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: November 16, 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 work 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.

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 [2, 3], 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 [4, 5]. Interestingly, however, a weak version of a coin toss can be implemented by quantum mechanical means [6].

In this article 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 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 [7]. In a similar way, we complement a result by Salvail, Schaffner and Sotáková [8] 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) [9]. 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 (nor perfectly correct). More precisely, if the protocol is secure up to a small error against cheating Bob, then Alice is

---

* The full version of this paper appeared in PRL and can be found on the arxiv [1].

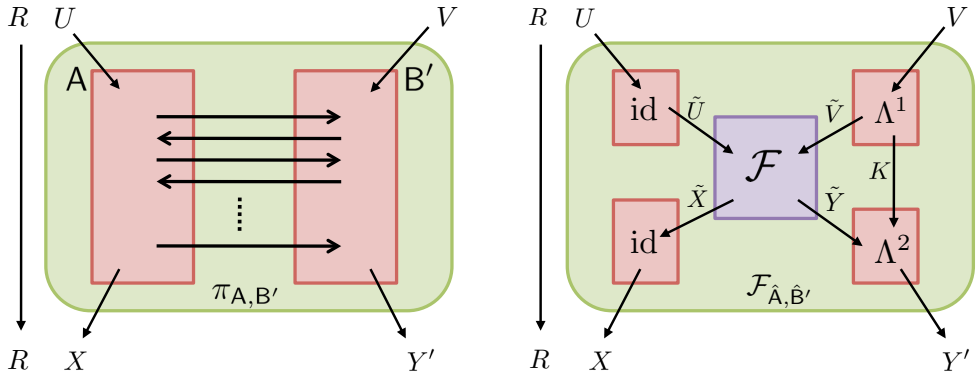

FIG. 1: Illustration of the security definition. A protocol is secure against dishonest Bob, if the *real protocol* (left) can be simulated as an interaction with the *ideal functionality* $\mathcal{F}$ (right).

able to compute the value of the function for all of her inputs with only a small error. Since the error is independent of the number of inputs that both Alice and Bob have, our analysis improves over Lo's result in the one-sided case. In fact, our results apply to this case since, more generally, they remain true should Bob receive the output of a function g, different from Alice's f, as a careful look at our argument reveals.

Following the real/ideal-world paradigm of modern cryptography, we first define an ideal situation in which everything is computed perfectly and securely and call this the *ideal functionality*. Informally, a two-party protocol is secure if it looks to the outside world just like the ideal functionality it is supposed to implement. More concretely, a protocol is deemed secure if for every adversarial strategy, or *real adversary*, there exists an *ideal adversary* interacting only with the ideal functionality such that the execution of the protocol in the real world is *indistinguishable* from this ideal world. If such a security guarantee holds, it is 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. See [10–12] and [13–16] for further information about this concept of security in the context of classical and quantum protocols, respectively.

There exist different meaningful ways to make the above informal notion of the real/ideal-world paradigm precise. All these notions have in common that the execution of the protocol by the honest and dishonest players is modeled by a completely positive trace preserving (CPTP) map. Likewise, every ideal adversary interacting with the ideal functionality is composed out of CPTP maps modeling the pre- and postprocessing of the in- and outputs to the ideal 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 interacting 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.

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 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 requirement 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 [14, 16].

Since we are faced with the task of the secure evaluation of a *classical* deterministic function, we consider an ideal functionality which measures the inputs it receives and outputs orthogonal states to the parties that correspond to the function values. Note that in certain situations one may be satisfied with different (possibly weaker) ideal functionalities for this task; we leave open the question to what extend our results remain valid in such situations.

Figure 1 gives an illustration of the security definition against dishonest Bob using the real/ideal-paradigm. The formal definition of security can be found in [1].

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 $p(u, v)$ for a protocol that is ε-secure against Bob. The proof can be found in [1].

Lemma. *If a protocol π for the evaluation of f is ε-correct and 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 $\sum_{u,v,\tilde{v}} p(u,v)|q(\tilde{v}|u,v)-\tilde{q}(\tilde{v}|v)| \leq 6\varepsilon$.*

Applying the lemma to the case $\varepsilon = 0$ with a uniform input distribution we immediately obtain the impossibility result for perfectly secure protocols.

Theorem 1. *Let π be a protocol for the evaluation of f which is perfectly correct and perfectly secure ($\varepsilon = 0$) against Bob. Then, if Bob has 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 non-trivial functions f. In order to conclude the impossibility also for approximately secure protocols we need to use the lemma for arbitrary input distributions. Note that the lemma guarantees that for every joint input distribution, there exists a successful cheating strategy for Alice. In order to conclude from this that there exists a cheating strategy for Alice that works for *all* inputs, we need to swap the order of quantifiers which we do with help of von Neumann's minimax theorem. Note that the resulting strategy is then randomised. For details see [1].

Theorem 2. *If a protocol π for the evaluation of f is ε-correct and 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: $\Pr_{\tilde{v}\sim Q}[f(u,v) = f(u,\tilde{v})] \geq 1-28\varepsilon$.*

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 ($\mathrm{EQ}(u,v) = 1$ iff $u = v$) and inner-product ($\mathrm{IP}(u,v) = \sum_i u_i \cdot v_i \mod 2$), the stronger conclusion is possible. However for disjointness ($\mathrm{DISJ}(u,v) = 0$ iff $\exists i : u_i = v_i = 1$) such a strengthening is not possible showing that our result is tight in general. Since this work presents impossibility results for the secure computation of f, one may wonder how the results are affected when (possibly) weaker notions of security, more akin to the ones used in the well-known no-go proofs for bit commitment and one-sided computation, are used. Whereas we do not know the answer to this question in general, we wish to emphasize the difficulty in formalizing such notions of security satisfactorily. With respect to our notion of security one may wonder if one could not omit the purification of the inputs. Note that such an omission would correspond to a serious limitation of the environment to distinguish the real and from the ideal world. With respect to the stronger notion of security discussed above, for instance, there can be a large difference between the diamond norm (which corresponds to purified inputs) and the induced norm (where the maximisation is over inputs that are not purified) (see e.g. [17]). This difference does not occur in the case of perfectly secure protocols, where one can therefore omit the reference. The omission of the reference has a more serious effect on the weaker notion of security considered here, even in the case of perfect security, since we only consider (purified) classical inputs; in fact, omission would invalidate the no-go result (see Appendix of full version). We leave it as an open question whether Theorem 1 can be proven were arbitrary (unpurified) inputs considered.

[1] H. Buhrman, M. Christandl, and C. Schaffner, Phys. Rev. Lett. **109**, 160501 (2012), URL `http://link.aps.org/doi/10.1103/PhysRevLett.109.160501`.

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

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

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

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

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

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

[8] 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.

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

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

[11] R. Canetti, Ph.D. thesis, The Weizmann Institute of Science (1996).

[12] O. Goldreich, *Foundations of Cryptography*, vol. II: Basic Applications (Cambridge University Press, 2004).

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

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

[15] M. Ben-Or and D. Mayers (2004), arXiv:quant-ph/0409062.
[16] S. Fehr and C. Schaffner, in *Theory of Cryptography Conference (TCC)* (Springer, 2009), vol. 5444, pp. 350–367.
[17] G. M. D'Ariano, D. Kretschmann, D. Schlingemann, and R. F. Werner, Phys. Rev. A **76**, 032328 (2007).