

Exploring the Limits of Multi-Party Computation

Doctoral Thesis

Author(s):

Raub, Dominik

Publication date:

2009

Permanent link:

<https://doi.org/https://doi.org/10.3929/ethz-a-005954517>

Rights / license:

[In Copyright - Non-Commercial Use Permitted](#)

Diss. ETH No. 18771

Exploring the Limits of Multi-Party Computation

A dissertation submitted to

ETH ZURICH

for the degree of
Doctor of Sciences

presented by

Dominik Raub
Dipl.-Inform., Universität Karlsruhe

born April 15, 1979, in Freudenstadt, Germany
citizen of Germany

accepted on the recommendation of

Prof. Dr. Ueli Maurer, examiner
Prof. Dr. Ronald Cramer, co-examiner

2009

Abstract

In this thesis we explore the limits of multi-party computation and secure function evaluation. Secure function evaluation (SFE) protocols enable distrusting parties to compute an arbitrary function f on their joint inputs, without revealing anything besides the function output. In multi-party computation (MPC) protocols parties can additionally securely maintain a state and thus emulate an arbitrary stateful, reactive, possibly randomized functionality F .

SFE or MPC protocols need to tolerate a number of misbehaving participants that may try to learn secret information or to disrupt the computation. We generally make the worst case assumption that misbehaving participants are corrupted by a central adversary and collude. One distinguishes *computationally* (CO) secure protocols that rely on unproven computational assumptions and could in principle be broken by a very powerful adversary and *information theoretically* (IT) secure protocols which withstand even an unlimited attacker.

Unfortunately there are broad impossibility results for IT secure general MPC in presence of a majority of corrupted parties. These results motivate the following two lines of inquiry:

1. If *general* MPC guaranteeing full IT security against a corrupted majority is impossible, then what *specific* functions can still be computed in this setting?
2. If general MPC guaranteeing *full IT security* against a corrupted majority is impossible, is it at least possible to obtain a graceful degradation of security properties? Can we devise a protocol that is fully IT secure in case of few corruptions, but still provides CO security without fairness in case of many corruptions?

Pursuing the first line of inquiry we derive a combinatorial characterization of the functions computable with IT security in presence of arbitrarily many corrupted parties, in a number of adversarial and communication models.

Furthermore, we derive a combinatorial characterization of the functions computable with long-term security in a very natural, internet-like setting, where a network of insecure channels and a public-key infrastructure are available to the participants. For long-term security, we admit computational assumptions for the duration of a computation, but require IT security once the computation is concluded. Long-term security is a very interesting paradigm because the problem with CO assumptions is not so much that these could be unjustified right now, but rather that concrete CO assumptions could *eventually* be broken by an adversary whose power increases over time, e.g. due to new technical or algorithmic developments.

Following the second line of inquiry, we construct a hybrid secure MPC protocol that provides different levels of security depending on the number of corrupted parties. Our protocol allows for graceful degradation of security, from full IT security to weaker CO security, with an increasing number of corrupted parties, and is optimal under a number of bounds from the literature.

Finally, we discuss homomorphic encryption as a tool for non-interactive protocols. We show that there are no field-homomorphic one-way permutation (OWP), at least for fields of small characteristic. We conclude that field homomorphic cryptosystems are not obtainable using constructions along the lines of group homomorphic schemes, which are generally based on a group homomorphic OWP, e.g. RSA.

Zusammenfassung

In dieser Arbeit erkunden wir die Grenzen von Mehrparteienberechnungen (MPC) und sicherer Funktionsauswertung (SFE). Sichere Funktionsauswertungsprotokolle versetzen einander misstrauende Parteien in die Lage eine beliebige Funktion f ihrer Eingaben zu berechnen, ohne jenseits des Funktionsergebnisses etwas über ihre jeweiligen Eingaben preiszugeben. In Mehrparteienberechnungsprotokollen können Parteien zusätzlich auf sichere Weise einen Zustand halten und damit beliebige, zustandsbehaftete, möglicherweise randomisierte Funktionalitäten F emulieren.

