This is a repository copy of *Error-tolerant oblivious transfer in the noisy-storage model*.

White Rose Research Online URL for this paper:
https://eprints.whiterose.ac.uk/205777/

Version: Published Version

Error-tolerant oblivious transfer in the noisy-storage model

Cosmo Lupo [1,2] James T. Peat [3] Erika Andersson,[3] and Pieter Kok [4]

[1]*Dipartimento Interateneo di Fisica, Politecnico di Bari & Università di Bari, 70126 Bari, Italy*
[2]*INFN, Sezione di Bari, 70126 Bari, Italy*
[3]*SUPA, Institute of Photonics and Quantum Sciences, School of Engineering and Physical Sciences,*
Heriot-Watt University, EH14 4AS Edinburgh, United Kingdom
[4]*Department of Physics and Astronomy, The University of Sheffield, S3 7RH Sheffield, United Kingdom*

The noisy-storage model of quantum cryptography allows for information-theoretically secure two-party computation based on the assumption that a cheating user has at most access to an imperfect, noisy quantum memory, whereas the honest users do not need a quantum memory at all. In general, the more noisy the quantum memory of the cheating user, the more secure the implementation of oblivious transfer, which is a primitive that allows universal secure two-party and multiparty computation. For experimental implementations of oblivious transfer, one has to consider that also the devices held by the honest users are lossy and noisy, and error correction needs to be applied to correct these trusted errors. The latter are expected to reduce the security of the protocol, since a cheating user may hide themselves in the trusted noise. Here we leverage entropic uncertainty relations to derive tight bounds on the security of oblivious transfer with a trusted and untrusted noise. In particular, we discuss noisy storage and bounded storage, with independent and correlated noise.

I. INTRODUCTION

Two-party computation denotes a family of problems whose goal is to allow two users, Alice and Bob, who do not trust each other, to evaluate a function of two arguments, $f(x, y)$, where Alice provides x and Bob provides y. Informally, the protocol is secure if no more information leaks to Alice about y, or to Bob about x, than what they can infer from the value of $f(x, y)$. For example, x and y are n-bit strings and $f(x, y) = x \cdot y$, where $\cdot$ is the scalar product modulo 2. Neither Alice nor Bob will always be able to infer both x and y from $f(x, y)$ and their respective inputs x or y. In a highly influential paper [1], Kilian showed that the ability to perform oblivious transfer (OT) securely is sufficient for two-party computation. In OT, a receiver (Bob) of two incoming bits sent by Alice can read out exactly one of them, thereby making the readout of the other bit impossible. The protocol is secure if Bob obtains no information about the other bit, and if Alice does not know which of the two bits is learned by Bob. Specifically, this is known as 1-out-of-2 OT (1-2 OT) [2]. While OT has been formulated in a number of different flavors [3–5], we focus on 1-out-of-2 randomized oblivious string transfer (1-2 ROT$^\ell$). Other important primitives are bit commitment (BC) and weak string erasure (WSE). Both OT and BC can be obtained from WSE [6].

Implementation of two-party computation with computational security leverages the complexity of solving some hard mathematical problems, e.g., factoring [1,6]. Quantum mechanics cannot help in making two-party computation unconditionally secure [7,8]. However, information-theoretic security can be achieved if the users have constrained capabilities, for example, if they have access only to a limited pool of quantum resources. This may happen if the users have no quantum memory [9–11], or if they have an imperfect quantum memory that can store only a limited number of qubits, for a limited time [12,13], or with nonunit fidelity. The assumption of a quantum memory with limited capacity is known as the *bounded quantum storage model* [5,14,15]. In general, the memory can be bounded and noisy, in which case one refers to the *noisy-storage model* [6,16–18]. Protocols that achieve OT, BC, and WSE within the noisy-storage model have been discussed in detail in Refs. [5,6,14–21] and demonstrated experimentally [22,23]. In general, experimental implementations of two-party computation are more demanding than quantum key distribution (QKD). This is essentially due to the fact that users of two-party computation do not trust each other, which places limits on how they can cooperate. However, Refs. [5,6,14–23] have shown that primitives such as OT and BC are nevertheless feasible and secure within the noisy-storage model. Device-independent OT can also be achieved by invoking suitable assumptions [24,25]. Otherwise, without imposing any constraint on the users' resources, two-party computation can be implemented with partial security. In this latter case, one aims at computing bounds on the probability of successful cheating of a dishonest user; see, e.g., Refs. [26,27] and references therein.

In this paper we analyze the security of OT within the noisy-storage model. We focus on the protocol of Damgård *et al.* [5], which in turn is based on the same building blocks as the well-known BB84 protocol of QKD developed by Bennett and Brassard in 1984 [28]. Building on previous results from Refs. [6,20], we derive tighter entropic uncertainty relations and quantify the security of OT in terms of the conditional min-entropy. Compared with previous works, we extend the region of experimental parameters that allows for secure OT, and improve the trade-off between trusted noise (from the devices of the honest users) and noise in the quantum memory of a cheating user. We show that, in order to achieve secure OT, the overall trusted noise should be below $\simeq 22\%$, for a noisy but unbounded quantum memory, and that this value decreases with decreasing noise in the quantum memory.

The paper is organized as follows. We start in Sec. II by recalling the implementation of 1-2 ROT$^\ell$ of Ref. [5], including measures to make it robust to loss and noise [8,16,17]. The security of this protocol in the noisy-storage model is discussed in Sec. III. In Sec. IV we review the entropic uncertainty relations derived in Refs. [5,6,20] and their application to prove the security of OT. We leverage these results to obtain new, tighter entropic bounds in Sec. V. In Sec. VI, these new bounds are applied to characterize the security of noise-resilient OT and to determine the trade-off between trusted and untrusted noise. In Sec. VII we discuss a quantum memory with correlated noise, showing that the new bounds are particularly advantageous in this case. Finally, conclusions are presented in Sec. VIII.

II. OBLIVIOUS TRANSFER

In this paper we focus on the task of 1-2 ROT$^\ell$, i.e., 1-out-of-2 randomized oblivious string transfer, and on the protocol introduced by Damgård *et al.* [5]. In 1-2 ROT$^\ell$, the sender Alice outputs two random strings, each of ℓ bits. The receiver Bob outputs only one of these strings, chosen at random. The task is executed securely if (sender security) Bob gets little or no information about the other string and (receiver security) Alice does not know which string has been obtained by Bob. The task can be realized using BB84 operations [5], where Alice randomly prepares states using two conjugate bases, and Bob independently measures in either basis. Bob makes a single choice of basis in which he measures all the physical bits received.

Furthermore, the protocol can be made resilient to noise by adding a layer of error correction [16]. We need to use some care when dealing with error correction in two-party computation since, in contrast to QKD, here Alice and Bob do not trust each other. Therefore they cannot cooperate to estimate the loss and noise in the communication channel and in their devices, as they would do in QKD.

Remark 1. To implement error correction in two-party computation, the loss and noise need to be well characterized before running the protocol. This includes errors in the communication channels and in the devices held by the honest users.

This is a nontrivial requirement. Note that if the users exploit a trusted third party to certify the level of noise, then they can also implement OT using said trusted third party with a classical protocol.

In view of photonic applications, and following Refs. [8,16,17], it makes sense to treat loss and noise in two different ways. To deal with photon loss, Alice and Bob first need to agree on a common time reference, which allows them to time-tag each photon sent by Alice. If Bob is honest, he will measure each photon as soon as he gets it, and will confirm receipt to Alice. Only the photons that made it to Bob will be actually used for the protocol. All the other, lost photons will be disregarded [29]. Photons that are eventually detected by Bob may still be subject to noise in their internal degrees of freedom. To deal with this noise, Alice will send an error syndrome to allow Bob to error-correct.

