Complete Insecurity of Quantum Protocols for Classical Two-Party Computation

Harry Buhrman,[1] Matthias Christandl,[2] and Christian Schaffner[1]

[1] *University of Amsterdam and CWI Amsterdam, The Netherlands*

[2] *Institute for Theoretical Physics, ETH Zurich, Wolfgang-Pauli-Strasse 27, CH-8093 Zurich, Switzerland*

(Dated: January 5, 2012)

A fundamental task in modern cryptography is the joint computation of a classical deterministic function which has two inputs, one from Alice and one from Bob, such that neither of the two can learn more about the other's input than what is implied by the value of the function (secure two-party computation). In this work we show that any quantum protocol that outputs the result to both parties (two-sided computation) and that is secure against a cheating Bob can be completely broken by a cheating Alice. Whereas it is known that quantum protocols for this task cannot be completely secure, our result implies that even partial security cannot be obtained. Our findings stand in stark contrast to recent works on coin tossing, where interesting quantum mechanical advantages can be obtained, and highlight the limits of cryptography within quantum mechanics. With help of von Neumann's minimax theorem we extend the result to the imperfect case, where the quantum protocol may not work perfectly and may not be perfectly secure.

PACS numbers:

Traditionally, cryptography has been understood as the art of "secret writing“, i.e., of sending messages securely from one party to another. Today, the research field cryptography comprises much more than encryption and studies all aspects of secure communication and computation among players that do not trust each other. Examples of such multi-party computations are the millionaire's problem, electronic voting, auctions etc.

A wave of excitement was sparked when it was proposed that quantum mechanics may offer the possibility to distribute a perfectly secure key among distant parties, thereby achieving a level of security unattainable by classical means [1, 2]. The immediate question arose whether other fundamental cryptographic tasks such as oblivious transfer, bit commitment and coin tossing could be implemented with the same level of security with help of quantum mechanical effects. Unfortunately, this is not the case as was illustrated with oblivious transfer and bit commitment which are impossible within a quantum mechanical framework [3, 4]. Interestingly, however, a weak version of a coin toss can be implemented by quantum mechanical means [5]. In this Letter we study the task of secure two-party computation. Here, two mistrustful players, Alice and Bob, wish to compute the value of a classical function f, which takes an input u from Alice and v from Bob, in such a way that both learn the result of the computation (two-sided classical computation) and that no one can learn more about the other's input, even if they cheat during the execution of the protocol.

We prove two main results. Our first result (Theorem 1) is that any protocol which is secure against a cheating Bob can be completely broken by Alice. Formally, we design an attack by Alice which allows her to compute the value of the function f for all of her inputs (rather than only a single one, which would be required from a secure protocol).

Our result strengthens the impossibility result for two-sided two-party computation by Colbeck, where he showed that Alice can always obtain more information about Bob's input than what is implied by the value of the function [6]. In a similar way, we improve a result by Salvail, Schaffner and Sotáková [7] showing that any quantum protocol for a non-trivial primitive necessarily leaks information to a dishonest player. Our result is motivated by Lo's impossibility result for the case where only Alice obtains the result of the function (one-sided computation) [8]. Lo's approach is based on the idea that Bob does not have any output, hence his quantum state cannot depend on Alice's input. Then, Bob has learned nothing about Alice's input and a cheating Alice can therefore still change her input value (by purifying the protocol) and thus cheat. In the two-sided case, this approach to proving the insecurity of two-party computation fails as Bob knows the value of the function and has thus some information about Alice's input. In order to overcome this problem we develop a new approach. We start with a formal definition of security based on the standard real/ideal-world paradigm from modern cryptography. If a protocol is secure, this definition guarantees the existence of a classical input on Bob's side [17]. When Alice then purifies her protocol, she is able to obtain a copy of this input and break the protocol in the stated way.

