Entwicklung und Validierung von post-Quanten-sicheren Kryptoverfahren auf Hardware-Security-Modulen (HSM)

Erläuterung der Problemstellung, die mit der Idee gelöst werden soll:

Schon jetzt verwendet die Bundeswehr eine Public-Key-Infrastruktur (PKI), um Nutzern in Netzwerken bestimmte Rechte einzuräumen oder zu entziehen. In Zukunft wird auch das Cloud-Computing stärker in den Fokus militärischer Anwendung rücken. Zusätzlich ist es denkbar, dass Schlüsselmittel nicht mehr symmetrisch und auf speziell dafür entwickelter Hardware transportiert werden, sondern diese in geschützten Netzen oder „Over the Air" übertragen werden. Auch sind mannigfaltige Anwendungsmöglichkeiten asymmetrischer Kryptoverfahren für die Kommunikation über Satelliten, zu Kampfflugzeugen bis hin zu Soldaten-Funkgeräten vorstellbar. Hierbei ist vor allem die Authentifizierung und Kommunikation untereinander von Bedeutung, zwischen Maschine und Maschine, zwischen Mensch und Maschine als auch zwischen Mensch und Mensch.

Aktuellen und zukünftigen Anwendungen für sichere Kommunikation liegen asymmetrische Kryptoverfahren zu Grunde. Für den hochsicheren militärischen Bereich wird zusätzlich spezielle Hardware, sogenannte Hardware-Security-Module (HSM), benötigt. Diese kleinen Geräte ermöglichen die sichere Ausführung von kryptografischen Operationen und bilden somit die Grundlage für eine sichere Kommunikation. Jedoch haben all diese Geräte einen Schwachpunkt, welcher sich aus der Angreifbarkeit der eingesetzten asymmetrischen Algorithmen durch zukünftige Quantencomputer ergibt. Eine sichere Kommunikation kann damit nicht mehr gewährleistet werden. Ähnliches gilt für Operationen auf der Cloud, weil sie heute auf den Klardaten ausgeführt werden müssen.

Beschreibung der Idee und wie sie das Problem lösen soll:

Die Grundidee zur Lösung dieser Probleme besteht in der Weiterentwicklung von bestehenden post-Quanten-sicheren Kryptoalgorithmen und ihrer Implementierung auf Hardware-Security-Modulen. Dabei sollen die angewandten post-Quanten-sicheren asymmetrischen Algorithmen das komplette Spektrum aller Anwendungsfälle umfassen, vom asymmetrischen Schlüsselaustausch über die digitale Signierung bis zur Authentifizierung und der Anwendung von homomorphen Verschlüsselungsverfahren. Somit ist es möglich, auch in einem Zeitalter vor Verwendung von Quantencomputern, Geheimnisse so zu verschlüsseln, das sie auch in der Zukunft nicht entschlüsselbar sind. Natürlich wäre man damit auch in einem Post-Quanten-Zeitalter vor Attacken mit Quantencomputern geschützt und durch homomporphe Verschlüsselung eine Grundlage für eine Weiterentwicklung von sicherem Cloud-Computing gelegt. Die konkrete technische Realisierung besteht dabei im Kern aus zwei aufeinander aufbauenden Bausteinen. Zum einen müssen die vorhandenen post-Quanten-sicheren Kryptoalgorithmen mathematisch weiterentwickelt werden. Zum anderen müssen sichere Algorithmen aus der mathematischen Beschreibung hergeleitet werden, welche die vielen bestehenden anderweitigen Angriffsformen unterbinden. Hierbei sei vor allem an die Möglichkeit von Seitenkanalangriffen erinnert. Darüber hinaus müssen die Algorithmen sodann sicher auf Hardware-Security-Modulen implementiert werden und die Schnittstellen zu vorhandenen

Systemen angepasst werden. Die geeignete Hardware-Basis liegt bereits vor. So können HSMs mit verfügbaren Chips (Field Programmable Gate Array), die eine sichere und schnelle Verwendung der angedachten Algorithmen ermöglichen, bestückt werden. Erste post-Quanten-sichere Algorithmen liegen vor, jedoch ist vor allem in den mathematischen Grundlagen und auf dem Gebiet der konkreten Algorithmenentwicklung noch viel Arbeit zu leisten. Die drei zentralen Akteure sind die Bundeswehr, die Wissenschaft und die Industrie. Die Wissenschaft sollte in Zusammenarbeit mit der Industrie die theoretischen Fragen so weit wie möglich klären. Die Industrie sollte dann konkrete Implementierungen auf HSMs anbieten, welche auf die Anforderungen der Bundeswehr zugeschnitten sind. Die Bundeswehr muss dann den Übergang von nicht post-Quanten-sicherer Kryptografie zur post-Quanten-sicheren Kryptografie gewährleisten.

