Impossibility of Growing Quantum Bit Commitments

Severin Winkler
Computer Science Department, ETH Zurich, 8092 Zurich, Switzerland

Marco Tomamichel, Stefan Hengl, and Renato Renner
Institute for Theoretical Physics, ETH Zurich, 8093 Zurich, Switzerland

(Received 25 May 2011; published 26 August 2011)

Quantum key distribution (QKD) is often, more correctly, called key growing. Given a short key as a seed, QKD enables two parties, connected by an insecure quantum channel, to generate a secret key of arbitrary length. Conversely, no key agreement is possible without access to an initial key. Here, we consider another fundamental cryptographic task, commitments. While, similar to key agreement, commitments cannot be realized from scratch, we ask whether they may be grown. That is, given the ability to commit to a fixed number of bits, is there a way to augment this to commitments to strings of arbitrary length? Using recently developed information-theoretic techniques, we answer this question in the negative.

DOI: 10.1103/PhysRevLett.107.090502 PACS numbers: 03.67.Dd, 03.67.Hk

Introduction.—Quantum key distribution [1,2] allows two honest parties, Alice and Bob, to establish a shared secret key, using only insecure quantum communication. However, a necessary precondition for this to be possible is that they have access to a preshared initial key, to be used for authentication—a fact that is sometimes overlooked in the literature. It is easy to see that without such an initial key, it is impossible for Alice to distinguish between Bob and an eavesdropper pretending to be Bob—rendering all further security considerations futile. Nevertheless, once an initial key is available, this key can be grown, i.e., expanded to arbitrary length [3].

Another similar example is coin tossing. It is known that there is no unconditionally secure two-party protocol that generates a fair random coin which cannot be biased by a dishonest party [5]. However, if the two parties have access to a certain number of ideal coin tosses to start with, they can use protocols to obtain a larger number of secure coin tosses. (Here, security holds in a standalone model, where it is assumed that the protocol is invoked only once [6].)

Following this line of thought, one may wonder whether other cryptographic primitives, such as commitments [5], can be grown in a similar way. A string commitment protocol allows a sender to commit to a bit string that is revealed to a receiver at a later point. The protocol is secure for the sender (hiding) if the receiver cannot gain information about the commitment before she reveals it and it is secure for the receiver (binding) if the sender cannot change the string once committed. Here, we are only interested in unconditionally secure protocols, i.e., protocols that are secure against dishonest parties with unlimited computing power.

While it is known that unconditionally secure commitments cannot be implemented using classical or quantum communication only [7,8] (see also [9,10]), this Letter strives to answer the question whether it is possible to implement a long string commitment with a protocol that uses a smaller number of bit commitments that are provided as a resource. (A bit commitment is a string commitment of length one.) We will answer this question to the negative, showing that it is impossible to expand commitments even minimally, and even under relaxed security criteria.

Commitments have a wide variety of applications in theoretical cryptography, ranging from zero-knowledge proofs [11] to secure coin tossing. In particular, commitments can be used to implement statistically secure and universally composable oblivious transfer [12–14], a functionality that is sufficient to realize universal secure two-party computation [15].

In [16] it has been shown that unconditionally secure oblivious transfer cannot be extended using quantum protocols. We note that this already imposes certain bounds on the resources that can be obtained from a limited number of bit commitments [17]. Furthermore, bounds on the quality of commitments for relaxed security definitions have been shown in [18–20]. Conversely, it has been shown that secure commitments can be implemented in relativistic settings involving multiple sites [21] or using trusted resources such as a noisy channel [22] or (trusted) distributed randomness [23,24].

We now proceed with a more detailed specification of string commitment as well as the class of protocols we consider. We then briefly review the smooth entropy calculus, which is required for our technical arguments. Our main result that commitments cannot be grown is stated as Theorem 1. This is supplemented with an alternative version of the claim, which applies if the initial functionality enables committing to quantum bits.

String commitments.—A (classical) string commitment of length ℓ is a functionality that takes a bit string $x \in \{0, 1\}^\ell$ from the sender and outputs the message committed to the receiver. Later, on input open from the sender, the functionality sends x to the receiver.