Our second result (Theorem 2) shows that the above conclusion is still valid if the protocol is not required to be perfectly secure (nor perfectly correct). More precisely, if the protocol is secure up to a small error against cheating Bob, then Alice is able to compute the value of the function for all of her inputs with only a small error. It is important to note that the error is independent of the number of inputs that both Alice and Bob have. Thus our analysis dramatically improves Lo's analysis in the one-sided case to which it can also be applied. We achieve this result by use of von Neumann's minimax theorem together with a robust version of the previous result.

The Letter is structured as follows. We first introduce two-party computation and the relevant notions of security. Then we derive a technical lemma and show how it implies that perfectly secure two-party computation is impossible. In a final step, we extend the analysis to the case of imperfect protocols and give examples illustrating our results and demonstrating that they are tight.

Security Definition. Alice and Bob are interested in computing the outcome of a classical function f that takes an input u from Alice and an input v from Bob. Since Alice does not trust Bob, she wants to be sure that the protocol does not allow him to extract more information about her input than what is implied by the output value of the function. The same should be true if Alice is cheating and Bob is honest.

In cryptography, a good way to define security of a protocol has turned out to be the following. First we define an ideal situation in which everything is computed perfectly and securely and call this the *ideal functionality* $\mathcal{F}$. We are then interested in a two-party protocol π that securely implements this ideal functionality. The informal definition of security is then straightforward: A protocol is called secure if it looks to the outside world just as the ideal functionality it is supposed to implement. Concretely, for every adversarial strategy, or *real adversary* who does not necessarily follow the protocol and outputs some state, we require an explanation of this behavior in the ideal world, i.e. there has to exist an *ideal adversary* interacting only with the ideal functionality but producing the same output as the real adversary. If such a security guarantee based on this real/ideal-world paradigm holds, it is intuitively clear that a secure protocol can be treated as a call to the ideal functionality and hence, it is possible to construct and prove secure more complicated protocols in a modular fashion. For further information about the concept of *composability* in cryptography, see [9] in the context of classical protocols and [10–13] for developments in the context of quantum protocols.

Rather than choosing the input themselves, it turns out to be convenient to provide an input to all players (honest or adversarial). Security will be considered with respect to a purification of this input, a natural concept in quantum information theory. Security then means that for all inputs and for all real adversaries, there exists an ideal adversary such that the output state of the real and the ideal situation are indistinguishable. This notion of security was introduced in [13] and is called *statistical security in the quantum stand-alone model* [11] [18].

We follow the notation of [13] and denote by A and B the real honest Alice and Bob and add a prime to denote dishonest players A', B' and a hat for the ideal versions $\hat{\mathsf{A}}, \hat{\mathsf{B}}$. The corresponding protocol for honest Alice and a dishonest Bob is denoted by $\pi_{\mathsf{A},\mathsf{B}'}$. Both honest and dishonest players obtain an input, in Alice's case u (in register U) and in Bob's case v (in register V) drawn from the joint distribution $p(u,v)$. The output state of the protocol, augmented by the reference R, takes the form $\mathrm{id}_R \otimes \pi_{\mathsf{A},\mathsf{B}'}(\rho_{UVR})$, where ρ_{UVR} is a purification of the input $\sum_{u,v} p(u,v)|u\rangle\langle u|_U \otimes |v\rangle\langle v|_V$.

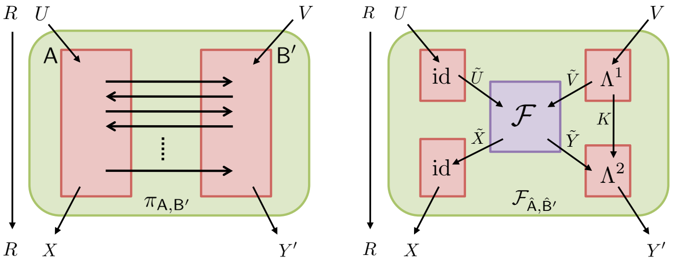

FIG. 1: Illustration of the security definition against dishonest Bob. A protocol is secure if the *real protocol* (left) can be simulated as an interaction with the *ideal functionality* $\mathcal{F}$ (right).

