Simple protocols for oblivious transfer and secure identification in the noisy-quantum-storage model

Christian Schaffner*
Centrum Wiskunde & Informatica (CWI), P.O. Box 94079, NL-1090 GB Amsterdam, Netherlands
(Received 1 April 2010; published 10 September 2010)

We present simple protocols for oblivious transfer and password-based identification which are secure against general attacks in the noisy-quantum-storage model as defined in R. König, S. Wehner, and J. Wullschleger [e-print arXiv:0906.1030]. We argue that a technical tool from König *et al.* suffices to prove security of the known protocols. Whereas the more involved protocol for oblivious transfer from König *et al.* requires less noise in storage to achieve security, our "canonical" protocols have the advantage of being simpler to implement and the security error is easier control. Therefore, our protocols yield higher OT rates for many realistic noise parameters. Furthermore, a proof of security of a direct protocol for password-based identification against general noisy-quantum-storage attacks is given.

DOI: 10.1103/PhysRevA.82.032308 PACS number(s): 03.67.Dd, 03.67.Ac

I. INTRODUCTION

Throughout history, a main goal of cryptography has been to provide secure communication over insecure channels. In today's internet-driven society, however, more advanced tasks arise: People need to do business and interact with peers they neither know nor trust. A simple example is *secure identification*: Users Alice and Bob share a password P, and when setting up a communication, Alice wants to make sure she is really interacting with Bob—the only other person who knows P. Simply announcing P is insecure, as any eavesdropper can intercept P and use it later to impersonate Bob. We need a method for checking whether two parties are in possession of the same password, but without revealing any additional information.

Secure identification is a special case of the more general problem of *secure two-party computation*: Alice and Bob want to perform a computation on private inputs in a way so that they obtain the correct result but no additional information about their inputs is revealed. An interesting example consists of sealed-bit auctions where the winner should be determined without opening the losing bids. Closer to everyday life, almost any interaction with an automated teller machine can be seen as an instance of secure two-party computation.

The techniques used in modern classical cryptography to secure communication and provide secure two-party computation are based on unproven mathematical assumptions such as the hardness of finding the prime factors of large integer numbers (for example, in the widely used RSA scheme by Rivest-Shamir-Adleman [1]). We do not know any practical schemes which are provably infeasible to break and it is unlikely that the currently known mathematical techniques allow for such a scheme. In contrast, quantum cryptography, which is based on transmitting information stored in the state of single elementary particles, offers schemes with *provable security*.

The most prominent example is quantum key distribution (QKD), which allows two honest parties to securely communicate. In 1984, Bennett and Brassard proposed a QKD protocol [2] which was proven unconditionally secure [3–5]. In other words, security does not rely on any unproven assumptions but holds against any eavesdropper Eve with unbounded (quantum) computing power. Such provably secure key-distribution schemes cannot be achieved by any classical means (without additional assumptions). It is important to realize that the technical requirements for honest parties to perform QKD protocols are well within reach of current technology. As of today, the technology has even reached commercial level: At least three different companies are selling hardware for QKD [6–8].

After the discovery of QKD, researchers thought it was possible to use quantum communication to implement more advanced cryptographic primitives such as secure two-party computation. However, it was shown in the late 1990s that essentially *no* cryptographic two-party primitives can be realized if only a quantum channel is available and no further restriction on the adversary is assumed [9–11]. In other words, secure two-party computation is more difficult to achieve than key distribution. This is not completely surprising given the generality of secure two-party computation. Nevertheless, quantum cryptography might still help to achieve significantly better schemes than purely classical constructions.

Indeed, in joint work with Damgård, Fehr, and Salvail, we proposed in 2005 a realistic assumption for quantum protocols under which provably secure two-party computation becomes possible [12]. The basic idea is to exploit the technical difficulty of storing quantum information. In this *bounded-quantum-storage model*, security holds based on the sole assumption that the parties' *quantum memory during the execution of the protocol* is upper bounded. No further restrictions on the (quantum) computing power or the classical memory size are assumed. Storing quantum information requires keeping the state of very small physical systems such as single atoms or photons under stable conditions over a long time. Building a reliable quantum memory is a major research goal in experimental quantum physics [13–17]. Despite these efforts, current technology only allows storage times of at most a few milliseconds.

Even though breaking the security of our protocols requires a large quantum memory with long storage times, neither quantum memory nor the ability to perform quantum computations are needed to actually run the protocols; the technological requirements for honest parties are comparable to QKD and hence well within reach of current technology. Therefore,

*c.schaffner@cwi.nl

cryptographic schemes based on storage imperfections provide potentially very useful solutions for secure two-party computation with the advantage of much stronger security guarantees compared to classical technology.

A. Bounded- vs noisy-quantum-storage model

In the bounded-quantum-storage model, we assume that a dishonest receiver can perfectly store the incoming photons and perform perfect quantum operations under the sole restriction that at a certain point of the protocol, the size of his quantum memory is limited to a constant fraction of the total number of received photons. Bounding the size of the adversary's quantum storage in this way is a handy assumption to work with in security proofs. In a series of works over the past years [12,18–22], it has been shown that any type of secure two-party computation is possible in the bounded-quantum-storage model.

On the other hand, simply limiting the adversary's quantum memory size does not capture correctly the difficulty one currently faces when trying to store photons. A better formalization of this difficulty is to assume that the dishonest receiver uses the best available (but still imperfect) photon-storage device. The imperfection of the storage-device is modeled as a noisy quantum channel where the noise level of the channel increases with the amount of time during which the quantum information needs to be stored. With current technology, the noise reaches maximum level (i.e., the quantum information is completely lost) if a storage time on the order of milliseconds is required [13].

First results in this *noisy-quantum-storage model* have been established in joint work with Terhal and Wehner [23,24]. Assuming "individual-storage attacks"—where the adversary treats all incoming qubits in the same way—the security of oblivious transfer and password-based identification was established using the original protocols from the bounded-quantum-storage model [18,22].

The most general storage attacks were first mentioned in [20], but addressed only recently by König, Wehner, and Wullschleger [25]. In this most general model, the adversary can for example try to use a quantum error-correcting code in order to protect himself from storage errors. Concretely, he is allowed to first perform an arbitrary perfect "encoding attack" on the incoming quantum state, then he uses his (noisy) quantum-storage device together with unlimited classical memory and finally, he can again perform perfect quantum computations.[1] The authors of [25] show how the security of protocols in this general model can be related to the maximal rate of classical information that can be transmitted over the noisy storage channel.

In more detail, [25] introduces the conceptual novelty of splitting the security analysis of protocols for oblivious transfer and bit commitment in two phases. In the first phase, the players use the well-known BB84 quantum coding scheme to achieve a (quantum) primitive which the authors call *weak string erasure*. At the end of this phase, the sender has a classical n-bit string X and the receiver holds an "erased version" of the string where a uniformly random half of the bits of X have been erased. Note that this primitive is only classical for honest players, as a dishonest receiver might hold quantum information about the sender's classical output string.

For the second (purely classical) phase, they propose classical reductions to build bit commitment and oblivious transfer based on weak string erasure. Their approach to realize oblivious transfer is quite involved. It uses interactive hashing [26], for which the standard classical protocol requires a lot of communication rounds [27].[2] The analysis is complicated by the fact that the dishonest receiver holds quantum information, but can be handled by techniques of min-entropy sampling developed by König and Renner [29]. It was left as open question how to build password-based identification based on weak string erasure or in general, secure against noisy-quantum-storage attacks.

B. Our results and outline of the article

The main contribution of this article is the insight that the new technical tool derived in [25] already suffices to prove secure the original protocols from the bounded-quantum-storage model for bit commitment, oblivious transfer [18], and password-based identification [19,22]. These original protocols have the advantage that the classical postprocessing is extremely simple. No communication-intensive protocols such as interactive hashing are needed.

Comparing the protocol for oblivious transfer from [25] with our protocol, it turns out that the highly interactive protocol [25] can in theory be shown to be secure for less noisy quantum-storage channels if infinitely many pulses are available, that is, security holds against a larger class of adversarial receivers. However, the original protocols with the simpler analysis presented here outperform the ones from [25] in terms of the security error. Thus, for a fixed number of pulses and a given security threshold, the simpler protocols and our analysis yield oblivious transfer of longer bit strings most of the time.

We show the security against general noisy-storage attacks of a direct protocol for password-based identification, answering an open question posed in [25].

From a theoretical point of view, our insight shows that despite the generality of the noisy-quantum-storage model, having the right tools from [18,25] at hand, the protocols and security proofs do not need to be much more complicated than in the conceptually simpler bounded-quantum-storage model.

C. Outline of the article

In Sec. II, we define concepts and notation and elaborate on the essential tool of min-entropy splitting in Sec. II C. We present the noisy quantum storage model and the key ingredient from [25] in Sec. III. Sections IV, V, and VI contain the security analyses for oblivious transfer and password-based identification.

[1] A detailed description of the model of [25] is given in Sec. III (see also Fig. 1).

[2] A constant-round variant of interactive hashing has been proposed in [28]. However, it is unclear how the weaker security guarantees affect the security proof in [25]. The use of η-almost t-wise independent permutations might render this variant "prohibitively complicated to implement in practice" [26].

II. PRELIMINARIES

We start by introducing the necessary definitions, tools, and technical lemmas that we need in the remainder of this text.

A. Basic concepts

We use $\in_R$ to denote the uniform choice of an element from a set. We further use $x|_{\mathcal{I}}$ to denote the string $x = x_1, \ldots, x_n$ restricted to the bits indexed by the set $\mathcal{I} \subseteq \{1, \ldots, n\}$. For a binary random variable C, we denote by $\overline{C}$ the bit different from C.

