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

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

DOI
10.1103/PhysRevA.78.022316

Publication date
2008

Published in
Physical Review A

Possibility, Impossibility and Cheat-Sensitivity of Quantum Bit String Commitment

Harry Buhrman,[1] Matthias Christandl,[2,*] Patrick Hayden,[3] Hoi-Kwong Lo,[4] and Stephanie Wehner[1,†]

[1] *CWI, Kruislaan 413, 1098 SJ Amsterdam, The Netherlands*
[2] *DAMTP, University of Cambridge, Wilberforce Road, Cambridge, CB3 0WA, U.K.*
[3] *School of Computer Science, McGill University, Montreal, Canada*
[4] *Department of ECE and Physics, University of Toronto, Canada M5G 3G4*

(Dated: November 9, 2007)

Unconditionally secure non-relativistic bit commitment is known to be impossible in both the classical and the quantum worlds. But when committing to a string of n bits at once, how far can we stretch the quantum limits? In this paper, we introduce a framework for quantum schemes where Alice commits a string of n bits to Bob in such a way that she can only cheat on a bits and Bob can learn at most b bits of information before the reveal phase. Our results are two-fold: we show by an explicit construction that in the traditional approach, where the reveal and guess probabilities form the security criteria, no good schemes can exist: $a+b$ is at least n. If, however, we use a more liberal criterion of security, the accessible information, we construct schemes where $a = 4\log_2 n + O(1)$ and $b = 4$, which is impossible classically. We furthermore present a cheat-sensitive quantum bit string commitment protocol for which we give an explicit tradeoff between Bob's ability to gain information about the committed string, and the probability of him being detected cheating.

PACS numbers:

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 x. To convince Bob that she made up her mind, Alice sends Bob a commitment. From the commitment alone, Bob cannot deduce x. 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

*matthias.christandl@qubit.org
†wehner@cwi.nl

small constant). We write (n,a,b)-QBSC for a quantum bit string commitment protocol where the string has length n and a and b are the security parameters for Alice and Bob as explained in detail below. In Section II, we show

Impossibility of (n,a,b)-QBSC:
Every (n,a,b)-QBSC scheme with $a+b+c<n$ is insecure, where $c\approx 7.61$.

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 QBSCs 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 $a = 4\log_2 n + O(1)$ 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 ℓ classical bits can increase the total amount of correlation by more than ℓ bits. In Section III, we show

Possibility of $(n,a,b)-\mathbf{QBSC}_{I_{acc}}$:
For $n\geq 3$, there exist $(n, 4\log_2 n+O(1), 4)-\mathrm{QBSC}_{I_{acc}}$ 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 $(n,1,n/2)-\mathbf{QBSC}_{I_{acc}}$:
There exist a $(n,1,n/2)-\mathrm{QBSC}_{I_{acc}}$ that is cheat-sensitive against Bob. If Bob is detected cheating with probability less than ε, then his classical information gain is less than $4\sqrt{\varepsilon}\log_2 d + 2\mu(2\sqrt{\varepsilon})$ with $\mu(x)=\min\{-x\log_2 x, 1/e\}$.

B. Related Work

To obtain bit commitment, different restrictions have been introduced into the model. Salvail [19] showed that, for any fixed n, secure bit commitment is possible provided that the sender is not able to perform generalized measurements on more then n qubits coherently. Large n coherent measurements are not yet feasible, so his result provides an implementation which is secure under a plausible technological assumption. DiVincenzo, Smolin and Terhal took a different approach [20], showing that if the bit commitment is forced to be ancilla-free, a type of asymptotic security is still possible. Bit commitment is also possible if the adversary's quantum storage is bounded [21, 22, 23] or noisy [24]. Classically, introducing restrictions can also open new possibilities. Cachin, Crépeau and Marcil have shown how to implement bit commitment via oblivious transfer under the assumption that the size of the receiver's memory is bounded [25]. Furthermore, the assumption of a noisy channel can be sufficient for oblivious transfer [26, 27]. A new cryptographic task—called cheat-sensitive bit commitment—has been studied by Hardy and Kent [28], as well as Aharanov, Ta-Shma, Vazirani and Yao [29]: no restrictions are placed on the adversary initially, but an honest party should stand a good chance of catching a cheater. Kent also showed that bit commitment can be achieved using relativistic constraints [30].

Classically, string commitment is directly linked to bit commitment and no interesting protocols are possible. Kent [31] first asked what kind of quantum string commitment (QBSC) can be achieved. He gave a protocol under the restrictive assumption that Alice does not commit to a superposition [32]. His protocol was modified for experimental purposes by Tsurumaru [33].

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 ρ_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, $\sum_{x\in\{0,1\}^n} p^B_{x|x} \leq 2^b$, where $p^B_{x|x}$ is the probability that Bob correctly guesses x before the reveal phase.

- (Binding) If Bob is honest, then for all commitments of Alice: $\sum_{x\in\{0,1\}^n} p_x^A \leq 2^a$, where p_x^A is the probability that Alice successfully reveals x.

