J. Cryptol. (2008) 21: 579–592
DOI: 10.1007/s00145-008-9025-y

Journal of
CRYPTOLOGY

New Binding-Concealing Trade-Offs for Quantum String Commitment

Rahul Jain
School of Computer Science and Institute for Quantum Computing, University of Waterloo, Waterloo, ON, Canada, N2L 3G1
rjain@cs.uwaterloo.edu

Communicated by Stefan Wolf

Received 5 July 2006 and revised 28 April 2008
Online publication 29 May 2008

Abstract. *String commitment* schemes are similar to the well-studied *bit commitment* schemes in cryptography with the difference that the committing party, say Alice, is supposed to commit a long string instead of a single bit to another party, say Bob. Similar to bit commitment schemes, such schemes are supposed to be *binding*, i.e., Alice cannot change her choice after committing, and *concealing*, i.e., Bob cannot find Alice's committed string before Alice reveals it. Ideal commitment schemes are known to be impossible. Even if some degree of cheating is allowed, Buhrman et al. (quant-ph/0504078, Nov. 2007)[1] have recently shown that there are some *binding-concealing* trade-offs that any quantum string commitment scheme (QSC) must follow. They showed trade-offs both in the scenario of single execution of the protocol and in the asymptotic regime of sufficiently large number of parallel executions of the protocol.

We present here new trade-offs in the scenario of single execution of a QSC protocol. Our trade-offs also immediately imply the trade-off shown by Buhrman et al. in the asymptotic regime. We show our results by making a central use of an important information theoretic tool called the *substate theorem* due to Jain et al. (Proceedings of the 43rd Annual IEEE Symposium on Foundations of Computer Science, pp. 429–438, 2002). Our techniques are quite different from that of Buhrman et al. (quant-ph/0504078, Nov. 2007) and may be of independent interest.

Key words. String commitment, Quantum channels, Observational divergence, Relative entropy, Substate theorem.

1. Introduction

Commitment schemes are powerful cryptographic primitives. In a bit commitment scheme Alice, the committee is supposed to commit a bit $b \in \{0, 1\}$ to Bob in such a way that after the *commit phase* she cannot change her choice of the committed bit. This is referred to as the binding property. Also at this stage Bob should not be able

[1] A short version of this paper appeared previously in [1].

to figure out what the committed bit is. This is referred to as the concealing property. Later in the *reveal phase* Alice is supposed to reveal the bit b and convince Bob that this was indeed the bit which she committed earlier. Bit commitment schemes have been very well studied in both the classical and quantum models, since the existence of such schemes imply several interesting results in cryptography. It has been shown that bit commitment schemes imply the existence of *quantum oblivious transfer* [18], which in turn provides a way to do any two-party secure computation [13]. They are also useful in constructing *zero knowledge proofs* [5] and imply another very useful cryptographic primitive called secure *coin tossing* [3]. But unfortunately strong negative results are known about them in case Alice and Bob are assumed to possess arbitrary computation power and information theoretic security is required. In this paper, we are concerned with this setting of information theoretic security with unbounded computational resources with cheating parties. Classically bit commitment schemes are known to be impossible. In the quantum setting several schemes were proposed, but later several impossibility results were shown [4,14–16]. Negative results were also shown for approximate implementations of bit commitment schemes [4,17] in which trade-offs were shown for cheating probabilities of Alice and Bob, referred to as binding-concealing trade-offs. Interestingly however Kent [12] has exhibited that bit-commitment can be achieved using relativistic constraints. However we point out that in this work we do not keep considerations of relativity into picture, and our setting is nonrelativistic.

Now suppose that instead of wanting to commit a bit $b \in \{0,1\}$, Alice wants to commit an entire string $x \in \{0,1\}^n$. One way to do this might be to commit all the bits of x separately. Binding-concealing trade-offs of such schemes will be limited by the binding-concealing trade-offs allowable for bit commitment schemes. But is it conceivable that there might exist cleverer schemes which allow for better binding and concealing properties? This question was originally raised by Kent [11]. Let us first begin by formally defining a quantum string commitment protocol. Our definition is similar to the one considered by Buhrman et al. [2]

Definition 1 (Quantum string commitment). Let $P = \{p_x : x \in \{0,1\}^n\}$ be a probability distribution, and let B be a *measure of information* (we define several measures of information later). A $(n, a, b) - B -$ QSC protocol for P is a *quantum communication protocol* [15,18] between Alice and Bob. Alice gets an input $x \in \{0,1\}^n$ (chosen according to the distribution P), which is supposed to be the string to be committed. The starting joint state of the qubits of Alice and Bob is some pure state. There are no intermediate measurements during the protocol, and Bob has a final checking POVM measurement $\{M_y | y \in \{0,1\}^n\} \cup \{I - \sum_y M_y\}$ (please see Sect. 2 for definition of POVM) to determine the value of the committed string by Alice or to detect her cheating. The protocol runs in two phases called the commit phase followed by the reveal phase. The following properties need to be satisfied.

1. **(Correctness)** Let Alice and Bob act honestly. Let ρ_x be the state of Bob's qubits at the end of the reveal phase of the protocol when Alice gets input x. Then $\forall x, y \ \ \mathrm{Tr} M_y \rho_x = 1$ iff $x = y$ and 0 otherwise.
2. **(Concealing)** Let Alice act honestly and Bob be possibly cheating. Let σ_x be the state of Bob's qubits after the commit phase when Alice gets input x. Then the B

information of the ensemble $\mathcal{E} = \{p_x, \sigma_x\}$ is at most b. In particular this is also true for both Alice and Bob acting honestly.

