ETH zürich

ETH Library

Multi-party computation

efficient protocols, general adversaries, and voting

Doctoral Thesis

Author(s):
Hirt, Martin

Publication date:
2001

Permanent link:
https://doi.org/https://doi.org/10.3929/ethz-a-004255960

Rights / license:
In Copyright - Non-Commercial Use Permitted

This page was generated automatically upon download from the ETH Zurich Research Collection.
For more information, please consult the Terms of use.

Diss. ETH No. 14376

Multi-Party Computation: Efficient Protocols, General Adversaries, and Voting

A dissertation submitted to

ETH ZURICH

for the degree of
Doctor of Technical Sciences

presented by

Martin Hirt
Dipl. Informatik-Ing. ETH

born July 26, 1970, in Biel
citizen of Birrhard AG, Switzerland

accepted on the recommendation of

Prof. Dr. Ueli Maurer, examiner
Prof. Dr. Birgit Pfitzmann, co-examiner

2001

Abstract

Secure multi-party computation allows a set of players to jointly compute an arbitrary function of their inputs, without revealing these inputs to each other. For example, the players can compute the average of their incomes in such a way that no player learns the income of any other player. Or, as a more applied example, a set of voters can compute the sum of their votes without revealing any particular vote.

The classical results in the literature state that n players can compute any function in such a way that any subset of up to $t < n/2$ players obtains no (zero) information about the other players' inputs, except for what can be derived from the public function output. If the bad players may deviate from the protocol and try both to obtain information about the other players inputs as well as to falsify the public output of the computation, then up to $t < n/3$ can be tolerated. Both bounds are tight.

The achievements of this thesis are three-fold: First, we investigate the efficiency of multi-party protocols. Especially those protocols that allow the bad players to deviate from the protocol are very inefficient. We show that protocols that tolerate misbehavior of the players are almost as efficient as protocols that require all players to follow the protocol correctly. The framework that allows this speed-up is generic and might be used for other distributed tasks as well.

Second, we generalize the existential results for multi-party computation. We show that one can tolerate certain collusions to be larger than the mentioned threshold t, at the cost that some other collusions of size t cannot be tolerated. This models well the fact that in the real-world, some players might be more likely to cheat than others. For various models, we give complete characterizations of the collusions that can be tolerated.

Third, we study secret-ballot voting, a particular application of multi-party computation. We are especially interested in the so-called "receipt-

freeness" property, which essentially means that voters should not be able to sell their right to vote. Receipt-freeness is known to be a subtle property, because one has to deal with voters who are willing to do anything for convincing the vote-buyer that they have submitted the requested vote. We propose a modular framework for such protocols, and construct two concrete receipt-free voting protocols that are more efficient than any receipt-free voting protocol in the literature.

Zusammenfassung

Sichere Multi-Party Berechnungen erlauben einer Menge von Spielern, gemeinsam eine beliebige Funktion von mehreren Inputs zu berechnen, ohne dass sich die Spieler gegenseitig die Inputs geben müssen. Zum Beispiel können die Spieler den Durchschnitt ihrer Einkommen bestimmen, ohne dass ein Spieler das Einkommen eines anderen Spielers erfährt. Oder eine Menge von Wählern kann die Summe ihrer Stimmen berechnen, ohne dass eine einzige Stimme bekannt wird.

Die klassischen Resultate in der Literatur besagen, dass n Spieler jede beliebige Funktion so berechnen können, dass eine beliebige Teilmenge von bis zu $t < n/2$ Spielern absolut keine Information über die Inputs der anderen Spielern erhält, ausser natürlich, was aus dem publiken Ergebnis der Berechnung gefolgert werden kann. Die Korrektheit des Ergebnisses und die Geheimhaltung der Inputs der ehrlichen Spieler kann selbst dann noch gewährleistet werden, wenn bis zu $t < n/3$ Spieler unehrlich sind und vom vorgeschriebenen Protokoll abweichen.

In dieser Dissertation betrachten wir drei Themenbereiche: Erstens behandeln wir die Effizienz solcher Multi-Party Berechnungen. Insbesonders jene Protokolle, die selbst aktiven Attacken von Spielern widerstehen, sind sehr ineffizient. Wir zeigen in dieser Arbeit, dass Protokolle, die robust sind gegen aktive Attacken, fast so effizient realisiert werden können wie die effizientesten nicht-robusten Protokolle aus der Literatur.

Zweitens verallgemeinern wir die bekannten Schwellenresultate aus der Literatur. Wir führen allgemeine Gegnerstrukturen ein und zeigen, dass gewisse Gegnermengen durchaus grösser als die erwähnte Schwelle t sein dürfen, falls dafür andere Gegnermengen kleiner als t sind. Solche allgemeinen Gegnerstrukturen modellieren zum Beispiel den Umstand, dass gewisse Spieler a priori mit grösserer Wahrscheinlichkeit betrügen

werden als andere Spieler. In diversen Modellen kann man mit allgemeinen Gegnerstrukturen auch echt mehr Betrüger tolerieren als mit den Schwellenresultaten.

Drittens betrachten wir das Problem von sicheren elektronischen Wahlen und Abstimmungen, einer der wohl populärsten Anwendungen von Multi-Party Berechnungen. Dabei konzentrieren wir uns vor allem auf das Problem von Stimmenverkauf und stellen uns die Frage, wie dieser verhindert werden kann. Dazu schlagen wir ein Framework vor, in welchem effiziente und sichere Wahlprotokolle konzipiert werden können, die Stimmenverkauf verhindern. Ausserdem entwickeln wir zwei konkrete Wahlprotokolle innerhalb dieser Umgebung, welche beide effizienter sind als alle bisherigen publizierten Wahlprotokolle.