The ideal functionality for two-party computation $\mathcal{F}$ of a deterministic classical function f that takes inputs u from Alice and v from Bob and outputs $f(u,v)$ to Alice and Bob can be defined formally as the following completely positive trace preserving (CPTP) map $\mathcal{F} : \tilde{U}\tilde{V} \to \tilde{X}\tilde{Y}$: $\mathcal{F}(|u\rangle\langle u'|_{\tilde{U}} \otimes |v\rangle\langle v'|_{\tilde{V}}) = \delta_{u,u'}\delta_{v,v'}|f(u,v)\rangle\langle f(u,v)|_{\tilde{X}} \otimes |f(u,v)\rangle\langle f(u,v)|_{\tilde{Y}}$, where δ denotes the Kronecker delta function. When an ideal honest $\hat{\mathsf{A}}$ and an ideal adversary $\hat{\mathsf{B}}'$ interact with the ideal functionality, we denote the ideal protocol by $\mathcal{F}_{\hat{\mathsf{A}},\hat{\mathsf{B}}'} : UV \to XY'$. It is described in Figure 1 and takes the form $\mathcal{F}_{\hat{A},\hat{\mathsf{B}}'} = [\mathrm{id}_{\tilde{X}\to X} \otimes \Lambda^2_{K\tilde{Y}\to Y'}] \circ [\mathcal{F}_{\tilde{U}\tilde{V}\to\tilde{X}\tilde{Y}} \otimes \mathrm{id}_K] \circ [\mathrm{id}_{U\to\tilde{U}} \otimes \Lambda^1_{V\to\tilde{V}K}]$, where $\circ$ denotes sequential application of CPTP maps. The CPTP maps $\Lambda^1_{V\to\tilde{V}K}$ and $\Lambda^2_{K\tilde{Y}\to Y'}$ determine $\hat{\mathsf{B}}'$. $\hat{\mathsf{A}}$, the counterpart of honest Alice in the ideal world, forwards the input and output to and from the functionality. In the following let $\varepsilon \geq 0$.

Definition. *A (two-party quantum) protocol* π ε-securely implements *an ideal classical functionality* $\mathcal{F}$ *if the following holds:*

ε-correctness: *For any distribution* $p(u,v)$ *of the inputs*

$$[\mathrm{id}_R \otimes \pi_{\mathsf{A},\mathsf{B}}](\rho_{UVR}) \approx_\varepsilon [\mathrm{id}_R \otimes \mathcal{F}_{\hat{\mathsf{A}},\hat{\mathsf{B}}}](\rho_{UVR}),$$

where ρ_{UVR} *is defined as above and the approximation is quantified in the purified distance* $C(\rho,\sigma) := \sqrt{1 - F(\rho,\sigma)^2}$. $F(\rho,\sigma) := \mathrm{tr}\,\sqrt{\sqrt{\rho}\sigma\sqrt{\rho}}$ *is the fidelity.*

ε-security against dishonest Bob*: For any distribution* $p(u,v)$ *and for any real adversary* B'*, there exists an ideal adversary* $\hat{\mathsf{B}}'$ *such that*

$$[\mathrm{id}_R \otimes \pi_{\mathsf{A},\mathsf{B}'}](\rho_{UVR}) \approx_\varepsilon [\mathrm{id}_R \otimes \mathcal{F}_{\hat{\mathsf{A}},\hat{\mathsf{B}}'}](\rho_{UVR}) \,.$$

ε-security against dishonest Alice *is defined analogously.*

Since $\mathcal{F}$ is classical, we can augment it so that it outputs $\tilde{v}$ in addition. More precisely, we can define

