Ein IP-Core Design für Schlüsselaustausch, Stromchiffre und Identifikation auf ressourcenbeschränkten Geräten

Markus Volkmer, Sebastian Wallner

Technische Universität Hamburg-Harburg
Technische Informatik VI
Schwarzenbergstraße 95, D-21073 Hamburg
markus.volkmer@tuhh.de¹
wallner@tuhh.de²

Abstract: Das Design und die Implementierung für einen sogenannten Lightweight IP-Core für symmetrischen Schlüsselaustausch, Stromverschlüsselung und Identifikation (Entity Authentication) werden vorgestellt. Diese dedizierte Hardware-Lösung bezieht seine drei kryptographischen Funktionen aus einem einzigen adaptiven Interaktionsprotokoll. Sie beansprucht extrem wenig Logik-Fläche und eignet sich besonders, um die Sicherheit der Kommunikation zwischen ressourcen-beschränkten Geräten oder zwischen Komponenten (ICs) auf Board-Ebene zu erhöhen. Der IP-Core beansprucht eine Logik-Fläche von ca. 0.1 mm² bei einem Sechs-Lagen UMC 0.18µ-Prozess.

1 Kryptographie und Ressourcenbeschränkte Geräte

Als ressourcenbeschränkte Geräte gelten im Allgemeinen Systeme mit einem Mikrocontroller (MC) von 8-Bit an abwärts oder Geräte ohne MC mit einfachen Steuerautomaten, die zudem oft nur über eine begrenzte Energieversorgung z.B. aus Batterien verfügen. Die typischen Anwendungsszenarien reichen von Sensornetzwerken bis hin zu Tags in Systemen zur Radiofrequenzidentifikation (RFID). Oft liegen hier extreme und gekoppelte Beschränkungen hinsichtlich Logik-Fläche, Stromverbrauch und verfügbarer Rechenleistung vor. Dies betrifft insbesondere kryptographische Verfahren, die aufwändige arithmetische Operationen durchführen, welche entweder als Software-Realisierung viel Rechenzeit erfordern, oder als Hardware-Realisierung viel Logik-Fläche beanspruchen.

Hinzu kommt, dass asymmetrische kryptographische Verfahren bzw. Public-Key-Verfahren, wie z.B. RSA, ECC und NTRU, prinzipiell eine Infrastruktur (Public-Key-Infrastructure (PKI), Certificate Authority, Trusted Center) für die Vergabe, Verwaltung und Zertifizierung der Schlüssel erfordern. In leistungsfähigen Systemen wie Desktop-

¹ volkmer@keyXchange.de

² wallner@keyXchange.de

Rechnern, Laptops etc. stellt die Implementierung und Ausführung von Algorithmen der Kryptographie zur Absicherung der Kommunikation aufgrund der vorhandenen Prozessorleistung in der Regel kein praktisches Problem dar. In gerouteten Netzwerken mit Serverstrukturen ist auch das Einrichten von PKIs oder anderen Server-zentrierten Diensten prinzipiell immer möglich. Beim Vorliegen von Punkt-zu-Punkt Verbindungen oder (mobilen) Ad-Hoc Netzwerken hingegen stellen derartige Sicherheitsinfrastrukturen mangels nicht vorhandener genereller Infrastruktur ein Problem dar.

Dynamische und kurzlebige Netzwerktopologien verlangen jedoch einen häufigen Austausch von Schlüsseln. Sichere Gruppenkommunikation kann beispielsweise nur gewährleistet werden, wenn beim Eintritt in eine Gruppe und beim Verlassen einer Gruppe ein neuer Schlüssel die Kommunikation der Gruppe gegenüber Dritten absichert. In dieser Hinsicht sind kryptographische Methoden mit angemessener Komplexität erforderlich, die auch dem immer vorhandenen Protokoll-Overhead Rechnung tragen. Während die Verfahren zur Verschlüsselung in der Regel unkritisch sind, stellen Authentifizierung und Schlüsselaustausch herausragend wichtige und schwierige Probleme dar.