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 $\sum_{x\in\{0,1\}^n} p_x^A \leq 1$, whereas classically one wants that $p_{x'}^A = \delta_{x,x'}$. 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 B to express the security against Bob. In general, we consider an (n, a, b)-QBSC$_B$ where the new concealing condition $B(\mathcal{E}) \leq b$ holds for any ensemble $\mathcal{E} = \{p_x, \rho_x\}$ that Bob can obtain by a cheating strategy. In the latter part of this paper we show that for B being the *accessible information* non-trivial protocols, i.e. protocols with $a + b \ll n$, exist. The accessible information is defined as $I_{acc}(\mathcal{E}) = \max_M I(X;Y)$, where P_X is the prior distribution of the random variable X, Y is the random variable of the outcome of Bob's measurement on $\mathcal{E}$, and the maximization is taken over all measurements M.

B. Model

We work in the model of two-party non-relativistic quantum protocols of Yao [2] and then simplified by Lo and Chau [12] which is usually adopted in this context. Here, any two-party quantum protocol can be regarded as a pair of quantum machines (Alice and Bob), interacting through a quantum channel. Consider the product of three Hilbert spaces $\mathcal{H}_A$, $\mathcal{H}_B$ and $\mathcal{H}_C$ of bounded dimensions representing the Hilbert spaces of Alice's and Bob's machines and the channel, respectively. Without loss of generality, we assume that each machine is initially in a specified pure state. Alice and Bob perform a number of rounds of communication over the channel. Each such round can be modeled as a unitary transformation on $\mathcal{H}_A \otimes \mathcal{H}_C$ and $\mathcal{H}_B \otimes \mathcal{H}_C$ respectively. Since the protocol is known to both Alice and Bob, they know the set of possible unitary transformations used in the protocol. We assume that Alice and Bob are in possession of both a quantum computer and a quantum storage device. This enables them to add ancillae to the quantum machine and use reversible unitary operations to replace measurements. By doing so, Alice and Bob can delay measurements and thus we can limit ourselves to protocols where both parties only measure at the very end. Moreover, any classical computation or communication that may occur can be simulated by a quantum computer. Furthermore, any probabilistic operation can be modeled as an operation that is conditional on the outcome of a coin flip. Instead of a classical coin, we can use a quantum coin and in this way keep the whole system fully quantum mechanical.

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

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

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 [34] $H_2(\rho^{AB}|\rho) \equiv -\log \mathrm{Tr}((\mathbb{I} \otimes \rho^{-\frac{1}{2}})\rho_{AB})^2$. 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.* $\sup_M \sum_x p_x p_{x|x}^{B,M}$ *where* M *ranges over all measurements and* $p_{y|x}^{B,M}$ *is the conditional probability of guessing* y *given* ρ_x*, obeys*

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

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 $M_x = p_x \rho^{-\frac{1}{2}} \rho_x \rho^{-\frac{1}{2}}$. $p_{x|x}^B = \mathrm{Tr}(M_x \rho_x)$ is the probability that Bob guesses x given ρ_x, hence

$$\begin{aligned} \log_2 \sum_x p_x p_{x|x}^{B,\max} &\geq \log_2 \sum_x p_x^2 \mathrm{Tr}(\rho^{-\frac{1}{2}} \rho_x \rho^{-\frac{1}{2}} \rho_x) \\ &= \log \mathrm{Tr}\left(\left[(\mathbb{I} \otimes \rho^{-\frac{1}{2}})\rho_{AB}\right]^2\right) \\ &= -H_2(\rho_{AB}|\rho) \end{aligned}$$

□

Related estimates were derived in [35]. For the uniform distribution $p_x = 2^{-n}$ we have from the concealing condition that $\sum_x p_{x|x}^B \leq 2^b$ 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 $\mathcal{G}$ be a class of two-universal hash functions from $\{0,1\}^n$ to $\{0,1\}^s$. Application of $g \in \mathcal{G}$ to the random variable X maps the ensemble $\mathcal{E} = \{p_x, \rho_x\}$ to $\mathcal{E}_g = \{q_y^g, \sigma_y^g\}$ with probabilities $q_y^g = \sum_{x \in g^{-1}(y)} p_x$ and quantum states $\sigma_y^g = \sum_{x \in g^{-1}(y)} p_x \rho_x$. Then*

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

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

Finally, the following reasoning, previously used to prove the impossibility of quantum bit commitment [11, 12], will be essential: Suppose ρ_0 and ρ_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 ρ_0 equals ρ_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 $\max_U |\langle\phi_0|U \otimes \mathbb{I}|\phi_1\rangle|$ 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

$$\begin{aligned} \delta(|\phi_0\rangle\langle\phi_0|, |\psi_0\rangle\langle\psi_0|) &= \sqrt{1 - |\langle\phi_0|\psi_0\rangle|} \\ &\leq \sqrt{1 - (1-\epsilon)^2} \\ &\leq \sqrt{2\epsilon}. \end{aligned}$$

If both parties are honest, the reveal phase can be regarded as a measurement resulting in a distribution P_Y (P_Z) if $|\phi_0\rangle$ ($|\psi_0\rangle$) 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 $\frac{1}{2}(|P_Y(0) - P_Z(0)| + |P_Y(1) - P_Z(1)| + |P_Y(r) - P_Z(r)|) \leq \sqrt{2\epsilon}$. 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 small 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 for 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 $g(x) = y'$ with $y \neq y'$ as we saw above! The following figure illustrates this idea.