$\mathcal{F}_{aug} : \tilde{U}\tilde{V} \to \tilde{X}\tilde{Y}\tilde{V}$ by $\mathcal{F}_{aug}(|u\rangle\langle u'|_{\tilde{U}} \otimes |v\rangle\langle v'|_{\tilde{V}}) := \delta_{u,u'}\delta_{v,v'}|f(u,v)\rangle\langle f(u,v)|_{\tilde{X}} \otimes |f(u,v)\rangle\langle f(u,v)|_{\tilde{Y}} \otimes |v\rangle\langle v|_{\tilde{V}}$. which has the property that $\mathcal{F} = \mathrm{tr}_{\tilde{V}}\,\mathcal{F}_{aug}$. Formulated for a concrete input state we define $\sigma_{RX\tilde{V}Y'} := [\mathrm{id}_R \otimes \mathcal{F}_{\mathsf{A},\hat{\mathsf{B}}',aug}](\rho_{UVR})$ which satisfies $\sigma_{RXY'} \approx_\varepsilon \rho_{RXY'}$ for $\rho_{RXY'} := [\mathrm{id}_R \otimes \pi_{\mathsf{A},\mathsf{B}'}](\rho_{UVR})$ if the protocol is secure against cheating Bob. We call $\sigma_{RX\tilde{V}Y'}$ a *secure state for input distribution* $p(u,v)$.

Main Results. The proof of our results builds upon the following lemma which constructs a cheating strategy for Alice that works *on average* over the input distribution $p(u,v)$ for a protocol that is ε-secure against Bob. Subsequently we will show how this result can be used to devise a cheating strategy that works *for all* distributions at the same time.

Lemma. *If a protocol π for the evaluation of f is ε-secure against Bob, then for all input distributions $p(u,v)$ there is a cheating strategy for Alice such that she obtains $\tilde{v}$ with some probability distribution $q(\tilde{v}|u,v)$ satisfying $\sum_{u,v,\tilde{v}} p(u,v)q(\tilde{v}|u,v)\delta_{f(u,v),f(u,\tilde{v})} \geq 1-6\varepsilon$. Furthermore, $q(\tilde{v}|u,v)$ is almost independent of u; i.e., there exists a distribution $\tilde{q}(\tilde{v}|v)$ such that $\sum_{u,v,\tilde{v}} p(u,v)|q(\tilde{v}|u,v) - \tilde{q}(\tilde{v}|v)| \leq 6\varepsilon$.*

Proof. The proof consists of two parts. We first construct a "cheating unitary" T for Alice and show in the second step how Alice can use it to cheat successfully.

Let Alice and Bob play honestly but let them purify their protocol with purifying registers X_1' and Y_1' respectively. We assume without loss of generality that honest parties measure their classical input and hence, X_1' and Y_1' contain copies of u and v, respectively. We denote by $|\Phi\rangle_{RXX_1'Y_1'Y}$ the state of all registers at the end of the protocol. Notice that tracing out X_1' from $|\Phi\rangle_{RXX_1'Y_1'Y}$ results in a state $\mathrm{tr}_{X_1'}|\Phi\rangle\langle\Phi|_{RXX_1'Y_1'Y} = \rho_{RXY_1'Y}$ which is exactly the final state when Alice played honestly and Bob played dishonestly with the following strategy: He plays the honest but purified strategy and outputs the purification of the protocol (register Y_1') and the output values $f(u,v)$ (register Y). His combined dishonest register is $Y' = Y_1'Y$. Since the protocol is ε-secure against Bob by assumption, there exists a secure state $\sigma_{RX\tilde{V}Y'}$ satisfying

$$\sigma_{RXY'} \approx_\varepsilon \rho_{RXY'}. \tag{1}$$

Let $|\Psi\rangle_{RXP\tilde{V}Y'}$ be a purification of $\sigma_{RX\tilde{V}Y'}$ with purifying register P. Note that $|\Psi\rangle_{RXP\tilde{V}Y'}$ is also a purification of $\sigma_{RXY'}$, this time with purifying registers $P\tilde{V}$.

