CRYPTOGRAPHY IN THE
BOUNDED-QUANTUM-STORAGE MODEL[*]

IVAN B. DAMGÅRD[†], SERGE FEHR[‡], LOUIS SALVAIL[§], AND CHRISTIAN SCHAFFNER[‡]

Abstract. We initiate the study of two-party cryptographic primitives with unconditional security, assuming that the adversary's *quantum* memory is of bounded size. We show that oblivious transfer and bit commitment can be implemented in this model using protocols where honest parties need no quantum memory, whereas an adversarial player needs quantum memory of size at least $n/2$ in order to break the protocol, where n is the number of qubits transmitted. This is in sharp contrast to the classical bounded-memory model, where we can only tolerate adversaries with memory of size quadratic in honest players' memory size. Our protocols are efficient and noninteractive and can be implemented using today's technology. On the technical side, a new entropic uncertainty relation involving min-entropy is established.

Key words. quantum cryptography, quantum-bounded-storage model, quantum uncertainty relation, oblivious transfer, bit commitment

AMS subject classifications. 81P68, 94A60

DOI. 10.1137/060651343

1. Introduction. It is well known that nontrivial two-party cryptographic primitives cannot be securely implemented if only error-free communication is available and there is no limitation assumed on the computing power and memory of the players. Fundamental examples of such primitives are bit commitment (BC) and oblivious transfer (OT). In BC, a committer C commits himself to a choice of a bit b by exchanging information with a verifier V. We want that V does not learn b (we say the commitment is hiding), yet C can later choose to reveal b in a convincing way; i.e., only the value fixed at commitment time will be accepted by V (we say the commitment is binding). In (Rabin) OT, a sender S sends a bit b to a receiver R by executing some protocol in such a way that R receives b with probability $\frac{1}{2}$ and nothing with probability $\frac{1}{2}$, yet S does not learn what was received.

Informally, BC is not possible with unconditional security since hiding means that when 0 is committed, exactly the same information exchange could have happened when committing to a 1. Hence, even if 0 was actually committed to, C could always compute a complete view of the protocol consistent with having committed to 1, and pretend that this was what he had in mind originally. A similar type of argument shows that OT is also impossible in this setting.

One might hope that allowing the protocol to make use of quantum communication would make a difference. Here, information is stored in qubits, i.e., in the state of two-level quantum mechanical systems, such as the polarization state of a single photon. It is well known that quantum information behaves in a way that is fundamentally different from classical information, enabling, for instance, unconditionally secure key exchange between two honest players. However, in the case of two mutually distrusting parties, we are not so fortunate: even with quantum communication, unconditionally secure BC and OT remain impossible [31, 34].

There are, however, several scenarios where these impossibility results do not apply, namely:

   (i) if the computing power of players is bounded,
  (ii) if the communication is noisy,
 (iii) if the adversary is under some physical limitation, e.g., the size of the available memory is bounded.

The first scenario is the basis of many well-known solutions based on plausible but unproven complexity assumptions, such as hardness of factoring or discrete logarithms. The second scenario has been used to construct both BC and OT protocols in various models for the noise [13, 15, 14]. The third scenario is our focus here. In this model, OT and BC can be done using classical communication, assuming, however, quite restrictive bounds on the adversary's memory size [10, 19]; namely, it can be at most quadratic in the memory size of honest players. Such an assumption is on the edge of being realistic; it would clearly be more satisfactory to have a larger separation between the memory size of honest players and that of the adversary. However, this was shown to be impossible [22].

In this paper, we study for the first time what happens if instead we consider protocols where quantum communication is used and we place a bound on the adversary's *quantum* memory size. There are two reasons why this may be a good idea: first, if we do not bound the classical memory size, we avoid the impossibility result of [22]. Second, the adversary's typical goal is to obtain a certain piece of classical information that we want to keep hidden from him. However, if he cannot store all the quantum information that is sent, he must convert some of it to classical information by measuring. This may irreversibly destroy information, and we may be able to arrange it such that the adversary cannot afford to lose information this way, while honest players can.

It turns out that this is indeed possible: we present protocols for both BC and OT in which n qubits are transmitted, where honest players need *no quantum memory*, but where the adversary must store at least $n/2$ qubits to break the protocol. We emphasize that no bound is assumed on the adversary's computing power, nor on his classical memory. This is clearly much more satisfactory than the classical case, not only from a theoretical point of view, but also in practice: while sending qubits and measuring them immediately as they arrive is well within reach of current technology, storing even a single qubit for more than a fraction of a second is a formidable technological challenge. Furthermore, we show that our protocols also work in a non-ideal setting where we allow the quantum source to be imperfect and the quantum communication to be noisy.

We emphasize that what makes OT and BC possible in our model is not so much the memory bound per se, but rather the loss of information on the part of the adversary. Indeed, our results also hold if the adversary's memory device holds an arbitrary number of qubits but is imperfect in certain ways. This is discussed in more detail in section 6.2.

Our protocols are noninteractive; only one party sends information when doing OT, commitment, or opening. Furthermore, the commitment protocol has the interesting property that the only message is sent *to* the committer; i.e., it is possible to commit while only *receiving* information. Such a scheme clearly does not exist without a bound on the committer's memory, even under computational assumptions and using quantum communication: a corrupt committer could always store (possibly quantumly) all the information sent, until opening time, and only then follow the honest committer's algorithm to figure out what should be sent to convincingly open a 0 or a 1. Note that in the classical bounded-storage model, it is known how to do time-stamping that is noninteractive in our sense: a player can time-stamp a document while only receiving information [35]. However, no reasonable BC or protocol that time-stamps a bit exists in this model. It is straightforward to see that any such protocol can be broken by an adversary with classical memory of size twice that of an honest player, while our protocol requires no memory for the honest players and remains secure against any adversary unable to store more than half the size of the quantum transmission.

We also note that it has been shown earlier that BC is possible using quantum communication, assuming a different type of physical limitation, namely, a bound on the size of coherent measurement that can be implemented [39]. This limitation is incomparable to ours: it does not limit the total size of the memory; instead it limits the number of bits that can be simultaneously operated on to produce a classical result. Our adversary has a limit on the total memory size, but can measure all of it coherently. The protocol from [39] is interactive and requires a bound on the maximal measurement size that is sublinear in n.

On the technical side, we derive a new type of uncertainty relation involving the min-entropy of a quantum encoding (see Theorem 3.1 and Corollary 3.3), which might be useful in other contexts as well. The new relation is then used in combination with a proof technique by Shor and Preskill [41], where the actions of honest players are purified, and with privacy amplification against quantum adversaries as introduced by Renner and König [37, 36].

2. Preliminaries.

2.1. Notation and terminology. For a set $I = \{i_1, i_2, \ldots, i_\ell\} \subseteq \{1, \ldots, n\}$ and an n-bit string $x \in \{0, 1\}^n$, we define $x|_I := x_{i_1} x_{i_2} \cdots x_{i_\ell}$, and we write $B^{\delta n}(x)$ for the set of all n-bit strings at Hamming distance at most δn from x. Note that the number of elements in $B^{\delta n}(x)$ is the same for all x; we denote it by $B^{\delta n} := |B^{\delta n}(x)|$. It is well known that $B^{\delta n} \leq 2^{nh(\delta)}$, where $h(p)$ denotes the binary entropy function $h(p) := -\big(p \cdot \log p + (1-p) \cdot \log(1-p)\big)$. All logarithms in this paper are to base two. We denote by $negl(n)$ any function of n smaller than any polynomial provided that n is sufficiently large.

For a discrete probability space (Ω, P), we write $P[\mathcal{E}]$ for the probability of the event $\mathcal{E} \subset \Omega$, and we write P_X for the distribution of the random variable $X : \Omega \to \mathcal{X}$. We use similar notation for conditional probabilities and distributions. As is common practice, we do not refer to the probability space (Ω, P) but leave it implicitly defined by the joint probabilities of all considered events and random variables. For a probability distribution Q over $\mathcal{X}$, we abbreviate the (overall) probability of a set $L \subseteq \mathcal{X}$ with $Q(L) := \sum_{x \in L} Q(x)$.

The pair $\{|0\rangle, |1\rangle\}$ denotes the computational or rectilinear or "+" basis for the two-dimensional complex Hilbert space $\mathbb{C}^2$. The diagonal or "×" basis is defined as $\{|0\rangle_\times, |1\rangle_\times\}$, where $|0\rangle_\times = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ and $|1\rangle_\times = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$. Measuring a qubit in

the $+$-basis (resp., $\times$-basis) means applying the measurement described by projectors $|0\rangle\langle 0|$ and $|1\rangle\langle 1|$ (resp., projectors $|0\rangle_\times\langle 0|_\times$ and $|1\rangle_\times\langle 1|_\times$). When the context requires it, we write $|0\rangle_+$ and $|1\rangle_+$ instead of $|0\rangle$ and $|1\rangle$, respectively, and for any $x \in \{0,1\}^n$ and $r \in \{+,\times\}$, we write $|x\rangle_r = \bigotimes_{i=1}^n |x_i\rangle_r$. If we want to choose the $+$- or $\times$-basis according to the bit $b \in \{0,1\}$, we write $\{+,\times\}_{[b]}$.

The behavior of a quantum state in a register E is fully described by its density matrix ρ_E. We often consider cases where a quantum state may depend on some classical random variable X, in that it is described by the density matrix ρ_E^x if and only if $X = x$. For an observer who has access only to the register E but not to X, the behavior of the state is determined by the density matrix $\sum_x P_X(x)\rho_\mathsf{E}^x$. The joint state, consisting of the classical X and the quantum register E and therefore called a *cq-state*, is described by the density matrix $\sum_x P_X(x)|x\rangle\langle x| \otimes \rho_\mathsf{E}^x$. In order to have more compact expressions, we use the following notation. We write

$$\rho_{X\mathsf{E}} = \sum_x P_X(x)|x\rangle\langle x| \otimes \rho_\mathsf{E}^x \quad \text{and} \quad \rho_\mathsf{E} = \mathrm{tr}_X(\rho_{X\mathsf{E}}) = \sum_x P_X(x)\rho_\mathsf{E}^x.$$

More generally, for any event $\mathcal{E}$, we write

$$(2.1) \quad \rho_{X\mathsf{E}|\mathcal{E}} = \sum_x P_{X|\mathcal{E}}(x)|x\rangle\langle x| \otimes \rho_\mathsf{E}^x \quad \text{and} \quad \rho_{\mathsf{E}|\mathcal{E}} = \mathrm{tr}_X(\rho_{X\mathsf{E}|\mathcal{E}}) = \sum_x P_{X|\mathcal{E}}(x)\rho_\mathsf{E}^x.$$

We also write $\rho_X = \sum_x P_X(x)|x\rangle\langle x|$ for the quantum representation of the classical random variable X (and similarly for $\rho_{X|\mathcal{E}}$). This notation extends naturally to quantum states that depend on several classical random variables (i.e., to ccq-states, etc.).

This notation extends naturally to quantum states that depend on several classical random variables (i.e., to ccq-states, etc.), defining the density matrices $\rho_{XY\mathsf{E}}$, $\rho_{XY\mathsf{E}|\mathcal{E}}$, $\rho_{Y\mathsf{E}|X=x}$, etc. We tend to slightly abuse notation and write $\rho_{Y\mathsf{E}}^x = \rho_{X\mathsf{E}|X=x}$ and $\rho_{Y\mathsf{E}|\mathcal{E}}^x = \rho_{Y\mathsf{E}|X=x,\mathcal{E}}$, as well as $\rho_\mathsf{E}^x = \mathrm{tr}_Y(\rho_{Y\mathsf{E}}^x)$ and $\rho_{\mathsf{E}|\mathcal{E}}^x = \mathrm{tr}_Y(\rho_{Y\mathsf{E}|\mathcal{E}}^x)$.[1] Note that writing $\rho_{X\mathsf{E}} = \mathrm{tr}_Y(\rho_{XY\mathsf{E}})$ and $\rho_\mathsf{E} = \mathrm{tr}_{X,Y}(\rho_{XY\mathsf{E}})$ is consistent with the above notation. We also write $\rho_{X\mathsf{E}|\mathcal{E}} = \mathrm{tr}_Y(\rho_{XY\mathsf{E}|\mathcal{E}})$ and $\rho_{\mathsf{E}|\mathcal{E}} = \mathrm{tr}_{X,Y}(\rho_{XY\mathsf{E}|\mathcal{E}})$, where one has to be aware that in contrast to (2.1), here the state E may depend on the event $\mathcal{E}$ when given x (namely, via Y), so that, e.g., $\rho_{\mathsf{E}|\mathcal{E}} = \sum_x P_{X|\mathcal{E}}(x)\rho_{\mathsf{E}|\mathcal{E}}^x$.