1. Classical-quantum states

A *classical-quantum* (cq)-*state* ρ_{XE} is a state that is partly classical, partly quantum, and can be written as

$$\rho_{XE} = \sum_{x \in \mathcal{X}} P_X(x) |x\rangle\langle x| \otimes \rho_E^x. \tag{1}$$

Here, X is a classical random variable distributed over the finite set $\mathcal{X}$ according to distribution P_X, $\{|x\rangle\}_{x \in \mathcal{X}}$ is a set of orthonormal states, and the register E is in state ρ_E^x when X takes on value x. This notion extends to states with more than two registers, either of which can be classical or quantum. For example, a cqq-state ρ_{XED} has one classical register X and two quantum registers E and D.

2. Conditional independence

We also need to express that a random variable X is (close to) independent of a quantum state E *when given a random variable* Y. This means that when given Y, the state E gives no additional information on X. Formally, this is expressed by requiring that ρ_{XYE} equals (or is close to) $\rho_{X \leftrightarrow Y \leftrightarrow E}$, which is defined as[3]

$$\rho_{X \leftrightarrow Y \leftrightarrow E} := \sum_{x,y} P_{XY}(x,y) |x\rangle\langle x| \otimes |y\rangle\langle y| \otimes \rho_E^y. \tag{2}$$

In other words, $\rho_{XYE} = \rho_{X \leftrightarrow Y \leftrightarrow E}$ precisely if $\rho_E^{x,y} = \rho_E^y$ for all x and y. To further illustrate its meaning, notice that if the Y register is measured and value y is obtained, then the state $\rho_{X \leftrightarrow Y \leftrightarrow E}$ collapses to $(\sum_x P_{X|Y}(x|y)|x\rangle\langle x|) \otimes \rho_E^y$, so that indeed no further information on x can be obtained from the E register. This notation naturally extends to $\rho_{X \leftrightarrow Y \leftrightarrow E|\mathcal{E}}$ simply by considering $\rho_{XYE|\mathcal{E}}$ instead of ρ_{XYE}. Explicitly, $\rho_{X \leftrightarrow Y \leftrightarrow E|\mathcal{E}} = \sum_{x,y} P_{XY|\mathcal{E}}(x,y)|x\rangle\langle x| \otimes |y\rangle\langle y| \otimes \rho_{E|\mathcal{E}}^y$.

3. Nonuniformity

We can say that a quantum adversary has little information about X if the distribution P_X given his quantum state is close to uniform. Formally, this distance is quantified by the *nonuniformity* of X given $\rho_E = \sum_x P_X(x)\rho_E^x$ defined as

$$d(X|E) := \frac{1}{2} \left\| \mathbb{1}/|\mathcal{X}| \otimes \rho_E - \sum_x P_X(x)|x\rangle\langle x| \otimes \rho_E^x \right\|_1. \tag{3}$$

Intuitively, $d(X|E) \leqslant \varepsilon$ means that the distribution of X is ε close to uniform even given ρ_E; that is, ρ_E gives hardly any information about X. A simple property of the nonuniformity which follows from its definition is that it does not change given independent information. Formally,

$$d(X|E,D) = d(X|E) \tag{4}$$

for any cqq state of the form $\rho_{XED} = \rho_{XE} \otimes \rho_D$.

B. Entropic quantities

Throughout this article we use a number of entropic quantities. The *binary-entropy* function is defined as $h(p) := -p \log_2 p - (1-p)\log_2(1-p)$.

1. (Conditional) smooth min-entropy

For a cq-state ρ_{XE} as introduced in (1), we define the *guessing probability of* X *given* E as the success probability of the best measurement carried out on E in order to guess X,

$$p_{\text{guess}}(X|E) := \max_{\{M_x\}} \sum_x P_X(x) \text{Tr}\left(M_x \rho_E^x\right),$$

where the maximization is over all positive operator-valued measurements (POVMs) $\{M_x\}$ acting on register E. The conditional min-entropy of X given E is defined as $H_{\min}(X|E) := -\log_2 p_{\text{guess}}(X|E)$.

In case the adversary's information E is described by a classical variable Y, one can show that the guessing probability becomes

$$p_{\text{guess}}(X|Y) := \sum_y P_Y(y) \max_x P_{X|Y}(x|y) = \sum_y \max_x P_{XY}(x,y).$$

More generally, we define $H_{\min}(X\mathcal{E}|Y)$ for any event $\mathcal{E}$ as $H_{\min}(X\mathcal{E}|Y) := -\log_2[p_{\text{guess}}(X\mathcal{E}|Y)]$, where[4]

$$\begin{aligned} p_{\text{guess}}(X\mathcal{E}|Y) &:= \sum_y P_Y(y) \max_x P_{X\mathcal{E}|Y}(x|y) \\ &= \sum_y \max_x P_{XY\mathcal{E}}(x,y). \end{aligned}$$

The *conditional smooth min-entropy* $H_{\min}^{\varepsilon}(X|Y)$ is then defined as

$$H_{\min}^{\varepsilon}(X|Y) := \max_{\mathcal{E}} H_{\min}(X\mathcal{E}|Y),$$

where the max is over all events $\mathcal{E}$ with $P[\mathcal{E}] \geqslant 1 - \varepsilon$.

Obviously, the unconditional versions of smooth and nonsmooth min-entropy are obtained by using a constant Y. Furthermore, conditional smooth min-entropy can also be defined for quantum side information, we refer to [25,30] for the formal definitions.

In this article, we will use the fact that smooth min-entropy obeys the chain rule [30], Theorem 3.2.12]; that is for a ccq-state ρ_{XYE}, we have

$$H_{\min}^{\varepsilon}(X|YE) \geqslant H_{\min}^{\varepsilon}(X|E) - \log_2 |\mathcal{Y}|, \tag{5}$$

where $|\mathcal{Y}|$ is the alphabet size of Y.

[3] The notation is inspired by the classical setting where the corresponding independence of X and Z given Y can be expressed by saying that $X \leftrightarrow Y \leftrightarrow Z$ forms a Markov chain.

[4] $p_{\text{guess}}(X\mathcal{E}|Y)$ can be understood as the optimal probability of guessing X *and* having $\mathcal{E}$ occur when given Y.

C. Min-entropy splitting

The key ingredients for the security proofs of both the 1-2 oblivious transfer (OT) and the secure identification schemes in [18,19] are uncertainty relations and variants of the *min-entropy splitting lemma*. In this section, we present an overview over the variants known and derived for the bounded-quantum-storage model and point out how they can be applied in the noisy-quantum-storage model.

If the joint entropy of two random variables X_0 and X_1 is large, then one is tempted to conclude that at least one of X_0 and X_1 must still have large entropy, for example, half of the original entropy. Whereas such a reasoning is correct for Shannon entropy (it follows easily from the chain rule and the fact that conditioning does not increase the entropy), it is in general incorrect for min-entropy. There exist joint probability distributions $P_{X_0X_1}$ for which guessing X_0 and X_1 individually is easy, but guessing X_0 and X_1 simultaneously is hard. Intuitively, for these distributions, guessing the value x_i with the highest probability is easy, because the probabilities over the other variable X_{1-i} are uniform, but still sum up to a significant mass.

However, the following basic version of the min-entropy splitting lemma, which first appeared in a preliminary version of [31] and was later developed further in the context of randomness extraction [29], shows that the intuition about splitting the min-entropy *is* correct in a randomized sense. This lemma (with a slightly different notion of min-entropy) is used in the security proof of the 1-2 OT scheme in [18].

Lemma 1 (*min-entropy-splitting lemma* [18]). Let $\varepsilon \geqslant 0$, and let X_0, X_1, and Z be random variables with $H_{\min}^{\varepsilon}(X_0X_1|Z) \geqslant \alpha$. Then there exists a random variable $D \in \{0,1\}$ such that

$$H_{\min}^{\varepsilon}(X_D|DZ) \geqslant \alpha/2 - 1.$$

In order to prove the security of the identification scheme (see Sec. VI), a more refined version of the min-entropy splitting lemma was derived in [22]. We reproduce it here for convenience.

Lemma 2 (*entropy-splitting lemma* [22]). Let $\varepsilon \geqslant 0$. Let $X_1,\ldots,X_m$ and Z be random variables such that $H_{\min}^{\varepsilon}(X_iX_j|Z) \geqslant \alpha$ for all $i \neq j$. Then there exists a random variable V over $\{1,\ldots,m\}$ such that for any *independent* random variable W over $\{1,\ldots,m\}$ with $H_{\min}(W) \geqslant 1$,

$$H_{\min}^{2m\varepsilon}(X_W|VWZ, V \neq W) \geqslant \alpha/2 - \log_2(m) - 1.$$

D. Quantum uncertainty relation

At the very core of our security proofs lies (a special case of) the quantum uncertainty relation from [18][5] that lower bounds the (smooth) min-entropy of the outcome when measuring an arbitrary n-qubit state in a random basis $\theta \in \{0,1\}^n$.

Theorem 1 (*uncertainty relation* [18]). Let E be an arbitrary fixed n-qubit state. Let Θ be uniformly distributed over $\{+,\times\}^n$ (independent of E), and let $X \in \{0,1\}^n$ be the random variable for the outcome of measuring E in basis Θ. Then, for any $\delta > 0$, the conditional smooth min-entropy is lower bounded by

$$H_{\min}^{\varepsilon}(X|\Theta) \geqslant \left(\tfrac{1}{2} - 2\delta\right) n,$$

with $\varepsilon \leqslant 2^{-\sigma(\delta)n}$ and

$$\sigma(\delta) := \frac{\delta^2 \log_2(e)}{32[2 - \log_2(\delta)]^2}. \tag{6}$$

E. Privacy amplification

We will make use of two-universal hash functions. A class $\mathcal{F}$ of functions $f : \{0,1\}^n \to \{0,1\}^\ell$ is called two universal, if for all $x \neq y \in \{0,1\}^n$, we have $\Pr_{f\in_R\mathcal{F}}[f(x) = f(y)] \leqslant 2^{-\ell}$ [32]. The following theorem expresses how the application of hash functions increases the privacy of a random variable X given a quantum adversary holding ρ_E, the function F, and a classical random variable U:

Theorem 2 [18,30]. Let $\mathcal{F}$ be a class of two-universal hash functions from $\{0,1\}^n$ to $\{0,1\}^\ell$. Let F be a random variable that is uniformly and independently distributed over $\mathcal{F}$, and let ρ_{XUE} be a ccq state. Then, for any $\varepsilon \geqslant 0$,

$$d[F(X)|F,U,E] \leqslant 2^{-\frac{1}{2}[H_{\min}^{\varepsilon}(X|UE)-\ell]-1} + \varepsilon.$$

III. THE NOISY-QUANTUM-STORAGE MODEL

The *noisy-quantum-storage model* has been established in [23,24] for the special case where the dishonest receiver is limited to so-called "individual-storage attacks", that is, he treats every incoming pulse independently (akin to individual attacks in QKD).

