Diss. ETH No. 20500

Graceful Degradation in Multi-Party Computation

A dissertation submitted to

ETH ZURICH

for the degree of
Doctor of Sciences

presented by

Christoph Lucas
MSc ETH CS, ETH Zurich

born May 03, 1983
citizen of the Federal Republic of Germany

accepted on the recommendation of

Prof. Dr. Ueli Maurer, examiner
Prof. Dr. Jesper Buus Nielsen, co-examiner
Dr. Martin Hirt, co-examiner

2012

Abstract

The goal of *Multi-Party Computation* (MPC) is to perform an arbitrary computation in a distributed, private, and fault-tolerant way. For this purpose, a fixed set of n parties runs a protocol that tolerates an adversary corrupting a subset of the parties, preserving certain security guarantees like correctness, secrecy, robustness, and fairness. Corruptions can be either *passive* or *active*: A passively corrupted party follows the protocol correctly, but the adversary learns the entire internal state of this party. An actively corrupted party is completely controlled by the adversary, and may deviate arbitrarily from the protocol. Security can be maintained against more passive corruptions than is possible for active corruptions.

Most MPC protocols provide security guarantees in an *all-or-nothing* fashion: Either the set of corrupted parties is tolerated and the protocol provides all specified security guarantees, or the set of corrupted parties is not tolerated and the protocol provides no security guarantees at all. Similarly, corruptions are in an all-or-nothing fashion: Either a party is fully honest, or it is fully corrupted. For example, an actively secure protocol is rendered completely insecure when just one party is corrupted additionally to what is tolerated, even if all corrupted parties are only passive.

In this thesis, we provide the first treatment of MPC with graceful degradation of both security and corruptions. First of all, our protocols provide graceful degradation of security, i.e., different security guarantees depending on the actual number of corrupted parties: the more corruptions, the weaker the security guarantee (so-called *hybrid* security). We consider all security properties generally discussed in the literature (secrecy, correctness, robustness, fairness, and agreement on abort). Furthermore, the protocols provide graceful degradation with respect to the corruption type, by distinguishing fully honest parties, passively corrupted parties, and actively corrupted parties (so-called *mixed* adversaries).

We prove exact bounds for which MPC with graceful degradation of security and corruptions is possible for both threshold and general adversaries and for all security levels (perfect, statistical, and computational). Furthermore, we provide protocols that meet these bounds. This strictly generalizes known results on hybrid security and mixed adversaries.

Among our technical contributions, especially two might be of independent interest: First, we introduce the notion of *multi-thresholds*. To the best of our knowledge, all known protocols for threshold mixed adversaries characterize the tolerable adversaries with a single pair of thresholds (one threshold for the number of actively, and one for the number of passively corrupted parties). This pair represents the single maximal adversary that can be tolerated. We generalize this basic characterization to allow for several incomparable maximal adversaries. It turns out that, in our setting, multi-thresholds allow to construct protocols that tolerate strictly more adversaries than a single pair of thresholds, without losing efficiency. Second, we present a new secret-sharing scheme that, in the reconstruction phase, releases secrecy *gradually*. This allows to construct non-robust MPC protocols which, in case of an abort, still provide as much secrecy as possible.

Zusammenfassung

Das Ziel von Mehr-Parteien-Berechnungen ist es, eine beliebige Berechnung verteilt, geheim und fehlertolerant durchzuführen. Dafür führt eine gegebene Menge von n Parteien ein Protokoll aus, das gewisse Sicherheitsgarantien wie zum Beispiel Korrektheit, Geheimhaltung, Robustheit und Fairness erhält, auch wenn eine Teilmenge der Parteien von einem Gegner korrumpiert ist. Korruptionen sind entweder *passiv* oder *aktiv*: Eine passiv korrumpierte Partei führt das Protokoll wie eine ehrliche Partei korrekt aus, der Gegner erfährt allerdings den kompletten internen Zustand dieser Partei. Eine aktiv korrumpierte Partei wird vollständig vom Gegner kontrolliert und kann beliebig vom Protokoll abweichen. Protokolle können Sicherheit gegen mehr passiv als aktiv korrumpierte Parteien garantieren.