3. **(Binding)** Let Bob act honestly and Alice be possibly cheating. Let $c \in \{0,1\}^n$ be a string in a special cheating register C with Alice that she keeps independent of the rest of the registers till the end of the commit phase. Let ρ'_c be the state of Bob's qubits at the end of the reveal phase when Alice has c in the cheating register. Let $\tilde{p}_c \stackrel{\text{def}}{=} \mathrm{Tr} M_c \rho'_c$. Then for all input strings x,

$$\sum_{c \in \{0,1\}^n} p_c \tilde{p}_c \leq 2^{a-n}.$$

The idea behind the above definition is as follows. At the end of the reveal phase of an honest run of the protocol, Bob figures out x from ρ_x by performing the POVM measurement $\{M_x\} \cup \{I - \sum_x M_x\}$. He accepts the committed string to be x iff M_x succeeds, and this happens with probability $\mathrm{Tr} M_x \rho_x$. He declares Alice cheating if $I - \sum_x M_x$ succeeds. Thus due to the first condition, at the end of an honest run of the protocol, Bob accepts the committed string to be exactly the input string of Alice with probability 1. The second condition above takes care of the concealing property stating that the amount of B information about x that a possibly cheating Bob gets is bounded by b. In bit-commitment protocols, the concealing property was quantified in terms of the probability with which Bob can guess Alice's bit. Buhrman et al. [2] in fact do consider Bob's probability of guessing Alice's input string as quantifying the concealing property. However in the proof of their trade-off result, they consider a related notion of information as a quantification of the concealing property. In this paper, we use various notions of information to quantify the concealing property of the protocol. The third condition guarantees the binding property. It makes sure that if a cheating Alice wants to postpone committing or wants to change her choice at the end of the commit phase, then she cannot succeed in making an honest Bob accept her new choice with good probability, for a lot of different strings of her choice.

A few points regarding the above definition are important to note. We assume that the combined state of Alice and Bob at the beginning of the protocol is a pure state. Given this assumption, it can be assumed without loss of generality (due to the arguments of [15,18]) that it remains a pure state till the end of the protocol (in an honest run). This is because Alice and Bob need not apply any intermediate measurements, before Bob applies the final checking POVM at the end of the protocol. Our impossibility result makes a critical use of this fact and fails to hold if the starting combined state is not a pure state. However, there are no restrictions on the starting pure state shared between Alice and Bob, it could even be an entangled state between them. The impossibility result in [2] has also been shown under this assumption. This assumption has also been made in showing impossibility results for bit-commitment schemes [14–16]. The main reason why these arguments do not work, both for bit commitment and string commitment schemes, if the combined state is not a pure state is that the *Local Transition Theorem* (Theorem 8 mentioned later) fails to hold for mixed states. It is conceivable that, and will be interesting to see if better QSC schemes exist when Alice and Bob are forced (by some third party say) to start in some mixed state. Please look at [4] for extension of impossibility results for bit-commitment to a very large class of protocols.

1.1. *Measures of Information*

As we will see later, the notion of information used in the above definition is very important, and therefore let us briefly define various notions of information that we will be concerned with in this paper. The following notion of information, referred to as the quantum mutual information or the Holevo-χ information, is one of the most commonly used.

Definition 2 (Holevo-χ information). Given a quantum state ρ, the *von-Neumann* entropy of ρ is defined as $\mathsf{S}(\rho) \stackrel{\text{def}}{=} -\mathsf{Tr}\rho\log_2\rho$. Given quantum states ρ and σ, the *Kullback–Leibler divergence* or *relative entropy* between them is defined as $\mathsf{S}(\rho\|\sigma) \stackrel{\text{def}}{=} \mathsf{Tr}\rho(\log_2\rho - \log_2\sigma)$. Given an ensemble $\mathcal{E} = \{p_x, \rho_x\}$, let $\rho \stackrel{\text{def}}{=} \sum_x p_x\rho_x$, then its Holevo-$\chi$ information is defined as

$$\chi(\mathcal{E}) \stackrel{\text{def}}{=} \sum_x p_x\big(\mathsf{S}(\rho) - \mathsf{S}(\rho_x)\big) = \sum_x p_x\mathsf{S}(\rho_x\|\rho).$$

The following notion captures the amount of information that can be made available to the real world through measurements on the quantum encoding of a classical random variable.

Definition 3 (Accessible information). Let $\mathcal{E} = \{p_x, \rho_x\}$ be an ensemble, and let X be a classical random variable such that $\Pr(X = x) \stackrel{\text{def}}{=} p_x$. Let $Y^{\mathcal{M}}$, correlated with X, be the classical random variable that represents the result of a POVM measurement $\mathcal{M}$ performed on $\mathcal{E}$. The *accessible information* $I_{\text{acc}}(\mathcal{E})$ of the ensemble $\mathcal{E}$ is then defined to be

$$I_{\text{acc}}(\mathcal{E}) \stackrel{\text{def}}{=} \max_{\mathcal{M}} I\big(X : Y^{\mathcal{M}}\big). \tag{1}$$

As mentioned before, Buhrman et al. used Bob's probability of guessing Alice's input string as the measure of concealment of the protocol. However, in the proofs of their impossibility result, they used the following notion of information.

Definition 4 (ξ information [2]). The ξ information of an ensemble $\mathcal{E} = \{p_x, \rho_x\}$ is defined as

$$\xi(\mathcal{E}) \stackrel{\text{def}}{=} n + \log_2 \sum_x \mathsf{Tr}\big(p_x\rho^{-1/2}\rho_x\big)^2,$$

where $\rho = \sum_x p_x\rho_x$.

