Elif Bilge Kavun

Resource-efficient Cryptography for Ubiquitous Computing:
Lightweight Cryptographic Primitives from a Hardware & Software Perspective

Kurzfassung

Ressourcen-effiziente Kryptographie für Ubiquitous Computing: Kryptographische Primitive aus einer Hardware & Software Perspektive

Technologische Fortschritte in der Halbleiterindustrie in den letzten Jahrzehnten haben die Massenproduktion von Mikrorechnern möglich gemacht. Dank der Kompaktheit und Mobilität dieser Geräte können diese "durchdringend" eingesetzt werden, mit anderen Worten, überall und an jedem Ort – wie in Smart Homes, Logistik, E-Commerce, und Medizintechnik. Das Einbetten der kleinen Controller in Alltagsgegenstände zeigt die zunehmende Realisierung des prophezeiten "Ubiquitous Computing" Konzepts. Allerdings bringt dieses neue Paradigma und sein Massenseinsatz auch neue Bedrohungen mit sich – vor allem mit Blick auf Datenschutz und Privatsphäre.

Viele Menschen kritisieren aktuelle Sicherheitskonzepte in diesem allgegenwärtigen Kontext. Es wird sogar angenommen, dass ein unzureichendes Sicherheitsniveau die größte Barriere für den langfristigen Erfolg des Ubiquitous Computing sein könnte. Anders als in traditionellen Bereichen der Datenverarbeitung sind das Angreifermodell und die Sicherheitslevel nicht die gleichen. Dies liegt vor allem an den begrenzten Ressourcen in Mikrokontrollern und Chips – Chipfläche, Rechenleistung, und Energie sind ökonomisch bedingte Einschränkungen für solche Geräte. Aus diesem Grund sind die vorhandenen Verschlüsselungslösungen für die neuen, allgegenwärtigen Anwendungen in der Regel nicht tauglich. Um das Sicherheitsproblem der ressourcenbeschränkte Geräte zu adressieren wurde das Forschungsgebiet der "Hocheffizienten Kryptographie" vor über einem Jahrzehnt definiert. In diesem Gebiet wurden bereits viele verschiedene kryptographische Primitive vorgeschlagen. Die veröffentlichten Arbeiten beschäftigen sich bisher meist mit der Kostenreduktion bei Implementierungen in Hardware (d.h. wenn ein eigener Chip gebaut werden soll). Dies ist jedoch nicht die einzige wichtige Metrik für solche Geräte. Je nach Anwendung brauchen ressourcenbeschränkte Geräte eine Chiffre, die in einem Taktzyklus ausgeführt werden kann und trotzdem ein hohes Sicherheitsniveau bietet. Ferner, da die meisten durchdringend Anwendungen in Software auf Mikrocontrollern implementiert werden, gibt es auch hier Bedarf für geeignete Chiffren mit effizienter Codegröße und Ausführungszeit.

In dieser Arbeit bezeichnen wir die Hocheffiziente Kryptographie auch als "Ressourceneffiziente Kryptographie" und wir wollen neue "Ressourcen-effiziente" Lösungen für ressourcenbeschränkte Geräte bieten, die die genannten Lücken adressieren. Wir beginnen mit Untersuchungen von bestehenden Primitiven, deren Characteristika wir auf verschiedenen Plattformen präsentieren. Angesichts unserer ersten Untersuchungen schlagen wir zunächst eine neue Blockchiffre mit dem Namen PRINCE vor, die besonders wenig Chipfläche und Ausführungszeit benötigt. Danach zielen wir auf Softwareimplementierungen auf Mikrocontrollern. Der erste Schritt in diese Richtung ist ein Hardware/Software Codesign genannt NLU ISE, das sich an

den 8-Bit-AVR-Befehlssatz der weit verbreiteten Atmel Mikrocontroller-Familie richtet. Danach definieren wir eine weitere neue Chiffre optimiert für den Einsatz in Software (ohne notwendige Hardwareerweiterung) die den Namen PRIDE trägt.

Zusätzlich zu unserem Beitrag zu effizienten Implementierungen im ersten Teil dieser Arbeit präsentieren wir damit zwei neuartige Designs; die Chiffren PRINCE und PRIDE erreichen besten bisher veröffentlichten akademischen Ergebnisse. Ergebnisse zu Untersuchungen von Harware/Software Codesign ermutigen weitere Codesigns von verschiedenen Chiffren auf verschiedenen Mikrocontroller. Natürlich ist es nicht einfach, alle aktuellen Lücken in der Hocheffizienten Kryptographie in nur einer Arbeit zu überwinden, daher sind andere Konzepte und Lösungen sowie die Adressierung von verschiedene Metriken offene Forschungsprobleme für Nachfolgearbeiten.

Schlagworte.

Hocheffiziente Kryptographie, Ressourcen-effiziente Kryptographie, Entwurf, Ubiquitous Computing, symmetrische Kryptographie, Blockchiffre, Hashfunktion, Hardware Implementierung, Software Implementierung, ASIC, FPGA, Mikrocontroller, Atmel AVR, IT-Sicherheit