Cryptography from Noisy Storage

Stephanie Wehner,[1] Christian Schaffner,[1] and Barbara M. Terhal[2]
[1]*CWI, Kruislaan 413, 1098 SJ Amsterdam, The Netherlands*
[2]*IBM, Watson Research Center, P.O. Box 218, Yorktown Heights, New York, USA*
(Received 8 January 2008; published 5 June 2008)

We show how to implement cryptographic primitives based on the realistic assumption that quantum storage of qubits is noisy. We thereby consider individual-storage attacks; i.e., the dishonest party attempts to store each incoming qubit separately. Our model is similar to the model of bounded-quantum storage; however, we consider an explicit noise model inspired by present-day technology. To illustrate the power of this new model, we show that a protocol for oblivious transfer is secure for *any* amount of quantum-storage noise, as long as honest players can perform perfect quantum operations. Our model also allows us to show the security of protocols that cope with noise in the operations of the honest players and achieve more advanced tasks such as secure identification.

DOI: 10.1103/PhysRevLett.100.220502 PACS numbers: 03.67.Dd, 03.67.Ac

Traditional cryptography is concerned with the secure and reliable transmission of messages. With the advent of widespread electronic communication new cryptographic tasks have become increasingly important. Examples of such tasks are secure identification, electronic voting, online auctions, contract signing and other applications where the protocol participants do not necessarily trust each other. It is well known that almost all of these interesting tasks are impossible to realize without any restrictions on the participating players, neither classically nor with the help of quantum communication [1]. It is therefore an important task to come up with a cryptographic model which restricts the capabilities of adversarial players and in which these tasks become feasible. It turns out that all such two-party protocols can be based on a simple primitive called 1–2 oblivious transfer [2] (1–2 OT), first introduced in [3]. Hence, 1–2 OT is commonly used to provide a "proof of concept" for the universal power of a new model. In 1–2 OT, the sender Alice starts off with two bit strings S_0 and S_1, and the receiver Bob holds a choice bit C. The protocol allows Bob to retrieve S_C in such a way that Alice does not learn any information about C (thus, Bob cannot simply ask for S_C). At the same time, Alice must be ensured that Bob only learns S_C, and no information about the other string S_{1-C} (thus, Alice cannot simply send him both S_0 and S_1). A 1–2 OT protocol is called unconditionally secure when neither Alice nor Bob can break these conditions, even when given unlimited resources.

In this Letter, we propose a *cryptographic model* based on current practical and near-future technical limitations, namely, that quantum storage is noisy. Thus the presence of noise, the very problem that makes it so hard to implement a quantum computer, can actually be turned to our advantage. Recently it was shown that secure OT is possible when the receiver Bob has a limited amount of quantum memory [4,5] at his disposal. Within this "bounded-quantum-storage model" OT can be implemented securely as long as a dishonest receiver Bob can store at most $n/4 - O(1)$ qubits coherently, where n is the number of qubits transmitted from Alice to Bob. However, at present we do not know of any practical physical situation which enforces such a storage limit. We therefore propose an alternative model of noisy quantum storage inspired by present-day physical implementations: We require no explicit memory bound, but we assume that any qubit that is placed into quantum storage undergoes a certain amount of decoherence. The advantage of our model is that we can evaluate the security parameters of a protocol explicitly in terms of the noise. In this Letter, we show that the OT protocol from [5] is secure in our new model. This simple OT protocol could be implemented using photonic qubits (using polarization or phase encoding) with standard BB84 quantum key distribution [6,7] hardware, only with different classical postprocessing.

We analyze the case where the adversary performs individual-storage attacks. More precisely, Bob may choose to (partially) measure (a subset of) his qubits immediately upon reception using an error-free *product* measurement. In addition he can store each incoming qubit, or postmeasurement state from a prior partial measurement, separately and wait until he gets additional information from Alice (at step 3 in Protocol 1). Once he obtains the additional information he may perform an arbitrary coherent measurement on his stored qubits using the stored classical data. We thereby assume that qubit q_i undergoes some noise while in storage, and we also assume that the noise acts independently on each qubit. In the following, we use the superoperator $\mathcal{S}_i$ to denote the combined channel given by Bob's initial (partial) measurement and the noise. Practically, noise can arise as a result of transferring the qubit onto a different physical carrier, such as an atomic ensemble or atomic state, for example, or into an error-correcting code with fidelity less than 1. In addition, the (encoded) qubit will undergo noise once it has been transferred into "storage." Hence, the quantum operation $\mathcal{S}_i$ in any real world setting necessarily includes some form of noise.