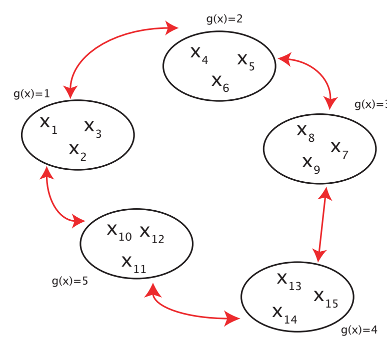

FIG. 1: Moving from y to y'.

Theorem 2 *(n,a,b)-QBSC$_\xi$ schemes, and thus also (n,a,b)-QBSC schemes, with $a+b+c < n$ do not exist. c is a constant equal to $5\log_2 5 - 4 \approx 7.61$.*

Proof. Consider an (n,a,b)-QBSC$_\xi$ and the case where both Alice and Bob are honest. Alice committed to x. We denote the joint state of the Alice-Bob-Channel system $\mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_C$ after the commit phase by $|\phi_x\rangle$ for input state $|x\rangle$. Let ρ_x be Bob's reduced density matrix and let $\mathcal{E} = \{p_x, \rho_x\}$ where $p_x = 2^{-n}$.

Assuming that Bob is honest, we will give a cheating strategy for Alice in the case where $a+b+5\log_2 5 - 4 < n$. The strategy will depend on the two-universal hash function $g : \mathcal{X} = \{0,1\}^n \to \mathcal{Y} = \{0,1\}^{n-m}$, for appropriately chosen m. Alice picks a $y \in \mathcal{Y}$ and prepares the state $(\sum_{x \in g^{-1}(y)} |x\rangle|x\rangle)/\sqrt{|g^{-1}(y)|}$. She then gives the second half of this state as input to the protocol and stays honest for the rest of the commit phase. The joint state of Alice and Bob at the end of the commit phase is thus $|\psi_y^g\rangle = (\sum_{x\in g^{-1}(y)} |x\rangle|\phi_x\rangle)/\sqrt{|g^{-1}(y)|}$. The reduced states on Bob's side are $\sigma_y^g = \frac{1}{q_y^g}\sum_{x\in g^{-1}(y)} p_x\rho_x$ with probability $q_y^g = \sum_{x\in g^{-1}(y)} p_x$. We denote this ensemble by $\mathcal{E}_g$. Let $\sigma = \sigma^g = \sum_y q_y^g \sigma_y^g$ for all g.

We now apply Theorem 1 with $s = n-m$ and $\xi(\mathcal{E}) \le b$ to obtain $\frac{1}{|\mathcal{G}|}\sum_{g\in\mathcal{G}} d(\mathcal{E}_g) \le \varepsilon$ where $\varepsilon = \frac{1}{2}2^{-\frac{1}{2}(m-b)}$. Hence, there is at least one g such that $d(\mathcal{E}_g) \le \varepsilon$; 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 $d(\mathcal{E}_g) \le \varepsilon$ implies

$$2^{-(n-m)}\sum_y \delta(\sigma,\sigma_y^g) \le 2\varepsilon. \tag{3}$$

Let us therefore assume without loss of generality that Alice chooses $y_0 \in \mathcal{Y}$ with $\delta(\sigma,\sigma_{y_0}^g) \le 2\varepsilon$.

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

$$\sum_x \tilde{p}_x = \sum_y \tilde{q}_y^g \sum_{x\in g^{-1}(y)} \tilde{p}_{x|y}^g \ge \sum_y \tilde{q}_y^g.$$

Recall that Alice can transform $|\psi_{y_0}^g\rangle$ approximately into $|\psi_y^g\rangle$ if $\sigma_{y_0}^g$ is sufficiently close to σ_y^g 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 $|\psi_{y_0}\rangle$. Since this reasoning applies to all y, on average, we have

$$\begin{aligned}
\sum_y \tilde{q}_y^g &\ge \sum_y (1 - 2^{\frac{1}{2}}\delta(\sigma_{y_0}^g,\sigma_y^g)^{\frac{1}{2}}) \\
&\ge 2^{n-m} - 2^{\frac{1}{2}}2^{n-m}\big(2^{m-n}\sum_y \delta(\sigma_{y_0}^g,\sigma_y^g)\big)^{\frac{1}{2}} \\
&\ge 2^{n-m}[1 - 2^{\frac{1}{2}}(2^{m-n}(\sum_y \delta(\sigma_{y_0}^g,\sigma) + \delta(\sigma,\sigma_y^g)))^{\frac{1}{2}}] \\
&\ge 2^{n-m}(1 - 2(2\varepsilon)^{\frac{1}{2}}),
\end{aligned}$$

