IMES | Institut für Mikroelektronik und Embedded Systems
securosys

OST Ostschweizer Fachhochschule

# Quantencomputer-resistente Verschlüsselungsalgorithmen

## Fachbereich Mikroelektronik

Die Firma Securosys SA sichert mit ihren Produkten digitale Identitäten und Finanztransaktionen über öffentliche Telekommunikationsnetzwerke. Dafür entwickelt und vertreibt sie Hardware-Security-Module (HSM), welche unter anderem digitale Daten mit standardisierten Verfahren verschlüsseln und authentisieren.

### Gefahr Quantencomputer

Leistungsstarke Quantencomputer werden in Zukunft aktuelle kryptografische Verfahren brechen können. Auf jenen lässt sich Shors Algorithmus zum Berechnen von Primfaktoren und Logarithmen so effizient umsetzen, dass aktuelle Public-Key-Verfahren als geknackt gelten müssen. Sollte es eines Tages gelingen, einen Quantencomputer zu bauen, so steht die sichere Kommunikation via Internet vor einem riesigen Problem. Protokolle wie https, SSL/TLS, IPsec usw. würden mit einem Schlag unsicher und damit z. B. der Zahlungsverkehr über das Internet faktisch verunmöglicht. Dies stellt somit eine wesentliche Bedrohung für das künftige HSM-Business von Securosys dar.

### Lösungsansatz

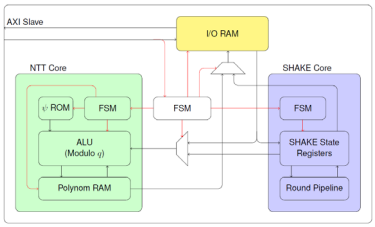
Zeitgleich mit dem Projekt am IMES findet ein von der NIST geleitetes internationales Forschungsprojekt statt, welches auf die Standardisierung von Quantencomputer-resistenten Verfahren abzielt. In mehreren Runden werden aus 69 vorgeschlagenen Verfahren die vielversprechendsten ausgewählt, im Detail analysiert und im besten Fall standardisiert. Verschiedene Algorithmen aus dem NIST Projekt wurden auf deren Praxistauglichkeit untersucht. Weiter wurde geprüft wie gut sich die zeitkritischen Rechenanteile zwecks Beschleunigung in einem FPGA umsetzen lassen. Neben diversen Angriffsszenarien wurden Durchsatz, Skalierbarkeit und Bedarf an Ressourcen auf dem FPGA berücksichtigt. Die Grundsatzfrage lautete: Ist es möglich, die bestehenden Verfahren mit Quantencomputerresistenten Verfahren zu ersetzen?

### Ergebnis

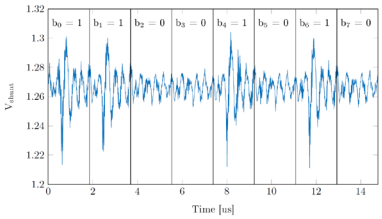
Unsere Erkenntnisse konnten an verschiedenen internationalen Top-Konferenzen publiziert werden. Als eines von wenigen Forschungsteams weltweit konnten wir FPGA Performance Daten zu den von uns untersuchten Algorithmen liefern. Konkret konnten wir die Latenzzeit der Berechnung einer SPHINCS+ Signatur auf 1 Millisekunde reduzieren. Dies entspricht einer Beschleunigung um den Faktor 6 verglichen mit dem bisherigen Rekord. Ein weiteres Highlight ist die Entdeckung und Publikation eines neuartigen Hardware-Angriffs auf das ansonsten vielversprechende NewHope Schlüsseltauschverfahren. Mit diesen Publikationen leistete das IMES einen essenziellen Beitrag ans NIST Forschungsprojekt. Durch das Projekt hat Securosys gegenüber seinen Mitbewerbern einen Kompetenzvorsprung. Dies ermöglicht eine schnellere Adaption, sobald die neuen Algorithmen standardisiert werden.

Mitfinanziert durch Innosuisse

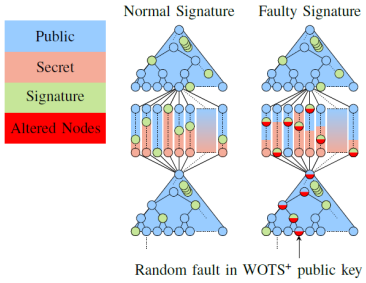
**Hardware-Security-Module (HSM) von Securosys**




**Architektur der New-Hope FPGA Implementation**




**Seitenkanalattacke auf New-Hope**




**Fault Attacke auf SPHINCS**

**Kontakt**
Prof. Dr. Paul Zbinden
OST – Ostschweizer Fachhochschule,
Campus Rapperswil-Jona
IMES Institut für Mikroelektronik und Embedded Systems
Oberseestrasse 10, 8640 Rapperswil
+41 58 257 45 84, paul.zbinden@ost.ch