

Simple Protocols for Oblivious Transfer and Secure Identification in the Noisy-Quantum-Storage Model

Christian Schaffner¹

¹ *Centrum Wiskunde & Informatica (CWI) Amsterdam, The Netherlands*

March 31, 2010

Abstract

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 [KWW09]. We argue that a technical tool from [KWW09] suffices to prove security of the known protocols. Whereas the more involved protocol for oblivious transfer from [KWW09] 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, the first proof of security of a direct protocol for password-based identification against general noisy-quantum-storage attacks is given.

1 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 to check 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 that they obtain the correct result but no additional information about their inputs is revealed. An interesting example are 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 (ATM) 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 [RSA78]). 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 [BB84] which was proven unconditionally secure [May95, Yao95, SP00]. 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 [Sma, idQ, Mag].

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 90s 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 [May97, LC97, Lo97]. 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 new realistic assumption for quantum protocols under which provably secure two-party computation becomes possible [DFSS05]. 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 nor the classical memory size are assumed. Storing quantum information requires to keep 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 [JSC⁺04, CMJ⁺05, EAM⁺05, CDLK08, AFK⁺08]. 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, 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.

1.1 Bounded- versus 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 last

years [DFSS05, DFR⁺07, DFSS07, Sch07, DFSS08, DFSS10], 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 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 in the order of milliseconds is required [JSC⁺04].

First results in this *noisy-quantum-storage model* have been established in joint work with Terhal and Wehner [WST08, STW09]. 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 [DFR⁺07, DFSS10].

The most general storage attacks were first mentioned in [Sch07], but addressed only recently by König, Wehner and Wullschleger [KWW09]. 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 [KWW09] 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, [KWW09] 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 [Sav07], for which the standard classical protocol requires a lot of communication rounds [NOVY98]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 [KR07]. 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.

¹A detailed description of the model of [KWW09] will be given in Section 3, see also Figure 1.

²A constant-round variant of interactive hashing has been proposed in [DHRS04]. However, it is unclear how the weaker security guarantees affect the security proof in [KWW09]. The use of η -almost t -wise independent permutations might render this variant “prohibitively complicated to implement in practice” [Sav07].

	Secure 1-2 OT	Canonical Protocol	Secure Identification
[WST08, STW09]	individual attacks	Yes	individual attacks
[KWW09]	general attacks	No	No
This work	general attacks	Yes	general attacks

Table 1: Summary of previous results in the noisy-quantum-storage model and the results presented here.

1.2 Our Results and Outline of the Paper

The main contribution of this paper is the insight that the new technical tool derived in [KWW09] already suffices to prove secure the original protocols from the bounded-quantum-storage model for bit commitment, oblivious transfer [DFR⁺07] and password-based identification [DFSS07, DFSS10]. These original protocols have the advantage that the classical post-processing is extremely simple. No communication-intensive protocols such as interactive hashing are needed.

Comparing the protocol for oblivious transfer from [KWW09] with our protocol, it turns out that the highly interactive protocol [KWW09] can in theory be shown secure for less noisy quantum-storage channels if infinitely many pulses are available, i.e., security holds against a larger class of adversarial receivers. However, the original protocols with the simpler analysis presented here outperform the ones from [KWW09] 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 for the first time the security against general noisy-storage attacks of a direct protocol for password-based identification, answering an open question posed in [KWW09].

From a theoretical point of view, our insight shows that despite the generality of the noisy-quantum-storage model, having the right tools from [DFR⁺07, KWW09] at hand, the protocols and security proofs do not need to be much more complicated than in the conceptually simpler bounded-quantum-storage model.

1.3 Outline of the Paper

In Section 2, we define concepts and notation and elaborate on the essential tool of min-entropy splitting in Section 2.3. We present the noisy-quantum-storage and the key ingredient from [KWW09] in Section 3. Sections 4, 5 and 6 contain the security analyses for oblivious transfer and password-based identification.

2 Preliminaries

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

2.1 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 $x = x_1, \dots, x_n$ restricted to the bits indexed by the set $\mathcal{I} \subseteq \{1, \dots, n\}$. For a binary random variable C , we denote by \overline{C} the bit different from C .

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

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

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 .

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 as³

$$\rho_{X \leftrightarrow Y \leftrightarrow E} := \sum_{x,y} P_{XY}(x,y) |x\rangle\langle x| \otimes |y\rangle\langle y| \otimes \rho_E^y. \quad (1)$$

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

Non-uniformity 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 *non-uniformity* of X given $\rho_E = \sum_x P_X(x) \rho_E^x$ defined as

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

Intuitively, $d(X|E) \leq \varepsilon$ means that 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 non-uniformity which follows from its definition is that it does not change given independent information. Formally,

$$d(X|E, D) = d(X|E) \quad (3)$$

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

2.2 Entropic Quantities

Throughout this paper we use a number of entropic quantities. The *binary-entropy* function is defined as $h(p) := -p \log p - (1-p) \log(1-p)$, where \log denotes the logarithm to base 2 throughout this paper.

³The 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.

2.2.1 (Conditional) Smooth Min-Entropy

We are concerned with the situation where an attacker holds quantum information in register E about a classical variable X , described by a classical-quantum state (cq-state) of the form

$$\rho_{XE} = \sum_x P_X(x) |x\rangle\langle x| \otimes \rho_E^x.$$

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 ,

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

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

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 $H_{\min}(X\mathcal{E}|Y) := -\log(p_{\text{guess}}(X\mathcal{E}|Y))$ where⁴

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

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 $P[\mathcal{E}] \geq 1 - \varepsilon$.

Obviously, the unconditional versions of smooth and non-smooth 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 [Ren05, KWW09] for the formal definitions.

In this paper, we will use the fact that smooth min-entropy obeys the chain rule [Ren05, Theorem 3.2.12], i.e. for a cq-state ρ_{XYE} , we have

$$H_{\min}^\varepsilon(X|YE) \geq H_{\min}^\varepsilon(X|E) - \log |\mathcal{Y}|, \tag{4}$$

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

2.3 Min-Entropy Splitting

The key ingredients for the security proofs of both the 1-2 OT and the secure identification schemes in [DFR⁺07, DFSS07] 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.

⁴ $p_{\text{guess}}(X\mathcal{E}|Y)$ can be understood as the optimal probability in guessing X and have \mathcal{E} occur, when given Y .

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, e.g. 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 [Wul07] and was later developed further in the context of randomness extraction [KR07], 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 [DFR⁺07].

Lemma 2.1 (Min-Entropy-Splitting Lemma [DFR⁺07]) *Let $\varepsilon \geq 0$, and let X_0, X_1 and Z be random variables with $H_{\min}^\varepsilon(X_0X_1|Z) \geq \alpha$. Then, there exists a random variable $D \in \{0, 1\}$ such that*

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

Proof. Let \mathcal{E} be an event such that $P[\mathcal{E}] \geq 1 - \varepsilon$ and

$$\sum_z P_Z(z) \cdot \max_{x_0, x_1} P_{X_0X_1\mathcal{E}|Z}(x_0, x_1|z) \leq 2^{-\alpha}. \quad (5)$$