Given a cq-state $\rho_{X\mathsf{E}}$, by saying that there exists a random variable Y such that $\rho_{XY\mathsf{E}}$ satisfies some condition, we mean that $\rho_{X\mathsf{E}}$ can be understood as $\rho_{X\mathsf{E}} = \mathrm{tr}_Y(\rho_{XY\mathsf{E}})$ for a ccq-state $\rho_{XY\mathsf{E}}$ that satisfies the required condition.

Obviously, $\rho_{X\mathsf{E}} = \rho_X \otimes \rho_\mathsf{E}$ if and only if the quantum part is independent of X (in that $\rho_\mathsf{E}^x = \rho_\mathsf{E}$ for any x), where the latter in particular implies that no information on X can be learned by observing only ρ_E. Furthermore, if $\rho_{X\mathsf{E}}$ and $\rho_X \otimes \rho_\mathsf{E}$ are ε-close in terms of their trace distance $\delta(\rho,\sigma) = \frac{1}{2}\mathrm{tr}(|\rho - \sigma|)$, then the real system $\rho_{X\mathsf{E}}$ "behaves" as the ideal system $\rho_X \otimes \rho_\mathsf{E}$ except with probability ε [37] in that for any evolution of the system no observer can distinguish the real system from the ideal one with advantage greater than ε. Throughout the paper, $\mathbb{1}$ stands for the identity matrix (describing the fully mixed state) renormalized by the appropriate dimension.

We consider the notion of the classical *Rényi entropy* $\mathrm{H}_\alpha(X)$ of order α of a random variable X [38], as well as its generalization to the Rényi entropy $\mathrm{H}_\alpha(\rho)$ of

---

[1] The density matrix $\rho_{\mathsf{E}|\mathcal{E}}^x$ describes the quantum state E in the case that the event $\mathcal{E}$ occurs and X takes on the value x. The corresponding convention holds for the other density matrices considered here.

a quantum state ρ [37]. It holds that $H_\alpha(\rho_X) = H_\alpha(X)$ and $H_\alpha(\rho_X) \leq H_\beta(\rho_X)$ if $\alpha \geq \beta$. The cases that are relevant for us are the classical *min-entropy* $H_\infty(X) = -\log(\max_x P_X(x))$ as well as the quantum versions of the *max-* and *collision-entropy* $H_0(\rho) = \log(\mathrm{rank}(\rho))$, respectively, $H_2(\rho) = -\log\left(\sum_i \lambda_i^2\right)$, where $\{\lambda_i\}_i$ are the eigenvalues of ρ.

2.2. Bounded quantum storage and privacy amplification. All our protocols take place in the *bounded-quantum-storage model*, which concretely means the following: the state of an adversarial player may consist of an arbitrary number of qubits, and he may perform arbitrary quantum computation. At a certain point in time, though, we say that *the memory bound applies*, which means that a measurement is applied to the system with the restriction that the resulting quantum state can be stored in at most q qubits. The classical outcome of the measurement can be of arbitrary size and (classically) stored for later use. After this point, the player is again unbounded in (quantum) memory. Throughout, the adversary may have unbounded computing power and classical memory. We note that our results also apply to some cases where the adversary's memory is not bounded but is noisy in certain ways; see section 6.2.

An important tool we use is universal hashing. A class $\mathcal{F}_n$ of hashing functions from $\{0,1\}^n$ to $\{0,1\}$ is called *two-universal* if for any pair $x, y \in \{0,1\}^n$ with $x \neq y$, and F uniformly chosen from $\mathcal{F}_n$,

$$P\big[F(x) = F(y)\big] \leq \frac{1}{2}.$$

Several two-universal classes of hashing functions are such that evaluating and picking a function uniformly and at random in $\mathcal{F}_n$ can be done efficiently [11, 42].

THEOREM 2.1 (see [37]). *Let $\rho_{X\mathsf{E}}$ be a cq-state, where X is distributed over $\{0,1\}^n$ and register E contains q qubits. Let F be the random variable corresponding to the random choice (with uniform distribution and independent from X) of a member of a two-universal class of hashing functions $\mathcal{F}_n$. Then*

$$(2.2) \qquad \delta\big(\rho_{F(X)F\mathsf{E}}, \mathbb{1} \otimes \rho_{F\mathsf{E}}\big) \leq \frac{1}{2}\, 2^{-\frac{1}{2}(H_2(\rho_{X\mathsf{E}}) - H_0(\rho_\mathsf{E}) - 1)}$$

$$(2.3) \qquad\qquad\qquad\qquad\qquad \leq \frac{1}{2}\, 2^{-\frac{1}{2}(H_\infty(X) - q - 1)}.$$

The first inequality (2.2) is the original theorem from [37], and (2.3) follows by observing that $H_2(\rho_{X\mathsf{E}}) \geq H_2(\rho_X) = H_2(X) \geq H_\infty(X)$. In this paper, we use only this weaker version of the theorem.

Note that if the rightmost term of (2.3) is negligible, i.e., say, smaller than $2^{-\varepsilon n}$, then this situation is $2^{-\varepsilon n}$-close to the ideal situation where $F(X)$ is perfectly uniform and independent of E and F. In particular, replacing $F(X)$ by an independent and uniformly distributed bit results in a common state which essentially cannot be distinguished from the original one.

The following lemma is a direct consequence of Theorem 2.1. In section 5, this lemma will be useful for proving the binding condition of our commitment scheme. Recall that for $X \in \{0,1\}^n$, $\mathrm{B}^{\delta n}(X)$ denotes the set of all n-bit strings at Hamming distance at most δn from X and $\mathrm{B}^{\delta n} := |\mathrm{B}^{\delta n}(X)|$ is the number of such strings.

LEMMA 2.2. *Let $\rho_{X\mathsf{E}}$ be a cq-state, where X is distributed over $\{0,1\}^n$ and register E contains q qubits. Let $\hat{X}$ be a guess for X obtained by measuring E. Then,*

for all $\delta < \frac{1}{2}$ it holds that

$$P\big[\hat{X} \in \mathrm{B}^{\delta n}(X)\big] \leq 2^{-\frac{1}{2}(\mathrm{H}_\infty(X)-q-1)+\log(\mathrm{B}^{\delta n})}.$$

In other words, given a quantum memory of q qubits arbitrarily correlated with a classical random variable X, the probability of finding $\hat{X}$ at Hamming distance at most δn from X, where $nh(\delta) < \frac{1}{2}(\mathrm{H}_\infty(X)-q)$, is negligible.

Proof. Here is a strategy to try to bias $F(X)$ when given $\hat{X}$ and $F \in_R \mathcal{F}_n$. Sample $X' \in_R \mathrm{B}^{\delta n}(\hat{X})$ and output $F(X')$. Note that, using p_{succ} as shorthand for the probability $P\big[\hat{X} \in \mathrm{B}^{\delta n}(X)\big]$ to be bounded,

$$P\big[F(X') = F(X)\big] = \frac{p_{\mathrm{succ}}}{\mathrm{B}^{\delta n}} + \left(1 - \frac{p_{\mathrm{succ}}}{\mathrm{B}^{\delta n}}\right)\frac{1}{2}$$
$$= \frac{1}{2} + \frac{p_{\mathrm{succ}}}{2 \cdot \mathrm{B}^{\delta n}},$$

where the first equality follows from the fact that if $X' \neq X$, then, as $\mathcal{F}_n$ is two-universal, $P[F(X) = F(X')] = \frac{1}{2}$. Note that, given F and being allowed to measure E, the probability of correctly guessing a binary $F(X)$ is upper bounded by $\frac{1}{2} + \delta(\rho_{F(X)F\mathsf{E}}, \mathbb{1} \otimes \rho_{F\mathsf{E}})$ [24]. In combination with Theorem 2.1, the above results in

$$\frac{1}{2} + \frac{p_{\mathrm{succ}}}{2 \cdot \mathrm{B}^{\delta n}} \leq \frac{1}{2} + \frac{1}{2}2^{-\frac{1}{2}(\mathrm{H}_\infty(X)-q-1)},$$

and the claim follows immediately. □

2.3. Operators and norms. For a linear operator A on the complex Hilbert space $\mathcal{H}$, we define the *operator norm*

$$\|A\| := \sup_{\langle x | x \rangle = 1} \|Ax\|$$

for the Euclidean norm $\|x\| := \sqrt{\langle x|x \rangle}$. When A is Hermitian, we have

$$\|A\| = \lambda_{\max}(A) := \max\{|\lambda_j| : \lambda_j \text{ an eigenvalue of } A\}.$$

From an equivalent definition of the norm $\|A\| = \sup_{\langle y|y \rangle = \langle x|x \rangle = 1} |\langle y|A|x \rangle|$, it is easy to see that $\|A^*\| = \|A\|$. For two Hermitian matrices A and B, we have that $\|AB\| = \|(AB)^*\| = \|B^*A^*\| = \|BA\|$. The operator norm is *unitarily invariant*; i.e., for all unitary U, V, $\|A\| = \|UAV\|$ holds. It is easy to show that

$$\left\|\begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix}\right\| = \max\{\|A\|, \|B\|\}.$$

LEMMA 2.3. *Let X, Y be any two $n \times n$ matrices such that the products XY and YX are Hermitian. Then, we have*

$$\|XY\| = \|YX\|.$$

Proof. For any two $n \times n$ matrices X and Y, XY and YX have the same eigenvalues; see, e.g., [5, Exercise I.3.7]. Therefore, $\|XY\| = \lambda_{\max}(XY) = \lambda_{\max}(YX) = \|YX\|$. □

A linear operator P such that $P^2 = P$ and $P^* = P$ is called an *orthogonal projector*.

PROPOSITION 2.4. *For two orthogonal projectors A and B, it holds that*

$$\|A + B\| \leq 1 + \|AB\|.$$

Proof. We adapt a technique by Kittaneh [28] to our case. We define two 2×2-block matrices X and Y as

$$X := \begin{pmatrix} A & B \\ 0 & 0 \end{pmatrix} \quad \text{and} \quad Y := \begin{pmatrix} A & 0 \\ B & 0 \end{pmatrix}$$

and using $A^2 = A$ and $B^2 = B$, we compute

$$XY := \begin{pmatrix} A + B & 0 \\ 0 & 0 \end{pmatrix} \quad \text{and} \quad YX := \begin{pmatrix} A & AB \\ BA & B \end{pmatrix} = \begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix} + \begin{pmatrix} 0 & AB \\ BA & 0 \end{pmatrix}.$$

As A and B are Hermitian, so are $A + B$, AB, BA, XY, and YX. We use Lemma 2.3 and the triangle inequality to obtain

$$\left\| \begin{pmatrix} A + B & 0 \\ 0 & 0 \end{pmatrix} \right\| = \left\| \begin{pmatrix} A & AB \\ BA & B \end{pmatrix} \right\| \leq \left\| \begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix} \right\| + \left\| \begin{pmatrix} 0 & AB \\ BA & 0 \end{pmatrix} \right\|.$$

Using the unitary invariance of the operator norm to permute the columns in the rightmost matrix and the facts that $\|A\| = \|B\| = 1$ as well as $\|AB\| = \|BA\|$, we conclude that $\|A + B\| \leq 1 + \|AB\|$. □

3. Uncertainty relations. In this section, we prove a general uncertainty result and derive from that a corollary that plays the crucial role in the security proof of our protocols. The uncertainty result concerns the situation where the sender holds an arbitrary quantum register of n qubits. He may measure them in either the +- or the ×-basis. We are interested in the distribution of both these measurement results, and we claim that they cannot *both* be "very far from uniform."