The error-tolerant protocol is as follows [16].

(i) Alice randomly chooses the binary values $x'_j \in \{0, 1\}$ and $\theta'_j \in \{0, 1\}$, for $j = 1, 2, \ldots, n'$. According to the agreed time reference, at the jth time Alice prepares and sends to Bob the state $|x'_j, \theta'_j\rangle = H^{\theta'_j}|x'_j\rangle$, where $|x'_j\rangle \in \{|0\rangle, |1\rangle\}$ is an element of the computational basis and H is the Hadamard gate.

(ii) Bob randomly chooses a bit value $B \in \{0, 1\}$ and measures all the qubits he receives in the basis $\{H^B|0\rangle, H^B|1\rangle\}$.

(iii) Due to photon loss and detection inefficiency, some of the qubits are erased. Bob keeps track of the timings when no photon is detected and communicates this information to Alice. Only the bit values associated with the photons detected are retained for the rest of the protocol. If n photons are detected, this identifies the substrings $X = x_1, \ldots, x_n$ and $\Theta = \theta_1, \ldots, \theta_n$ associated with Alice's binary values and basis choices. On Bob's side, he keeps track of the bit values measured in the basis of his choice, $Y = y_1, \ldots, y_n$.

(iv) The overall loss is described by an attenuation factor $\eta \in (0, 1)$, which is the probability that a photon is detected by Bob. As stated above, the honest users know the expected value of this parameter. The protocol aborts if such a value is not compatible with the empirical loss factor n/n' and, within statistical errors, independent of the state prepared by Alice.

(v) The protocol pauses for a waiting time Δt, counted from when Bob is expected to receive the last photon.

(vi) Alice announces her basis choices. This corresponds to revealing two subsets of indices $\mathcal{I}_0, \mathcal{I}_1$, where $\mathcal{I}_C = \{j \mid \theta_j = C\}$. She also announces a pair of hash functions F_0 and F_1 from n to ℓ, and the syndrome vectors $\Sigma_0 = \mathrm{syn}(X_0)$ and $\Sigma_1 = \mathrm{syn}(X_1)$, where X_C is the substring of X restricted to the indices in $\mathcal{I}_C$. Similarly, one defines Bob's substrings Y_0 and Y_1. The syndrome vectors are obtained in order to allow Bob to correct the errors in his local string.

(vii) Alice outputs two strings of ℓ bits, $S_0 = F_0(X_0)$ and $S_1 = F_1(X_1)$ [30].

(viii) Bob uses the syndrome Σ_B to correct the errors in Y_B and retrieve $\widetilde{X}_B$. Finally, he applies the corresponding hash function and outputs $\widetilde{S}_B = F_B(\widetilde{X}_B)$.

Remark 2. Note the role of the waiting time Δt. If Bob is honest, he will measure as soon as he receives the photons. If Bob is dishonest, and is storing the received qubits in a quantum memory, the waiting time will give some guarantees to Alice that Bob's quantum memory has at least partially decohered.

Remark 3. If the users are honest, then the protocol implements 1-2 ROT$^\ell$ correctly, up to a probability ϵ_{EC} that error correction fails. Successful error correction means $\widetilde{X}_B = X_B$ and $\widetilde{S}_B = S_B$.

III. SECURITY OF THE PROTOCOL

The security analysis can be found in the literature [5,16] and is based on the following assumptions.

(1) Users have full knowledge and control of their own devices.

(2) Users have access to a noisy quantum memory. (The security analysis relies on modeling the noise in the quantum memory. Below we make use of a few explicit models.).

(3) Loss and noise in the communication line and in the devices held by honest users are known publicly.

Assumption 1 puts this protocol in the framework of device-dependent cryptography. Assumption 2 is the core assumption of the noisy-storage model. Assumption 3 is necessary to allow for error correction. Furthermore, when analyzing the security we need to consider that only one user is cheating (either Alice or Bob) and the other is honest, since the OT protocol is designed to protect at least one honest user. Receiver security is for Bob when Alice is cheating. Sender security is for Alice when Bob is cheating.

Receiver security follows from the fact that physical qubits only travel from Alice to Bob. Note that there is some information flowing from Bob to Alice, due to the fact that Bob needs to confirm which photons have arrived. However, if Bob has full control over his device (from assumption 1) and behaves honestly (here we are considering the case where it is Alice who may cheat), this information cannot be used by Alice to guess the value of B. In fact, the data sent from Bob to Alice are only to confirm receipt of a photon, and do not convey any information about its internal degrees of freedom. Information about the state of the received photons may leak to Alice only if Bob's device is compromised.

Sender security relies on the noisy-storage assumption. The parameter ℓ depends on the amount of noise that affects dishonest Bob's quantum storage during the waiting time Δt. It also depends on the trusted noise, as some information will leak through the error syndromes. Consider first the ideal case where error correction is not needed (i.e., there is no noise for honest users); ℓ is estimated from the leftover hash lemma and expressed in terms of the smooth min-entropy [31]

$$\ell \geqslant H_{\min}^{\epsilon_s}(X_{1-B}|\mathcal{F}(Q)\Theta B) - 2\log_2 \frac{1}{\epsilon_h} + 1, \qquad (1)$$

where Q is the quantum information stored in the memory and $\mathcal{F}$ is the map that describes the noisy storage for time Δt. Such a value for ℓ, if larger than zero, would ensure that the dishonest receiver cannot do much more than a random guess to determine the value of the complementary string X_{1-B}. Quantitatively, the probability that the string remains unknown is given by the sum of the smoothing and hashing parameters, $\epsilon_s + \epsilon_h$. However, noise also affects the honest users; therefore we need to employ error correction. In turn, this reduces the value of ℓ, as a cheating receiver can in principle leverage the syndrome Σ_{1-B} to acquire more information about the complementary bit string,

$$\ell \geqslant H_{\min}^{\epsilon_s}(X_{1-B}|\mathcal{F}(Q)\Theta B \Sigma_{1-B}) - 2\log_2 \frac{1}{\epsilon_h} + 1 \qquad (2)$$

$$\geqslant H_{\min}^{\epsilon_s}(X_{1-B}|\mathcal{F}(Q)\Theta B) - |\Sigma_{1-B}| - 2\log_2 \frac{1}{\epsilon_h} + 1, \quad (3)$$

where in the second line we have applied a chain rule and $|\Sigma_{1-B}|$ is the size of the syndrome in bits. In principle, security is achieved whenever $\ell > 0$, for sufficiently small values of $\epsilon_s + \epsilon_h$. Note that $\mathcal{F}(Q)$ is the quantum information in the noisy quantum memory, at the time when the basis information Θ^n is obtained by Bob.

Both the min-entropy and the length of the syndromes can be computed given a suitable model for the noisy storage. This will be discussed in detail in the next section.

Remark 4. Alice needs to run a statistical test to check that empirical attenuation factors are compatible with the expected value. Such a test is probabilistic and can fail with a probability ϵ_{test}, which contributes to the security parameter of the protocol.

In conclusion, if the protocol does not abort, it correctly implements 1-2 ROT$^\ell$ up to a failure probability ϵ_{EC}. The implementation is secure against a dishonest receiver with noisy storage up to a probability $\epsilon_s + \epsilon_h + \epsilon_{test}$.

