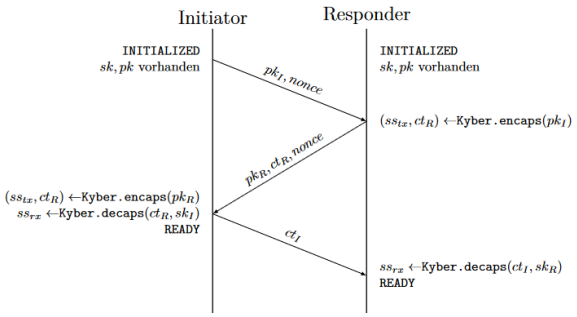
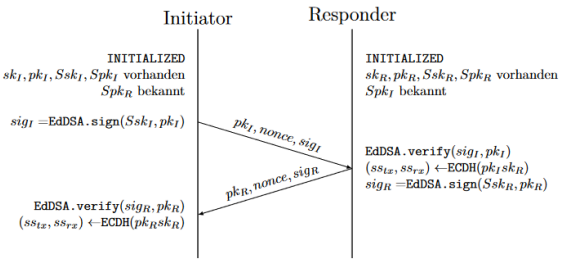
Quantensichere Verschlüsselung für CSP

Das Cubesat Space Protocol (CSP) wird für die Datenübertragung bei Cubesats genutzt. Um die Kommunikation zu verschlüsseln, wurde eine Library gebaut, welche klassische, wie auch Post-Quantum Public-Key Systeme kombiniert, um die quantensichere Verschlüsselung zu ermöglichen.



Authentifizierter Schlüsselaustausch mit ECC



Schlüsselaustausch mit dem quantensicheren Kyber Algorithmus

Ausgangslage

Das Cubesat Space Protocol(CSP) wird als Übertragungsprotokoll zwischen Cubesats genutzt. Der Übertragungskanal zwischen Bodenstation und dem Satelliten ist zwangsläufig exponiert für Abhörattacken. Der mögliche Eintritt in die Post-Quantum-Ära verschärft das Risiko für die Datenkommunikation zusätzlich, indem die Sicherheit herkömmlicher Kryptographieverfahren abgeschwächt wird.

Elliptic Curve Cryptography

Elliptic Curve Cryptography (ECC) gehört zu den Pre-Quantum Systemen und basiert auf endlichen Körpern über elliptische Kurven. Die Sicherheit basiert auf dem diskreten Logarithmusproblem. Dadurch ist sie anfällig auf Angriffe von Quantencomputern.

Post-Quantum Cryptography

Mögliche Verfahren für eine quantensichere Verschlüsselung werden aktuell geprüft. Auch wenn die Standardisierung noch nicht abgeschlossen ist, wirken die Algorithmen der Cryptographic Suite for Algebraic Lattices (CRYSTALS) erfolgsversprechend. Sie basieren auf dem Gitterproblem, wodurch sie nicht anfällig gegenüber Quantencomputern sind.

Umsetzung

Es wurde eine standalone Library entwickelt, die zwei verschiedene Schlüsselaustauschverfahren ermöglicht, und Funktionen zur Ver- und Entschlüsselung des Datenverkehrs bereitstellt. Beide Verfahren sind mit ECC und den Post-Quantum Systemen umgesetzt. Der Hauptteil der Arbeit fiel bei den Schlüsselaustauschverfahren an. Für die kryptografischen Primitiven wurde auf weitere Libraries zurückgegriffen. Die Library an sich kann für beliebige Kommunikationsprotokolle verwendet werden. Die Implementation in CSP konnte noch nicht abschliessend durchgeführt werden.

Cubesats und das CSP

Cubesats sind modulare Kleinsatelliten, die hauptsächlich für die Forschung und Amateurprojekte eingesetzt werden. Aufgrund der Modularität und den Limitierungen der geringen Grösse, wurde das CSP spezifiziert.

CSP wurde entwickelt für die flexible Vernetzung verteilter Systeme. Es ist stark inspiriert vom TCP/IP Modell und kann die Netzwerk- und Transportschicht zur Verfügung stellen. Es ist sehr ressourceneffizient, sodass es auch auf kleinen Mikrocontrollern implementiert werden kann.

Arbeitsgruppe:
Pascal Michel

Auftraggeber:
Ateleris GmbH, Brugg

Betreuer:
Prof. Dr. Christoph Wildfeuer