3.1. History and previous work. The history of uncertainty relations starts with Heisenberg, who showed that the outcomes of two noncommuting observables A and B applied to any state ρ are not easy to predict simultaneously. However, Heisenberg speaks only about the variance of the measurement results, and his result was shown to have several shortcomings in [25, 18]. More general forms of uncertainty relations were proposed in [6] and [18] to resolve these problems. The new relations were called *entropic uncertainty relations*, because they are expressed using Shannon entropy instead of the statistical variance. Entropic uncertainty relations have the advantage of being pure information theoretic statements. The first entropic uncertainty relation was introduced by Deutsch [18] and stated that

$$(3.1) \qquad \mathrm{H}(P) + \mathrm{H}(Q) \geq -2 \log \frac{1 + c}{2},$$

where P, Q are the distributions representing the measurement results and c is the maximum inner product norm between any eigenvectors of A and B. First conjectured by Kraus [29], Deutsch's relation was improved by Maassen and Uffink [32] to the optimal

$$(3.2) \qquad \mathrm{H}(P) + \mathrm{H}(Q) \geq -2 \log c.$$

Although a bound on Shannon entropy can be helpful in some cases, it is usually not good enough in cryptographic applications. The main tool to reduce the adversary's information—privacy amplification [4, 27, 3, 37, 36]—works only if a bound

on the adversary's min-entropy (in fact collision entropy) is known. Unfortunately, knowing a lower bound on the Shannon entropy of a distribution does not in general allow one to lower bound its higher order Rényi entropies.

An entropic uncertainty relation involving Rényi entropy of order 2 (i.e., *collision entropy*) was introduced by Larsen [30, 40]. Larsen's relation quantifies precisely the collision entropy for the set $\{A_i\}_{i=1}^{d+1}$ of *all* maximally noncommuting observables, where d is the dimension of the Hilbert space. Its use is therefore restricted to quantum coding schemes that take advantage of *all* $d+1$ observables, i.e., to schemes that are difficult to implement in practice.

3.2. Two mutually unbiased bases. In this section, we show that two distributions obtained by measuring in two mutually unbiased bases cannot *both* be "very far from uniform." One way to express this is to say that a distribution is very nonuniform if one can identify a subset of outcomes that has much higher probability than for a uniform choice. Intuitively, the theorem below says that such sets cannot be found for both measurements. In Appendix A, we generalize the results of this section to more than two mutually unbiased bases.

THEOREM 3.1. *Let ρ be an arbitrary state of n qubits, and let $Q^+(\cdot)$ and $Q^\times(\cdot)$ be the respective distributions of the outcome when ρ is measured in the $+$-basis and the $\times$-basis, respectively. Then, for any two sets $L^+ \subset \{0,1\}^n$ and $L^\times \subset \{0,1\}^n$ it holds that*

$$Q^+(L^+) + Q^\times(L^\times) \leq 1 + 2^{-n/2}\sqrt{|L^+||L^\times|}.$$

Proof. We define the two orthogonal projectors

$$A := \sum_{x \in L^+} |x\rangle\langle x| \quad \text{and} \quad B := \sum_{y \in L^\times} H^{\otimes n}|y\rangle\langle y|H^{\otimes n}.$$

Using the spectral decomposition of $\rho = \sum_w \lambda_w |\varphi_w\rangle\langle\varphi_w|$, we have

$$\begin{aligned}
Q^+(L^+) + Q^\times(L^\times) &= \mathrm{tr}\,(A\rho) + \mathrm{tr}\,(B\rho) \\
&= \sum_w \lambda_w \left(\mathrm{tr}\,(A|\varphi_w\rangle\langle\varphi_w|) + \mathrm{tr}\,(B|\varphi_w\rangle\langle\varphi_w|)\right) \\
&= \sum_w \lambda_w \left(\langle\varphi_w|A|\varphi_w\rangle + \langle\varphi_w|B|\varphi_w\rangle\right) \\
&= \sum_w \lambda_w \langle\varphi_w|(A+B)|\varphi_w\rangle \\
&\leq \|A+B\| \leq 1 + \|AB\|,
\end{aligned}$$

where the last line is Proposition 2.4. In order to finish the proof, we show that $\|AB\| \leq 2^{-n/2}\sqrt{|L^+||L^\times|}$. Note that an arbitrary state $|\psi\rangle = \sum_z \lambda_z H^{\otimes n}|z\rangle$ can be expressed with coordinates λ_z in the diagonal basis. Then, with the sums over x and y understood as over $x \in L^+$ and $y \in L^\times$, respectively,

$$\begin{aligned}
\big\|AB|\psi\rangle\big\| &= \left\|\sum_{x,y}|x\rangle\langle x|H^{\otimes n}|y\rangle\langle y|H^{\otimes n}|\psi\rangle\right\| = 2^{-n/2}\left\|\sum_{x,y}|x\rangle\langle y|H^{\otimes n}|\psi\rangle\right\| \\
&= 2^{-n/2}\left\|\sum_x |x\rangle\right\|\left|\sum_y \lambda_y\right| \leq 2^{-n/2}\sqrt{|L^+|}\sum_y |\lambda_y| \leq 2^{-n/2}\sqrt{|L^+||L^\times|}.
\end{aligned}$$

The second equality holds since $|x\rangle$ and $H^{\otimes n}|y\rangle$ are mutually unbiased, the first inequality follows from Pythagoras and the triangle inequality, and the last inequality follows from Cauchy–Schwarz. This implies that $\|AB\| \leq 2^{-n/2}\sqrt{|L^+||L^\times|}$ and finishes the proof.   □

This theorem yields a meaningful bound as long as $|L^+| \cdot |L^\times| < 2^n$, e.g., if L^+ and $L^\times$ both contain less than $2^{n/2}$ elements. The relation is tight in the sense that for the Hadamard-invariant state

$$|\varphi\rangle = \left(|0\rangle^{\otimes n} + (H|0\rangle)^{\otimes n}\right)/\sqrt{2(1 + 2^{-n/2})}$$

and $L^+ = L^\times = \{0^n\}$, it is straightforward to verify that $Q^+(L^+) = Q^\times(L^\times) = (1 + 2^{-n/2})/2$ and therefore $Q^+(L^+) + Q^\times(L^\times) = 1 + 2^{-n/2}$. Another state that achieves equality (for n even) is $|\varphi\rangle = |0\rangle^{\otimes n/2} \otimes (H|0\rangle)^{\otimes n/2}$ with $L^+ = \{0^{n/2}x \mid x \in \{0,1\}^{n/2}\}$ and $L^\times = \{x0^{n/2} \mid x \in \{0,1\}^{n/2}\}$. We get that $Q^+(L^+) = Q^\times(L^\times) = 1$ and thus $Q^+(L^+) + Q^\times(L^\times) = 2 = 1 + 2^{-n/2}\sqrt{2^n}$.

If for $r \in \{+, \times\}$, L^r contains only the n-bit string with the maximal probability of Q^r, we obtain a known tight relation (see inequality (9) in [32]).

COROLLARY 3.2. *Let q_∞^+ and $q_\infty^\times$ be the maximal probabilities of the distributions Q^+ and $Q^\times$ from above. It then holds that $q_\infty^+ \cdot q_\infty^\times \leq \frac{1}{4}(1 + c)^2$, where $c = 2^{-n/2}$.*

Equality is achieved for the same state $|\varphi\rangle = \left(|0\rangle^{\otimes n} + (H|0\rangle)^{\otimes n}\right)/\sqrt{2(1 + 2^{-n/2})}$ as above.

The following corollary plays a crucial role in the security proof of the OT protocol in the next section.

COROLLARY 3.3. *Let R be a random variable over $\{+, \times\}$, and let X be the outcome when ρ is measured in basis R, such that $P_{X|R}(x|r) = Q^r(x)$. Then, for any $\lambda < \frac{1}{2}$ there exists an event $\mathcal{E}$ such that*

$$P[\mathcal{E}|R=+] + P[\mathcal{E}|R=\times] \geq 1 - negl(n)$$

and thus $P[\mathcal{E}] \geq \frac{1}{2} - negl(n)$ in case R is uniform, and such that

$$\mathrm{H}_\infty(X|R=r, \mathcal{E}) \geq \lambda n$$

for $r \in \{+, \times\}$ with $P_{R|\mathcal{E}}(r) > 0$.

Proof. Choose $\varepsilon > 0$ such that $\lambda + \varepsilon < \frac{1}{2}$, define

$$S^+ := \left\{x \in \{0,1\}^n : Q^+(x) \leq 2^{-(\lambda+\varepsilon)n}\right\} \text{ and}$$
$$S^\times := \left\{z \in \{0,1\}^n : Q^\times(z) \leq 2^{-(\lambda+\varepsilon)n}\right\}$$

to be the sets of strings with small probabilities, and denote by $L^+ := \overline{S}^+$ and $L^\times := \overline{S}^\times$ their complements.[2] Note that for all $x \in L^+$, we have that $Q^+(x) > 2^{-(\lambda+\varepsilon)n}$ and therefore $|L^+| < 2^{(\lambda+\varepsilon)n}$. Analogously, we have $|L^\times| < 2^{(\lambda+\varepsilon)n}$. For ease of notation, we abbreviate the probabilities that strings with small probabilities occur with $q^+ := Q^+(S^+)$ and $q^\times := Q^\times(S^\times)$. It follows immediately from Theorem 3.1 that $q^+ + q^\times \geq 1 - negl(n)$.

We define $\mathcal{E}$ to be the event $X \in S^R$. Then $P[\mathcal{E}|R=+] = P[X \in S^+|R=+] = q^+$ and similarly $P[\mathcal{E}|R=\times] = q^\times$, and the first claim follows immediately. Furthermore,

---

[2]Here is the mnemonic: S for the strings with Small probabilities, L for Large.

if R is uniformly distributed, then $P[\mathcal{E}] = P[\mathcal{E}|R\!=\!+]P_R(+) + P[\mathcal{E}|R\!=\!\times]P_R(\times) = \frac{1}{2}(q^+ + q^\times) \geq \frac{1}{2} - negl(n)$. Regarding the second claim, in case $R = +$, we have

$$
\mathrm{H}_\infty(X|R\!=\!+,\mathcal{E}) = -\log\left(\max_{x\in S^+} \frac{Q^+(x)}{q^+}\right)
$$

$$
\geq -\log\left(\frac{2^{-(\lambda+\varepsilon)n}}{q^+}\right) = \lambda n + \varepsilon n + \log(q^+).
$$

Thus, if $q^+ \geq 2^{-\varepsilon n}$, then indeed $\mathrm{H}_\infty(X|R\!=\!+, X \in S^+) \geq \lambda n$. The corresponding holds for the case $R = \times$.

Finally, if $q^+ < 2^{-\varepsilon n}$ (or similarly $q^\times < 2^{-\varepsilon n}$), then instead of the above, we define $\mathcal{E}$ as the *empty event* if $R = +$ and as the event $X \in S^\times$ if $R = \times$. It follows that $P[\mathcal{E}|R = +] = 0$ and $P[\mathcal{E}|R = \times] = q^\times \geq 1 - negl(n)$, as well as $\mathrm{H}_\infty(X|R\!=\!\times,\mathcal{E}) = \mathrm{H}_\infty(X|R\!=\!\times, X \in S^\times) \geq \lambda n + \varepsilon n + \log(q^\times) \geq \lambda n$ (for n large enough), both by the bound on $q^+ + q^\times$ and on q^+, whereas $P_{R|\mathcal{E}}(+) = 0$.   □

4. Rabin oblivious transfer.

4.1. The definition. A protocol for Rabin oblivious transfer (ROT) between sender Alice and receiver Bob allows for Alice to send a bit b through an erasure channel to Bob. Each transmission delivers b or an erasure with probability $\frac{1}{2}$. Intuitively, a protocol for ROT is secure if

   (i) the sender Alice gets no information on whether b was received or not, no matter what she does, and

   (ii) the receiver Bob gets no information about b with probability at least $\frac{1}{2}$, no matter what he does.

In this paper, we are considering quantum protocols for ROT. This means that while the inputs and outputs of the honest senders are classical, described by random variables, the protocol may contain quantum computation and quantum communication, and the view of a dishonest player is quantum and is thus described by a quantum state.