In the following, we consider implementations of this task by quantum protocols between two parties, Alice (who holds system A) and Bob (B). They have access to a noiseless quantum and a noiseless classical channel, as well as to an additional resource, C (to be specified later). In any round of the protocol, the parties may perform an arbitrary quantum operation on the system in their possession conditioned on the available classical information [25]—this includes generating the input for the available communication interfaces. The use of the quantum channel then corresponds to a party transferring a part of her system to the other party. The classical channel measures the input in a canonical basis and sends the outcome to the receiver. We assume that the total number of rounds of the protocol is bounded by some finite number. By padding the protocol with empty rounds, this corresponds to the assumption that the number of rounds is equal in every execution.

A string commitment scheme over strings of length ℓ generally consists of two phases. In the first, the commit phase, the sender commits to an ℓ-bit string x. Later, in the opening phase the sender reveals x to the receiver. The total system (consisting of the subsystems controlled by Alice and Bob) is assumed to be in a pure state initially. By introducing an additional space the quantum operations of both parties can be purified; i.e., we can assume that the parties apply, conditioned on the information shared over the classical channel, isometries to their systems. Thus, we will assume in the following that the state at the end of the commit phase conditioned on all the classical communication is pure.

Security definitions.—Our main technical contribution will be a quantitative statement on the impossibility of growing string commitments. To formulate this statement, we introduce two definitions that capture the cheating probability of Alice and the information gain of Bob, respectively. We emphasize that the properties required in these definitions are only necessary (we therefore call the definitions "weak"), but would not be sufficient for the security of a protocol [26]. Since we are interested in the impossibility of certain protocols, this only strengthens our results.

Using a commitment protocol, a (quantum) Alice can always commit to a superposition of strings [7,27] as follows: she prepares a state $\frac{1}{\sqrt{|\mathcal{X}|}}\sum_{x\in\mathcal{X}}|x\rangle_X \otimes |x\rangle_{X'}$, where $\mathcal{X}$ is a subset of the ℓ-bit strings. Then she honestly executes the commit protocol with the first half of this state as input and keeps the system X'. We denote the resulting joint state of Alice, Bob, and the resource system by $\rho^{\mathcal{X}}_{A'BC}$, where A' stands for $XX'A$. Later, Alice can measure X' and execute the opening phase of the protocol with the resulting string x. Thus, even for a perfectly binding commitment scheme, we cannot require that there is a fixed value x Alice is committed to after the commit phase. Rather, we can only demand that $\sum_{x\in\{0,1\}^n} p_x \leq 1$ where p_x is the probability that Alice successfully reveals some x in the opening phase.

In order to quantify the degree of bindingness of a protocol, we consider the following attack by Alice. First, she commits to a superposition of strings from a set $\mathcal{X}_0 \subseteq \{0, 1\}^\ell$ as before. Then, she tries to map (by a local transformation $\mathcal{E}_A$ on her system) the resulting state $\rho^{\mathcal{X}_0}_{A'BC}$ to $\rho^{\mathcal{X}_1}_{A'BC}$, corresponding to the commitment to a set $\mathcal{X}_1 \subseteq \{0, 1\}^\ell$ which is disjoint from $\mathcal{X}_0$. Such an attack is successful with probability at least Δ if the protocol cannot detect the transformation with probability more than $1 - \Delta$. Using the trace distance, $D(\rho, \tau) := \frac{1}{2}\|\rho - \tau\|_1$, this can be turned into a necessary condition for security, formulated in terms of the closeness of the transformed state, $(\mathcal{E}_{A'} \otimes \mathbb{1}_{BC})(\rho^{\mathcal{X}_0}_{A'BC})$, to the target state $\rho^{\mathcal{X}_1}_{A'BC}$.

Definition: (Weakly Δ-binding.) We call a commitment scheme weakly Δ-binding if

$$\min_{\mathcal{X}_0,\mathcal{X}_1}\min_{\mathcal{E}_{A'}} D((\mathcal{E}_{A'} \otimes \mathbb{1}_{BC})(\rho^{\mathcal{X}_0}_{A'BC}), \rho^{\mathcal{X}_1}_{A'BC}) \geq 1 - \Delta,$$

where $\mathcal{X}_0$ and $\mathcal{X}_1$ are disjoint sets of strings from $\{0, 1\}^\ell$ and $\mathcal{E}_{A'}$ is a completely positive trace preserving map acting on Alice's system.