By assumption, such an events exist.⁵ For a given z , we define D to be 0 if and only if $P_{X_0|Z}(X_0|z) < 2^{-\alpha/2}$. Then,

$$\begin{aligned} \sum_z P_Z(z) \cdot \max_{x_0} P_{X_0D\mathcal{E}|Z}(x_0, 0|z) &\leq \sum_z P_Z(z) \cdot \max_{x_0} P_{X_0D|Z}(x_0, 0|z) \\ &= \sum_z P_Z(z) \cdot \max_{x_0} P_{X_0|Z}(x_0|z) P_{D|X_0Z}(0|x_0, z) < 2^{-\alpha/2}, \end{aligned} \quad (6)$$

because either $P_{X_0|Z}(x_0|z) < 2^{-\alpha/2}$ or $P_{D|X_0Z}(0|x_0, z) = 0$ by definition of D . On the other hand, we have

$$\begin{aligned} \sum_z P_Z(z) \cdot \max_{x_1} P_{X_1D\mathcal{E}|Z}(x_1, 1|z) &= \sum_z P_Z(z) \cdot \max_{x_1} \sum_{x_0} P_{X_0X_1D\mathcal{E}|Z}(x_0, x_1, 1|z) \\ &\leq 2^{\alpha/2} \sum_z P_Z(z) \cdot \max_{x_0, x_1} P_{X_0X_1\mathcal{E}|Z}(x_0, x_1|z) \leq 2^{-\alpha/2}, \end{aligned} \quad (7)$$

where the last inequality follows from the assumption (5) and the first is a consequence of the fact that the number of non-zero summands (in the sum over x_0) cannot be larger than $2^{\alpha/2}$, because for any x_0 with $P_{X_0X_1D|Z}(x_0, x_1, 1|z) > 0$, it also holds (by the definition of D) that $P_{X_0|Z}(x_0|z) \geq 2^{-\alpha/2}$ and the sum over all those x_0 would exceed 1 if there were more than $2^{\alpha/2}$ summands.

⁵In case $\varepsilon = 0$, i.e., α lower bounds the ordinary (rather than the smooth) min-entropy, the \mathcal{E} is the events “that always occurs” and can be ignored from the rest of the analysis.

Combining (6) and (7), we conclude that

$$p_{\text{guess}}(X_D \mathcal{E} | DZ) = \sum_d \sum_z P_Z(z) \max_x P_{X_D D \mathcal{E} | Z}(x_d, d | z) \leq 2 \cdot 2^{-\alpha/2}.$$

The claim now follows by definition of H_{\min}^ε . \square

In order to prove the security of the identification scheme (see Section 6), a more refined version of the min-entropy splitting lemma was derived in [DFSS10]. We reproduce it here for convenience.

Lemma 2.2 (Entropy-Splitting Lemma [DFSS10]) *Let $\varepsilon \geq 0$. Let X_1, \dots, X_m and Z be random variables such that $H_{\min}^\varepsilon(X_i X_j | Z) \geq \alpha$ for all $i \neq j$. Then there exists a random variable V over $\{1, \dots, m\}$ such that for any independent random variable W over $\{1, \dots, m\}$ with $H_{\min}(W) \geq 1$,*

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

Proof. For any pair $i \neq j$ let \mathcal{E}_{ij} be an event such that $P[\mathcal{E}_{ij}] \geq 1 - \varepsilon$ and

$$\sum_z P_Z(z) \cdot \max_{x_i, x_j} P_{X_i X_j \mathcal{E}_{ij} | Z}(x_i, x_j | z) \leq 2^{-\alpha} \quad (8)$$

for all $x_i \in \mathcal{X}_i$, $x_j \in \mathcal{X}_j$ and $z \in \mathcal{Z}$. By assumption, such events exist.⁶ For any $j = 1, \dots, m-1$ define

$$L_j = \{(x_1, \dots, x_m, z) : P_{X_1 | Z}(x_1 | z), \dots, P_{X_{j-1} | Z}(x_{j-1} | z) < 2^{-\alpha/2} \wedge P_{X_j | Z}(x_j | z) \geq 2^{-\alpha/2}\}$$

Informally, L_j consists of the tuples (x_1, \dots, x_m, z) , where x_j has “large” probability given z whereas all previous entries have small probabilities. We define V as follows. We let V be the index $j \in \{1, \dots, m-1\}$ such that $(X_1, \dots, X_m, Z) \in L_j$, and in case there is no such j we let V be m . Note that if there does exist such an j then it is unique.

We need to show that this V satisfies the claim. Fix $j \in \{1, \dots, m\}$. Clearly, for $i < j$,

$$\begin{aligned} \sum_z P_Z(z) \cdot \max_{x_i} P_{X_i V \mathcal{E}_{ij} | Z}(x_i, j | z) &\leq \sum_z P_Z(z) \cdot \max_{x_i} P_{X_i V | Z}(x_i, j | z) \\ &= \sum_z P_Z(z) \cdot \max_{x_i} P_{X_i | Z}(x_i | z) P_{V | X_i Z}(j | x_i, z) < 2^{-\alpha/2}. \end{aligned} \quad (9)$$

Indeed, either $P_{X_i | Z}(x_i | z) < 2^{-\alpha/2}$ or $P_{V | X_i Z}(j | x_i, z) = 0$ by definition of V . Consider now $i > j$. Note that

$$\begin{aligned} \sum_z P_Z(z) \cdot \max_{x_i} P_{X_i V \mathcal{E}_{ij} | Z}(x_i, j | z) &= \sum_z P_Z(z) \cdot \max_{x_i} \sum_{x_j} P_{X_i X_j V \mathcal{E}_{ij} | Z}(x_i, x_j, j | z) \\ &\leq 2^{\alpha/2} \sum_z P_Z(z) \cdot \max_{x_i, x_j} P_{X_i X_j \mathcal{E}_{ij} | Z}(x_i, x_j | z) \leq 2^{-\alpha/2}, \end{aligned} \quad (10)$$

⁶In case $\varepsilon = 0$, i.e., α lower bounds the ordinary (rather than the smooth) min-entropy, the \mathcal{E}_{ij} are the events “that always occur” and can be ignored from the rest of the analysis.

where the last inequality follows from the assumption (8) and the first is a consequence of the fact that the number of non-zero summands (in the sum over x_j) cannot be larger than $2^{\alpha/2}$, because for any x_j with $P_{X_i X_j V \mathcal{E}_{ij}|Z}(x_i, x_j, j|z) > 0$, it also holds that $P_{X_j|Z}(x_j|z) \geq 2^{-\alpha/2}$ and the sum over all those x_j would exceed 1 if there were more than $2^{\alpha/2}$ summands. Note that per-se, \mathcal{E}_{ij} is only defined in the probability space given by X_i, X_j and Z , but it can be naturally extended to the probability space given by X_1, \dots, X_n, Z, V by assuming it to be independent of anything else when given X_i, X_j, Z , so that e.g. $P_{X_i V \mathcal{E}_{ij}|Z}$ is indeed well-defined.