Any such (two-party) protocol is specified by a family $\{(\mathsf{S}_n, \mathsf{R}_n)\}_{n>0}$ of pairs of interactive quantum circuits (i.e., interacting through a quantum channel). Each pair is indexed by a security parameter $n > 0$, where S_n and R_n denote the circuits for sender Alice and receiver Bob, respectively. In order to simplify the notation, we often omit the index n, leaving the dependency on it implicit.

For the formal definition of the security requirements of a ROT protocol, let us fix the following notation. Let B denote the binary random variable describing S's input bit b, and let A and Y denote the binary random variables describing R's two output bits, where the meaning is that A indicates whether the bit was received or not. Furthermore, for a dishonest sender $\tilde{\mathsf{S}}$, we have the ccq-state $\rho_{AY\tilde{\mathsf{S}}}$, where (by slight abuse of notation) we also denote by $\tilde{\mathsf{S}}$ the quantum register that the sender outputs. Its state may depend on A and Y. Similarly, for a dishonest receiver $\tilde{\mathsf{R}}$, we have the cq-state $\rho_{B\tilde{\mathsf{R}}}$.

DEFINITION 4.1. *A (statistically) secure ROT is a two-party (quantum) protocol* (S, R) *with the following properties.*

Correctness: *For honest* S *and* R, $P[B = Y|A = 1] \geq 1 - negl(n)$.

Receiver-security: *For honest* R *and any dishonest* $\tilde{\mathsf{S}}$, *there exists a binary random variable* B' *such that* $P[B' = Y|A = 1] \geq 1 - negl(n)$ *and* $\delta\big(\rho_{AB'\tilde{\mathsf{S}}}, \mathbb{1} \otimes \rho_{B'\tilde{\mathsf{S}}}\big) \leq negl(n)$.

Sender-security: *For any* $\tilde{\mathsf{R}}$, *there exists an event* $\mathcal{E}$ *with* $P[\mathcal{E}] \geq \frac{1}{2} - negl(n)$ *such that*
$$\delta\left(\rho_{B\tilde{\mathsf{R}}|\mathcal{E}}, \rho_B \otimes \rho_{\tilde{\mathsf{R}}|\mathcal{E}}\right) \leq negl(n).$$
If any of the negligible terms above equals 0, *then the corresponding property is said to hold* perfectly. *If one of the properties holds only with respect to a restricted class* $\mathfrak{S}$ *of* $\tilde{\mathsf{S}}$*'s (resp.,* $\mathfrak{R}$ *of* $\tilde{\mathsf{R}}$*'s), then this property is said to hold and the protocol is said to be secure* against $\mathfrak{S}$ *(resp.,* $\mathfrak{R}$*).*

Statistical receiver-security guarantees that the joint quantum state after the execution of the protocol is, up to a negligible difference, the same as when the dishonest sender prepares the cq-state $\rho_{B'\tilde{\mathsf{S}}}$, and gives the classical bit B' to an ideal functionality which then passes it on to the receiver with probability $\frac{1}{2}$.[3] Statistical sender-security guarantees that the joint quantum state is, up to a negligible difference, the same as when the dishonest receiver gets the sender's bit B with probability at most $\frac{1}{2}$ and prepares the state $\rho_{\tilde{\mathsf{R}}|\mathcal{E}}$ in case he does not receive it, and else the state $\rho_{\tilde{\mathsf{R}}|\bar{\mathcal{E}}}^b = \rho_{\tilde{\mathsf{R}}|B=b,\bar{\mathcal{E}}}$ if $B = b$. In other words, security guarantees that the dishonest party cannot do more than when attacking an ideal functionality.

A formal treatment of the *composability* is beyond the scope of this paper. However, upcoming work of the authors implies that any quantum ROT protocol which satisfies Definition 4.1 securely replaces an ideal ROT functionality when used sequentially in a purely *classical* protocol. We also refer to [43] for recent results about the composition of quantum protocols in the bounded-quantum-storage model.

4.2. The protocol. We introduce a quantum protocol for ROT that will be shown to be perfectly receiver-secure (against any sender) and statistically sender-secure against any quantum-memory-bounded receiver. Our protocol exhibits some similarity to quantum conjugate coding introduced by Wiesner [44].

The protocol is very simple (see Figure 4.1): S picks $x \in_R \{0,1\}^n$ and sends to R n qubits in either state $|x\rangle_+$ or $|x\rangle_\times$, each chosen with probability $\frac{1}{2}$. R then measures all received qubits either in the rectilinear or in the diagonal basis. With probability $\frac{1}{2}$, R picks the right basis and gets x, while any $\tilde{\mathsf{R}}$ that is forced to measure part of the state (due to a memory bound) can have full information on x only in case the $+$-basis was used *or* in case the $\times$-basis was used (but not in both cases). Privacy amplification based on any two-universal class of hashing functions $\mathcal{F}_n$ is then used to destroy partial information. (In order to avoid aborting, we specify that if a dishonest $\tilde{\mathsf{S}}$ refuses to participate or sends data in incorrect format, then R samples both of its output bits a and y at random in $\{0,1\}$.)

We first consider receiver-security.

PROPOSITION 4.2. QOT *is perfectly receiver-secure.*

It is obvious that no information about whether R has received the bit is leaked to any sender $\tilde{\mathsf{S}}$, since R does not send anything. However, one needs to show the existence of a random variable B' as required by receiver-security.

Proof. Recall that the density matrix $\rho_{AY\tilde{\mathsf{S}}}$ is defined by the experiment where the dishonest sender $\tilde{\mathsf{S}}$ interacts with the honest memory-bounded R. Consider a modification of the experiment where we allow R to be *unbounded* in memory and where R waits to receive r and then measures all qubits in basis r. Let X' be the

---

[3]Note that the original definition given in [17] does not guarantee that the distribution of the input bit is determined at the end of the execution of ROT. This is a strictly weaker definition and does not fully capture what is expected from a ROT: it is easy to see that if the dishonest sender can still influence his input bit after the execution of the protocol, then known schemes based on ROT, such as bit commitments, are not secure anymore. The security definition given here is in the spirit of the security definition from [16] for 1-2 OT.

QOT(b):
1. S picks $x \in_R \{0,1\}^n$, and $r \in_R \{+, \times\}$.
2. S sends $|\psi\rangle := |x\rangle_r$ to R (i.e., the string x in basis r).
3. R picks $r' \in_R \{+, \times\}$ and measures all qubits of $|\psi\rangle$ in basis r'. Let $x' \in \{0,1\}^n$ be the result.
4. S announces r, $f \in_R \mathcal{F}_n$, and $e := b \oplus f(x)$.
5. R outputs $a := 1$ and $y := e \oplus f(x')$ if $r' = r$ and else $a := 0$ and $y := 0$.

FIG. 4.1. *Protocol for quantum Rabin OT.*

resulting string. Nevertheless, R picks $r' \in_R \{+, \times\}$ at random and outputs $(A, Y) = (0,0)$ if $r' \neq r$ and $(A, Y) = (1, e \oplus f(X'))$ if $r' = r$. Since the only difference between the two experiments is *when* R measures the qubits and *in what basis* R measures them when $r \neq r'$, in which case his final output is independent of the measurement outcome, the two experiments result in the same $\rho_{AY\tilde{S}}$. However, in the modified experiment we can choose B' to be $e \oplus f(X')$ such that by construction $B' = Y$ if $A = 1$ and A is uniformly distributed, independent of anything, and thus $\rho_{AB'\tilde{S}} = \mathbb{1} \otimes \rho_{B'\tilde{S}}$. ☐

As we shall see in section 4.4, the security of the QOT protocol against receivers with bounded-size quantum memory holds as long as the bound applies before step 4 is reached. An equivalent protocol is obtained by purifying the sender's actions. Although QOT is easy to implement, the purified or EPR-based version [23] depicted in Figure 4.2 is easier to prove secure. A similar approach was taken in the Shor–Preskill proof of security for the BB84 quantum key distribution scheme [41].

EPR-QOT(b):
1. S prepares n EPR pairs each in state $|\Omega\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$.
2. S sends one half of each pair to R and keeps the other halves.
3. R picks $r' \in_R \{+, \times\}$ and measures all received qubits in basis r'. Let $x' \in \{0,1\}^n$ be the result.
4. S picks $r \in_R \{+, \times\}$ and measures all kept qubits in basis r. Let $x \in \{0,1\}^n$ be the outcome. S announces r, $f \in_R \mathcal{F}_n$, and $e := b \oplus f(x)$.
5. R outputs $a := 1$ and $y := e \oplus f(x')$ if $r' = r$ and else $a := 0$ and $y := 0$.

FIG. 4.2. *Protocol for EPR-based quantum Rabin OT.*

Notice that while QOT requires no quantum memory for honest players, quantum memory for S seems to be required in EPR-QOT. The following lemma shows the strict equivalence between QOT and EPR-QOT.

LEMMA 4.3. QOT *is sender-secure if and only if* EPR-QOT *is.*

Proof. The proof follows easily after observing that S's choices of r and f, together with the measurements, all commute with $\tilde{R}$'s actions. Therefore, they can be performed right after step 1 with no change for $\tilde{R}$'s view. Modifying EPR-QOT that way results in QOT. ☐

Note that for a dishonest receiver it is not only irrelevant whether he tries to attack QOT or EPR-QOT, but in fact there is no difference in the two protocols from his point of view.

4.3. Modeling dishonest receivers. We model dishonest receivers in QOT, respectively, EPR-QOT, under the assumption that the maximum size of their quantum storage is bounded. These adversaries are required to have bounded quantum storage only when they reach step 4 in (EPR-)QOT. Before that, the adversary can store and carry out quantum computations involving any number of qubits. Apart from the restriction on the size of the quantum memory available to the adversary, no other assumption is made. In particular, the adversary is not assumed to be computationally bounded, and the size of its classical memory is not restricted.

DEFINITION 4.4. *The set $\mathfrak{R}_\gamma$ denotes all possible quantum dishonest receivers $\{\tilde{\mathsf{R}}_n\}_{n>0}$ in QOT or EPR-QOT where for each $n > 0$, $\tilde{\mathsf{R}}_n$ has quantum memory of size at most γn when step 4 is reached.*

In general, the adversary $\tilde{\mathsf{R}}$ is allowed to perform any quantum computation compressing the n qubits received from S into a quantum register M of size at most γn when step 4 is reached. More precisely, the compression function is implemented by some unitary transform C acting upon the quantum state received and an ancilla of arbitrary size. The compression is performed by a measurement that we assume in the computational basis without loss of generality. Before starting step 4, the adversary first applies a unitary transform C:

$$2^{-n/2} \sum_{x \in \{0,1\}^n} |x\rangle \otimes C|x\rangle|0\rangle \mapsto 2^{-n/2} \sum_{x \in \{0,1\}^n} |x\rangle \otimes \sum_y \alpha_{x,y} |\varphi_{x,y}\rangle^M |y\rangle^Y,$$

where for all x, $\sum_y |\alpha_{x,y}|^2 = 1$. Then, a measurement in the computational basis is applied to register Y providing classical outcome y. The result is a quantum state in register M of size γn qubits. Ignoring the value of y to ease the notation, the renormalized state of the system in its most general form when step 4 in EPR-QOT is reached is thus of the form

$$|\psi\rangle = \sum_{x \in \{0,1\}^n} \alpha_x |x\rangle \otimes |\varphi_x\rangle^M,$$

where $\sum_x |\alpha_x|^2 = 1$. We will prove security for any such state $|\psi\rangle$ and thus conditioned on any value y that may be observed. It is therefore safe to leave the dependency on y implicit.

4.4. Security against dishonest receivers. In this section, we show that EPR-QOT is secure against any dishonest receiver having access to a quantum storage device of size strictly smaller than half the number of qubits received at step 2.