To define the hiding property, we consider the joint state ρ^x_{AB} of Alice's and Bob's systems that results from an execution of the protocol where both parties are honest and Alice commits to x. For a commitment scheme to be ε-hiding, we require that $D(\rho^x_B, \rho^{x'}_B) \leq \varepsilon$ for any x, x'. This immediately implies the following (necessary) security condition.

Definition: (Weakly ε-hiding.) A bit commitment protocol is weakly ε-hiding for uniform X if the marginal state ρ_{XB} after the commit phase is ε-close to a state where X is uniform with respect to B, i.e.,

$$\min_{\sigma_B} D\left(\rho_{XB}, \frac{1}{|X|}\mathbb{1}_X \otimes \sigma_B\right) \leq \varepsilon. \tag{1}$$

Smooth entropies.—Our proof is based on the insight that every conceivable protocol that aims to extend bit commitment allows for an attack, which can be established using known results on privacy amplification and the smooth entropy formalism. (Privacy amplification has also been used in [19] to construct attacks on commitment schemes.) The detailed proofs of the technical statements can be found in [28].

Let $\rho_{XB} = \sum_x P(x)|x\rangle\langle x| \otimes \rho^x_B$ be a classical-quantum (CQ) state. Then the min-entropy of X conditioned on B, denoted $H_{\min}(X|B)_\rho$, corresponds to the negative logarithm of the probability of guessing X correctly from a quantum memory B [29]. The smooth min-entropy of a state is defined as $H^{\varepsilon}_{\min}(X|B)_{\rho}: = \max_{\tilde{\rho}} H_{\min}(X|B)_{\tilde{\rho}}$, where the optimization is over all (subnormalized) states ε-close to ρ_{XB} in terms of the purified distance, which corresponds to the minimum trace distance between their purifications. The purified distance between two states, ρ and $\tilde{\rho}$, is upper bounded by $\sqrt{2D(\rho, \tilde{\rho})}$ [30].

The leftover hash lemma against quantum side information [31] (see also [32]) asserts that the smooth min-entropy of $H^{\varepsilon}_{\min}(X|B)_{\rho}$ characterizes the amount of uniform randomness that can be extracted from X with respect to the quantum side information B. A consequence of this is the following fact: for any CQ state $\rho_{XB} = \frac{1}{2^{\ell}}\sum_{x\in\{0,1\}^{\ell}} |x\rangle\langle x| \otimes \rho^{x}_{B}$ there exists a function $f:\{0,1\}^{\ell} \to \{0,1\}$ such that

$$D(\rho^{f,X_0}_{B}, \rho^{f,X_1}_{B}) \leq 2\epsilon + \sqrt{2^{1-H^{\varepsilon}_{\min}(X|B)_{\rho}}}, \qquad (2)$$

where $\rho^{f,X_z}_{B} = \frac{1}{|f^{-1}(z)|}\sum_{x\in f^{-1}(z)} \rho^{x}_{B}$.

In order to derive bounds on the conditional min-entropy when the conditioning system is manipulated, we use the following data-processing inequalities. Let ρ_{XBC} be a CQ state, where C is an additional quantum register with dimension $|C|$. Then, the min-entropy $H^{\varepsilon}_{\min}(X|BC)_{\rho}$ cannot increase by more than $\log|C|$ when a projective measurement $C \to Z$ is applied,

$$H^{\varepsilon}_{\min}(X|BC)_{\rho} \geq H^{\varepsilon}_{\min}(X|BZ)_{\rho} - \log|C|. \qquad (3)$$

Moreover, if the classical register Z is discarded, we have

$$H^{\varepsilon}_{\min}(X|BZ)_{\rho} \geq H^{\varepsilon}_{\min}(X|B)_{\rho} - \log|Z|. \qquad (4)$$