We show that for any initial measurement, and *any* noisy superoperator $\mathcal{S}_i$ the 1–2 OT protocol is secure if the

 © 2008 The American Physical Society

honest participants can perform *perfect* noise-free quantum operations. As an explicit example we consider the case of depolarizing noise during storage. In particular, we can show the following all-or-nothing result: if Bob's storage noise is above a certain threshold, his optimal cheating strategy is to perform a measurement in the so-called Breidbart basis. On the other hand, if the noise level is below the threshold, he is best off storing each qubit as is.

In [8] we show how our analysis can be extended to a more practical model where the honest player's actions are also subjected to noise. Our cryptographic model can be applied to protocols for secure identification scheme such as [9]. This scheme achieves password-based identification and is of great practical relevance for banking applications.

Related work.—Precursors of the idea of basing cryptographic security on storage-noise are already present in [10], but no rigorous analysis was carried through in that paper. Furthermore, it was pointed out in [11,12] how the original bounded-quantum-storage analysis applies in the case of noise levels which are so large that the rank of a dishonest player's quantum storage state is reduced to $n/4$. In contrast, we are able to give an explicit security trade off even for small amounts of noise. We note that our security proof does not exploit the noise in the communication channel (which has been done in the classical setting to achieve cryptographic tasks, see, e.g., [13]), but is solely based on the fact that the dishonest receiver's quantum storage is noisy. A model based on classical noisy storage is akin to the setting of a classical noisy channel, if the operations are noisy, or the classical bounded-storage model, both of which are difficult to enforce in practice. Another technical limitation has been considered in [14] where a bit-commitment scheme was shown secure under the assumption that the dishonest committer can only measure a limited amount of qubits coherently. Our analysis differs in that we can in fact allow any coherent destructive measurement at the end of the protocol.

Definitions and tools.—We start by introducing some tools, definitions, and technical lemmas. To define the security of OT we need to formalize what it means for a dishonest quantum player not to gain any information. Let ρ_{XE} be a state that is part classical, part quantum, i.e., a cq state $\rho_{XE} = \sum_{x\in\mathcal{X}} P_X(x)|x\rangle\langle x| \otimes \rho_E^x$. Here, X is a classical random variable distributed over the finite set $\mathcal{X}$ according to distribution P_X. The *nonuniformity* of X given $\rho_E = \sum_x P_X(x)\rho_E^x$ is defined as $d(X|\rho_E) := \frac{1}{2}\|\mathbb{1}/|\mathcal{X}| \otimes \rho_E - \sum_x P_X(x)|x\rangle\langle x| \otimes \rho_E^x\|_{\mathrm{tr}}$, where $\|A\|_{\mathrm{tr}} = \mathrm{Tr}\sqrt{A^\dagger A}$. Intuitively, if $d(X|\rho_E) \le \varepsilon$ the distribution of X is ε-close to uniform even given ρ_E; i.e., ρ_E gives hardly any information about X. A simple property of the nonuniformity which follows from its definition is that for any cq state of the form $\rho_{XED} = \rho_{XE} \otimes \rho_D$, we have

$$d(X|\rho_{ED}) = d(X|\rho_E). \tag{1}$$

We prove the security of a (sender-)randomized version of OT (ROT), where Alice does not choose her input strings herself, but instead two uniformly random strings $S_0, S_1 \in \{0,1\}^\ell$ are output to her by the protocol. It is well known how to convert this variant into regular OT by an additional classical message using the output strings of ROT as one-time pads for the inputs of OT [15]. The security of a quantum protocol implementing ROT is formally defined in [5] and justified in [16]:

Definition 1.—An ε-secure 1–2 ROT$^\ell$ is a protocol between Alice and Bob, where Bob has input $C \in \{0,1\}$, and Alice has no input. For any distribution of C: (i) (correctness) If both parties are honest, Alice gets output $S_0, S_1 \in \{0,1\}^\ell$ and Bob learns $Y = S_C$ except with probability ε. (ii) (Receiver-security) If Bob is honest and obtains output Y, then for any cheating strategy of Alice resulting in her state ρ_A, there exist random variables S_0' and S_1' such that $\Pr[Y = S_C'] \ge 1 - \varepsilon$ and C is independent of S_0', S_1', and ρ_A. (iii) (Sender-security) If Alice is honest, then for any cheating strategy of Bob resulting in his state ρ_B, there exists a random variable $C' \in \{0,1\}$ such that $d(S_{1-C'}|S_{C'}C'\rho_B) \le \varepsilon$.

The protocol makes use of two-universal hash functions that are used for privacy amplification similar as in QKD. A class $\mathcal{F}$ of functions $f:\{0,1\}^n \to \{0,1\}^\ell$ is called two-universal if for all $x \ne y \in \{0,1\}^n$ and $f \in \mathcal{F}$ chosen uniformly at random from $\mathcal{F}$, we have $\Pr[f(x) = f(y)] \le 2^{-\ell}$. E.g., the set of all affine functions from $\{0,1\}^n$ to $\{0,1\}^\ell$ is two-universal [17].

For a measurement M with positive operator-valued measure elements $\{M_x\}_{x\in\mathcal{X}}$ let $p_{y|x}^M = \mathrm{Tr}M_y\rho_E^x$ be the probability of outputting guess y given ρ_E^x. Then $P_g(X|\rho_E) := \sup_M \sum_x P_X(x)p_{x|x}^M$ is the maximal average success probability of guessing $x \in \mathcal{X}$ given the reduced state ρ_E of the cq state ρ_{XE}. The following Lemma 1 is derived from Theorem 5.5.1 in [18] and follows directly from ([19], Lemma 1); it quantifies how much hash functions can increase the privacy of a random variable X given a quantum adversary holding ρ_E and function F.

Lemma 1.—Let F be chosen uniformly from a class $\mathcal{F}$ of two-universal hash functions from $\{0,1\}^n$ to $\{0,1\}^\ell$, and let ρ_{XE} be a cq state. Then, given additional k bits of classical information D about X, we have that $d(F(X)|FD\rho_E) \le 2^{((\ell+k)/2)-1}\sqrt{P_g(X|\rho_E)}$.

Intuitively, the optimal strategy to guess $X = x \in \{0,1\}^n$ given a product state $\rho^x = \rho^{x_1} \otimes \ldots \otimes \rho^{x_n}$ for bits $x = x_1, \ldots, x_n$, is to measure each state ρ^{x_i} individually. A formal proof is given in [8].

The last tool we need is an uncertainty relation for noisy channels and measurements. Let $\sigma_{0,+} = |0\rangle\langle 0|$, $\sigma_{1,+} = |1\rangle\langle 1|$, $\sigma_{0,\times} = |+\rangle\langle +|$, and $\sigma_{1,\times} = |-\rangle\langle -|$ denote the BB84 states corresponding to the encoding of a bit $z \in \{0,1\}$ into basis $b \in \{+,\times\}$ (computational or Hadamard basis, respectively). Consider the state $\mathcal{S}(\sigma_{z,b})$ for some superoperator $\mathcal{S}$. Let $P_g(X|\mathcal{S}(\sigma_b))$ denote the maximal average success probability for guessing a uniformly distributed X when $b = +$ or $b = \times$. An uncertainty relation for such success probabilities can be stated as

$$P_g(X|\mathcal{S}(\sigma_+)) \cdot P_g(X|\mathcal{S}(\sigma_\times)) \leq \Delta(\mathcal{S})^2, \qquad (2)$$