THEOREM 4.5. *For all $\gamma < \frac{1}{2}$, QOT is statistically secure against $\mathfrak{R}_\gamma$.*

Proof. After Lemmas 4.3 and 4.2, it remains to show that EPR-QOT is sender-secure against $\mathfrak{R}_\gamma$. Since $\gamma < \frac{1}{2}$, we can find $\varepsilon > 0$ with $\gamma + \varepsilon < \frac{1}{2}$. Consider a dishonest receiver $\tilde{\mathsf{R}}$ in EPR-QOT with quantum memory of size γn. Let R and X denote the random variables describing the basis r and the outcome x of S's measurement (in basis r) in step 4 of EPR-QOT, respectively. We implicitly understand the distribution of X given R to be conditioned on the classical outcome y of the measurement $\tilde{\mathsf{R}}$ performed when the memory bound applies, as described in section 4.3; the following analysis works no matter what y is. Corollary 3.3 with $\lambda = \gamma + \varepsilon$ implies the existence of an event $\mathcal{E}$ such that $P[\mathcal{E}] \geq \frac{1}{2} - negl(n)$ and such that $\mathrm{H}_\infty(X|R{=}r, \mathcal{E}) \geq \gamma n + \varepsilon n$ for any relevant r. Note that by construction, the random variables X and R, and thus also the event $\mathcal{E}$, are independent of the sender's input bit B, and hence $\rho_{B|\mathcal{E}} = \rho_B$. It remains to show that $\delta(\rho_{B\tilde{\mathsf{R}}|\mathcal{E}}, \rho_{B|\mathcal{E}} \otimes \rho_{\tilde{\mathsf{R}}|\mathcal{E}}) \leq negl(n)$. As the bit B is masked by the

output of the hash function $F(X)$ in step 4 of EPR-QOT (where the random variable F represents the random choice for f), it suffices to show that $F(X)$ is close to uniform and essentially independent from $\tilde{\mathsf{R}}$'s view, conditioned on $\mathcal{E}$. But this is guaranteed by the above bound on $\mathrm{H}_\infty(X|R=r,\mathcal{E})$ and by Theorem 2.1.   □

4.5. On the necessity of privacy amplification. In this section, we show that randomized privacy amplification is needed for protocol QOT to be secure. For instance, it is tempting to believe that the sender could use the XOR $\bigoplus_i x_i$ in order to mask the bit b, rather than $f(x)$ for a randomly sampled $f \in \mathcal{F}_n$. This would reduce the communication complexity as well as the number of random coins needed. However, we argue in this section that this is not secure (against an adversary as we model it). Indeed, somewhat surprisingly, this variant can be broken by a dishonest receiver that has *no quantum memory at all* (but that can do coherent measurements on pairs of qubits) in the case n is even. For odd n, the dishonest receiver needs to store *a single qubit*.

Clearly, a dishonest receiver can break the modified scheme QOT and learn the bit b with probability 1 if he can compute $\bigoplus_i x_i$ with probability 1. Note that, using the equivalence between QOT and EPR-QOT, x_i can be understood as the outcome of the measurement in either the +- or the ×-basis, performed by the sender on one part of an EPR pair while the other has been handed over to the receiver. The following proposition shows that indeed the receiver can learn $\bigoplus_i x_i$ by a suitable measurement of his parts of the EPR pairs. Concretely, he measures the qubits he receives pairwise by a suitable measurement which allows him to learn the XOR of the two corresponding x_i's, no matter what the basis is (and he needs to store one single qubit in case n is odd). This obviously allows him to learn the XOR of all x_i's in all cases.

PROPOSITION 4.6. *Consider two EPR pairs, i.e., $|\psi\rangle = \frac{1}{2}\sum_x |x\rangle^S |x\rangle^R$, where x ranges over $\{0,1\}^2$. Let $r \in \{+,\times\}$, and let x_1 and x_2 be the result when measuring the two qubits in register S in basis r. There exists a fixed measurement for register R so that the outcome together with r uniquely determines $x_1 \oplus x_2$.*

Proof. The measurement that does the job is the *Bell measurement*, i.e., the measurement in the Bell basis $\{|\Phi^+\rangle, |\Psi^+\rangle, |\Phi^-\rangle, |\Psi^-\rangle\}$. Recall that

$$\left|\Phi^+\right\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle_+ + |11\rangle_+\right) = \frac{1}{\sqrt{2}}\left(|00\rangle_\times + |11\rangle_\times\right),$$

$$\left|\Psi^+\right\rangle = \frac{1}{\sqrt{2}}\left(|01\rangle_+ + |10\rangle_+\right) = \frac{1}{\sqrt{2}}\left(|00\rangle_\times - |11\rangle_\times\right),$$

$$\left|\Phi^-\right\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle_+ - |11\rangle_+\right) = \frac{1}{\sqrt{2}}\left(|01\rangle_\times + |10\rangle_\times\right),$$

$$\left|\Psi^-\right\rangle = \frac{1}{\sqrt{2}}\left(|01\rangle_+ - |10\rangle_+\right) = \frac{1}{\sqrt{2}}\left(|10\rangle_\times - |01\rangle_\times\right).$$

Due to the special form of the Bell basis, when register R is measured and, as a consequence, one of the four Bell states is observed, the state in register S collapses to that *same* Bell state. Indeed, when doing the basis transformation, all cross-products cancel each other out. It now follows by inspection that knowledge of the Bell state and the basis r allows one to predict the XOR of the two bits observed when measuring the Bell state in basis r. For instance, for the Bell state $|\Psi^+\rangle$, the XOR is 1 if $r = +$ and 0 if $r = \times$.   □

Note that from the above proof one can see that the receiver's attack (resp., his

measurement on each pair of qubits) can be understood as teleporting one of the two entangled qubits from the receiver to the sender using the other as EPR pair. However, the receiver does not send the outcome of his measurement to the sender, but keeps it in order to predict the XOR.

Clearly, the same strategy also works against any fixed linear function. Therefore, the only hope for doing deterministic privacy amplification is by using a nonlinear function. However, it has been shown recently in [1] that this approach is also doomed to fail in our scenario, because the outcome of *any Boolean function* can be perfectly predicted by a dishonest receiver who can store a single qubit and later learns the correct basis $r \in \{+, \times\}$.

4.6. Weakening the assumptions. Observe that QOT requires error-free quantum communication, in that a transmitted bit b that is encoded by the sender and measured by the receiver using the same basis is always received as b. In addition, it also requires a perfect quantum source which on request produces *one and only one* qubit in the right state, e.g., *one* photon with the right polarization. Indeed, in case of noisy quantum communication, an honest receiver in QOT is likely to receive an incorrect bit, and the sender-security of QOT is vulnerable to imperfect sources that once in a while transmit more than one qubit in the same state: a malicious receiver $\tilde{\mathsf{R}}$ can easily determine the basis $r \in \{+, \times\}$ and measure all the following qubits in the right basis. However, current technology only allows one to approximate the behavior of single-photon sources and noise-free quantum communication. It would be preferable to find a variant of QOT that allows one to weaken the technological requirements put upon the honest parties.

In this section, we present such a protocol based on BB84 states [2], BB84-QOT (see Figure 4.3). The security proof follows essentially by adapting the security analysis of QOT in a rather straightforward way, as will be discussed later.

Let us consider a quantum channel with an error probability $\phi < \frac{1}{2}$; i.e., ϕ denotes the probability that a transmitted bit b that is encoded by the sender and measured by the receiver using the same basis is received as $1 - b$. For the sake of simplicity we assume that the error rate is the same for qubits encoded in the +- and ×-basis. It is straightforward to adapt the analysis below to basis-dependent error rates. In order to not have the security rely on any level of noise, we assume the error probability to be zero when considering a *dishonest* receiver. Also, let us consider a quantum source which produces two or more qubits (in the same state), rather than just one, with probability $\eta < 1 - \phi$. We assume that the parameters ϕ and η which describe the precision of the physical apparatus being used are known to the players.

We call this the (ϕ, η)-weak quantum model. By adjusting the parameters, this model can also cope with dark counts and empty pulses; see section 6.1.

In order to deal with noisy quantum communication, we need to do error-correction without giving the adversary too much information. Techniques for solving this problem are known as *information reconciliation* (e.g., [9]) or as *secure sketches* [20]. Let $x \in \{0, 1\}^\ell$ be an arbitrary string, and let $x' \in \{0, 1\}^\ell$ be the result of flipping every bit in x (independently) with probability ϕ. It is well known that learning the syndrome $S(x)$ of x, with respect to a suitable efficiently decodable linear error-correcting code C of length ℓ, allows us to recover x from x', except with negligible probability in ℓ (e.g., [33, 12, 20]). Furthermore, it is known from coding theory that, for large enough ℓ, such a code can be chosen with rate R arbitrarily close to but smaller than $1 - h(\phi)$, i.e., such that the syndrome length s is bounded by $s < (h(\phi) + \varepsilon)\ell$, where $\varepsilon > 0$ (see, e.g., [12] or the full version of [20] and the references therein).

Regarding the loss of information, we can analyze privacy amplification in a similar way as before, just by appending a register for the syndrome $S(x)$ to the quantum register E. Using that $S_0(\rho_{S(X)\mathsf{E}}) \leq q + s$, Theorem 2.1 then reads

$$(4.1) \qquad \delta\big(\rho_{F(X)FS(X)\mathsf{E}}, \mathbb{1} \otimes \rho_{FS(X)\mathsf{E}}\big) \leq \frac{1}{2} 2^{-\frac{1}{2}(\mathrm{H}_\infty(X) - q - s - 1)}.$$

Consider the protocol BB84-QOT in the (ϕ, η)-weak quantum model shown in Figure 4.3. The protocol uses an efficiently decodable linear code C_ℓ, parametrized in $\ell \in \mathbb{N}$, with codeword length ℓ, rate $R = 1 - h(\phi) - \varepsilon$ for some small $\varepsilon > 0$, and the ability to correct errors occurring with probability ϕ (except with negligible probability). Let S_ℓ be the corresponding syndrome function. As before, the memory bound in BB84-QOT applies before step 4.

BB84-QOT(b):
1. S picks $x \in_R \{0,1\}^n$ and $\theta \in_R \{+, \times\}^n$.
2. S sends x_i in the corresponding bases $|x_1\rangle_{\theta_1}, \ldots, |x_n\rangle_{\theta_n}$ to R.
3. R picks $r' \in_R \{+, \times\}$ and measures all qubits in basis r'. Let $x' \in \{0,1\}^n$ be the result.
4. S picks $r \in_R \{+, \times\}$, sets $I := \{i : \theta_i = \{+, \times\}_{[r]}\}$ and $\ell := |I|$, and announces r, I, $syn := S_\ell(x|_I)$, $f \in_R \mathcal{F}_\ell$, and $e := b \oplus f(x|_I)$.
5. R recovers $x|_I$ from $x'|_I$ and syn, and outputs $a := 1$ and $b' := e \oplus f(x|_I)$ if $r' = r$ and else $a := 0$ and $b' := 0$.

FIG. 4.3. *Protocol for the BB84 version of quantum Rabin OT.*

By the abovementioned properties of the code C_ℓ, it is obvious that R receives the correct bit b if $r' = r$, except with negligible probability. (The error probability is negligible in ℓ, but by Bernstein's law of large numbers, ℓ is linear in n except with negligible probability.) Also, since there is no communication from R to S, a dishonest sender $\tilde{\mathsf{S}}$ cannot learn whether R received the bit. In fact, BB84-QOT can be shown to be perfectly receiver-secure in the same way as in Proposition 4.2. In a manner similar to that for protocol QOT, in order to argue about sender-security we compare BB84-QOT with a purified version shown in Figure 4.4. BB84-EPR-QOT runs in the $(\phi, 0)$-weak quantum model, and the imperfectness of the quantum source assumed in BB84-QOT is simulated by S in BB84-EPR-QOT so that there is no difference from R's point of view.

The security equivalence between BB84-QOT (in the (ϕ, η)-weak quantum model) and BB84-EPR-QOT (in the $(\phi, 0)$-weak quantum model) is omitted here as it follows essentially along the same lines as in section 4.2.

