Flächen-Zeit Optimierte Hardware-Architekturen für die Kryptographie und Kryptanalyse

Kurzfassung

Martin Novotný (novotnym@fel.cvut.cz)

Die vorliegende Dissertation gliedert sich thematisch in zwei Teile. Der erste Teil beschäftigt sich mit skalierbaren Arithmetikeinheiten über endlichen Körpern der Form $GF(2^m)$ in Normalbasis-Repräsentation. Die Skalierbarkeit dieser Architekturen ist dabei essentiell, um den Anforderungen unterschiedlicher Anwendungen – zum Beispiel kleine, eingebettete Systeme mit geringer Leistungsaufnahme im Gegensatz zu Backbone-Systemen mit hohem Datendurchsatz – gerecht zu werden.

Skalierung durch Serialisierung ist eine wohlbekannte Methode, jedoch bringt ihre Anwendung auf Normalbasis-Multiplizierer Probleme durch bestimmte Irregularitäten mit sich. In der einschlägigen Literatur wurde der Fall, dass die Wortbreite kein Teiler des Erweiterungsgrades ist, so gut wie nicht behandelt, obwohl dieser Fall für kryptographische Anwendungen praktisch unvermeidbar ist.

In dieser Arbeit werden vier neuartige „digit-serial“ Normalbasis-Multiplizierer vorgestellt. Dabei handelt es sich um serialisierte Varianten des Multiplizierers von Agnew et al. Es ist erwähnenswert, dass die dazu entwickelten Serialisierungsmethoden auch auf anderere Architekturen, wie zum Beispiel den Multiplizierer von Kwon et al., angewandt werden können. Alle vorgestellten Architekturen können für beliebige Wortbreiten implementiert werden. Die durchgeführte Evaluierung zeigt, dass die Vorteile der Architekturen sich hinsichtlich der Wortbreite komplementär verhalten.

Als weiterer Forschungsbeitrag wird eine vollständig skalierbare Arithmetikeinheit entwickelt, die auf den vorgestellten Multiplizierern basiert. Diese Einheit wurde darauf optimiert möglichst wenig Chipfläche einzunehmen und ist in der Tat nur unwesentlich größer als der enthaltene Multiplizierer. In diesem Kontext stellt sich das bisher wenig untersuchte Problem der Dimensionierung eines Bausteins in der Gegenwart eines zweiten, der das Gesamtsystem bezüglich Fläche und Zeit dominiert. Eine allgemeine Optimierungsstrategie für derartige Fälle wird vorgeschlagen.

Der zweite Teil dieser Arbeit beschäftigt sich mit der hardware-basierten Kryptanalyse der im GSM-Mobilfunknetz eingesetzten Stromchiffre A5/1. Basierend auf dem kürzlich vorgestellten, kosteneffizienten FPGA-Cluster COPACOBANA werden zwei Angriffe gegen A5/1 realisiert. Im Gegensatz zu bisherigen Arbeiten handelt es sich hierbei um zwei äußerst praktikable und vollständig implementierte Attacken.

Der erste Angriff fällt in die Klasse der sogenannten „guess-and-determine“ Attacken und ist in der Lage den geheimen internen Zustand der Chriffre in durchschnittlich 6 Stunden (12 Stunden im „worst-case“) zu bestimmen. Um diesen Angriff durchzuführen werden nur 64 (aufeinanderfolgende) Bits des Schlüsselstroms und keinerlei Vorberechnungen benötigt. Die vorgeschlagene Attacke, sowie eine optimierte Variante wurden komplett auf COPACOBANA implementiert und getestet.

Beim zweiten Angriff handelt es sich um eine „time-memory-data trade-off“ Attacke. Mittels der entwickelten hardware-basierten Realisierung dieses Angriffs kann, mit einer gewissen aber signifikanten Wahrscheinlichkeit, der Initialzustand von A5/1 innerhalb von Minuten wiederhergestellt werden. Die Spezialhardware COPACOBANA wird sowohl für die benötigten (umfangreichen) Vorberechnungen als auch für den eigentlichen Angriff eingesetzt. Idealerweise könnte das hier vorgeschlagene Design als Referenz für gleichartige Angriffe auf Stromchiffren dienen.

Schlüsselworte:
Public-Key-Kryptographie, Elliptische-Kurven-Kryptographie, Hardwarearithmetik, Endliche Körper, Normalbasen, Multiplikation, Inversion, Kryptanalyse, Brute-Force Attacken, TMDTO Attacken, A5/1, COPACOBANA, FPGA