Cryptography in a quantum world
Wehner, S.D.C.

Citation for published version (APA):

General rights
It is not permitted to download or to forward/distribute the text or part of it without the consent of the author(s) and/or copyright holder(s), other than for strictly personal, individual use, unless the work is under an open content license (like Creative Commons).

Disclaimer/Complaints regulations
If you believe that digital publication of certain material infringes any of your rights or (privacy) interests, please let the Library know, stating your reasons. In case of a legitimate complaint, the Library will make the material inaccessible and/or remove it from the website. Please Ask the Library: http://uba.uva.nl/en/contact, or a letter to: Library of the University of Amsterdam, Secretariat, Singel 425, 1012 WP Amsterdam, The Netherlands. You will be contacted as soon as possible.
Quantum computing had a profound impact on cryptography. Shor’s discovery of an efficient quantum algorithm for factoring large integers implies that nearly all existing classical systems based on computational assumptions can be broken, once a quantum computer is built. It is therefore imperative to find other means of implementing secure protocols. This thesis aims to contribute to the understanding of both the physical limitations, as well as the possibilities of cryptography in the quantum setting. To this end, we first investigate two notions that are crucial to the security of quantum protocols: uncertainty relations and entanglement. How can we find good uncertainty relations for a large number of measurement settings? How does the presence of entanglement affect classical protocols? And, what limitations does it impose on implementing quantum protocols? Finally, can we circumvent some of those limitations using realistic assumptions?

Information in Quantum States

In this part, we start by investigating how to extract information from quantum states. One of the most basic tasks is the discrimination of quantum states. Given an ensemble of known quantum states, which one do we hold in our hands? We study a variant of this problem which is of central importance for the security of protocols in the bounded-quantum-storage model. Here, we are given additional information about the state after the measurement or, more generally, after a quantum memory bound is applied. We prove general bounds on the success probability which answer in the negative the question whether deterministic privacy amplification is possible in all known protocols in the bounded-quantum-storage model. To this end, we introduce a general algebraic framework which allows us to solve this problem for any set of states and provide two explicit examples.
We then turn to examine entropic uncertainty relations, which are an alternative way to state Heisenberg's uncertainty principle. They are frequently a more useful characterization, because the “uncertainty” is lower bounded by a quantity that does not depend on the state to be measured. Recently, entropic uncertainty relations have gained importance in the context of quantum cryptography in the bounded-storage model, where proving the security of protocols ultimately reduces to bounding such relations. Proving new entropic uncertainty relations could thus give rise to new protocols. Such relations are known for two or $d + 1$ mutually unbiased measurements. We prove tight entropic uncertainty relations for measurements in a large number of specific mutually unbiased bases (MUBs) in square dimensions. In a similar way, we show that such MUBs are unsuitable for locking classical correlations in quantum states: Using 2 or all of them does not increase the locking effect.

Our result shows that one needs to be careful about thinking of “maximally incompatible” measurements as being necessarily mutually unbiased. But what properties do measurements need to have in order to give strong uncertainty relations? We find very strong uncertainty relations from the generators of a Clifford algebra. In particular, we prove that for $k$ such anti-commuting observables $X_1, \ldots, X_k$ we obtain optimal uncertainty relations for the Shannon entropy and nearly optimal relations for the collision entropy. Our results have immediate applications to quantum cryptography in the bounded-storage model.

**Entanglement**

In this part, we investigate the intriguing notion of quantum entanglement. We demonstrate how to find the optimal quantum strategies for correlation inequalities where each measurement has exactly two outcomes using semidefinite programming. As an example, we prove a tight upper bound for a well-known generalized CHSH inequality.

Furthermore, we consider how a classical two-prover interactive proof system changes if the provers are allowed to share entanglement. In this setting, a polynomial time bounded verifier is allowed to ask questions to two unbounded provers, who are trying to convince the verifier of the validity of a specific statement, even if the statement is false. The provers may thereby agree on any strategy ahead of time, but can no longer communicate once the protocol starts. Surprisingly, it turns out that, when the provers are allowed to share entanglement, it is possible to simulate two such classical provers using a single quantum prover. This indicates that entanglement among provers truly weakens the proof system, and provides an example of how classical systems can be affected, even if we only allow a very limited set of quantum operations.
Applications to Cryptography

In this part, we consider the consequences of uncertainty relations and entanglement in quantum systems to cryptography. Traditional cryptography is concerned with the secure and reliable transmission of messages. With the advent of widespread electronic communication and the internet, however, new cryptographic tasks have become increasingly important. We would like to construct secure protocols for electronic voting, online auctions, contract signing and many other applications where the protocol participants themselves do not trust each other. The main focus is on two primitives, which form an important building block for constructing multi-party protocols: bit commitment and oblivious transfer. Classical protocols for such problems are usually based on computational assumptions which do not stand up to a quantum computer. Unfortunately, it has been shown that even quantum computers do not help in this case and that perfect quantum bit commitment and oblivious transfer are impossible. In the face of such negative statements, what can we still hope to achieve?

Given that perfect bit commitment is impossible, perhaps we can alter the task slightly and obtain useful protocols? Here, we considered commitments to an entire string of bits at once, when the attacker has unbounded resources at his disposal. Evidently, if perfect bit commitment is impossible, perfect string commitment is also impossible as well. However, we showed that we can obtain non-trivial quantum protocols, where the participants have a small ability to cheat. To this end, we introduced a framework for the classification of string commitment protocols. In particular, we proved that the measure of information is crucial to the security: For a very strong notion of security, we showed that even slightly imperfect quantum string commitments are also impossible. Nevertheless, we showed that for a weaker measure of information we can indeed obtain nontrivial protocols, which are impossible in a classical world.

Luckily, it turns out that we can implement oblivious transfer if we are willing to assume that storing qubits is noisy. We introduce the model of noisy quantum storage, which is similar to the model of bounded quantum storage. Here, however, we consider an explicit noise model inspired by present day technology. If the honest parties can perform perfect quantum operations, then we show that the protocol is secure for any amount of noise. In case the honest participants are only able to perform noisy operations themselves, we analyze a practical protocol that can be implemented using present-day hardware. We show how to derive explicit tradeoffs between the amount of storage noise, the amount of noise in the operations performed by the honest participants and the security of the protocol. Here, the very problem that makes it so hard to implement a quantum computer can actually be turned to our advantage.