THEOREM 4.7. *In the (ϕ, η)-weak quantum model, BB84-QOT is statistically secure against $\mathfrak{R}_\gamma$ for any $\gamma < \frac{1-\eta}{4} - \frac{h(\phi)}{2}$ (if parameter ε is chosen small enough).*

Proof sketch. It remains to show that BB84-EPR-QOT is statistically sender-secure against $\mathfrak{R}_\gamma$ (in the $(\phi, 0)$-weak quantum model). The reasoning goes exactly along the lines of the proof of Theorem 4.5, except that we restrict our attention to those i's which are in J. By Bernstein's law of large numbers, ℓ lies within $(1 \pm \varepsilon)n/2$ and $|J|$ within $(1 - \eta \pm \varepsilon)n/2$ except with negligible probability. In order to make the proof easier to read, we assume that $\ell = n/2$ and $|J| = (1 - \eta)n/2$ and also treat the ε occurring in the rate of the code C_ℓ as zero. For the full proof, we simply need to carry the ε's along and then choose them small enough at the end of the proof.

BB84-EPR-QOT(b):
1. S prepares n EPR pairs each in state $|\Omega\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$. Additionally, S initializes $I'_+ := \emptyset$ and $I'_\times := \emptyset$.
2. For every $i \in \{1, \ldots, n\}$, S does the following. With probability $1 - \eta$, S sends one half of the ith pair to R and keeps the other half. While with probability η, S picks $\theta_i \in_R \{+, \times\}$, replaces I'_{θ_i} by $I'_{\theta_i} \cup \{i\}$, and sends two or more qubits in the same state $|x_i\rangle_{\theta_i}$ to R, where $x_i \in_R \{0, 1\}$.
3. R picks $r' \in_R \{+, \times\}$ and measures all received qubits in basis r'. Let $x' \in \{0, 1\}^n$ be the result.
4. S picks a random index set $J \subset_R \{1, \ldots, n\} \setminus (I'_+ \cup I'_\times)$. Then, it picks $r \in_R \{+, \times\}$, sets $I := J \cup I'_r$ and $\ell := |I|$, and for each $i \in J$ measures the corresponding qubit in basis r. Let x_i be the corresponding outcome, and let $x|_I$ be the collection of all x_i's with $i \in I$. S announces r, I, $syn = S_\ell(x|_I)$, $f \in_R \mathcal{F}_\ell$, and $e = b \oplus f(x|_I)$.
5. R recovers $x|_I$ from $x'|_I$ and syn, and outputs $a := 1$ and $b' := e \oplus f(x|_I)$, if $r' = r$ and else $a := 0$ and $b' := 0$.
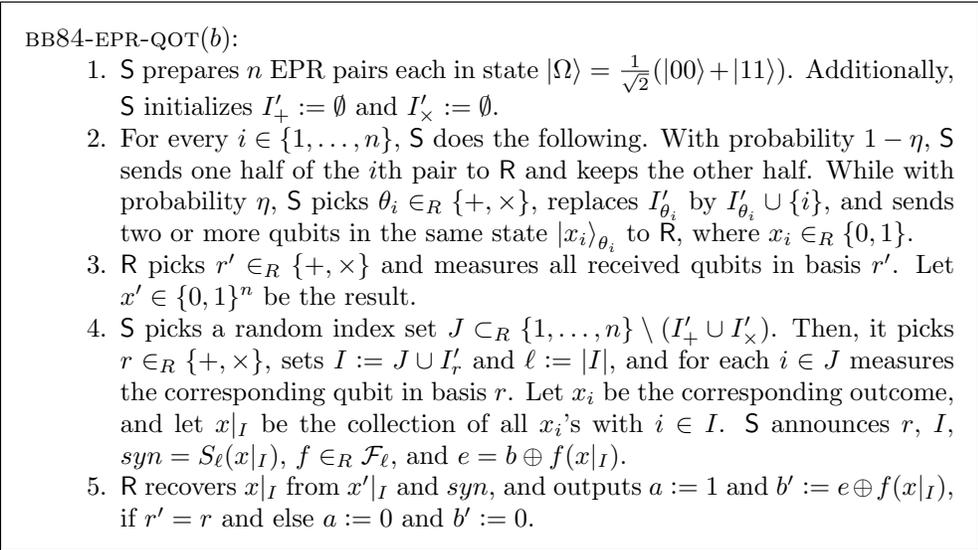
FIG. 4.4. *Protocol for EPR-based quantum Rabin OT, BB84 version.*

Write $n' = |J| = (1 - \eta)n/2$, and let γ' be such that $\gamma n = \gamma' n'$, i.e., $\gamma' = 2\gamma/(1 - \eta)$. Assume $\kappa > 0$ such that $\gamma' + \kappa < \frac{1}{2}$, where we make sure later that such κ exists. It then follows from Corollary 3.3 that there exists an event $\mathcal{E}$ such that $P[\mathcal{E}] \geq \frac{1}{2} - negl(n') = \frac{1}{2} - negl(n)$ and

$$\mathrm{H}_\infty\big(X|_J \big| R = r, \mathcal{E}\big) \geq (\gamma' + \kappa)n' = \gamma n + \kappa(1 - \eta)n/2\,.$$

By (4.1), it remains to argue that this is larger than $q + s = \gamma n + h(\phi)n/2$; i.e.,

$$\kappa(1 - \eta) > h(\phi)\,,$$

where κ has to satisfy

$$\kappa < \frac{1}{2} - \gamma' = \frac{1}{2} - \frac{2}{\gamma/(1 - \eta)}\,.$$

This can obviously be achieved (by choosing κ appropriately) if and only if the claimed bound on γ holds. ∎

5. Quantum commitment scheme. In this section, we present a BC scheme from a committer C with bounded quantum memory to an unbounded receiver V. The scheme is peculiar since in order to commit to a bit, the committer does not send anything. During the committing stage information goes only from V to C. The security analysis of the scheme uses similar techniques as the analysis of EPR-QOT.

5.1. The protocol. The objective of this section is to present a bounded-quantum-memory BC scheme COMM (see Figure 5.1). Intuitively, a commitment to a bit b is made by measuring random BB84-states in basis $\{+, \times\}_{[b]}$.

It is clear that EPR-COMM is hiding, i.e., that the commit phase reveals no information on the committed bit, since no information is transmitted to V at all. Hence we have the following lemma.

COMM(b):
1. V picks $x \in_R \{0,1\}^n$ and $r \in_R \{+, \times\}^n$.
2. V sends x_i in the corresponding bases $|x_1\rangle_{r_1}, |x_2\rangle_{r_2}, \ldots, |x_n\rangle_{r_n}$ to C.
3. C commits to the bit b by measuring all qubits in basis $\{+, \times\}_{[b]}$. Let $x' \in \{0,1\}^n$ be the result.
4. To open the commitment, C sends b and x' to V.
5. V verifies that $x_i = x_i'$ for those i where $r_i = \{+, \times\}_{[b]}$. V accepts if and only if this is the case.

FIG. 5.1. *Protocol for quantum commitment.*

LEMMA 5.1. EPR-COMM *is perfectly hiding.*

As for the OT-protocol of section 4.2, we present an equivalent EPR-version of the protocol that is easier to analyze (see Figure 5.2).

EPR-COMM(b):
1. V prepares n EPR pairs each in state $|\Omega\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$.
2. V sends one half of each pair to C and keeps the other halves.
3. C commits to the bit b by measuring all received qubits in basis $\{+, \times\}_{[b]}$. Let $x' \in \{0,1\}^n$ be the result.
4. To open the commitment, C sends b and x' to V.
5. V measures all his qubits in basis $\{+, \times\}_{[b]}$ and obtains $x \in \{0,1\}^n$. He chooses a random subset $I \subseteq \{1, \ldots, n\}$. V verifies that $x_i = x_i'$ for all $i \in I$ and accepts if and only if this is the case.

FIG. 5.2. *Protocol for EPR-based quantum commitment.*

LEMMA 5.2. COMM *is secure against dishonest* $\tilde{\mathsf{C}}$ *if and only if* EPR-COMM *is.*

Proof. The proof uses similar reasoning as the proof of Lemma 4.3. First, it clearly makes no difference if we change step 5 to the following:

5′. V chooses the subset I, measures all qubits with index in I in basis $\{+, \times\}_{[b]}$ and all qubits not in I in basis $\{+, \times\}_{[1-b]}$. V verifies that $x_i = x_i'$ for all $i \in I$ and accepts if and only if this is the case.

Finally, we can observe that the view of $\tilde{\mathsf{C}}$ does not change if V would have done his choice of I and his measurement already in step 1. Doing the measurements at this point means that the qubits to be sent to $\tilde{\mathsf{C}}$ collapse to a state that is distributed identically to the state prepared in the original scheme. The EPR-version is therefore equivalent to the original commitment scheme from $\tilde{\mathsf{C}}$'s point of view. ☐

5.2. Modeling dishonest committers. A dishonest committer $\tilde{\mathsf{C}}$ with bounded memory of at most γn qubits in EPR-COMM can be modeled very similarly to the dishonest OT-receiver $\tilde{\mathsf{R}}$ from section 4.3: $\tilde{\mathsf{C}}$ consists first of a circuit acting on all n qubits received, then of a measurement of all but at most γn qubits, and finally of a circuit that takes the following input: a bit b that $\tilde{\mathsf{C}}$ will attempt to open, the γn qubits in memory, and some ancilla in a fixed state. The output is a string $x' \in \{0,1\}^n$ to be sent to V at the opening stage.

DEFINITION 5.3. *We define $\mathfrak{C}_\gamma$ to be the class of all committers $\{\tilde{\mathsf{C}}_n\}_{n>0}$ in* COMM *or* EPR-COMM *that, at the start of the opening phase (i.e., at step 4), have a quantum memory of size at most γn qubits.*

We adopt the binding condition for quantum BC from [21].

DEFINITION 5.4. *A (quantum) BC scheme is* (statistically) binding *against $\mathfrak{C}$ if for all $\{\tilde{\mathsf{C}}_n\}_{n>0} \in \mathfrak{C}$, the probability $p_b(n)$ that $\tilde{\mathsf{C}}_n$ opens $b \in \{0,1\}$ with success satisfies*

$$p_0(n) + p_1(n) \leq 1 + negl(n).$$

In the next section, we show that EPR-COMM is binding against $\mathfrak{C}_\gamma$ for any $\gamma < \frac{1}{2}$.

Note that the binding condition given here in Definition 5.4 is weaker than the classical one, where one would require that a bit b exists such that $p_b(n)$ is negligible. For a general quantum adversary who can always commit to 0 and 1 in superposition, however, this is too strong a requirement; thus, it is typically argued that Definition 5.4 is the best one can hope for. In upcoming work [16], though, we show that one *can* ask for a stronger binding property, and in fact protocol COMM proposed here does satisfy a stronger binding property (but for a smaller bound on the committer's quantum memory). While the weaker condition is sufficient for many applications, the stronger one seems to be necessary in some cases. For instance, intuitively, COMM can easily be transformed into a *string* commitment scheme simply by committing bitwise, but in order to prove this string commitment secure, it is necessary that COMM is secure with respect to the stronger security definition. However, proving COMM secure with respect to the stronger binding condition requires quite different techniques, and therefore we settle here for the weaker version and refer the interested reader to [16].

5.3. Security proof of the commitment scheme. Note that the first three steps of EPR-QOT and EPR-COMM (i.e., before the memory bound applies) are exactly the same! This allows us to reuse Corollary 3.3 and the analysis of section 4.4 to prove the binding property of EPR-COMM.

