Complete insecurity of quantum protocols for classical two-party computation

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

DOI
10.1103/PhysRevLett.109.160501

Publication date
2012

Document Version
Final published version

Published in
Physical Review Letters

Citation for published version (APA):
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, Amsterdam, The Netherlands
2 Institute 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 nontrivial 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.
and only connected with a quantum channel, wish to
Likewise, every ideal adversary interacting with the ideal
classical and quantum protocols, respectively.
All these notions have in common that the execution of the
informal notion of the real–ideal-world paradigm precise.
concretely, a protocol is deemed secure if for every adver-
sarial strategy, or real adversary, there exists an ideal
security naturally embeds into a composable framework
approximately secure. We therefore follow the modern lit-
known as the real–ideal-world paradigm, has been firmly
A is honest. Whereas for simple functions this
possible to construct and prove secure more complicated
function. The same should be true if Alice is cheating
the execution of the
computing perfectly and securely and
of a function

\[ f(u, v) \]

which Alice and Bob, such an approach seems very compli-
called with the ideal functionality, and hence, it is
A \& B is honest. Whereas for simple functions this
intuitive notion of security can be made precise by stating
a list of security requirements for certain quantum states
in the center of attention for many years (cf., zero knowledge,
composability and where a suitable notion of security,
known as the real–ideal-world paradigm, has been firmly
In this paradigm, we first define an ideal situation in
where everything is computed perfectly and securely and
established.
In this paradigm, we first define an ideal situation in
which everything is computed perfectly and securely and
call this the ideal functionality. Informally, a two-party
functionality (which is a CPTP map itself). A desirable
notion of security is the following: for every real adversary
there exists an ideal adversary such that the corresponding
CPTP maps are (approximately) indistinguishable.
The natural measure of distinguishability of CPTP maps in
this context is the diamond norm, since it can be viewed
as the maximal bias of distinguishing real and ideal world
by supplying inputs to the CPTP maps and attempting to
distinguish the outputs by measurements (i.e., by interact-
ing with an environment). This rather strong notion of
security naturally embeds into a composable framework
for security in which also quantum key distribution can be
proven 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 environ-
ment to supply an arbitrary input state but only the purifi-
cation of a classical input (see definition of \( \rho_{UVR} \) below),
and second, we consider a different order of quantifiers:
instead of “\( \forall \) real adversary \( \exists \) ideal adversary \( \forall \) input,
the output states are indistinguishable” as a security require-
ment we only require “\( \forall \) real adversary \( \forall \) input \( \exists \) ideal
adversary, the outputs states are indistinguishable.” This
notion of security is closely related to notions of security
considered in Ref. [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
distribution \( p(u, v) \). The output state of the protocol,
augmented by the reference \( R \), takes the form \( \rho_{UVR} \), where \( \rho_{UVR} \) is a purification of
\[ \sum_{u,v} p(u, v) |u| U |v| V \].

Since we are faced with the task of the secure evalu-
ation of a classical deterministic function, we con-
sider an ideal functionality \( \mathcal{F} \) which measures the
inputs in registers \( U \) and \( V \) and outputs orthogonal
states in registers \( \hat{X} \) and \( \hat{Y} \) that correspond to the
function values. Formally, \( \mathcal{F}(|u|U|v|V) := \delta_{u,v} \delta_{f(v),f(u)} |f(u, v)\rangle \langle f(u, v)|_{\hat{Y}} \),
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 \( \mathcal{F}_{\hat{A}\hat{B}} : UV \rightarrow XY \) (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 \( \Lambda^1_{\hat{V}\rightarrow\hat{Y}K} \) and \( \Lambda^2_{\hat{X}\rightarrow\hat{Y}Y} \). resulting in a joint map \( \mathcal{F}_{\hat{A}\hat{B}} = (id_{XY} \otimes \Lambda^2_{\hat{X}\rightarrow\hat{Y}Y}) \circ (F_{\hat{B}\hat{V}\rightarrow\hat{X}\hat{Y}} \otimes id_{\hat{K}}) \circ (id_{U\rightarrow Y} \otimes \Lambda^1_{\hat{Y}\rightarrow\hat{K}}) \), where \( \circ \) denotes sequential application of
CPTP maps.
We say that a (two-party quantum) protocol \( C \) is \( \epsilon \)-secure if for any distribution \( p(u,v) \) of the inputs and any adversary \( A \) there exists a secure state \( \rho \) that satisfies

\[
\sum_{u,v} |\langle i|_u \langle v|_v \rangle \rangle_{i} \rho \geq 1 - \epsilon.
\]

We say that a (two-party quantum) protocol \( \pi \) is \( \epsilon \)-correct if for any distribution \( p(u,v) \) of the inputs and any adversary \( A \) there exists a secure state \( \rho \) that satisfies

\[
\sum_{u,v} |\langle i|_u \langle v|_v \rangle \rangle_{i} \rho \geq 1 - \epsilon.
\]

The following lemma describes 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 \( \epsilon \)-correct and \( \epsilon \)-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 \( \sum_{u,v} q(\tilde{v}|u,v) \geq 1 - \epsilon \).