The following fact, also used in the proofs of [7,8,33], is an essential building block of our impossibility proofs: let ϕ^{0}_{AB} and ϕ^{1}_{AB} be two pure states corresponding to the joint state of Alice and Bob when committing to "0" and "1", respectively. If the marginal state of ϕ^{0}_{AB} and ϕ^{1}_{AB} on Bob's system is (almost) the same, then there exists a unitary U_A on Alice system that (approximately) transforms ϕ^{0}_{AB} into ϕ^{1}_{AB}, i.e., $(U_A \otimes \mathbb{1}_B)|\phi^{0}_{AB}\rangle \approx |\phi^{1}_{AB}\rangle$. This reasoning can be generalized to joint states ρ^{b}_{YAYB} that are pure conditioned on all the classical information Y available to both Alice and Bob as follows. If $D(\rho^{0}_{YB}, \rho^{1}_{YB}) \leq \varepsilon$, then there exists a unitary U_{YA} such that

$$D(U_{YA}\rho^{0}_{YAYB}U^{\dagger}_{YA}, \rho^{1}_{YAYB}) \leq \sqrt{2\varepsilon}, \qquad (5)$$

where we omitted the identity operator on YB.

Main result.—One can trivially implement a string commitment of length n from n bit commitments. Furthermore, it is easy to see that, using a resource which allows the parties to commit to n qubits, one can implement n individual commitments to 2 bits each using superdense coding [34], and, therefore, also a string commitment of length $2n$. Our main result essentially states that these two trivial implementations are essentially optimal.

More precisely, we first consider implementations of string commitments based on a functionality that enables n perfect (classical) bit commitments. We show that the length of the implemented string commitment is approximately upper bounded by n if this is required to be highly binding and hiding.

Theorem 1.—Every quantum protocol which uses n_A bit commitments from Alice to Bob and n_B bit commitments from Bob to Alice with $n = n_A + n_B$ as a resource and implements an ε-hiding and Δ-binding string commitment of length ℓ must satisfy

$$\ell \leq n - 2\log\left(\frac{(1-\Delta)^2}{4} - \sqrt{2\varepsilon}\right) - 1.$$

In particular, if $\Delta = \varepsilon \leq 0.01$, then $\ell < n + 6$.

Proof.—In the following, we construct an attack by Alice on a modified protocol that does not use the resource bit commitments and is not necessarily hiding. In this protocol we make Bob more powerful in the sense that he can simulate the original protocol locally. Thus, any successful attack of Alice against the modified protocol implies a successful attack against the original protocol.

In the modified protocol, Alice, instead of using the resource bit commitments, measures the bits to be committed, stores a copy, and sends them to Bob, who stores them in a classical register C_A. When one of these commitments is opened, he moves the corresponding bit to his register B. Bob simulates the action of his commitments locally as follows: instead of measuring a register Y and sending the outcome to the commitment functionality, he applies the isometry $U:|y\rangle_Y \mapsto |yy\rangle_{YY'}$ purifying the measurement of the committed bit and stores Y' in another register C_B. When Bob has to open the commitment, he measures Y' and sends the outcome to Alice over the classical channel. Furthermore, the state conditioned on the classical communication is again pure.

Let $\rho_{XABC} = \frac{1}{2^{\ell}}\sum_{x}|x\rangle\langle x| \otimes \rho^{x}_{ABC}$, where C stands for $C_A C_B$, be the state resulting from the execution of the modified protocol when the input X of Alice is uniformly distributed. Its marginal state ρ_{XAB} is the corresponding state at the end of the commit phase of the original commitment protocol. The state ρ_{XB} must be weakly ε-hiding. Thus, by the definition of the smooth min-entropy and setting $\tilde{\varepsilon}: = \sqrt{2\varepsilon}$, we get

$$H^{\tilde{\varepsilon}}_{\min}(X|B)_{\rho} \geq \log|X| = \ell. \qquad (6)$$

Therefore, inequalities (3) and (4) imply that

$$H^{\tilde{\varepsilon}}_{\min}(X|BC_AC_B)_{\rho} \geq H^{\tilde{\varepsilon}}_{\min}(X|B)_{\rho} - n \geq \ell - n. \qquad (7)$$