Consider now an independent random variable W with $H_{\min}(W) \geq 1$. By the assumptions on W it holds that $P[V \neq W] \geq \frac{1}{2}$ and $P_{X_W V W Z}(x_i, j, i, z) = P_{X_i V W Z}(x_i, j, i, z) = P_{X_i V Z}(x_i, j, z) P_W(i)$. In the probability space determined by the random variables X_1, \dots, X_n, V, W, Z and all of the events \mathcal{E}_{ij} , define the event \mathcal{E} as $\mathcal{E} := \mathcal{E}_{WV}$, so that $P_{X_W V W \mathcal{E}|Z}(x_i, j, i|z) = P_{X_i V W \mathcal{E}_{ij}|Z}(x_i, j, i|z) = P_{X_i V \mathcal{E}_{ij}|Z}(x_i, j|z) P_W(i)$. Note that

$$P[\bar{\mathcal{E}}] = \sum_{i,j} P_{V W \bar{\mathcal{E}}_{WV}}(j, i) = \sum_{i,j} P_{V \bar{\mathcal{E}}_{ij}}(j) P_W(i) \leq \sum_{i,j} P[\bar{\mathcal{E}}_{ij}] P_W(i) \leq m\varepsilon$$

and thus $P[\bar{\mathcal{E}}|V \neq W] \leq P[\bar{\mathcal{E}}]/P[V \neq W] \leq 2m\varepsilon$. From the above, it follows that

$$\begin{aligned} p_{\text{guess}}(X_W, \mathcal{E}|VWZ, V \neq W) &= \sum_{z,i,j} \max_x P_{X_W V W Z \mathcal{E}|V \neq W}(x, j, i, z) \leq 2 \sum_{z,i \neq j} \max_x P_{X_W V W Z \mathcal{E}}(x, j, i, z) \\ &= 2 \sum_{z,i \neq j} P_Z(z) \cdot \max_x P_{X_W V W \mathcal{E}|Z}(x, j, i|z) = 2 \sum_{z,i \neq j} P_Z(z) \cdot \max_{x_i} P_{X_i V \mathcal{E}_{ij}|Z}(x_i, j|z) \cdot P_W(i) \\ &= 2 \sum_i P_W(i) \sum_{j \neq i} \sum_z P_Z(z) \cdot \max_{x_i} P_{X_i V \mathcal{E}_{ij}|Z}(x_i, j|z) \leq 2m \cdot 2^{-\alpha/2}, \end{aligned}$$

where we used (9) and (10) in the last inequality. The claim now follows by definition of H_{\min}^ε . \square

2.4 Quantum Uncertainty Relation.

At the very core of our security proofs lies (a special case of) the quantum uncertainty relation from [DFR⁺07]⁷, 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 2.3 (Uncertainty Relation [DFR⁺07]) *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*

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

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

$$\sigma(\delta) := \frac{\delta^2 \log(e)}{32(2 - \log(\delta))^2}. \quad (11)$$

⁷In [DFR⁺07], a stricter notion of conditional smooth min-entropy was used, which in particular implies the bound as stated here.

2.5 Privacy Amplification

We will make use of two-universal hash functions. A class \mathcal{F} of functions $f : \{0, 1\}^n \rightarrow \{0, 1\}^\ell$ is called two-universal, if for all $x \neq y \in \{0, 1\}^n$, we have $\Pr_{f \in_R \mathcal{F}}[f(x) = f(y)] \leq 2^{-\ell}$ [CW79]. 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 2.4 ([Ren05, DFR⁺07]) *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 $\varepsilon \geq 0$,*

$$d(F(X)|F, U, E) \leq 2^{-\frac{1}{2}(\mathbb{H}_{\min}^\varepsilon(X|UE) - \ell) - 1} + \varepsilon.$$

3 The Noisy-Quantum-Storage Model

The *noisy-quantum-storage model* has been established in [WST08, STW09] for the special case where the dishonest receiver is limited to so-called “individual-storage attacks”, i.e. 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 [KWW09, Sections 1.3 and 3.3], see Figure 1 for an illustration. The cheating receiver is computationally unbounded, has unlimited classical storage and can perform 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 $\mathcal{F} : \mathcal{B}(\mathcal{H}_{in}) \rightarrow \mathcal{B}(\mathcal{H}_{out})$.

As in [KWW09], let

$$P_{succ}^{\mathcal{F}}(n) := \max_{\{D_x\}_x, \{\rho_x\}_x} \frac{1}{2^n} \sum_{x \in \{0, 1\}^n} \text{Tr}(D_x \mathcal{F}(\rho_x)) \quad (12)$$

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}_{in} and decoding POVMs $\{D_x\}_{x \in \{0, 1\}^n}$ on \mathcal{H}_{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 [KWW09] formalize this intuition and are the key ingredients to connect the security of protocols in the noisy-storage model for such channels with their ability to transmit classical information.

Lemma 3.1 ([KWW09]) *Consider an arbitrary cq-state ρ_{XQ} and a CPTP map $\mathcal{F} : \mathcal{B}(\mathcal{H}_Q) \rightarrow \mathcal{B}(\mathcal{H}_{out})$. Then, $\mathbb{H}_{\min}(X|\mathcal{F}(Q)) \geq -\log P_{succ}^{\mathcal{F}}(\lfloor \mathbb{H}_{\min}(X) \rfloor)$.*

Lemma 3.2 ([KWW09]) *Consider an arbitrary ccq-state ρ_{XTQ} , and let $\varepsilon, \varepsilon' \geq 0$ be arbitrary. Let $\mathcal{F} : \mathcal{B}(\mathcal{H}_Q) \rightarrow \mathcal{B}(\mathcal{H}_{Q_{out}})$ be an arbitrary CPTP map. Then,*

$$\mathbb{H}_{\min}^{\varepsilon + \varepsilon'}(X|T\mathcal{F}(Q)) \geq -\log P_{succ}^{\mathcal{F}} \left(\lfloor \mathbb{H}_{\min}^\varepsilon(X|T) - \log \frac{1}{\varepsilon'} \rfloor \right).$$

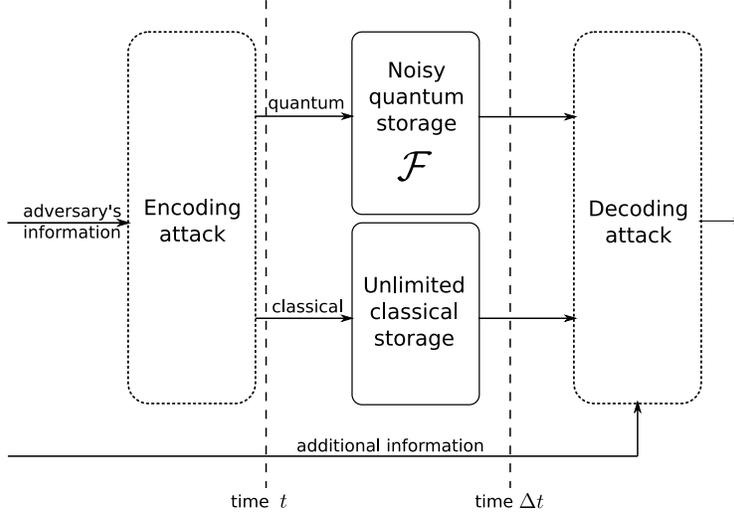


Figure 1: (from [WCSL10]): During waiting times Δt , the adversary must use his noisy quantum storage described by the CPTP map \mathcal{F} . Before using his quantum storage, he performs any (error-free) “encoding attack” of his choosing, which consists of a measurement or an encoding into an error-correcting code. After time Δt , he receives some additional information that he can use for decoding.

We are interested in channels \mathcal{N} which satisfy the following *strong-converse property*: The success probability (12) decays exponentially for rates R above the capacity, i.e., it takes the form

$$P_{succ}^{\mathcal{N}^{\otimes n}}(nR) \leq 2^{-n\gamma^{\mathcal{N}}(R)} \quad \text{where} \quad \gamma^{\mathcal{N}}(R) > 0 \text{ for all } R > C_{\mathcal{N}}. \quad (13)$$

In [KW09], property (13) was shown to hold for a large class of channels. An important example for which we obtain security is the d -dimensional depolarizing channel $\mathcal{N}_r : \mathcal{B}(\mathbb{C}^d) \rightarrow \mathcal{B}(\mathbb{C}^d)$ defined for $d \geq 2$ as

$$\mathcal{N}_r(\rho) := r\rho + (1-r)\frac{\mathbb{1}}{d} \quad \text{for some fixed } 0 \leq r \leq 1, \quad (14)$$

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 [Kin03]. For $d=2$, i.e., qubits, it is given by

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

4 1-2 Oblivious Transfer

4.1 Security Definition and Protocol

In this section we prove the security of a randomized version of 1-2 OT (Theorem 4.2) 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 , i.e. 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 $\hat{S}_{\bar{C}}$ since he is ignorant about $S_{\bar{C}}$. The security of a quantum protocol implementing ROT is formally defined in [DFR⁺07] and justified in [FS09] (see also [WW08]).

