


On the Power of Two-Party Quantum Cryptography

View metadata, citation and similar papers at core.ac.uk

brought to you by  CORE

provided by CWI's Institutional Repository

¹ Université de Montréal (DIRO), QC, Canada
salvail@iro.umontreal.ca

² Centrum Wiskunde & Informatica (CWI) Amsterdam, The Netherlands
c.schaffner@cwi.nl

³ SUNY Stony Brook (Dept. of Computer Science), NY, USA
mirka@cs.au.dk

Abstract. We study quantum protocols among two distrustful parties. Under the sole assumption of correctness—guaranteeing that honest players obtain their correct outcomes—we show that every protocol implementing a non-trivial primitive necessarily leaks information to a dishonest player. This extends known impossibility results to all non-trivial primitives. We provide a framework for quantifying this leakage and argue that leakage is a good measure for the privacy provided to the players by a given protocol. Our framework also covers the case where the two players are helped by a trusted third party. We show that despite the help of a trusted third party, the players cannot amplify the cryptographic power of any primitive. All our results hold even against quantum honest-but-curious adversaries who honestly follow the protocol but purify their actions and apply a different measurement at the end of the protocol. As concrete examples, we establish lower bounds on the leakage of standard universal two-party primitives such as oblivious transfer.

Keywords: two-party primitives, quantum protocols, quantum information theory, oblivious transfer.

1 Introduction

Quantum communication allows to implement tasks which are classically impossible. The most prominent example is quantum key distribution [4] where two honest players establish a secure key against an eavesdropper. In the two-party setting however, quantum and classical cryptography often show similar limits. Oblivious transfer [22], bit commitment [24,23], and even fair coin tossing [18] are impossible to realize securely both classically and quantumly. On the other

* Supported by QUSEP (funded by the Danish Natural Science Research Council), Canada's NSERC, and the QuantumWorks network.

** Supported by EU fifth framework project QAP IST 015848 and the NWO VICI project 2004-2009.

hand, quantum cryptography allows for some weaker primitives impossible in the classical world. For example, quantum coin-flipping protocols with maximum bias of $\frac{1}{\sqrt{2}} - \frac{1}{2}$ exist¹ against any adversary [8] while remaining impossible based solely on classical communication. A few other weak primitives are known to be possible with quantum communication. For example, the generation of an additive secret-sharing for the product xy of two bits, where Alice holds bit x and Bob bit y , has been introduced by Popescu and Rohrlich as machines modeling non-signaling non-locality (also called NL-boxes) [29]. If Alice and Bob share an EPR pair, they can simulate an NL-box with symmetric error probability $\sin^2 \frac{\pi}{8}$ [29,3]. Equivalently, Alice and Bob can implement *1-out-of-2 oblivious transfer* (1-2-OT) privately provided the receiver Bob gets the bit of his choice only with probability of error $\sin^2 \frac{\pi}{8}$ [1]. It is easy to verify that even with such imperfection these two primitives are impossible to realize in the classical world. This discussion naturally leads to the following question:

- Which two-party cryptographic primitives are possible to achieve using quantum communication?

Most standard classical two-party primitives have been shown impossible to implement securely against weak quantum adversaries reminiscent to the classical honest-but-curious (HBC) behavior [22]. The idea behind these impossibility proofs is to consider parties that *purify* their actions throughout the protocol execution. This behavior is indistinguishable from the one specified by the protocol but guarantees that the joint quantum state held by Alice and Bob at any point during the protocol remains pure. The possibility for players to behave that way in any two-party protocol has important consequences. For instance, the impossibility of quantum bit commitment follows from this fact [24,23]: After the commit phase, Alice and Bob share the pure state $|\psi^x\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$ corresponding to the commitment of bit x . Since a proper commitment scheme provides no information about x to the receiver Bob, it follows that $\text{tr}_A |\psi^0\rangle\langle\psi^0| = \text{tr}_A |\psi^1\rangle\langle\psi^1|$. In this case, the Schmidt decomposition guarantees that there exists a unitary $U_{0,1}$ acting only on Alice's side such that $|\psi^1\rangle = (U_{0,1} \otimes \mathbb{I}_B)|\psi^0\rangle$. In other words, if the commitment is concealing then Alice can open the bit of her choice by applying a suitable unitary transform only to her part. A similar argument allows to conclude that 1-2-OT is impossible [22]: Suppose Alice is sending the pair of bits (b_0, b_1) to Bob through 1-2-OT. Since Alice does not learn Bob's selection bit, it follows that Bob can get bit b_0 before undoing the reception of b_0 and transforming it into the reception of b_1 using a local unitary transform similar to $U_{0,1}$ for bit commitment. For both these primitives, privacy for one player implies that local actions by the other player can transform the honest execution with one input into the honest execution with another input.

In this paper, we investigate the cryptographic power of two-party quantum protocols against players that purify their actions. This *quantum honest-but-curious* (QHBC) behavior is the natural quantum version of classical HBC

¹ In fact, protocols with better bias are known for weak quantum coin flipping [25,26,27].

behavior. We consider the setting where Alice obtains random variable X and Bob random variable Y according to the joint probability distribution $P_{X,Y}$. Any $P_{X,Y}$ models a two-party cryptographic primitive where neither Alice nor Bob provide input. For the purpose of this paper, this model is general enough since any two-party primitive with inputs can be randomized (Alice and Bob pick their input at random) so that its behavior can be described by a suitable joint probability distribution $P_{X,Y}$. If the randomized version $P_{X,Y}$ is shown to be impossible to implement securely by any quantum protocol then also the original primitive with inputs is impossible.

Any quantum protocol implementing $P_{X,Y}$ must produce, when both parties purify their actions, a joint pure state $|\psi\rangle \in \mathcal{H}_{AA'} \otimes \mathcal{H}_{BB'}$ that, when subsystems of A and B are measured in the computational basis, leads to outcomes X and Y according to the distribution $P_{X,Y}$. Notice that the registers A' and B' only provide the players with extra working space and, as such, do not contribute to the output of the functionality (so parties are free to measure them the way they want). In this paper, we adopt a somewhat strict point of view and define a quantum protocol π for $P_{X,Y}$ to be *correct* if and only if the correct outcomes X, Y are obtained *and* the registers A' and B' do not provide any additional information about Y and X respectively since otherwise π would be implementing a different primitive $P_{XX',YY'}$ rather than $P_{X,Y}$.

The state $|\psi\rangle$ produced by any correct protocol for $P_{X,Y}$ is called a *quantum embedding* of $P_{X,Y}$. An embedding is called *regular* if the registers A' and B' are empty. Any embedding $|\psi\rangle \in \mathcal{H}_{AA'} \otimes \mathcal{H}_{BB'}$ can be produced in the QHBC model by the trivial protocol asking Alice to generate $|\psi\rangle$ before sending the quantum state in $\mathcal{H}_{BB'}$ to Bob. Therefore, it is sufficient to investigate the cryptographic power of embeddings in order to understand the power of two-party quantum cryptography in the QHBC model.