where Δ is a function from the set of superoperators to the real numbers. For example, when $\mathcal{S}$ is a quantum measurement $\mathcal{M}$ mapping the state $\sigma_{z,b}$ onto purely classical information it can be argued (e.g., by using a purification argument and Corollary 4.15 in [11]) that $\Delta(\mathcal{M}) \equiv \frac{1}{2}(1 + 2^{-1/2})$ which can be achieved by a measurement in the Breidbart basis, where the Breidbart basis is given by $\{|0\rangle_B, |1\rangle_B\}$ with $|0\rangle_B = \cos(\pi/8)|0\rangle + \sin(\pi/8)|1\rangle$ and $|1\rangle_B = \sin(\pi/8)|0\rangle - \cos(\pi/8)|1\rangle$.

It is clear that for a unitary superoperator U we have $\Delta(U)^2 = 1$ which can be achieved. It is not hard to show (see Lemma 3 in [8]) that the only superoperators $\mathcal{S}: \mathbb{C}_2 \rightarrow \mathbb{C}_k$ for which $P_g(X|\mathcal{S}(\sigma_+)) \cdot P_g(X|\mathcal{S}(\sigma_\times)) = 1$ are reversible operations.

Protocol and Analysis.—We use $\in_R$ to denote the uniform choice of an element from a set. We further use $x_{|\mathcal{T}}$ to denote the string $x = x_1, \ldots, x_n$ restricted to the bits indexed by the set $\mathcal{T} \subseteq \{1, \ldots, n\}$. For convenience, we take $\{+, \times\}$ instead of $\{0, 1\}$ as the domain of Bob's choice bit C and denote by $\bar{C}$ the bit different from C.

Protocol 1.—1–2 $\mathrm{ROT}^\ell(C, T)$ [5] (1) Alice picks $X \in_R \{0, 1\}^n$ and $\Theta \in_R \{+, \times\}^n$. Let $\mathcal{I}_b = \{i \mid \Theta_i = b\}$ for $b \in \{+, \times\}$. At time $t = 0$, she sends $\sigma_{X_1,\Theta_1} \otimes \ldots \otimes \sigma_{X_n,\Theta_n}$ to Bob. (2) Bob measures all qubits in the basis corresponding to his choice bit $C \in \{+, \times\}$. This yields outcome $X' \in \{0, 1\}^n$. (3) Alice picks two hash functions $F_+, F_\times \in_R \mathcal{F}$, where $\mathcal{F}$ is a class of two-universal hash functions. At time $t = T$, she sends $\mathcal{I}_+, \mathcal{I}_\times, F_+, F_\times$ to Bob. Alice outputs $S_+ = F_+(X_{|\mathcal{I}_+})$ and $S_\times = F_\times(X_{|\mathcal{I}_\times})$ [20]. (4) Bob outputs $S_C = F_C(X'_{|\mathcal{I}_C})$.

Analysis.—We first show that this protocol is secure according to Definition 1. (i) Correctness: Bob can determine the string $X_{|\mathcal{I}_C}$ (except with negligible probability 2^{-n} the set $\mathcal{I}_C$ is nonempty) and hence obtains S_C. (ii) Security against dishonest Alice: this holds in the same way as shown in [5]. As the protocol is noninteractive, Alice never receives any information from Bob at all, and Alice's input strings can be extracted by letting her interact with an unbounded receiver. (iii) Security against dishonest Bob: Our goal is to show that there exists a $C' \in \{+, \times\}$ such that Bob is completely ignorant about $S_{\bar{C}'}$. In our model Bob's individual-storage strategy can be described by some superoperator $\mathcal{S} = \bigotimes_{i=1}^n \mathcal{S}_i$ that is applied on the qubits between the time they arrive at Bob's and the time T that Alice sends the classical information. We define the choice bit C' as a fixed function of $\mathcal{S}$. Formally, we set $C' \equiv +$ if $\prod_{i=1}^n P_g(X_i|\mathcal{S}_i(\sigma_+)) \geq \prod_{i=1}^n P_g(X_i|\mathcal{S}_i(\sigma_\times))$ and $C' \equiv \times$ otherwise.