Definition 4.1 *An ε -secure 1-2 ROT ^{ℓ} is a protocol between Alice and Bob, where Bob has input $C \in \{0, 1\}$, and Alice has no input.*

- (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 .*
- (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 $\Pr[Y = S'_C] \geq 1 - \varepsilon$ and C is independent of S'_0, S'_1 and ρ_A ⁸.*
- (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 $d(S_{\bar{D}} | S_D \rho_B) \leq \varepsilon$.*

We consider the same protocol for ROT as in [BBCS91, DFL⁺09].

Protocol 1 ([BBCS91, DFL⁺09]) 1-2 ROT ^{ℓ}

1. Alice picks $x \in_R \{0, 1\}^n$ and $\theta \in_R \{+, \times\}^n$. At time $t = 0$, she sends $|x_1\rangle_{\theta_1}, \dots, |x_n\rangle_{\theta_n}$ to Bob.
2. Bob picks $\hat{\theta} \in_R \{+, \times\}^n$ at random and measures the i th 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 $\theta = \theta_1, \dots, \theta_n$ 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 $s_1 = f_1(x|_{\mathcal{I}_1})$ ⁹.
6. Bob outputs $s_c = f_c(\hat{x}|_{\mathcal{I}_c})$.

⁸Existence 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 $\rho_{YS'_0S'_1A}$ such that tracing out the registers of S'_0, S'_1 yields the original state ρ_{YA} and the stated properties hold.

⁹If $x|_{\mathcal{I}_b}$ 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.

4.2 Security Analysis

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 non-empty) and hence obtains s_c . Alice's outputs s_0, s_1 are perfectly independent of each other and of c .

Security against Dishonest Alice Security holds in the same way as shown in [DFR⁺07]. 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.

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 Section 3 is completely ignorant about $S_{\bar{D}}$. 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 4.2 Fix $0 < \delta < \frac{1}{4}$ and let

$$\varepsilon = 2 \exp \left(- \frac{(\delta/4)^2}{32(2 + \log \frac{4}{\delta})^2} \cdot n \right). \quad (15)$$

Then, for any attack of a dishonest Bob with storage $\mathcal{F} : \mathcal{B}(\mathcal{H}_{in}) \rightarrow \mathcal{B}(\mathcal{H}_{out})$, Protocol 1 is 2ε -secure against a dishonest receiver Bob according to Definition 4.1, if $n \geq 4/\delta$ and

$$\ell \leq -\frac{1}{2} \log P_{succ}^{\mathcal{F}} \left(\left(\frac{1}{4} - \delta \right) n \right) - \log \left(\frac{1}{\varepsilon} \right).$$

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 (Section 3.3 in [KWW09]) that

$$H_{\min}^{\varepsilon/2} (X_0 X_1 | \Theta K) \geq \frac{n}{2} - \frac{n\delta}{2},$$

where K denotes Bob's classical information obtained from the encoding attack. Classical min-entropy splitting (Lemma 2.1) then ensures that there exists a binary random variable $D \in \{0, 1\}$ such that

$$H_{\min}^{\varepsilon/2} (X_{\bar{D}} | D \Theta K) \geq \frac{n}{4} - \frac{n\delta}{4} - 1.$$

One can now continue to argue as in the proof of Theorem 3.3 in [KWW09], i.e. we use Lemma 3.2 to get

$$H_{\min}^{\varepsilon} (X_{\bar{D}} | D \Theta K Q_{out}) \geq -\log P_{succ}^{\mathcal{F}} \left(\frac{n}{4} - \frac{n\delta}{4} - 1 - \log \frac{2}{\varepsilon} \right) \geq -\log P_{succ}^{\mathcal{F}} \left(\left(\frac{1}{4} - \delta \right) n \right),$$

where the last step follows in the same way as in [KWW09] from the monotonicity of the success probability $P_{succ}^{\mathcal{F}}(m) \leq P_{succ}^{\mathcal{F}}(m')$ for $m \geq m'$ and the fact that $\log \frac{2}{\varepsilon} \leq \frac{\delta}{2}n \leq \frac{3\delta}{4}n - 1$.

The rest of the security proof is analogous to the proof in [DFR⁺07]: It follows from the chain rule for smooth min-entropy (4) that

$$\begin{aligned} H_{\min}^{\varepsilon}(X_{\overline{D}}|D\Theta S_D K Q_{out}) &\geq H_{\min}^{\varepsilon}(X_{\overline{D}} S_D | D\Theta K Q_{out}) - \ell \\ &\geq -\log P_{succ}^{\mathcal{F}}\left(\left(\frac{1}{4} - \delta\right)n\right) - \ell. \end{aligned}$$

The privacy amplification Theorem 2.4 yields

$$d(F_{\overline{D}}(X_{\overline{D}}) | D\Theta F_D S_D K Q_{out}) \leq 2^{-\frac{1}{2}(-\log P_{succ}^{\mathcal{F}}((\frac{1}{4}-\delta)n)-2\ell)} + \varepsilon \quad (16)$$

which is smaller than 2ε as long as

$$-\frac{1}{2}\log P_{succ}^{\mathcal{F}}\left(\left(\frac{1}{4} - \delta\right)n\right) - \ell \geq \log\left(\frac{1}{\varepsilon}\right).$$

from which our claim follows. \square

4.3 Tensor-product channels

Corollary 4.3 *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 (13), and*

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

Fix $\delta \in]0, \frac{1}{4} - C_{\mathcal{N}} \cdot \nu[$, and let ε be defined as in (18). Then, for any attack of a dishonest Bob, Protocol 1 is 2ε -secure against a dishonest receiver Bob according to Definition 4.1, if $n \geq 4/\delta$ and

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

Proof. We can substitute n by νn and R by R/ν in the strong-converse property (13) to obtain

$$-\frac{1}{n}\log P_{succ}^{\mathcal{N}^{\otimes \nu n}}(nR) \geq \nu \cdot \gamma^{\mathcal{N}}(R/\nu).$$

The claim then follows from Theorem 4.2 by setting $R := \frac{1}{4} - \delta$. \square

For the d -dimensional depolarizing channel

$$\mathcal{N}_r(\rho) = r\rho + (1-r)\frac{\mathbb{1}}{d}. \quad (17)$$

which preserves a d -dimensional input state with probability r and depolarizes it completely with probability $1-r$, it has been shown in [KW09, KWW09] that

$$\gamma^{\mathcal{N}}(R) = \max_{\alpha \geq 1} \frac{\alpha - 1}{\alpha} \left(R - \log d + \frac{1}{1 - \alpha} \log \left(\left(r + \frac{1-r}{d} \right)^{\alpha} + (d-1) \left(\frac{1-r}{d} \right)^{\alpha} \right) \right).$$

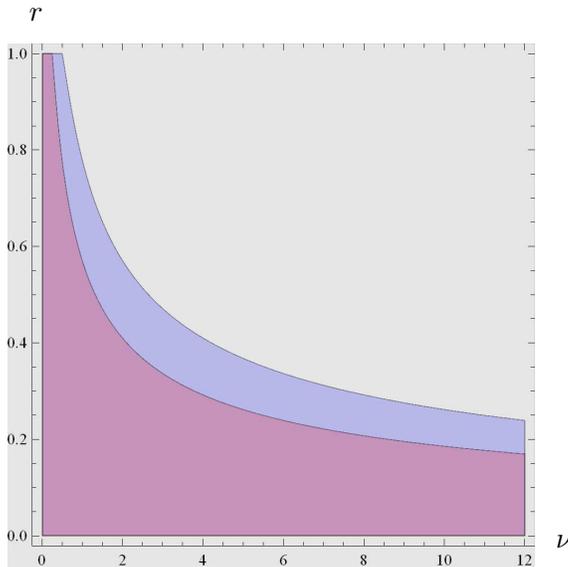


Figure 2: Possible regions of a depolarizing qubit channel with noise parameter r and storage rate ν where security for OT can be established for asymptotically many pulses. The [KWW09]-approach yields the blue region, whereas our simpler approach gives the red subset of it.