Notice that if X and Y were provided privately to Alice and Bob—through a trusted third party for instance—then the expected amount of information one party gets about the other party’s output is minimal and can be quantified by the Shannon mutual information $I(X; Y)$ between X and Y . Assume that $|\psi\rangle \in \mathcal{H}_{AA'} \otimes \mathcal{H}_{BB'}$ is the embedding of $P_{X,Y}$ produced by a correct quantum protocol. We define the leakage of $|\psi\rangle$ as

$$\Delta_\psi := \max \{ S(X; BB') - I(X; Y), S(Y; AA') - I(Y; X) \}, \quad (1)$$

where $S(X; BB')$ (resp. $S(Y; AA')$) is the information the quantum registers BB' (resp. AA') provide about the output X (resp. Y). That is, the leakage is the maximum amount of extra information about the other party’s output given the quantum state held by one party. It turns out that $S(X; BB') = S(Y; AA')$ holds for all embeddings, exhibiting a symmetry similar to its classical counterpart $I(X; Y) = I(Y; X)$ and therefore, the two quantities we are taking the maximum of (in the definition of leakage above) coincide.

CONTRIBUTIONS. Our first contribution establishes that the notion of leakage is well behaved. We show that the leakage of any embedding for $P_{X,Y}$ is lower bounded by the leakage of some regular embedding of the same primitive. Thus,

in order to lower bound the leakage of any correct implementation of a given primitive, it suffices to minimize the leakage over all its regular embeddings. We also show that the only non-leaking embeddings are the ones for trivial primitives, where a primitive $P_{X,Y}$ is said to be (*cryptographically*) *trivial* if it can be generated by a classical protocol against HBC adversaries². It follows that any quantum protocol implementing a non-trivial primitive $P_{X,Y}$ must leak information under the sole assumption that it produces (X,Y) with the right joint distribution. This extends known impossibility results for two-party primitives to all non-trivial primitives.

Embeddings of primitives arise from protocols where Alice and Bob have full control over the environment. Having in mind that any embedding of a non-trivial primitive leaks information, it is natural to investigate what tasks can be implemented without leakage with the help of a trusted third party. The notion of leakage can easily be adapted to this scenario. We show that no cryptographic two-party primitive can be implemented without leakage with just one call to the ideal functionality of a weaker primitive³. This new impossibility result does not follow from the ones known since they all assume that the state shared between Alice and Bob is pure.

We then turn our attention to the leakage of correct protocols for a few concrete universal primitives. From the results described above, the leakage of any correct implementation of a primitive can be determined by finding the (regular) embedding that minimizes the leakage. In general, this is not an easy task since it requires to find the eigenvalues of the reduced density matrix $\rho_A = \text{tr}_B |\psi\rangle\langle\psi|$ (or equivalently $\rho_B = \text{tr}_A |\psi\rangle\langle\psi|$). As far as we know, no known results allow us to obtain a non-trivial lower bound on the leakage (which is the difference between the mutual information and accessible information) of non-trivial primitives. One reason being that in our setting we need to lower bound this difference with respect to a measurement in one particular basis. However, when $P_{X,Y}$ is such that the bit-length of either X or Y is short, the leakage can be computed precisely. We show that any correct implementation of 1-2-OT necessarily leaks $\frac{1}{2}$ bit. Since NL-boxes and 1-2-OT are locally equivalent, the same minimal leakage applies to NL-boxes [38]. This is a stronger impossibility result than the one by Lo [22] since he assumes perfect/statistical privacy against one party while our approach only assumes correctness (while both approaches apply even against QHBC adversaries). We finally show that for Rabin-OT and 1-2-OT of r -bit strings (i.e. ROT^r and $1\text{-}2\text{-OT}^r$ respectively), the leakage approaches 1 exponentially in r . In other words, correct implementations of these two primitives trivialize as r increases since the sender gets almost all information about Bob's

² We are aware of the fact that our definition of triviality encompasses cryptographically interesting primitives like coin-tossing and generalizations thereof for which highly non-trivial protocols exist [27,8]. However, the important fact (for the purpose of this paper) is that all these primitives can be implemented by *trivial* classical protocols against HBC adversaries.

³ The weakness of a primitive will be formally defined in terms of entropic monotones for classical two-party computation introduced by Wolf and Wullschlegel [36], see Section 4.2.

reception of the string (in case of ROT^r) and Bob's choice bit (in case of $1\text{-}2\text{-OT}^r$). These are the first quantitative impossibility results for these primitives and certainly the first time the hardness of implementing different flavors of string OTs is shown to increase as the strings to be transmitted get longer.

Finally, we note that our lower bounds on the leakage of the randomized primitives also lower-bound the minimum leakage for the standard versions of these primitives⁴ where the players choose their inputs uniformly at random. While we focus on the typical case where the primitives are run with uniform inputs, the same reasoning can be applied to primitives with arbitrary distributions of inputs.

RELATED WORK. Our framework allows to quantify the minimum amount of leakage whereas standard impossibility proofs as the ones of [23,24,22,2,7] do not in general provide such quantification since they usually assume privacy for one player in order to show that the protocol must be totally insecure for the other player⁵. By contrast, we derive lower bounds for the leakage of any correct implementation. At first glance, our approach seems contradictory with standard impossibility proofs since embeddings leak the same amount towards both parties. To resolve this apparent paradox it suffices to observe that in previous approaches only the adversary purified its actions whereas in our case both parties do. If a honest player does not purify his actions then some leakage may be lost by the act of irreversibly and unnecessarily measuring some of his quantum registers.

Our results complement the ones obtained by Colbeck in [10] for the setting where Alice and Bob have inputs and obtain identical outcomes (called single-function computations). [10] shows that in any correct implementation of primitives of a certain form, an honest-but-curious player can access more information about the other party's input than it is available through the ideal functionality. Unlike [10], we deal in our work with the case where Alice and Bob do not have inputs but might receive different outputs according to a joint probability distributions. We show that only trivial distributions can be implemented securely in the QHBC model. Furthermore, we introduce a quantitative measure of protocol-insecurity that lets us answer which embedding allow the least effective cheating.

Another notion of privacy in quantum protocols, generalizing its classical counterpart from [9,21], is proposed by Klauck in [19]. Therein, two-party quantum protocols with inputs for computing a function $f : \mathcal{X} \times \mathcal{Y} \rightarrow \mathcal{Z}$, where \mathcal{X} and \mathcal{Y} denote Alice's and Bob's respective input spaces, and privacy against QHBC

⁴ The definition of leakage of an embedding can be generalized to protocols with inputs, where it is defined as $\max\{\sup_{V_B} S(X; V_B) - I(X; Y), \sup_{V_A} S(V_A; Y) - I(X; Y)\}$, where X and Y involve both inputs and outputs of Alice and Bob, respectively. The supremum is taken over all possible (quantum) views V_A and V_B of Alice and Bob obtained by their (QHBC-consistent) actions (and containing their inputs).