Recall that $|\Phi\rangle_{RXX_1'Y'}$ purifies $\rho_{RXY'}$ with purifying register X_1'. By (1) and Uhlmann's theorem [14] there exists an isometry $T_{X_1'\to P\tilde{V}}$ (with induced CPTP map $\mathcal{T}_{X_1'\to P\tilde{V}}$) such that

$$(T_{X_1'\to P\tilde{V}} \otimes \mathbb{1}_{RXY'})|\Phi\rangle_{RXX_1'Y'} \approx_\varepsilon |\Psi\rangle_{RXP\tilde{V}Y'}. \tag{2}$$

The approximation is measured in the purified distance of the corresponding density matrices. This concludes the construction of $T \equiv T_{X_1'\to P\tilde{V}}$.

We will now show how Alice can use the isometry $T_{X_1'\to P\tilde{V}}$ to cheat. Notice that tracing out Y_1' from $|\Phi\rangle_{RXX_1'YY_1'}$ results exactly in the final state when Bob played honestly and Alice played dishonestly with the following strategy: She plays the honest but purified strategy and outputs the purification of the protocol (register X_1') and the output values $f(u,v)$ (register X). She then applies $T_{X_1'\to P\tilde{V}}$, measures register $\tilde{V}$ in the computational basis and obtains a value $\tilde{v}$. It remains to argue that Alice can compute $f(u,v)$ with good probability based on the value $\tilde{v}$ that she has obtained from measuring register $\tilde{V}$.

Let $\mathcal{M}_{R\tilde{V}X}$ be the CPTP map that measures registers R, X and $\tilde{V}$ in the computational basis. Tracing over PY' and applying $\mathcal{M}_{R\tilde{V}X}$ on both sides of (2), we find

$$\begin{aligned}&[\mathcal{M}_{RX\tilde{V}} \otimes \mathrm{tr}_{PY'}]([\mathcal{T}_{X_1'\to P\tilde{V}} \otimes \mathrm{id}_{RXY'}](|\Phi\rangle\langle\Phi|_{RXX_1'Y'}))\\ &\qquad \approx_\varepsilon [\mathcal{M}_{RX\tilde{V}}\,\mathrm{tr}_{PY'}](|\Psi\rangle\langle\Psi|_{RXP\tilde{V}Y'})\end{aligned} \tag{3}$$

by the monotonicity of the purified distance under CPTP maps. The right hand side of (3) equals

$$\sum_{u,v,\tilde{v}} p(u,v)\tilde{q}(\tilde{v}|v)|uv\rangle\langle uv|_R \otimes |\tilde{v}\rangle\langle\tilde{v}|_{\tilde{V}} \otimes |f(u,\tilde{v})\rangle\langle f(u,\tilde{v})|_X.$$

for some probability distribution $\tilde{q}(\tilde{v}|v)$ that is conditioned only on Bob's input v, since $|\Psi\rangle_{RXP\tilde{V}Y'}$ is a purification of the secure state $\sigma_{RX\tilde{V}Y'}$. The left hand side of (3) equals

$$\begin{aligned}\sum_{u,v,\tilde{v},x} p(u,v)q(\tilde{v}|u,v)|uv\rangle\langle uv|_R \otimes |\tilde{v}\rangle\langle\tilde{v}|_{\tilde{V}}\\ \otimes r(x|u,v,\tilde{v})|x\rangle\langle x|_X\end{aligned} \tag{4}$$

for some conditional probability distributions $\tilde{q}(\tilde{v}|u,v)$ and $r(x|u,v,\tilde{v})$. Due to the correctness of the protocol, (4) is ε-close to the state

$$\sum_{u,v,\tilde{v}} p(u,v)\bar{q}(\tilde{v}|u,v)|uv\rangle\langle uv|_R \otimes |\tilde{v}\rangle\langle\tilde{v}|_{\tilde{V}} \otimes |f(u,v)\rangle\langle f(u,v)|_X \tag{5}$$

