Hocheffiziente Kryptographie -
Ingenieurtechnische Entwicklungen für pervasive Geräte

Lehrstuhl Embedded Security
Dipl.-Ing. Dipl.-Kfm. Axel Poschmann

Kurzfassung

Alltagsgegenstände werden zunehmend durch das Einbetten von Prozessoren zu pervasiven Geräten erweitert. Die Vernetzung solch pervasiver Geräte führt zu Mark Weiser 's berühmter Vision des *Ubiquitous Computing*. Gemeinhin wird angenommen, dass sich die Informationstechnologie in einem Paradigmenwechsel—weg vom Personal Computing, hin zum Ubiquitous Computing—befindet. Dazu passt die Tatsache, dass momentan 98,8% aller produzierten Mikroprozessoren in eingebetteten System verbaut werden und nur 0,2% in klassischen Computern. Der erwartete Nutzen ist vielverpsrechend: geringere Logistikkosten, höhere Prozessgranularität, optimierte Supply-Chains oder standortbezogene Dienste sind nur ein kleiner Ausschnitt. Auch wird erwartet, dass das Internet der Dinge durch einen Masseneinsatz der RFID[1]-Technologie überhaupt erst ermöglicht wird. Jedoch sind viele vorhergesehenen Anwendungen—wie z.B. kabellose Sensornetze fürs Militär, Banken oder Automobilbranche—sicherheitskritisch und durch die weite Verbreitung von eingebetteten Systemen in diesen Szenarien steigt auch der potenzielle Schaden durch einen Angreifer. Schlimmer noch, durch den Einsatz der eingebetteten Systeme in "feindlicher " Umgebung, hat ein möglicher Angreifer volle physikalische Kontrolle über die Geräte. Dadurch wird die gesamte Klasse der physikalischen Angriffe überhaupt erst ermöglicht. Insbesondere so genannte Seitankanal-Angriffe, wie DPA/CPA oder EM Angriffe, stellen eine große Gefahr dar. Abschließend sei noch auf die Gefahren für die Privatsphäre und anderer Bürgerrechte durch die Allgegenwärtigkeit von eingebetteten Systemen hingewiesen. Sicherheit ist also von zentraler Bedeutung.

Durch die hohen Stückzahlen, die mit einer Allgegenwärtigkeit einhergehen, entstehen scharfe Kostenvorgaben. Für anwendungsspezifische integrierte Schaltkreise (ASICs) bedeutet dies insbesondere eine starke Beschränkung hinsichtlich des Strom-, Energie-, und Flächenverbrauchs. Demgegenüber gibt es kaum Beschränkungen hinsichtlich des Durchsatzes, weil viele Anwendungen nur geringe Datenmengen wie Zähler, Initialisierungsvektoren oder Identifikationsnummern verarbeiten. Das allbekannte Moore'sche Gesetz muss in diesem Kontext konträr interpretiert werden: viele vorhergesehene Anwendungen benötigen ein Minimum an Rechen- bzw. Speicherkapazität, das im Moment noch zu teuer für eine Massenanwendung ist (Stichwort: RFID-Etiketten auf Tetrapaks). Sinken die Preise jedoch unter einen gewissen Schwellwert, so wiegt der zusätzliche Nutzen die Kosten auf. Auf diese Weise werden immer komplexere Anwendungen erschwinglich und können realisiert werden wodurch sich ein konstanter oder sogar steigender Bedarf nach hocheffizienten Implementierungen ergibt.

In dieser Dissertation werden verschiedene Ansätze verfolgt um hocheffiziente Implementierungen von kryptographischen Primitiven wie Block Chiffren, Hashfunktionen und asymmetrischen Identifikationssysteme zu untersuchen. Der Fokus liegt dabei auf hocheffizienten Hardwarerealisierungen, die so wenig Fläche wie möglich—gemessen in Gatter Äquivalenten (GE)—verbrauchen. Anfangs wird der Data Encryption Standard (DES)—ein standardisierter und gut-untersuchter Algorithmus—effizient implementiert, wodurch sich mit 2309 GE die kleinste bekannte Hardwarerealisierung des DES ergibt. Um den Flächenverbrauch weiter zu verringern wird der DES etwas verändert. Dazu ist es notwendig, die Substitutions-Boxen (sog. S-Boxen) des DES näher zu untersuchen. Hierbei wurden S-Boxen gefunden, die nicht nur stärker gegen die relevantesten Angriffe resistent sind, sondern darüber hinaus einen geringeren Flächenverbrauch haben. Diese DES Variante heißt DESL und seine Implementierung benötigt mit 1848 GE 20% weniger Fläche als der DES. Um eine größere Sicherheit zu erlangen ist es möglich, analog wie beim DES, sog. *Key-Whitening* Techniken anzuwenden. Die resultierende Chiffre, DESXL, benötigt 2168 GE.