Because of the uncertainty relation for each $\mathcal{S}_i$, Eq. (2), it then holds that $\prod_i P_g(X_i|\mathcal{S}_i(\sigma_{\bar{C}'})) \leq \prod_i \Delta(\mathcal{S}_i) \leq (\Delta_{\max})^n$ where $\Delta_{\max} := \max_i \Delta(\mathcal{S}_i)$. This will be used in the proof below.

In the remainder of this section, we show that the nonuniformity $\delta_{\mathrm{sec}} := d(S_{\bar{C}'}|S_{C'}C'\rho_B)$ is negligible in n for individual-storage attacks. Here ρ_B is the complete quantum state of Bob's lab at the end of the protocol including the classical information $\mathcal{I}_+, \mathcal{I}_\times, F_+, F_\times$, he got from Alice and his quantum information $\bigotimes_{i=1}^n \mathcal{S}_i(\sigma_{X_i,\Theta_i})$. Expressing the nonuniformity in terms of the trace distance allows us to observe that $\delta_{\mathrm{sec}} = 2^{-n}\sum_{\theta\in\{+,\times\}^n} d(S_{\bar{C}'}|\Theta = \theta, S_{C'}C'\rho_B)$. Now, for fixed $\Theta = \theta$, it is clear from the construction that $S_{C'}$, C', $F_{C'}$ and $\bigotimes_{i\in\mathcal{I}_{C'}} \mathcal{S}_i(\sigma_{X_i,C'})$ are independent of $S_{\bar{C}'} = F_{\bar{C}'}(X_{|\mathcal{I}_{\bar{C}'}})$ and we can use Eq. (1). Hence, one can bound the nonuniformity as in Lemma 1, i.e., by the square root of the probability of correctly guessing $X_{|\mathcal{I}_{\bar{C}'}}$ given the state $\bigotimes_{i\in\mathcal{I}_{\bar{C}'}} \mathcal{S}_i(\sigma_{X_i,\bar{C}'})$. We show in detail in [8] that to guess X, Bob can measure each remaining qubit individually and hence we obtain

$$\begin{aligned}\delta_{\mathrm{sec}} &\leq 2^{(\ell/2)-1}2^{-n} \sum_{\theta\in\{+,\times\}^n} \left(\prod_{i\in\mathcal{I}_{\bar{C}'}} P_g(X_i|\mathcal{S}_i(\sigma_{\bar{C}'}))\right)^{1/2} \\ &\leq 2^{(\ell/2)-1}\left(2^{-n}\prod_{i=1}^n [1 + P_g(X_i|\mathcal{S}_i(\sigma_{\bar{C}'}))]\right)^{1/2},\end{aligned}$$

where we used the concavity of the square-root function in the last inequality. From the bound $\prod_i P_g(X_i|\mathcal{S}_i(\sigma_{\bar{C}'})) \leq (\Delta_{\max})^n$, it is not hard to see (see [8]) that

$$\delta_{\mathrm{sec}} \leq 2^{(\ell/2)-1}(\Delta_{\max})^{(\log(4/3)/2)n}.$$

Recall that for essentially any noisy superoperator $\Delta(\mathcal{S}) < 1$. This shows that for any individual-storage attacks there exists an n which yields arbitrarily high security.