IV. REVIEW OF ENTROPIC BOUNDS

In this section we review a few *entropic uncertainty relations* that have been used in the literature to prove the security of 1-2 ROT$^\ell$ [5,6,20], in particular to establish sender security. In fact, an entropic uncertainty relation can be applied to obtain a lower bound on the uncertainty of Bob in guessing the other string.

As a first step, consider a simplified scenario where Bob does not have any quantum memory. Therefore he is forced to measure the quantum states as soon as he obtains them. If the protocol passes the statistical test, we focus on the n photons that have been tagged as received. Alice has encoded the variables X into their quantum states, using the BB84 encoding scheme with two conjugate bases. After the waiting time Δt, Alice has announced her basis choices Θ. It is crucial, in this scenario, that Bob has already measured his quantum states when this basis information is revealed. For example, this could happen because Bob has no quantum memory at all, or a quantum memory that is completely decohered after the waiting time Δt. In either case, Bob is expected to have already measured the states when he receives the basis information, that is, he has no quantum side information to rely upon. In this scenario, the following entropic bound applies [5]:

$$H_{\min}^{\epsilon}(X|\Theta) \geqslant \left(\tfrac{1}{2} - 2\lambda\right)n, \qquad (4)$$

where the parameter λ can be chosen in the open interval $(0, 1/2)$ such that

$$\epsilon = \exp\left[-\frac{\lambda^2 n}{32(\log_2(4/\lambda))}\right]. \qquad (5)$$

To make things more interesting, consider that a cheating receiver, when obtaining the basis information, still has $q = \nu n$ qubits stored in its quantum memory Q, which he has

not measured yet. In this case we have

$$H_{\min}^\epsilon(X|Q\Theta) \geqslant H_{\min}^\epsilon(X|\Theta) - q \qquad (6)$$

$$\geqslant \left(\tfrac{1}{2} - 2\lambda\right)n - q \qquad (7)$$

$$= \left(\tfrac{1}{2} - \nu - 2\lambda\right)n, \qquad (8)$$

where the first inequality follows from the chain rule. The parameter $\nu \in (0, 1)$ represents the quantum storage rate. Asymptotically in n, the bound in Eq. (8) is nontrivial for $\nu < 1/2$, i.e., when a cheating receiver can store no more that one-half of the qubits [32].

A. Noisy storage

In the case of noisy storage, the qubits stored in the quantum memory are partially degraded. To analyze the security of OT in this scenario, we need to specify a model for the noisy quantum memory, described by the quantum channel $\mathcal{F}$. Consider a quantum memory where each qubit is subject to independent and identically distributed (i.i.d.) noise. For example, each qubit undergoes depolarizing noise

$$\rho \to r\rho + (1 - r)I/2, \qquad (9)$$

which maps ρ into the maximally mixed state with probability $1 - r$ and leaves it untouched with probability r.

Note that a cheating receiver does not know if a particular qubit has been depolarized or not. However, if we give him this additional information, we are making his quantum memory less noisy. In turn, this means that his uncertainty about the string can only decrease [6,33]. On average, if $q = \nu n$ are stored in the quantum memory, about $r\nu n$ of them are preserved without noise, whereas the remaining $(1 - r)\nu n$ are completely depolarized. Therefore, starting from (8), we obtain the following lower bound on the min-entropy (asymptotically in n):

$$H_{\min}^\epsilon(X|\mathcal{F}(Q)\Theta) \geqslant \left(\tfrac{1}{2} - r\nu - 2\lambda\right)n. \qquad (10)$$

For large n, this is a nontrivial bound as long as $r\nu < 1/2$ [32].

The bound can be improved using the notion of the *strong converse* of a quantum channel for sending classical information [6,34]. Given that the noisy quantum memory is described by a map $\mathcal{F}$ applied to the qubits stored in the quantum memory, the ability of this channel to preserve (classical) information is quantified by

$$P_{\text{succ}}^{\mathcal{F}}(nR) = \max_{\{\rho_x, D_x\}_x} \frac{1}{2^{nR}} \sum_{x \in \{0,1\}^{nR}} \text{Tr}[D_x \mathcal{F}(\rho_x)], \qquad (11)$$

which is the maximum achievable (average) guessing probability, where the maximization is over encoding states ρ_x and decoding positive operator-valued measure (POVM) D_x, given a bit rate of R bits per qubit. The bound of König *et al.* [6] reads

$$H_{\min}^{\epsilon+\epsilon'}(X|\mathcal{F}(Q)\Theta) \geqslant -\log_2 P_{\text{succ}}^{\mathcal{F}}\left(H_{\min}^\epsilon(X|\Theta) - \log_2 \frac{1}{\epsilon'}\right). \qquad (12)$$

If the channel $\mathcal{F} = \mathcal{N}^{\otimes n}$ is i.i.d., then the entropic bound can be written explicitly for any $R > C_\mathcal{N}$, where $C_\mathcal{N}$ is the strong-converse capacity of the channel $\mathcal{N}$, and if the error
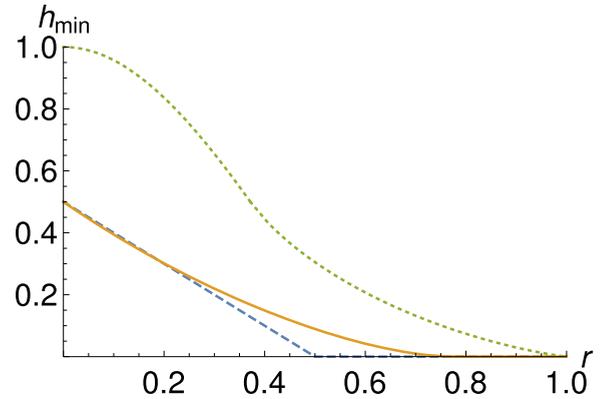

FIG. 1. Min-entropy rate vs the depolarizing channel parameter. Dashed blue line, computed from Eq. (10) with $\nu = 1$; solid orange line, computed from Eq. (19); dotted green line, computed from Eq. (29).

exponent $\gamma(R)$ is known such that

$$P_{\text{succ}}^{\mathcal{N}^{\otimes n}}(nR) \leqslant 2^{-n\gamma(R)}. \qquad (13)$$

Note that, if a strong converse exists, then $\gamma(R) > 0$ for any $R > C_\mathcal{N}$.

For $\mathcal{N}$ being the depolarizing channel in Eq. (9), the strong-converse capacity is [34]

$$C_\mathcal{N} = 1 - h\left(\frac{1 + r}{2}\right), \qquad (14)$$

where

$$h(x) := -x\log_2 x - (1 - x)\log_2(1 - x) \qquad (15)$$

is the binary Shannon entropy, and the error exponent is

$$\gamma_r(R) = 1 + \max_{\alpha > 1}$$
$$\times \frac{(\alpha - 1)(R - 1) - \log_2[(1 + r)^\alpha + (1 - r)^\alpha]}{\alpha}. \qquad (16)$$

This yields the entropy bound

$$H_{\min}^{\epsilon+\epsilon'}(X|\mathcal{F}(Q)\Theta) \geqslant n\gamma_r\left(\frac{H_{\min}^\epsilon(X|\Theta) - \log_2(1/\epsilon')}{n}\right). \qquad (17)$$

Using Eq. (4), we obtain

$$H_{\min}^{\epsilon+\epsilon'}(X|\mathcal{F}(Q)\Theta) \geqslant n\gamma_r\left(\frac{1}{2} - 2\lambda - \frac{1}{n}\log_2\frac{1}{\epsilon'}\right). \qquad (18)$$

For n that is sufficiently large, we obtain a bound on the asymptotic entropy rate (note that this rate, as well as all the entropy rates computed in this paper, is expressed in bits per photon received)

$$h_{\min} = \lim_{n \to \infty} \frac{1}{n} H_{\min}^{\epsilon+\epsilon'}(X|\mathcal{F}(Q)\Theta) \geqslant \gamma_r(1/2), \qquad (19)$$

which is a nontrivial bound for all values of r such that $C_\mathcal{N} < 1/2$.