for some conditional probability distribution $\bar{q}(\tilde{v}|u,v)$. Noting that the ε-closeness of (4) and (5) implies that $p(\cdot,\cdot)q(\cdot|\cdot,\cdot)$ and $p(\cdot,\cdot)\bar{q}(\cdot|\cdot,\cdot)$ (when interpreted as quantum states) are ε-close in purified distance, we can replace $p(\cdot,\cdot)\bar{q}(\cdot|\cdot,\cdot)$ in (5) by $p(\cdot,\cdot)q(\cdot|\cdot,\cdot)$ increasing the purified distance to the left hand side of (3) only to 2ε. Putting things together, (3) implies

$$\begin{aligned}&\sum_{u,v,\tilde{v}} p(u,v)q(\tilde{v}|u,v)|uv\rangle\langle uv|_R \otimes |\tilde{v}\rangle\langle\tilde{v}|_{\tilde{V}}\\ &\quad \otimes |f(u,v)\rangle\langle f(u,v)|_X \approx_{3\varepsilon} \sum_{u,v,\tilde{v}} p(u,v)\tilde{q}(\tilde{v}|v)\\ &\quad \times |uv\rangle\langle uv|_R \otimes |\tilde{v}\rangle\langle\tilde{v}|_{\tilde{V}} \otimes |f(u,\tilde{v})\rangle\langle f(u,\tilde{v})|_X.\end{aligned} \tag{6}$$

Sandwiching both sides with $\mathrm{tr}[Z\cdot]$, where $Z = \sum_{u,v,\tilde{v}} |uv\rangle\langle uv|_R \otimes |\tilde{v}\rangle\langle\tilde{v}|_{\tilde{V}} \otimes |f(u,\tilde{v})\rangle\langle f(u,\tilde{v})|_X$ we find the first claim since the purified distance does not increase under trace-non-increasing completely positive maps such as $\mathrm{tr}[Z\cdot]$, and since the purified distance of two distributions upper bounds their total variation distance. The second claim follows similarly by tracing out register X from (6). □

Theorem 1. *If a protocol π for the evaluation of f is perfectly secure (i.e. $\varepsilon = 0$) against Bob, then Alice can completely break the protocol, i.e. if Bob has input v, she can compute $f(u,v)$ for all u.*

Proof. Letting $p(u,v) = \frac{1}{|U||V|}$ and $\varepsilon = 0$ in the Lemma results in the statement that if Alice has input u_0, then she will obtain $\tilde{v}$ from the distribution $q(\tilde{v}|u_0,v)$ which equals $\tilde{q}(\tilde{v}|v)$. But since also $q(\tilde{v}|u,v) = \tilde{q}(\tilde{v}|v)$ for all u, we have $\frac{1}{|U||V|}\sum_{u,v,\tilde{v}} q(\tilde{v}|u_0,v)\delta_{f(u,v),f(u,\tilde{v})} = 1$. In other words, all $\tilde{v}$ that occur (i.e. that have $\tilde{q}(\tilde{v}|v) > 0$) satisfy for all u, $f(u,v) = f(u,\tilde{v})$. Alice can therefore compute the function for all u. □

Theorem 2. *If a protocol π for the evaluation of f is ε-secure against Bob, then there is a cheating strategy for Alice (where she uses input u_0 while Bob has input v) which gives her $\tilde{v}$ distributed according to some distribution $Q(\tilde{v}|u_0,v)$ such that for all u: $\sum_{\tilde{v}} Q(\tilde{v}|u_0,v)\delta_{f(u,v),f(u,\tilde{v})} \geq 1 - 28\varepsilon$.*