where the first inequality follows from Lemma 3, the second from Jensen's inequality and the concavity of the square root function, the third from the triangle inequality and the fourth from eq. (3) and $\delta(\sigma_{y_0}^g,\sigma) \le 2\varepsilon$. Recall that to be secure against Alice, we require $2^a \ge 2^{n-m}(1-2(2\varepsilon)^{\frac{1}{2}})$. We insert $\epsilon = \frac{1}{2}2^{-\frac{1}{2}(m-b)}$, define $m = b+\gamma$ and take the logarithm on both sides to get

$$a + b + \delta \ge n, \tag{4}$$

where $\delta = \gamma - \log_2(1 - 2^{-\gamma/4+1})$. Keeping in mind that $1 - 2^{-\gamma/4+1} > 0$ (or equivalently $\gamma > 4$), we find that the minimum value of δ for which eq. (4) is satisfied is $\delta = 5\log_2 5 - 4$ and arises from $\gamma = 4(\log_2 5 - 1)$. Thus, no (n,a,b)-QBSC$_\xi$ 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 $a + b \ge n$:

Proposition 1 *Let P be an (n,a,b)-QBSC$_\xi$ 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$_\xi$ 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$_\chi$ with $a+b<n$ and χ 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,a_m,b_m)-QBSC$_\xi$ or (nm,a_m,b_m)-QBSC protocol obtained by executing P m times in parallel. By Theorem 2, Q is insecure if $a_m + b_m < nm - c$. 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 $a_m \ge am$ and $b_m \ge bm$, respectively. Therefore, the m fold execution of P is insecure, if $am + bm \le a_m + b_m < nm - c$ or $a + b < n - c/m$.

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. (2) is replaced by $\kappa + 2^{-\frac{1}{2}[H_{\min}^{\kappa}(\rho_{AB}|\rho_B)-s]}$ for an arbitrary $\kappa > 0$ [34, Corollary 5.6.1]. Going through the proof with this change in mind, one sees that Q is not a (nm,a_m,b_m)-QBSC$_\Xi$ for $\Xi(\tilde{\mathcal{E}}) = nm - H_{\min}^{\kappa}(\tilde{\rho}_{AB}|\tilde{\rho})$ if $a_m + b_m + \delta \le mn$. Here, $\tilde{\mathcal{E}}$ is the ensemble corresponding to Q and $\tilde{\rho}_{AB}$ and $\tilde{\rho}$ the related states; $\delta \equiv \delta(\kappa)$ is a positive constant independent of n. Since $\tilde{\mathcal{E}} = \mathcal{E}^{\otimes m}$ and thus $\tilde{\rho}_{AB} = \rho_{AB}^{\otimes m}$ and $\tilde{\rho}_{AB} = \rho_{AB}^{\otimes m}$ we are able to invoke the estimate

$$\frac{1}{m}H_{\min}^{\kappa}(\rho_{AB}^{\otimes m}|\rho^{\otimes m}) \ge H(\rho_{AB}) - H(\rho) - 3\lambda$$

where $\lambda(\kappa,m) \to 0$ as $m \to \infty$ [34, Chain rule in Theorem 3.1.12 and Theorem 3.3.4] in order to conclude that Q is not a (nm,a_m,b_m)-QBSC$_{m(\chi(\mathcal{E})+2\lambda)}$ if $a_m+b_m+\delta < mn$. This shows that if P is a (nm,a_m,b_m)-QBSC$_{m(\chi(\mathcal{E})+2\lambda)}$ with $\alpha_m m + \beta_m m \le a_m + b_m < nm - \delta$, i.e. $\alpha_m + \beta_m < n - \delta/m$, then its m-fold execution cannot be secure. Taking m to infinity we see that if P is an (n,a,b)-QBSC$_\chi$ 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, $\mathcal{U}$), uses this effect and is specified by a set $\mathcal{U} = \{U_1, \ldots, U_{|\mathcal{U}|}\}$ of unitaries.

- Commit phase: Alice has the string $x \in \{0,1\}^n$ and randomly chooses $r \in \{1, \ldots, |\mathcal{U}|\}$. She sends the state $U_r|x\rangle$ to Bob, where $U_r \in \mathcal{U}$.
- Reveal phase: Alice announces r and x. Bob applies $U_r^\dagger$ and measures in the computational basis to obtain x'. He accepts if and only if $x' = x$.