Figure 1 shows a comparison of the asymptotic entropy rate $h_{\min}$ for the depolarizing channel, computed from Eq. (10) with $\nu = 1$ (dashed blue line) and from Eq. (19) (solid orange line). This shows that Eq. (19) is generally tighter for the

depolarizing-noise channel but Eq. (10) is tighter for small values of the depolarizing parameter r, though with a relatively small gap.

For simplicity, for most of the rest of this paper we assume $\nu = 1$. The general case of bounded storage ($\nu < 1$) will be discussed in Sec. VI.

B. Uncertainty relations for any amount of noise

As we have seen for the depolarizing channel, the entropic bounds we have obtained become trivial if the channel is not sufficiently noisy. This goes against our physical intuition, which suggests that even a relatively weak noise may wipe at least some information. In this section we review an entropy bound, obtained by Dupuis *et al.* [20], which is nontrivial even for low-noise quantum memory.

To write down this entropic bound explicitly, first consider a purification of the BB84-like protocol where Alice prepares n copies of the maximally entangled two-qubit states Ψ, and sends to Bob one qubit from each pair. To these states, which are stored in cheating Bob's quantum memory, a certain noisy channel is applied, yielding the $2n$-qubit state

$$\sigma_{AE} = \mathrm{id} \otimes \mathcal{F}(\Psi^{\otimes n}), \tag{20}$$

where id is the identity channel acting on the first qubit of each pair. The qubits on Alice's side are collectively indicated as A, and those stored in the quantum memory are indicated as $E = \mathcal{F}(Q)$.

The entropic bound is written in terms of the *collision entropy rate* of such a state:

$$h_2(\sigma) := \frac{1}{n} H_2(A|E)_\sigma. \tag{21}$$

Recall that the collision entropy of the bipartite state σ is defined as

$$H_2(A|E)_\sigma = -\log_2 \mathrm{Tr}\big[\big(\sigma_E^{-1/4} \sigma_{AE} \, \sigma_E^{-1/4}\big)^2\big], \tag{22}$$

where $\sigma_E = \mathrm{Tr}_A \sigma_{AE}$ is the reduced state obtained by partial tracing.

The following min-entropy bound is proven in Ref. [20]:

$$H_{\min}^\epsilon(X|E\Theta) \geqslant n\Gamma(h_2(\sigma)) - 1 - \log_2 \frac{2}{\epsilon^2}, \tag{23}$$

where the function Γ is defined as

$$\Gamma(x) = \begin{cases} x & \text{if} \quad x \geqslant 1/2 \\ g^{-1}(x) & \text{if} \quad x < 1/2 \end{cases} \tag{24}$$

and

$$g(y) = -y\log_2 y - (1-y)\log_2 (1-y) + y - 1. \tag{25}$$

If the noisy quantum memory is described by an i.i.d. depolarizing channel, then the state σ is a direct product, i.e., $\sigma = \tau^{\otimes n}$, with

$$\tau = r\Psi + (1-r)I/2 \otimes I/2, \tag{26}$$

and the collision entropy reads

$$h_2(\sigma) = -\log_2 2\mathrm{Tr}(\tau^2) = 1 - \log_2 (1 + 3r^2). \tag{27}$$

This yields

$$H_{\min}^\epsilon(X|\mathcal{F}(Q)\Theta) \geqslant n\Gamma[1 - \log_2 (1 + 3r^2)] - 1 - \log_2 \frac{2}{\epsilon^2}. \tag{28}$$

Note that, at least for n that is large enough, this bound remains nontrivial even when r is arbitrarily close to 1, with the asymptotic entropy rate

$$h_{\min} \geqslant \Gamma[1 - \log_2 (1 + 3r^2)]. \tag{29}$$

This is plotted in Figure 1 (dotted green line), showing that this latter bound supersedes those obtained in the previous sections.

V. IMPROVED MIN-ENTROPY BOUNDS

In this section we derive a new min-entropy bound using the uncertainty relation of Ref. [20]. The argument is analogous to the one used in Sec. IV A to obtain Eq. (10). The difference is that (10) was obtained from the uncertainty relation (4), whereas here our starting point is the uncertainty relation in Eq. (23). To obtain this bound, we assume that each qubit received by Bob is affected by identical and independent noise. As above, this qubit noise is modeled as a depolarizing channel.

Consider the depolarizing channel of Eq. (26), which preserves the state with probability r and completely depolarizes it with probability $1 - r$. Cheating Bob does not know whether a given qubit has been depolarized or not while stored in his quantum memory. However, if we give him this additional information, the depolarizing channel is replaced by the erasure channel:

$$\tau' = r\Psi + (1-r)I/2 \otimes \omega, \tag{30}$$

where ω is the erasure flag, which allows Bob to know if the state has been stored without error by applying a nondestructive measurement. Given that n_1 qubits have been preserved without error, and $n - n_1$ have been erased, the overall n-qubit state reads

$$\sigma' = \Psi^{\otimes n_1} \otimes (I/2 \otimes \omega)^{\otimes (n-n_1)}. \tag{31}$$

Assume Bob is given knowledge of which qubits have been erased. Denote by X^{n_1} the substring of bits corresponding to the qubit that have been preserved without noise, and by X^{n-n_1} the substring corresponding to the qubits that have been erased, with $X = X^{n_1} X^{n-n_1}$. We can then write a lower bound on the min-entropy:

$$H_{\min}^\epsilon(X|E\Theta) \geqslant H_{\min}^\epsilon(X^{n-n_1}|E\Theta) \tag{32}$$

$$\geqslant (n-n_1)\Gamma(h_2(\sigma'')) - 1 - \log_2 \frac{2}{\epsilon^2}, \tag{33}$$

where the first inequality comes from the fact that the entropy of a bit string is always larger than the entropy of a substring, the second inequality is an application of Eq. (23), and $\sigma'' = (I/2 \otimes \omega)^{\otimes (n-n_1)}$. Noting that $h_2(I/2 \otimes \omega) = 1$ and $\Gamma(1) = 1$, we obtain

$$H_{\min}^\epsilon(X|E\Theta) \geqslant n - n_1 - 1 - \log_2 \frac{2}{\epsilon^2}. \tag{34}$$
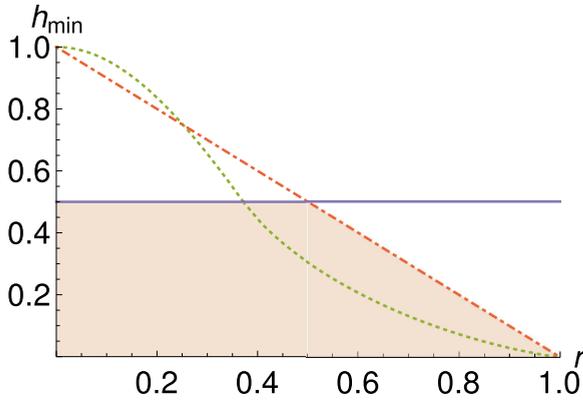
FIG. 2. Min-entropy rate vs the depolarizing noise parameter. Dotted green line, computed from Eq. (29) (same as shown in Fig. 1); dash-dotted red line, computed from Eq. (35). The best entropy rate for each value of r is obtained by taking the maximum of the two curves, as in Eq. (36). Solid blue line, min-entropy for the honest receiver, obtained from Eq. (4) in the limit of large n. If the receiver behaves rationally, his entropy rate is always above the shadowed region.