Das relativ junge Forschungsgebiet der Eingebetteten Sicherheit (engl. Embedded Security) beschäftigt sich mit insbesondere mit effizienten Realisierungen kryptographischer Verfahren, aber auch mit alternativen Lösungen für oben beschriebene eingebettete Systeme in (mobilen) Klein- und Kleinstgeräten mit starken Beschränkungen [P03]. Es werden auch alternative kryptographische Technologien zur Erhöhung der Sicherheit verfolgt, die Ihre Sicherheit nicht aus der Komplexität eines zahlentheoretischen Problems schöpfen und begründen, sondern aus statistischen Argumenten, informationstheoretischen Konzepten [M93] und schwierigen Lernproblemen [J05].

In diesem Beitrag wird für die kürzlich in [VW05] vorgestellte Technologie skizziert, warum sie extrem vorteilhaft als Hardware-Komponente implementiert werden kann. Aus den praktischen Erfahrungen bei der Implementierung und der erzielbaren Performance wird das Potential für aktuelle und zukünftige Anwendungen abgeleitet.

2 Kryptographie mit Tree Parity Machines

Kryptographie mit Tree Parity Machines (TPMs) basiert auf einem adaptiven Interaktionsprinzip und einem Synchronisationseffekt zwischen deterministischen endlichen Automaten. In [VW05] werden drei wesentliche kryptographische Funktionen aus diesem Prinzip gewonnen: symmetrischer Schlüsselaustausch, Identifikation (Entity Authentication) und Stromverschlüsselung im Output-Feedback- sowie im Cipher-Feedback-Modus (OFB/CFB). Weiterhin ist es auf einfache Weise möglich, die Technologie auf einen symmetrischen Mehrparteienschlüsselaustausch zu erweitern.

Beim Schlüsselaustausch [KKK02] adaptieren zwei (oder mehr) TPMs ihren internen (initial unabhängigen und zufälligen) vorläufigen Schlüssel (Zustand) in einem Interaktionsprozess, so dass beide Maschinen auf dieselbe pseudozufällige Eingabe immer dieselbe Ausgabe produzieren und dann damit gleiche Schlüssel (Zustände) besitzen. Die Schlüssellänge wird durch die Wahl der Parameter der TPM-Struktur bestimmt und beeinflusst dabei neben der Sicherheit auch die Synchronisationszeit.

Die Sicherheit des Schlüsselaustausches mit TPMs basiert auf dem Vorteil der Interaktion gegenüber einem Angreifer, der lediglich passiv lernen kann: Lernen ohne Interaktion ist schwieriger als Lernen mit Interaktion. Dieser Vorteil (und damit die Sicherheit) lässt sich insbesondere gegenüber dem sog. Flipping-Angriff u.a. auch durch Anwenden paralleler Interaktion (Bit-Paket-Lernen) in Zusammenhang mit dem von uns eingesetzten Interleaved Learning bzw. Decoupled Learning, sowie generell durch eine hinreichende Schlüssellänge erhöhen.

Die Identifikation mit TPMs beruht auf der Eigenschaft, das eine Synchronisation sich nur bei gleichen Eingaben an die TPMs einstellen kann. Somit kann der Initialwert des zur Erzeugung der Eingabewerte eingesetzten LFSR als ID genutzt werden. Stellt sich beim (sequentiellen oder parallelen) Interaktionsprotokoll (zum Schlüsselaustausch) keine Synchronisation ein, besitzt die angefragte Partei nicht die erforderliche ID. Diese inhärente Entity Authentication verhindert auch den Man-In-The-Middle-Angriff und alle bekannten Angriffe mit TPMs, da ohne die gleiche Eingabefolge kein Lernen und Synchronisieren möglich ist.

Eine Stromchiffre per TPMs lässt sich über den sogenannten Trajektorie-Modus realisieren. Sind zwei TPMs synchron, so sind alle internen Zustände der Maschinen und insbesondere die von ihnen erzeugten Ausgaben identisch. Die beiden TPMs ändern fortan in gleicher Weise ihre internen Zustände ohne weitere Kommunikation auf Basis ihrer eigenen Ausgabe und den pseudozufälligen Eingaben. Die nicht-lineare Folge der internen Schlüssel (nicht-lineare Zustandsübergänge) wird Trajektorie genannt und dient zur Ableitung einer Stromchiffre. Diese wird entweder auf Basis der Ausgaben abgeleitet (OFB und CFB möglich) oder verwendet blockweise einen Hash-Wert (z.B. per Keyed/Universal Hashing) der Schlüssel aus der Trajektorie. Die Schlüssellänge kann prinzipiell beliebig gewählt werden. Der Initialwert des o.g. LFSR stellt in diesem Zusammenhang einen Initialvektor der Stromchiffre dar, dessen maximale Länge von den gewählten TPM-Parametern bestimmt wird.