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,$\mathcal{U}$) protocol is* $\log(|\mathcal{U}|)$*-binding, i.e.* $2^a \leq |\mathcal{U}|$*,*

Proof. Let p_x^A denote the probability that Alice reveals x successfully. Then, $p_x^A \leq \sum_r p_{x,r}^A$, where $p_{x,r}^A$ is the probability that x is accepted by Bob when the reveal information was r. Let ρ denote the state of Bob's system. Summation over x now yields

$$\begin{aligned}\sum_x p_x^A &\leq \sum_{x,r} p_{x,r}^A \\ &= \sum_{x,r} \mathrm{Tr}|x\rangle\langle x|U_r^\dagger \rho U_r \\ &= \sum_r \mathrm{Tr}\rho = |\mathcal{U}|,\end{aligned}$$

hence $a \leq \log_2 |\mathcal{U}|$ □

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 $\mathcal{U}$ to Bob. They then perform LOCKCOM(n,$\mathcal{U}$). Following the work of [38], 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: $I_{acc}(\mathcal{E}) \leq 4$:

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

Proof. Let $\mathcal{U}_{ran}$ denote the set of m randomly chosen bases and consider the LOCKCOM(n, a, b) scheme using unitaries $\mathcal{U} = \mathcal{U}_{ran}$. 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

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

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 [38, Appendix B] there is a constant $C' > 0$ such that

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

for $d \geq 7$ and $\epsilon \leq 2/5$. Set $\epsilon = \frac{1}{\log_2 d}$. The RHS of the above equation then decreases provided that $m > \frac{8}{C'}(\log_2 d)^4$. 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 ϵ. □

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, $\{\mathbb{I}^{\otimes n}, H^{\otimes n}\}$) 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,$\mathcal{U}$) which incorporates cheat-sensitivity against Bob.

Protocol 1: CS-Bob-LOCKCOM(n,$\mathcal{U}$)

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

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 'abort'.

We proved in Theorem 4 that CS-Bob-LOCKCOM($n, \{\mathbb{I}^{\otimes n}, H^{\otimes n}\}$) is a $(n, 1, n/2)$-I_{acc}-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($\log_2 d, \{\mathbb{I}, U\}$), where U is the Fourier transform, is a $(\log_2 d, 1, \frac{\log_2 d}{2})$-$I_{acc}$-quantum string commitment protocol.

We now restrict our attention to this 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 [48] . 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 ϵ, then his* Holevo information gain *obeys*

$$\chi(\mathcal{E}^C) \leq 4\sqrt{\epsilon}\log_2 d + 2\mu(2\sqrt{\epsilon}).$$

As a corollary we find that CS-Bob-LOCKCOM($\log_2 d, \{\mathbb{I}, U\}$) 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 $LOCKCOM(\log_2 d, \{\mathbb{I}, U\})$ is equivalent to the following procedure: Alice prepares the state
$$|\psi\rangle = \frac{1}{\sqrt{2d}} \sum_{x,r} |x\rangle^X |r\rangle^R |r\rangle^{R'} U^r |x\rangle^Y$$
on the system $XRYR'$ and sends system Y (over a noiseless quantum channel) to Bob. It is understood that $U^0 = \mathbb{I}$ 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_{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] .
$$V_{cheat} : Y \to CQ$$
The map V_{cheat} followed by the partial trace over Q is denoted by Λ^C and likewise V_{cheat} followed by the partial trace over C is denoted by Λ^Q.

- Alice sends the reveal information R' to Bob.

- Bob applies a preparation unitary $V_{prepare}$ to his system. Since C will not be touched upon, the most general operation acts on $R'Q$ only:
$$V_{prepare} : R'Q \to R'ST.$$
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
$$\frac{1}{d}\sum_{x=1}^{d} \left(1 - \mathrm{Tr}|x\rangle\langle x|\rho_x^S\right),$$
where $\rho_x^S = \mathrm{Tr}_{XRR'T}|x\rangle\langle x||\psi\rangle\langle\psi|^{XRR'ST}$, and $|\psi\rangle^{XRR'ST}$ is the pure state of the total system after Bob's application of $V_{prepare}$.

Note that Alice measures in the computational basis since for honest Bob $V_{prepare} = \sum_{r' \in \{0,1\}} |r'\rangle\langle r'| \otimes (U^r)^\dagger$, 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 $\mathcal{E}_r^Z = \{p_x, \rho_{xr}^Z\}$ with

$$\rho_{xr}^Z = \frac{1}{p_x p_r}\mathrm{Tr}_{XRR'CQ\setminus Z}|xr\rangle\langle xr||\psi\rangle\langle\psi|^{XRR'CQ}$$

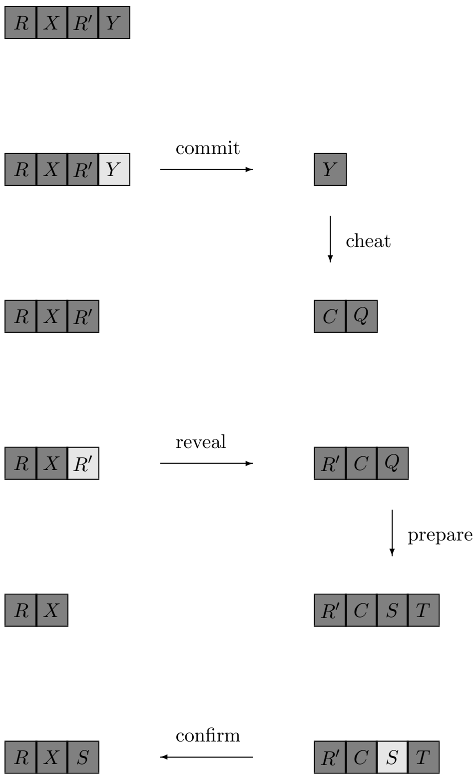

FIG. 2: Execution of CS-Bob-LOCKCOM with honest Alice on the left and cheating Bob on the right. Time flows downwards.