In the limit of large n, the number of virtually erased qubits is expected to be $n - n_1 \simeq (1 - r)n$. Therefore we obtain the bound on the asymptotic min-entropy rate

$$h_{\min} \geqslant 1 - r. \qquad (35)$$

This new bound is shown together with the previous one in Fig. 2. In conclusion, for the depolarizing channel, the best bound on the entropic rate obtained so far is

$$h_{\min} \geqslant \max\{\gamma[1 - \log_2(1 + 3r^2)], 1 - r\}. \qquad (36)$$

As shown in the figure, for smaller values of r (noisier quantum memory) the best bound is $h_{\min} = \gamma[1 - \log_2(1 + 3r^2)]$, whereas for higher values of r (less noisy quantum memory) the best bound is $h_{\min} = 1 - r$.

Optimal strategies for a dishonest receiver

The entropic bounds obtained so far allow us to estimate the uncertainty of the dishonest receiver in guessing Alice's string, as a function of the noise affecting the quantum memory. Recall that this is the noise describing the state of the qubits stored in the quantum memory when Bob obtains the basis information Θ. We suppose that Bob is not acting honestly, as according to the protocol he should measure the qubits as soon as he receives them. Equation (36) shows that the uncertainty increases with increasing noise in the quantum memory. Eventually, if the memory is too noisy, crime does not pay anymore, and being dishonest (i.e., Bob waiting for the basis announcement before measuring) is no longer the rational choice.

In fact, we know from Eq. (4) that the min-entropy rate for the honest receiver is $h_{\min} \geqslant 1/2$. Therefore dishonest behavior is no longer rational if the value on the right-hand side of Eq. (36) is larger than $1/2$. When the receiver acts

rationally and applies the best strategy, the entropy rate is

$$h_{\min} \geqslant \min\{1/2, \max\{\gamma[1 - \log_2(1 + 3r^2)], 1 - r\}\} \quad (37)$$

$$= \min\{1/2, 1 - r\}. \qquad (38)$$

In conclusion, for a rational receiver the entropy rate is always above the shadowed region in Fig. 2.

This result is indeed intuitive. Since the honest receiver can measure without error about 50% of the qubits, behaving honestly is the rational choice whenever the quantum memory corrupts more than 50% of the qubits. Therefore we expect the bound (38) to be tight if the memory is modeled as an erasure channel (with a flag), where $1 - r$ is the probability of erasing the qubit. However, for the depolarizing channel this bound is not expected to be tight, and there might be room for improvement.

VI. ERROR-TOLERANT OT

The entropic uncertainty relations of the previous sections can be directly applied to bound the uncertainty of the receiver Bob about the string X. Note, however, that for application to OT, we are interested in bounding the uncertainty of a cheating receiver, not about the whole string X, but only about the substring X_{1-B}. Therefore we need a lower bound on the min-entropy of X_{1-B}, as in Eq. (1). For large enough n, the substring X_{1-B} is expected to have size of about $n/2$ bits, which are randomly sampled from X. According to the min-entropy sampling discussed in Ref. [6], the min-entropy rate of a randomly chosen substring is the same as X, if n is large enough, up to finite-size corrections. Therefore in the asymptotic limit of large n we can use the min-entropy rates as obtained in the previous sections. To account for noise in their devices, Alice and Bob will also apply error correction, which further reduces the min-entropy as in Eq. (3).

We consider two scenarios, depicted in Figs. 3(a) and 3(b). In both scenarios, Alice's device introduces some noise during the phase of state preparation, and photon loss occurs in the transmission from Alice to Bob. In scenario 1, Bob's device is noisy and lossy, for example, due to nonunit detector efficiency. In scenario 2, Bob's devices is noiseless, and only affected by loss. In both cases, to simplify the analysis, we model all noises (in preparation and measurement) as depolarizing noise. Also, loss during state preparation and measurement is (with no loss of generality) associated with the communication channel. This is consistent as loss commutes with depolarizing noise. Let η indicate the total attenuation factor, accounting for loss in state preparation, transmission, and measurement (nonunit detection efficiency). As discussed above, to deal with loss, Alice needs to know the expected value of η, and she will abort the protocol if the empirical value is too different from the expected one given the statistical fluctuations.

In scenario 1, the total noise is obtained by combining two depolarizing channels (modeling preparation noise and measurement noise), yielding to an overall depolarizing channel with parameter

$$r_1 = r_{\text{pre}} r_{\text{mea}}. \qquad (39)$$

(a) Honest receiver, scenario 1

(b) Honest receiver, scenario 2
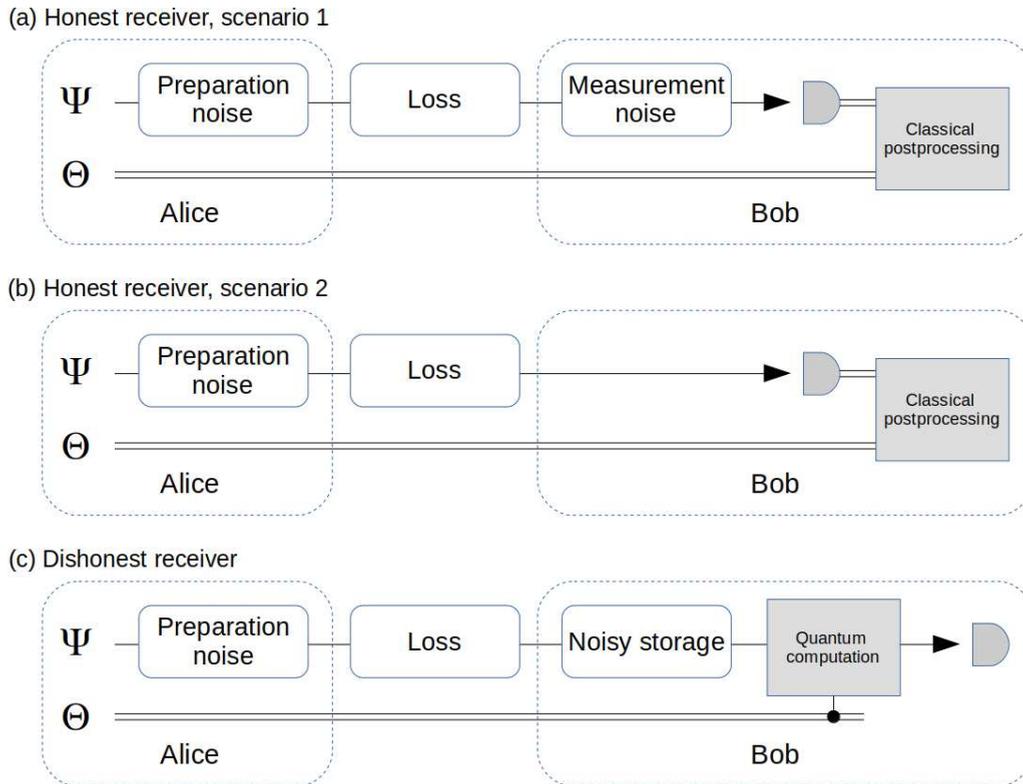

(c) Dishonest receiver

FIG. 3. Preparation noise is associated with the sender (Alice) station. Losses, including those occurring during the preparation phase and due to detector inefficiencies, are associated with the communication channel between Alice and Bob. (a) In scenario 1, honest receiver Bob measures the quantum states as soon as he gets them, using a noisy measurement apparatus. (b) In scenario 2, the honest receiver's measurement apparatus has negligible noise. (c) A cheating receiver holds the quantum states in a noisy quantum memory until he receives the basis information from Alice.