3 Ein Multifunktionaler Lightweight-Crypto IP-Core

Die in [VW05] vorgestellte Technologie realisiert die oben genannten kryptographischen Funktionen in einer Hardware-Realisierung als IP-Core.

Die komplexeste Operation in diesem Verfahren ist die Addition kleiner begrenzter ganzer Zahlen und es basiert wesentlich auf einem adaptiven Interaktionsprotokoll. Um bei Paket-basierten Kommunikationskanälen den Protokoll-Overhead gering zu halten, wird das Bit-Packaging als eine Form der parallelen Interaktion implementiert.

Design-Entscheidungen bei der Realisierung als IP-Core bestimmen wesentlich die resultierende Performance. Die Additionsoperationen können in Abhängigkeit von dem benötigten Durchsatz parallel oder seriell realisiert werden. Weitere notwendige Operationen lassen sich als einfache Bit-Operationen realisieren. Für das Bit-Packaging sind zusätzliche Register notwendig, welche aufgrund der simplen Arithmetik primär die Logik-Fläche beeinflussen. Diese können aber zum Großteil durch Neuberechnen von internen Zuständen eingespart werden. Neben einem Linear Rückgekoppelten Schieberegister als Pseudozufallszahlengenerator wird für den Schlüsselaustausch ein echter Zufallszahlengenerator benötigt. Hier kann ein auf internen Rückkopplungsmechanismen und Signallaufzeiten basierender Generator Verwendung finden.

Bei dem resultierenden Lightweight IP-Core und seinen Varianten handelt es sich um eine dedizierte Hardware-Lösung, die sehr wenig Ressourcen (Logik-Fläche) beansprucht (small footprint). Der IP-Core ermöglicht die Schlüsselgenerierung mit einem Durchsatz im kHz-Bereich bei einer Logik-Fläche im Bereich 0.1 mm² (Sechslagen 0.18µ UMC Prozess). Der Durchsatz wird dabei oft nur durch den im Allgemeinen langsamen Kommunikationskanal begrenzt.

Der IP-Core bietet damit eine Technologie zur Absicherung von Kommunikation mit neuartigen Eigenschaften und neuen Möglichkeiten zur Erhöhung der Sicherheit bei gleichzeitiger Kostenreduktion durch Einsparung von Ressourcen "Logik-Fläche" bzw. "Rechenleistung" für kryptographische Operationen. Anwendungsfelder liegen insbesondere im Umfeld ressourcenbeschränkter Geräte, aber auch bei Handhelds, Smartcards, Mobiltelefonen, Ad-hoc-Netzwerk-Anwendungen etc. Technologien des Pervasive und Ubiquitous Computing eröffnen zukünftige Anwendungsfelder, da auch hier Sicherheit eine Grundvoraussetzung für die Akzeptanz von Produkten sein wird.

Ein Forschungsprototyp wurde bereits in Systeme integriert und ein optimierter Produktprototyp mit einer universellen und einfachen Schnittstelle befindet sich in der Entwicklung.

Literaturverzeichnis

- [P03] Paar, C.: Past and future of cryptographic engineering. Tutorial at HOT CHIPS 2003, Stanford University, USA 2003.
- [M93] Maurer, U.: Secret key agreement by public discussion. IEEE Transactions on Information Theory 39 (1993) 733-742.
- [J05] Juels, A., Weis, S.: Authenticating Pervasive Devices with Human Protocols. The 25th Annual International Cryptology Conference Crypto'05, August 14-18, 2005, Santa Barbara, California, USA. (To appear).
- [VW05] Volkmer, M., Wallner, S.: Lightweight Key Exchange and Stream Cipher based solely on Tree Parity Machines ECRYPT (European Network of Excellence for Cryptology) Workshop on RFID and Lightweight Crypto, July 14-15th 2005, Graz University of Technology, Graz, Austria, 102-113.
- [KKK02] Ido Kanter, Wolfgang Kinzel and Eran Kanter, Secure exchange of information by synchronization of neural networks, Europhysics Letters 57(3), 141-147, 2002.