Let q_x be the probability that Bob correctly guesses Alice's input string x (with Alice honest) before the start of the reveal phase. [2] showed that any $(n, a, b) - \mathsf{QSC}$ protocol with $\sum_{x\in\{0,1\}^n} q_x \leq 2^b$ also is an $(n, a, b) - \xi - \mathsf{QSC}$ protocol. Hence their impossibility results for $(n, a, b) - \xi - \mathsf{QSC}$ protocols implied the same impossibility results for $(n, a, b) - \mathsf{QSC}$ protocols with $\sum_{x\in\{0,1\}^n} q_x \leq 2^b$.

In this paper, we also consider a notion of *divergence information*. It is based on the following notion of distance between two quantum states considered by Jain, Radhakrishnan, and Sen [9].

Definition 5 (Observational divergence [9]). Let ρ and σ be two quantum states. The observational divergence between them, denoted $\mathsf{D}(\rho\|\sigma)$, is defined as

$$\mathsf{D}(\rho\|\sigma) \stackrel{\text{def}}{=} \max_{\text{M:POVM element}} \mathrm{Tr}M\rho \log_2 \frac{\mathrm{Tr}M\rho}{\mathrm{Tr}M\sigma}.$$

The definition of divergence information of an ensemble is similar to the Holevo-χ information except the notion of distance between quantum states used is now observational divergence instead of relative entropy.

Definition 6 (Divergence information). Let $\mathcal{E} = \{p_x, \rho_x\}$ be an ensemble, and let $\rho \stackrel{\text{def}}{=} \sum_x p_x \rho_x$. Its divergence information is defined by

$$\mathcal{D}(\mathcal{E}) \stackrel{\text{def}}{=} \sum_x p_x \mathsf{D}(\rho_x\|\rho).$$

1.2. *Previous Results*

The impossibility of a strong string commitment protocol, in which both a and b are required to be 0, is immediately implied by the impossibility of strong bit-commitment protocols. The question of a trade-off between a and b was studied by Buhrman et al. They studied this trade-off both in the scenario of single execution of the protocol and also in the asymptotic regime with several parallel executions of the protocol. In the scenario of single execution of the protocol, they showed the following result.

Theorem 1 [2]. *For single execution of the protocol of an* (n, a, b)-ξ-QSC, $a + b + 5\log_2 5 - 4 \geq n$.

This then (as argued before) implied similar trade-off for an (n, a, b)-QSC with $\sum_{x\in\{0,1\}^n} q_x \leq 2^b$ (where q_x is the probability that Bob correctly guesses Alice's input string x, with Alice honest, before the start of the reveal phase). In the asymptotic regime, they showed the following result in terms of the Holevo-χ information.

Theorem 2 [2]. *Let* Π *be an* $(n, *, b) - \chi -$ QSC *scheme. Let* Π_m *represent* m *parallel executions of* Π. *Let* a_m *represent the binding parameter of* Π_m, *and let* $a \stackrel{\text{def}}{=} \lim_{m\to\infty} \frac{a_m}{m}$. *Then,* $a + b \geq n$.

There are two reasons why Theorem 2 may appear stronger than Theorem 1. The first one is that there is no additive constant, and the other is that, for many ensembles $\mathcal{E}$, $\chi(\mathcal{E}) \leq \xi(\mathcal{E})$, as we show in Appendix A. In fact, as we also show in Appendix A, there exists ensembles $\mathcal{E}$ for which $\xi(\mathcal{E})$ is exponentially (in n) larger than $\chi(\mathcal{E})$.

Along with these impossibility results, Buhrman et al. interestingly also showed that if the measure of information considered is the accessible information, the above trade-offs no longer hold. For example, there exists a QSC scheme where $a = 4\log_2 n + O(1)$ and $b = 4$ when measure of information is the accessible information. This therefore asserts that the choice of measure of information is crucial to (im)possibility. Previously Kent [11] also exhibited trade-offs for some schemes on Alice's probability of cheating and the amount of accessible information that Bob gets about the committed string. However he did not allow Alice to be arbitrarily cheating, in particular Alice could not have started with a superposition of strings in the input register. Therefore the schemes that he considered were truly not QSCs as we have defined them.

1.3. *Our Results*

We show the following binding-concealing trade-off for QSCs.

Theorem 3. *For single execution of the protocol of an* $(n, a, b) - \mathcal{D} -$ QSC *scheme*,

$$a + b + 8\sqrt{b+1} + 16 \geq n.$$

It was shown by Jain, Radhakrishnan, and Sen [9] that for any two states ρ and σ, $\mathsf{D}(\rho\|\sigma) \leq \mathsf{S}(\rho\|\sigma) + 1$, which implies by Definitions 2 and 6 that, for any ensemble $\mathcal{E}$, $\mathcal{D}(\mathcal{E}) \leq \chi(\mathcal{E}) + 1$. This immediately gives us the following impossibility result in terms of Holevo-χ information.

Theorem 4. *For single execution of the protocol of an* $(n, a, b) - \chi -$ QSC *scheme*,

$$a + b + 8\sqrt{b+2} + 17 \geq n.$$

We also consider the notion of *maximum possible divergence information* (similar to the notion of maximum possible Holevo-χ information considered by Jain [8]) of an *encoding* $E : x \mapsto \rho_x$. For a probability distribution $\mu \stackrel{\text{def}}{=} \{p_x\}$ over $\{0,1\}^n$, let the ensemble $\mathcal{E}_\mu(E) \stackrel{\text{def}}{=} \{p_x, \rho_x\}$. Let $\rho_\mu \stackrel{\text{def}}{=} \sum_x p_x \rho_x$.

