Diss. ETH No. 20342

Classical and Quantum Secure Two-Party Computation

A dissertation submitted to

ETH ZURICH

for the degree of
Doctor of Sciences

presented by

SEVERIN WINKLER
MSc in Computer Science, ETH Zurich

born May 5, 1975
citizen of Adliswil, ZH, Switzerland

accepted on the recommendation of

Prof. Dr. Stefan Wolf, examiner
Prof. Dr. Ivan Damgård, co-examiner
Prof. Dr. Renato Renner, co-examiner

2012

Abstract

Given a classical communication channel only, it is impossible for two parties to perform an arbitrary joint computation on their respective inputs in such a way that a computationally unbounded player cannot learn more than what he can derive from his own input and the output of the computation. While quantum information is in general fundamentally different from classical information, it seems not more powerful in this context: Even if the parties can communicate over a quantum channel, this task cannot be solved without restricting the computational power of the parties. However, there is a solution once the two parties share a black-box which computes a certain function of the two inputs of the players and gives the outcome to one of them. A simple example of such a function, which allows the two parties to perform any joint computation securely, is *oblivious transfer*. In the first part of this thesis, we study the possibility and efficiency of such computations. In particular, we provide lower bounds on the number of invocations of oblivious transfer that are needed to securely compute a general function.

A *bit commitment* protocol consists of two phases, where after the first phase the sender is committed to a bit. The protocol is secure if the value of the bit is fixed and cannot be changed, while the receiver still has no information about the value of the bit. At a later time, the players may execute the second phase, where the bit is revealed to the receiver. It is known that there is no information-theoretically secure bit commitment protocol if the two parties can only use a communication channel - even if the communication is quantum. In the second part of this thesis, we study two-party protocols that implement bit commitments from trusted correlated randomness that is pre-distributed to the parties. We consider protocols that implement many bit commitments at the same time and show that the entropy and, therefore, also the number of the random bits that is needed per bit commitment grows linearly with the statistical secu-

rity parameter. This result is in contrast to known results for implementations of oblivious transfer that only use a constant number of instances of certain distributed correlations per instance if a large number of instances is realized at once.

While quantum communication allows two parties to establish a secret key that remains unknown to any computationally unbounded eavesdropper, neither bit commitment nor oblivious transfer can be realized from quantum communication. However, establishing a secret key is only possible if the two parties already share a short secret key initially. In the third part of this thesis, we ask whether similar quantum protocols could exist that *extend* commitments in the sense that a commitment to a large string can be securely realized from a smaller number of bit commitments. We answer this question in the negative. Next, we show that quantum protocols that implement oblivious transfer from trusted distributed randomness can violate our impossibility results for classical protocols. However, we prove lower bounds on the entropy of the distributed randomness that is needed by such protocols, which show in particular that also oblivious transfer cannot be extended by quantum protocols. Finally, we present a lower bound on the number of commitments which are necessary to implement oblivious transfer in the quantum setting and a protocol which is optimal with respect to this result.

Zusammenfassung

Es ist unmöglich für zwei Parteien, welche nur über einen klassischen Kommunikationskanal verfügen, eine beliebige gemeinsame Berechnung auf ihren jeweiligen Eingaben sicher auszuführen. Sicherheit bedeutet in diesem Kontext, dass ein Spieler mit unbegrenzten rechnerischen Resourcen aus der Berechnung nicht mehr lernen kann als das, was er bereits aus seiner Eingabe und der Ausgabe der Berechnung ableiten kann. Während sich Quanteninformation im Allgemeinen grundlegend von klassischer Information unterscheidet, so scheint sie in diesem Zusammenhang nicht mächtiger: Auch wenn die Parteien über einen Quantenkanal kommunizieren können, kann diese Aufgabe nicht gelöst werden ohne die Rechenleistung der Parteien zu begrenzen. Es gibt jedoch eine Lösung, sobald die beiden Parteien eine Black-Box teilen, welche eine bestimmte Funktion der beiden Eingaben der Spieler berechnet und das Ergebnis an einen der Spieler ausgibt. Ein einfaches Beispiel einer solche Funktion, die den beiden Parteien erlaubt, jede beliebige gemeinsame Berechnung sicher durchzuführen, ist *Oblivious Transfer*. Im ersten Teil dieser Arbeit untersuchen wir die Möglichkeit und Effizienz solcher Berechnungen. Insbesondere zeigen wir untere Schranken für die Anzahl der Aufrufe von Oblivious Transfer, die benötigt werden, um eine allgemeine Funktion sicher zu berechnen.

Ein *Bit Commitment* Protokoll besteht aus zwei Phasen. In der der ersten Phase legt der Sender den Wert eines Bits fest. Das Protokoll ist sicher, wenn der Wert des Bits nicht mehr verändert werden kann, während der Empfänger noch keine Information über den Wert des Bits erhält. Zu einem späteren Zeitpunkt können die Spieler die zweite Phase ausführen, in welcher der Sender den Wert des Bits offenlegt. Es ist bekannt, dass keine informationstheoretisch sicheren Protokolle für Bit Commitment existieren, wenn die beiden Parteien nur einen Kommunikationskanal benutzen können - auch wenn der Kanal Quanteninformation überträgt. Im

zweiten Teil dieser Arbeit untersuchen wir Protokolle für zwei Parteien, die Bit Commitment aus korrelierten zufälligen Bits, welche im Voraus an die Parteien verteilt werden, implementieren. Wir betrachten Protokolle, die mehrere Instanzen von Bit Commitment gleichzeitig erzeugen und zeigen, dass die Entropie und damit auch die Anzahl der Zufallsbits, die pro Bit Commitment notwendig ist, linear mit dem statistischen Sicherheitsparameter zunimmt. Dieses Ergebnis steht im Gegensatz zu bekannten Protokollen, welche viele Instanzen von Oblivious Transfer gleichzeitig implementieren und nur eine konstante Anzahl Zufallsbits pro implementierter Instanz benötigen.

Während zwei Spieler, die über einen Quantenkanal kommunizieren können, einen Schlüssel vereinbaren können, der vor jedem rechnerisch unbegrenzten Gegner sicher bleibt, kann weder Bit Commitment noch Oblivious Transfer allein aus Quantenkommunikation realisiert werden. Allerdings ist die Vereinbarung eines geheimen Schlüssels auch nur dann möglich, wenn die beiden Parteien bereits einen kurzen geheimen Schlüssel besitzen. Im dritten Teil dieser Arbeit stellen wir die Frage, ob ähnliche Protokolle existieren könnten, welche ein Commitment zu einem langen String aus einer kleineren Anzahl von Bit Commitments und einem Quantenkanal realisieren. Wir beantworten diese Frage negativ. Danach zeigen wir, dass Protokolle, die Oblivious Transfer aus verteilten Korrelationen und einem Quantenkanal implementieren können, existieren, welche gegen die gezeigten Schranken für den klassischen Fall verstossen. Allerdings beweisen wir dann untere Schranken an die Entropie der verteilten Korrelationen, welche für jedes sichere Protokoll gelten, das einen Quantenkanal benutzen kann. Diese Schranken implizieren insbesondere, dass auch Oblivious Transfer mit einem Quantenkanal nicht erweitert werden kann. Schließlich beweisen wir eine untere Schranke für die Anzahl Bit Commitments, die erforderlich ist, um Oblivious Transfer mit Hilfe eines Quantenkanals zu realisieren, und präsentieren ein Protokoll, welches gemäss diesem Ergebnis optimal ist.