Diss. ETH No. 15669

Distributed Cryptographic Protocols in Asynchronous Networks with Universal Composability

A dissertation submitted to the

SWISS FEDERAL INSTITUTE OF TECHNOLOGY ZÜRICH

for the degree of
Doctor of Technical Sciences

presented by

RETO STROBL
Dipl. Informatik-Ing. ETH

born January 14, 1977
citizen of St. Gallen SG

accepted on the recommendation of

Prof. Dr. U. Maurer, referee
Dr. C. Cachin, co-referee
Prof. Dr. R. Wattenhofer, co-referee

2004

Abstract

Consider a group of n servers that do not fully trust each other, nor the network by which they communicate. Still, they want to perform correctly some collaborative ongoing task that depends on the local state of each server, while keeping these states as private as possible. This dissertation studies a set of fundamental tasks in such a setting and provides practical protocols for solving these tasks.

All protocols are designed in an asynchronous network model, where messages may be delayed arbitrarily, and no common clock exists. They can therefore also be applied on wide-area networks such as the Internet. The security properties of all protocols are proven such that they hold no matter how the protocols are composed. This is called universal composability. It allows for modular proofs of security of systems, which build on the protocols presented in this dissertation.

The first protocol considered is *Group Key Exchange.* It allows a group of servers communicating over an authentic network to compute a common key, which remains hidden from anyone outside the group that can only observe the network traffic. We propose the first solution for Group Key Exchange in a purely asynchronous network that terminates for every server even if an attacker crashes a minority of the participants. It relies on the existence of public-key encryption schemes.

The second protocol considered is κ-out-n *Verifiable Secret Sharing.* It allows a designated server to distribute a secret among a group of n servers such that every server only learns a *κ-out-n share* of the secret. Such shares have the property that any set of at least κ shares allows to reconstruct the secret, whereas any smaller set of shares does not reveal any information on the secret at all. We propose the first *practical* Verifiable Secret Sharing protocol for asynchronous networks that tolerates the malicious behavior of t servers, where $t < n/3$ and $t < \kappa < n - 2t$. It relies on secure point-to-point links among every pair of servers and on the difficulty of computing Discrete Logarithms in certain finite fields.

The third and last protocol considered is κ-out-n *Proactive Verifiable Secret Sharing.* Such a protocol operates in a sequence of time periods called epochs. It allows to protect the secrecy and integrity of a secret shared among n servers against an attacker that breaks into less than κ servers in every epoch. Technically, this is achieved by computing in every epoch a fresh set of κ-out-n shares of the secret, and erasing the old shares.

We propose the first formalization of κ-out-n Proactive Verifiable Secret Sharing in *asynchronous* networks, along with two different solutions. Both solutions assume secure point-to-point links among every pair of servers in every epoch. The first solution tolerates an attacker that may break-into and control t servers in every epoch, provided that $t < n/3$ and $t < \kappa < n - 2t$. The second solution tolerates an attacker that crashes in every epoch t servers and additionally, eavesdrops up to f servers, provided that $t + f < n/2$ and $f < \kappa$. The difference between the two solutions is that the first one tolerates a stronger attacker, whereas the second one is more efficient.

Zusammenfassung

Betrachten Sie ein verteiltes System, in welchem sich die Mitglieder weder gegenseitig vertrauen, noch den Kanälen über welche sie kommunizieren. Trotzdem möchten sie eine bestimmte Aufgabe erledigen, welche auf gegenseitiger Kooperation beruht. Um der Privatsphäre jedes einzelnen Mitglieds gerecht zu werden, sind also verteilte Protokolle gefragt, welche die gewünschte Aufgabe erledigen ohne mehr als unbedingt notwendig über den internen Zustand der Mitglieder zu verraten. Diese Dissertation präsentiert eine Reihe von solchen Protokollen zur Lösung von Aufgaben, die als fundamental für die Sicherheit in verteilten Systemen gelten.