⁵ Trade-offs between the security for one and the security for the other player have been considered before, but either the relaxation of security has to be very small [22] or the trade-offs are restricted to particular primitives such as commitments [34,6].

adversaries are considered. Privacy of a protocol is measured in terms of *privacy loss*, defined for each round of the protocol and fixed distribution of inputs $P_{X',Y'}$ by $S(B; X|Y) = H(X|Y) - S(X|B, Y)$, where B denotes Bob's private working register, and $X := (X', f(X', Y'))$, $Y := (Y', f(X', Y'))$ represent the complete views of Alice and Bob, respectively. Privacy loss of the entire protocol is then defined as the supremum over all joint input distributions, protocol rounds, and states of working registers. In our framework, privacy loss corresponds to $S(X; YB) - I(X; Y)$ from Alice point's of view and $S(Y; XA) - I(X; Y)$ from Bob's point of view. Privacy loss is therefore very similar to our definition of leakage except that it requires the players to get their respective honest outputs. As a consequence, the protocol implementing $P_{X,Y}$ by asking one party to prepare a regular embedding of $P_{X,Y}$ before sending her register to the other party would have no privacy loss. Moreover, the scenario analyzed in [19] is restricted to primitives which provide the same output $f(X, Y)$ to both players. Another difference is that since privacy loss is computed over all rounds of a protocol, a party is allowed to abort which is not considered QHBC in our setting. In conclusion, the model of [19] is different from ours even though the measures of privacy loss and leakage are similar. [19] provides interesting results concerning trade-offs between privacy loss and communication complexity of quantum protocols, building upon similar results of [9,21] in the classical scenario. It would be interesting to know whether a similar operational meaning can also be assigned to the new measure of privacy, introduced in this paper.

A recent result by Künzler et al. [20] shows that two-party functions that are securely computable against active quantum adversaries form a strict subset of the set of functions which are securely computable in the classical HBC model. This complements our result that the sets of securely computable functions in both HBC and QHBC models are the same.

ROADMAP. In Section 2, we introduce the cryptographic and information-theoretic notions and concepts used throughout the paper. We define, motivate, and analyze the generality of modeling two-party quantum protocols by embeddings in Section 3 and define triviality of primitives and embeddings. In Section 4, we define the notion of leakage of embeddings, show basic properties and argue that it is a reasonable measure of privacy. In Section 5, we explicitly lower bound the leakage of some universal two-party primitives. Finally, in Section 6 we discuss possible directions for future research and open questions.

2 Preliminaries

QUANTUM INFORMATION THEORY. Let $|\psi\rangle_{AB} \in \mathcal{H}_{AB}$ be an arbitrary pure state of the joint systems A and B . The states of these subsystems are $\rho_A = \text{tr}_B |\psi\rangle\langle\psi|$ and $\rho_B = \text{tr}_A |\psi\rangle\langle\psi|$, respectively. We denote by $S(A) := S(\rho_A)$ and $S(B) := S(\rho_B)$ the von Neumann entropy (defined as the Shannon entropy of the eigenvalues of the density matrix) of subsystem A and B respectively. Since the joint system is in a pure state, it follows from the Schmidt decomposition that $S(A) = S(B)$ (see e.g. [28]). Analogously to their classical counterparts, we

can define quantum conditional entropy $S(A|B) := S(AB) - S(B)$, and quantum mutual information $S(A; B) := S(A) + S(B) - S(AB) = S(A) - S(A|B)$. Even though in general, $S(A|B)$ can be negative, $S(A|B) \geq 0$ is always true if A is a classical register. Let $R = \{(P_X(x), \rho_R^x)\}_{x \in \mathcal{X}}$ be an ensemble of states ρ_R^x with prior probability $P_X(x)$. The average quantum state is $\rho_R = \sum_{x \in \mathcal{X}} P_X(x) \rho_R^x$. The famous result by Holevo upper-bounds the amount of classical information about X that can be obtained by measuring ρ_R :

Theorem 2.1 (Holevo bound [14,32]). *Let Y be the random variable describing the outcome of some measurement applied to ρ_R for $R = \{P_X(x), \rho_R^x\}_{x \in \mathcal{X}}$. Then, $I(X; Y) \leq S(\rho_R) - \sum_x P_X(x) S(\rho_R^x)$, where equality can be achieved if and only if $\{\rho_R^x\}_{x \in \mathcal{X}}$ are simultaneously diagonalizable.*

Note that if all states in the ensemble are pure and all different then in order to achieve equality in the theorem above, they have to form an orthonormal basis of the space they span. In this case, the variable Y achieving equality is the measurement outcome in this orthonormal basis.

DEPENDENT PART. The following definition introduces a random variable describing the correlation between two random variables X and Y , obtained by collapsing all values x_1 and x_2 for which Y has the same conditional distribution, to a single value.

Definition 2.2 (Dependent part [36]). *For two random variables X, Y , let $f_X(x) := P_{Y|X=x}$. Then the dependent part of X with respect to Y is defined as $X \searrow Y := f_X(X)$.*

The dependent part $X \searrow Y$ is the minimum random variable among the random variables computable from X for which $X \leftrightarrow X \searrow Y \leftrightarrow Y$ forms a Markov chain [36]. In other words, for any random variable $K = f(X)$ such that $X \leftrightarrow K \leftrightarrow Y$ is a Markov chain, there exists a function g such that $g(K) = X \searrow Y$. Immediately from the definition we get several other properties of $X \searrow Y$ [36]: $H(Y|X \searrow Y) = H(Y|X)$, $I(X; Y) = I(X \searrow Y; Y)$, and $X \searrow Y = X \searrow (Y \searrow X)$. The second and the third formula yield $I(X; Y) = I(X \searrow Y; Y \searrow X)$.

The notion of dependent part has been further investigated in [13,15,37]. Wullschleger and Wolf have shown that quantities $H(X \searrow Y|Y)$ and $H(Y \searrow X|X)$ are monotones for two-party computation [37]. That is, none of these values can increase during classical two-party protocols. In particular, if Alice and Bob start a protocol from scratch then classical two-party protocols can only produce (X, Y) such that: $H(X \searrow Y|Y) = H(Y \searrow X|X) = 0$, since $H(X \searrow Y|Y) > 0$ if and only if $H(Y \searrow X|X) > 0$ [37]. Conversely, any primitive satisfying $H(X \searrow Y|Y) = H(Y \searrow X|X) = 0$ can be implemented securely in the honest-but-curious (HBC) model. We call such primitives *trivial*⁶.

⁶ See Footnote 2 for a caveat about this terminology.

PURIFICATION. All security questions we ask are with respect to (*quantum*) *honest-but-curious* adversaries. In the classical honest-but-curious adversary model (HBC), the parties follow the instructions of a protocol but store all information available to them. Quantum honest-but-curious adversaries (QHBC), on the other hand, are allowed to behave in an arbitrary way that cannot be distinguished from their honest behavior by the other player.