The most general setting considered here is exactly the one described in detail in [25], Secs. 1.3 and 3.3] (see Fig. 1 for an illustration). The cheating receiver is computationally unbounded, has unlimited classical storage, and can perform

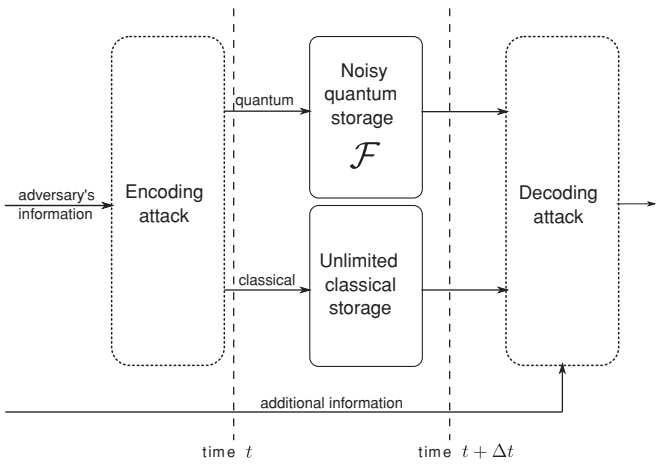

FIG. 1. During waiting times Δt, the adversary must use his noisy quantum storage described by the CPTP map $\mathcal{F}$. Before using his quantum storage, he performs any (error-free) "encoding attack" of his choosing, which consists of a measurement or an encoding into an error-correcting code. After time Δt, he receives some additional information that he can use for decoding. Figure from [33].

[5]In [18], a stricter notion of conditional smooth min-entropy was used, which in particular implies the bound as stated here.

perfect quantum operations. If the protocol instructs parties to wait for time Δt, a dishonest player has to discard all quantum information, except for what he can encode arbitrarily into his (noisy) quantum storage. This storing process is formally described by a completely positive and trace-preserving (CPTP) map $\mathcal{F}:\mathcal{B}(\mathcal{H}_{\text{in}})\to\mathcal{B}(\mathcal{H}_{\text{out}})$.

As in [25], let

$$P_{\text{succ}}^{\mathcal{F}}(n):=\max_{\{D_x\}_x,\{\rho_x\}_x}\frac{1}{2^n}\sum_{x\in\{0,1\}^n}\text{Tr}[D_x\mathcal{F}(\rho_x)] \tag{7}$$

be the maximal success probability of correctly decoding a randomly chosen n-bit string $x\in\{0,1\}^n$ sent over the quantum channel $\mathcal{F}$. Here, the maximum is over families of code states $\{\rho_x\}_{x\in\{0,1\}^n}$ on $\mathcal{H}_{\text{in}}$ and decoding POVMs $\{D_x\}_{x\in\{0,1\}^n}$ on $\mathcal{H}_{\text{out}}$.

Intuitively, if the quantum channel $\mathcal{F}$ does not allow to transmit enough classical information over it, we should be able to prove security against a dishonest Bob with such a storage channel. Indeed, the following two lemmas from [25] formalize this intuition and are the key ingredients in connecting the security of protocols in the noisy-storage model for such channels with their ability to transmit classical information.

Lemma 3 [25]. Consider an arbitrary cq-state ρ_{XQ} and a CPTP map $\mathcal{F}:\mathcal{B}(\mathcal{H}_Q)\to\mathcal{B}(\mathcal{H}_{\text{out}})$. Then $H_{\min}[X|\mathcal{F}(Q)]\geqslant -\log_2 P_{\text{succ}}^{\mathcal{F}}(\lfloor H_{\min}(X)\rfloor)$.

Lemma 4 [25]. Consider an arbitrary ccq-state ρ_{XTQ}, and let $\varepsilon,\varepsilon'\geqslant 0$ be arbitrary. Let $\mathcal{F}:\mathcal{B}(\mathcal{H}_Q)\to\mathcal{B}(\mathcal{H}_{Q_{\text{out}}})$ be an arbitrary CPTP map. Then

$$H_{\min}^{\varepsilon+\varepsilon'}[X|T\mathcal{F}(Q)]\geqslant -\log_2 P_{\text{succ}}^{\mathcal{F}}\left(\left\lfloor H_{\min}^{\varepsilon}(X|T)-\log_2\frac{1}{\varepsilon'}\right\rfloor\right).$$

We are interested in channels $\mathcal{N}$ which satisfy the following *strong-converse property*: The success probability (7) decays exponentially for rates R above the capacity; that is, it takes the form

$$\begin{aligned}&P_{\text{succ}}^{\mathcal{N}^{\otimes n}}(nR)\leqslant 2^{-n\gamma^{\mathcal{N}}(R)},\quad \text{where}\\ &\gamma^{\mathcal{N}}(R)>0\quad \text{for all}\quad R>C_{\mathcal{N}}.\end{aligned} \tag{8}$$

In [34], property (8) was shown to hold for a large class of channels. An important example for which we obtain security is the d-dimensional depolarizing channel $\mathcal{N}_r:\mathcal{B}(\mathbb{C}^d)\to\mathcal{B}(\mathbb{C}^d)$ defined for $d\geqslant 2$ as

$$\mathcal{N}_r(\rho):=r\rho+(1-r)\frac{\mathbb{1}}{d}\quad \text{for some fixed}\quad 0\leqslant r\leqslant 1, \tag{9}$$

which replaces the input state ρ with the completely mixed state with probability $1-r$. For $d=2$, having storage channel $\mathcal{N}_r^{\otimes n}$ means that the adversary can store n qubits which are affected by independent and identically distributed noise. To see for which values of r we can obtain security, we need to consider the classical capacity of the depolarizing channel as evaluated by King [35]. For $d=2$, that is, qubits, it is given by

$$C_{\mathcal{N}_r}=1+\frac{1+r}{2}\log_2\frac{1+r}{2}+\frac{1-r}{2}\log_2\frac{1-r}{2}.$$

IV. 1-2 OBLIVIOUS TRANSFER

A. Security definition and protocol

In this section we prove the security of a randomized version of 1-2 OT (Theorem 3) from which we can easily obtain 1-2 OT. In such a randomized 1-2 OT protocol, Alice does not input two strings herself, but instead receives two strings $S_0, S_1\in\{0,1\}^\ell$ chosen uniformly at random. Randomized OT (ROT) can easily be converted into OT. After the ROT protocol is completed, Alice uses her strings S_0,S_1 obtained from ROT as one-time pads to encrypt her original inputs $\hat{S}_0$ and $\hat{S}_1$; that is, she sends an additional classical message consisting of $\hat{S}_0\oplus S_0$ and $\hat{S}_1\oplus S_1$ to Bob. Bob can retrieve the message of his choice by computing $S_C\oplus(\hat{S}_C\oplus S_C)=\hat{S}_C$. He stays completely ignorant about the other message $\hat{S}_{\overline{C}}$ since he is ignorant about $S_{\overline{C}}$. The security of a quantum protocol implementing ROT is formally defined in [18] and justified in [36] (see also [37]).

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.

(i) (Correctness) If both parties are honest, then for any distribution of Bob's input C, Alice gets outputs $S_0,S_1\in\{0,1\}^\ell$ which are ε close to uniform and independent of C and Bob learns $Y=S_C$ except with probability ε.

(ii) (Security against dishonest Alice) 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 $\Pr[Y=S_C']\geqslant 1-\varepsilon$ and C is independent of S_0',S_1' and ρ_A.[6]

(iii) (Security against dishonest Bob) If Alice is honest, then for any cheating strategy of Bob resulting in his state ρ_B, there exists a random variable $D\in\{0,1\}$ such that $d(S_{\overline{D}}|S_D D\rho_B)\leqslant\varepsilon$.

We consider the same protocol for ROT as in [38,39].

Protocol 1 [38,39](*1-2 ROT$^\ell$*).

1. Alice picks $x\in_R\{0,1\}^n$ and $\theta\in_R\{+,\times\}^n$. At time $t=0$, she sends $|x_1\rangle_{\theta_1},\ldots,|x_n\rangle_{\theta_n}$ to Bob.

2. Bob picks $\hat{\theta}\in_R\{+,\times\}^n$ at random and measures the ith qubit in the basis $\hat{\theta}_i$. He obtains outcome $\hat{x}\in\{0,1\}^n$. Both parties wait time Δt.

3. Alice sends the basis information $\theta=\theta_1,\ldots,\theta_n$ to Bob.

4. Bob, holding choice bit c, forms the sets $\mathcal{I}_c=\{i\in[n]\mid\theta_i=\hat{\theta}_i\}$ and $\mathcal{I}_{1-c}=\{i\in[n]\mid\theta_i\neq\hat{\theta}_i\}$. He sends $\mathcal{I}_0,\mathcal{I}_1$ to Alice.

5. Alice picks two hash functions $f_0,f_1\in_R\mathcal{F}$, where $\mathcal{F}$ is a class of two-universal hash functions. She sends f_0,f_1 to Bob. Alice outputs $s_0=f_0(x|_{\mathcal{I}_0})$ and $s_1=f_1(x|_{\mathcal{I}_1})$.[7]

6. Bob outputs $s_c=f_c(\hat{x}|_{\mathcal{I}_c})$.

In case any of the players sends incorrectly formed messages, the other player aborts.

