(bm ≥ bm\), respectively. Therefore, the \(m\) fold execution of \(P\) is insecure, if \(am + bm ≤ am + bm < nm - c\) or \(a + b < c/m\).

In order to prove the result about Holevo information QBSC, we will use a slightly different characterisation of privacy amplification in the proof of Theorem 2. In this characterisation, the right hand side of eq. (1) is replaced by \(κ + 2^{-\frac{1}{2}} |H_{min}(ρ_{AB} | ρ_{AB}^{-})|\) for an arbitrary \(κ > 0\) [34 Corollary 5.61]. Going through the proof with this change in mind, one sees that \(Q\) is not a \((nm, am, bm)\)-QBSC\(_{ξ}\) for \(ξ(E) = nm - H^{κ}_{min}(ρ_{AB} | ρ_{AB}^{-})\) if \(am + bm + δ ≤ mn\). Here, \(E\) is the ensemble corresponding to \(Q\) and \(ρ_{AB}\) and \(ρ_{AB}^{-}\) the related states; \(δ ≡ δ(κ)\) is a positive constant independent of \(n\). Since \(E\) is \(Ε^{⊗m}\) and thus \(ρ_{AB} = ρ_{AB}^{⊗m}\) and \(ρ_{AB}^{-} = ρ_{AB}^{⊗m}\) we are able to invoke the estimate

\[
\frac{1}{m} H^{κ}_{min}(ρ_{AB}^{⊗m} | ρ_{AB}^{⊗m}) ≥ H(ρ_{AB}) - H(p) - 3λ
\]

where \(λ(κ, m) → 0\) as \(m → ∞\) [34] Chain rule in Theorem 3.1.12 and Theorem 3.3.4] in order to conclude that \(Q\) is not a \((nm, am, bm)\)-QBSC\(_{m(ξ) + 2κ}\) if \(am + bm + δ < mn\). This shows that if \(P\) is a \((nm, am, bm)\)-QBSC\(_{m(ξ) + 2κ}\) with \(a_{m}m + β_{m}m ≤ am + bm < nm - δ\), i.e. \(a_{m} + β_{m} < n - δ/m\), then its \(m\)-fold execution cannot be secure. Taking \(m\) to infinity we see that if \(P\) is an \((n, a, b)\)-QBSC\(_{ξ}\) with \(a + b < n\) then it cannot be executed securely an arbitrary number of times in parallel.

It follows directly from [37] that the results in this section also hold in the presence of superselection rules.
III. POSSIBILITY

Surprisingly, if one is willing to measure Bob’s ability to learn $x$ using the accessible information, non-trivial protocols become possible. These protocols are based on a discovery known as “locking of classical information in quantum states” [18].

A. A Family of Protocols

The protocol, which we call LOCKCOM($n$, $U$), uses this effect and is specified by a set $U = \{U_1, \ldots, U_{|U|}\}$ of unitaries.

- Commit phase: Alice has the string $x \in \{0,1\}^n$ and randomly chooses $r \in \{1, \ldots, |U|\}$. She sends the state $U_r|x\rangle$ to Bob, where $U_r \in U$.

- Reveal phase: Alice announces $r$ and $x$. Bob applies $U_r^\dagger$ and measures in the computational basis to obtain $x'$.

We first show that our protocol is secure with respect to Definition 1 if Alice is dishonest. Note that our proof only depends on the number of unitaries used, and is independent of a concrete instantiation of the protocol.

Lemma 4 Any LOCKCOM($n$,$U$) protocol is log($|U|$)-binding, i.e. $2^a \leq |U|$,.

Proof. Let $p_A^x$ denote the probability that Alice reveals $x$ successfully. Then, $p_A^x = \sum_r p_A^x,r$, where $p_A^x,r$ is the probability that $x$ is accepted by Bob when the reveal information was $r$. Let $\rho$ denote the state of Bob’s system. Summation over $x$ over yields

$$\sum_x p_A^x \leq \sum_{x,r} p_A^x,r = \sum_r \text{Tr}\{|x\rangle\langle x|U_r^\dagger\rho U_r\} = \sum_r \text{Tr}\rho \leq |U|,$$

hence $a \leq \log_2 |U|$.