Definition 7 (Maximum possible divergence information). *Maximum possible divergence information* of an encoding $E : x \mapsto \rho_x$ is defined as $\tilde{\mathcal{D}}(E) \stackrel{\text{def}}{=} \max_\mu \mathcal{D}(\mathcal{E}_\mu(E))$.

We show the following theorem which states that if the maximum possible divergence information in the qubits of Bob at the end of the commit phase is small, then Alice can actually cheat with good probability for any string $x \in \{0,1\}^n$ and not just on the average.

Theorem 5. *For a* QSC *scheme, let* σ_x *be as in Definition* 1 *when* Alice *and* Bob *act honestly in the commit phase. If for the encoding* $E : x \mapsto \sigma_x$, $\tilde{\mathcal{D}}(E) \leq b$, *then for all strings* $c \in \{0,1\}^n$,

$$\tilde{p}_c \geq 2^{-(b+8\sqrt{b+1}+16)},$$

where $\tilde{p}_c$ (*as in Definition* 1) *represents the probability of successfully revealing string* c (*in the cheating string*) *by cheating* Alice.

Again using the fact that, for all ensembles, $\mathsf{D}(\rho\|\sigma) \leq \mathsf{S}(\rho\|\sigma) + 1$, we immediately get the following theorem in terms of maximum possible Holevo-χ information $\tilde{\chi}(E)$ (which is similar to maximum possible divergence information and obtained by just replacing divergence with relative entropy).

Theorem 6. *For a* QSC *scheme, let* σ_x *be as in Definition* 1 *when* Alice *and* Bob *act honestly in the commit phase. If for the encoding* $E : x \mapsto \sigma_x$, $\tilde{\chi}(E) \leq b$, *then for all strings* $c \in \{0,1\}^n$,

$$\tilde{p}_c \geq 2^{-(b+8\sqrt{b+2}+17)},$$

where $\tilde{p}_c$ (*as in Definition* 1) *represents the probability of successfully revealing string* c (*in the cheating string*) *by cheating* Alice.

Now let us now discuss some aspects of our results.

1. In Theorem 4, the trade-off between a and b is similar (up to lower order terms of b) to the one shown by Buhrman et al. [2] as in Theorem 1. However the fact that b in Theorem 4 represents the Holevo-χ information instead of the ξ-information (as in Theorem 1) makes it significantly stronger in certain cases as follows. We show in Appendix A that for any ensemble $\mathcal{E} \stackrel{\text{def}}{=} \{2^{-n}, \rho_x\}$, where for all x, ρ_x commutes with $\rho \stackrel{\text{def}}{=} \sum_x 2^{-n}\rho_x$, we have $\xi(\mathcal{E}) \geq \chi(\mathcal{E})$. In fact, as we also show in Appendix A, there exists ensembles $\mathcal{E}$ for which $\xi(\mathcal{E})$ is exponentially (in n) larger than $\chi(\mathcal{E})$. Theorem 4 therefore becomes much stronger than Theorem 1 for ensembles where $\xi(\mathcal{E}) \gg \chi(\mathcal{E})$.
2. As mentioned before, Jain et al. [9] have shown that for any ensemble $\mathcal{E}$, $\mathcal{D}(\mathcal{E}) \leq \chi(\mathcal{E}) + 1$. However recently, Jain et al. [10] have shown that there exist ensembles $\mathcal{E}$ such that $\chi(\mathcal{E}) \gg \mathcal{D}(\mathcal{E})$ ($\chi(\mathcal{E}) = \Omega(\log_2 n \cdot \mathcal{D}(\mathcal{E}))$ for some ensembles $\mathcal{E}$ supported on $\{0,1\}^n$). For ensembles where this holds, Theorem 3 becomes much stronger than Theorem 4.
3. As we show in Sect. 3, our one shot result, Theorem 4, immediately implies the asymptotic result, Theorem 2 of Buhrman et al.
4. No counterparts of Theorems 5 and 6 were shown by Buhrman et al. and are therefore completely new.
5. If b is large, then the cheating attack (that we present) of Alice would succeed with low probability (like 2^{-b}). However, as we show in a remark in Sect. 3, in case Alice's cheating attack succeeds with low probability, she would still be able to 'reverse' her cheating operations and reveal, with a high probability, at least some $x' \in \{0,1\}^n$ to Bob. That is, with a high probability, Alice will be able to prevent herself from being detected cheating by Bob.
6. It is easily seen that up to lower order terms in b, the above trade-offs are achieved by trivial protocols. For Theorem 3 above, consider the following protocol. Alice in the concealing phase sends the first b bits of the n-bit string x. In this case, Bob gets to know b bits of divergence information about x. In the reveal phase, a

cheating Alice can now reveal any of the 2^{n-b} strings x (consistent with the first b bits being the ones sent) with probability 1. Hence $a = \log_2 2^{n-b} = n - b$. For Theorem 5 above, let Alice send one of the 2^b strings $s \in \{0,1\}^b$ uniformly to Bob representing the first b bits of x. The condition of Theorem 5 is satisfied. Now if, in the reveal phase, she wants to commit any x, she can do so with probability 2^{-b} (in the event that the sent s is consistent with x).

In the next section, we state some quantum information theoretic facts that will be useful in the proofs of the impossibility results that we present in Sect. 3.