THEOREM 5.5. *For any $\gamma < \frac{1}{2}$,* COMM *is perfectly hiding and statistically binding against $\mathfrak{C}_\gamma$.*

Proof. It remains to show that EPR-COMM is binding against $\mathfrak{C}_\gamma$. Let $\varepsilon, \delta > 0$ be such that $\gamma + 2h(\delta) + 2\varepsilon < 1/2$, where h is the binary entropy function. Recall that $\mathrm{B}^{\delta n} \leq 2^{h(\delta)n}$. Let R be the basis, determined by the bit that $\tilde{\mathsf{C}}$ claims in step 4, in which V measures the quantum state in step 5, and let X be the outcome. Corollary 3.3 implies the existence of an event $\mathcal{E}$ such that $P[\mathcal{E}|R{=}+] + P[\mathcal{E}|R{=}\times] \geq 1 - negl(n)$ and $\mathrm{H}_\infty(X|R{=}r, \mathcal{E}) \geq (\gamma + 2h(\delta) + 2\varepsilon)n$. Applying Lemma 2.2, it follows that any guess $\hat{X}$ for X satisfies

$$P\big[\hat{X} \in \mathrm{B}^{\delta n}(X) \,|\, R{=}r, \mathcal{E}\big] \leq 2^{-\frac{1}{2}(\mathrm{H}_\infty(X|X\in S^+)-\gamma n-1)+\log(\mathrm{B}^{\delta n})} \leq 2^{-\varepsilon n+\frac{1}{2}}.$$

However, if $\hat{X} \notin \mathrm{B}^{\delta n}(X)$, then sampling a random subset of the positions will detect an error except with probability at most $2^{-\delta n}$. Hence, writing $q^+ := P[\mathcal{E}|R{=}+]$ and $q^\times := P[\mathcal{E}|R{=}\times]$,

$$p_0(n) \leq (1 - q^+) + q^+ \cdot (2^{-\varepsilon n+\frac{1}{2}} + 2^{-\delta n}) \leq 1 - q^+ + negl(n),$$

and analogously $p_1(n) \leq 1 - q^\times + negl(n)$. We conclude that

$$p_0(n) + p_1(n) \leq 2 - q^+ - q^\times + negl(n) \leq 1 + negl(n). \qquad \square$$

5.4. Weakening the assumptions. As argued earlier, assuming that a party can produce single qubits (with probability 1) is not reasonable given current technology. Also the assumption that there is no noise on the quantum channel is impractical. It can be shown that a straightforward modification of COMM remains secure in the (ϕ, η)-weak quantum model as introduced in section 4.6 (see also section 6.1), with $\phi < \frac{1}{2}$ and $\eta < 1 - \phi$.

Let COMM$'$ be the modification of COMM where in step 5 V accepts if and only if $x_i = x'_i$ for all *but about a ϕ-fraction* of the i, where $r_i = \{+, \times\}_{[b]}$. More precisely, for all but a $(\phi + \varepsilon)$-fraction, where $\varepsilon > 0$ is sufficiently small.

THEOREM 5.6. *In the (ϕ, η)-weak quantum model, COMM$'$ is perfectly hiding and is binding against $\mathfrak{C}_\gamma$ for any γ satisfying $\gamma < \frac{1}{2}(1 - \eta) - 2h(\phi)$.*

Proof sketch. Using Bernstein's law of large numbers, one can argue that for *honest* C and V, the opening of a commitment is accepted except with negligible probability. The hiding property holds using the same reasoning as in Lemma 5.1. And the binding property can be argued essentially along the lines of Theorem 5.5, with the following modifications. Let J denote the set of indices i where V succeeds in sending a single qubit. We restrict the analysis to those i's which are in J. By Bernstein's law of large numbers, the cardinality of J is about $(1 - \eta)n$ (meaning within $(1 - \eta \pm \varepsilon)n$), except with negligible probability. Thus, restricting to these i's has the same effect as replacing γ by $\gamma/(1 - \eta)$ (neglecting the $\pm\varepsilon$ to simplify notation). Assuming that $\tilde{\mathsf{C}}$ knows every x_i for $i \notin J$, for all x_i's with $i \in J$ he has to be able to guess all but about a $\phi/(1 - \eta)$-fraction correctly, in order to be successful in the opening. However, $\tilde{\mathsf{C}}$ succeeds with only negligible probability if

$$\phi/(1 - \eta) < \delta \,.$$

Additionally, δ must be such that

$$\frac{\gamma}{1 - \eta} + 2h(\delta) < \frac{1}{2} \,.$$

δ can be chosen that way if

$$2\,h\left(\frac{\phi}{1 - \eta}\right) + \frac{\gamma}{1 - \eta} < \frac{1}{2} \,.$$

Using the fact that $h(\nu p) \leq \nu h(p)$ for any $\nu \geq 1$ and $0 \leq p \leq \frac{1}{2}$ such that $\nu p \leq 1$, this is clearly satisfied if $2h(\phi) + \gamma < \frac{1}{2}(1 - \eta)$. □

6. Towards practice. In the following two sections, we elaborate on the question of how close to practice our systems are. First, we argue that imperfections occurring in practice like dark counts and empty pulses are covered by our (ϕ, η)-weak quantum model used in sections 4.6 and 5.6. Second, we sketch how our techniques can be extended to the more realistic setting of *noisy quantum memory*.

6.1. More imperfections. In practice, quantum transmissions are subject to other imperfections: dark counts and empty pulses. Dark counts occur due to thermal fluctuation in the detector hardware which results in detection even though no qubit was received. Dark counts contribute to the error rate (i.e., each dark count accounts for a bit error with probability $\frac{1}{2}$) of the channel. This imperfection can therefore be included in the (ϕ, η)-weak quantum model by an appropriate choice of parameter ϕ without the need for any further modification.

Empty pulses occur in two cases: when the quantum channel lets a transmitted qubit escape (or when it is absorbed) and when the source does not produce any qubit for a given time slot. The latter is unavoidable for sources using weak coherent pulses as is the case in most experimental settings. Weak coherent pulses approximate a single-qubit source by producing on average only a small fraction of one qubit per pulse. It means that although most of the pulses are empty, the probability for a multiqubit pulse is very small. In this case, the receiver must report to the sender the positions of all pulses detected. Assuming the honest sender knows a tight upper bound on the rate at which the source produces empty pulses, the adversary can only take advantage of empty pulses caused by absorption in the fiber. The best the adversary can do is to substitute the fiber for one that preserves all qubits sent and to report empty pulses when a single pulse has been received. The effect is to increase the rate at which multiqubit pulses occur. This attack is known as the *photon number splitting attack* [7, 8, 26] in quantum key distribution applications. It follows that empty pulses can also be included in the (ϕ, η)-weak quantum model by an appropriate adjustment of parameter η.

Assume that a practical implementation of BB84-QOT or COMM takes place in a setting where ϕ_X is the probability for a bit error caused by the channel, ϕ_{DC} is the probability for a dark count, η_{MQ} is the probability for a multiqubit transmission, and η_{AB} is the probability for an empty pulse caused by absorption. These parameters are defined under the condition that the source is sending out a signal. It follows that if BB84-QOT and COMM are secure in the $(\phi_X + \frac{\phi_{DC}}{2}, \frac{\eta_{MQ}}{1-\eta_{AB}})$-weak quantum model, then their implementation is also secure provided that it is accurately modeled by these four parameters.

A variety of imperfections specific to particular implementations can be adapted to the weak quantum model in a similar way.

6.2. Generalizing the memory model. The bounded-quantum-storage model limits the number of physical qubits the adversary's memory can contain. A more realistic model would rather address the noise process which the adversary's memory undergoes. For instance, it is not hard to build a very large but unreliable memory device containing a large number of qubits. It is reasonable to expect that our protocols remain secure also in a scenario where the adversary's memory is of arbitrary size, but where some quantum operation (modeling noise) is applied to it. Inequality (2.2) of the privacy amplification theorem, Theorem 2.1, allows us to apply our constructions to slightly more general memory models. In particular, all our protocols that are secure against adversaries with memory of no more than γn qubits are also secure against any noise model that reduces the rank of the mixed state ρ_E, held by the adversary, to at most $2^{\gamma n}$.

An example of a noise process resulting in a reduction of $H_0(\rho_E)$ is an erasure channel. Assuming the n initial qubits are each erased with probability larger than $1 - \gamma$ when the memory bound applies, it holds except with negligible probability in n that $H_0(\rho_E) < \gamma n$. The same applies if the noise process is modeled by a depolarizing channel with error probability $p = 1 - \gamma$. Such a depolarizing channel replaces each qubit by a random one with probability p and does nothing with probability $1 - p$.

The technique we have developed does not allow us to deal with depolarizing channels with $p < 1 - \gamma$ although one would expect that some $0 < p < 1 - \gamma$ should be sufficient to ensure security against such adversaries. The reason for this is that not knowing the positions where the errors occurred should make it more difficult for the adversary than when the noise process is modeled by an erasure channel. However,

it seems that our uncertainty relations (i.e., Theorems 3.1 and A.3) are not strong enough to address this case. Generalizing the bounded-quantum-storage model to more realistic noisy-memory models is an interesting open question.

7. Conclusion, further research, and open problems. We have shown how to construct ROT and BC securely in the bounded-quantum-storage model. Our protocols require no quantum memory for honest players and remain secure provided the adversary has access to only quantum memory of size bounded by a large fraction of all qubits transmitted. Such a gap between the amount of storage required for honest players and adversaries is not achievable by classical means. All our protocols are noninteractive and can be implemented using current technology.

In this paper, we considered ROT of only one bit per invocation. Our technique can easily be extended to deal with string ROT, essentially by using a class of two-universal functions with range $\{0,1\}^{\ell n}$ rather than $\{0,1\}$, for some ℓ with $\gamma + \ell < \frac{1}{2}$ (resp., $< \frac{1-\eta}{4} - \frac{h(\phi)}{2}$ for BB84-QOT).

Although other flavors of OTs can be constructed from ROT using standard reductions, a more direct approach would give a better ratio between storage bound and communication complexity. Recent extensions have shown that a 1-2 OT protocol built along the lines of BB84-QOT is secure against adversaries with bounded quantum memory [16]. Interestingly, the techniques used are quite different from the ones of this paper (which appear to fail in the case of 1-2 OT), and they additionally allow us to analyze and prove secure the BC scheme COMM with respect to the stronger security definition, as briefly discussed in section 5.2.

A main open problem is the optimality of the bound on the adversary's quantum memory. The protocol QOT for instance, appears to be secure against any adversary with memory less than n qubits, but our analysis requires the memory to be smaller than $n/2$. Also, finding protocols secure against adversaries in more general noisy-memory models, briefly discussed in section 6.2, would certainly be a natural and interesting extension of this work to more practical settings.

Appendix A. Uncertainty relation for more mutually unbiased bases. In this appendix, we generalize the uncertainty relations derived in section 3 to more than two mutually unbiased bases. Such uncertainty relations over more but not all mutually unbiased bases in terms of min-entropy may be of independent interest; see the discussion at the end of section 3.1.

First, we generalize Proposition 2.4 to more projectors.

PROPOSITION A.1. *For orthogonal projectors $A_0, A_1, A_2, \ldots, A_M$, it holds that*

$$(A.1) \qquad \left\| \sum_{i=0}^{M} A_i \right\| \leq 1 + M \cdot \max_{0 \leq i < j \leq M} \|A_i A_j\|.$$

Proof. Defining

$$X := \begin{pmatrix} A_0 & A_1 & \cdots & A_M \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & 0 \end{pmatrix} \quad \text{and} \quad Y := \begin{pmatrix} A_0 & 0 & \cdots & 0 \\ A_1 & 0 & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ A_M & 0 & \cdots & 0 \end{pmatrix}$$

yields

$$XY = \begin{pmatrix} A_0 + A_1 + \ldots + A_M & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & & \vdots & \vdots \\ 0 & 0 & \cdots & 0 \end{pmatrix} \quad \text{and}$$

$$YX = \begin{pmatrix} A_0 & A_0 A_1 & \cdots & A_0 A_M \\ A_1 A_0 & A_1 & \cdots & A_1 A_M \\ \vdots & \vdots & \ddots & \vdots \\ A_M A_0 & A_M A_1 & \cdots & A_M \end{pmatrix}.$$

The matrix YX can be additively decomposed into $M+1$ matrices according to the following pattern:

$$YX = \begin{pmatrix} * & & & \\ & * & & \\ & & \ddots & \\ & & & * \\ & & & & * \end{pmatrix} + \begin{pmatrix} 0 & * & & \\ & 0 & & \\ & & \ddots & \ddots \\ & & & 0 & * \\ * & & & & 0 \end{pmatrix} + \cdots + \begin{pmatrix} 0 & & & * \\ * & 0 & & \\ & \ddots & \ddots & \\ & & & 0 \\ & & * & 0 \end{pmatrix},$$

where the $*$'s stand for entries of YX and for $i = 0, \ldots, M$ the ith star pattern after the diagonal pattern is obtained by i cyclic shifts of the columns of the diagonal pattern.

