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

Complete Insecurity of Quantum Protocols for Classical Two-Party Computation: Supplemental Information on the Security Definition

Harry Buhrman, Matthias Christandl, and Christian Schaffner

Since this work presents impossibility results for the secure computation of f, one may wonder how the results are affected when the notions of security are weakened. In particular, one may ask whether similar results can be obtained when, instead of the real/ideal-world paradigm, notions of security more akin to the ones used in the well-known no-go proofs for bit commitment and one-sided computation would be 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 regards to the real/ideal-world paradigm we will now comment on some specific notions of security used in this work. A central object in the real/ideal-world paradigm is the ideal functionality. Since we are faced with the task of the secure evaluation of a *classical* deterministic function, we chose to 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.

One may also wonder if the purification of the inputs could not be omitted. 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 in the main text, 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) 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 in this work, even in the case of perfect security, since we only consider (purified) classical inputs; in fact, omission would invalidate the no-go result as we will now show. We leave it as an open question whether Theorem 2 can be proven were arbitrary (unpurified) inputs considered.

The following example was suggested to us by an anonymous referee and shows the necessity of requiring the register R in our security definition. Consider the classical deterministic function $f((s_0, s_1), b) = (b, s_b)$ of n-bit strings s_0, s_1 and a choice bit b which is inspired by a one-out-of-two-string-oblivious transfer but outputs both the choice bit and the string of choice to both Alice and Bob. Let us consider the following protocol $\pi_{\mathsf{A},\mathsf{B}}$: Bob sends b to Alice and Alice responds with s_b.

Clearly, this protocol is secure against cheating Bob, who learns no more than either s_0 or s_1. One might also think that this protocol is perfectly secure against cheating Alice because Alice learns Bob's choice bit anyway. Indeed, if we defined security without purifying register R one could construct an ideal adversary Alice $\hat{\mathsf{A}}'$ from any real adversary A' as follows. Let $\hat{\mathsf{A}}'$ simulate two independent copies of A' and give $b = 0$ to the first and $b = 1$ to the second copy which both respond with a string s_0 and s_1, respectively. Let $\hat{\mathsf{A}}'$ input these two strings (s_0, s_1) into the ideal functionality $\mathcal{F}$ and receive (b, s_b) as output from $\mathcal{F}$. Output whatever the real copy of A' corresponding to the bit b outputs (and discard the other copy). This simulation generates an output in the ideal world which is identically distributed to the one from the real protocol. Hence, the protocol would be perfectly secure against Alice. Notice that this example shows that an analogue of our Theorem 1 cannot be proven for this weaker security definition.

We stress that the above protocol is *not* secure according to our security definition by virtue of the purifying register R. Consider the uniform input distribution over n-bit strings (s_0, s_1) in the $2n$-qubit register U and the choice bit b in register V. Hence, the input state ρ_{RUV} if fully entangled between R and UV. Let us consider the following real adversary A' who measures the first n qubits of U in the computational basis in case $b = 0$ or performs the measurement in the Hadamard basis if $b = 1$ and returns the measurement outcome as s_b. Due to the entanglement, the first n qubits of R collapse to the measured state. Notice that for this adversary A', the argument above is no longer applicable, because $\hat{\mathsf{A}}'$ cannot simulate two independent copies of A' as the U register is only available once. In fact, for this adversarial strategy A', only one of the two strings s_0, s_1 is well-defined as the other string corresponds to the measurement outcome in a complementary basis of the same quantum state. This highlights the intuitive security problem of the suggested protocol, namely that it is not guaranteed that both s_0 and s_1 classically exist for a cheating Alice. This shows that the protocol is not secure against cheating Alice and that it therefore does not stand in contradiction with our results.