We compare the parameters in terms of OT- and error-rate of our approach to the ones in [KWW09]. In Figure 2, the regions of the noise-parameter r and storage-rate ν from our approach (red) and the [KWW09]-approach (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 post-processing with interactive hashing in [KWW09] 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 4.3, the security error is 2ε where ε is defined in (18), 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 Figure 3 for different noise rates r and a storage rate of $\nu = 1$. In the approach of [KWW09], 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 blue dashed line in Figure 3. Note that this amount of pulses are not sufficient to keep the security error below 10^{-8} for noise rates r above 0.21.

In Figure 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 [KWW09]-approach and leads to higher OT-rates compared to our approach for noise parameters between $0.34 < r < 0.52$. In all other cases, our simpler approach allows to get OT of longer strings while keeping the security error below 10^{-8} .

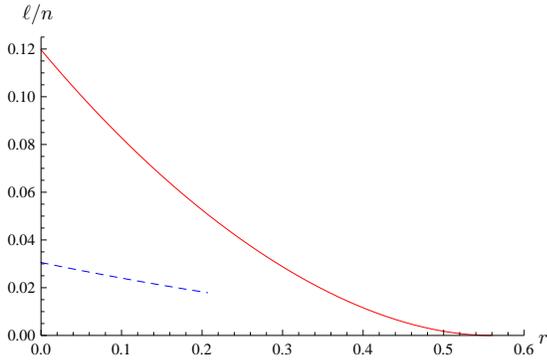


Figure 3: The adversary’s storage is depolarizing qubit noise $\mathcal{F} = \mathcal{N}_r^{\otimes n}$ with $d = 2$, $\nu = 1$, and $n = 10^{10}$. The horizontal axis represents the noise parameter r , while the vertical axis represents the OT-rate ℓ/n . The rates are only plotted for regions where the security error stays below 10^{-8} . The red line represents the OT-rate obtained from our approach (Corollary 4.3 with $\delta = 0.0106$). The dashed blue line is the rate from the [KWW09]-approach with optimised 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.

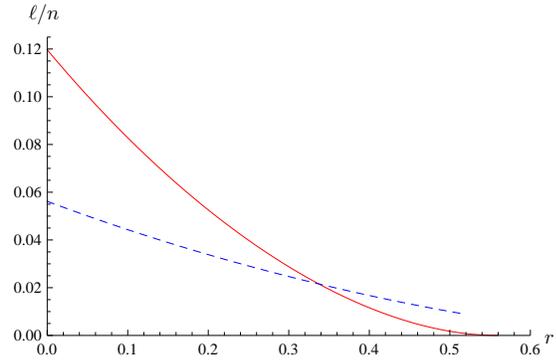


Figure 4: As in Figure 3, but for many more pulses, namely $n = 10^{15}$. The red line represents the OT-rate obtained from our approach (Corollary 4.3 with $\delta = 0.000057588$). The dashed blue line is the rate from the [KWW09]-approach with optimised extra parameters $\delta = 0.0005$ and $\omega = 10$. For $r > 0.47$, the security error is above the allowed threshold 10^{-8} . For noise parameters between $0.34 < r < 0.52$, the [KWW09]-approach yields higher OT-rates. For all other noise rates r , our simpler approach yields higher rates.

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

5 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 [STW09] and for general attacks in [WCSL10]. In the following, we present an upgraded protocol for oblivious transfer along the lines of [WCSL10] but with a much simpler and natural post-processing.

5.1 Protocol

We consider the same setup as in [WCSL10]. Before engaging in the actual protocol, Alice and Bob agree on a security-error probability $\varepsilon > 0$. The parameter $p_{\text{B,no click}}^h$ denotes the probability

that an honest Bob observes no click in his detection apparatus and the corresponding parameter $\zeta_{\text{B,no click}}^h$ says how much fluctuations we allow. Typically, we use a $\zeta_{\text{B,no click}}^h$ of order $\sqrt{\ln(2/\varepsilon)/(2n)}$ such that the Chernoff bound allows us to argue that $p_{\text{B,no click}}^h$ lies in the interval $[(p_{\text{B,no click}}^h - \zeta_{\text{B,no click}}^h)n, (p_{\text{B,no click}}^h + \zeta_{\text{B,no click}}^h)n]$ except with probability ε .

Error-correction is done using a one-way (forward) error correction scheme, e.g. by using low-density parity-check (LDPC) 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 $p_{\text{B,err}}^h$, this procedure amounts to sending error-correcting information of at most $1.2 \cdot h(p_{\text{B,err}}^h) \cdot k$ bits [ELAB09].

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

Protocol 2 *Robust 1-2 ROT^ℓ(C, T, ε)*

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 $i = 1, \dots, n$: 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 qubit in basis $\hat{\theta}_i$ and records whether he detects a photon or not. He obtains some bit-string $\hat{x} \in \{0, 1\}^m$ with $m \leq n$.
4. Bob reports back to Alice in which time slots he recorded a click.
5. Alice restricts herself to the set of $m < n$ bits that Bob did not report as missing. Let this set of qubits be S_{remain} with $|S_{\text{remain}}| = m$. If m does not lie in the interval $[(1 - p_{\text{B,no click}}^h - \zeta_{\text{B,no click}}^h)n, (1 - p_{\text{B,no click}}^h + \zeta_{\text{B,no click}}^h)n]$, then Alice aborts the protocol.

Both parties wait time Δt .

6. Alice sends the basis information $\theta = \theta_1, \dots, \theta_m$ 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 $\text{syn}(x|_{\mathcal{I}_0})$ and $\text{syn}(x|_{\mathcal{I}_1})$ to Bob. Alice outputs $s_0 = f_0(x|_{\mathcal{I}_0})$ and $s_1 = f_1(x|_{\mathcal{I}_1})$.
9. Bob uses $\text{syn}(x|_{\mathcal{I}_c})$ to correct the errors on his output $\hat{x}|_{\mathcal{I}_c}$. He obtains the corrected bit-string x_{cor} and outputs $s'_c = f_c(x_{\text{cor}})$.

5.2 Security Analysis

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 .

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 2.

Security against Dishonest Bob In the previous Section 4, we have seen that the security analysis for weak string erasure from [KWW09] essentially carries over to 1-2 oblivious transfer. Similarly, the security analysis for weak string erasure with errors from [WCSL10] can be adapted to analyse Protocol 1.

