Complete insecurity of quantum protocols for classical two-party computation

Buhrman, H.; Christandl, M.; Schaffner, C.

Published in:
Physical Review Letters

DOI:
10.1103/PhysRevLett.109.160501

Citation for published version (APA):
Complete Insecurity of Quantum Protocols for Classical Two-Party Computation

Harry Buhrman,¹ Matthias Christandl,² and Christian Schaffner¹

¹University of Amsterdam and CWI Amsterdam, Amsterdam, The Netherlands
²Institute for Theoretical Physics, ETH Zurich, Wolfgang-Pauli-Strasse 27, CH-8093 Zurich, Switzerland

(Received 4 January 2012; published 17 October 2012)

A fundamental task in modern cryptography is the joint computation of a 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. In this Letter, we show that any quantum protocol for the computation of a classical deterministic function 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 security for one party implies complete insecurity for the other. Our findings stand in stark contrast to recent protocols for weak coin tossing and highlight the limits of cryptography within quantum mechanics. We remark that our conclusions remain valid, even if security is only required to be approximate and if the function that is computed for Bob is different from that of Alice.

DOI: 10.1103/PhysRevLett.109.160501 PACS numbers: 03.67.Dd, 03.67.Hk

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 of cryptography comprises much more than encryption and studies all aspects of secure communication and computation among players that do not trust each other, including tasks such as electronic voting and auctioning. Following the excitement that the exchange of quantum particles may allow for the distribution of a key that is unconditionally secure [1,2], a level of security unattainable by classical means, the question arose whether other fundamental cryptographic tasks could be implemented with the same level of security using quantum mechanical effects. For oblivious transfer and bit commitment, it was shown that the answer is negative [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 deterministic 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 and that none of the parties can learn more about the other’s input, even by deviating from the protocol. As our main result, we show that any quantum protocol which is secure against a cheating Bob can be completely broken by a cheating 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 secure 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 complement a result by Salvail et al. [7] showing that any quantum protocol for a nontrival 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. In our case of a classical functionality, this definition guarantees the existence of a classical input for Bob in the ideal world, even if he is, in the real world, dishonestly purifying his steps of the protocol. Since real and ideal are indistinguishable for a secure protocol and since a purification of the classical input cannot be part of Bob’s systems, Alice can now obtain a copy of this input by applying a unitary—constructed with help of Uhlmann’s theorem—to her output registers and, henceforth, break the protocol.

We wish to emphasize that the above conclusion remains valid if the protocol is not required to be perfectly secure.
execute a protocol that takes an input and only connected with a quantum channel, wish to pre- and postprocessing of the in- and outputs to the ideal functionality is composed out of CPTP maps modeling the a completely positive trace-preserving (CPTP) map. Informal notion of the real–ideal-world paradigm precise. Classical and quantum protocols, respectively. It is possible to construct and prove secure more complicated treatments as a call to the ideal functionality, and hence, it is guaranteed holds, it is clear that a secure protocol can be constructed and prove secure (see, e.g., Ref. [16]).

Since our goal is the establishment of a no-go theorem, we consider a notion of security which is weaker than the above in two respects. First, we do not allow the environment to supply an arbitrary input state but only the purification of a classical input (see definition of $\rho_{UVR}$ below), and second, we consider a different order of quantifiers: instead of “$\forall$ real adversary $A$ ideal adversary $\tilde{V}$ input, the output states are indistinguishable” as a security requirement, we only require “$\forall$ real adversary $A$ input $\tilde{V}$ ideal adversary, the outputs are indistinguishable.” This notion of security is closely related to notions of security considered in Refs. [13,15] and is further discussed in the Supplemental Material [17].

We will now give a formal definition of security. Following the notation of Ref. [15], we 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 $\hat{A}$, $\hat{B}$. The CPTP map corresponding to the protocol for honest Alice and dishonest Bob is denoted by $\pi_{AB}$. 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 $id_\rho \otimes \pi_{AB}(\rho_{UVR})$, where $\rho_{UVR}$ is a purification of $\sum_{u,v} p(u,v) |u\rangle |i_d\langle v| \otimes |v\rangle |\tilde{V}\rangle$.