THALES

Voll homomorphe und post-quanten-sichere Kryptoalgorithmik auf Hardware

Sicheres Cloud-Computing für die kommenden Dekaden

D.Jantner und K.Hauber

Ein zukünftiges Szenario des Cloud Computing

Kommunikation mit der Cloud

COMBAT CLOUD

Komplexe und sensible Anwendungen finden in der Cloud statt

Kommunikation mit der Cloud

Kommunikation mit der Cloud

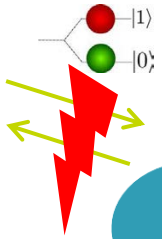
Kommunikation mit der Cloud

Kommunikation mit der Cloud

Denkbare Anwendungsfälle:
- **FCAS**
- **Künstliche Intelligenz**

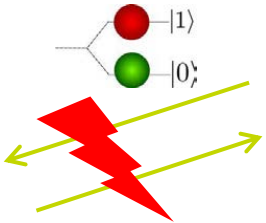
THALES

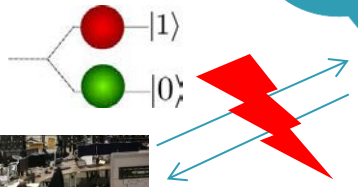
1. Angriffsmöglichkeit: Quantencomputing (zu der Cloud)

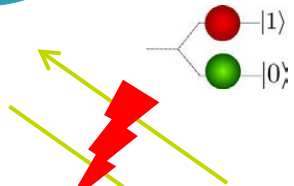


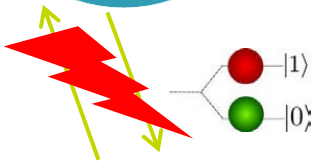
COMBAT CLOUD

Komplexe und sensible Anwendungen finden in der Cloud statt









Keine sichere Kommunikation zur Cloud mehr möglich, durch Angreifbarkeit von RSA, ECC