Scenario 2 is less noisy, and depolarization is only due to the preparation phase,

$$r_2 = r_{\text{pre}}. \qquad (40)$$

These relations hold for the honest receiver in the two scenarios. If the receiver is dishonest and stores the qubits in a quantum memory, from his point of view the noise in the quantum memory combines with the noise in the preparation phase, as shown in Fig. 3(c). As above, we model the noisy storage as a depolarizing channel with parameter r_{mem}. This means that the dishonest receiver will experience a total depolarizing noise with parameter

$$r_{\text{dis}} = r_{\text{pre}} r_{\text{mem}}. \qquad (41)$$

Note that $r_{\text{dis}} = r_2 r_{\text{mem}} \leqslant r_2$, and scenario 2 is more advantageous for the honest users, as the noise experienced by the cheating receiver is always larger than that experienced by the honest one.

For each scenario, the amount of error-correcting information per channel use is asymptotically equal to

$$h_{\text{EC}} = h\left(\frac{1 + r_j}{2}\right), \qquad (42)$$

for $j = 1, 2$ according to the scenario considered. From this we can compute the asymptotic communication rates, measured in bits per channel use, using Eq. (3). For scenario 1 we

obtain

$$b := \lim_{n \to \infty} \ell/n = \min\left\{1/2, \, 1 - r_{\text{dis}}\right\} - h\left(\frac{1 + r_1}{2}\right). \qquad (43)$$

The top panel of Fig. 4 shows the contour plot of the bit rate. The protocol is secure for values of r_{dis} and r_1 above the shadowed region. The figure also shows how this result improves on existing literature. The green dotted line and the orange dashed line are the boundaries between the regions of secure and nonsecure OT obtained from Eq. (19) and Eq. (29), respectively. In particular, for a rational receiver we obtain from Eq. (19) the bit rate

$$\min\left\{1/2, \, \gamma_{r_{\text{dis}}}(1/2)\right\} - h\left(\frac{1 + r_1}{2}\right). \qquad (44)$$

Similarly, from Eq. (29) we obtain

$$\min\left\{1/2, \, \Gamma\left[1 - \log_2\left(1 + 3r_{\text{dis}}^2\right)\right]\right\} - h\left(\frac{1 + r_1}{2}\right). \qquad (45)$$

For scenario 2, we can use r_{mem} as an independent variable, and the asymptotic rate is

$$b = \min\left\{1/2, \, 1 - r_2 r_{\text{mem}}\right\} - h\left(\frac{1 + r_2}{2}\right). \qquad (46)$$

The contour plot for this bound is shown in the bottom panel of Fig. 4, where secure OT is achieved above the shadowed
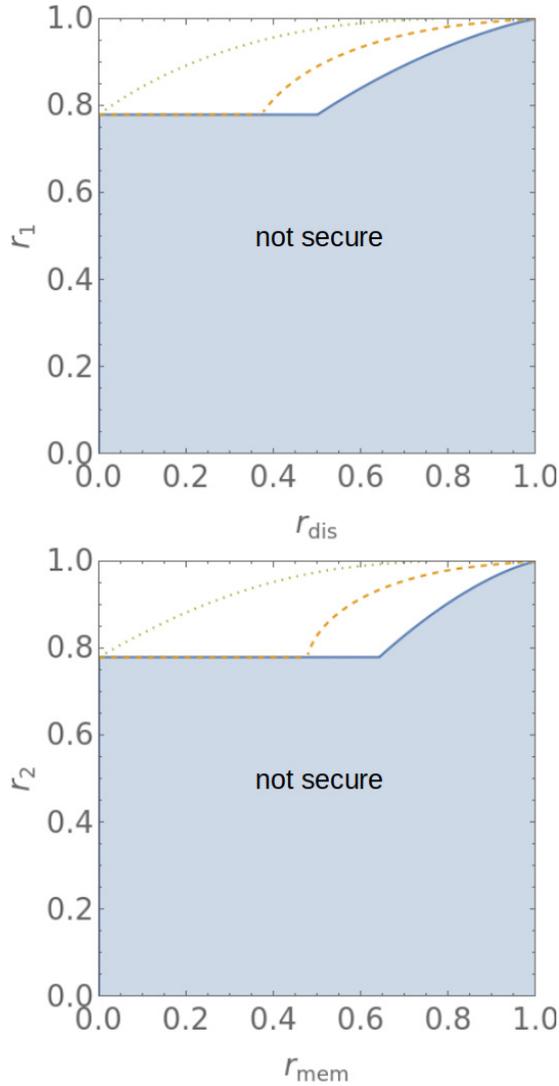
FIG. 5. Scenario 2, for $r_{\mathrm{mem}} = 0$. This refers to a noiseless yet bounded quantum memory, with storage rate ν. The shadowed region corresponds to where the protocol is not secure in the ν-r_2 plane, where r_2 is the trusted noise parameter.

$1/2$, i.e., $r_j \gtrsim 0.78$. This corresponds to a maximum tolerable trusted noise of about 22%.

Bounded storage

In case of noisy and bounded storage, suppose that the cheating receiver can at most store a fraction of the received qubits, quantified by the quantum storage rate ν. Equation (36) is thus replaced by

$$h_{\min} \geqslant \frac{1-\nu}{2} + \nu \max\{\gamma[1 - \log_2(1 + 3r^2)], 1 - r\}. \quad (49)$$

For a rational receiver, Eq. (38) is replaced by

$$h_{\min} \geqslant \frac{1-\nu}{2} \quad (50)$$
$$+ \nu \min\{1/2, \max\{\gamma[1 - \log_2(1 + 3r^2)], 1 - r\}\}$$
$$= \frac{1-\nu}{2} + \nu(1-r) = 1/2 + \nu(1/2 - r). \quad (51)$$

Finally, the asymptotic rate for scenario 1 becomes

$$b = \min\{1/2, 1/2 + \nu(1/2 - r_{\mathrm{dis}})\} - h\left(\frac{1+r_1}{2}\right). \quad (52)$$

Similarly for scenario 2 we obtain

$$b = \min\{1/2, 1/2 + \nu(1/2 - r_2 r_{\mathrm{mem}})\} - h\left(\frac{1+r_2}{2}\right). \quad (53)$$

Let us consider in more detail scenario 2. In the case of noiseless but bounded quantum memory, we put $r_{\mathrm{mem}} = 1$, and the bit rate becomes

$$b = \min\{1/2, 1/2 + \nu(1/2 - r_2)\} - h\left(\frac{1+r_2}{2}\right). \quad (54)$$

Figure 5 shows the region where the rate vanishes in the ν-r_2 plane. For ν approaching zero we recover the threshold