In order to examine security against a dishonest Bob, we have to consider the actual form of the unitaries. We first show that there do indeed exist interesting protocols. Secondly, we present a simple, implementable, protocol. To see that interesting protocols can exist, let Alice choose a set of $O(n^4)$ unitaries independently according to the Haar measure (approximated) and announce the resulting set $U$ to Bob. They then perform LOCKCOM($n$, $U$). Following the work of [39], we now show that this variant is secure against Bob with high probability in the sense that there exist $O(n^4)$ unitaries that bring Bob’s accessible information down to a constant: $I_{acc}(E) \leq 4$.

Theorem 3 For $n \geq 3$, there exist $(n, 4\log_2 n + O(1), 4)$-QBSC$_{I_{acc}}$ protocols.

Proof. Let $U_{ran}$ denote the set of $m$ randomly chosen bases and consider the LOCKCOM($n, a, b$) scheme using unitaries $U = U_{ran}$. Security against Alice is again given by Lemma 4. We now need to show that this choice of unitaries achieves the desired locking effect and thus security against Bob. Again, let $d = 2^n$ denote the dimension. It was observed in [18] that

$$I_{acc} \leq \log_2 d + \max_{|\phi\rangle} \sum_i \frac{1}{m} H(X_i),$$

where $X_j$ denotes the outcome of the measurement of $|\phi\rangle$ in basis $j$ and the maximum is taken over all pure states $|\phi\rangle$. According to [18, Appendix B] there is a constant $C' > 0$ such that

$$\text{Pr} \{\inf_{|\phi\rangle} \left( \sum_{j=1}^m \frac{1}{m} H(X_j) \right) \leq (1 - \epsilon) \log_2 d - 3 \} \leq \left( \frac{10}{\epsilon} \right)^{2d} 2^{-m(C' \log_2 d - 1)},$$

for $d \geq 7$ and $\epsilon \leq 2/5$. Set $\epsilon = 1/\log_2 d$. The RHS of the above equation then decreases provided that $m > \frac{8}{\epsilon^2} (\log_2 d)^4$. Thus with $d = 2^n$ and $\log_2 m = 4 \log_2 n + O(1)$, the accessible information is then $I_{acc} \leq \log_2 d - (1 - \epsilon) \log_2 d + 3 = \epsilon \log_2 d + 3 = 4$ for our choice of $\epsilon$. □

Unfortunately, the protocol is inefficient both in terms of computation and communication. It remains open to find an efficient constructive scheme with those parameters.

In contrast, for only two bases, an efficient construction exists and uses the identity and the Hadamard transform as unitaries. For this case, the security of the standard LOCKCOM protocol follows immediately:

Theorem 4 LOCKCOM($n$, $\{1^\otimes n, H^\otimes n\}$) is a $(n, 1, n/2)$ - QBSC$_{I_{acc}}$ protocol.

Proof. It is sufficient to apply Lemma 4 and the fact that for Bob $I_{acc} \leq n/2$ [18, 39]. □

IV. A CHEAT-SENSITIVE PROTOCOL

A. Scenario and Result

We now extend the protocol above to be cheat-sensitive against Bob. That is, even though Bob may be able to gain a lot of information on the committed string, Alice has a decent probability of catching Bob if he actually tries to extract such information [47].

We first extend our definition to accommodate cheat-sensitivity against Bob.
Definition 2 A \((n, a, b)\)-B-QBSC is cheat-sensitive against Bob if there is a non-zero probability that he will be detected by Alice when he cheats.

We elaborate below on the scenario in which we analyse Bob’s cheating and thus make precise what we mean by saying Bob cheats.

The following protocol is a modification of LOCKCOM\((n, U)\) which incorporates cheat-sensitivity against Bob.

**Protocol 1: CS-Bob-LOCKCOM\((n, U)\)**

1: Commit phase: Alice randomly chooses the string \(x \in \{0, 1\}^n\) and a unitary \(U_r\) from a set of unitaries \(U\) known to both Alice and Bob. She sends the state \(U_r|x\).

2: Reveal phase: Alice sends \(r\) to Bob, he applies \((U_r)^\dagger\) to the state that he received from Alice and measures in the computational basis. His outcome is denoted by \(y\).

3: Confirmation phase: Bob sends \(y\) to Alice. If Alice is honest, and if \(x = y\) she declares ‘accept’ otherwise ‘abject’.