Alle präsentierten Protokolle operieren vollkommen asynchron, d.h., sie basieren weder auf synchronisierten Uhren der Mitglieder, noch auf Obergrenzen für den Verzug der Kommunkation. Sie können deshalb auch für Weitverkehrsnetze angewended werden, wie zum Beispiel das Internet. Die Sichereheit der präsentierten Protokolle ist so bewiesen, dass sie selbst dann noch gilt, wenn die Protokolle in beliebiger Art und Weise mit anderen Protokollen kombiniert werden. Man nennt diese Eigenschaft auch universelle Kombinierbarkeit. Sie erlaubt, komplexe Systeme nicht nur modular auf den präsentierten Protokollen aufzubauen, sondern auch deren Sicherheit modular zu beweisen.

Als erstes Protokoll wird *Group Key Exchange* betrachtet. Ein solches Protokoll erlaubt es Mitgliedern einer Gruppe, die über authentische Kanäle kommunizieren, einen gemeinsamen Schlüssel auszutauschen. Das Protokoll garantiert, dass niemand ausserhalb der Gruppe aufgrund der Kommunikation den Schlüssel berechnen kann. Es wird das erste solche Protokoll präsentiert, welches selbst dann noch funktioniert, wenn eine beliebige Minderheit der Mitglieder ausfallen. Das Protokoll beruht auf der Existenz von asymetrischen Verschlüsselungsverfahren.

Als zweites Protokoll wird κ-out-n *Verifiable Secret Sharing* betrachtet. Ein solches Protokoll erlaubt es einem speziellen Mitglied einer Gruppe einen Schlüssel so an die anderen n Mitglieder zu verteilen, dass jeder nur einen κ-out-n Teilschlüssel erhält. Diese Teilschlüssel haben die Eigenschaft, dass jede Menge von mindestens κ solcher Teile erlaubt, den verteilten Schlüssel zu rekonstruieren. Jede kleinere Menge hingegen gibt keine Information über den Schlüssel preis. Es wird das erste *praxisnahe* Protokoll für κ-out-n Verifiable Secret Sharing präsentiert, welches das inkorrekte Verhalten von bis zu t Mitgliedern toleriert, solange $t < n/3$ und $t < \kappa < n-2t$. Die Sicherheit beruht auf sicheren Kanälen zwischen den Mitgliedern und auf der Schwierigkeit, diskrete Logarithmen in endlichen Gruppen zu berechnen.

Als drittes und letztes Protokoll wird κ-out-n *Proactive Secret Sharing* betrachtet. Ein solches Protokoll operiert in einer Sequenz von Zeit Intervallen, die man Epochen nennt. Es erlaubt es den n Mitgliedern einer Gruppe einen κ-out-n geteilten Schlüssel vor einem Angreifer zu verbergen, welcher in jeder Epoche die Teilschlüssel von höchstens $\kappa - 1$ Mitglieder erlernen kann. Technisch wird das realisiert, indem die Mitglieder in jeder Epoche neue Teilschlüssel berechnen und die alten löschen.

In dieser Arbeit wird das Konzept von κ-out-n Proaktive Secret Sharing zum ersten Mal im asynchronen Netzerkmodel formalisiert. Zusätzlich werden zwei Lösungen präsentiert, welche beide auf sicheren Kanälen zwischen den Mitgliedern beruhen. Die erste Lösung toleriert einen Angreifer, der in jeder Epoche bis zu t Mitgliedern kontrollieren kann, solange $t < n/3$ und $t < \kappa < n - t$. Die zweite Lösung toleriert einen Angreifer, der in jeder Epoche bis zu t Mitglieder ausschalten und f Mitglieder aushorchen kann, wobei $t + f < n/2$ und $\kappa < f$. Der Unterschied der beiden Lösungen liegt darin, dass die erste einen stärkeren Angreifer toleriert, dafür die zweite effizienter ist.