2. Preliminaries

All logarithms in this paper are taken with base 2 unless otherwise specified. Let $\mathcal{H}, \mathcal{K}$ be finite-dimensional Hilbert spaces. For a linear operator A, let $|A| = \sqrt{A^\dagger A}$ and let $\mathsf{Tr}A$ denote the trace of A. Given a state $\rho \in \mathcal{H}$ and a pure state $|\phi\rangle \in \mathcal{H} \otimes \mathcal{K}$, we call $|\phi\rangle$ a *purification* of ρ iff $\mathsf{Tr}_{\mathcal{K}}|\phi\rangle\langle\phi| = \rho$. A *positive operator-valued measurement* (POVM) *element* M is a positive semi-definite operator such that $I - M$ also is positive semi-definite, where I is the identity operator. A POVM is defined as follows.

Definition 8 (POVM). An m-valued POVM measurement $\mathcal{M}$ on a Hilbert space $\mathcal{H}$ is a set of operators $\{M_i, i \in [m]\}$ on $\mathcal{H}$ such that $\forall i$, M_i is positive semi-definite and $\sum_{i\in[m]} M_i = I$, where I is the identity operator on $\mathcal{H}$. A classical random variable $Y^{\mathcal{M}}$ representing the result of the measurement $\mathcal{M}$ on a state ρ is an m-valued random variable such that $\forall i \in [m], \Pr[Y^{\mathcal{M}} = i] \stackrel{\text{def}}{=} \mathsf{Tr}M_i\rho$.

The following fact easily follows from the definition of von-Neumann entropy.

Lemma 1. *Let ρ_1 and ρ_2 be quantum states. Then* $\mathsf{S}(\rho_1 \otimes \rho_2) = \mathsf{S}(\rho_1) + \mathsf{S}(\rho_2)$.

We make a central use the following information-theoretic result called the substate theorem due to Jain et al. [9].

Theorem 7 (Substate theorem, [9]). *Let $\mathcal{H}$ and $\mathcal{K}$ be two finite-dimensional Hilbert spaces with* $\dim(\mathcal{K}) \geq \dim(\mathcal{H})$. *Let $\mathbb{C}^2$ denote the two-dimensional complex Hilbert space. Let σ and τ be density matrices in $\mathcal{H}$ such that* $\mathsf{D}(\sigma\|\tau) < \infty$. *Let $|\overline{\sigma}\rangle$ be a purification of σ in $\mathcal{H} \otimes \mathcal{K}$. Then, for $r > 1$, there exist pure states $|\phi\rangle, |\theta\rangle \in \mathcal{H} \otimes \mathcal{K}$, and $|\overline{\tau}\rangle \in \mathcal{H} \otimes \mathcal{K} \otimes \mathbb{C}^2$, depending on r, such that $|\overline{\tau}\rangle$ is a purification of τ and* $\mathsf{Tr}||\overline{\sigma}\rangle\langle\overline{\sigma}| - |\phi\rangle\langle\phi|| \leq \frac{2}{\sqrt{r}}$, *where*

$$|\overline{\tau}\rangle \stackrel{\text{def}}{=} \sqrt{\frac{r-1}{r2^{rk}}}\,|\phi\rangle|1\rangle + \sqrt{1 - \frac{r-1}{r2^{rk}}}\,|\theta\rangle|0\rangle$$

and $k \stackrel{\text{def}}{=} \mathsf{D}(\sigma\|\tau) + 6\sqrt{\mathsf{D}(\sigma\|\tau) + 1} + 4$.

Remarks.

1. In the above theorem, if the last qubit in $|\overline{\tau}\rangle$ is measured in the computational basis, then the probability of obtaining 1 is $(1 - 1/r)2^{-rk}$.
2. Later in the proof below, we will let $\sigma \stackrel{\text{def}}{=} \rho_c$, $\tau \stackrel{\text{def}}{=} \rho_B$, and $|\overline{\sigma}\rangle \stackrel{\text{def}}{=} |\phi_c\rangle$, which will be explained later.

The following theorem is implicit in [7,14–16] although not explicitly called by the same name.

Theorem 8 (Local transition theorem). *Let ρ be a quantum state in $\mathcal{K}$. Let $|\phi_1\rangle$ and $|\phi_2\rangle$ be two purifications of ρ in $\mathcal{H} \otimes \mathcal{K}$. Then there is a local unitary transformation U acting on $\mathcal{H}$ such that $(U \otimes I)|\phi_1\rangle = |\phi_2\rangle$.*

We will also need the following theorem, which follows from arguments similar to those in Jain [8] for a similar theorem about relative entropy.

Theorem 9. *Let X be a finite set. Let $E : x \mapsto \rho_x$ be an encoding. If $\tilde{\mathcal{D}}(E) \leq b$, then there exists a distribution $\mu \stackrel{\text{def}}{=} \{q_x\}$ on X such that*

$$\forall x \in X, \quad \mathsf{D}(\rho_x \| \rho) \leq b,$$

where $\rho \stackrel{\text{def}}{=} \sum_x q_x \rho_x$.

The following theorem is shown by Helstrom [6].

