IMES | Institute for Microelectronics, Embedded Systems and Sensors

OST Eastern Switzerland University of Applied Sciences

Advanced System Technologies

Hacking for the Swiss Financial Center

The company Securosys SA has set itself the goal of securing data transmission over public telecom¬munications networks with its products. Therefore, they de¬velop hardware security modules (HSMs), which encrypt and authen¬ticate digital data using standard¬ized procedures.

Design

With HSMs, there are two competing goals: highest security and maximum data throughput. To process the data quickly, computationally intensive parts are accelerated using dedicated hardware. This FPGA-based acceleration was significantly co-developed by IMES.

Current measurements and attacks

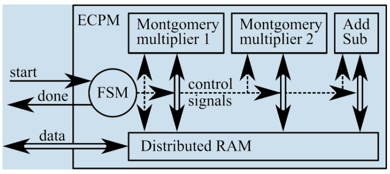
If only data throughput is considered during development, a system without protection against side-channel attacks can emerge. In this case, the device's power consumption is measured. This data trace is then used to identify the sequence of individual computing operations, which allows conclusions about the secret keys. To exclude such attacks, IMES attacked its own implementation and improved it until no relevant information could be measured anymore.

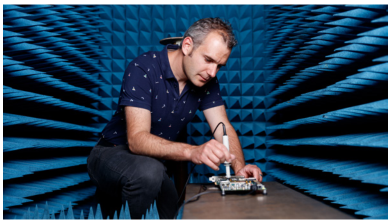
Product

Our hardware-accelerated algorithms are integrated into the HSMs of the company Securosys, which sells these devices successfully. The first major customer was SIX, which operates the SIC payment system under the supervision of the Swiss National Bank. Thus, IMES contributes to every electronic financial transaction in Switzerland.

New Challenges

Powerful quantum computers will be able to break current cryptographic methods in the future. There are proposals for new resistant methods, but these are often only available in software. In a follow-up project, IMES is investigating such proposals and testing whether the algorithms are suitable for hardware acceleration. This gives Securosys an important technological advantage. By publishing our results, IMES also makes a substantial contribution to the current standardization of new algorithms.





Contact
Prof. Dr. Paul Zbinden
OST – Ostschweizer Fachhochschule,
Campus Rapperswil-Jona
IMES Institute for Microelectronics, Embedded Systems and Sensors
Oberseestrasse 10, 8640 Rapperswil
+41 58 257 45 84, paul.zbinden@ost.ch