and for $Z \in \{S,T\}$ let $\mathcal{E}_r^Z = \{p_x, \rho_{xr}^Z\}$ with

$$\rho_{xr}^Z = \mathrm{Tr}_{XRR'CST\setminus Z}|xr\rangle\langle xr||\psi\rangle\langle\psi|^{XRR'CST}.$$

Sometimes we are only interested in the ensemble averaged over the values of r: for $Z \in \{C,Q,S,T\}$

$$\mathcal{E}^Z = \{p_x, \rho_x^Z\} \text{ where } \rho_x^Z = \frac{1}{2}\left(\rho_{x0}^Z + \rho_{x1}^Z\right). \tag{5}$$

Let us now come to two technical lemmas, most notably a channel uncertainty relation (Lemma 5) that was discovered in connection with squashed entanglement:

Consider a uniform ensemble $\mathcal{E}_0 = \{\frac{1}{d}, |i\rangle\}_{i=1}^d$ of basis states of a Hilbert space $\mathcal{H}$ and the ensemble $\mathcal{E}_1 = \{\frac{1}{d}, U|i\rangle\}_{i=1}^d$ rotated with a unitary U. Application of the completely positive trace preserving (CPTP) map Λ (with output in a potentially different Hilbert space) results in the two ensembles

$$\Lambda(\mathcal{E}_0) = \left\{\frac{1}{d}, \Lambda(|i\rangle\langle i|)\right\}$$
$$\Lambda(\mathcal{E}_1) = \left\{\frac{1}{d}, \Lambda(U|i\rangle\langle i|U^\dagger)\right\}$$

with Holevo information for $\mathcal{E}_0$ given by

$$\chi(\Lambda(\mathcal{E}_0)) = H\left(\frac{1}{d}\sum_i \Lambda(|i\rangle\langle i|)\right) - \frac{1}{d}\sum_i H\big(\Lambda(|i\rangle\langle i|)\big)$$

and similarly for $\mathcal{E}_1$. Consider also the quantum mutual information of Λ relative to the maximally mixed state $\tau = \frac{1}{d}\mathbb{I}$, which is the average state of either $\mathcal{E}_0$ or $\mathcal{E}_1$:

$$I(\tau;\Lambda) = H\big(\tau\big) + H\big(\Lambda(\tau)\big) - H\big((\mathbb{I}\otimes\Lambda)(|\psi_d\rangle\langle\psi_d|)\big),$$

where $|\psi_d\rangle$ is a maximally entangled state in dimension d purifying τ.

Lemma 5 (Channel Uncertainty Relation [39]) *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 $d = 2^\ell$, and the group $\mathbb{Z}_2^\ell$, $U = H^{\otimes\ell}$ with the Hadamard transform H of a qubit. Then for all CPTP maps Λ,*

$$\chi\big(\Lambda(\mathcal{E}_0)\big) + \chi\big(\Lambda(\mathcal{E}_1)\big) \le I(\tau;\Lambda). \tag{6}$$

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 $\sum_i p_i\langle\psi_i|\sigma_i|\psi_i\rangle \ge 1-\epsilon$, then*

$$|\chi(\tilde{\mathcal{E}}) - \chi(\mathcal{E})| \le 4\sqrt{\epsilon}\log_2 d + 2\mu(2\sqrt{\epsilon}),$$

where $\mu(x) = \min\{-x\log_2 x, \frac{1}{e}\}$.

Proof. The justification of the estimate

$$\epsilon \ge \sum_i p_i(1 - \mathrm{Tr}\rho_i\sigma_i) \ge \sum_i p_i\delta_i^2 \ge \big(\sum_i p_i\delta_i\big)^2,$$

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 $\delta(\rho,\sigma) \le \sqrt{\epsilon}$. Fannes' inequality will be applied to the overall state

$$|H(\rho) - H(\sigma)| \le 2\sqrt{\epsilon}\log_2 d + \min\{\eta(2\sqrt{\epsilon}), \frac{1}{e}\}$$

where $\eta(x) = -x\log_2 x$, and to the individual ones

$$\begin{aligned}\sum_i p_i|H(\sigma_i) - H(\rho_i)| \ &\le\ \big(\sum_i p_i\delta_i\big)2\log_2 d + \\ &\qquad \sum_i p_i \min\{\eta(2\delta_i), \frac{1}{e}\} \\ &\le\ \sqrt{\epsilon}2\log_2 d + \min\{\eta(2\sqrt{\epsilon}), \frac{1}{e}\}\end{aligned}$$

where the last inequality is true by the concavity of $\eta(x)$. Inserting these estimates in the Holevo χ quantities