Almost all impossibility results in quantum cryptography rely upon a quantum honest-but-curious behavior of the adversary. This behavior consists in *purifying* all actions of the honest players. Purifying means that instead of invoking classical randomness from a random tape, for instance, the adversary relies upon quantum registers holding all random bits needed. The operations to be executed from the random outcome are then performed quantumly without fixing the random outcomes. For example, suppose a protocol instructs a party to pick with probability p state $|\phi^0\rangle_C$ and with probability $1 - p$ state $|\phi^1\rangle_C$ before sending it to the other party through the quantum channel C . The purified version of this instruction looks as follows: Prepare a quantum register in state $\sqrt{p}|0\rangle_R + \sqrt{1-p}|1\rangle_R$ holding the random process. Add a new register initially in state $|0\rangle_C$ before applying the unitary transform $U : |r\rangle_R|0\rangle_C \mapsto |r\rangle_R|\phi^r\rangle_C$ for $r \in \{0, 1\}$, send register C through the quantum channel and keep register R .

From the receiver's point of view, the purified behavior is indistinguishable from the one relying upon a classical source of randomness because in both cases, the state of register C is $\rho = p|\phi^0\rangle\langle\phi^0| + (1-p)|\phi^1\rangle\langle\phi^1|$. All operations invoking classical randomness can be purified similarly [23,24,22,17]. The result is that measurements are postponed as much as possible and only extract information required to run the protocol in the sense that only when both players need to know a random outcome, the corresponding quantum register holding the random coin will be measured. If both players purify their actions then the joint state at any point during the execution will remain pure, until the very last step of the protocol when the outcomes are measured.

SECURE TWO-PARTY COMPUTATION. In Section 5, we investigate the leakage of several universal cryptographic two-party primitives. By universality we mean that any two-party secure function evaluation can be reduced to them. We investigate the completely randomized versions where players do not have inputs but receive randomized outputs instead. Throughout this paper, the term *primitive* usually refers to the joint probability distribution defining its randomized version. Any protocol implementing the standard version of a primitive (with inputs) can also be used to implement a randomized version of the same primitive, with the "inputs" chosen according to an arbitrary fixed probability distribution.

3 Two-Party Protocols and Their Embeddings

3.1 Correctness

In this work, we consider *cryptographic primitives* providing X to honest player Alice and Y to honest player Bob according to a joint probability distribution

$P_{X,Y}$. The goal of this section is to define when a protocol π *correctly implements* the primitive $P_{X,Y}$. The first natural requirement is that once the actions of π are purified by both players, measurements of registers A and B in the computational basis⁷ provide joint outcome $(X, Y) = (x, y)$ with probability $P_{X,Y}(x, y)$.

Protocol π can use extra registers A' on Alice's and B' on Bob's side providing them with (quantum) working space. The purification of all actions of π therefore generates a pure state $|\psi\rangle \in \mathcal{H}_{AB} \otimes \mathcal{H}_{A'B'}$. A second requirement for the correctness of the protocol π is that these extra registers are only used as working space, i.e. the final state $|\psi\rangle_{ABA'B'}$ is such that the content of Alice's working register A' does not give her any further information about Bob's output Y than what she can infer from her honest output X and vice versa for B' . Formally, we require that $S(XA'; Y) = I(X; Y)$ and $S(X; YB') = I(X; Y)$ or equivalently, that $A' \leftrightarrow X \leftrightarrow Y$ and $X \leftrightarrow Y \leftrightarrow B'$ form Markov chains⁸.

Definition 3.1. *A protocol π for $P_{X,Y}$ is correct if measuring registers A and B of its final state in the computational basis yields outcomes X and Y with distribution $P_{X,Y}$ and the final state satisfies $S(X; YB') = S(XA'; Y) = I(X; Y)$ where A' and B' denote the extra working registers of Alice and Bob. The state $|\psi\rangle \in \mathcal{H}_{AB} \otimes \mathcal{H}_{A'B'}$ is called an embedding of $P_{X,Y}$ if it can be produced by the purification of a correct protocol for $P_{X,Y}$.*

We would like to point out that our definition of correctness is stronger than the usual classical notion which only requires the correct distribution of the output of the honest players. For example, the trivial classical protocol for the primitive $P_{X,Y}$ in which Alice samples both player's outputs XY , sends Y to Bob, but keeps a copy of Y for herself, is *not correct* according to our definition, because it implements a fundamentally different primitive, namely $P_{XY,Y}$.

3.2 Regular Embeddings

We call an embedding $|\psi\rangle_{ABA'B'}$ *regular* if the working registers A', B' are empty. Formally, let $\Theta_{n,m} := \{\theta : \{0, 1\}^n \times \{0, 1\}^m \rightarrow [0 \dots 2\pi]\}$ be the set of functions mapping bit-strings of length $m + n$ to real numbers between 0 and 2π .

Definition 3.2. *For a joint probability distribution $P_{X,Y}$ where $X \in \{0, 1\}^n$ and $Y \in \{0, 1\}^m$, we define the set*

$$\mathcal{E}(P_{X,Y}) := \left\{ |\psi\rangle \in \mathcal{H}_{AB} : |\psi\rangle = \sum_{x \in \{0,1\}^n, y \in \{0,1\}^m} e^{i\theta(x,y)} \sqrt{P_{X,Y}(x,y)} |x, y\rangle_{AB}, \theta \in \Theta_{n,m} \right\},$$

⁷ It is clear that every quantum protocol for which the final measurement (providing (x, y) with distribution $P_{X,Y}$ to the players) is not in the computational basis can be transformed into a protocol of the described form by two additional local unitary transformations.

⁸ Markov chains with quantum ends have been defined in [11] and used in subsequent works such as [12]. It is straightforward to verify that the entropic condition $S(XA'; Y) = I(X; Y)$ is equivalent to $A' \leftrightarrow X \leftrightarrow Y$ being a Markov chain and similarly for the other condition.

and call any state $|\psi\rangle \in \mathcal{E}(P_{X,Y})$ a regular embedding of the joint probability distribution $P_{X,Y}$.

Clearly, any $|\psi\rangle \in \mathcal{E}(P_{X,Y})$ produces (X,Y) with distribution $P_{X,Y}$ since the probability that Alice measures x and Bob measures y in the computational basis is $|\langle\psi|x,y\rangle|^2 = P_{X,Y}(x,y)$. In order to specify a particular regular embedding one only needs to give the description of the *phase function* $\theta(x,y)$. We denote by $|\psi_\theta\rangle \in \mathcal{E}(P_{X,Y})$ the quantum embedding of $P_{X,Y}$ with phase function θ . The constant function $\theta(x,y) := 0$ for all $x \in \{0,1\}^n, y \in \{0,1\}^m$ corresponds to what we call *canonical embedding* $|\psi_0\rangle := \sum_{x,y} \sqrt{P_{X,Y}(x,y)}|x,y\rangle_{AB}$.

In Lemma 4.3 below we show that every primitive $P_{X,Y}$ has a regular embedding which is in some sense the most secure among all embeddings of $P_{X,Y}$.

3.3 Trivial Classical Primitives and Trivial Embeddings

In this section, we define *triviality* of classical primitives and (bipartite) embeddings. We show that for any non-trivial classical primitive, its canonical quantum embedding is also non-trivial. Intuitively, a primitive $P_{X,Y}$ is *trivial* if X and Y can be generated by Alice and Bob from scratch in the classical honest-but-curious (HBC) model⁹. Formally, we define triviality via an entropic quantity based on the notion of *dependent part* (see Section 2).