**Proof.**—We first construct a “cheating unitary” \( T \) for Alice and then show how Alice can use it to cheat successfully.

Let Alice and Bob play honestly, but let them purify their protocol with purifying registers \( X' \) and \( Y' \), 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 \( |\Phi|_{RX'Y'X'Y'} \) the state of all registers at the end of the protocol. Notice that tracing out \( X'_1 \) from \( |\Phi|_{RX'Y'X'Y'} \) results in a state \( \text{tr}_{X'_1} |\Phi|_{RX'Y'X'Y'} = \rho_{RX'Y'} \) 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 \( Y'_1 Y' \). Since the protocol is \( \epsilon \)-secure against Bob by assumption, there exists a secure state \( \sigma_{RX'Y'} \) satisfying \( \sigma_{RX'Y'} = \epsilon \rho_{RX'Y'} \).

Let \( |\Psi|_{RX'Y'Y'} \) be a purification of \( \sigma_{RX'Y'} \) with purifying register \( P \). Note that \( |\Psi|_{RX'Y'Y'} \) is also a purification of \( \sigma_{RX'Y'} \), this time with purifying registers \( PV \). Recall that \( |\Phi|_{RX'Y'} \) purifies \( \rho_{RX'Y'} \) with purifying register \( X'_1 \). Since \( \sigma_{RX'Y'} = \epsilon \rho_{RX'Y'} \) we can use Uhlmann’s theorem [18] to conclude that there exists an isometry \( T = T_{X'_1 \rightarrow PV} \) (with induced CPTP map \( T = T_{X'_1 \rightarrow PV} \)) such that

\[
[T_{X'_1 \rightarrow PV} \otimes \text{id}_{RX'Y'}]|\Phi|_{RX'Y'X'Y'} = |\Psi|_{RX'Y'Y'}.
\]

We will now show how Alice can use \( T \) to cheat. Notice that tracing out \( Y'_1 \) from \( |\Phi|_{RX'Y'X'Y'} \) 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 \( T_{X'_1 \rightarrow PV} \), measures register \( V \) 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 \( V \).

Let \( M_{RX'Y'} \) be the CPTP map that measures registers \( R \), \( X' \), and \( Y' \) in the computational basis. Tracing over \( PV \) and applying \( M_{RX'Y'} \) on both sides of Eq. (1), we find

\[
[M_{RX'Y'} \otimes \text{id}_{PY'}][(T_{X'_1 \rightarrow PV} \otimes \text{id}_{RX'Y'})(|\Phi|_{RX'Y'X'Y'})] = \epsilon [\rho_{RX'Y'} \otimes \text{id}_{PY'}](|\Psi|_{RX'Y'Y'})
\]

by the monotonicity of the purified distance under CPTP maps. The right-hand side of Eq. (2) equals

\[
\sum_{x' \in X', y' \in Y'} p(u,v,q(\tilde{v}|u,v)) q(\tilde{v}|u,v) |\langle i|_{x'} \langle y'|_y \rangle \rangle_{i} \rho_{X'Y'} \]

which is conditioned on Bob’s input \( v \), since \( |\Psi|_{RX'Y'Y'} \) is a purification of the secure state \( \sigma_{RX'Y'} \). The left-hand side of Eq. (2) equals

\[
\sum_{x', y'} p(u,v,q(\tilde{v}|u,v)) q(\tilde{v}|u,v) |\langle i|_{x'} \langle y'_1|_y \rangle \rangle_{i} \rho_{X'Y'} \]

for some conditional probability distributions \( q(\tilde{v}|u,v) \) and \( r(x'|u,v) \). Because of the correctness of the protocol, this state is \( \epsilon \)-close to

\[
\sum_{u,v,\tilde{v}} p(u,v,q(\tilde{v}|u,v)) q(\tilde{v}|u,v) |\langle i|_{x'} \langle y'_1|_y \rangle \rangle_{i} f(u,v) = f(u,v) |\langle i|_{x'} \rangle \rangle_{i} X
\]