Proof. The argument is inspired by [15]. Consider a finite ε-net $\mathcal{D}$ of distributions $p \equiv p(u,v)$ in the total variation distance; and to each such distribution the corresponding cheating unitary T constructed in the proof of the Lemma. We can assume that T determines p uniquely, as we could include the value p into T. Let $q(\tilde{v}|u,v,T)$ and $\tilde{q}(\tilde{v}|v,T)$ be the distributions from the Lemma. Define the payoff function $g(u,v,T) := \sum_{\tilde{v}} q(\tilde{v}|u,v,T)\delta_{f(u,v),f(u,\tilde{v})} - \sum_{\tilde{v}} |q(\tilde{v}|u,v,T) - \tilde{q}(\tilde{v}|v,T)|$ and consider the value

$$\min_{p'}\max_{T}\sum_{u,v} p'(u,v)g(u,v,T) \tag{7}$$

where the minimisation extends over all distributions p' but the maximum is only taken over unitaries T corresponding to p's from $\mathcal{D}$. We rewrite and bound (7) as

$$\begin{aligned}\min_{p\in\mathcal{D}}\min_{p'\approx_\epsilon p}\max_{T}\sum_{u,v} p'(u,v)g(u,v,T)\\ \geq \min_{p\in\mathcal{D}}\max_{T}\sum_{u,v} p(u,v)g(u,v,T) - 2\epsilon\end{aligned}$$

since replacing p' by p incurs only an overall change in the value by 2ε (since $-1 \leq g(u,v,T) \leq 1$). By the Lemma, the right hand side is larger than $1 - 12\varepsilon - 2\varepsilon = 1 - 14\varepsilon$.

Von Neumann's minimax theorem shows that (7) equals $\max_{p(T)}\min_{u,v}\sum_T p(T)g(u,v,T)$ and by the above discussion, this value is larger than $1 - 14\varepsilon$. This shows that there is a probabilistic strategy $p(T)$ and $\varepsilon_1 + \varepsilon_2 \leq 14\varepsilon$ such that for all u, v,

$$\sum_{\tilde{v}} Q(\tilde{v}|u,v)\delta_{f(u,v),f(u,\tilde{v})} \geq 1 - \varepsilon_1 \tag{8}$$

and $\sum_{\tilde{v}} |Q(\tilde{v}|u,v) - \tilde{Q}(\tilde{v}|v)| \leq \sum_{\tilde{v},T} p(T)|q(\tilde{v}|u,v,T) - \tilde{q}(\tilde{v}|v,T)| \leq \varepsilon_2$, where $Q(\tilde{v}|u,v) := \sum_T p(T)q(\tilde{v}|u,v,T)$ and $\tilde{Q}(\tilde{v}|v) := \sum_T p(T)\tilde{q}(\tilde{v}|v,T)$. This implies that for all u, v, $\sum_{\tilde{v}} |Q(\tilde{v}|u_0,v) - Q(\tilde{v}|u,v)| \leq 2\varepsilon_2$. Combining this inequality with (8), we find for all u, v, $\sum_{\tilde{v}} Q(\tilde{v}|u_0,v)\delta_{f(u,v),f(u,\tilde{v})} \geq 1 - \varepsilon_1 - 2\varepsilon_2 \geq 1 - 28\varepsilon$. □

In conclusion we have shown that classical two-party computation is not possible at all within quantum mechanics. We therefore significantly strengthen previous impossibility results and improve the understanding of the concept of security in quantum physics.

One might wonder whether Theorem 2 can be strengthened to obtain, with probability $1 - O(\varepsilon)$, a $\tilde{v}$ such that for all $u : f(u,v) = f(u,\tilde{v})$. It turns out that this depends on the function f: when f is equality ($\mathrm{EQ}(x,y) = 1$ iff $x = y$) and inner-product modulo-2 ($\mathrm{IP}(x,y) = \sum_i x_i \cdot y_i \mod 2$), the stronger conclusion is possible. However for disjointness ($\mathrm{DISJ}(x,y) = 0$ iff $\exists i : x_i = y_i = 1$) such a strengthening is not possible showing that our result is tight in general.