Definition 3.3. *A primitive $P_{X,Y}$ is called trivial if it satisfies $H(X \searrow Y|Y) = 0$, or equivalently, $H(Y \searrow X|X) = 0$. Otherwise, the primitive is called non-trivial.*

Definition 3.4. *A regular embedding $|\psi\rangle_{AB} \in \mathcal{E}(P_{X,Y})$ is called trivial if either $S(X \searrow Y|B) = 0$ or $S(Y \searrow X|A) = 0$. Otherwise, we say that $|\psi\rangle_{AB}$ is non-trivial.*

Notice that unlike in the classical case, $S(X \searrow Y|B) = 0 \Leftrightarrow S(Y \searrow X|A) = 0$ does not hold in general. As an example, consider a shared quantum state where the computational basis corresponds to the Schmidt basis for only one of its subsystems, say for A . Let $|\psi\rangle = \alpha|0\rangle_A|\xi_0\rangle_B + \beta|1\rangle_A|\xi_1\rangle_B$ be such that both subsystems are two-dimensional, $\{|\xi_0\rangle, |\xi_1\rangle\} \neq \{|0\rangle, |1\rangle\}$, $\langle\xi_0|\xi_1\rangle = 0$, and $|\langle\xi_0|0\rangle| \neq |\langle\xi_1|0\rangle|$. We then have $S(X|B) = 0$ and $S(Y|A) > 0$ while $X = X \searrow Y$ and $Y = Y \searrow X$.

To illustrate this definition of triviality, we argue in the following that if a primitive $P_{X,Y}$ has a trivial regular embedding, there exists a classical protocol which generates X,Y securely in the HBC model. Let $|\psi\rangle \in \mathcal{E}(P_{X,Y})$ be trivial and assume without loss of generality that $S(Y \searrow X|A) = 0$. Intuitively, this means that Alice can learn everything possible about Bob’s outcome Y (Y could include some private coin-flips on Bob’s side, but that is “filtered out” by the dependent part). More precisely, Alice holding register A can measure her part of

⁹ See Footnote 2 for a caveat about this terminology.

the shared state to completely learn a realization of $Y \setminus X$, specifying $P_{X|Y=y}$. She then chooses X according to the distribution $P_{X|Y=y}$. An equivalent way of trivially generating (X, Y) classically is the following classical protocol:

1. Alice samples $P_{X|Y=y'}$ from distribution $P_{Y \setminus X}$ and announces its outcome to Bob. She samples x from the distribution $P_{X|Y=y'}$.
2. Bob picks y with probability $P_{Y|Y \setminus X = P_{X|Y=y'}}$.

Of course, the same reasoning applies in case $S(X \setminus Y|B) = 0$ with the roles of Alice and Bob reversed.

In fact, the following lemma (whose proof can be found in the full version [33]) shows that any non-trivial primitive $P_{X,Y}$ has a non-trivial embedding, i.e. there exists a quantum protocol correctly implementing $P_{X,Y}$ while leaking less information to QHBC adversaries than any classical protocol for $P_{X,Y}$ in the HBC model.

Lemma 3.5. *If $P_{X,Y}$ is a non-trivial primitive then the canonical embedding $|\psi_0\rangle \in \mathcal{E}(P_{X,Y})$ is also non-trivial.*

4 The Leakage of Quantum Embeddings

We formally define the leakage of embeddings and establish properties of the leakage. The proofs of all statements in this section can be found in the full version [33].

4.1 Definition and Basic Properties of Leakage

A perfect implementation of $P_{X,Y}$ simply provides X to Alice and Y to Bob and does nothing else. The expected amount of information that one random variable gives about the other is $I(X; Y) = H(X) - H(X|Y) = H(Y) - H(Y|X) = I(Y; X)$. Intuitively, we define the *leakage of a quantum embedding* $|\psi\rangle_{ABA'B'}$ of $P_{X,Y}$ as the larger of the two following quantities: the extra amount of information Bob's quantum registers BB' provide about X and the extra amount Alice's quantum state in AA' provides about Y respectively in comparison to "the minimum amount" $I(X; Y)$.¹⁰

Definition 4.1. *Let $|\psi\rangle \in \mathcal{H}_{ABA'B'}$ be an embedding of $P_{X,Y}$. We define the leakage $|\psi\rangle$ as*

$$\Delta_\psi(P_{X,Y}) := \max\{S(X; BB') - I(X; Y), S(AA'; Y) - I(X; Y)\}.$$

Furthermore, we say that $|\psi\rangle$ is δ -leaking if $\Delta_\psi(P_{X,Y}) \geq \delta$.

¹⁰ There are other natural candidates for the notion of leakage such as the difference in difficulty between guessing Alice's output X by measuring Bob's final quantum state B and based on the output of the ideal functionality Y . While such definitions do make sense, they turn out not to be as easy to work with and it is an open question whether the natural properties described later in this section can be established for these notions of leakage as well.

It is easy to see that the leakage is non-negative since $S(X; BB') \geq S(X; \tilde{B})$ for \tilde{B} the result of a quantum operation applied to BB' . Such an operation could be the trace over the extra working register B' and a measurement in the computational basis of each qubit of the part encoding Y , yielding $S(X; \tilde{B}) = I(X; Y)$.

We want to argue that our notion of leakage is a good measure for the privacy of the player's outputs. In the same spirit, we will argue that the minimum achievable leakage for a primitive is related to the "hardness" of implementing it. We start off by proving several basic properties about leakage.

For a general state in $\mathcal{H}_{ABA'B'}$ the quantities $S(X; BB') - I(X; Y)$ and $S(AA'; Y) - I(X; Y)$ are not necessarily equal. Note though that they coincide for regular embeddings $|\psi\rangle \in \mathcal{E}(P_{X,Y})$ produced by a correct protocol (where the work spaces A' and B' are empty): Notice that $S(X; B) = S(X) + S(B) - S(X, B) = H(X) + S(B) - H(X) = S(B)$ and because $|\psi\rangle$ is pure, $S(A) = S(B)$. Therefore, $S(X; B) = S(A; Y)$ and the two quantities coincide. The following lemma states that this actually happens for *all* embeddings and hence, the definition of leakage is symmetric with respect to both players.

Lemma 4.2 (Symmetry). *Let $|\psi\rangle \in \mathcal{H}_{ABA'B'}$ be an embedding of $P_{X,Y}$. Then,*

$$\Delta_\psi(P_{X,Y}) = S(X; BB') - I(X; Y) = S(AA'; Y) - I(X; Y).$$

The next lemma shows that the leakage of an embedding of a given primitive is lower-bounded by the leakage of some regular embedding of the same primitive, which simplifies the calculation of lower bounds for the leakage of embeddings.

Lemma 4.3. *For every embedding $|\psi\rangle$ of a primitive $P_{X,Y}$, there is a regular embedding $|\psi'\rangle$ of $P_{X,Y}$ such that $\Delta_\psi(P_{X,Y}) \geq \Delta_{\psi'}(P_{X,Y})$.*

So far, we have defined the leakage of an embedding of a primitive. The natural definition of the leakage of a primitive is the following.

