Kurzfassung

Seit Durchbruch des Internets ist die Zahl an informationsverarbeitenden Systemen in vielen Bereichen des täglichen Lebens stark gewachsen. Dabei kommen bei der Kommunikation und Verarbeitung von Daten in den verschiedensten Gegenständen des Alltags eingebettete Systeme zum Einsatz, die oft harten Anforderungen, wie beispielsweise hohe Leistung bei optimaler Kosteneffizienz, gerecht werden müssen. Zusätzlich müssen diese – je nach Anwendungsfall – weitere Kriterien, wie z.B. Sicherheitsaspekte durch kryptografische Verfahren, ohne nennenswerte Einbußen bezüglich der Datenverarbeitungsgeschwindigkeit erfüllen. In diesem Zusammenhang sind kleine Mikrocontroller, wie sie typischerweise in diesen Systemen verwendet werden, schnell überfordert, so dass für kryptografische Funktionen in eingebetteten Hochleistungssystemen fast immer dedizierte Hardwarechips zum Einsatz kommen.

Ein erster Kernaspekt dieser Dissertation beschäftigt sich mit Hochleistungsimplementierungen von symmetrischen wie asymmetrischen Kryptosystemen für rekonfigurierbarer Hardwarechips (*Field Programmable Gate Arrays* oder kurz *FGPAs*). Ein Herausstellungsmerkmal der Arbeit ist hierbei die Implementierung der standardisierten AES-Blockchiffre (FIPS-197) sowie von Elliptischen Kurven Kryptosystemen (ECC) über Primkörpern (FIPS-186-2/3) unter Nutzung von dedizierten Arithmetikfunktionskernen moderner FPGAs, die primär für Filteroperationen der klassischen digitalen Signalverarbeitung entwickelt wurden. Neben dem Einsatz von FPGAs wird weiterhin die Eignung von modernen, handelsüblichen Grafikkarten als Koprozessorsystem für asymmetrische Kryptosysteme untersucht, die durch hohe parallele Rechenleistung sowie günstige Anschaffungskosten eine weitere Option für effiziente kryptografische Hochgeschwindigkeitslösungen darstellen. Basierend auf einer NVIDIA 8800 GTS Grafikkarte werden im Rahmen dieser Arbeit neuartige Implementierungen für das RSA sowie ECC Kryptosystem vorgestellt.

Ein zweiter Aspekt dieser Arbeit ist die Kryptanalyse mit Hilfe von FPGA-basierten Spezialhardwarearchitekturen. Alle praktikablen, kryptografischen Verfahren sind grundsätzlich der Abwägung zwischen Effizienz und dem gewünschten Maß an Sicherheit unterworfen; desto höher die Sicherheitsanforderungen sind, desto langsamer ist im Allgemeinen das Kryptosystem. Die Sicherheitsparameter eines Kryptosystems werden daher aus Effizienzgründen an die besten zu Verfügung stehenden Angriffsmöglichkeiten angepasst, wobei einem Angreifer ein hohes, aber beschränktes Maß an Rechenleistung zugesprochen wird, das dem gewünschten Sicherheitsniveau entsprechen soll. Aus diesem Grund muss die Komplexität eines Angriffs genau untersucht werden, damit eine präzise Angabe der durch das Kryptosystem *tatsächlich* erreich-

ten Sicherheit in praktikabler Weise gemacht werden kann. Im Rahmen dieser Arbeit wurde maßgeblich der FPGA-basierte Parallelcluster *COPACOBANA* mit- und weiterentwickelt. Dieser speziell auf eine optimale Kosten-Leistungseffizienz ausgelegte Cluster ermöglicht genaue Aufwandsabschätzungen von Angriffen auf verschiedenen Kryptosystemen, u.a. auf Basis einer finanziellen Metrik. Mit Hilfe dieser Clusterplattform können sowohl schwache oder ältere Kryptosysteme gebrochen, wie auch Angriffe auf aktuell als sicher geltende kryptografische Verfahren abgeschätzt werden. Neben der erfolgreichen Kryptanalyse der symmetrischen DES-Blockchiffre, sind ein weiterer Teil dieser Arbeit neuartige Hardwareimplementierungen von (unterstützenden) Angriffen auf asymmetrische Kryptosysteme, die auf dem Elliptischen Kurven Diskreten Logarithmus Problem (ECDLP) oder dem Faktorisierungsproblem (FP) basieren.

Ein dritter und letzter Bereich dieser Dissertation betrifft den Schutz der rekonfigurierbaren Hardware und seinen logischen Komponenten selbst. Es handelt sich bei typischen FPGAs zumeist um dynamische SRAM-basierte Logikschaltungen, die jederzeit zur Laufzeit konfiguriert und auch geändert werden können. Deshalb muss insbesondere bei sicherheitskritischen Funktionen darauf geachtet werden, dass die Konfiguration des FPGA durch einen Angreifer nicht manipuliert werden kann. Nur so kann beispielsweise ein Auslesen des geheimen Schlüssels oder die Kompromittierung des Sicherheitsprotokolls verhindert werden. Manchen FPGA hat der Hersteller bereits mit der Funktion ausgestattet, symmetrisch verschlüsselte Konfigurationsdateien zu verwenden. Jedoch besteht gerade bei komplizierteren Geschäftsmodellen in der Praxis das klassische Problem der Schlüsselverteilung, d.h. wie kann der Hersteller von FPGA-Konfigurationsdateien den vom FPGA zur Entschlüsselung der Konfiguration benötigten Schlüssel im Chip installieren, ohne dabei physischen Zugriff auf den FPGA zu haben? In dieser Dissertation wird hierfür ein sicheres Protokoll vorgestellt, welches sich diesem Schlüsselverteilungsproblem annimmt und auf dem Diffie-Hellman Schlüsselaustauschverfahren basiert.
Weiterhin werden FPGAs auf ihre Fähigkeit untersucht, einen dynamisch konfigurierbaren Sicherheitskern, ein so genanntes *Trusted Platform Module* (TPM), in einem dedizierten, dynamischen Bereich einzurichten, der anderen Applikationen der Konfigurationslogik vertrauenswürdige Sicherheitsfunktionen zu Verfügung stellen kann. Der große Vorteil dieses Systems in Bezug auf klassischen TPM-Architekturen, wie sie bereits im PC-Umfeld eingesetzt werden, ist dabei die wesentlich schwierige Auslesbarkeit und Manipulierbarkeit der Datenleitungen, da hier ein System-on-a-Chip (SoC)-Architektur zum Einsatz kommt. Weiterhin können durch die dynamische Erweiter- und Aktualisierbarkeit der Sicherheitsfunktionen im rekonfigurierbaren System schwache oder gebrochene Sicherheitskomponenten jederzeit ausgetauscht werden, ohne dafür das gesamte System ersetzen zu müssen.

Schlagworte.

Kryptographie, Kryptanalyse, Hochgeschwindigkeitsimplementierungen, Hardware, FPGA