THALES

2. Angriffsmöglichkeit: NICHT homomorphe Verschlüsselung (in der Cloud)

Kommunikation mit der Cloud

COMBAT CLOUD

Operationelle Daten müssen im Klartext vorliegen

Kommunikation mit der Cloud

Kommunikation mit der Cloud

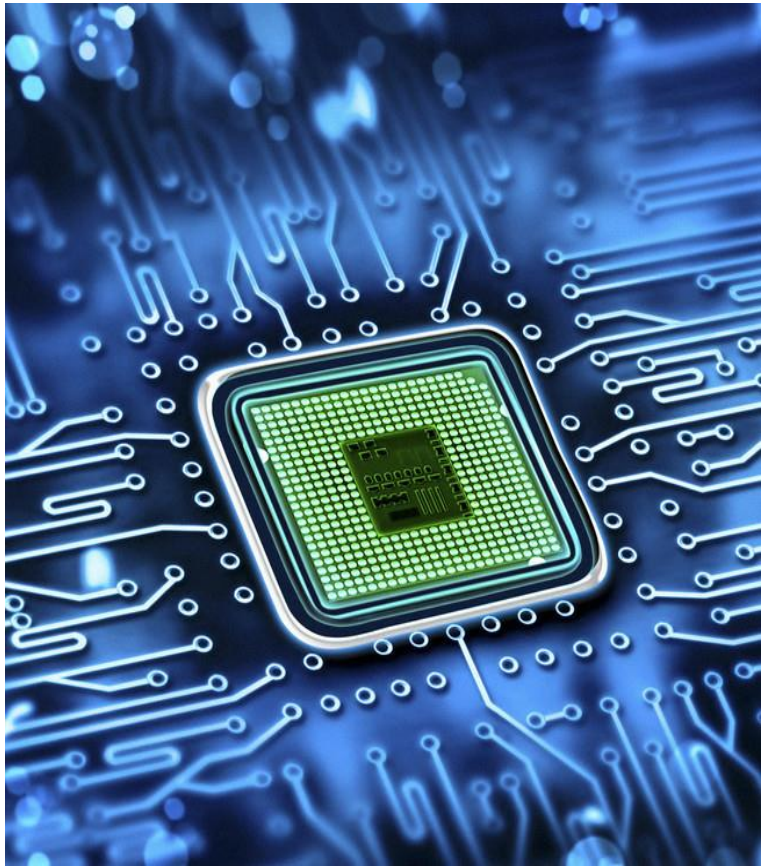
Kommunikation mit der Cloud

Kommunikation mit der Cloud

Kommunikation mit der Cloud

Grundlegende Problematik des Cloud Computing

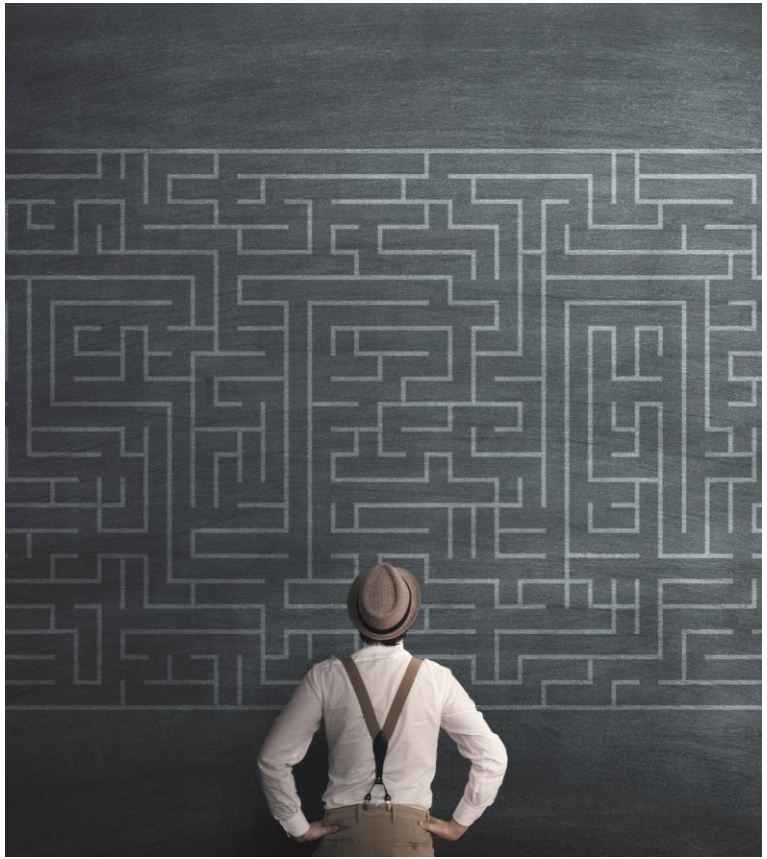
Gegenmittel zur Bedrohungsabwehr



Hardware Security Module auf einem FPGA:

- ✓ **Post-quanten sichere asymmetrische Algorithmen zur sicheren Kommunikation:**
  - Schlüsselaustausch
  - Digitale Signierung
  - Authentifizierung
- ✓ **Sichere voll homomorphe Verschlüsselungsalgorithmen**

Herausforderungen



- **Erste Algorithmen** auf Basis von Gittern, Supersingulären Isogenien etc. **existieren bereits**
- **Grundlagenforschung**
  - **Algorithmen**
  - **Algorithmischen Zahlentheorie**
- Algorithmen **effizient** und **sicher implementieren**
- **Schnittstellen** zu vorhandenen und zukünftigen Systemen müssen **angepasst werden**

Fazit

- **Sichere Kommunikation** für **Cloud Anwendungen** essentiell
- Sichere Kommunikation **bedroht durch:**
  - **Quanten Computer**
  - **nicht-homomorphe Verschlüsselung**
- Idee: **Hardware Security Module** mit **Algorithmen** für:
  - **post-quanten-sicherer Kommunikation**
  - **voll homomorpher Verschlüsselung**

→ Ermöglicht sicheres Cloud Computing auch für die kommenden Dekaden

Vielen Dank!

Kontakt:

Klaus Hauber
E-Mail: Klaus.HAUBER@thalesgroup.com

Daniela Jantner:
E-Mail: Daniela.JANTNER@thalesgroup.com

Thales Deutschland GmbH
Thalesplatz 1,
71254 Ditzingen

www.thalesgroup.com