$\chi(\mathcal{E}) = H(\rho)$ and $\chi(\tilde{\mathcal{E}}) = H(\sigma) - \sum_i p_i H(\sigma_i)$ concludes the proof. □

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 $\frac{1}{d}$). The justifications for the following estimate are given in a list below.

$$\begin{aligned}
& \chi(\mathcal{E}_0^C) + \chi(\mathcal{E}_1^C) & (7)\\
=\ & \chi(\Lambda^C(\mathcal{E}_0)) + \chi(\Lambda^C(\mathcal{E}_1)) & (8)\\
\leq\ & I(XRR';C) & (9)\\
=\ & 2H(XRR') - I(XRR';Q) & (10)\\
\leq\ & 2H(XRR') - \chi(\Lambda^Q(\mathcal{E}_0)) - \chi(\Lambda^Q(\mathcal{E}_1)) & (11)\\
=\ & 2H(XR) - \chi(\mathcal{E}_0^Q) - \chi(\mathcal{E}_1^Q) & (12)\\
\leq\ & 2H(XR) - \chi(\Lambda_0^S(\mathcal{E}_0^Q)) - \chi(\Lambda_1^S(\mathcal{E}_1^Q)) & (13)\\
=\ & 2H(XR) - \chi(\mathcal{E}_0^S) - \chi(\mathcal{E}_1^S) & (14)\\
\leq\ & 2H(XR) - 2\chi(\mathcal{E}^S). & (15)
\end{aligned}$$

The justifications:

- Equality (8): By definition of the string commitment scheme and the map Λ^C: $\mathcal{E}_r^C = \{p_x, \rho_{xr}^C\} = \{p_x, \Lambda^C(U^r|x\rangle\langle x|(U^\dagger)^r)\} =: \Lambda^C(\mathcal{E}_r)$.
- Inequality (9): Application of Lemma 5 for the map Λ^C. Note that system XRR' is a reference system for the completely mixed state on system Y on which the channel Λ^C is applied. Hence $I(\tau;\Lambda^C) = I(XRR';C)$.
- Equality (10): Simple rewriting of the entropy terms making use of the definition of quantum mutual information and the purity of $XRR'CQ$.
- Inequality (11): Application of Lemma 5 for the map Λ^Q. Note that system XRR' is a reference system for the completely mixed state on system Y on which the channel Λ^Q is applied. Hence $I(\tau;\Lambda^Q) = I(XRR';Q)$.
- Equality (12): R' is a copy of R: $H(XRR') = H(XR)$. By definition of the string commitment scheme and the map Λ^Q: $\mathcal{E}_r^Q = \{p_x, \rho_{xr}^Q\} = \{p_x, \Lambda^Q(U^r|x\rangle\langle x|(U^\dagger)^r)\}$.
- Inequality (13) and equality (14): follow from the data processing inequality $\chi(\Lambda^H(\mathcal{E}_r^Q)) \leq \chi(\mathcal{E}_r^Q)$ and from the definition $\Lambda^H(\mathcal{E}_r^Q) = \mathcal{E}_r^S$.
- Inequality (15): Finally $\mathcal{E}^S = \{p_x, \rho_x^S = \frac{1}{2}\left(\rho_{x0}^S + \rho_{x1}^S\right)\}$, which by the concavity of von Neumann entropy implies $\chi(\mathcal{E}^S) \leq \frac{1}{2}\left(\chi(\mathcal{E}_0^S) + \chi(\mathcal{E}_1^S)\right)$.

If Bob is detected cheating with probability less than ϵ, then by Lemma 6 the Holevo quantity $\chi(\mathcal{E}^S)$ of the ensemble given in S that Bob sends to Alice obeys

$$\chi(\mathcal{E}^S) \geq (1 - 4\sqrt{\epsilon}) \log d - 2\mu(2\sqrt{\epsilon}). \qquad (16)$$

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

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 [40], Tsurumaru [41] 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 [42, 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, QAP IST 015848, the FP6-FET Integrated Project SCALA, CT-015714, the Sloan Foundation and QuantumWorks.

