Diss. ETH No. 20499

Cryptanalysis of Hardware-Oriented Ciphers the Knapsack Generator, and SHA-1

A dissertation submitted to

ETH Zurich

for the degree of
Doctor of Science

presented by

Simon Knellwolf
MSc ETH Mathematics

born May 25, 1982
citizen of Herisau (AR)

accepted on the recommendation of

Prof. Dr. Ueli Maurer, examiner
Prof. Dr. Willi Meier, co-examiner
Prof. Dr. Lars Knudsen, co-examiner

2012

Abstract

Symmetric key cryptographic algorithms provide confidentiality, integrity, and authentication in modern communication systems. Our confidence in these algorithms is largely based on the fact that intense cryptanalysis has been carried out over several years without revealing any weakness. This thesis makes three independent contributions to the cryptanalysis of symmetric key primitives and hash functions. First, conditional differential cryptanalysis is proposed as a general framework for the analysis of a large class of hardware-oriented ciphers that build on non-linear feedback shift registers. As main applications, various improved distinguishing and key recovery attacks on reduced-round variants of the stream ciphers Grain v1, Grain-128, Grain-128a, and Trivium are obtained. Second, the security of the knapsack generator, a stream cipher construction proposed by Rueppel and Massey in 1985, is studied. A surprisingly effective guess-and-determine attack is shown that recovers large parts of the $n^2 + n$ secret key bits if only n bits are known. Quite different from standard techniques of symmetric cryptanalysis, our approach uses Babai's closest vertex algorithm and lattice reduction. Finally, meet-in-the-middle preimage attacks on hash functions are revisited. A new differential cryptanalytic perspective is proposed which is very suitable for hash functions with linear message expansion. As an application, previous preimage attacks against reduced variants of SHA-1 are significantly improved.

Zusammenfassung

In modernen Kommunikationssystemen sorgen symmetrische Verschlüsselungsverfahren für Vertraulichkeit, Unversehrtheit und Ursprungstreue. Das Vertrauen in die verwendeten Algorithmen basiert hauptsächlich darauf, dass trotz intensiver Kryptanalyse während mehreren Jahren keinerlei Schwachstellen gefunden wurden. Diese Arbeit macht drei voneinander unabhängige Beiträge zur Kryptanalyse von symmetrischen Verschlüsselungsverfahren und kryptographischen Streuwertfunktionen. Der erste Teil beschäftigt sich mit Verfahren, die auf nicht-linearen Schieberegistern aufbauen. Wir führen eine allgemeine Analysetechnick ein, die sogenannte bedingte differentielle Kryptanalyse. Als Anwendung erhalten wir verschiedene neue Attacken auf reduzierte Varianten der Stromchiffren Grain v1, Grain-128, Grain-128a und Trivium. Im zweiten Teil untersuchen wie die Sicherheit des Knapsack Generators, eines Schlüsselstromerzeugers, der 1985 von Rueppel und Massey vorgestellt wurde. Unter Verwendung von Werkzeugen, die in der symmetrischen Kryptanalyse eher unüblich sind, findet unsere Attacke einen grossen Teil der $n^2 + n$ geheimen Schlüsselbits, falls n davon bereits bekannt sind. Im letzten Teil betrachten wir die Meet-in-the-Middle Technik zur Berechnung von Urbildern kryptographischer Streufunktionen. Aufgrund einer neuen Betrachtungsweise vom Standpunkt der differentiellen Kryptanalyse aus erhalten wir deutlich bessere Urbildattacken für reduzierte Varianten von SHA-1.