Example 1.—Let us now consider the security in an explicit example: a depolarizing channel. In order to explicitly bound $\Delta(\mathcal{S}_i)$ we allow for intermediate strategies of Bob in which he partially measures the incoming qubits leaving some quantum information undergoing depolarizing noise. To model this noise we let $\mathcal{S}_i = \mathcal{N} \circ \mathcal{P}_i$, where $\mathcal{P}_i$ is any noiseless quantum operation of Bob's choosing from one qubit to one qubit that generates some classical output. For example, $\mathcal{P}_i$ could be a partial measurement providing Bob with some classical information and a slightly disturbed quantum state, or just a unitary operation. Let $\mathcal{N}(\rho) := r\rho + (1 - r)(\mathbb{1}/2)$ be the fixed depolarizing "quantum-storage" channel that Bob cannot influence (see Fig. 1). To determine δ_{sec}, we have to find an uncertainty relation similar to Eq. (2) by optimizing over all possible partial measurements $\mathcal{P}_i$, $\max_{\mathcal{S}_i}\Delta(\mathcal{S}_i)^2 = \max_{\mathcal{P}_i} P_g(X|\mathcal{S}_i(\sigma_+))P_g(X|\mathcal{S}_i(\sigma_\times))$. We can tackle this optimization problem for depolarizing noise using the symmetries inherent in our problem. In [8] we derive the following clear-cut theorem: Let $\mathcal{N}$ be the depolarizing channel and let $\max_{\mathcal{S}_i}\Delta(\mathcal{S}_i)$ be defined as above. Then for $r \geq 1/\sqrt{2}$ we have $\max_{\mathcal{S}_i}\Delta(\mathcal{S}_i) = \frac{1+r}{2}$ and for $r < 1/\sqrt{2}$, $\max_{\mathcal{S}_i}\Delta(\mathcal{S}_i) = \frac{1}{2} + \frac{1}{2\sqrt{2}}$. Our result shows that Bob's optimal strategies are the two trivial ones. In the case of high noise $r < 1/\sqrt{2}$, a direct measurement $\mathcal{M}$ in the Breidbart basis is the best attack Bob can perform in order to max-

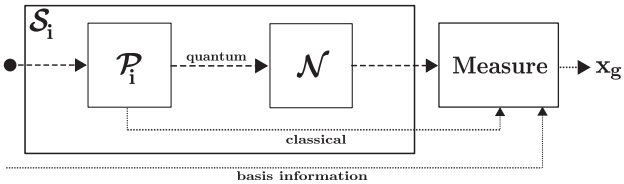

FIG. 1. Bob performs a partial measurement $\mathcal{P}_i$, followed by noise $\mathcal{N}$, and outputs a guess bit x_g depending on his classical measurement outcome, the remaining quantum state, and the additional basis information.

imize the product of the guessing probabilities. For this measurement, we have $\Delta(\mathcal{M}) = 1/2 + 1/(2\sqrt{2})$. If the depolarizing noise is low ($r \geq 1/\sqrt{2}$), then our result states that the best strategy for Bob is to simply store the qubit as is.

Discussion.—In future work one may consider removing the assumption about the independence of Bob's storage procedure, i.e., show security against general coherent noisy attacks. The problem with analyzing a coherent attack of Bob described by some superoperator $\mathcal{S}$ affecting all his incoming qubits is not merely a technical one: one first needs to determine a realistic noise model.

In terms of long-term security, *fault-tolerant* photonic computation (e.g., with the KLM scheme [21]) might allow a dishonest Bob to encode the incoming quantum information into a fault-tolerant quantum memory. This implies that in storage, the effective noise rate can be made arbitrarily small. The encoding of a single unknown state is *not* a fault-tolerant quantum operation. Hence, even in the presence of a quantum computer, there is a residual storage-noise rate due to the unprotected encoding operation. The question of security then becomes a question of a trade-off between this residual noise rate versus the intrinsic noise rate for honest parties. Intuitively—even in the long run—things can be arranged in such a way that tasks of honest players are technically easier to perform than the ones for dishonest players. We believe that this intrinsic gap can always be exploited for cryptographic purposes. This Letter can be appreciated as a first step in this direction.

We thank Charles Bennett, David DiVincenzo, Renato Renner, Falk Unger, and Ronald de Wolf for interesting discussions. C. S. and S. W. are supported by EU fifth framework Project No. QAP IST 015848 and the NWO VICI Project No. 2004-2009. B. M. T. acknowledges support by DTO through ARO Contract No. W911NF-04-C-0098. S. W. thanks IBM Watson and B. M. T. thanks the Instituut Lorentz in Leiden for their kind hospitality.