Theorem 10. *Given two quantum states ρ and σ, the probability of identifying the correct state is at most $\frac{1}{2} + \frac{\mathsf{Tr}|\rho-\sigma|}{4}$, or in other words the probability of distinguishing them is at most $\frac{\mathsf{Tr}|\rho-\sigma|}{2}$.*

3. Proofs of Impossibility

Proof of Theorem 3. Let us consider a QSC scheme, and let Alice get input x. After an honest run of the commit phase, let $|\phi_x\rangle$ be the combined state of Alice and Bob, and let ρ_x be the state of Bob's qubits. Let $\mathcal{E} = \{p_x, \rho_x\}$. From the concealing property of the QSC it follows that $\mathsf{D}(\mathcal{E}) \leq b$. Let c be the string in the cheating register C of Alice. Consider a cheating run of the protocol by Alice in which she starts with the superposition $\sum_x \sqrt{p_x}|x\rangle$ in the input register and proceeds with the rest of the commit phase as before in the honest protocol. Let Bob be honest all throughout our arguments. Since the input is classical and Alice can make its copy, we can assume without loss of generality that the operations of Alice in the honest run are such that they do not disturb the input register. Let $|\psi\rangle$ be the combined state of Alice and Bob in this cheating run at the end of the commit phase. Let A and B correspond to Alice and Bob's systems, respectively. Now it can be seen that in the cheating run, at the end of the commit phase, the qubits of Bob are in the state $\rho_B \stackrel{\text{def}}{=} \mathsf{Tr}_A|\psi\rangle\langle\psi| = \sum_x p_x \rho_x$. Let $r > 1$ to be chosen later.

Let us now invoke the substate theorem (Theorem 7) by putting $\sigma \stackrel{\text{def}}{=} \rho_c$, $|\overline{\sigma}\rangle \stackrel{\text{def}}{=} |\phi_c\rangle$, $\tau \stackrel{\text{def}}{=} \rho_B$, and $r \stackrel{\text{def}}{=} r$. Let $|\psi_c\rangle \stackrel{\text{def}}{=} |\overline{\tau}\rangle$ be obtained from Theorem 7 such that the extra single qubit register $\mathbb{C}^2$ is also with Alice. Since $\mathsf{Tr}_A|\psi_c\rangle\langle\psi_c| = \mathsf{Tr}_A|\psi\rangle\langle\psi| = \rho_B$, by Local transition theorem (Theorem 8) there exists a unitary transformation A_c acting just on Alice's system A such that $(A_c \otimes I_B)|\psi\rangle = |\psi_c\rangle$, where I_B is the identity transformation on Bob's system. Now the cheating Alice (who's intention is to reveal string c) applies the transformation A_c to $|\psi\rangle$ and then continues with the rest of the reveal phase as in the honest run. Let $|\phi'_c\rangle \stackrel{\text{def}}{=} |\phi\rangle$ be obtained from Theorem 7 and hence, $\mathsf{Tr}||\phi_c\rangle\langle\phi_c| - |\phi'_c\rangle\langle\phi'_c|| \leq 2/\sqrt{r}$. Now it can be seen that when Bob makes the final checking POVM, the probability of success $\tilde{p}_c$ for Alice is at least $(1 - 1/r)2^{-rk_c}(1 - 1/\sqrt{r})$, where $k_c = \mathsf{D}(\rho_c\|\rho_B) + 6\sqrt{\mathsf{D}(\rho_c\|\rho_B) + 1} + 4$. One way to see this is to imagine that Alice first measures the single qubit register $\mathbb{C}^2$ and then proceeds with the rest of the reveal phase. Now imagine that she obtains one on this measurement, which by Theorem 7 has probability $(1 - 1/r)2^{-rk_c}$. Also once she obtains one, the combined joint state of Alice and Bob is $|\phi'_c\rangle$ whose trace distance with $|\phi_c\rangle$ is at most $2/\sqrt{r}$. Since the trace distance is preserved by unitary operations and is only smaller for subsystems and since after this Alice follows the rest of the reveal phase honestly, we can conclude the following: the final state resulting with Bob will have the trace distance at most $2/\sqrt{r}$ with the state with him at the end of a completely honest run of the protocol in which Alice starts with c in the input register. Hence it follows from Theorem 10 that Bob will accept at the end with probability at least $1 - 1/\sqrt{r}$, since he was accepting with probability 1 in the complete honest run of the protocol. Hence the overall cheating probability $\tilde{p}_c$ of Alice is at least $(1 - 1/r)2^{-rk_c}(1 - 1/\sqrt{r})$.

Although here we have imagined Alice doing an intermediate measurement on the single qubit register $\mathbb{C}^2$, it is not necessary, and she will have the same cheating probability when she proceeds with the rest of the honest protocol after just applying the cheating transformation A_c, since the final qubits of Bob will be in the same state in either case. Now,

$$
\begin{aligned}
2^{a-n} &\geq \sum_c p_c \tilde{p}_c \\
&\geq (1 - 1/r)\big(1 - 1/\sqrt{r}\big)\left(\sum_c p_c 2^{-r(\mathsf{D}(\rho_c\|\rho_B)+6\sqrt{\mathsf{D}(\rho_c\|\rho_B)+1}+4)}\right) \\
&\geq (1 - 1/r)\big(1 - 1/\sqrt{r}\big)2^{\sum_c -rp_c(\mathsf{D}(\rho_c\|\rho_B)+6\sqrt{\mathsf{D}(\rho_c\|\rho_B)+1}+4)} \\
&\geq (1 - 1/r)\big(1 - 1/\sqrt{r}\big)2^{-r(b+6\sqrt{b+1}+4)}.
\end{aligned}
$$

The first inequality comes from the definition of a in Definition 1. The third inequality comes from the convexity of the exponential function, and the fourth inequality comes from definition of b in Definition 1, Definition 6, and the concavity of the square root function.