From (2) we know that there exists a function f such that $D(\rho^{X_0}_{BC}, \rho^{X_1}_{BC}) \leq 2\delta$, where $\delta: = \tilde{\varepsilon} + \frac{1}{2}\sqrt{2^{1-H^{\tilde{\varepsilon}}_{\min}(X|BC)_{\rho}}}$ and $\rho^{X_z}_{BC} = \frac{1}{|f^{-1}(z)|}\sum_{x\in f^{-1}(z)}\rho^{x}_{BC}$. In order to construct a concrete attack, let Alice choose a bit z and commit to a uniform superposition of all strings x with $f(x) = z$. Then the resulting joint state $\rho^{X_z}_{A'BC}$ at the end of the commit phase is pure conditioned an all the shared classical information. According to (5) there exists, therefore, a unitary $U_{A'}$ on Alice's system that transforms $\rho^{X_z}_{A'BC}$ into a state which is $2\sqrt{\delta}$-close to $\rho^{X_{1-z}}_{A'BC}$ in terms of the trace distance. The definition of weakly Δ-binding implies that $1-\Delta \leq 2\sqrt{\delta}$ and, together with (7), the statement follows.

Next, we consider protocols which use a quantum commitment functionality that allows the parties to commit to (and later reveal) n qubit states. By slightly modifying the proof of the theorem, we show that there cannot exist a protocol that uses such a resource and implements a string commitment of length larger than $2n$. We consider again a modified protocol, where Bob simulates the resource system as follows: Alice, instead of using the resource, sends the committed qubits to Bob, and Bob keeps all the qubits that he would send to the commitment functionality in the original protocol in a register C. Let ρ_{XABC} be the joint state after the execution of the commit phase when Alice's input X is uniformly distributed. We have $H^{\bar{\varepsilon}}_{\min}(X|B)_\rho \geq \log|X| = \ell$ as in (6). Inequalities (3) and (4) together imply that conditioning on an additional quantum system C cannot decrease the smooth min-entropy by more than $2\log|C|$. Thus, we have

$$H^{\bar{\varepsilon}}_{\min}(X|BC)_\rho \geq H^{\bar{\varepsilon}}_{\min}(X|B)_\rho - 2\log|C| = \ell - 2n. \quad (8)$$

Now we proceed as in the proof of the main theorem to get

$$\ell \leq 2n - 2\log\left(\frac{(1-\Delta)^2}{4} - \sqrt{2\varepsilon}\right) - 1. \quad (9)$$

Note that the same reasoning applies to any resource which can be simulated by Bob such that the resulting state at the end of the commit phase is pure conditioned on all the classical communication and the simulated resource uses an additional memory of size at most $\log|C|$. Thus, inequality (9) holds for arbitrary such resources with $\log|C| \leq n$.

Conclusions.—We proved that it is impossible to use a small number of bit commitments as a resource to implement a larger string commitment that is both arbitrarily binding and hiding. This is in stark contrast to corresponding positive results for other cryptographic primitives, such as quantum key distribution or coin flipping, where the resource of interest, once available in finite number, can be enlarged ad infinitum.

The techniques we use to show our impossibility results can be applied to prove more general results on the possibility and efficiency of two-party cryptography. In particular, they can be used to prove bounds on the efficiency of implementations of string commitments from oblivious transfer and, more generally, from resources that distribute trusted correlations to the parties. Moreover, the impossibility results on implementations of oblivious transfer presented in [16] can be improved using these techniques.

We thank Frédéric Dupuis and Jürg Wullschleger for helpful and inspiring discussions. We acknowledge support from the Swiss National Science Foundation (Grant No. 200020-135048), the European Research Council (Grant No. 258932), and an ETHIIRA grant of ETH's research commission.

