Diss. ETH No. 11404

# Efficiency and Security of Cryptosystems based on Number Theory

A dissertation submitted to the
SWISS FEDERAL INSTITUTE OF TECHNOLOGY ZÜRICH

for the degree of
Doctor of Technical Sciences

presented by

DANIEL BLEICHENBACHER
Dipl. Inform. Universität Bern

born August 4, 1964
citizen of Gottshaus, TG

accepted on the recommendation of

Prof. Dr. U. Maurer, referee
Prof. Dr. M. Bronstein, co-referee
Dr. A. K. Lenstra, co-referee

Zürich, 1996

# Abstract

Computational number theory plays an important role in cryptography because many cryptographic systems and protocols are based on algebraic and number-theoretic structures. Among the important number-theoretic problems relevant to cryptography are primality testing, factoring integers, and discrete logarithms in finite groups.

Efficiency and security are two natural but conflicting goals in cryptography. This dissertation is concerned with a number of security and efficiency aspects of cryptosystems based on number theory. It consists of three parts: contributions to primality testing, to the problem of finding optimal addition chains and Lucas chains, and to the security analysis of a number of proposed cryptographic schemes. Several pseudo-primality tests are analyzed and compared and algorithms for efficiently finding all counter-examples up to a given bound are described. A fundamental cryptographic operation is the exponentiation in finite groups. An exponentiation corresponds to an addition chain for the exponent. An efficient algorithm for computing shortest addition chains is described. The closely related problem of computing Lucas chains is also considered and an algorithm for computing shortest Lucas chains is described. Finally, some weaknesses in proposed cryptosystems are presented. It is shown that ElGamal signatures can be forged in certain cases and a new chosen message attack against a Lucas-based analogue of the RSA system is described.

# Zusammenfassung

Algorithmen der Zahlentheorie spielen eine wichtige Rolle in der Kryptographie, da viele kryptographische Systeme und Protokolle auf algebraischen und zahlentheoretischen Strukturen basieren. Zu den wichtigen zahlentheoretischen Problemen, die für die Kryptographie relevant sind, gehören Primzahltests, Faktorisierung von ganzen Zahlen und die Berechnung von diskreten Logarithmen in endlichen Gruppen.

Effizienz und Sicherheit sind zwei natürliche aber widersprüchliche Ziele in der Kryptographie. Diese Dissertation befasst sich mit einigen Aspekten zur Sicherheit und Effizienz von Kryptosystemen, die auf der Zahlentheorie basieren. Sie besteht aus drei Teilen: Primzahltests, Algorithmen um kürzeste Additions- und Lucas-Ketten zu finden und Analysen einiger vorgeschlagener Kryptosysteme. Verschiedene Pseudo-Primzahltests werden analysiert und verglichen. Algorithmen, die alle Gegenbeispiele zu Pseudo-Primzahltests bis zu einer vorgegebenen Grenze finden, werden beschrieben. Exponentiation ist eine grundlegende Operation in der Kryptographie. Eine Exponentiation entspricht einer Additionskette für dessen Exponenten. Ein Algorithmus, der kürzeste Additionsketten berechnet, wird beschrieben. Betrachtet wird ebenfalls das eng verwandte Problem, kürzeste Lucas Ketten zu berechnen. Zum Schluss werden einige Schwachpunkte in vorgeschlagenen Kryptosystemen vorgestellt. Es wird gezeigt, dass ElGamal Unterschriften in gewissen Fällen gefälscht werden können. Eine neue "chosen-message"-Attacke gegen ein auf den Lucas Funktionen basierendes Analogon des RSA Systemes wird vorgestellt.