We will use the following probabilities: (see [WCSL10] for details and some example parameters for concrete setups)

$p_{\text{B,no click}}^d$	dishonest Bob observes no click in his detection apparatus (due to imperfections in Alice’s apparatus)
$p_{\text{B,no click}}^h$	honest Bob observes no click in his detection apparatus (due to losses and imperfections of both player’s apparatus)
p_{sent}^1	Alice sends exactly 1 photon.
$p_{\text{B,err}}^h$	honest Bob outputs the wrong bit (due to misalignments and noise on the channel)

Theorem 5.1 (Security against dishonest Bob) Fix $0 < \delta < \frac{1}{4}$ and let

$$\varepsilon = 2 \exp \left(- \frac{(\delta/4)^2}{32(2 + \log \frac{4}{\delta})^2} \cdot m^1 \right). \quad (18)$$

Then, for any attack of a dishonest Bob with storage $\mathcal{F} : \mathcal{B}(\mathcal{H}_{in}) \rightarrow \mathcal{B}(\mathcal{H}_{out})$, Protocol 2 is 2ε -secure against a dishonest receiver Bob according to Definition 4.1, if $m^1 \geq 4/\delta$ and the length of the OT-strings

$$\ell \leq -\frac{1}{2} \log P_{succ}^{\mathcal{F}} \left(\left(\frac{1}{4} - \delta \right) m^1 \right) - 1.2 \cdot h(p_{\text{B,err}}^h) \cdot \frac{m}{2} - \log \left(\frac{1}{\varepsilon} \right),$$

where $m^1 := (p_{\text{sent}}^1 - p_{\text{B,no click}}^h + p_{\text{B,no click}}^d)n$ is the minimal number of single-photon rounds remaining and $m = (1 - p_{\text{B,no click}}^h)n$ is the total number of rounds remaining.

Proof. As in [WCSL10], we adopt the conservative viewpoint that a dishonest Bob does not experience any bit-errors nor 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 multi-photon 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 $p_{\text{B,no click}}^h$ 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 $p_{\text{B,no click}}^d$ 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 $(p_{\text{B,no click}}^h - p_{\text{B,no click}}^d)n$ *single-photon* rounds as missing. That means that of the total $m = (1 - p_{\text{B,no click}}^h)n$ rounds that Alice accepts, at least

$$m^1 := (p_{\text{sent}}^1 - (p_{\text{B,no click}}^h - p_{\text{B,no click}}^d))n \quad (19)$$

are single-photon rounds.

It can be argued as in [WCSL10] 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

$$H_{\min}^{\varepsilon/2}(X_0 X_1 | \Theta K) \geq \frac{m^1}{2} - \frac{m^1 \delta}{2}, \quad (20)$$

where X_0, X_1 are the sub-strings 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

$$\varepsilon = 2 \exp\left(-\frac{(\delta/4)^2}{32(2 + \log \frac{4}{\delta})^2} \cdot m^1\right). \quad (21)$$

Proceeding as in the proof of Protocol 1 (with m^1 instead of n), classical min-entropy splitting (Lemma 2.1) then ensures that there exists a binary random variable $D \in \{0, 1\}$ such that

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

Then, we use Lemma 3.2 to get

$$H_{\min}^{\varepsilon}(X_{\overline{D}} | D \Theta K Q_{\text{out}}) \geq -\log P_{\text{succ}}^{\mathcal{F}}\left(\frac{m^1}{4} - \frac{m^1 \delta}{4} - 1 - \log \frac{2}{\varepsilon}\right) \geq -\log P_{\text{succ}}^{\mathcal{F}}\left(\left(\frac{1}{4} - \delta\right) m^1\right),$$

where the last step follows in the same way as in [KWW09] from the monotonicity of the success probability $P_{\text{succ}}^{\mathcal{F}}(k) \leq P_{\text{succ}}^{\mathcal{F}}(k')$ for $k \geq k'$ and the fact that $\log \frac{2}{\varepsilon} \leq \frac{\delta}{2} m^1 \leq \frac{3\delta}{4} m^1 - 1$.

Additionally, the dishonest receiver learns the two syndromes $Syn(X_0), Syn(X_1)$. 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 $1.2 \cdot h(p_{\text{err}}^h) \cdot m$ bits of information.

It follows from the chain rule for smooth min-entropy (4) that

$$\begin{aligned} H_{\min}^{\varepsilon}(X_{\overline{D}} | D \Theta S_D Syn(X_0) Syn(X_1) K Q_{\text{out}}) &\geq H_{\min}^{\varepsilon}(X_{\overline{D}} | D \Theta K Q_{\text{out}}) - \ell - 1.2 \cdot h(p_{\text{err}}^h) \cdot m \\ &\geq -\log P_{\text{succ}}^{\mathcal{F}}\left(\left(\frac{1}{4} - \delta\right) m^1\right) - \ell - 1.2 \cdot h(p_{\text{err}}^h) \cdot m. \end{aligned}$$

The privacy amplification Theorem 2.4 yields

$$d(F_{\overline{D}}(X_{\overline{D}}) | D \Theta F_D S_D K Q_{\text{out}}) \leq 2^{-\frac{1}{2}(-\log P_{\text{succ}}^{\mathcal{F}}((\frac{1}{4}-\delta)m^1) - 2\ell - 1.2 \cdot h(p_{\text{err}}^h) \cdot m)} + \varepsilon \quad (22)$$

which is smaller than 2ε as long as

$$-\frac{1}{2} \log P_{succ}^{\mathcal{F}} \left(\left(\frac{1}{4} - \delta \right) m^1 \right) - \ell - 1.2 \cdot h(p_{err}^h) \cdot \frac{m}{2} \geq \log \left(\frac{1}{\varepsilon} \right).$$

from which our claim follows. \square

In the same way as Corollary 4.3, we can derive

Corollary 5.2 *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 (13) and having capacity $C_{\mathcal{N}}$ bounded by*

$$C_{\mathcal{N}} \cdot \nu < \left(\frac{1}{4} - \delta \right) (p_{sent}^1 - p_{B, no click}^h + p_{B, no click}^d). \quad (23)$$

Then Protocol 2 is 2ε -secure against a dishonest receiver Bob according to Definition 4.1 with the following parameters: Let $\delta \in]0, \frac{1}{4} - C_{\mathcal{N}} \cdot \nu[$ and $m^1 \geq 4/\delta$. Then the length ℓ of the OT-strings is bounded by

$$\ell \leq \frac{1}{2} \nu \cdot \gamma^{\mathcal{N}} \left(\frac{R}{\nu} \right) \cdot n - 1.2 \cdot h(p_{B, err}^h) \cdot (1 - p_{B, err}^h) \frac{n}{2} - \log \left(\frac{1}{\varepsilon} \right), \quad (24)$$

where $\gamma^{\mathcal{N}}$ is the strong converse parameter of \mathcal{N} (see (13)) and

$$\begin{aligned} m &= (1 - p_{B, no click}^h) n && \text{(the number of remaining rounds) ,} \\ m^1 &= (p_{sent}^1 - p_{B, no click}^h + p_{B, no click}^d) n && \text{(the minimal number of single-photon rounds) ,} \\ R &= \left(\frac{1}{4} - \delta \right) \frac{m^1}{n} && \text{(the rate at which dishonest Bob has to send information} \\ &&& \text{through storage) ,} \end{aligned}$$

for sufficiently large n . The error has the form

$$\varepsilon(\delta) \leq 2 \exp \left(- \frac{\delta^2}{512(4 + \log \frac{1}{\delta})^2} \cdot (p_{sent}^1 - p_{B, no click}^h + p_{B, no click}^d) n \right). \quad (25)$$

6 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 [DFSS07, DFSS10] achieving secure password-based identification in the bounded-quantum-storage model. This answers an open question posed in [KWW09].