[1] C. H. Bennett, G. Brassard, C. Crépeau, and M.-H. Skubiszewska, in *CRYPTO '91: Proceedings of the 11th Annual International Cryptology Conference on Advances in Cryptology* (Springer-Verlag, 1992), pp. 351–366.
[2] A. C.-C. Yao, in *Proceedings of 20th ACM STOC* (1995), pp. 67–75.
[3] C. Crépeau, Journal of Modern Optics **41**, 2455 (1994).
[4] C. Crépeau, J. van de Graaf, and A. Tapp, in *CRYPTO '95: Proceedings of the 15th Annual International Cryptology Conference on Advances in Cryptology* (Springer-Verlag, 1995), pp. 110–123.
[5] J. Kilian, in *Proceedings of 20th ACM STOC* (1988), pp. 20–31.
[6] O. Goldreich, *Foundations of Cryptography*, vol. Basic Tools (Cambridge University Press, 2001).
[7] M. Blum, SIGACT News **15**, 23 (1983).
[8] C. H. Bennett and G. Brassard, in *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing* (1984), pp. 175–179.
[9] G. Brassard and C. Crépeau, in *Advances in Cryptology – Proceedings of Crypto '90* (1990), pp. 49–61.
[10] G. Brassard, C. Crépeau, R. Jozsa, and D. Langlois, in *Proceedings of 34th IEEE FOCS* (1993), pp. 362–371.
[11] D. Mayers (1996), quant-ph/9603015.
[12] H.-K. Lo and H. F. Chau, Physical Review Letters **78**, 3410 (1997).
[13] D. Mayers, Physical Review Letters **78**, 3414 (1997).
[14] H.-K. Lo and H. Chau, Physica D **120**, 177 (1998).
[15] G. Brassard, C. Crépeau, D. Mayers, and L. Salvail (1997), quant-ph/9712023.
[16] H. Chau and H.-K. Lo, Fortsch. Phys. **46**, 507 (1998), republished in 'Quantum Computing, where do we want to go tomorrow?' edited by S. Braunstein,Wiley-VCH, Berlin, 1999; quant-ph/9709053.
[17] R. Spekkens and T. Rudolph, Physical Review A **65**, 012310 (2002).
[18] D. DiVincenzo, M. Horodecki, D. Leung, J. Smolin, and B. Terhal, Physical Review Letters **92** (2004).
[19] L. Salvail, in *Proceedings of CRYPTO'98* (1998), vol. 1462 of *Lecture Notes in Computer Science*, pp. 338–353.
[20] D. DiVincenzo, J. Smolin, and B. Terhal, New Journal of Physics **6** (2004).
[21] I. Damgård, S. Fehr, L. Salvail, and C. Schaffner, in *Proceedings of 46th IEEE FOCS* (2005), pp. 449–458.
[22] I. Damgard, S. Fehr, R. Renner, L. Salvail, and C. Schaffner, in *Proceedings of CRYPTO 2007* (2007), pp. 360–378.
[23] S. Wehner and J. Wullschleger (2007), arXiv:0709.0492.
[24] C. Schaffner, B. Terhal, and S. Wehner (2007), in preparation.
[25] C. Cachin, C. Crépeau, and J. Marcil, in *Proceedings of 39th IEEE FOCS* (1998), pp. 493–502.
[26] C. Crépeau and J. Kilian, in *Proceedings of 29th IEEE FOCS* (1988), pp. 42–52.
[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*.
[28] L. Hardy and A. Kent, Physical Review Letters **92** (2004).
[29] D. Aharonov, A. Ta-Shma, U. Vazirani, and A. Yao, in *Proceedings of the 32th ACM STOC* (2000), pp. 705–714.
[30] A. Kent, Journal of Cryptology **18**, 313 (2005).
[31] A. Kent, Physical Review Letters **90** (2003), quant-ph/111099.
[32] A. Kent, personal communication at QIS '04.
[33] T. Tsurumaru, Physical Review A **71**, 012313 (2005).
[34] R. Renner, Ph.D. thesis, ETH Zurich (2005), quant-ph/0512258.
[35] H. Barnum and E. Knill, Journal of Mathematical Physics **43**, 2097 (2002).
[36] R. König, U. Maurer, and R. Renner, IEEE Transactions on Information Theory **51**, 2391 (2005).
[37] A. Kitaev, D. Mayers, and J. Preskill, Physical Review A **69**, 052326 (2004).
[38] P. Hayden, D. Leung, P. Shor, and A. Winter, Communications in Mathematical Physics **250**, 371 (2004).
[39] M. Christandl and A. Winter, IEEE Transactions on Information Theory **51**, 3159 (2005).
[40] H. Buhrman, M. Christandl, P. Hayden, H.-K. Lo, and S. Wehner (2005), quant-ph/0504078.
[41] T. Tsurumaru, **74**, 042307 (2006).
[42] A. S. Holevo, Probl. Inf. Transm. **9**, 110 (1973).
[43] D. P. DiVincenzo, D. W. Leung, and B. M. Terhal, IEEE Trans. Inf Theory **48**, 580 (2002).
[44] M. Ballester and S. Wehner, Physical Review A **75**, 022319 (2007).
[45] R. Jain (2005), quant-ph/0506001.
[46] M. Christandl, Ph.D. thesis, University of Cambridge (2005), quant-ph/0604183.
[47] The results in this section are included in [46].
[48] This information is stored in a register C and not touched upon later on; Bob's remaining information is called Q. Note that this cheating scenario includes cheating by measurement, since here C contains the classical measurement result of which he can put a copy into Q. Any later manipulation of Q can therefore be achieved without touching C.