[6]The existence of the random variables S_0',S_1' has to be understood as follows: Given the cq-state ρ_{YA} of honest Bob and dishonest Alice, there exists a cccq-state $\rho_{YS_0'S_1'A}$ such that tracing out the registers of S_0',S_1' yields the original state ρ_{YA} and the stated properties hold.

[7]If $x|_{\mathcal{I}_b}$ is less than n bits long, Alice pads the string $x|_{\mathcal{I}_b}$ with 0's to get an n bit string in order to apply the hash function to n bits.

B. Security analysis

1. Correctness

First of all, note that it is clear that the protocol fulfills its task correctly. 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. Alice's outputs s_0,s_1 are perfectly independent of each other and of c.

2. Security against dishonest Alice

Security holds in the same way as shown in [18]. Alice cannot learn anything about Bob's choice bit from the index information $\mathcal{I}_0,\mathcal{I}_1$ she receives, and Alice's input strings can be extracted by letting her interact with an unbounded receiver.

3. Security against dishonest Bob

Proving that the protocol is secure against Bob requires more work. Our goal is to show that there exists a $D \in \{0,1\}$ such that Bob with noisy storage as described in Sec. III is completely ignorant about $S_{\overline{D}}$. Since we are performing 1-out-of-2 oblivious transfer of ℓ-bit strings, ℓ corresponds to the "amount" of oblivious transfer we can perform for a given security parameter ε and number of qubits n.

Theorem 3. Fix $0 < \delta < \frac{1}{4}$ and let

$$\varepsilon = 2\exp\left(-\frac{(\delta/4)^2}{32\left(2+\log_2\frac{4}{\delta}\right)^2}n\right). \tag{10}$$

Then, for any attack of a dishonest Bob with storage $\mathcal{F}: \mathcal{B}(\mathcal{H}_{\text{in}}) \to \mathcal{B}(\mathcal{H}_{\text{out}})$, Protocol 1 is 2ε-secure against a dishonest receiver Bob according to Definition 1 if $n \geqslant 4/\delta$ and

$$\ell \leqslant -\frac{1}{2}\log_2 P^{\mathcal{F}}_{\text{succ}}\left[\left(\frac{1}{4}-\delta\right)n\right] - \log_2\left(\frac{1}{\varepsilon}\right).$$

Proof. We need to show the existence of a binary random variable D such that $S_{\bar{D}}$ is ε close to uniform from Bob's point of view.

We can argue, as in the proof of the security of weak string erasure for honest Alice (Sec. 3.3 in [25]), that

$$H^{\varepsilon/2}_{\min}(X_0X_1|\Theta K) \geqslant \frac{n}{2} - \frac{n\delta}{2},$$

where K denotes Bob's classical information obtained from the encoding attack. Classical min-entropy splitting (Lemma 1) then ensures that there exists a binary random variable $D \in \{0,1\}$ such that

$$H^{\varepsilon/2}_{\min}(X_{\overline{D}}|D\Theta K) \geqslant \frac{n}{4} - \frac{n\delta}{4} - 1.$$

One can now continue to argue as in the proof of Theorem 3.3 in [25]; that is, we use Lemma 4 to get

$$\begin{aligned} H^{\varepsilon}_{\min}(X_{\overline{D}}|D\Theta K\,Q_{\text{out}}) &\geqslant -\log_2 P^{\mathcal{F}}_{\text{succ}}\left(\frac{n}{4}-\frac{n\delta}{4}-1-\log_2\frac{2}{\varepsilon}\right) \\ &\geqslant -\log_2 P^{\mathcal{F}}_{\text{succ}}\left[\left(\frac{1}{4}-\delta\right)n\right], \end{aligned}$$

where the last step follows in the same way as in [25] from the monotonicity of the success probability $P^{\mathcal{F}}_{\text{succ}}(m) \leqslant P^{\mathcal{F}}_{\text{succ}}(m')$ for $m \geqslant m'$ and the fact that $\log_2\frac{2}{\varepsilon} \leqslant \frac{\delta}{2}n \leqslant \frac{3\delta}{4}n - 1$.

The rest of the security proof is analogous to the proof in [18]: It follows from the chain rule for smooth min-entropy (5) that

$$\begin{aligned} H^{\varepsilon}_{\min}(X_{\overline{D}}|D\Theta S_D K\,Q_{\text{out}}) &\geqslant H^{\varepsilon}_{\min}(X_{\overline{D}}S_D|D\Theta K\,Q_{\text{out}}) - \ell \\ &\geqslant -\log_2 P^{\mathcal{F}}_{\text{succ}}\left[\left(\tfrac{1}{4}-\delta\right)n\right] - \ell. \end{aligned}$$

The privacy amplification Theorem 2 yields

$$d(F_{\overline{D}}(X_{\overline{D}}) \mid D\Theta F_D S_D K\,Q_{\text{out}}) \leqslant 2^{-\frac{1}{2}\{-\log_2 P^{\mathcal{F}}_{\text{succ}}[(\frac{1}{4}-\delta)n]-2\ell\}} + \varepsilon, \tag{11}$$

which is smaller than 2ε as long as

$$-\frac{1}{2}\log_2 P^{\mathcal{F}}_{\text{succ}}\left[\left(\frac{1}{4}-\delta\right)n\right] - \ell \geqslant \log_2\left(\frac{1}{\varepsilon}\right),$$

from which our claim follows. ∎

C. Tensor-product channels

Corollary 1. Let Bob's storage be described by $\mathcal{F} = \mathcal{N}^{\otimes\nu n}$, with $\nu > 0$, where $\mathcal{N}$ satisfies the strong-converse property (8), and

$$C_{\mathcal{N}}\nu < \tfrac{1}{4}.$$

Fix $\delta \in]0, \frac{1}{4} - C_{\mathcal{N}}\nu[$, and let ε be defined as in (10). Then, for any attack of a dishonest Bob, Protocol 1 is 2ε secure against a dishonest receiver Bob according to Definition 1, if $n \geqslant 4/\delta$ and

$$\ell \leqslant \gamma^{\mathcal{N}}\left(\frac{1/4-\delta}{\nu}\right)\frac{\nu n}{2} - \log_2\left(\frac{1}{\varepsilon}\right).$$

Proof. We can substitute n with νn and R with R/ν in the strong-converse property (8) to obtain

$$-\frac{1}{n}\log_2 P^{\mathcal{N}^{\otimes\nu n}}_{\text{succ}}(nR) \geqslant \nu\gamma^{\mathcal{N}}(R/\nu).$$

The claim then follows from Theorem 3 by setting $R := \frac{1}{4} - \delta$. ∎

For the d-dimensional depolarizing channel,

$$\mathcal{N}_r(\rho) = r\rho + (1-r)\frac{\mathbb{1}}{d}, \tag{12}$$

which preserves a d-dimensional input state with probability r and depolarizes it completely with probability $1-r$, it has been shown in [25,34] that

$$\begin{aligned} \gamma^{\mathcal{N}}(R) = \max_{\alpha\geqslant 1}\frac{\alpha-1}{\alpha}\Bigg\{R - \log_2 d + \frac{1}{1-\alpha} \\ \times \log_2\left[\left(r+\frac{1-r}{d}\right)^{\alpha} + (d-1)\left(\frac{1-r}{d}\right)^{\alpha}\right]\Bigg\}. \end{aligned}$$

We compare the parameters in terms of OT and error rate of our approach to the ones in [25]. In Fig. 2, the regions of the noise parameter r and storage rate ν from our approach (red) and that used in [25] (blue) are shown. As the information rate after min-entropy splitting in our approach is lower than without min-entropy splitting, the range of noisy storage channels for which security can theoretically be shown is smaller in our approach. However, we will see in the following that the error overhead due to the complicated postprocessing

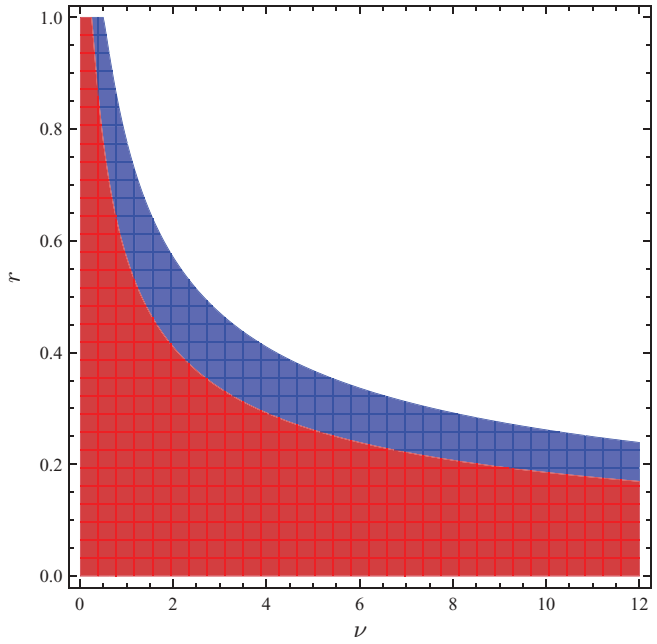

FIG. 2. (Color online) Possible regions of a depolarizing qubit channel with noise parameter r and storage rate ν where security for OT can be established for asymptotically many pulses. The approach used in [25] yields the blue meshed region, whereas our simpler approach gives the red subset of it.

with interactive hashing in [25] nullifies that advantage again.

We investigate two scenarios, in both of which we are ready to accept a security error of at most 10^{-8}. In the first scenario, we are given $n = 10^{10}$ pulses to work with against an adversary with depolarizing qubit channel ($d = 2$) with noise rate r and storage rate $\nu = 1$. In our approach, according to Corollary 1, the security error is 2ε, where ε is defined in (10); thus, for $n = 10^{10}$, we can choose $\delta = 0.0106$ to have the error small enough. The resulting OT rate ℓ/n is the red line in Fig. 3 for different noise rates r and a storage rate of $\nu = 1$. In the approach used in [25], the security error is harder to control as it also depends on other parameters such as the noise rate r and a new parameter ω. In order to keep it below the required 10^{-8}, we choose $\delta = 0.011$ and $\omega = 2$. The resulting OT rate is plotted as a blue dashed line in Fig. 3. Note that this amount of pulses is not sufficient to keep the security error below 10^{-8} for noise rates r above 0.21.