6.1 Task and Protocol

A user Alice wants to identify herself to a server Bob by means of a personal identification number (PIN). 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 [DFSS07] 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 6.1 *We call an identification protocol between user Alice and server Bob secure for the user Alice with error ε against (dishonest) server Bob \mathbf{B}' if the following is satisfied: whenever the initial state of \mathbf{B}' is independent of W , the joint state $\rho_{W E_{\mathbf{B}'}}$ after the execution of the protocol is such that there exists a random variable W' that is independent of W and such that*

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

The Markov-chain notation is explained in (1).

We consider the same protocol for password-based secure identification from [DFSS07], in the more practical form presented in [DFL⁺09], where the receiving party measures in a random basis. Let $\mathbf{c} : \mathcal{W} \rightarrow \{+, \times\}^n$ be the encoding function of a binary code of length n with $m = |\mathcal{W}|$ codewords and minimal distance d . \mathbf{c} can be chosen such that n is linear in $\log(m)$ 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 ([DFSS07, DFL⁺09]) *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 $|x_1\rangle_{\theta_1}, \dots, |x_n\rangle_{\theta_n}$ to Bob.
2. Bob picks $\hat{\theta} \in_R \{+, \times\}^n$ at random and measures the i th 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 $\hat{\theta} = \mathbf{c}(w) \oplus \kappa$ (interpreting $+$ as 0 and \times as 1 so that \oplus makes sense). He sends κ to Alice and they define the shifted code $\mathbf{c}'(w) := \mathbf{c}(w) \oplus \kappa$.
4. Alice sends θ and $f \in_R \mathcal{F}$ to Bob. Both compute $\mathcal{I}_w := \{i : \theta_i = \mathbf{c}'(w)_i\}$.
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 (non-trivially) extended to additionally withstand man-in-the-middle attacks [DFSS07, DFSS10].

6.2 Security Analysis

Theorem 6.2 (Security against dishonest Bob) *Fix $0 < \delta < \frac{1}{4}$ and let $\sigma(\delta)$ be defined as in (11). Then, for any attack of a dishonest Bob with storage channel $\mathcal{F} : \mathcal{B}(\mathcal{H}_{in}) \rightarrow \mathcal{B}(\mathcal{H}_{out})$, Protocol 3 is an ε -secure identification protocol against a dishonest receiver Bob according to Definition 6.1, if $d \geq \frac{4+4\log(m)}{\delta}$ and*

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

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 $\frac{d}{n}$, $\frac{\log(m)}{n}$, and $\frac{\ell}{n}$ are all constants. The result above 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 $0 < \delta < \frac{1}{4}$, $\frac{-\log P_{succ}^{\mathcal{F}}((\frac{1}{4}-\delta)d)}{n} - \frac{\ell}{n} > 0$ and $\sigma(\delta/4)\frac{d}{n} - \frac{\log(m)}{n} > 0$. See Theorem 6.4 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 $1 \leq i \neq j \leq m$, 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 2.3) 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 $\varepsilon' \leq 2^{-\sigma(\delta/4)d}$. 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 2.2 implies that there exists W' (called V in Lemma 2.2) such that if $W \neq W'$ then X_W has $(\frac{1}{4} - \delta/4)d - \log(m) - 1$ bits of $2m\varepsilon'$ -smooth min-entropy given W and W' (and Θ, K), i.e.,

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

By Lemma 3.2, it follows that for $Q_{out} = \mathcal{F}(Q_{in})$, we get

$$\begin{aligned} H_{\min}^{(2m+1)\varepsilon'}(X_W|WW'\Theta K Q_{out}, W \neq W') &\geq -\log P_{succ}^{\mathcal{F}}\left(\left(\frac{1}{4} - \delta/4\right)d - \log(m) - 1 - \log(1/\varepsilon')\right) \\ &\geq -\log P_{succ}^{\mathcal{F}}\left(\left(\frac{1}{4} - \delta\right)d\right), \end{aligned}$$

where the last inequality follows as in the OT-case (proof of Theorem 4.2) from $\log(1/\varepsilon') \leq \frac{\delta}{2}d \leq \frac{3\delta}{4}d - \log(m) - 1$ 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 $\varepsilon'' = \frac{1}{2} \cdot 2^{-\frac{1}{2}(-\log P_{succ}^{\mathcal{F}}((\frac{1}{4}-\delta)d)-\ell)} + (2m+1)\varepsilon'$. 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 [DFSS10].

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

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

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 $2(2m + 1) \leq 8m$. \square

Theorem 6.3 (Security against dishonest Alice [DFSS07]) *If $H_{\min}(W) \geq 1$, 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 6.4 *If $H_{\min}(W) \geq 1$, 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 (13), and*

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

and the security error is

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

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

Proof. First of all, we have that $-\log P_{succ}^{\mathcal{N}^{\otimes \nu n}}((1/4 - \delta)d) \geq \gamma^{\mathcal{N}} \left(\frac{1/4-\delta}{\nu}\right) \nu d$.

We choose $\ell = \frac{1}{3} \cdot \gamma^{\mathcal{N}} \left(\frac{1/4-\delta}{\nu}\right) \nu d$. Then security against dishonest Bob holds except with an error $\varepsilon = 2^{-\frac{1}{3} \cdot \gamma^{\mathcal{N}} \left(\frac{1/4-\delta}{\nu}\right) \nu d} + 2^{-(\sigma(\delta/4)d - \log(m) - 3)}$, and security against dishonest Alice holds except with an error $m^2/2^\ell = 2^{-\frac{1}{3}(\gamma^{\mathcal{N}} \left(\frac{1/4-\delta}{\nu}\right) \nu d - 6 \log(m))}$. Using a code \mathfrak{c} , which asymptotically meets the Gilbert-Varshamov bound [Tho83], d may be chosen arbitrarily close to $n \cdot h^{-1}(1 - \log(m)/n)$. In particular, we can ensure that d does not differ from this value by more than 1. Inserting $d = \mu \cdot n - 1$ in the expressions and using that $\gamma^{\mathcal{N}} \left(\frac{1/4-\delta}{\nu}\right) \nu \leq 1$ yields the theorem. \square

7 Conclusion

We have used the technical tool from [KWW09] 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 post-processing which makes them easier to implement in the lab compared to the protocols from [KWW09, WCSL10]. Their security analysis 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. We show for the first time 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 [STW09].

Acknowledgments

This work is supported by EU fifth framework project QAP IST 015848 and the Dutch NWO VICI project 2004-2009.

References

- [AFK⁺08] Jurgen Appel, Eden Figueroa, Dmitry Korystov, M. Lobino, and A. I. Lvovsky. Quantum memory for squeezed light. *Physical Review Letters*, 100(9):093602, 2008.
- [BB84] Charles H. Bennett and Gilles Brassard. Quantum cryptography: Public key distribution and coin tossing. In *IEEE International Conference on Computers, Systems, and Signal Processing*, pages 175–179, 1984.
- [BBCS91] Charles H. Bennett, Gilles Brassard, Claude Crépeau, and Marie-Hélène Skubiszewska. Practical quantum oblivious transfer. In *Advances in Cryptology—CRYPTO '91*, volume 576 of *Lecture Notes in Computer Science*, pages 351–366. Springer, 1991.
- [CDLK08] K. S. Choi, H. Deng, J. Laurat, and H. J. Kimble. Mapping photonic entanglement into and out of a quantum memory. *Nature*, 452(7183):67–U4, March 2008.
- [CMJ⁺05] T Chaneliere, DN Matsukevich, SD Jenkins, SY Lan, TAB Kennedy, and A Kuzmich. Storage and retrieval of single photons transmitted between remote quantum memories. *Nature*, 438(7069):833–836, December 2005.
- [CW79] J. Lawrence Carter and Mark N. Wegman. Universal classes of hash functions. *Journal of Computer and System Sciences*, 18(2):143–154, 1979.
- [DFL⁺09] Ivan B. Damgård, Serge Fehr, Carolin Lunemann, Louis Salvail, and Christian Schaffner. Improving the security of quantum protocols via commit-and-open. In *Advances in Cryptology—CRYPTO '09*, volume 5677 of *Lecture Notes in Computer Science*, pages 408–427. Springer, 2009. Full version available at: <http://arxiv.org/abs/0902.3918>.
- [DFR⁺07] Ivan B. Damgård, Serge Fehr, Renato Renner, Louis Salvail, and Christian Schaffner. A tight high-order entropic quantum uncertainty relation with applications. In *Advances in Cryptology—CRYPTO '07*, volume 4622 of *Lecture Notes in Computer Science*, pages 360–378. Springer, 2007.
- [DFSS05] Ivan B. Damgård, Serge Fehr, Louis Salvail, and Christian Schaffner. Cryptography in the bounded quantum-storage model. In *46th Annual IEEE Symposium on Foundations of Computer Science (FOCS)*, pages 449–458, 2005. Full version available at: <http://arxiv.org/abs/quant-ph/0508222v2>.

