Kurzfassung

Physikalischer Schutz durch kryptographische Hardwareagilität

Die Massenfertigung und der allgegenwärtige Einsatz von integrierten Logikschaltungen haben der Digitalen Revolution den Weg bereitet und das Informationszeitalter eingeläutet. Durch den Einsatz von neue Technologien und Endgeräten zur Informationsbearbeitung wurde eine Fülle an neuen Möglichkeiten und Innovationen geschaffen, – vom Internet der Dinge bis hin zu intelligenten Transportsystemen - die unser tägliches Leben und unsere Lebensgewohnheiten durchdringen und dramatisch verändern. Durch den ständigen Zuwachs und Fluss von Informationen wird das Thema der Sicherheit und des Datenschutzes immer bedeutsamer, insbesondere für nahezu allgegenwärtige Kleinstgeräte wie Mikrocontroller und eingebettete Systeme. Da moderne Sicherheitsmechanismen auf einer Vielzahl komplexer, kryptographischer Operationen beruhen, die diese beschränkten Systeme stark belasten, kann effiziente Kryptographie auf hardwarebasierten Beschleunigern, einschließlich Application-Specific Integrated Circuits (ASICs) und Field-Programmable Gate Arrays (FPGAs), helfen diese Belastung zu mindern. Außerdem sind, durch den ungehinderten und unbeschränkten physikalischen Zugriff und das statische Verhalten dieser Geräte, Seitenkanalangriffe eine ernstzunehmende Bedrohung für die kryptographischen Implementierungen. Demzufolge kann Hardwareagilität, d. h. dynamische Strukturen und fortwährende Änderungen an der Schaltung und ihrem Verhalten, helfen, die statischen Methoden der Seitenkanalanalyse gegenstandslos werden zu lassen.

Ein erster Forschungsaspekt dieser Dissertation beschäftigt sich mit der Entwicklung von kleinflächigen und hochperformanten kryptographischen Schaltungen für symmetrische und asymmetrische Kryptosysteme auf rekonfigurierbaren Geräten. Im Detail befasst sich diese Arbeit mit besonderen Funktionen und Eigenschaften moderner FPGAs und deren Anwendbarkeit für hocheffiziente, hardwarebasierte Kryptographie. Dazu werden neue Einsatzmöglichkeiten für *Distributed Memory*, d. h. FPGA – Konfigurationsspeicher, der in Anwendungsspeicher umgewandelt wurde, im Rahmen einer Kleinstschaltung einer AES Verschlüsselung betrachtet. Außerdem demonstriert die vorliegende Arbeit den Einsatz von Block-RAM und Digitalen Signalprozessoren für hochperformante Implementierungen der hoch-sicheren Elliptic Curve Cryptography, die auch in den nächsten Generationen des TLS Protokolls Verwendung finden soll. Zum Schutz gegen physikalische Angriffe verwenden alle beschriebenen Verfahren modernste Seitenkanalgegenmaßnahmen, die im Gray-Box Angreifermodell mittels eines praktischen Aufbaus evaluiert wurden.

Der zweite Kernaspekt dieser Arbeit behandelt das Thema der kryptographischen Hardwareagilität zum Schutz gegen physikalische Angriffe. Insbesondere FPGAs bieten als Hardwareplattform die einzigartige Fähigkeit der Rekonfigurierbarkeit, um zur Laufzeit bei Bedarf beliebige digitale Schaltungen zu laden und zu ersetzen. Zusammen mit algorithmischen Äquivalenzen besteht das Novum dieser Arbeit in der Kombination von struktureller und algorithmischer Rekonfiguration für kryptographische Implementierungen zum Schutz gegen passive Seitenkanalanalyse. Demzufolge untersucht und evaluiert diese Dissertation verschiedene Komponenten der FPGAs, die eine Restrukturierung der Hardwareschaltung erlauben. Auf dem Weg zur generischen Methodik zur Restrukturierung und Randomisierung von Schaltungen analysiert die vorliegende Arbeit algorithmische Strukturen zur äquivalenten Darstellung von Schaltkreisen und deren Einsatz zur Stärkung von bestehenden Threshold Implemertierungen. Letztendlich wird das Ziel der realisierbaren Hardwareagilität mittels generischer Methoden zur Schaltungsrandomisierung durch die Adaption von grundlegenden Konzepten der White-Box Cryptography erreicht und demonstriert.

Schlagworte.

Kryptographie, Hocheffizienzimplementierungen, Rekonfigurierbare Hardware, FPGA, Seitenkanalanalyse, Maskierung, Verschleierung, Dynamische Hardwareagilität, Threshold Implementierungen, t-Test, White-Box Kryptographie