Die meisten Protokolle für Mehr-Parteien-Berechnungen geben entweder alle oder keine Sicherheitsgarantien: Entweder wird die Menge der korrumpierten Parteien toleriert und das Protokoll garantiert alle spezifizierten Sicherheitseigenschaften, oder die Menge der korrumpierten Parteien wird nicht toleriert und das Protokoll gibt keine Sicherheitsgarantien. Das gleiche gilt für Korruptionen: Eine Partei ist entweder vollkommen ehrlich oder vollkommen korrumpiert. Zum Beispiel ist ein Protokoll, das sicher ist gegen aktive Korruptionen, komplett unsicher wenn auch nur eine einzige Partei mehr korrumpiert ist als toleriert wird, selbst wenn alle korrumpierten Parteien nur passiv korrumpiert sind.

In dieser Doktorarbeit behandeln wir zum ersten Mal Mehr-Parteien-Berechnungen mit „Graceful Degradation“ (z. Dt. fortschreitende Verschlechterung) sowohl der Sicherheit als auch der Korruptionen. Erstens bieten unsere Protokolle „Graceful Degradation“ der Sicherheit, d. h. die Sicherheitsgarantien nehmen mit steigender Anzahl korrumpierter Parteien graduell ab: je mehr Parteien korrumpiert sind, desto schwächer sind die Sicherheitsgarantien (sogenannte *hybride* Sicherheit). Wir betrachten alle Sicherheitseigen-

schaften, die gewöhnlich in der Literatur diskutiert werden (Geheimhaltung, Korrektheit, Robustheit, Fairness und Einigkeit über den Protokollabruch). Zweitens bieten die Protokolle „Graceful Degradation" der Korruptionen, d. h. die Sicherheitsgarantien hängen nicht von der Gesamtanzahl der Korruptionen ab, sondern davon, wieviele Parteien mit welchem Typ korrumpiert sind. Wir betrachten vollkommen ehrliche Parteien, passiv korrumpierte Parteien und aktiv korrumpierte Parteien in einem einzigen Protokolllauf (sogenannte *gemischte* Gegner).

Wir beweisen exakte Schranken, wann Mehr-Parteien-Berechnungen mit „Graceful Degradation" möglich sind, sowohl für Schwellwertgegner (also Gegner, die durch einen Schwellwert an die Anzahl korrumpierter Parteien charakterisiert sind) als auch für allgemeine Gegner (also Gegner, die durch eine allgemeine Bechreibung charakterisiert sind) und für alle Sicherheitsniveaus (perfekt, statistisch und berechenmässig). Ausserdem beschreiben wir Protokolle, die diese Schranken erreichen. Diese Resultate sind strikte Verallgemeinerungen von bekannten Resultaten bezüglich hybrider Sicherheit und gemischter Gegner.

Insbesondere zwei der in dieser Arbeit beschriebenen technischen Beiträge könnten von unabhängigem Interesse sein: Erstens führen wir die Idee der Mehrfachschwellwerte ein. So weit uns bekannt ist, charakterisieren alle bekannten Protokolle für gemischte Schwellwertgegner die tolerierten Gegner mit einem einzigen Paar von Schwellwerten (ein Schwellwert für die Anzahl aktiv und ein Schwellwert für die Anzahl passiv korrumpierter Parteien). Dieses Paar beschreibt den einzigen maximalen Gegner, der toleriert wird. Wir verallgemeinern diese einfache Charakterisierung, um mehrere unvergleichbare maximale Gegner berücksichtigen zu können. Tatsächlich können wir im Modell mit Mehrfachschwellwerte Protokolle konstruieren, die strikt mehr Gegner tolerieren, als es mit einem einzigen Paar von Schwellwerten möglich gewesen wäre, und die trotzdem effizient sind. Zweitens präsentieren wir ein neues Verfahren zum Verteilen geheimer Werte, welches in der Rekonstruktionsphase die Geheimhaltung schrittweise abbaut. Mit diesem Verfahren ist es möglich, Protokolle für Mehr-Parteien-Berechnungen zu konstruieren, die zwar nicht robust sind, aber bei einem Abbruch die bestmögliche Geheimhaltung garantieren.