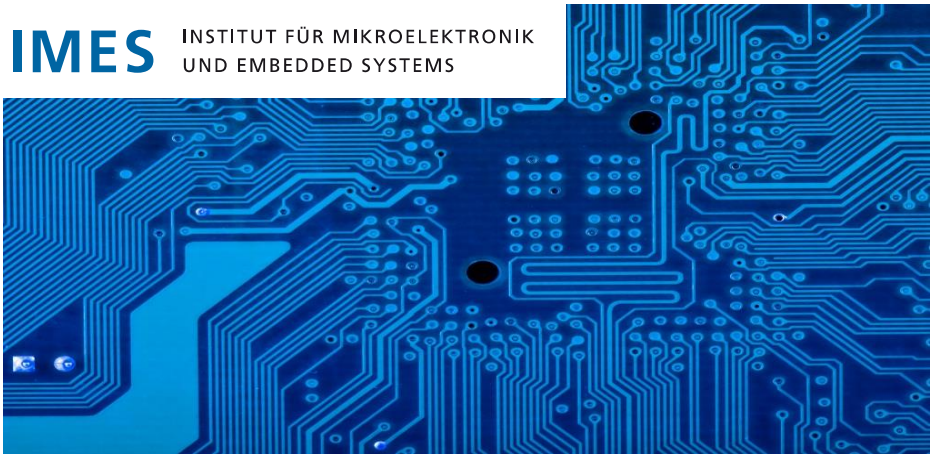
HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL
FHO Fachhochschule Ostschweiz

IMES INSTITUT FÜR MIKROELEKTRONIK UND EMBEDDED SYSTEMS

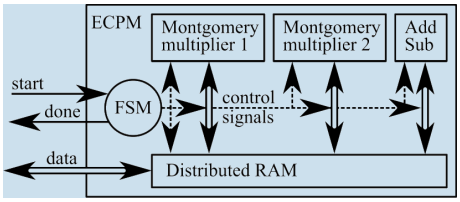


Fachbereich Mikroelektronik

Hacken für den Finanzplatz Schweiz

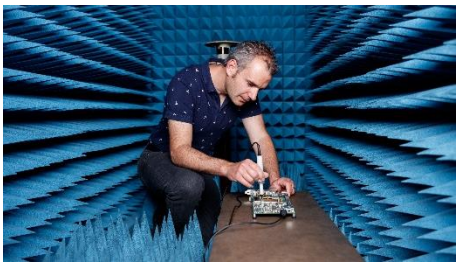
Ausgangslage

Die Firma Securosys SA hat sich zum Ziel gesetzt, mit ihren Produkten die Datenübertragung über öffentliche Telekommunikationsnetzwerke zu sichern. Dafür entwickeln sie Hardware-Security-Module (HSM), welche digitale Daten mit standardisierten Verfahren verschlüsselt und authentisiert.



Design

Bei HSMs gibt es zwei sich konkurrierende Ziele: höchste Sicherheit bei maximalem Datendurchsatz. Um die Daten schnell zu verarbeiten, werden rechenaufwändige Teile mittels dezidierter Hardware beschleunigt. Diese FPGA-basierte Beschleunigung hat das IMES entscheidend mitentwickelt.

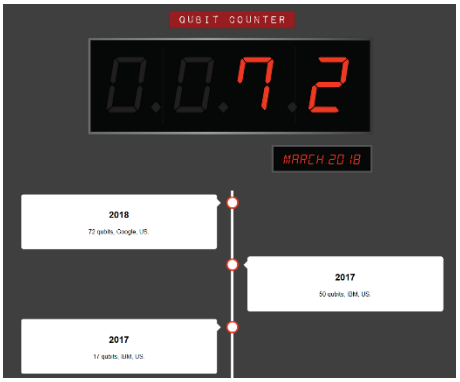


Strommessungen und Angriffe

Wird bei der Entwicklung nur auf den Datendurchsatz geachtet, kann ein System ohne Schutz vor Seitenkanalattacken entstehen. Dabei wird der Aufnahmestrom des Geräts gemessen und daraus auf die Abfolge der einzelnen Rechenoperationen geschlossen, was Rückschlüsse auf die geheimen Schlüssel zulässt. Um solche Angriffe auszuschliessen, hat das IMES die eigene Implementation angegriffen und so lange verbessert, bis keine relevanten Informationen mehr gemessen werden konnten.

Produkt

Unsere hardwarebeschleunigten Algorithmen sind in den HSMs der Firma Securosys integriert. Securosys verkauft diese erfolgreich. Der erste Grosskunde war SIX, der unter Aufsicht der Schweizerischen Nationalbank das Zahlungssystem SIC betreibt. Somit leistet das IMES bei jeder elektronischen Finanztransaktionen in der Schweiz einen Beitrag.



Neue Herausforderungen

Leistungsstarke Quantencomputer werden in Zukunft aktuelle kryptografischen Verfahren brechen können. Es gibt zwar Vorschläge für neue, resistente Verfahren, welche aber oft nur in Software verfügbar sind. In einem Nachfolgeprojekt untersucht das IMES solche Vorschläge und testet, ob sich die Algorithmen zur Hardwarebeschleunigung eignen. Somit erhält Securosys einen wichtigen technologischen Vorsprung. Durch die Publikation unserer Ergebnisse leistet das IMES zusätzlich einen substanzieller Beitrag an die aktuelle Standardisierung für neue Algorithmen.

Ihr Ansprechpartner: Prof. Dr. Paul Zbinden
Tel.: +41 (0)55 222 45 84
Email: pzbinden@hsr.ch