for some conditional probability distribution \( q(\tilde{v}|u,v) \). Noting that therefore also \( p(\cdot,\cdot)q(\cdot,\cdot) \) and \( p(\cdot,\cdot)q(\cdot,\cdot) \) (when interpreted as quantum states) are \( \epsilon \)-close in purified distance, we can replace \( p(\cdot,\cdot)q(\cdot,\cdot) \) in Eq. (3) by \( p(\cdot,\cdot)q(\cdot,\cdot) \) increasing the purified distance to the left-hand side of Eq. (2) only to \( 2\epsilon \). Putting things together, Eq. (2) implies
Consider a finite set $S$ assume that $T$ results in the statement that if Alice has input $u$, $v$ defined by use of von Neumann’s minimax theorem. The argument is inspired by Ref. [19]. For a protocol $\pi$ for the evaluation of $f$ is perfectly correct and perfectly secure ($\epsilon = 0$) 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 $\epsilon = 0$ in the lemma results in the statement that if Alice has input $u_0$, then she will obtain $v$ from the distribution $q(v|u_0, v)$ which equals $\frac{1}{|U|}\sum_{u,v}q(v|u_0, v)$ for all $u$, we have $\frac{1}{|U|}\sum_{u,v}q(v|u_0, v) = 1$. In other words, all $v$ that occur (i.e., that have $q(v|u_0, v) > 0$) satisfy for all $u$, $f(u, v) = f(u, v)$. 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 $T$ 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 $\epsilon$-correct and $\epsilon$-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 $v$ distributed according to some distribution $Q(v|u_0, v)$ such that for all $u$: $Pr_0 - Q(f(u, v) = f(u, v)) \geq 1 - 2\epsilon$.

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 $\epsilon$-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 $E$ and assume that $T$ determines $p$ uniquely, as we could include the value $p$ into $T$. For each such $T$, let $q(v|u, v, T)$ and $\tilde{q}(v|u, v, T)$ be the distributions from the lemma. Define the payoff function $g(u, v, T) := \sum_{v}q(v|u, v, T)\delta_{f(u, v), f(u, v)} - \sum_{v}\tilde{q}(v|u, v, T)\delta_{f(u, v), f(u, v)}$. The lemma then yields $1 - 12\epsilon \leq \min_{T}\max_{u,v}Pr_{u|\epsilon}(g(u, v, T) \leq g(u, v, T)) \geq 1 - 2\epsilon$.

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 $\epsilon_1 + \epsilon_2 \leq 2\epsilon$) for all $u, v$, the value by $2\epsilon$ as $-1 \leq g(u, v, T) \leq 1$. By von Neumann’s minimax theorem, this last term equals $2\epsilon + \max_{p'\in\Delta(S)}\min_{u,v}E_{u,v}p(g(u, v, T)p''(T)[20].$

One might wonder whether Theorem 2 can be strengthened to obtain, with probability $1 - O(\epsilon)$, a $\tilde{v}$ such that for all $u, v$: $f(u, v) = f(u, \tilde{v})$. It turns out that this depends on the function $f$: when $f$ is equality EQ$(u, v)$ $= 1$ if $u = v$ and inner product $IP(u, v) = \sum_{i}u_iv_i$ mod2, the stronger conclusion is possible. However, for disjointness [DISJ$(u, v)$ $= 0$] such 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 $\sum_{v}Q(v|u_0, v)\delta_{EQ(u, v), EQ(u, v)} \geq 1 - 2\epsilon$. Since $\delta_{EQ(u, v), EQ(u, v)} = 1$ if $v = \tilde{v}$, we find $Q(v|u_0, v) \geq 1 - 2\epsilon$. When $f$ is IP, we pick $u$ uniform at random and obtain $\sum_{v}Q(v|u_0, v)(2^{-n}\sum_{v}\delta_{IP(u, v), IP(u, v)}\geq 1 - 2\epsilon$. Using $2^{-n}\sum_{v}\delta_{IP(u, v), IP(u, v)} = 1$ if $v = \tilde{v}$, and $\frac{1}{2}$ if $\tilde{v} \neq v$, we find $Q(v|u_0, v) \geq 1 - 2\epsilon$, which implies $Q(v|u_0, v) \geq 1 - 56\epsilon$. Interestingly, for DISJ such an argument is not possible. Assume that we have a protocol that is $\epsilon$-secure against Bob. Bob could now run the protocol normally on strings $v$ with Hamming weight $|v| \leq n/2$, but on inputs $v$ with $|v| > n/2$ he could flip, at random, $\sqrt{n}$ of $v$’s bits that are 1. It is not hard to see that this new protocol is still $\epsilon$-secure and $\epsilon + O(\frac{1}{\sqrt{n}})$-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 or leak the complete input $v$ to Alice, simply because Bob does not use it.

We thank Ivan Damgård, Frédéric Dupuis, Louis Salvail, Christopher Portmann, and Renato Renner for valuable discussions and an anonymous referee for suggesting an example presented in the Supplemental Material. M. C. is supported by the Swiss National Science Foundation (Grants No. PPOOP2_128455 and No. 20CH21_138799), the NCCR “Quantum Science and Technology,” and the German Science Foundation (Grant No. CH 843/2-1). C. S. is supported by an NWO Veni grant. H. B. was supported by an NWO vici grant and by EU project QCS.
[20] In order to apply von Neumann’s theorem, note that the initial term equals \(\max_{p' \in \Delta(\mathcal{W})} \sum_{u,v} p'(u, v) \times g(u, v, T) p''(T)\) 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 \(\max_{p' \in \Delta(\mathcal{W})} \sum_{u,v,T} p'(u, v, T) p''(T)\) 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.