Diss. ETH No. 12520

Group Signature Schemes and Payment Systems Based on the Discrete Logarithm Problem

A dissertation submitted to the

SWISS FEDERAL INSTITUTE OF TECHNOLOGY ZÜRICH

for the degree of
Doctor of Technical Sciences

presented by

JAN LEONHARD CAMENISCH
Dipl. El.-Ing. ETH

born 25. April, 1968
citizen of Chur

accepted on the recommendation of

Prof. Dr. Ueli Maurer, referee
Prof. Dr. Ivan Bjerre Damgård, co-referee

1998

Abstract

The security of many cryptographic systems relies on the difficulty of computing discrete logarithms in certain finite groups.

This dissertation studies existing cryptographic protocols which are based on this problem. These protocols are then unified and extended to create a framework for designing cryptographic systems. Using this framework, new and efficient realizations of digital group signature schemes and digital payment systems are developed.

Group signature schemes allow a member of a group to sign messages anonymously on the group's behalf. In the case of later dispute, a designated group manager can reveal the signer's identity. An efficient realization of this concept is proposed. Furthermore, the concept of generalized group signatures is developed and realized. This type of scheme allows the definition of sets of group members which can jointly sign on the group's behalf.

Anonymous digital payment systems allow a customer to pay digitally and anonymously. Unfortunately, anonymity also opens the path to criminal misuse, for instance to launder money. As a compromise between the protection of privacy and the possibility of surveillance for crime inspection, the concept of revocable anonymity has been proposed. It introduces a trustworthy third-party which can reveal the identity of a payer in cases of misuse. From an operational point of view, it can be an important requirement that this third-party is not involved in ordinary transactions, but only in anonymity revocation. In this work we present an efficient anonymous digital payment systems satisfying this requirement.

Zusammenfassung

Die Sicherheit vieler kryptographischer Systeme beruht auf der Schwierigkeit, diskrete Logarithmen in endlichen Gruppen zu berechnen.

Diese Dissertation untersucht existierende kryptographische Protokolle, welche auf diesem Problem aufbauen. Diese Protokolle werden vereinheitlicht und zu einem Baukasten für kryptographische Systeme erweitert. In einem zweiten Teil werden damit neue und effizientere Realisierungen digitaler Gruppenunterschriften und anonymer digitaler Zahlungssysteme entwickelt.

Gruppenunterschriften erlauben es Mitgliedern einer Gruppe Dokumente anonym im Namen der Gruppe zu unterschreiben. Im Falle eines Missbrauchs kann jedoch ein Gruppenmanager die Identität des Mitglieds eruieren, welches die Unterschrift geleistet hat. Es wird eine effiziente Realisierung dieses Konzepts entwickelt. Weiter wird das Konzept der verallgemeinerten Gruppenunterschrift entworfen und realisiert. Dieses erlaubt Mengen von Gruppenmitgliedern zu definieren, so dass nur Gruppenmitglieder, die eine solche Menge bilden, gemeinsam im Namen der Gruppe unterschreiben können.

Anonyme digitale Zahlungssysteme ermöglichen es Kunden, digital und anonym zu bezahlen. Da die Anonymität aber auch missbraucht werden kann, um zum Beispiel Geld zu waschen, wurde die aufhebbare Anonymität als Kompromiss zwischen Privatsphärenschutz und Verbrechensbekämpfung vorgeschlagen. In einem solchen System gibt es eine vertrauenswürdige Instanz, welche in Fällen des Missbrauchs gezielt die Anonymität eines Kunden aufheben kann. Von einem operationellen Standpunkt aus gesehen kann es wichtig sein, dass diese vertrauenswürdige Instanz nur für das Aufdecken der Anonymität ak-

tiv sein muss. In dieser Arbeit wird ein solches System präsentiert.