Kurzfassung: Effiziente Implementierung Idealgitter-basierter Kryptographie

Antragsteller: Thomas Pöppelmann

Digitale Signatur- und Public-Key Verschlüsselung werden für nahezu jede sichere Kommunikation über das Internet oder zwischen eingebetteten Systemen benötigt. Die Sicherheit basiert dabei entweder auf der Faktorisierungsannahme (RSA) oder der Annahme, dass es schwer ist, das diskrete Logarithmus-Problem (DSA/ECDSA) zu lösen. Durch Fortschritte in der klassischen Kryptanalyse oder bei der Entwicklung von Quantencomputern, könnten diese Probleme allerdings in Zukunft ernsthaft geschwächt oder gelöst werden. Daher ist Forschung zu alternativen Public-Key Kryptosystemen erforderlich, die in der Lage sind, auch in diesem Fall Langzeitsicherheit zu gewährleisten.

In dieser Arbeit wird die effiziente Implementierung von alternativen Public-Key Kryptosysteme betrachtet, deren Sicherheit auf harten Problemen in Idealgittern basiert. Während in der Literatur bereits ein umfangreicher theoretischer Hintergrund zu Kryptographie basierend auf Gittern und Idealgittern vorhanden ist, ist die Effizienz solcher Konstruktionen, insbesondere auf eingeschränkten und kostensensitiven Plattformen, noch nicht gut untersucht. In dieser Arbeit werden daher neuartige Algorithmen und Implementierungstechniken für schnelle und flexible Polynommultiplikation und das Erzeugen von diskret normalverteilten Polynomen diskutiert. Diese Bausteine werden anschließend genutzt um Public-Key Verschlüsselungs- und digitale Signaturverfahren zu implementieren. Im Ergebnis kann nachgewiesen werden, dass gitterbasierte Systeme hohe Leistung erreichen und effizient auf Embedded-Mikrocontrollern und rekonfigurierbarer Hardware realisiert werden können. Ein Public-Key Verschlüsselungsverfahren basierend auf dem Ring Learning With Errors Problem (RLWE) oder das gitterbasierte Signaturschema BLISS übertreffen sogar klassische ECC- und RSA-basierte Implementierungen.

Gitterbasierte Kryptographie kann auch verwendet werden, um homomorphe Verschlüsselungsverfahren zu konstruieren, die das Durchführen von Rechenoperationen auf verschlüsselten Daten ermöglichen. Aufgrund der großen Parametersätze und umfangreicher Berechnungen, selbst für einfache Operation, ist die praktische Anwendbarkeit derzeit unklar. In dieser Arbeit werden daher Möglichkeiten betrachtet, um homomorphe Verschlüsselung in einer Cloud-Umgebung mit Hilfe von rekonfigurierbarer Hardware zu beschleunigen. Die vorgestellte Implementierung des homomorphen Verschlüsselungsverfahrens YASHE erlaubt das Durchführen aller Operationen, die für die Berechnung auf verschlüsselten Daten benötigt werden. Ein besonderer Fokus liegt auf der Entwicklung neuer Konzepte, um mit den großen Geheimtexten und Schlüsseln sowie begrenzter Speicherbandbreite umzugehen.