Since we are faced with the task of the secure evaluation of a classical deterministic function, we consider an ideal functionality $F$ which measures the inputs in registers $\tilde{U}$ and $\tilde{V}$ and outputs orthogonal states in registers $\tilde{X}$ and $\tilde{Y}$ that correspond to the function values. Formally, $F([u]_\tilde{U}|v\rangle |\tilde{V}\rangle := \delta_{u,v} \delta_{\tilde{v},v}|f(u,v)\rangle |\tilde{X}\rangle |f(u,v)\rangle |\tilde{Y}\rangle$, where $\delta$ denotes the Kronecker delta function. When an ideal honest $\hat{A}$ and an ideal adversary $\hat{B}$ interact with the ideal functionality, we denote the joint map by $F_{\hat{A}\hat{B}}:U\tilde{V} \rightarrow X\tilde{Y}'$ (see Fig. 1). $\hat{A}$ just forwards the in- and outputs to and from the functionality, whereas $\hat{B}$ pre- and postprocesses them with CPTP maps $\Lambda^1_{\tilde{V} \rightarrow \tilde{y}K}$ and $\Lambda^2_{\tilde{X} \rightarrow \tilde{y}'K}$ resulting in a joint map $F_{\hat{A}\hat{B}} = [id_{\tilde{X} \rightarrow \tilde{y}K} \otimes \Lambda^2_{\tilde{X} \rightarrow \tilde{y}'K}] \circ [F_{\tilde{U} \rightarrow \tilde{X}\tilde{Y}} \otimes id_R] \circ [id_{U \rightarrow \tilde{y}} \otimes \Lambda^1_{\tilde{V} \rightarrow \tilde{y}K}]$, where $\circ$ denotes sequential application of CPTP maps.
We say that a (two-party quantum) protocol is secure against dishonest Alice is defined analogously.

Since \( F \) is classical, we can augment it so that it outputs \( \tilde{v} \) in addition. More precisely, we define \( \mathcal{F}_{\text{aug}}: U \rightarrow X Y \tilde{Y} \) by \( \mathcal{F}_{\text{aug}}(u) \tilde{v} \rangle = \delta_{u, v} \delta_{f(u, v)} \delta_{g(f(u, v), f(u, v))} \mathcal{F}(u, v) \), which has the property that \( \mathcal{F} = \mathcal{F}_{\tilde{v}} \circ \mathcal{F}_{\text{aug}} \). For a concrete input distribution we define \( \sigma_{RXXY} := [\rho_{UVR}] \otimes \mathcal{F}_{\text{aug}}(\rho_{UVR}) \) which satisfies \( \sigma_{RXXY} = \rho_{RXXY} \) for \( \rho_{RXXY} := [\rho_{UVR}] \). e-security against dishonesty is defined analogously.

**Main results.**—The proofs of our main results build upon the following lemma which constructs a cheating strategy for Alice that works on average over the input distribution \( p(u, v) \).

**Lemma.**—If a protocol \( \pi \) for the evaluation of \( f \) is \( \varepsilon \)-correct and \( \varepsilon \)-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 \( \sum_{u, v, \tilde{v}} p(u, v) q(\tilde{v} | u, v) \delta_{f(u, v), f(u, v)} \geq 1 - 6 \varepsilon \). Furthermore, \( q(\tilde{v} | u, v) \) is independent of \( u \); i.e., there exists a distribution \( \tilde{q}(\tilde{v} | v) \) such that \( \sum_{u} p(u, v) q(\tilde{v} | u, v) = \tilde{q}(\tilde{v} | v) \). The correctness of the protocol, this state is \( \varepsilon \)-close to

\[
\sum_{u, v, \tilde{v}} p(u, v) q(\tilde{v} | u, v) |u\rangle |v\rangle |\tilde{v}\rangle |f(u, v)\rangle |f(u, v)\rangle |X\rangle
\]

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

\[
\mathcal{M}_{RXXY} \otimes \mathcal{T}_{Y \rightarrow Y'} \mathcal{T}_{X \rightarrow X'} (|\Phi\rangle_{RXXY} |Y\rangle_{Y'}) = \varepsilon \mathcal{M}_{RXXY} \otimes \mathcal{T}_{Y \rightarrow Y'} (|\Phi\rangle_{RXXY} |Y\rangle_{Y'})
\]
Theorem 1.—If a protocol \( \pi \) for the evaluation of \( f \) is perfectly correct and perfectly secure (\( \varepsilon = 0 \)) against Bob, then, if Bob holds input \( v \), Alice can compute \( f(u, v) \) for all \( u \).