[1] C.H. Bennett and G. Brassard, in *Proceedings of the International Conference on Computers, Systems, and Signals Processing* (IEEE, Bangalore, 1984), pp. 175–179.
[2] A.K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).
[3] An explicit calculation that shows that a constant-length initial key is sufficient to generate arbitrarily many novel key bits is given, for example, in [4].
[4] J. Müller-Quade and R. Renner, New J. Phys. **11**, 085006 (2009).
[5] M. Blum, SIGACT News **15**, 23 (1983).
[6] D. Hofheinz, J. Müller-Quade, and D. Unruh, in *EUROCRYPT*, edited by S. Vaudenay, Lecture Notes in Computer Science Vol. 4004 (Springer, New York, 2006), pp. 504–521.
[7] D. Mayers, Phys. Rev. Lett. **78**, 3414 (1997).
[8] H.K. Lo and H.F. Chau, Phys. Rev. Lett. **78**, 3410 (1997).
[9] G.M. D'Ariano, D. Kretschmann, D. Schlingemann, and R.F. Werner, Phys. Rev. A **76**, 032328 (2007).
[10] G. Chiribella, G.M. D'Ariano, P. Perinotti, D.M. Schlingemann, and R.F. Werner, arXiv:0905.3801.
[11] S. Goldwasser, S. Micali, and C. Rackoff, in *Proceedings of the ACM Symposium on Theory of Computing (STOC)* (ACM, New York, 1985), pp. 291–304.
[12] C.H. Bennett, G. Brassard, C. Crépeau, and H. Skubiszewska, in *Advances in Cryptology: Proceedings of CRYPTO '91*, Lecture Notes in Computer Science Vol. 576 (Springer, New York, 1992), pp. 351–366.
[13] I. Damgård, S. Fehr, C. Lunemann, L. Salvail, and C. Schaffner, in *Proceedings of CRYPTO*, edited by S. Halevi, Lecture Notes in Computer Science Vol. 5677 (Springer, New York, 2009), pp. 408–427.
[14] D. Unruh, in *Proceedings of EUROCRYPT*, edited by H. Gilbert, Lecture Notes in Computer Science Vol. 6110 (Springer, New York, 2010), pp. 486–505.
[15] J. Kilian, in *Proceedings of the 20th Annual ACM Symposium on Theory of Computing (STOC '88)* (ACM Press, New York, 1988), pp. 20–31.
[16] S. Winkler and J. Wullschleger, in *Proceedings of CRYPTO*, edited by T. Rabin, Lecture Notes in Computer Science Vol. 6223 (Springer, New York, 2010), pp. 707–723.
[17] Using the equivalence of oblivious transfer and commitments, the result of [14] implies that there exists no composable protocol that implements $(m+1)$ individual bit commitments using m bit commitments as a resource, if one demands that the error decreases exponentially in m.
[18] R.W. Spekkens and T. Rudolph, Phys. Rev. A **65**, 012310 (2001).
[19] H. Buhrman, M. Christandl, P. Hayden, H.-K. Lo, and S. Wehner, Phys. Rev. Lett. **97**, 250501 (2006).
[20] A. Chailloux and I. Kerenidis, arXiv:1102.1678.

[21] A. Kent, arXiv:1101.4620.

[22] C. Crépeau, in *Advances in Cryptology: Proceedings of CRYPTO '97*, Lecture Notes in Computer Science Vol. 1233 (Springer, New York, 1997), pp. 306–317.

[23] H. Imai, J. Müller-Quade, A. Nascimento, and A. Winter, in *Proceedings of the IEEE International Symposium on Information Theory (ISIT '04)* (IEEE, New York, 2004).

[24] S. Wolf and J. Wullschleger, in *Proceedings of the 2004 IEEE Information Theory Workshop (ITW '04)* (IEEE, New York, 2004).

[25] This assumption is not justified in the relativistic setting considered in [21].

[26] In particular, one would have to consider arbitrary malicious strategies of dishonest parties to prove the security of a protocol.

[27] P. Dumais, D. Mayers, and L. Salvail, in *Proceedings of EUROCRYPT*, edited by B. Preneel, Lecture Notes in Computer Science Vol. 1807 (Springer, New York, 2000), pp. 300–315.

[28] See Supplemental Material at http://link.aps.org/supplemental/10.1103/PhysRevLett.107.090502 for technical details and the full proofs.

[29] R. König, R. Renner, and C. Schaffner, IEEE Trans. Inf. Theory **55**, 4337 (2009).

[30] M. Tomamichel, R. Colbeck, and R. Renner, IEEE Trans. Inf. Theory **56**, 4674 (2010).

[31] R. Renner, Ph.D. thesis, ETH Zurich, arXiv:quant-ph/0512258.

[32] M. Tomamichel, R. Renner, C. Schaffner, and A. Smith, in *Proceedings of the 2010 IEEE International Symposium on Information Theory (ISIT 2010)* (IEEE, New York, 2010), pp. 2703 –2707.

[33] H. K. Lo, Phys. Rev. A **56**, 1154 (1997).

[34] C. H. Bennett and S. J. Wiesner, Phys. Rev. Lett. **69**, 2881 (1992).