Zusammenfassung | Call 11 | Projekt ID 1866

1. Projektziel

In ein paar Jahren wird das Internet der Dinge (IoT) 50 Milliarden intelligente Geräte vernetzen, die vollkommen autonom miteinander interagieren und Daten an Server in einer Cloud senden bzw. von dort gesteuert werden. Eine der größten Herausforderungen für praktische IoT-Anwendungen ist die Sicherheit und Zuverlässigkeit der Daten, die von den Geräten gesammelt, übertragen und ausgewertet werden. So gut wie alle heute verwendeten kryptografischen Algorithmen und Protokolle (z.B. TLS) werden in nicht allzu ferner Zukunft unsicher sein weil sie mit Hilfe eines Quantencomputers relativ einfach geknackt werden können. Im Rahmen dieses Projekts wurde ein Prototyp eines TLS-ähnlichen sicheren Kommunikationsprotokolls für das IoT entwickelt, welches kryptografischen Angriffen mit zukünftigen Quantencomputern standhält. Dazu wurde das NTRU-Verschlüsselungssystem, das gegen solche Quanten-kryptanalytischen Angriffe resistent ist, implementiert und in die Open-Source DTLS-Software TinyDTLS integriert. Um sicher zu stellen, dass NTRU auch auf IoT- Kleingeräten mit 8, 16 und 32-bit Mikrocontrollern lauffähig ist, wurden alle Performance-kritischen Teile, insbesondere die Polynom-Arithmetik und die Hashfunktion SHA-2, in Assembler implementiert.

2. Projektendergebnisse

1	*Source-Code des NTRU-Verschlüsselungssystems (mit Assembler-Optimierungen für Polynom-Arithmetik und SHA-2)*	*GPLv3*	*github.com/grojoh/quasikom/tree/master/src/ntru*
2	*Source-Code der um das NTRU-Verschlüsselungssystem erweiterten TinyDTLS Software*	*EPLv1*	*github.com/grojoh/quasikom/tree/master/src/ntru*
3	*Entwickler-Dokumentation*	*CC-BY-SA*	*netidee.at/quasikom*
4	*Wissenschaftlicher Fachartikel über die Implementierung der Hashfunktion SHA-512 (wurde bei SECITC 2018 präsentiert)*	*CC-BY-SA*	*netidee.at/quasikom/secitc2018*
5	*Wissenschaftlicher Fachartikel über die Implementierung der Polynom-Arithmetik (wird bei WISTP 2018 präsentiert)*	*CC-BY-SA*	*netidee.at/quasikom/wistp2018*
6	*Projekt-Endbericht*	*CC-BY-SA*	*netidee.at/quasikom*

3. Geplante weiterführende Aktivitäten nach netidee-Projektende

Sowohl die NTRU-Implementierung als auch die TinyDTLS-Software werden nach Projektende in zwei Richtungen weiter entwickelt. Im November 2017 wurde im Rahmen einer Initiative des amerikanischen National Institute of Standards and Technology (NIST) zur Standardisierung von Post-Quanten-Kryptografie eine neue Version von NTRU vorgestellt, die sich erheblich von der aktuellen Version unterscheidet und einige Verbesserungen mit sich bringt. Es ist geplant, die zurzeit in TinyDTLS integrierte NTRU-Version durch die neue Version zu ersetzen. Auch bei TinyDTLS selbst gibt es noch viel Potential für Optimierungen, insbesondere um den Speicherverbrauch zu reduzieren und die Laufzeit weiter zu verbessern. Es ist geplant, NTRU auch in zukünftige Versionen von TinyDTLS zu integrieren.

4. Anregungen für Weiterentwicklungen durch Dritte

Die um NTRU erweiterte TinyDTLS-Implementierung ist in erster Linie für Entwickler von IoT-Anwendungen interessant und kann im Prinzip in jedem Projekt zum Einsatz kommen, in dem sensible Daten zwischen zwei IoT-Geräten übertragen werden müssen. Typische Beispiele sind Anwendungen in der Medizintechnik oder im Bereich “Home Automation” bzw. “Smart Home”.