We proved in Theorem 4 that CS-Bob-LOCKCOM\((n, \{I^n, H^n\})\) is a \((n, 1, n/2)\)-Iacc-quantum string commitment protocol. In fact this result can be extended to dimensions different from \(d = 2^n\) where one can show that CS-Bob-LOCKCOM\((\log_2 d, \{I, U\})\), where \(U\) is the Fourier transform, is a \((\log_2 d, 1, \log_2 d/2)\)-Iacc-quantum string commitment protocol.

We now restrict our attention to these protocols and prove that a dishonest Bob is detected whenever he has obtained a non-zero amount of information about \(x\) before the reveal stage [18]. More precisely, we give a tradeoff for cheat detection versus Holevo-information gain against a dishonest Bob, with the property that every nonzero Holevo-information gain leads to a nonzero detection probability of Bob.

**Theorem 5** If Bob is detected cheating with probability less than \(\epsilon\), then his Holevo information gain obeys

\[
\chi (C^C) \leq 4\sqrt{\epsilon} \log_2 d + 2\mu(2\sqrt{\epsilon}).
\]

As a corollary we find that CS-Bob-LOCKCOM\((\log_2 d, \{I, U\})\) is cheat sensitive against Bob.

**Corollary 1** Bob will be detected cheating with a nonzero probability, if he gathers a nonzero amount of Holevo information.

**B. Proof**

We start this section with a description of the sequence of events for the case where Alice is honest and Bob applies a general cheating strategy (see also Figure 2).

- The commit phase of the protocol \(\text{LOCKCOM}(\log_2 d, \{I, U\})\) is equivalent to the following procedure: Alice prepares the state

\[
|\psi\rangle = \frac{1}{\sqrt{2d}} \sum_{x,r} |x\rangle \chi (r) |r\rangle |r'\rangle U^r |x\rangle^Y
\]

on the system \(XRYR'\) and sends system \(Y\) (over a noiseless quantum channel) to Bob. It is understood that \(U^0 = I\) and \(U^1 = U\). Note that \(R'\) contains an identical copy of \(R\) and corresponds to the reveal information.

- Bob’s most general cheating operation can be described by a unitary matrix \(V_{\text{cheat}}\) that splits the system \(Y\) into \(C\) and \(Q\). \(C\) contains by definition the information gathered during cheating and is not touched upon later on [48].

\[
V_{\text{cheat}} : Y \rightarrow CQ
\]

The map \(V_{\text{cheat}}\) followed by the partial trace over \(Q\) is denoted by \(\Lambda^C\) and likewise \(V_{\text{cheat}}\) followed by the partial trace over \(C\) is denoted by \(\Lambda^Q\).

- Alice sends the reveal information \(R'\) to Bob.

- Bob applies a preparation unitary \(V_{\text{prepare}}\) to his system. Since \(C\) will not be touched upon, the most general operation acts on \(R'Q\) only:

\[
V_{\text{prepare}} : R'Q \rightarrow R'ST.
\]

Bob then sends \(S\) to Alice and keeps \(T\).

- Alice measures \(S\) in the computational basis and compares the outcome to her value in \(X\). If the values do not agree, we say that Alice has detected Bob cheating. The probability for this happening is given by

\[
\frac{1}{d} \sum_{x=1}^d \left(1 - \text{Tr} |x\rangle \langle x| \rho_x^S\right),
\]

where \(\rho_x^S = \text{Tr}_{XRR'R} |x\rangle \langle x| |\psi\rangle \langle \psi|_{XRR'RST}\), and \(|\psi\rangle_{XRR'RST}\) is the pure state of the total system after Bob’s application of \(V_{\text{prepare}}\).

Note that Alice measures in the computational basis since for honest Bob \(V_{\text{prepare}} = \sum_{r' \in \{0, 1\}} |r\rangle \langle r'| \otimes (U^r)^\dagger\), in which case his outcome agrees with the committed value of an honest Alice.