[1] H.-K. Lo, Phys. Rev. A **56**, 1154 (1997); D. Mayers, arXiv:quant-ph/9603015; H.-K. Lo and H. F. Chau, Phys. Rev. Lett. **78**, 3410 (1997); D. Mayers, Phys. Rev. Lett. **78**, 3414 (1997); H.-K. Lo and H. F. Chau, in *Proceedings of the Fourth Workshop on Physics and Computation, PhysComp' 96, Boston, 1996* (New England Complex Systems Institute, Boston, 1996), p. 76.

[2] J. Kilian, in *Proceedings of the Twentieth Annual ACM Symposium on Theory of Computing (STOC), Chicago, 1988* (ACM Press, New York, 1988), pp. 20–31; O. Goldreich and R. Vainish, in *Proceedings of the Annual Cryptology Conference (CRYPTO '87), Santa Barbara, 1987* (Springer, New York, 1988), pp. 73–86.

[3] S. Wiesner, SIGACT News **15**, 78 (1983); M. Rabin, Aiken Comp. Lab., Harvard University, Technical Report No. 81, 1981; S. Even, O. Goldreich, and A. Lempel, Commun. ACM **28**, 637 (1985).

[4] I. Damgård *et al.*, in *Proceedings of 46th Annual IEEE Symposium on Foundations of Computer Science (FOCS '05), Pittsburgh, PA, 1995* (IEEE Computer Society, New York, 2005), pp. 449–458.

[5] I. Damgård *et al.*, in *Proceedings of the Annual International Cryptology Conference (CRYPTO '07), Santa Barbara, 2007* (Springer, New York, 2007), pp. 360–378.

[6] C. H. Bennett and G. Brassard, in *Proceedings of the IEEE ICCSS* (IEEE, New York, 1984), pp. 175–179.

[7] N. Gisin *et al.*, Rev. Mod. Phys. **74**, 145 (2002).

[8] S. Wehner, C. Schaffner, and B. M. Terhal, arXiv:0711.2895.

[9] Damgård *et al.*, in *Proceedings of the Annual International Cryptology Conference (CRYPTO '07)* (Ref. [5]), pp. 342–359.

[10] C. H. Bennett *et al.*, in *Proceedings of the Annual International Cryptology Conference (CRYPTO '91), Santa Barbara, 1991* (Springer Verlag, Berlin, 1992), pp. 351–366.

[11] C. Schaffner, Ph.D. thesis, University of Aarhus, 2007, arXiv:0709.0289.

[12] I. Damgård *et al.*, SIAM J. Comput. **37**, 1865 (2008).

[13] C. Crépeau and J. Kilian, in *Proceedings of the 29th Annual Symposium on Foundations of Computer Science (FOCS '88), White Plains, NY, 1988* (IEEE, New York, 1988); C. Crépeau, K. Morozov, and S. Wolf, in *Proceedings of the Security in Communication Networks (SCN) 4th International Conference, Amalfi, Italy* (Springer, New York, 2004); C. Crépeau, in *Proceedings of EUROCRYPT '97, Konstanz, Germany, 1997* (Springer, New York, 1997).

[14] L. Salvail, in *Proceedings of the 18th Annual International Cryptology Conference (CRYPTO '98), Santa Barbara, 1998* (Springer, New York, 1998), pp. 338–353.

[15] D. Beaver, in *Proceedings of the Annual International Cryptology Conference (CRYPTO '95), Santa Barbara, 1995* (Springer, New York, 1995), pp. 97–109.

[16] S. Fehr and C. Schaffner, arXiv:0804.1059; S. Wehner and J. Wullschleger, arXiv:0709.0492 [in Proceedings of ICALP '08 (to be published)].

[17] J. L. Carter and M. N. Wegman, J. Comput. Syst. Sci. **18**, 143 (1979).

[18] R. Renner, Ph.D. thesis, ETH Zurich, 2005, arXiv:quant-ph/0512258.

[19] Buhrman *et al.*, Phys. Rev. Lett. **97**, 250501 (2006).

[20] If $X_{|I_b}$ is less than n bits long Alice pads the string $X_{|I_b}$ with 0's to get an n bit-string in order to apply the hash function to n bits.

[21] E. Knill, R. Laflamme, and G. Milburn, Nature (London) **409**, 46 (2001).