- [DFSS07] Ivan B. Damgård, Serge Fehr, Louis Salvail, and Christian Schaffner. Secure identification and QKD in the bounded-quantum-storage model. In *Advances in Cryptology—CRYPTO '07*, volume 4622 of *Lecture Notes in Computer Science*, pages 342–359. Springer, 2007.
- [DFSS08] Ivan B. Damgård, Serge Fehr, Louis Salvail, and Christian Schaffner. Cryptography in the bounded-quantum-storage model. *SIAM Journal on Computing*, 37(6):1865–1890, 2008.
- [DFSS10] Ivan B. Damgård, Serge Fehr, Louis Salvail, and Christian Schaffner. Secure identification and QKD in the bounded-quantum-storage model. to appear in a special BB84 issue of *Theoretical Computer Science*, 2010.
- [DHRS04] Yan Zong Ding, Danny Harnik, Alon Rosen, and Ronen Shaltiel. Constant-round oblivious transfer in the bounded storage model. In *Theory of Cryptography Conference (TCC)*, volume 2951 of *Lecture Notes in Computer Science*, pages 446–472. Springer, 2004.
- [EAM⁺05] MD Eisaman, A Andre, F Massou, M Fleischhauer, AS Zibrov, and MD Lukin. Electromagnetically induced transparency with tunable single-photon pulses. *Nature*, 438(7069):837–841, December 2005.
- [ELAB09] David Elkouss, Anthony Leverrier, Romain Alléaume, and Joseph Boutros. Efficient reconciliation protocol for discrete-variable quantum key distribution. In *IEEE International Symposium on Information Theory, ISIT 2009*, pages 1879–1883, July 2009.
- [FS09] Serge Fehr and Christian Schaffner. Composing quantum protocols in a classical environment. In *Theory of Cryptography Conference (TCC)*, volume 5444 of *Lecture Notes in Computer Science*, pages 350–367. Springer, 2009.
- [idQ] idQuantique. at <http://www.idquantique.com>.
- [JSC⁺04] B Julsgaard, J Sherson, JI Cirac, J Fiurasek, and ES Polzik. Experimental demonstration of quantum memory for light. *Nature*, 432(7016):482–486, November 2004.
- [Kin03] C. King. The capacity of the quantum depolarizing channel. *IEEE Transactions on Information Theory*, 49(1):221–229, 2003.
- [KR07] Robert König and Renato Renner. Sampling of min-entropy relative to quantum knowledge. <http://arxiv.org/abs/0712.4291>, 2007.
- [KW09] Robert König and Stephanie Wehner. A strong converse for classical channel coding using entangled inputs. *Physical Review Letters*, 103(7):070504, 2009.
- [KWW09] Robert König, Stephanie Wehner, and Jürg Wullschleger. Unconditional security from noisy quantum storage. <http://arxiv.org/abs/0906.1030>, 2009.
- [LC97] Hoi-Kwong Lo and Hoi Fung Chau. Is quantum bit commitment really possible? *Physical Review Letters*, 78(17):3410–3413, April 1997.

- [Lo97] Hoi-Kwong Lo. Insecurity of quantum secure computations. *Physical Review A*, 56(2):1154–1162, 1997.
- [Mag] MagicQ. at <http://www.magicqtech.com/>.
- [May95] Dominic Mayers. On the security of the quantum oblivious transfer and key distribution protocols. In *Advances in Cryptology—CRYPTO '95*, volume 963 of *Lecture Notes in Computer Science*, pages 124–135. Springer, 1995.
- [May97] Dominic Mayers. Unconditionally secure quantum bit commitment is impossible. *Physical Review Letters*, 78(17):3414–3417, April 1997.
- [NOVY98] Moni Naor, Rafail Ostrovsky, Ramarathnam Venkatesan, and Moti Yung. Perfect zero-knowledge arguments for p using any one-way permutation. *Journal of Cryptology*, 11(2):87–108, 1998.
- [Ren05] Renato Renner. *Security of Quantum Key Distribution*. PhD thesis, ETH Zürich (Switzerland), September 2005. <http://arxiv.org/abs/quant-ph/0512258>.
- [RSA78] R. L. Rivest, A. Shamir, and L. Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Commun. ACM*, 21(2):120–126, 1978.
- [Sav07] George Savvides. *Interactive Hashing and reductions between Oblivious Transfer variants*. PhD thesis, School of Computer Science, McGill University, Montréal, Canada, 2007.
- [Sch07] Christian Schaffner. *Cryptography in the Bounded-Quantum-Storage Model*. PhD thesis, University of Aarhus, 2007. <http://arxiv.org/abs/0709.0289>.
- [Sma] SmartQuantum. at <http://www.smartquantum.com>.
- [SP00] Peter W. Shor and John Preskill. Simple proof of security of the BB84 quantum key distribution protocol. *Physical Review Letters*, 85(2):441–444, July 2000.
- [STW09] Christian Schaffner, Barbara M. Terhal, and Stephanie Wehner. Robust cryptography in the noisy-quantum-storage model. *Quantum Information & Computation*, 9(11&12):963–996, 2009.
- [Tho83] Christian Thommesen. The existence of binary linear concatenated codes with Reed-Solomon outer codes which asymptotically meet the Gilbert-Varshamov bound. *IEEE Transactions on Information Theory*, 29(6):850–853, 1983.
- [WCSL10] Stephanie Wehner, Marcos Curty, Christian Schaffner, and Hoi-Kwong Lo. How to implement two-party protocols in the noisy-storage model. <http://arxiv.org/abs/0911.2302>, to appear in PRA, 2010.
- [WST08] Stephanie Wehner, Christian Schaffner, and Barbara M. Terhal. Cryptography from noisy storage. *Physical Review Letters*, 100(22):220502, 2008.
- [Wul07] Jürg Wullschleger. Oblivious-Transfer amplification. In *Advances in Cryptology—EUROCRYPT '07*, volume 4515 of *Lecture Notes in Computer Science*. Springer, 2007.

- [WW08] Stephanie Wehner and Jürg Wullschleger. Composable security in the bounded-quantum-storage model. In *Automata, Languages and Programming, 35th International Colloquium, ICALP 2008*, volume 5126 of *Lecture Notes in Computer Science*, pages 604–615. Springer, 2008.
- [Yao95] Andrew Chi-Chih Yao. Security of quantum protocols against coherent measurements. In *27th Annual ACM Symposium on the Theory of Computing (STOC)*, pages 67–75, 1995.