A Paradox of Quantum Universal Composability

D. Hofheinz[†] and J. Müller-Quade[†]

1 Introduction

Security of cryptographic protocols under composition is a major concern in cryptography. For classical cryptography Canetti gave a definition of security implying *universal composability* [Can01]. A protocol proven secure in that sense may replace *ideal functionalities* in arbitrary applications preserving the overall security of the application.

In this contribution we sketch the modifications necessary to the work of Canetti to obtain *quantum universal composability* (cf. [BOM02]). We show that the bit commitment protocol described in [BB84] can be binding and concealing relative to a strong physical assumption, but it cannot be quantum universally composable. If a bit commitment is given as a primitive, one can use the protocol of [Yao95] to obtain the strong primitive *oblivious transfer*. We show that the use of a universally composable bit commitment in this construction yields a quantum universally composable oblivious transfer.

Finally we show a paradoxical situation where an intuitive improvement in security causes a protocol to lose the property of quantum universal composability. This "paradox" proves that the notion of universal composability does not yet reflect all aspects of the intuition of security.

2 Preliminaries

The general modeling [Can01] of Multi-Party-Computation defines a simulatability-based notion of security: runs of a given protocol π along with a strong, so-called *real-model adversary* $\mathcal{A}$ are compared with runs of an idealization $\mathcal{F}$ of the functionality which π is to provide. Together with $\mathcal{F}$ runs a very limited *ideal-model adversary* (also called *simulator*) $\mathcal{S}$ which is to mimick attacks carried out by $\mathcal{A}$ on π.

Protocol π is said to *securely realize* the ideal functionality $\mathcal{F}$ if for every real-model adversary $\mathcal{A}$ there exists a simulator $\mathcal{S}$ so that no environment $\mathcal{Z}$ can distinguish running with $\mathcal{A}$ and parties executing π from running with $\mathcal{S}$ and $\mathcal{F}$. $\mathcal{Z}$ is to represent arbitrary protocol environments in which π is executed, possibly as a sub-protocol; therefore, $\mathcal{Z}$ may write input to parties and read their outputs as well as communicate with the respective adversary.

Security in the sense of [Can01] implies *universal composability* (UC): assume that protocol τ securely realizes functionality $\mathcal{G}$ by means of using instances of another ideal functionality $\mathcal{F}$ as subroutines. Then τ still realizes $\mathcal{G}$ when these $\mathcal{F}$-instances are substituted by executions of any protocol π which securely realizes $\mathcal{F}$. Thus, when the reference to $\mathcal{F}$ is clear, a protocol which securely realizes $\mathcal{F}$ is said to be *universally composable*.

3 Quantum UC

In [Can01], the environment, all parties and adversaries are modeled as (classical) *interactive Turing machines* (ITMs, cf. [Can01]). We consider protocol runs with modified ITMs which are *classical* w. r. t. input, output and transition function, yet allow for quantum inter-party communication and are able to store qubits and perform measurements on these as well as evaluate quantum gates. More specifically, say that a *Quantum ITM* (QITM) is an ITM which has additionally an *incoming quantum communication tape* and an *outgoing quantum communication tape*, each cell containing one qubit along with classically encoded sender, resp. receiver, per cell. These tapes may be used to send quantum messages to and receive quantum messages from other QITMs. Furthermore, a QITM has a *quantum work tape* on which measurements and quantum gate evaluations may be performed. The (classical) descriptions for these measurements and gates must be supplied by the QITM on its classical work tape. Quantum bits may be copied freely between the three quantum tapes of the QITM.

When substituting all ITMs by QITMs, we call the resulting security definition of [Can01]

[†] IAKS, Arbeitsgruppe Systemsicherheit, Prof. Dr. Th. Beth, Fakultät für Informatik, Universität Karlsruhe, Am Fasanengarten 5, 76 131 Karlsruhe, Germany

quantum universal composability. Note that input and output of a QITM (in particular $\mathcal{Z}$'s output) are still classical. The crucial *composition theorem* sketched above still holds in this modified setting. The proof given in [Can01] simply carries over; note that there is a canonical quantum analog to the *dummy adversary* of [Can01], which is *complete* in the sense that for showing security, it suffices to find a simulator mimicking attacks mounted by the dummy adversary in the real model.

4 The Relay Attack

In [BB84], a bit commitment scheme (for the purpose of coin tossing) is described which is binding and concealing relative to the security assumption that no quantum memory is available. We prove that this commitment scheme is not universally composable by extending an attack of [CF01] to the quantum setting.

Interestingly the above bit commitment has a different property which is necessary for universal composability, namely the equivocability in the ideal model. This equivocability, which allows the simulator to fake a run of a real protocol without knowing the contents of the ideal commitment, can be obtained by the cheating strategy of Mayers and Lo/Chau. But to employ this strategy the simulator has to store qubits and maintain entanglement and would hence not be subject to the same restriction as the real adversary (see below for a discussion).

5 Oblivious Transfer from Bit Commitment and a Paradox

Given a protocol for bit commitment, it is possible to derive a protocol for oblivious transfer [Yao95]. We prove that this construction yields a quantum universally composable oblivious transfer if the bit commitment used is universally composable. To be able to mimick real attacks the simulator has to be able to store quantum information. This leads to the paradoxical situation which we discuss as a hot topic here.

There are two properties which a notion of security should intuitively satisfy: (a) every restriction imposed on the real adversary should hold for the ideal adversary (simulator), too, and (b) an additional security assumption (restriction on the adversary) cannot make a protocol insecure. The first point lies at the heart of the intuition behind simulation based notions of security. Every ability of the simulator reflects a (trivial) attack which can in principle not be avoided. Thus every additional ability of the simulator can cover up security leaks. Therefore the abilities of the simulator are assumed to be a subset of the abilities of the real adversary. The second point is intuitively clear as an additional restriction should not increase the number of possible attacks.

We prove that for a simulation based notion of security point (a) and point (b) cannot both be valid. In the proof of security for the construction of [Yao95] the simulator has to be able to store quantum information. We present an attack which allows to distinguish between the real and the ideal model if the simulator cannot store quantum information. If we impose the additional security assumption that no quantum memory is available no proof of security is possible any more.

So either we have to sometimes give abilities to the simulator the real adversary does not have or we have to accept a notion of security where an improvement in (intuitive) security can make a protocol insecure. A paradoxical situation.

Acknowledgments

This research was partially funded by the project ProSecCo of the IST-FET programme of the EC.

References

[BB84] C. H. Bennett and G. Brassard. Quantum cryptography: Public key distribution and coin tossing. Proceedings of IEEE International Conference on Computers, Systems and Signal Processing. Bangalore, India, 1984.

[BOM02] M. Ben-Or and D. Mayers. Quantum universal composability. talk given at the workshop *Quantum Computation*, December 2002. The slides are available through http://www.msri.org/.

[Can01] Ran Canetti. Universally Composable Security: A New Paradigm for Cryptographic Protocols. In *FOCS 2001, Proceedings*, pages 136–145. IEEE Computer Society, 2001. Full version at `http://eprint.iacr.org/2000/067`.

[CF01] Ran Canetti and Marc Fischlin. Universally Composable Commitments. In Joe Kilian, editor, *CRYPTO 2001, Proceedings*, volume 2139 of *Lecture Notes in Computer Science*, pages 19–40. Springer, 2001. Full version at `http://eprint.iacr.org/2001/055`.

[Yao95] A. Yao. Security of quantum protocols against coherent measurements. In *Procedings of the 27th Symposium on the Theory of Computing*, pages 67–75. ACM, Las Vegas, June 1995.