In Fig. 4, we investigate the same setting but with many more pulses, namely $n = 10^{15}$. With that many pulses, the error is better to control in the approach used in [25] and leads to higher OT rates than our approach for noise parameters in the range $0.34 < r < 0.52$. In all other cases, our simpler approach makes it possible to get OTs of longer strings while keeping the security error below 10^{-8}.

To put these numbers of pulses into perspective, one can think of a weak-coherent pulse setup which runs at 1 GHz and emits single photons with Poisson distribution with parameter $\mu = 1$, that is, with probability $e^{-\mu}\mu \approx 0.3679$ per pulse. Hence, we have to wait approximately 27 s to obtain $n = 10^{10}$ single pulses, whereas it takes $10^6 e$ s, that is, roughly 30 days, to generate $n = 10^{15}$ single pulses.

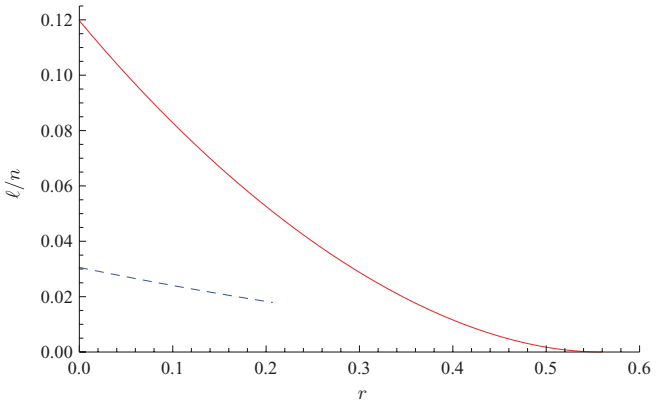

FIG. 3. (Color online) The adversary's storage is depolarizing qubit noise $\mathcal{F} = \mathcal{N}_r^{\otimes n}$, with $d = 2$, $\nu = 1$, and $n = 10^{10}$. The horizontal axis represents the noise parameter r, while the vertical axis represents the OT rate ℓ/n. The rates are only plotted for regions where the security error stays below 10^{-8}. The red solid line represents the OT rate obtained from our approach (Corollary 1, with $\delta = 0.0106$). The dashed blue line is the rate from the approach used in [25], with optimized extra parameters $\delta = 0.011$ and $\omega = 2$. For $r > 0.21$, the security error is above the allowed threshold 10^{-8}. For this many pulses, our approach provides a higher OT rate for all possible noise parameters r while keeping the security error reasonably low.

V. ROBUST OBLIVIOUS TRANSFER

In a practical setting, imperfections in Alice's and Bob's apparatus as well as in the communication channel manifest themselves in form of erasures and bit-flip errors. This setting has been analyzed for individual attacks in [24] and for general attacks in [33]. In the following, we present an upgraded protocol for oblivious transfer along the lines of [33] but with a much simpler and natural postprocessing.

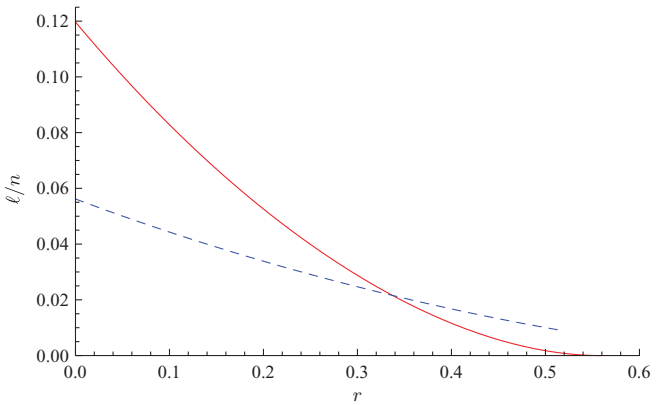

FIG. 4. (Color online) As in Fig. 3, but for many more pulses, namely, $n = 10^{15}$. The red solid line represents the OT rate obtained from our approach (Corollary 1, with $\delta = 0.000\,057\,588$). The dashed blue line is the rate from the approach used in [25], with optimized extra parameters $\delta = 0.0005$ and $\omega = 10$. For $r > 0.47$, the security error is above the allowed threshold 10^{-8}. For noise parameters in the range $0.34 < r < 0.52$, the approach used in [25] yields higher OT-rates. For all other noise rates r, our simpler approach yields higher rates.

A. Protocol

We consider the same setup as in [33]. Before engaging in the actual protocol, Alice and Bob agree on a security-error probability $\varepsilon > 0$. The parameter $p^h_{\mathrm{B,no\ click}}$ denotes the probability that an honest Bob observes no click in his detection apparatus and the corresponding parameter $\zeta^h_{\mathrm{B,no\ click}}$ says how much fluctuation we allow. Typically, we use a $\zeta^h_{\mathrm{B,no\ click}}$ of order $\sqrt{\ln(2/\varepsilon)/(2n)}$ such that the Chernoff bound allows us to argue that $p^h_{\mathrm{B,no\ click}}$ lies in the interval $[(p^h_{\mathrm{B,no\ click}} - \zeta^h_{\mathrm{B,no\ click}})n, (p^h_{\mathrm{B,no\ click}} + \zeta^h_{\mathrm{B,no\ click}})n]$ except with probability ε.

Error-correction is done using a one-way (forward) error correction scheme, for example, by using low-density parity-check codes. The players agree on a linear code which can correct errors in a k-bit string by announcing the syndrome of the string. If each bit of the string is flipped independently with probability $p^h_{\mathrm{B,err}}$, this procedure amounts to sending error-correcting information of at most $1.2h(p^h_{\mathrm{B,err}})k$ bits [40].

We assume that the players have synchronized clocks. In each time slot, Alice sends one light pulse to Bob.

Protocol 2 [*robust 1-2 ROT*$^\ell(C,T,\varepsilon)$].

1. Alice picks $x \in_R \{0,1\}^n$ and $\theta \in_R \{+,\times\}^n$ uniformly at random.
2. Bob picks $\hat{\theta} \in_R \{+,\times\}^n$ uniformly at random.
3. For $i = 1,\ldots,n$: In time slot $t = i$, Alice sends bit x_i encoded in basis θ_i to Bob. In each time slot, Bob measures the incoming light pulse in basis $\hat{\theta}_i$ and records whether he registers a click or not. He obtains some bit string $\hat{x} \in \{0,1\}^m$, with $m \leqslant n$.
4. Bob reports back to Alice in which time slots he recorded a click.
5. Alice restricts herself to the set of $m < n$ positions that Bob did not report as missing. Let this set of bits be S_{remain} with $|S_{\mathrm{remain}}| = m$. If m does not lie in the interval $[(1 - p^h_{\mathrm{B,no\ click}} - \zeta^h_{\mathrm{B,no\ click}})n, (1 - p^h_{\mathrm{B,no\ click}} + \zeta^h_{\mathrm{B,no\ click}})n]$, then Alice aborts the protocol.

Both parties wait time Δt.

6. Alice sends the basis information $\theta = \theta_1,\ldots,\theta_m$ of the remaining positions to Bob.
7. Bob, holding choice bit c, forms the sets $\mathcal{I}_c = \{i \in [m] \mid \theta_i = \hat{\theta}_i\}$ and $\mathcal{I}_{1-c} = \{i \in [m] \mid \theta_i \neq \hat{\theta}_i\}$. He sends $\mathcal{I}_0, \mathcal{I}_1$ to Alice.
8. Alice picks two two-universal hash functions $f_0, f_1 \in_R \mathcal{F}$ and sends f_0, f_1 and the syndromes $\mathrm{syn}(x|_{\mathcal{I}_0})$ and $\mathrm{syn}(x|_{\mathcal{I}_1})$ to Bob. Alice outputs $s_0 = f_0(x|_{\mathcal{I}_0})$ and $s_1 = f_1(x|_{\mathcal{I}_1})$.
9. Bob uses $\mathrm{syn}(x|_{\mathcal{I}_c})$ to correct the errors on his output $\hat{x}|_{\mathcal{I}_c}$. He obtains the corrected bit string x_{cor} and outputs $s'_c = f_c(x_{\mathrm{cor}})$.

In case any of the players sends incorrectly formed messages, the other player aborts.

B. Security analysis

1. Correctness

If both players are honest, Bob reports back enough rounds to Alice. Therefore, in Step 5 the protocol is aborted with probability at most ε. The error-correcting codes are chosen such that Bob can decode except with probability ε. These facts imply that if both parties are honest, the protocol is correct except with probability 2ε.

2. Security against dishonest Alice

Even though in this scenario Bob *does* communicate to Alice, the information about which qubits were erased is independent of Bob's choice bit c as this bit is only used in Step 7. Hence, Alice does not learn anything about his choice bit c. Her input strings can be extracted as in the analysis of Protocol 1 (see [18]).

3. Security against dishonest Bob

In the previous section, we saw that the security analysis for weak string erasure from [25] essentially carries over to 1-2 OT. Similarly, the security analysis for weak string erasure with errors from [33] can be adapted to analyze Protocol 1 .

We use the following probabilities (see [33] for details and some example parameters for concrete setups).