Before we start with the proof of Theorem 5 we define ensembles depending on the classical information contained in \(XR\), i.e. for \(Z \in \{C, Q\}\), define \(\mathcal{E}_Z^Z = \{p_r, \rho_{x|r}\}\) with

\[
\rho_{x|r} = \frac{1}{p_r \rho_r} \text{Tr}_{XRR'CQ \setminus Z} |x\rangle \langle x| |\psi\rangle \langle \psi|_{XRR'CQ}
\]
with Holevo information for $\mathcal{E}_0$ given by
\[
\chi(\Lambda(\mathcal{E}_0)) = H\left(\frac{1}{d} \sum_i \Lambda(|i\rangle\langle i|)\right) - \frac{1}{d} \sum_i H(\Lambda(|i\rangle\langle i|))
\]
and similarly for $\mathcal{E}_1$. Consider also the quantum mutual information of $\Lambda$ relative to the maximally mixed state $\tau = \frac{1}{d} I$, which is the average state of either $\mathcal{E}_0$ or $\mathcal{E}_1$:
\[
I(\tau; \Lambda) = H(\tau) + H(\Lambda(\tau)) - H((I \otimes \Lambda)(|\psi_d\rangle\langle \psi_d|))
\]
where $|\psi_d\rangle$ is a maximally entangled state in dimension $d$ purifying $\tau$.

**Lemma 5 (Channel Uncertainty Relation)**

Let $U$ be the Fourier transform of dimension $d$, i.e. of the Abelian group $\mathbb{Z}_d$ of integers modulo $d$. More generally, $U$ can be a Fourier transform of any finite Abelian group labeling the ensemble $\mathcal{E}_0$, e.g. for $d = 2^t$, and the group $\mathbb{Z}_2^t$, $U = H^\otimes t$ with the Hadamard transform $H$ of a qubit. Then for all CPTP maps $\Lambda$,
\[
\chi(\Lambda(\mathcal{E}_0)) + \chi(\Lambda(\mathcal{E}_1)) \leq I(\tau; \Lambda).
\]

The following technical lemma is a technical consequence of Fannes’ inequality.

**Lemma 6** Let $\mathcal{E} = \{p_i, \rho_i = |\psi_i\rangle\langle \psi_i|\}$ be an ensemble of pure states and $\tilde{\mathcal{E}} = \{p_i, \sigma_i\}$ be an ensemble of mixed states, both on $\mathbb{C}^d$. If $\sum_i p_i |\psi_i\rangle\langle \psi_i| \geq 1 - \epsilon$, then
\[
|\chi(\tilde{\mathcal{E}}) - \chi(\mathcal{E})| \leq 4\sqrt{\epsilon} \log_2 d + 2\mu(2\sqrt{\epsilon}),
\]
where $\mu(x) = \min\{-x \log_2 x, \frac{1}{e}\}$.

**Proof.** The justification of the estimate
\[
e \geq \sum_i p_i (1 - Tr \rho_i \sigma_i) \geq \sum_i p_i \delta_i^2 \geq \left(\sum_i p_i \delta_i\right)^2,
\]
where $\delta_i = \delta(\rho_i, \sigma_i)$ is as follows: the second inequality is a standard relation between the fidelity and the trace distance and the third follows from the convexity of the square function. Strong convexity of the trace distance implies $\delta(\rho, \sigma) \leq \sqrt{\epsilon}$. Fannes’ inequality will be applied to the overall state
\[
|H(\rho) - H(\sigma)| \leq 2\sqrt{\epsilon} \log_2 d + \min\{\eta(2\sqrt{\epsilon}), \frac{1}{e}\}
\]
where $\eta(x) = -x \log_2 x$, and to the individual ones
\[
\sum_i p_i |H(\sigma_i) - H(\rho_i)| \leq \left(\sum_i p_i \delta_i\right)2 \log_2 d + \sum_i p_i \min\{\eta(2\delta_i), \frac{1}{e}\}
\leq \sqrt{\epsilon} 2 \log_2 d + \min\{\eta(2\sqrt{\epsilon}), \frac{1}{e}\}
\]
where the last inequality is true by the concavity of $\eta(x)$. Inserting these estimates in the Holevo $\chi$ quantities.
\( \chi(\mathcal{E}) = H(\rho) \) and \( \chi(\tilde{\mathcal{E}}) = H(\sigma) - \sum_i p_i H(\sigma_i) \) concludes the proof. \( \square \)

Proof. [Proof of Theorem 5.] Let \( \mathcal{E}_0 \) and \( \mathcal{E}_1 \) be defined as in Lemma 5. In the commit phase of the protocol, Alice chooses one of the ensembles (each with probability \( \frac{1}{2} \)), and one of the states in the ensemble (each with probability \( \frac{1}{2} \)). The justifications for the following estimate are given in a list below.