Definition 4.4. *We define the leakage of a primitive $P_{X,Y}$ as the minimal leakage among all protocols correctly implementing $P_{X,Y}$. Formally,*

$$\Delta_{P_{X,Y}} := \min_{|\psi\rangle} \Delta_\psi(P_{X,Y}),$$

where the minimization is over all embeddings $|\psi\rangle$ of $P_{X,Y}$.

Notice that the minimum in the previous definition is well-defined, because by Lemma 4.3, it is sufficient to minimize over regular embeddings $|\psi\rangle \in \mathcal{E}(P_{X,Y})$. Furthermore, the function $\Delta_\psi(P_{X,Y})$ is continuous on the compact (i.e. closed and bounded) set $[0, 2\pi]^{|\mathcal{X} \times \mathcal{Y}|}$ of complex phases corresponding to elements $|x, y\rangle_{AB}$ in the formula for $|\psi\rangle_{AB} \in \mathcal{E}(P_{X,Y})$ and therefore it achieves its minimum.

The following theorem shows that the leakage of any embedding of a primitive $P_{X,Y}$ is lower-bounded by the minimal leakage achievable for primitive $P_{X \setminus Y, Y \setminus X}$ (which due to Lemma 4.3 is achieved by a regular embedding).

Theorem 4.5. *For any primitive $P_{X,Y}$, $\Delta_{P_{X,Y}} \geq \Delta_{P_{X \setminus Y, Y \setminus X}}$.*

Proof (Sketch). The proof idea is to pre-process the registers storing X and Y in a way allowing Alice and Bob to convert a regular embedding of $P_{X,Y}$ (for which the minimum leakage is achieved) into a regular embedding of $P_{X \setminus Y, Y \setminus X}$ by measuring parts of these registers. It follows that on average, the leakage of the resulting regular embedding of $P_{X \setminus Y, Y \setminus X}$ is at most the leakage of the embedding of $P_{X,Y}$ the players started with. Hence, there must be a regular embedding of $P_{X \setminus Y, Y \setminus X}$ leaking at most as much as the best embedding of $P_{X,Y}$. See [33] for the complete proof. \square

4.2 Leakage as Measure of Privacy and Hardness of Implementation

The main results of this section are consequences of the Holevo bound (Theorem 2.1).

Theorem 4.6. *If a two-party quantum protocol provides the correct outcomes of $P_{X,Y}$ to the players without leaking extra information, then $P_{X,Y}$ must be a trivial primitive.*

Proof. Theorem 4.5 implies that if there is a 0-leaking embedding of $P_{X,Y}$ than there is also a 0-leaking embedding of $P_{X \setminus Y, Y \setminus X}$. Let us therefore assume that $|\psi\rangle$ is a non-leaking embedding of $P_{X,Y}$ such that $X = X \setminus Y$ and $Y = Y \setminus X$. We can write $|\psi\rangle$ in the form $|\psi\rangle = \sum_x \sqrt{P_X(x)}|x\rangle|\varphi_x\rangle$ and get $\rho_B = \sum_x P_X(x)|\varphi_x\rangle\langle\varphi_x|$. For the leakage of $|\psi\rangle$ we have: $\Delta_\psi(P_{X,Y}) = S(X;B) - I(X;Y) = S(\rho_B) - I(X;Y) = 0$. From the Holevo bound (Theorem 2.1) follows that the states $\{|\varphi_x\rangle\}_x$ form an orthonormal basis of their span (since $X = X \setminus Y$, they are all different) and that Y captures the result of a measurement in this basis, which therefore is the computational basis. Since $Y = Y \setminus X$, we get that for each x , there is a single $y_x \in \mathcal{Y}$ such that $|\varphi_x\rangle = |y_x\rangle$. The primitives $P_{X \setminus Y, Y \setminus X}$ and $P_{X,Y}$ are therefore trivial. \square

In other words, the only primitives that two-party quantum protocols can implement correctly (without the help of a trusted third party) and without leakage are the trivial ones! We note that it is not necessary to use the strict notion of correctness from Definition 3.1 in this theorem, but a more complicated proof can be done solely based on the correct distribution of the values. This result can be seen as a quantum extension of the corresponding characterization for the cryptographic power of classical protocols in the HBC model. Whereas classical two-party protocols cannot achieve anything non-trivial, their quantum counterparts necessarily leak information when they implement non-trivial primitives.

The notion of leakage can be extended to protocols involving a trusted third party (see [33]). A special case of such protocols are the ones where the players are allowed one call to a black box for a certain non-trivial primitive. It is natural to ask which primitives can be implemented without leakage in this case. As it turns out, the monotones $H(X \setminus Y|Y)$ and $H(Y \setminus X|X)$, introduced in [36], are also monotones for quantum computation, in the sense that all joint

random variables X', Y' that can be generated by quantum players without leakage using one black-box call to $P_{X,Y}$ satisfy $H(X' \searrow Y'|Y') \leq H(X \searrow Y|Y)$ and $H(Y' \searrow X'|X') \leq H(Y \searrow X|X)$.

Theorem 4.7. *Suppose that primitives $P_{X,Y}$ and $P_{X',Y'}$ satisfy $H(X' \searrow Y'|Y') > H(X \searrow Y|Y)$ or $H(Y' \searrow X'|X') > H(Y \searrow X|X)$. Then any implementation of $P_{X',Y'}$ using just one call to the ideal functionality for $P_{X,Y}$ leaks information.*

4.3 Reducibility of Primitives and Their Leakage

This section is concerned with the following question: Given two primitives $P_{X,Y}$ and $P_{X',Y'}$ such that $P_{X,Y}$ is reducible to $P_{X',Y'}$, what is the relationship between the leakage of $P_{X,Y}$ and the leakage of $P_{X',Y'}$? We use the notion of reducibility in the following sense: We say that a primitive $P_{X,Y}$ is *reducible in the HBC model* to a primitive $P_{X',Y'}$ if $P_{X,Y}$ can be securely implemented in the HBC model from (one call to) a secure implementation of $P_{X',Y'}$. The above question can also be generalized to the case where $P_{X,Y}$ can be computed from $P_{X',Y'}$ only with certain probability. Notice that the answer, even if we assume perfect reducibility, is not captured in our previous result from Lemma 4.3, since an embedding of $P_{X',Y'}$ is not necessarily an embedding of $P_{X,Y}$ (it might violate the correctness condition). However, under certain circumstances, we can show that $\Delta_{P_{X',Y'}} \geq \Delta_{P_{X,Y}}$.

Theorem 4.8. *Assume that primitives $P_{X,Y}$ and $P_{X',Y'} = P_{X'_0 X'_1, Y'_0 Y'_1}$ satisfy the condition:*

$$\sum_{x,y: P_{X'_0, Y'_0} |_{X'_1=x, Y'_1=y} \simeq P_{X,Y}} P_{X'_1, Y'_1}(x, y) \geq 1 - \delta,$$

where the relation \simeq means that the two distributions are equal up to relabeling of the alphabet. Then, $\Delta_{P_{X',Y'}} \geq (1 - \delta)\Delta_{P_{X,Y}}$.