$p^d_{\mathrm{B,no\ click}}$	Dishonest Bob observes no click in his detection apparatus (due to imperfections in Alice's apparatus)
$p^h_{\mathrm{B,no\ click}}$	Honest Bob observes no click in his detection apparatus (due to losses and imperfections of both player's apparatus)
p^1_{sent}	Alice sends exactly 1 photon
$p^h_{\mathrm{B,err}}$	Honest Bob outputs the wrong bit (due to misalignments and noise on the channel)

Theorem 4 (security against dishonest Bob). Fix $0 < \delta < \frac{1}{4}$ and let

$$\varepsilon = 2\exp\left(-\frac{(\delta/4)^2}{32\left(2+\log_2\frac{4}{\delta}\right)^2}m^1\right). \tag{13}$$

Then, for any attack of a dishonest Bob with storage $\mathcal{F}: \mathcal{B}(\mathcal{H}_{\mathrm{in}}) \to \mathcal{B}(\mathcal{H}_{\mathrm{out}})$, Protocol 2 is 2ε secure against a dishonest receiver Bob according to Definition 1, if $m^1 \geqslant 4/\delta$ and the length of the OT strings,

$$\ell \leqslant -\frac{1}{2}\log_2 P^{\mathcal{F}}_{\mathrm{succ}}\left[\left(\frac{1}{4}-\delta\right)m^1\right] - 1.2h\left(p^h_{\mathrm{B,err}}\right)\frac{m}{2} - \log_2\left(\frac{1}{\varepsilon}\right),$$

where $m^1 := (p^1_{\mathrm{sent}} - p^h_{\mathrm{B,no\ click}} + p^d_{\mathrm{B,no\ click}})n$ is the minimal number of single-photon rounds remaining and $m = (1 - p^h_{\mathrm{B,no\ click}})n$ is the total number of rounds remaining.

Proof. As in [33], we adopt the conservative viewpoint that a dishonest Bob does not experience any bit errors or losses on the channel. Furthermore, we assume that a dishonest receiver can detect when multiple photons arrive and extract the encoded bit without knowledge of the encoding basis. These multiphoton rounds will thus not contribute to the uncertainty of a dishonest Bob. He will also not keep any quantum information about these bits.

The main complication in this more practical scenario is that a dishonest Bob might falsely report back rounds as missing in order to decrease the overall fraction of single-photon rounds where he has uncertainty about the encoded bits.

Let $p^h_{\mathrm{B,no\ click}}$ be the probability that honest Bob does not register a click (due to losses in the channel and imperfect apparatus of both players). On the other hand, let $p^d_{\mathrm{B,no\ click}}$

be the probability that a dishonest Bob does not register a click (due to imperfections in Alice's apparatus). We assume that a dishonest Bob will always report a round as missing if he did not register a click (because there is no advantage for him not doing so). We also assumed that Bob gets full information when more than one photon was sent and, hence, he will not report these rounds as missing. We conclude that out of the n rounds, dishonest Bob will report the maximal amount of $(p^h_{\mathrm{B,no\ click}} - p^d_{\mathrm{B,no\ click}})n$ *single-photon* rounds as missing. That means that of the total $m = (1 - p^h_{\mathrm{B,no\ click}})n$ rounds that Alice accepts, at least

$$m^1 := \left[p^1_{\mathrm{sent}} - \left(p^h_{\mathrm{B,no\ click}} - p^d_{\mathrm{B,no\ click}}\right)\right]n \tag{14}$$

are single-photon rounds.

It can be argued, as in [33], that these m^1 single-photon rounds are the (only) ones contributing to the uncertainty in terms of min-entropy about the string X. Formally, we have

$$H^{\varepsilon/2}_{\min}(X_0X_1|\Theta K) \geqslant \frac{m^1}{2} - \frac{m^1\delta}{2}, \tag{15}$$

where X_0, X_1 are the substrings of X formed according to the index sets $\mathcal{I}_0$ and $\mathcal{I}_1$, $0 < \delta < \frac{1}{4}$ is fixed, and the error parameter ε is

$$\varepsilon = 2\exp\left(-\frac{(\delta/4)^2}{32\left(2+\log_2\frac{4}{\delta}\right)^2}m^1\right). \tag{16}$$

Proceeding as in the proof of Protocol 1 (with m^1 instead of n), classical min-entropy splitting (Lemma 1) then ensures that there exists a binary random variable $D \in \{0,1\}$ such that

$$H^{\varepsilon/2}_{\min}(X_{\overline{D}}|D\Theta K) \geqslant \frac{m^1}{4} - \frac{m^1\delta}{4} - 1.$$

Then we use Lemma 4 to get

$$\begin{aligned} &H^{\varepsilon}_{\min}(X_{\overline{D}}|D\Theta K Q_{\mathrm{out}}) \\ &\quad\geqslant -\log_2 P^{\mathcal{F}}_{\mathrm{succ}}\left(\frac{m^1}{4} - \frac{m^1\delta}{4} - 1 - \log_2\frac{2}{\varepsilon}\right) \\ &\quad\geqslant -\log_2 P^{\mathcal{F}}_{\mathrm{succ}}\left[\left(\frac{1}{4}-\delta\right)m^1\right], \end{aligned}$$

where the last step follows in the same way as in [25] from the monotonicity of the success probability $P^{\mathcal{F}}_{\mathrm{succ}}(k) \leqslant P^{\mathcal{F}}_{\mathrm{succ}}(k')$ for $k \geqslant k'$ and the fact that $\log_2\frac{2}{\varepsilon} \leqslant \frac{\delta}{2}m^1 \leqslant \frac{3\delta}{4}m^1 - 1$.

Additionally, the dishonest receiver learns the two syndromes $\mathrm{syn}(X_0)$,$\mathrm{syn}(X_1)$. As X_0 and X_1 are not necessarily independent from dishonest Bob's point of view, the two syndromes reduce Bob's min-entropy about $X_{\overline{D}}$ by at most $1.2h(p^h_{\mathrm{err}})m$ bits of information.

It follows from the chain rule for smooth min-entropy (5) that

$$\begin{aligned} &H^{\varepsilon}_{\min}(X_{\overline{D}}|D\Theta S_D \mathrm{syn}(X_0)\mathrm{syn}(X_1)K Q_{\mathrm{out}}) \\ &\quad\geqslant H^{\varepsilon}_{\min}(X_{\overline{D}}|D\Theta K Q_{\mathrm{out}}) - \ell - 1.2h\left(p^h_{\mathrm{err}}\right)m \\ &\quad\geqslant -\log_2 P^{\mathcal{F}}_{\mathrm{succ}}\left[\left(\tfrac{1}{4}-\delta\right)m^1\right] - \ell - 1.2h\left(p^h_{\mathrm{err}}\right)m. \end{aligned}$$

The privacy amplification Theorem 2 yields

$$\begin{aligned} &d[F_{\overline{D}}(X_{\overline{D}}) \mid D\Theta F_D S_D K Q_{\mathrm{out}}] \\ &\quad\leqslant 2^{-\frac{1}{2}\{-\log_2 P^{\mathcal{F}}_{\mathrm{succ}}[(\frac{1}{4}-\delta)m^1]-2\ell-1.2h(p^h_{\mathrm{err}})m\}} + \varepsilon, \end{aligned} \tag{17}$$

which is smaller than 2ε as long as

$$\begin{aligned} &-\frac{1}{2}\log_2 P^{\mathcal{F}}_{\mathrm{succ}}\left[\left(\frac{1}{4}-\delta\right)m^1\right] - \ell - 1.2h\left(p^h_{\mathrm{err}}\right)\frac{m}{2} \\ &\quad\geqslant \log_2\left(\frac{1}{\varepsilon}\right), \end{aligned}$$

from which our claim follows. ■

In the same way as Corollary 1, we can derive the following.

Corollary 2. Let Bob's storage be given by $\mathcal{F} = \mathcal{N}^{\otimes\nu n}$ for a storage rate $\nu > 0$, $\mathcal{N}$ satisfying the strong converse property (8) and having capacity $C_{\mathcal{N}}$ bounded by

$$C_{\mathcal{N}}\nu < \left(\tfrac{1}{4}-\delta\right)\left(p^1_{\mathrm{sent}} - p^h_{\mathrm{B,no\ click}} + p^d_{\mathrm{B,no\ click}}\right). \tag{18}$$

Then Protocol 2 is 2ε secure against a dishonest receiver Bob according to Definition 1 with the following parameters: Let $\delta \in]0, \frac{1}{4} - C_{\mathcal{N}}\nu[$ and $m^1 \geqslant 4/\delta$. Then the length ℓ of the OT strings is bounded by

$$\begin{aligned} \ell \leqslant\ &\frac{1}{2}\nu\gamma^{\mathcal{N}}\left(\frac{R}{\nu}\right)n - 1.2h\left(p^h_{\mathrm{B,err}}\right)\left(1-p^h_{\mathrm{B,err}}\right)\frac{m}{2} \\ &- \log_2\left(\frac{1}{\varepsilon}\right), \end{aligned} \tag{19}$$

where $\gamma^{\mathcal{N}}$ is the strong converse parameter of $\mathcal{N}$ [see (8)] and $m = (1 - p^h_{\mathrm{B,no\ click}})n$ (the number of remaining rounds), $m^1 = (p^1_{\mathrm{sent}} - p^h_{\mathrm{B,no\ click}} + p^d_{\mathrm{B,no\ click}})n$ (the minimal number of single-photon rounds), $R = (\frac{1}{4} - \delta)\frac{m^1}{n}$ (the rate at which dishonest Bob has to send information through storage), for sufficiently large n. The error has the form

$$\begin{aligned} \varepsilon(\delta) \leqslant\ &2\exp\left(-\frac{\delta^2}{512(4+\log_2\frac{1}{\delta})^2}\left(p^1_{\mathrm{sent}} - p^h_{\mathrm{B,no\ click}}\right.\right. \\ &\left.\left. + p^d_{\mathrm{B,no\ click}}\right)n\right). \end{aligned} \tag{20}$$

VI. PASSWORD-BASED IDENTIFICATION

In this section, we show how the techniques for proving security in the noisy-quantum-storage model also apply to the protocol from [19,22] achieving secure password-based identification in the bounded-quantum-storage model. This answers an open question posed in [25].

A. Task and protocol

A user Alice wants to identify herself to a server Bob by means of a personal identification number. This task can be achieved by securely evaluating the equality function on the player's inputs: Both Alice and Bob input passwords w_A and w_B from a set of possible passwords $\mathcal{W}$ into the protocol and Bob learns as output whether $w_A = w_B$ or not.