We note that this notion of insecurity implies that Alice can completely break the security for nontrivial functions \( f \).

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 \( q(\tilde{v}|u_0) \) which equals \( \tilde{q}(\tilde{v}|v) \). But since also \( q(\tilde{v}|u_0) = \tilde{q}(\tilde{v}|v) \) for all \( u \), we have \( \frac{1}{|\{u|v\}|} \sum_{u,v} p(\tilde{v}|u) q(\tilde{v}|u_0) = 1 \). 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 \( u \).

The impossibility result for the case of imperfect protocols is also based on the lemma but requires a subtle swap in the order of quantifiers (from “\( \forall \) input \( \exists \) ideal adversary” to “\( \exists \) ideal adversary \( \forall \) input”) which we achieve by use of von Neumann’s minimax theorem.

Theorem 2.—If a protocol \( \pi \) for the evaluation of \( f \) is \( \varepsilon \)-correct and \( \varepsilon \)-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 \( u \): \( P_{R_{\tilde{v}=Q}}[f(u, v) \neq f(u, \tilde{v})] \geq 1 - 2\varepsilon \).

Proof. The argument is inspired by Ref. [19]. For a finite set \( S \), we denote by \( \Delta(S) \) the simplex of probability distributions over \( S \). Denote by \( W \) the set of pairs \( (u, v) \). Consider a finite \( \varepsilon \)-net \( D \) of \( \Delta(W) \) in total variation distance and to each distribution in \( D \) the corresponding cheating unitary \( T \) constructed in the proof of the lemma. We collect all these unitaries in the (finite) set \( \tilde{E} \) and assume that \( T \) determines \( p \) uniquely, as we could include the value \( p \) into \( T \). For each such \( T \), let \( q(\tilde{v}|u, v, T) \) and \( \tilde{q}(\tilde{v}|v, T) \) be the distributions from the lemma. Define the payoff function \( g(u, v, T) := \sum_{u,v} q(\tilde{v}|u, v, T) \delta_{f(u, v), f(u, \tilde{v})} - \sum_{v} q(\tilde{v}|u, v, T) \delta_{f(u, v), f(u, \tilde{v})} \). The lemma then yields \( 1 - 2\varepsilon \leq \min_{p' \in D} \max_{T} \sum_{u,v} p'(u, v) g(u, v, T) \) which is at most \( 2\varepsilon + \min_{p' \in D} \max_{T} \sum_{u,v} p'(u, v) g(u, v, T) \), since replacing \( p \) by \( p' \) incurs only an overall change in the value by \( 2\varepsilon \) [as \( -1 \leq g(u, v, T) \leq 1 \)]. By von Neumann’s minimax theorem, this last term equals \( 2\varepsilon + \max_{p' \in D} \min_{T} \sum_{u,v} p'(u, v) g(u, v, T) \).

Hence, we have shown that there is a strategy for Alice, where she chooses her cheating unitary \( T \) with probability \( p'(T) \), such that (for some \( \varepsilon_1 + \varepsilon_2 \leq 14\varepsilon \)) for all \( u, v \),

\[
\sum_{T} Q(\tilde{v}|u, v) \delta_{f(u, v), f(u, \tilde{v})} \geq 1 - \varepsilon_1
\]
[20] In order to apply von Neumann’s theorem, note that the initial term equals \( \min_{\rho' \in \Delta(\mathcal{W})} \max_{\rho \in \Delta(\mathcal{E})} \sum_{u,v} p'(u, v) \times g(u, v, T) p''(T) \) since the maximal value of the latter is attained at an extreme point. Von Neumann’s minimax theorem [21] allows us to swap minimization and maximization leading to \( \max_{\rho \in \Delta(\mathcal{E})} \sum_{u,v,T} p(u, v) g(u, v, T) p''(T) \) without changing the value. This expression corresponds to the final term since the minimization can without loss of generality be restricted to its extreme points.