This theorem allows us to derive a lower bound on the leakage of 1-out-of-2 Oblivious Transfer of r -bit strings in Section 5.

5 The Leakage of Universal Cryptographic Primitives

In this section, we exhibit lower bounds on the leakage of some universal two-party primitives. In the following table, ROT^r denotes the r -bit string version of randomized Rabin OT, where Alice receives a random r -bit string and Bob receives the same string or an erasure symbol, each with probability 1/2. Similarly, $1\text{-}2\text{-OT}^r$ denotes the string version of 1-2-OT, where Alice receives two r -bit strings and Bob receives one of them. By $1\text{-}2\text{-OT}_p$ we denote the noisy version of 1-2-OT, where the 1-2-OT functionality is implemented correctly only with probability $1 - p$. Table 1 summarizes the lower bounds on the leakage of these primitives (the derivations can be found in the full version [33]). We note that Wolf and Wullschlegel [38] have shown that a randomized 1-2-OT can be

Table 1. Lower bounds on the leakage for universal two-party primitives

primitive	leaking at least	comments
ROT^1	$(h(\frac{1}{4}) - \frac{1}{2}) \approx 0.311$	same leakage for all regular embeddings
ROT^r	$(1 - O(r2^{-r}))$	same leakage for all regular embeddings
1-2-OT, SAND	$\frac{1}{2}$	minimized by canonical embedding
1-2-OT ^r	$(1 - O(r2^{-r}))$	(suboptimal) lower bound
1-2-OT _p	$\frac{(1/2-p-\sqrt{p(1-p)})^2}{8 \ln 2}$	if $p < \sin^2(\pi/8) \approx 0.15$, (suboptimal) lower bound

transformed by local operations into an additive sharing of an AND (here called SAND). Therefore, our results for 1-2-OT below also apply to SAND.

1-2-OT^r and 1-2-OT_p are primitives where the direct evaluation of the leakage for a general embedding $|\psi_\theta\rangle$ is hard, because the number of possible phases increases exponentially in the number of qubits. Instead of computing $S(A)$ directly, we derive (suboptimal) lower bounds on the leakage.

Based on the examples of ROT^r and 1-2-OT, it is tempting to conjecture that the leakage is always minimized for the canonical embedding, which agrees with the geometric intuition that the minimal pairwise distinguishability of quantum states in a mixture minimizes the von Neumann entropy of the mixture. However, Jozsa and Schlienz have shown that this intuition is sometimes incorrect [16]. In a quantum system of dimension at least three, we can have the following situation: For two sets of pure states $\{|u_i\rangle\}_{i=1}^n$ and $\{|v_i\rangle\}_{i=1}^n$ satisfying $|\langle u_i|u_j\rangle| \leq |\langle v_i|v_j\rangle|$ for all i, j , there exist probabilities p_i such that for $\rho_u := \sum_{i=1}^n p_i |u_i\rangle\langle u_i|$, $\rho_v := \sum_{i=1}^n p_i |v_i\rangle\langle v_i|$, it holds that $S(\rho_u) < S(\rho_v)$. As we can see, although each pair $|u_i\rangle, |u_j\rangle$ is more distinguishable than the corresponding pair $|v_i\rangle, |v_j\rangle$, the overall ρ_u provides us with less uncertainty than ρ_v . It follows that although for the canonical embedding $|\psi_0\rangle = \sum_y |\varphi_y\rangle|y\rangle$ of $P_{X,Y}$ the mutual overlaps $|\langle \varphi_y|\varphi_{y'}\rangle|$ are clearly maximized, it does not necessarily imply that $S(A)$ in this case is minimal over $\mathcal{E}(P_{X,Y})$. It is an interesting open question to find a primitive whose canonical embedding does not minimize the leakage or to prove that no such primitive exists.

For the primitive $P_{X,Y}^{\text{OT}_p}$, our lower bound on the leakage only holds for $p < \sin^2(\pi/8) \approx 0.15$. Notice that in reality, the leakage is strictly positive for any embedding of $P_{X,Y}^{\text{OT}_p}$ with $p < 1/4$, since for $p < 1/4$, $P_{X,Y}^{\text{OT}_p}$ is a non-trivial primitive. On the other hand, $P_{X,Y}^{\text{OT}_{1/4}}$ is a trivial primitive implemented securely by the following protocol in the classical HBC model:

1. Alice chooses randomly between her input bits x_0 and x_1 and sends the chosen value x_a to Bob.
2. Bob chooses his selection bit c uniformly at random and sets $y := x_a$.

Equality $x_c = y$ is satisfied if either $a = c$, which happens with probability $1/2$, or if $a \neq c$ and $x_a = x_{1-a}$, which happens with probability $1/4$. Since the

two events are disjoint, it follows that $x_c = y$ with probability $3/4$ and that the protocol implements $P_{X,Y}^{\text{ot}_{1/4}}$. The implementation is clearly secure against honest-but-curious Alice, since she does not receive any message from Bob. It is also secure against Bob, since he receives only one bit from Alice. By letting Alice randomize the value of the bit she is sending, the players can implement $P_{X,Y}^{\text{ot}_p}$ securely for any value $1/4 < p \leq 1/2$.

6 Conclusion and Open Problems

We have provided a quantitative extension of qualitative impossibility results for two-party quantum cryptography. All non-trivial primitives leak information when implemented by quantum protocols. Notice that demanding a protocol to be non-leaking does in general not imply the privacy of the players' outputs. For instance, consider a protocol implementing 1-2-OT but allowing a curious receiver with probability $\frac{1}{2}$ to learn both bits simultaneously or with probability $\frac{1}{2}$ to learn nothing about them. Such a protocol for 1-2-OT would be non-leaking but nevertheless insecure. Consequently, Theorem 4.6 not only tells us that any quantum protocol implementing a non-trivial primitive must be insecure, but also that a privacy breach will reveal itself as leakage. Our framework allows to quantify the leakage of any two-party quantum protocol correctly implementing a primitive. The impossibility results obtained here are stronger than standard ones since they only rely on the cryptographic correctness of the protocol. Furthermore, we present lower bounds on the leakage of some universal two-party primitives.

A natural open question is to find a way to identify good embeddings for a given primitive. In particular, how far can the leakage of the canonical embedding be from the best one? Such a characterization, even if only applicable to special primitives, would allow to lower bound their leakage and would also help to understand the power of two-party quantum cryptography in a more concise way.

It would also be interesting to find a measure of cryptographic non-triviality for two-party primitives and to see how it relates to the minimum leakage of any implementation by quantum protocols. For instance, is it true that quantum protocols for primitive $P_{X,Y}$ leak more if the minimum (total variation) distance between $P_{X,Y}$ and any trivial primitive increases?

Another question we leave for future research is to define and investigate other notions of leakage, e.g. in the one-shot setting instead of in the asymptotic regime (as outlined in Footnote 10). Results in the one-shot setting have already been established for data compression [30], channel capacities [31], state-merging [35,5] and other (quantum-) information-theoretic tasks.