FIG. 4. Top: scenario 1. Secure OT can be achieved above the shadowed region in the r_{dis}-r_1 plane. Bottom: scenario 2. Secure OT can be achieved above the shadowed region in the r_{mem}-r_2 plane. For comparison with previous results from Refs. [6,20], the dotted green line shows the boundary between secure and nonsecure regions that would be obtained using the min-entropy bound of Eq. (19) [see Eqs. (44) and (47)]. The orange dashed line is the boundary that would be obtained from the min-entropy rate in Eq. (29) [see Eqs. (45) and (48)].

region in the r_{mem}-r_2 plane. The figure also shows the boundary between regions corresponding to secure and nonsecure OT that would be obtained using the min-entropy bounds in Eqs. (19) and (29). The latter are computed from the bit rates

$$\min\{1/2, \gamma_{r_2 r_{\mathrm{mem}}}(1/2)\} - h\left(\frac{1+r_2}{2}\right), \quad (47)$$

$$\min\{1/2, \Gamma[1 - \log_2(1 + 3(r_2 r_{\mathrm{mem}})^2)]\} - h\left(\frac{1+r_2}{2}\right). \quad (48)$$

Note that scenario 2 is always more advantageous for the honest users, but in both cases secure OT is possible only if the trusted noise parameter r_j is such that $h((1+r_j)/2) \leqslant$
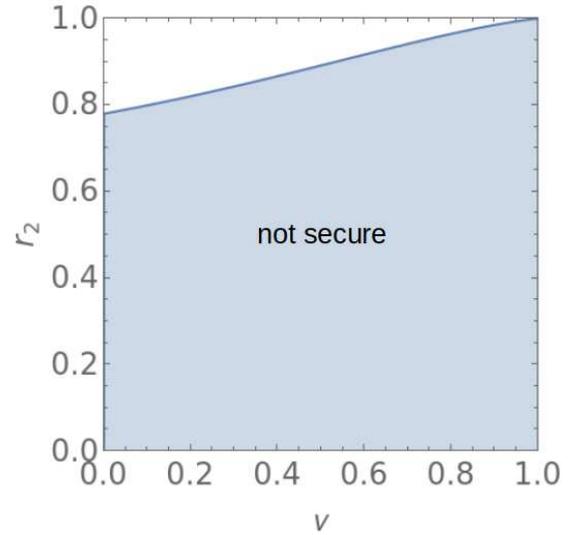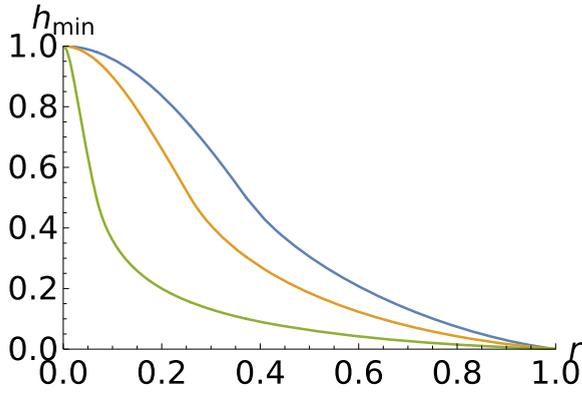
FIG. 6. Min-entropy bound in Eq. (57) plotted vs the noise parameter r. Shown for different values of the correlation parameter m. From top to bottom, the curves are obtained for $m = 1, 2, 5$.

of 22% trusted noise. This threshold value decreases nearly linearly with increasing ν.

VII. CORRELATED NOISE

In this section we discuss the case of quantum memory affected by correlated noise [35]. We consider a model of burst errors where $m > 1$ neighbor qubits are collectively depolarized. The integer m plays the role of a correlation parameter. Given m copies of the maximally entangled two-qubit states Ψ, this model is represented by the map

$$\Psi^{\otimes m} \rightarrow \sigma_{AE} = r\Psi^{\otimes m} + 2^{-2m}(1-r)I^{\otimes 2m}, \qquad (55)$$

which replaces (26). To compute the bound in Eq. (23), we first need to compute the collision entropy of the state σ_{AE}; we obtain

$$h_2 = 1 - \frac{1}{m}\log_2[1 + (2^{2m} - 1)r^2], \qquad (56)$$

which extends Eq. (27) to any $m > 1$. From this we obtain the min-entropy rate for the correlated-noise quantum memory:

$$h_{\min} \geqslant \Gamma\left[1 - \frac{1}{m}\log_2[1 + (2^{2m} - 1)r^2]\right]. \qquad (57)$$

As shown in Fig. 6 this bound decreases with increasing m.

As we did in Sec. V, we now improve this bound by introducing a virtual erasure channel. This time the erasure channel acts on m qubits. A collection of m neighbor qubits is erased with probability $(1 - r)$. If erased, we obtain the erasure flag ω. To see the action on the whole set of n qubits, we may split them in groups of m neighbors. Each group is erased with probability $(1 - r)$. Overall, for large n, we expect about $n_e = (1 - r)n$ qubits to be erased. This corresponds to the n-qubit state

$$\sigma' = \Psi^{\otimes(n-n_e)} \otimes (I/2 \otimes \omega)^{\otimes n_e} \qquad (58)$$

$$= \Psi^{\otimes rn} \otimes (I/2 \otimes \omega)^{\otimes(1-r)n}. \qquad (59)$$

From this state we compute the min-entropy rate

$$h_{\min} \geqslant 1 - r, \qquad (60)$$

which is independent of m and equal to the bound obtained in the case of i.i.d. noise.

In conclusion, our new bound is always tighter, and the gap with the previous bound increases with increasing value of the correlation parameter m.

VIII. CONCLUSIONS

Quantum mechanics allows for information-theoretically secure two-party computation. Unlike quantum key distribution, however, two-party computation is not unconditionally secure, but requires additional assumptions as to the capability of a cheating party. In particular, one can achieve provably secure OT from Alice to Bob if the receiver Bob is limited in the amount or quality of his quantum memory, known as the noisy-storage model of quantum cryptography.

Experimental implementations of OT are particularly challenging, and much more challenging than QKD, because in two-party computation the users do not trust each other. This requires attention because Alice and Bob cannot cooperate, as they would do in QKD, in order to estimate the noise in the communication channel and apply error correction. In two-party computation, the honest users need to know in advance the noise and loss characteristics of the communication channel and of their trusted devices.

Intuitively, the more noisy the devices of the honest users are, the easier it is for a cheating user to hide in this trusted noise. This induces a trade-off between trusted noise (in the devices of the trusted users) and untrusted noise (in the quantum memory of a cheating receiver). This trade-off is ultimately quantified by the uncertainty relation used to assess the security of the OT protocol.

In this paper we have introduced improved entropic uncertainty relations and applied them to characterize the trade-off between trusted noise and quantum memory noise. We have also noted that cheating is not a rational behavior if the quantum memory is too noisy. We have shown that, even if the quantum memory is arbitrarily noisy, yet unbounded, the trusted noise, modeled as depolarizing noise, cannot surpass 22%. For low-noise quantum memory, secure OT can be achieved only if the trusted noise is also low, with an improved trade-off as shown in Fig. 4, or in the case of limited storage.

We have discussed depolarizing noise, but our results directly apply to a more general noise model of the form

$$\rho \rightarrow r\rho + (1-r)\rho_0, \qquad (61)$$

where ρ_0 is a fixed point independent of ρ. For simplicity and clarity of exposition, here we have focused on the asymptotic limit of many channel uses. However, our approach can be applied to the finite-size regime as well.

[1] J. Kilian, Founding cryptography on oblivious transfer, in *Proceedings of the Twentieth Annual ACM Symposium on Theory of Computing* (Association for Computing Machinery, New York, 1988), pp. 20–31.