The protocol proposed in [19] is secure against an unbounded user Alice and a quantum-memory bounded server Bob in the sense that it is guaranteed that if a dishonest player starts with quantum side information which is uncorrelated with the honest player's password w, this dishonest player is restricted to guess a possible w' and find out whether $w = w'$ or not while not learning anything more than this mere bit

of information about the honest user's password w. Formally, security is defined as follows.

Definition 2. We call an identification protocol between user Alice and server Bob *secure for the user Alice with error* ε against (dishonest) server Bob B' if the following is satisfied: Whenever the initial state of B' is independent of W, the joint state $\rho_{WE_{\mathsf{B}'}}$ after the execution of the protocol is such that there exists a random variable W' that is independent of W and such that

$$\rho_{WW'E_{\mathsf{B}'}|W'\neq W} \approx_\varepsilon \rho_{W\leftrightarrow W'\leftrightarrow E_{\mathsf{B}'}|W'\neq W}.$$

The Markov-chain notation is explained in (2).

We consider the same protocol for password-based secure identification from [19], in the more practical form presented in [39], where the receiving party measures in a random basis. Let $\mathfrak{c}:\mathcal{W}\to\{+,\times\}^n$ be the encoding function of a binary code of length n with $m=|\mathcal{W}|$ code words and minimal distance d. $\mathfrak{c}$ can be chosen such that n is linear in $\log_2(m)$ or larger, and d is linear in n. Furthermore, let $\mathcal{F}$ and $\mathcal{G}$ be strongly two-universal classes of hash functions from $\{0,1\}^n$ to $\{0,1\}^\ell$ and from $\mathcal{W}$ to $\{0,1\}^\ell$, respectively, for some parameter ℓ.

Protocol 3 [19,39] [*Password-based identification Q-ID (w)*].

1. Alice picks $x\in_R\{0,1\}^n$ and $\theta\in_R\{+,\times\}^n$. At time $t=0$, she sends $|x_1\rangle_{\theta_1},\ldots,|x_n\rangle_{\theta_n}$ to Bob.
2. Bob picks $\hat{\theta}\in_R\{+,\times\}^n$ at random and measures the ith qubit in basis $\hat{\theta}_i$. He obtains outcome $\hat{x}\in\{0,1\}^n$.

Both parties wait time Δt.

3. Bob computes a string $\kappa\in\{+,\times\}^n$ such that $\hat{\theta}=\mathfrak{c}(w)\oplus\kappa$ (interpreting $+$ as 0 and $\times$ as 1 so that $\oplus$ makes sense). He sends κ to Alice and they define the shifted code $\mathfrak{c}'(w):=\mathfrak{c}(w)\oplus\kappa$.
4. Alice sends θ and $f\in_R\mathcal{F}$ to Bob. Both compute $\mathcal{I}_w:=\{i:\theta_i=\mathfrak{c}'(w)_i\}$.
5. Bob sends $g\in_R\mathcal{G}$ to Alice.
6. Alice sends $z:=f(x|_{\mathcal{I}_w})\oplus g(w)$ to Bob.
7. Bob accepts if and only if $z=f(\hat{x}|_{\mathcal{I}_w})\oplus g(w)$.

We note that this protocol can also be (nontrivially) extended to additionally withstand man-in-the-middle attacks [19,22].

B. Security analysis

Theorem 5 (security against dishonest Bob). Fix $0<\delta<\frac{1}{4}$ and let $\sigma(\delta)$ be defined as in (6). Then for any attack of a dishonest Bob with storage channel $\mathcal{F}:\mathcal{B}(\mathcal{H}_{\text{in}})\to\mathcal{B}(\mathcal{H}_{\text{out}})$, Protocol 3 is an ε-secure identification protocol against a dishonest receiver Bob according to Definition 2 if $d\geqslant\frac{4+4\log_2(m)}{\delta}$ and

$$\varepsilon=2^{-\frac{1}{2}\{-\log_2 P_{\text{succ}}^{\mathcal{F}}[(\frac{1}{4}-\delta)d]-\ell\}}+2^{-[\sigma(\delta/4)d-\log_2(m)-3]}.$$

To understand what the result on ε means, note that using a family of asymptotically good codes, we can assume that d grows linearly with the main security parameter n, while still allowing m (the number of passwords) to be exponential in n. So we may choose the parameters such that $\frac{d}{n}$, $\frac{\log_2(m)}{n}$, and $\frac{\ell}{n}$ are all constants. The preceding result now says that ε is exponentially small as a function of n if these constants and the noisy channel $\mathcal{F}$ fulfill that for some $0<\delta<\frac{1}{4}$, $\frac{-\log_2 P_{\text{succ}}^{\mathcal{F}}[(\frac{1}{4}-\delta)d]}{n}-\frac{\ell}{n}>0$ and $\sigma(\delta/4)\frac{d}{n}-\frac{\log_2(m)}{n}>0$. See Theorem 7 for a choice of parameters that also takes server security into account.

Proof. We use upper-case letters W, X, Θ, K, F, G, and Z for the random variables that describe the respective values w, x, θ, etc., in an execution of *Q-ID*.

Recall that in the noisy-storage model, we denote by K the classical outcome of Bob's encoding attack and Q_{in} denotes Bob's quantum state right before the waiting time.

We write $X_j=X|_{\mathcal{I}_j}$ for any j. Note that dishonest Bob starts without any knowledge about honest Alice's password W and hence, W is independent of X, Θ, K, F, G, and Q_{in}.

For $1\leqslant i\neq j\leqslant m$, fix the value of X, and correspondingly of X_i and X_j, at the positions where $\mathfrak{c}(i)$ and $\mathfrak{c}(j)$ coincide, and focus on the remaining (at least) d positions. The uncertainty relation (Theorem 1) implies that the restriction of X to these positions has $(\frac{1}{2}-\delta/2)\,d$ bits of ε'-smooth min-entropy given Θ, where $\varepsilon'\leqslant 2^{-\sigma(\delta/4)d}$. Since every bit in the restricted X appears in one of X_i and X_j, the pair X_i,X_j also has $(\frac{1}{2}-\delta/2)\,d$ bits of ε'-smooth min-entropy given Θ and K. The entropy splitting Lemma 2 implies that there exists W' (called V in Lemma 2 such that if $W\neq W'$ then X_W has $(\frac{1}{4}-\delta/4)\,d-\log_2(m)-1$ bits of $2m\varepsilon'$-smooth min-entropy given W and W' (and Θ,K); that is,

$$H_{\min}^{2m\varepsilon'}(X_W|WW'\Theta K,W\neq W')\geqslant\left(\frac{1}{4}-\delta/4\right)d-\log_2(m)-1.$$

By Lemma 4, it follows that for $Q_{\text{out}}=\mathcal{F}(Q_{\text{in}})$, we get

$$\begin{aligned}H_{\min}^{(2m+1)\varepsilon'}&(X_W|WW'\Theta KQ_{\text{out}},W\neq W')\\&\geqslant-\log_2 P_{\text{succ}}^{\mathcal{F}}\left[\left(\tfrac{1}{4}-\delta/4\right)d-\log_2(m)-1-\log_2(1/\varepsilon')\right]\\&\geqslant-\log_2 P_{\text{succ}}^{\mathcal{F}}\left[\left(\tfrac{1}{4}-\delta\right)d\right],\end{aligned}$$

where the last inequality follows as in the OT case (proof of Theorem 3) from $\log_2(1/\varepsilon')\leqslant\frac{\delta}{2}d\leqslant\frac{3\delta}{4}d-\log_2(m)-1$ and the assumption on d.

Privacy amplification then guarantees that $F(X_W)$ is ε'' close to random and independent of F, W, W', Θ, K, and Q_{out}, conditioned on $W\neq W'$, where $\varepsilon''=\frac{1}{2}\cdot 2^{-\frac{1}{2}\{-\log_2 P_{\text{succ}}^{\mathcal{F}}[(\frac{1}{4}-\delta)d]-\ell\}}+(2m+1)\varepsilon'$. It follows that $Z=F(X_W)\oplus G(W)$ is ε'' close to random and independent of F, G, W, W', Θ, K, and Q_{out}, conditioned on $W\neq W'$. The rest of the argument is the same as in the original proof [22].

Formally, we want to upper bound the trace distance between $\rho_{WW'E_{\mathsf{B}'}|W'\neq W}$ and $\rho_{W\leftrightarrow W'\leftrightarrow E_{\mathsf{B}'}|W'\neq W}$. Since the output state $E_{\mathsf{B}'}$ is, without loss of generality, obtained by applying some unitary transform to the set of registers $(Z,F,G,W',\Theta,K,Q_{\text{out}})$, the preceding distance is equal to the distance between $\rho_{WW'(Z,F,G,\Theta,K,Q_{\text{out}})|W'\neq W}$ and $\rho_{W\leftrightarrow W'\leftrightarrow(Z,F,G,\Theta,K,Q_{\text{out}})|W'\neq W}$. We then get

$$\begin{aligned}&\rho_{WW'(Z,F,G,\Theta,Q_{\text{out}})|W'\neq W}\\&\quad\approx_{\varepsilon''}\frac{1}{2^\ell}\mathbb{1}_Z\otimes\rho_{WW'(F,G,\Theta,K,Q_{\text{out}})|W'\neq W}\\&\quad=\frac{1}{2^\ell}\mathbb{1}_Z\otimes\rho_{W\leftrightarrow W'\leftrightarrow(F,G,\Theta,K,Q_{\text{out}})|W'\neq W}\\&\quad\approx_{\varepsilon''}\rho_{W\leftrightarrow W'\leftrightarrow(Z,F,G,\Theta,K,Q_{\text{out}})|W'\neq W},\end{aligned}$$

where approximations follow from privacy amplification and the exact equality comes from the independency of W, which, when conditioned on $W' \neq W$, translates to independency given W'. The claim follows with $\varepsilon = 2\varepsilon''$ and the (crude) estimation $2(2m+1) \leqslant 8m$. ■

Theorem 6 (*security against dishonest Alice* [19]). If $H_{\min}(W) \geqslant 1$, then *Q-ID* is secure against dishonest user Alice with security error $\varepsilon = m^2/2^{\ell}$.

