Kurzfassung

Effiziente Implementierung von Codierungs- und Hash-basierter Kryptographie – Ingo von Maurich

Die Vielzahl verschlüsselter Verbindungen im Internet wird mit Hilfe sogenannter Public-Key Kryptographie hergestellt. Weitverbreitete Standards für Public-Key Verschlüsselung, digitale Signaturen sowie Protokolle zur Schlüsselvereinbarung und -verteilung stellen Authentizität, Vertraulichkeit, Integrität und Nicht-Zurückweisbarkeit der Verbindungen sicher. Die Sicherheit der eingesetzten Verfahren lässt sich dabei auf zwei miteinander verwandte Annahmen reduzieren: die Schwierigkeit der Primfaktorzerlegung großer Zahlen bei RSA-basierten Verfahren und dem diskreten Logarithmus-Problem bei DH- und ECC-basierten Verfahren. Wenn auch unwahrscheinlich, so ist es nicht ausgeschlossen, dass keine kryptanalytischen Fortschritte mehr bei der Lösung dieser Probleme erzielt werden und dadurch die Annahmen heute weitverbreiteter Verfahren der Public-Key Kryptographie ihre Gültigkeit verlieren. Die Verfügbarkeit eines skalierbaren Quantencomputers würde die getroffenen Annahmen ebenfalls außer Kraft setzen, da der Shor-Quantenalgorithmus beide Probleme effizient in Polynomialzeit löst. Betrachtet man zudem die langen Übergangszeiten zu neuen kryptographischen Standards, z.B. im Bankensektor, so wird deutlich, dass alternative Public-Key Kryptosysteme frühzeitig untersucht und geeignete Kandidaten identifiziert werden müssen. In Anbetracht dieser Situation hat der NSA Central Security Service kürzlich in einer Pressemitteilung angekündigt die kryptographischen Algorithmen für „Secret“ und „Top Secret“ klassifizierte Daten auf quantenresistente Algorithmen umzustellen und rät, so noch nicht geschehen, sogar davon ab den Wechsel von RSA- auf ECC-basierte Kryptographie vorzunehmen und stattdessen quantenresistente Kryptographie einzusetzen. Des Weiteren initiierte das National Institute of Standards and Technology (NIST) den Standardisierungsprozess für quantenresistente Kryptographie.

In diesem Kontext werden in der vorliegenden Arbeit neuartige Techniken zur effizienten Implementierung alternativer Kryptographieverfahren aus den Familien der codierungs- und hash-basierten Kryptographie untersucht, um Public-Key Verschlüsselung, hybride Verschlüsselung und digitale Signaturen zu realisieren. Insbesondere liegt der Fokus dabei auf maßgeschneiderten Designs für eingebettete Systeme wie FPGAs und Mikrocontroller und deren Konkurrenzfähigkeit im Vergleich zu heutigen RSA und ECC Implementierungen. Quantenresistente Public-Key Verschlüsselung wird in dieser Arbeit auf Basis zweier vielversprechender Verfahren realisiert die der Codierungstheorie entstammen: McEliece und Niederreiter. Beide Verschlüsselungsverfahren werden mit QC-MDPC Codes instanziiert, welche im Vergleich zu binären Goppa Codes kleinere Schlüssel und leichtgewichtige Implementierungen ermöglichen. Wir entwickeln hoch performante und flächeneffiziente FPGA Prozessoren die die heutigen RSA und ECC Implementierungen leistungsmäßig übertreffen können. Zudem werden erste Seitenkanalangriffe und Gegenmaßnahmen ebenso wie IND-CCA-sichere hybride Verschlüsselung für ARM Cortex-M Mikrocontroller präsentiert. Quantenresistente digitale Signaturen werden in dieser Arbeit mithilfe von hash-basierten Signaturen durch Kombination des Merkle Signaturschemas mit Winternitz Einwegsignaturen realisiert. Wir entwickeln neuartige algorithmische Verbesserungen für die Berechnung des Authentifikationspfades und zeigen wie das Design den Verlust von Schlüsselinformationen durch Seitenkanäle begrenzt.

Schlagworte. Public-Key Verschlüsselung, Digitale Signaturen, Codierungs-basierte Kryptographie, Hash-basierte Kryptographie, Quantenresistenz, Eingebettete Systeme, FPGAs, Mikrocontroller