[2] S. Even, O. Goldreich, and A. Lempel, A randomized, protocol for signing contracts, Commun. ACM **28**, 637 (1985).

[3] M. O. Rabin, How to exchange secrets with oblivious transfer, Technical Report TR-81 (Aiken Computation Lab, Harvard University, 1981), https://eprint.iacr.org/2005/187.pdf.

[4] G. Brassard and C. Crépeau, Oblivious transfers and privacy amplification, in *International Conference on the Theory and Applications of Cryptographic Techniques* (Springer, New York, 1997), pp. 334–347.

[5] I. B. Damgård, S. Fehr, R. Renner, L. Salvail, and C. Schaffner, A tight high-order entropic quantum uncertainty relation with applications, in *Advances in Cryptology—CRYPTO 2007*, Lecture Notes on Computer Science Vol. 4622 (Springer, New York, 2007), pp. 360–378.

[6] R. König, S. Wehner, and J. Wullschleger, Unconditional security from noisy quantum storage, IEEE Trans. Inf. Theory **58**, 1962 (2012).

[7] D. Mayers, Unconditionally Secure Quantum Bit Commitment is Impossible, Phys. Rev. Lett. **78**, 3414 (1997).

[8] H.-K. Lo, Insecurity of quantum secure computations, Phys. Rev. A **56**, 1154 (1997).

[9] H. Buhrman, M. Christandl, P. Hayden, H.-K. Lo, and S. Wehner, Possibility, impossibility, and cheat sensitivity of quantum-bit string commitment, Phys. Rev. A **78**, 022316 (2008).

[10] D. P. DiVincenzo, M. Horodecki, D. W. Leung, J. A. Smolin, and B. M. Terhal, Locking Classical Correlations in Quantum States, Phys. Rev. Lett. **92**, 067902 (2004).

[11] S. Guha, P. Hayden, H. Krovi, S. Lloyd, C. Lupo, J. H. Shapiro, M. Takeoka, and M. M. Wilde, Quantum Enigma Machines and the Locking Capacity of a Quantum Channel, Phys. Rev. X **4**, 011016 (2014).

[12] C. Lupo, Quantum data locking for secure communication against an eavesdropper with time-limited storage, Entropy **17**, 3194 (2015).

[13] Z. Huang, P. P. Rohde, D. W. Berry, P. Kok, J. P. Dowling, and C. Lupo, Photonic quantum data locking, Quantum **5**, 447 (2021).

[14] I. B. Damgård, S. Fehr, L. Salvail, and C. Schaffner, Cryptography in the bounded-quantum-storage model, in *Proceedings of 46th IEEE FOCS* (IEEE Computer Society, Los Alamitos, CA, 2005), pp. 449–458.

[15] I. Damgård, S. Fehr, L. Salvail, and C. Schaffner, Secure identification and QKD in the bounded-quantum-Sstorage model, in *Advances in Cryptology—CRYPTO 2007*, Lecture Notes on Computer Science Vol. 4622 (Springer, New York, 2007), pp. 342–359.

[16] S. Wehner, C. Schaffner, and B. M. Terhal, Cryptography from Noisy Storage, Phys. Rev. Lett. **100**, 220502 (2008).

[17] C. Schaffner, B. Terhal, and S. Wehner, Robust Cryptography in the noisy-quantum-storage model, Quantum Inf. Comput. **9**, 963 (2009).

[18] C. Schaffner, Simple protocols for oblivious transfer and secure identification in the noisy-quantum-storage model, Phys. Rev. A **82**, 032308 (2010).

[19] S. Wehner, M. Curty, C. Schaffner, and H.-K. Lo, Implementation of two-party protocols in the noisy-storage model, Phys. Rev. A **81**, 052336 (2010).

[20] F. Dupuis, O. Fawzi, and S. Wehner, Entanglement sampling and applications, IEEE Trans. Inf. Theory **61**, 1093 (2015).

[21] N. Ng, M. Berta, and S. Wehner, Min-entropy uncertainty relation for finite-size cryptography, Phys. Rev. A **86**, 042315 (2012).

[22] N. H. Y. Ng, S. K. Joshi, C. C. Ming, C. Kurtsiefer, and S. Wehner, Experimental implementation of bit commitment in the noisy-storage model, Nat. Commun. **3**, 1326 (2012).

[23] C. Erven, N. H. Y. Ng, N. Gigov, R. Laflamme, S. Wehner, and G. Weihs, An experimental implementation of oblivious transfer in the noisy storage model, Nat. Commun. **5**, 3418 (2014).

[24] J. Ribeiro, L. P. Thinh, J. Kaniewski, J. Helsen, and S. Wehner, Device independence for two-party cryptography and position verification with memoryless devices, Phys. Rev. A **97**, 062307 (2018).

[25] A. Broadbent and P. Yuen, Device-independent oblivious transfer from the bounded-quantum-storage-model and computational assumptions, New J. Phys. **25**, 053019 (2023).

[26] R. Amiri, R. Stárek, D. Reichmuth, I. V. Puthoor, M. Mičuda, L. Mišta, Jr., M. Dušek, P. Wallden, and E. Andersson, Imperfect 1-out-of-2 quantum oblivious transfer: Bounds, a protocol, and its experimental implementation, PRX Quantum **2**, 010335 (2021).

[27] L. Stroh, N. Horová, R. Stárek, I. V. Puthoor, M. Mičuda, M. Dušek, and E. Andersson, Noninteractive XOR quantum oblivious transfer: Optimal protocols and their experimental implementations, PRX Quantum **4**, 020320 (2023).

[28] C. H. Bennett and G. Brassard, Quantum cryptography: Public key distribution and coin tossing, in *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India, 10–12 December, 1984* (IEEE, Piscataway, NJ, 1984), pp. 175–179.

[29] This is a nontrivial assumption, as it may generally allow a dishonest receiver to cheat more often by claiming that they did not receive the photon when they failed in cheating in some way, and also may allow a sender to cheat, by sending pulses that are more or less likely to be lost; the fact of whether the pulse is lost or not can provide information on how it was measured, or what the result was more likely to be (see Ref. [36], which discusses related issues). In this paper, this issue is not considered because we assume that loss and noise are well characterized (see Sec. III).

[30] Note that X_0 and X_1 are shorter than n bits, whereas the hash functions are from n to ℓ bits. The notation $F_C(X_C)$ implicitly implies that a sufficient number of 0s are appended to X_C.

[31] M. Tomamichel, A framework for non-asymptotic quantum information theory, Ph.D. thesis, Swiss Federal Institute of Technology (ETH) Zurich, 2012, arXiv:1203.2142.

[32] König *et al.* [6] reported this bound as 1/4 instead of 1/2. This is due to a different definition of n.

[33] C. Schaffner, Cryptography in the bounded-quantum-storage model, Ph.D. thesis, University of Aarhus, 2007, arXiv:0709.0289.

[34] R. König and S. Wehner, A Strong Converse for Classical Channel Coding Using Entangled Inputs, Phys. Rev. Lett. **103**, 070504 (2009).

[35] F. Caruso, V. Giovannetti, C. Lupo, and S. Mancini, Quantum channels and memory effects, Rev. Mod. Phys. **86**, 1203 (2014).

[36] M. Bozzio, A. Cavaillès, E. Diamanti, A. Kent, and D. Pitalúa-García, Multiphoton and side-channel attacks in mistrustful quantum cryptography, PRX Quantum **2**, 030338 (2021).