Furthermore, it would be interesting to find more applications for the concept of leakage, considered also for protocols using an environment as a trusted third party. In this direction, we have shown in Theorem 4.7 that any two-party quantum protocol for a given primitive, using a black box for an "easier" primitive, leaks information. Lower-bounding this leakage is an interesting open question.

We might also ask how many copies of the “easier” primitive are needed to implement the “harder” primitive by a quantum protocol, which would give us an alternative measure of non-triviality of two-party primitives.

References

1. Ambainis, A.: personal communication (2005)
2. Ariano, G.M.D., Kretschmann, D., Schlingemann, D., Werner, R.F.: Reexamination of quantum bit commitment: The possible and the impossible. *Physical Review A (Atomic, Molecular, and Optical Physics)* 76(3), 032328 (2007)
3. Barrett, J., Linden, N., Massar, S., Pironio, S., Popescu, S., Roberts, D.: Nonlocal correlations as an information-theoretic resource. *Physical Review A* 71, 022101 (2005)
4. Bennett, C.H., Brassard, G.: Quantum cryptography: Public key distribution and coin tossing. In: *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing*, pp. 175–179 (1984)
5. Berta, M.: Single-shot quantum state merging. Master’s thesis, ETH Zurich (2008)
6. Buhrman, H., Christandl, M., Hayden, P., Lo, H.-K., Wehner, S.: Possibility, impossibility and cheat-sensitivity of quantum bit string commitments. *Physical Review A* 78, 022316 (2008)
7. Buhrman, H., Christandl, M., Schaffner, C.: Impossibility of two-party secure function evaluation (in preparation, 2009)
8. Chailloux, A., Kerenidis, I.: Optimal quantum strong coin flipping (2009), <http://arxiv.org/abs/0904.1511>
9. Chor, B., Kushilevitz, E.: A zero-one law for boolean privacy. *SIAM J. Discrete Math.* 4(1), 36–47 (1991)
10. Colbeck, R.: The impossibility of secure two-party classical computation (August 2007), <http://arxiv.org/abs/0708.2843>
11. Damgård, I.B., Fehr, S., Salvail, L., Schaffner, C.: Secure identification and QKD in the bounded-quantum-storage model. In: Menezes, A. (ed.) *CRYPTO 2007*. LNCS, vol. 4622, pp. 342–359. Springer, Heidelberg (2007)
12. Fehr, S., Schaffner, C.: Composing quantum protocols in a classical environment. In: Reingold, O. (ed.) *TCC 2009*. LNCS, vol. 5444, pp. 350–367. Springer, Heidelberg (2009)
13. Fitz, M., Wolf, S., Wullschlegel, J.: Pseudo-signatures, broadcast, and multi-party computation from correlated randomness. In: Franklin, M. (ed.) *CRYPTO 2004*. LNCS, vol. 3152, pp. 562–579. Springer, Heidelberg (2004)
14. Holevo, A.S.: Information-theoretical aspects of quantum measurement. *Problemy Peredači Informacii* 9(2), 31–42 (1973)
15. Imai, H., Müller-Quade, J., Nascimento, A., Winter, A.: Rates for bit commitment and coin tossing from noisy correlation. In: *Proceedings of 2004 IEEE International Symposium on Information Theory*, p. 47 (June 2004)
16. Jozsa, R., Schlienz, J.: Distinguishability of states and von neumann entropy. *Phys. Rev. A* 62(1), 012301 (2000)
17. Kent, A.: Promising the impossible: Classical certification in a quantum world (2004), <http://arxiv.org/abs/quant-ph/0409029>
18. Kitaev, A.: Quantum coin-flipping. presented at QIP 2003. A review of this technique can be found in (2003), <http://lightlike.com/~carlosm/publ>

19. Klauck, H.: On quantum and approximate privacy. *Theory of Computing Systems* 37(1), 221–246 (2004); <http://arxiv.org/abs/quant-ph/0110038>, also in the Proceedings of STACS (2002)
20. Künzler, R., Müller-Quade, J., Raub, D.: Secure computability of functions in the it setting with dishonest majority and applications to long-term security. In: Reingold, O. (ed.) TCC 2009. LNCS, vol. 5444, pp. 238–255. Springer, Heidelberg (2009)
21. Kushilevitz, E.: Privacy and communication complexity. *SIAM J. Discrete Math.* 5(2), 273–284 (1992)
22. Lo, H.-K.: Insecurity of quantum secure computations. *Physical Review A* 56(2), 1154–1162 (1997)
23. Lo, H.-K., Chau, H.F.: Is quantum bit commitment really possible? *Physical Review Letters* 78(17), 3410–3413 (1997)
24. Mayers, D.: Unconditionally secure quantum bit commitment is impossible. *Physical Review Letters* 78(17), 3414–3417 (1997)
25. Mochon, C.: Quantum weak coin-flipping with bias of 0.192. In: 45th Annual IEEE Symposium on Foundations of Computer Science (FOCS), pp. 2–11 (2004)
26. Mochon, C.: A large family of quantum weak coin-flipping protocols. *Phys. Rev. A* 72, 022341 (2005)
27. Mochon, C.: Quantum weak coin flipping with arbitrarily small bias (2007), <http://arxiv.org/abs/0711.4114>
28. Nielsen, M.A., Chuang, I.L.: *Quantum Computation and Quantum Information*. Cambridge University Press, Cambridge (2000)
29. Popescu, S., Rohrlich, D.: Quantum nonlocality as an axiom. *Foundations of Physics* 24(3), 379–385 (1994)
30. Renner, R., Wolf, S.: Simple and tight bounds for information reconciliation and privacy amplification. In: Roy, B. (ed.) ASIACRYPT 2005. LNCS, vol. 3788, pp. 199–216. Springer, Heidelberg (2005)
31. Renner, R., Wolf, S., Wullschleger, J.: The single-serving channel capacity. In: Proceedings of the International Symposium on Information Theory (ISIT). IEEE, Los Alamitos (July 2006), <http://arxiv.org/abs/cs.IT/0608018>
32. Ruskai, M.B.: Inequalities for quantum entropy: A review with conditions for equality. *Journal of Mathematical Physics* 43(9), 4358–4375 (2002)
33. Salvail, L., Sotáková, M., Schaffner, C.: On the power of two-party quantum cryptography (2009), <http://arxiv.org/abs/0902.4036>
34. Spekkens, R.W., Rudolph, T.: Degrees of concealment and bindingness in quantum bit commitment protocols. *Phys. Rev. A* 65(1), 012310 (2001)
35. Winter, A., Renner, R.: Single-shot state merging (2007) (unpublished note)
36. Wolf, S., Wullschleger, J.: Zero-error information and applications in cryptography. In: IEEE Information Theory Workshop (ITW), San Antonio, Texas (October 2004)
37. Wolf, S., Wullschleger, J.: New monotones and lower bounds in unconditional two-party computation. In: Shoup, V. (ed.) CRYPTO 2005. LNCS, vol. 3621, pp. 467–477. Springer, Heidelberg (2005)
38. Wolf, S., Wullschleger, J.: Oblivious transfer and quantum non-locality. In: International Symposium on Information Theory (ISIT 2005), pp. 1745–1748 (2005)