Um den Flächenverbrauch weiter zu verringern, wird im nächsten Schritt ein komplett neuer Algorithmus entworfen. Beim Entwurf von PRESENT konnte auf die während des Studiums der DES S-Boxen gewonnenen Erkenntnisse aufgebaut werden. Die Hardwarerealisierung von PRESENT benötigt nur 1000 GE und stellt damit die kleinste bekannte Hardwarerealisierung einer kryptographischen Primitive mit angemessener Sicherheit dar. In dieser Dissertation wird ausführlich auf verschiedene Hard- und Softwarerealisierungen von PRESENT für verschiedene Plattformen eingegangen.

Weiterhin werden neue hocheffiziente Hashfunktionen, die auf PRESENT basieren oder ähnliche Komponenten haben, untersucht. Es werden zwei Varianten basierend auf PRESENT im *Davies-Meyer*-Modus mit einer Ausgabelänge von 64 Bits (DM-PRESENT-80 und DM-PRESENT-128) vorgestellt. Für Hashfunktionen mit 128 Bits Ausgabe kann PRESENT im *Hirose*-Modus (H-PRESENT-128) betrieben werden. Um Ausgabelängen von 160 oder mehr Bits mit einer auf PRESENT basierenden Hashfunktion zu bekommen, wird C-PRESENT- 192 vorgeschlagen. Dessen Implementierungsergebnisse (8048 GE) bzw. Abschätzungen (> 4600 GE) zeigen jedoch, dass diese Konstruktion nicht sehr effizient ist. Stattdessen werden die Hardwarerealisierungen von zwei weiteren Vorschlägen—PROP-1 und PROP-2—abgeschätzt, die mit > 2520 GE bzw. > 3010 GE vielversprechender sind.

Schließlich werden die Implementierungsergebnisse von *crypto-GPS*, einem asymmetrischen Identifikationssystem, das vorberechnete Coupons benutzt, vorgestellt. Hier kommt PRESENT im Output-Feedback-Modus als Pseudozufallszahlengenerator zum Einsatz und verschiedene Architekturen werden vorgestellt. Die Implementierungsergebnisse werden durch die Performanzzahlen eines speziell gefertigten ASIC-Prototypen von *crypto-GPS* ergänzt.

Zusammenfassend lassen sich aus den in dieser Dissertation beschriebenen Ergebnissen die folgenden Schlussfolgerungen ableiten:

1. Die weit verbreitete Annahme, dass Stromchiffren effizienter in Hardware zu realisieren sein als Blockchiffren ist so nicht mehr haltbar, da die hier vorgestellte Blockchiffre PRESENT nur 1000 GE benötigt.
2. Dadurch lassen sich Hashfunktionen mit einer Ausgabelänge von 64 oder 128 Bits, die auf Blockchiffren basieren, ebenfalls hocheffizient implementieren. Dieses trifft jedoch nicht auf Hashfunktionen mit Ausgabelängen von 160 oder mehr Bits zu. Berücksichtigt man die Parameter des NIST SHA-3 Hashfunktions-Wettbewerbs, ist es sehr unwahrscheinlich, dass hieraus eine hocheffiziente Hashfunktion resultiert und folglich bleibt diese Forschungsfrage weiterhin offen.
3. Die Implementierungen von *crypto-GPS* zeigen, dass es möglich ist auch asymmetrische Verfahren hocheffizient zu implementieren. Jedoch benötigt das *crypto-GPS* Verfahren eine begrenzte (aber wählbare) Anzahl von vorberechneten Coupons. Zukünftige Forschungen könnten sich auf asymmetrische Verfahren konzentrieren, die diese Beschränkungen nicht aufweisen.

Schlüsselworte

Hocheffiziente Kryptographie, Entwurf, Eingebette Systeme, Hardware, ASIC, S-Box, Block Chiffre, Hashfunktion, Pervasive Sicherheit, IT-Sicherheit.

---

[1] Radio Frequency IDentification, Funkerkennung.