SFE oder MPC Protokolle müssen tolerieren, dass eine gewisse Teilnehmer sich fehlverhalten, mit dem Ziel in den Besitz geheimer Informationen zu gelangen oder die Berechnung zu stören. Wir gehen gemeinhin vom schlechtesten anzunehmenden Fall aus, dass alle sich fehlverhaltenden Parteien von einem zentralen Gegner korrumpiert wurden und zusammenarbeiten. Man unterscheidet zwischen berechnemässig (CO) sicheren Protokollen, die auf unbewiesenen berechnemässigen Annahmen beruhen und prinzipiell von einem sehr mächtigen Gegner gebrochen werden könnten, und informationstheoretisch (IT) sicheren Protokollen, die sogar unbeschränkten Gegnern widerstehen.

Unglücklicherweise gibt es breite Unmöglichkeitsergebnisse für informationstheoretisch sichere allgemeine Mehrparteienberechnungen in Gegenwart einer Mehrheit von korrumpierten Parteien. Diese Resultate motivieren die folgenden zwei Fragestellungen:

1. Wenn *allgemeine* Mehrparteienberechnungen mit voller informationstheoretischer Sicherheit gegen eine korrumpierte Mehrheit unmöglich sind, welche *speziellen* Funktionen lassen sich dann in dieser Situation noch sicher berechnen?

2. Wenn allgemeine Mehrparteienberechnungen mit *voller informationstheoretischer Sicherheit* gegen eine korrumpierte Mehrheit unmöglich sind, ist es zumindest möglich eine graduelle Schächung der Sicherheitseigenschaften mit zunehmender Anzahl von korrumpierten Parteien zu erreichen? Können wir ein Protokoll angeben das im Fall weniger Korruptionen volle informationstheoretische Sicherheit bietet, aber immer noch berechenmässige Sicherheit gewährleistet, wenn viele Parteien korrumpiert sind?

Der ersten Fragestellung folgend leiten wir für verschiedene Gegner- und Kommunikationsmodelle eine kombinatorische Charakterisierung der Funktionen her, die mit informationstheoretischer Sicherheit in Gegenwart beliebig vieler korrumpierter Parteien berechenbar sind.

Weiterhin leiten wir eine kombinatorische Charakterisierung der Funktionen ab, die mit langfristiger Sicherheit berechenbar sind, in einem sehr natürlichen, internet-artigen Kommunikationsmodell, wo ein Netzwerk unsicherer Kanäle und eine Public-Key Infrastruktur gegeben sind. Langfristige Sicherheit bedeutet, dass wir berechenmässige Annahmen zulassen, aber nur während der Ausführung des Protokolls. Nach Abschluss der Berechnung fordern wir informationstheoretische Sicherheit. Langfristige Sicherheit ist ein sehr interessantes Paradigma, da das Problem mit berechenmässige Annahmen weniger darin besteht, dass sie zum jetzigen Zeitpunkt falsch sein könnten, als vielmehr darin, dass konkrete berechenmässige Annahmen schlussendlich von einem Gegner gebrochen werden könnten, der mit der Zeit mächtiger wird, e.g. auf Grund technischen oder algorithmischen Fortschritts.

Im Sinne der zweiten Fragestellung konstruieren wir hybrid-sichere Mehrparteienberechnungsprotokolle, welche verschiedene Sicherheitsgarantien bieten, abhängig davon wieviele Parteien korrumpiert sind. Unser Protokoll gewährleistet eine graduelle Schächung der Sicherheitseigenschaften mit steigender Anzahl korrumpierter Parteien, von voller informationstheoretischer Sicherheit zu schwacher, berechenmässige Sicherheit, und ist optimal unter Schranken aus der Literatur.

Zuletzt diskutieren wir homomorphe Verschlüsselung als ein Werkzeug für nicht-interaktive Protokolle. Wir zeigen, dass es keine körperhomomorphen Einwegpermutationen für Körper kleiner Charakteristik gibt. Wir folgern, dass körperhomomorphe Kryptosysteme nicht analog zu gruppenhomomorphen Systemen konstruierbar sind, welche gemeinhin auf gruppenhomomorphen Einwegpermutationen, e.g. RSA, basieren.