We call an identification scheme ε *secure against impersonation attacks* if the protocol is secure for both players with error at most ε in both cases. The following holds.

Theorem 7. If $H_{\min}(W) \geqslant 1$, then the identification scheme *Q-ID* (with suitable choice of parameters) is ε secure against impersonation attacks for any unbounded user Alice and for any server Bob with noisy storage of the form $\mathcal{F} = \mathcal{N}^{\otimes \nu n}$ with $\nu > 0$, where $\mathcal{N}$ satisfies the strong-converse property (8), and

$$C_{\mathcal{N}}\nu < \tfrac{1}{4},$$

and the security error is

$$\varepsilon = 2^{-\frac{1}{3}[\gamma^{\mathcal{N}}(\frac{1/4-\delta}{\nu})\nu\mu n - 6\log_2(m) - 1]} + 2^{-[\sigma(\delta/4)\mu n - \log_2(m) - 4]}$$

for an arbitrary $0 < \delta < \frac{1}{4}$, and where $\mu = h^{-1}[1 - \log_2(m)/n]$, and h^{-1} is the inverse function of the binary entropy function: $h(p) := -p\log_2(p) - (1-p)\log_2(1-p)$ restricted to $0 < p \leqslant \frac{1}{2}$. In particular, if $\log_2(m)$ is sublinear in n, then ε is negligible in n as long as $\gamma^{\mathcal{N}}(\frac{1/4-\delta}{\nu}) > 0$.

Proof. First of all, we have that $-\log_2 P_{\text{succ}}^{\mathcal{N}^{\otimes \nu n}}[(1/4 - \delta)d] \geqslant \gamma^{\mathcal{N}}(\frac{1/4-\delta}{\nu})\nu d$.

We choose $\ell = \frac{1}{3}\gamma^{\mathcal{N}}(\frac{1/4-\delta}{\nu})\nu d$. Then security against dishonest Bob holds except with an error $\varepsilon = 2^{-\frac{1}{3}\gamma^{\mathcal{N}}(\frac{1/4-\delta}{\nu})\nu d} + 2^{-[\sigma(\delta/4)d - \log_2(m) - 3]}$, and security against dishonest Alice holds except with an error $m^2/2^{\ell} = 2^{-\frac{1}{3}[\gamma^{\mathcal{N}}(\frac{1/4-\delta}{\nu})\nu d - 6\log_2(m)]}$. Using a code $\mathfrak{c}$, which asymptotically meets the Gilbert-Varshamov bound [41], d may be chosen arbitrarily close to $nh^{-1}[1 - \log_2(m)/n]$. In particular, we can ensure that d does not differ from this value by more than 1. Inserting $d = \mu n - 1$ in the expressions and using that $\gamma^{\mathcal{N}}(\frac{1/4-\delta}{\nu})\nu \leqslant 1$ yields the theorem. ■

VII. CONCLUSION

We have used the technical tool from [25] to prove the security of the original protocols for oblivious transfer and secure identification against adversaries performing general noisy-quantum-storage attacks. The main advantage of our protocols is the straightforward constant-round classical postprocessing which makes them easier to implement in the laboratory compared to the protocols from [25,33]. The security analysis given here yields simpler expressions for the security error. For a given number of pulses and a low security threshold, our approach generally yields higher OT rates. Additionally, we show the security of a password-based identification protocol against general noisy-quantum-storage attacks.

This work leads to the question whether a similar result as in QKD holds, namely, that general storage attacks are no better than coherent (or individual) storage attacks for which the best encoding attack is known [24].

ACKNOWLEDGMENTS

This work is supported by EU fifth framework Project No. QAP IST 015848 and a Dutch NWO VICI Project 2004-2009.

[1] R. L. Rivest, A. Shamir, and L. Adleman, Commun. ACM **21**, 120 (1978).
[2] C. H. Bennett and G. Brassard, in *IEEE International Conference on Computers, Systems, and Signal Processing* (1984), p. 175.
[3] D. Mayers, in *Advances in Cryptology—CRYPTO '95*, Lecture Notes in Computer Science (Springer, Berlin, 1995), Vol. 963, p. 124.
[4] A. C.-C. Yao, in *Proceedings of the 27th Annual ACM Symposium on the Theory of Computing (STOC)* (ACM, Las Vegas, NV, USA, 1995), p. 67.
[5] P. W. Shor and J. Preskill, Phys. Rev. Lett. **85**, 441 (2000).
[6] SmartQuantum [http://www.smartquantum.com].
[7] idQuantique [http://www.idquantique.com].
[8] MagicQ [http://www.magiqtech.com/].
[9] D. Mayers, Phys. Rev. Lett. **78**, 3414 (1997).
[10] H.-K. Lo and H. F. Chau, Phys. Rev. Lett. **78**, 3410 (1997).
[11] H.-K. Lo, Phys. Rev. A **56**, 1154 (1997).
[12] I. B. Damgård, S. Fehr, L. Salvail, and C. Schaffner, in *46th Annual IEEE Symposium on Foundations of Computer Science (FOCS)* (IEEE Computer Society, Pittsburgh, PA, USA, 2005), p. 449.
[13] B. Julsgaard, J. Sherson, J. Cirac, J. Fiurasek, and E. Polzik, Nature (London) **432**, 482 (2004).
[14] T. Chaneliere, D. Matsukevich, S. Jenkins, S. Lan, T. Kennedy, and A. Kuzmich, Nature (London) **438**, 833 (2005).
[15] M. Eisaman, A. Andre, F. Massou, M. Fleischhauer, A. Zibrov, and M. Lukin, Nature (London) **438**, 837 (2005).
[16] K. S. Choi, H. Deng, J. Laurat, and H. J. Kimble, Nature (London) **452**, 67 (2008).
[17] J. Appel, E. Figueroa, D. Korystov, M. Lobino, and A. I. Lvovsky, Phys. Rev. Lett. **100**, 093602 (2008).
[18] I. B. Damgård, S. Fehr, R. Renner, L. Salvail, and C. Schaffner, in *Advances in Cryptology—CRYPTO '07*, Lecture Notes in Computer Science (Springer, Berlin, 2007), Vol. 4622, p. 360.
[19] I. B. Damgård, S. Fehr, L. Salvail, and C. Schaffner, in *Advances in Cryptology—CRYPTO '07*, Lecture Notes in Computer Science (Springer, Berlin, 2007), Vol. 4622, p. 342.
[20] C. Schaffner, Ph.D. thesis, University of Aarhus, 2007.
[21] I. B. Damgård, S. Fehr, L. Salvail, and C. Schaffner, SIAM J. Comput. **37**, 1865 (2008).
[22] I. B. Damgård, S. Fehr, L. Salvail, and C. Schaffner, Theor. Computer Sci. (to be published), e-print arXiv:0708.2557v3.
[23] S. Wehner, C. Schaffner, and B. M. Terhal, Phys. Rev. Lett. **100**, 220502 (2008).
[24] C. Schaffner, B. M. Terhal, and S. Wehner, Quantum Inf. Comput. **9**, 963 (2009).

[25] R. König, S. Wehner, and J. Wullschleger, e-print arXiv:0906.1030.
[26] G. Savvides, Ph.D. thesis, School of Computer Science, McGill University, Montréal, Canada, 2007.
[27] M. Naor, R. Ostrovsky, R. Venkatesan, and M. Yung, J. Cryptol. **11**, 87 (1998).
[28] Y. Z. Ding, D. Harnik, A. Rosen, and R. Shaltiel, in *Theory of Cryptography Conference (TCC)*, Lecture Notes in Computer Science (Springer, Berlin, 2004), Vol. 2951, p. 446.
[29] R. König and R. Renner, e-print arXiv:0712.4291.
[30] R. Renner, Ph.D. thesis, ETH Zürich, Switzerland, 2005.
[31] J. Wullschleger, in *Advances in Cryptology—EUROCRYPT '07*, Lecture Notes in Computer Science (Springer, Berlin, 2007), Vol. 4515.
[32] J. L. Carter and M. N. Wegman, J. Comput. Syst. Sci. **18**, 143 (1979).
[33] S. Wehner, M. Curty, C. Schaffner, and H.-K. Lo, Phys. Rev. A **81**, 052336 (2010).
[34] R. König and S. Wehner, Phys. Rev. Lett. **103**, 070504 (2009).
[35] C. King, IEEE Trans. Inf. Theory **49**, 221 (2003).
[36] S. Fehr and C. Schaffner, in *Theory of Cryptography Conference (TCC)*, Lecture Notes in Computer Science (Springer, Berlin, 2009), Vol. 5444, p. 350.
[37] S. Wehner and J. Wullschleger, in *Automata, Languages and Programming, 35th International Colloquium, ICALP 2008*, Lecture Notes in Computer Science (Springer, Berlin, 2008), Vol. 5126, p. 604.
[38] C. H. Bennett, G. Brassard, C. Crépeau, and M.-H. Skubiszewska, in *Advances in Cryptology—CRYPTO '91*, Lecture Notes in Computer Science (Springer, Berlin, 1991), Vol. 576, p. 351.
[39] I. B. Damgård, S. Fehr, C. Lunemann, L. Salvail, and C. Schaffner, in *Advances in Cryptology—CRYPTO '09*, Lecture Notes in Computer Science (Springer, Berlin, 2009), Vol. 5677, p. 408.
[40] D. Elkouss, A. Leverrier, R. Alleaume, J. J. Boutros, *Information Theory, 2009. ISIT 2009. IEEE International Symposium on Information Theory, Seoul, 28 June–3 July 2009* (Telecom ParisTech, France, 2009), pp. 1879–1883.
[41] C. Thommesen, IEEE Trans. Inf. Theory **29**, 850 (1983).