As in the proof of Proposition 2.4, XY and YX are Hermitian, and we use Lemma 2.3, the triangle inequality, the unitary invariance of the operator norm, and the fact that for all $i \neq j : \|A_i\| = 1$ and $\|A_i A_j\| = \|A_j A_i\|$ to obtain the desired statement (A.1). □

DEFINITION A.2. *Sets* $\mathcal{B}^0, \mathcal{B}^1, \ldots, \mathcal{B}^M$ *of bases of the complex Hilbert space* $\mathbb{C}^{2^n}$ *are called* mutually unbiased *if for all* $i \neq j \in \{0, \ldots, M\}$, *it holds that*

$$\forall |\varphi\rangle \in \mathcal{B}^i, \quad \forall |\psi\rangle \in \mathcal{B}^j : |\langle \varphi | \psi \rangle|^2 = 2^{-n}.$$

THEOREM A.3. *Let the density matrix* ρ *describe the state of* n *qubits, and let* $\mathcal{B}^0, \mathcal{B}^1, \ldots, \mathcal{B}^M$ *be mutually unbiased bases of* $\mathbb{C}^{2^n}$. *Let* $Q^0(\cdot), Q^1(\cdot), \ldots, Q^M(\cdot)$ *be the distributions of the outcome when* ρ *is measured in bases* $\mathcal{B}^0, \mathcal{B}^1, \ldots, \mathcal{B}^M$, *respectively. Then, for any sets* $L^0, L^1, \ldots, L^M \subset \{0,1\}^n$, *it holds that*

$$\sum_{i=0}^{M} Q^i(L^i) \leq 1 + M \cdot 2^{-n/2} \max_{0 \leq i < j \leq M} \sqrt{|L^i||L^j|}.$$

Proof. The proof is analogous to that of Theorem 3.1. □

Analogous to Corollary 3.2, we derive an uncertainty relation about the sum of the min-entropies of up to $2^{n/2}$ distributions.

COROLLARY A.4. *For an* $\varepsilon > 0$, *let* $0 < M < 2^{\frac{n}{2} - \varepsilon n}$. *For* $i = 0, \ldots, M$, *let* H_∞^i *be the min-entropies of the distributions* Q^i *from the theorem above. Then,*

$$\sum_{i=0}^{M} \mathrm{H}_\infty^i \geq (M+1)\big(\log(M+1) - negl(n)\big).$$

Proof. For $i = 0, \ldots, M$, we denote by q_∞^i the maximal probability of Q^i and let L^i be the set containing only the n-bit string x with this maximal probability q_∞^i. Theorem A.3 together with the assumption about M assures $\sum_{i=0}^{M} q_\infty^i \leq 1 + negl(n)$. By the inequality of the geometric and arithmetic mean it follows that

$$\sum_{i=0}^{M} \mathrm{H}_\infty^i = -\log \prod_{i=0}^{M} q_\infty^i \geq -\log \left(\frac{1 + negl(n)}{M+1} \right)^{M+1}$$
$$= (M+1)\big(\log(M+1) - negl(n)\big). \quad \square$$

REFERENCES

[1] M. A. BALLESTER, S. WEHNER, AND A. WINTER, *State Discrimination with Post-Measurement Information*, http://arxiv.org/abs/quant-ph/0608014 (2006).

[2] 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, 1984, pp. 175–179.

[3] C. H. BENNETT, G. BRASSARD, C. CRÉPEAU, AND U. M. MAURER, *Generalized privacy amplification*, IEEE Trans. Inform. Theory, 41 (1995), pp. 1915–1923.

[4] C. H. BENNETT, G. BRASSARD, AND J.-M. ROBERT, *Privacy amplification by public discussion*, SIAM J. Comput., 17 (1988), pp. 210–229.

[5] R. BHATIA, *Matrix Analysis*, Grad. Texts in Math. 169, Springer, Berlin, 1997.

[6] I. BIALYNICKI-BIRULA AND J. MYCIELSKI, *Uncertainty relations for information entropy in wave mechanics*, Comm. Math. Phys., 44 (1975), pp. 129–132.

[7] G. BRASSARD, N. LÜTKENHAUS, T. MOR, AND B. C. SANDERS, *Limitations on practical quantum cryptography*, Phys. Rev. Lett., 85 (2000), pp. 1330–1333.

[8] G. BRASSARD, N. LÜTKENHAUS, T. MOR, AND B. C. SANDERS, *Security aspects of practical quantum cryptography*, in Advances in Cryptology—EUROCRYPT '00, Lecture Notes in Comput. Sci. 1807, Springer, Berlin, 2000, pp. 289–299.

[9] G. BRASSARD AND L. SALVAIL, *Secret-key reconciliation by public discussion*, in Advances in Cryptology—EUROCRYPT '93, Lecture Notes in Comput. Sci. 765, Springer, Berlin, 1993, pp. 410–423.

[10] C. CACHIN, C. CRÉPEAU, AND J. MARCIL, *Oblivious transfer with a memory-bounded receiver*, in Proceedings of the 39th Annual IEEE Symposium on Foundations of Computer Science (FOCS), 1998, pp. 493–502.

[11] J. L. CARTER AND M. N. WEGMAN, *Universal classes of hash functions*, in Proceedings of the 9th Annual ACM Symposium on Theory of Computing (STOC), 1977, pp. 106–112.

[12] C. CRÉPEAU, *Efficient cryptographic protocols based on noisy channels*, in Advances in Cryptology—EUROCRYPT '97, Lecture Notes in Comput. Sci. 1233, Springer, Berlin, 1997, pp. 306–317.

[13] C. CRÉPEAU AND J. KILIAN, *Achieving oblivious transfer using weakened security assumptions*, in Proceedings of the 29th Annual IEEE Symposium on Foundations of Computer Science (FOCS), 1988, pp. 42–53.

[14] I. DAMGÅRD, J. KILIAN, AND L. SALVAIL, *On the (im)possibility of basing oblivious transfer and bit commitment on weakened security assumptions*, in Advances in Cryptology—EUROCRYPT '99, Lecture Notes in Comput. Sci. 1592, Springer, Berlin, 1999, pp. 56–73.

[15] I. B. DAMGÅRD, S. FEHR, K. MOROZOV, AND L. SALVAIL, *Unfair noisy channels and oblivious transfer*, in Theory of Cryptography Conference (TCC), Lecture Notes in Comput. Sci. 2951, Springer, Berlin, 2004, pp. 355–373.

[16] 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 '07, Lecture Notes in Comput. Sci. 4622, Springer, Berlin, 2007, pp. 360–378.

[17] I. B. DAMGÅRD, S. FEHR, L. SALVAIL, AND C. SCHAFFNER, *Cryptography in the bounded quantum-storage model*, in Proceedings of the 46th Annual IEEE Symposium on Foundations of Computer Science (FOCS), 2005, pp. 449–458.

[18] D. DEUTSCH, *Uncertainty in quantum measurements*, Phys. Rev. Lett., 50 (1983), pp. 631–633.

[19] Y. Z. DING, D. HARNIK, A. ROSEN, AND R. SHALTIEL, *Constant-round oblivious transfer in the bounded storage model*, in Theory of Cryptography Conference (TCC), Lecture Notes in Comput. Sci. 2951, Springer, Berlin, 2004, pp. 446–472.

[20] Y. DODIS, L. REYZIN, AND A. SMITH, *Fuzzy extractors: How to generate strong keys from biometrics and other noisy data*, in Advances in Cryptology—EUROCRYPT '04, Lecture Notes in Comput. Sci. 3027, Springer, Berlin, 2004, pp. 523–540.

[21] P. DUMAIS, D. MAYERS, AND L. SALVAIL, *Perfectly concealing quantum bit commitment from any quantum one-way permutation*, in Advances in Cryptology—EUROCRYPT '00, Lecture Notes in Comput. Sci. 1807, Springer, Berlin, 2000, pp. 300–315.

[22] S. DZIEMBOWSKI AND U. M. MAURER, *On generating the initial key in the bounded-storage model*, in Advances in Cryptology—EUROCRYPT '04, Lecture Notes in Comput. Sci. 3027, Springer, Berlin, 2004, pp. 126–137.

[23] A. K. EKERT, *Quantum cryptography based on Bell's theorem*, Phys. Rev. Lett., 67 (1991), pp. 661–663.

[24] C. A. FUCHS AND J. VAN DE GRAAF, *Cryptographic distinguishability measures for quantum-mechanical states*, IEEE Trans. Inform. Theory, 45 (1999), pp. 1216–1227.

[25] J. HILGEVOORD AND J. B. M. UFFINK, *The mathematical expression of the uncertainty principle*, in Microphysical Reality and Quantum Description, Kluwer Academic Publishers, Norwell, MA, 1988, pp. 91–114.

[26] B. HUTTNER, N. IMOTO, N. GISIN, AND T. MOR, *Quantum cryptography with coherent states*, Phys. Rev. A, 51 (1995), pp. 1863–1869.

[27] R. IMPAGLIAZZO, L. A. LEVIN, AND M. LUBY, *Pseudorandom generation from one-way functions*, in Proceedings of the 21st Annual ACM Symposium on Theory of Computing (STOC), 1989, pp. 12–24.

[28] F. KITTANEH, *Norm inequalities for certain operator sums*, J. Funct. Anal., 143 (1997), pp. 337–348.

[29] K. KRAUS, *Complementary observables and uncertainty relations*, Phys. Rev. D, 35 (1987), pp. 3070–3075.

[30] U. LARSEN, *Superspace geometry: The exact uncertainty relationship between complementary aspects*, J. Phys. A, 23 (1990), pp. 1041–1061.

[31] H.-K. LO AND H. F. CHAU, *Is quantum bit commitment really possible?*, Phys. Rev. Lett., 78 (1997), pp. 3410–3413.

[32] H. MAASSEN AND J. B. M. UFFINK, *Generalized entropic uncertainty relations*, Phys. Rev. Lett., 60 (1988), pp. 1103–1106.

[33] U. M. MAURER, *Perfect cryptographic security from partially independent channels*, in Proceedings of the 23rd Annual ACM Symposium on Theory of Computing (STOC), 1991, pp. 561–572.

[34] D. MAYERS, *Unconditionally secure quantum bit commitment is impossible*, Phys. Rev. Lett., 78 (1997), pp. 3414–3417.

[35] T. MORAN, R. SHALTIEL, AND A. TA-SHMA, *Non-interactive timestamping in the bounded storage model*, in Advances in Cryptology—CRYPTO '04, Lecture Notes in Comput. Sci. 3152, Springer, Berlin, 2004, pp. 460–476.

[36] R. RENNER, *Security of Quantum Key Distribution*, Ph.D. thesis, ETH Zürich, Zürich, Switzerland, 2005; available online from http://arxiv.org/abs/quant-ph/0512258.

[37] R. RENNER AND R. KÖNIG, *Universally composable privacy amplification against quantum adversaries*, in Theory of Cryptography Conference (TCC), Lecture Notes in Comput. Sci. 3378, Springer, Berlin, 2005, pp. 407–425.

[38] A. RÉNYI, *On measures of entropy and information*, in Proceedings of the 4th Berkeley Symposium on Mathematical Statistics and Probability, Vol. 1, University of California Press, Berkeley, CA, 1961, pp. 547–561.

[39] L. SALVAIL, *Quantum bit commitment from a physical assumption*, in Advances in Cryptology—CRYPTO '98, Lecture Notes in Comput. Sci. 1462, Springer, Berlin, 1998, pp. 338–353.

[40] J. SÁNCHEZ-RUIZ, *Improved bounds in the entropic uncertainty and certainty relations for complementary observables*, Phys. Lett. A, 201 (1995), pp. 125–131.

[41] P. W. SHOR AND J. PRESKILL, *Simple proof of security of the BB84 quantum key distribution protocol*, Phys. Rev. Lett., 85 (2000), pp. 441–444.

[42] M. N. Wegman and J. L. Carter, *New classes and applications of hash functions*, in Proceedings of the 20th Annual IEEE Symposium on Foundations of Computer Science (FOCS), 1979, pp. 175–182.

[43] S. Wehner and J. Wullschleger, *Composable Security in the Bounded-Quantum-Storage Model*, http://arxiv.org/abs/0709.0492 (2007).

[44] S. Wiesner, *Conjugate coding*, SIGACT News, 15 (1983), pp. 78–88.