\[
\begin{align*}
\chi(\mathcal{E}_C^0) + \chi(\mathcal{E}_C^1) & = \chi(\Lambda_C(\mathcal{E}_0)) + \chi(\Lambda_C(\mathcal{E}_1)) \\
& \leq I(X|RR';C) \\
& = 2H(X|RR') - I(XRR';Q) \\
& \leq 2H(XR) - \chi(A^Q(\mathcal{E}_0)) - \chi(A^Q(\mathcal{E}_1)) \\
& = 2H(XR) - \chi(\mathcal{E}_0^C) - \chi(\mathcal{E}_1^C) \\
& \leq 2H(XR) - \chi(\mathcal{E}_0^C) - \chi(\mathcal{E}_1^C) - \chi(\mathcal{E}_1^C) \\
& = 2H(XR) - 2\chi(\mathcal{E}_1^C).
\end{align*}
\]

Inserting inequality (16) into inequality (15) and noting that \( H(XR) = H(Y) = \log_2 d \) proves the claim. \( \square \)

This proves cheat-sensitivity against Bob for the simplest protocol of the LOCKCOM family.

V. CONCLUSION

We have introduced a framework for quantum commitments to a string of bits. Even though string commitments are weaker than bit commitments, we showed that under strong security requirements, there are no such non-trivial protocols. A property of quantum states known as locking, however, allowed us to propose meaningful protocols for a weaker security demand. Since the completion of our original work [10], Tsurumaru [11] has also proposed a different QBSC protocol within our framework.

Furthermore, we have shown that one such protocol can be made cheat-sensitive. It is an interesting open question to derive a tradeoff between Bob’s ability to gain information and Alice’s ability to detect him cheating for the protocol of Theorem 3 as well.

A drawback of weakening the security requirement is that LOCKCOM protocols are not necessarily composable. Thus, if LOCKCOM is used as a sub-protocol in a larger protocol, the security of the resulting scheme has to be evaluated on a case by case basis. However, LOCKCOM protocols are secure when executed in parallel. This is a consequence of the definition of Alice’s security parameter and the additivity of the accessible information [12, 43], and sufficient for many cryptographic purposes.

However, two important open questions remain: First, how can we construct efficient protocols using more than two bases? It may be tempting to conclude that we could simply use a larger number of mutually unbiased bases, such as given by the identity and Hadamard transform. Yet, it has been shown [44] that using more mutually unbiased bases does not necessarily lead to a better locking effect and thus better string commitment protocols. Second, are there any real-life applications for this weak quantum string commitment?

Acknowledgments

We thank J. Barrett, A. Broadbent, I. Damgård, A. Kent, S. Massar, R. Renner, R. Spekkens and R. de Wolf for discussions. We also thank R. Jain for discussion on his work [45], where, following our preprint [40], he used a different method to prove that \((n,a,b))\)-QBSC_{\chi}_s with \(a + 16b + 31 < n\) do not exist.

We thank a DAAD Doktorandenstipendium, the EPSRC, the Magdalene College Cambridge, CFI, CIFAR, CIPI, CRC, NSERC, PREA and OIT, the NWO vici project 2004-2009, EU project RESQ IST-2001-37559,
[1] C. H. Bennett, G. Brassard, C. Crépeau, and M.-H. Kus- 

bieszewski, in CRYPTO ’91: Proceedings of the 11th An-

nual International Cryptology Conference on Advances in


30–39.


IEEE International Conference on Computers, Systems and


[10] G. Brassard, C. Crépeau, R. Jozsa, and D. Langlois, in


3410 (1997).


republished in “Quantum Computing, where do we want

to go tomorrow?” edited by S. Braunstein, Wiley-VCH, 


012310 (2002).

[18] D. DiVincenzo, M. Horodecki, D. Leung, J. Smolin, and


1462 of Lecture Notes in Computer Science, pp. 338–353.


of Physics 6 (2004).

[21] I. Damgård, S. Fehr, L. Salvail, and C. Schaffner, in


[22] I. Damgård, S. Fehr, R. Renner, L. Salvail, and C.


360–378.


ration.


[27] A. Winter, A. Nascimento, and H. Imai, in Proceedings

of 9th Cirencester Crypto and Coding (Springer, 2003),

vol. 2989 of Lecture Notes in Computer Science.