Post Quantum Cryptography: Implementing Alternative Public Key Schemes on Embedded Devices

Stefan Heyse

Nahezu alle heutigen Sicherheitssysteme beruhen auf kryptographischen Primitiven als Kernkomponenten, welche in der Regel als vertrauenswürdigster Teil des Sytems gelten. Die Realisierung dieser Primitiven auf der zugrunde liegenden Plattform spielt eine entscheidende Rolle für jeden realen Einsatz. In dieser Arbeit diskutieren wir neue Primitiven für Public-Key-Kryptographie, die sich als potenzielle Alternativen zu den derzeit verwendeten RSA und ECC Kryptosystemen etablieren könnten. Die Analyse dieser Primitiven im ersten Teil der Arbeit aus der Perspektive eines Entwicklers, zeigt die Vorteile der neuen Systeme. Darüber hinaus untersuchen wir durch die Implementierung auf eingebetteten Systemen mit eingeschränkten Ressourcen, ob sich diese Verfahren bereits zu echten Alternativen entwickelt haben.

Die zweite und wichtigste Teil der Arbeit untersucht das Potenzial der kodierungsbasierten Kryptographie, namentlich das McEliece und Niederreiter Kryptosystem. Nach einer Diskussion der klassischen Beschreibung und einer modernen Variante, bewerten wir verschiedene Umsetzungsaspekte, z. B. Decoder, Encoder und Festgewichtskonvertierungen um CCA2-Sicherheit zu erreichen. Anschließend evaluieren wir die Leistung der Systeme mit einfachen binären Goppa Codes, quasi-dyadischen Goppa Codes und quasi-zyklischen MDPC Codes auf Mikrocontroller der Smartcard-Klasse und einer Reihe von FPGAs. Darüberhinaus weisen wir auf Schwächen in einer einfachen Implementierung hin, die den geheimen Schlüssel oder den Klartext mittels Seitenkanal-Angriffen extrahieren können.

Der dritte Teil präsentiert zwei weitere alternative Kryptosysteme. Zunächst untersucht wir die vielversprechendsten Mitglieder der MQPKS-Familie und deren Varianten, UOV, Rainbow und enTTS. UOV widerstand allen Arten von Angriffen für 13 Jahre und kann als eines der bestuntersuchtesten MQPKS angesehen werden. Wir evaluieren Implementierungen von UOV, Rainbow und enTTS auf einem 8-Bit-Mikrocontroller. Um das Problem der großen Schlüssel zu addressieren, haben wir einige Optimierungen implementiert, sowie das 0/1-UOV Schemata implementiert. Um eine praktisch nutzbare Sicherheitsstufe auf dem ausgewählten Gerät zu gewährleisten, werden alle jüngsten Angriffe zusammengefasst und Parameter für Standard-Sicherheitsstufen werden gegeben. Um die Skalierung zu beurteilen, werden die Verfahren mit den gängigsten Sicherheitsstufen für eingebetteten Systeme 2^{64}, 2^{80} und 2^{128} bits symmetrischer Sicherheit implementiert. Der zweite Beitrag ist eine Umsetzung des modernen symmetrischen Authentifizierungsprotokoll Lapin, welches auf dem Ring-LPN-Problem basiert. Wir zeigen dass, mit klassischen AES-basierten Protokollen verglichen, Lapin einen sehr kompakte Speicherbedarf hat, während zur gleichen Zeit eine Leistung in der gleichen Größenordnung erreicht wird.