Now for $b > 15$, we let $r = 1 + \frac{1}{b}$ and, therefore,

$$(1 - 1/r)\big(1 - 1/\sqrt{r}\big)2^{-r(b+6\sqrt{b+1}+4)} \geq \frac{0.5}{(b+1)^2}2^{-(b+6\sqrt{b+1}+7)}$$
$$\geq 2^{-(b+8\sqrt{b+1}+8)}.$$

For $b \leq 15$, we let $r = 1 + 1/15$ and, therefore,

$$(1 - 1/r)\big(1 - 1/\sqrt{r}\big)2^{-r(b+6\sqrt{b+1}+4)} \geq 2^{-(b+6\sqrt{b+1}+16)}.$$

Therefore, we always get $2^{a-n} \geq 2^{-(b+8\sqrt{b+1}+16)}$, which finally implies

$$a + b + 8\sqrt{b+1} + 16 \geq n. \qquad \square$$

Proof of Theorem 2. Let b_m represent the concealing parameter for Π_m. It is easy to verify from Lemma 1, the definition of Holevo-χ information, and Definition 2 that $b = b_m/m$. Then Theorem 4 applied to Π_m implies

$$\Rightarrow a_m + b_m + 8\sqrt{b_m + 2} + 17 \geq mn$$
$$\Rightarrow \lim_{m\to\infty} \frac{1}{m}\big(a_m + b_m + 8\sqrt{b_m + 2} + 17\big) \geq n$$
$$\Rightarrow a + b \geq n. \qquad \square$$

Proof of Theorem 5. Let $\mu = \{\lambda_x\}$ be the distribution on $\{0,1\}^n$ obtained from Theorem 9. Consider the cheating strategy of Alice in which she puts the superposition $\sum_x \sqrt{\lambda_x}|x\rangle$ in the register where she keeps the commit string. Let c be the string in the cheating register of Alice. Now by arguments as above, the probability of success $\tilde{p}_c$ for Alice is at least $(1 - 1/\sqrt{r})(1 - 1/r)2^{-rk_c}$, where k_c, ρ_c, ρ being as before. Since for all c, $\mathsf{D}(\rho_c \| \rho) \leq b$, this implies (by setting r appropriately) that $\forall c$, $\tilde{p}_c \geq 2^{-(b+8\sqrt{b+1}+16)}$. $\square$

Remark. Let us now see how, with a good probability overall, Alice will be able to prevent herself from being detected cheating by Bob. Let Alice have c in the cheating register. Let r_c be the probability of getting one on performing the two-outcome measurement (obtained from Theorem 7) after the commit phase as in the cheating strategy described above in the proof of Theorem 3. In case she gets one, she proceeds with the cheating strategy. In case she gets zero, she tries to rollback so that she can successfully reveal at least some string to Bob. For this, she does the following.

1. She applies the transformation $A_c^\dagger$ (the inverse of A_c).
2. She measures the input register in the computational basis and say she obtains x'.
3. She proceeds with the rest of the reveal phase as if her actual input was x'.

Assume that Alice obtains zero on performing the two-outcome measurement as in the cheating strategy described above, which happens with probability $1 - r_c$. Now it can be verified that the trace distance between $|\psi_c\rangle\langle\psi_c|$ and the combined state of Alice

and Bob after obtaining zero on performing the measurement is at most $2r_c$. Since $A_c^\dagger$ is unitary, this implies that the combined state of Alice and Bob after applying $A_c^\dagger$ and $|\psi\rangle\langle\psi|$ will be at most $2r_c$. Now we can argue as before that Alice can reveal some string successfully to Bob with probability at least $1 - r_c$. Therefore overall, the probability that Alice will be able to reveal some string is at least $r_c + (1 - r_c)^2 \geq 1 - r_c$. Now since typically r_c is quite small (like 2^{-b}), $1 - r_c$ is quite close to 1.

Acknowledgement

We thank Harry Buhrman, Matthias Christandl, Hoi-Kwong Lo, Jaikumar Radhakrishnan, and Pranab Sen for discussions. We also thank the anonymous referees for suggestions on an earlier draft. This work was mostly done while the author was at U.C. Berkeley, California, USA, where it was supported by an Army Research Office (ARO), North California, grant number DAAD 19-03-1-00082. Part of the work was done at U. Waterloo, where it was supported in part by ARO/NSA USA.

Appendix A. Separations for $\xi(\mathcal{E})$ and $\chi(\mathcal{E})$

Let $\mathcal{E} \stackrel{\text{def}}{=} \{1/2^n, \rho_x\}$ be an ensemble with $x \in \{0,1\}^n$. Let $\rho \stackrel{\text{def}}{=} \sum_x 2^{-n}\rho_x$. Lets assume that for all x, ρ_x commutes with ρ as is the case in classical ensembles. We show that in this case $\xi(\mathcal{E}) \geq \chi(\mathcal{E})$. Consider

$$\begin{aligned}
\xi(\mathcal{E}) &= n + \log \sum_x \mathsf{Tr}\big(2^{-n}\rho^{-1/2}\rho_x\big)^2 \\
&= \log \sum_x 2^{-n}\mathsf{Tr}\big(\rho^{-1/2}\rho_x\big)^2 \\
&\geq 2^{-n}\sum_x \log \mathsf{Tr}\big(\rho^{-1/2}\rho_x\big)^2 \quad \text{(from concavity of log function)} \\
&= 2^{-n}\sum_x \log \mathsf{Tr}\big(\rho_x\rho^{-1}\rho_x\big) \quad \text{(since } \rho_x \text{ and } \rho \text{ commute)} \\
&\geq 2^{-n}\sum_x \mathsf{Tr}\rho_x \log\big(\rho_x\rho^{-1}\big) \quad \text{(since } \log \mathsf{Tr}BA \geq \mathsf{Tr}A\log B \\
&\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \text{for quantum states } A, B) \\
&= 2^{-n}\sum_x \mathsf{Tr}\rho_x(\log\rho_x - \log\rho) \quad \text{(since } \rho_x \text{ and } \rho \text{ commute)} \\
&= \chi(\mathcal{E}).
\end{aligned}$$

Next we show that there exist classical ensembles for which $\xi(\mathcal{E})$ could be exponentially larger than $\chi(\mathcal{E})$. Consider the ensemble of classical distributions $\{2^{-n}, P_x\}$ for $x \in \{0,1\}^n$. Here each P_x has support on $\{0,1\}^n$. Let $\epsilon \in (0,1)$ be a constant.