For EQ, we reason as follows. Set $u = v$ in Theorem 2. Alice is able to sample a $\tilde{v}$ such that $\sum_{\tilde{v}} Q(\tilde{v}|u_0,v)\delta_{EQ(v,v),EQ(v,\tilde{v})} \geq 1 - 28\varepsilon$. Since $\delta_{\mathrm{EQ}(v,v),\mathrm{EQ}(v,\tilde{v})} = 1$ iff $v = \tilde{v}$, $Q(v|u_0,v) \geq 1 - 28\varepsilon$. When f is IP, we pick u uniform at random and obtain: $\sum_{\tilde{v}} Q(\tilde{v}|u_0,v)(2^{-n}\sum_u \delta_{\mathrm{IP}(u,v),\mathrm{IP}(u,\tilde{v})}) \geq 1 - 28\varepsilon$. Using that $2^{-n}\sum_u \delta_{\mathrm{IP}(u,v),\mathrm{IP}(u,\tilde{v})} = 1$ if $\tilde{v} = v$, and $\frac{1}{2}$ if $\tilde{v} \neq v$, we have that $Q(v|u_0,v) + \frac{1}{2}(1 - Q(v|u_0,v)) \geq 1 - 28\varepsilon$, which implies that $Q(v|u_0,v) \geq 1 - 56\varepsilon$. Interestingly, for DISJ such an argument is not possible. Assume that we have a protocol that is ε-secure against Bob. Bob could now run the protocol normally on strings y with Hamming weight $|y| \leq n/2$, but on inputs y with $|y| > n/2$ he could flip, at random, $\sqrt{n}$ of y's bits that are 1. It is not hard to see that this new protocol is still ε-secure and $\varepsilon + O(\frac{1}{\sqrt{n}})$-correct. The loss in the correctness is due to the fact, that on high-Hamming-weight strings, the protocol may, with a small probability, not be correct. On the other hand, on high-Hamming-weight inputs, the protocol can not transmit/leak the complete input v to Alice, simply because Bob does not use it.

Acknowledgments. MC is supported by the Swiss National Science Foundation (grant PP00P2-128455) and the NCCR QSIT. CS is supported by a NWO Veni grant.

[1] C. H. Bennett and G. Brassard, in *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing* (1984), pp. 175–179.

[2] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).

[3] H.-K. Lo and H. Chau, Phys. Rev. Lett. **78**, 3410 (1997).

[4] D. Mayers, Phys. Rev. Lett. **78**, 3414 (1997).

[5] C. Mochon, *Quantum weak coin flipping with arbitrarily small bias* (2007), arXiv:0711.4114.

[6] R. Colbeck, Phys. Rev. A **76**, 062308 (2007).

[7] L. Salvail, M. Sotáková, and C. Schaffner, in *Advances in Cryptology—ASIACRYPT* (Springer-Verlag, 2009), vol. 5912 of *Lecture Notes in Computer Science*, pp. 70–87.

[8] H.-K. Lo, Phys. Rev. A **56**, 1154 (1997).

[9] R. Canetti, Journal of Cryptology **13**, 143 (2000).

[10] D. Unruh, *Simulatable security for quantum protocols* (2004), arXiv:quant-ph/0409125.

[11] D. Unruh, in *Advances in Cryptology EUROCRYPT* (Springer, 2010), vol. 6110 of *Lecture Notes in Computer Science*, pp. 486–505.

[12] M. Ben-Or and D. Mayers (2004), arXiv:quant-ph/0409062.

[13] S. Fehr and C. Schaffner, in *Theory of Cryptography Conference (TCC)* (Springer, 2009), vol. 5444, pp. 350–367.

[14] A. Uhlmann, Rep. Math. Phys. **9**, 273 (1976).

[15] G. M. D'Ariano, D. Kretschmann, D. Schlingemann, and R. F. Werner, Phys. Rev. A **76**, 032328 (2007).

[16] A. Kent, Quantum Information Processing (2011).

[17] See also [16] for recent work on the impossibility of certifying a classical input.

[18] One may also consider the stronger notion of security called *universal composability*, see [11]. We choose in this work to use the weaker notion of stand-alone security as we prove an impossibility result.