Let $P_x(x) = 2^{-\frac{\epsilon n}{2}}$, and let the other values for $P_x(y)$, $y \neq x$ be the same. Let $P \stackrel{\text{def}}{=} \sum_x 2^{-n} P_x$. It is easy to verify that in this case P is the uniform distribution on $\{0,1\}^n$. Now,

$$\begin{aligned}
\xi(\mathcal{E}) &= n + \log \sum_x \mathsf{Tr}\left(2^{-2n} P^{-1} P_x^2\right) \\
&= -n + \log \sum_x \mathsf{Tr}\left(P^{-1} P_x^2\right) \\
&\geq -n + \log \sum_x 2^{n(1-\epsilon)} \quad \left(\text{since for all } x,\ \mathsf{Tr} P^{-1} P_x^2 \geq 2^{n(1-\epsilon)}\right. \\
&\qquad\qquad \left.\text{and since log is monotonic}\right) \\
&= -n + \log 2^{n(2-\epsilon)} = n(1-\epsilon)
\end{aligned}$$

Also we note that for all x, $\mathsf{Tr} P_x(\log P_x - \log P) \leq 2^{-\frac{\epsilon n}{2}} \cdot n \cdot (1 - \epsilon/2)$, and hence

$$\begin{aligned}
\chi(\mathcal{E}) &= 2^{-n} \sum_x \mathsf{Tr} P_x(\log P_x - \log P) \leq 2^{-n} \sum_x 2^{-\frac{\epsilon n}{2}} \cdot n \cdot (1 - \epsilon/2) \\
&= 2^{-\frac{\epsilon n}{2}} \cdot n \cdot (1 - \epsilon/2)
\end{aligned}$$

Therefore, by letting ϵ to be a constant very close to 0 we can let $\xi(\mathcal{E})$ to be very close to n, whereas $\chi(\mathcal{E})$ would still be exponentially small in n.

References

[1] H. Buhrman, M. Christandl, P. Hayden, H.K. Lo, S. Wehner, Security of quantum bit string commitment depends on the information measure. *Phys. Rev. Lett.* **97**, 250501 (2006)

[2] H. Buhrman, M. Christandl, P. Hayden, H.K. Lo, S. Wehner, Possibility, impossibility and cheat-sensitivity of quantum bit string commitment, quant-ph/0504078, Nov. 2007

[3] M. Blum, Coin flipping by telephone a protocol for solving impossible problems, in *SIGACT News*, 1983

[4] G.M. D'Ariano, D. Kretschmann, D. Schlingemann, R.F. Werner, Reexamination of quantum bit commitment: the possible and the impossible. *Phys. Rev. A* **76**, 032328 (2007)

[5] O. Goldreich, *Foundations of Cryptography* (Cambridge University Press, Cambridge, 2001)

[6] C.W. Helstrom, Detection theory and quantum mechanics. *Inf. Control* **10**(1), 254–291 (1967)

[7] L.P. Hughston, R. Jozsa, W.K. Wootters, A complete classification of quantum ensembles having a given density matrix. *Phys. Rev. A* **183**, 14–18 (1993)

[8] R. Jain, Communication complexity of remote state preparation with entanglement. *Quant. Inf. Comput.* **6**(4-5), 461–464 (2006)

[9] R. Jain, J. Radhakrishnan, P. Sen, Privacy and interaction in quantum communication complexity and a theorem about the relative entropy of quantum states, in *Proceedings of the 43rd Annual IEEE Symposium on Foundations of Computer Science*, pp. 429–438, 2002

[10] R. Jain, A. Nayak, Y. Su, A separation between divergence and Holevo information for ensembles, in *Proceedings of the Theory and Applications of Models of Computation (TAMC)*, 2008

[11] A. Kent, Quantum bit string commitment. *Phys. Rev. Lett.* **90**, 237901 (2003)

[12] A. Kent, Cheat sensitive quantum bit commitment. *Phys. Rev. Lett.* **92**, 157901 (2004)

[13] J. Killian, Founding cryptography on oblivious transfer, in *Proceedings of the 20th Annual ACM Symposium on Theory of Computing*, pp. 20–31, 1988

[14] H.-K. Lo, H.F. Chau, Is quantum bit commitment really possible? *Phys. Rev. Lett.* **78**, 3410–3413 (1997)
[15] H.-K. Lo, H.F. Chau, Why quantum bit commitment and ideal quantum coin tossing are impossible. *Physica D* **120**, 177–187 (1998)
[16] D. Mayers, Unconditionally secure quantum bit commitment is impossible. *Phys. Rev. Lett.* **78**, 3414–3417 (1997)
[17] R. Spekkens, T. Rudolph, Degrees of concealment and bindingness in quantum bit commitment protocols. *Phys. Rev. A* **65**, 012310 (2002)
[18] A. Yao, Security of quantum protocols against coherent measurements, in *Proceedings of the 27th Annual ACM Symposium on Theory of Computing*, pp. 67–75, 1995