IMES | Institute for Microelectronics, Embedded Systems and Sensors

securosys

OST Eastern Switzerland University of Applied Sciences

Advanced System Technologies

Quantum computer-resistant cryptographic algorithms

Securosys SA secures digital identities and financial transactions via public telecommunications networks with its products. Therefore, Securosys develops and distributes hardware security modules (HSMs) that, among other things, encrypt and authenticate digital data by the use of standardized procedures.

Danger of quantum computers

Powerful quantum computers will be able to break some current cryptographic methods in the future. Shor's algorithm for calculating prime factors and logarithms can be implemented so efficiently on these computers that current public key procedures must be considered cracked. If the quantum computer can be built one day, secure communication via the internet will face a huge problem. Protocols such as https, SSL/TLS, IPsec etc. would become insecure in one fell swoop. This would, for example, make payment transactions over the internet effectively impossible and therefore represents a significant threat to the future HSM business of Securosys.

Solution approach

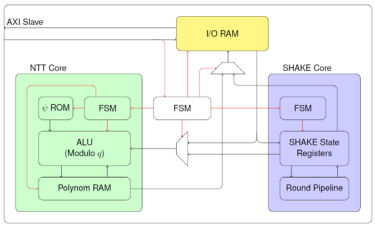
At the same time as this project at IMES, an international research project lead by NIST is taking place. The NIST project aims to standardize quantum computer-resistant methods. In several rounds, the most promising of 69 proposed methods are being selected, analyzed in detail and standardized. Various algorithms from the NIST project were analyzed for their practical suitability. It was also tested how well the time-consuming parts in the algorithms can be implemented in an FPGA for the purpose of acceleration. In addition to various attack scenarios, throughput, scalability and resource requirements on the FPGA were taken into account. The fundamental question was: Is it possible to replace the existing methods with quantum computer-resistant methods?

Result

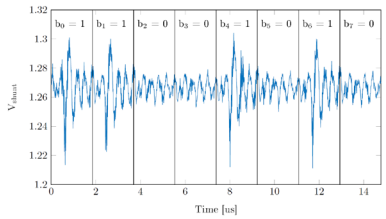
Our findings have been published at various international top conferences. We were one of a few research teams worldwide to deliver FPGA performance data for the algorithms we analyzed. Specifically, we were able to reduce the latency of the calculation of a SPHINCS+ signature to 1 millisecond. This corresponds to an acceleration by a factor of 6 compared to the previous record. Another highlight is the discovery and publication of a new type of hardware attack on the otherwise promising NewHope key exchange procedure. With these publications, IMES made an essential contribution to the NIST research project. The project has given Securosys a competence advantage over its competitors. This enables faster adaptation as soon as the new algorithms are standardized.

Co-financed by Innosuisse

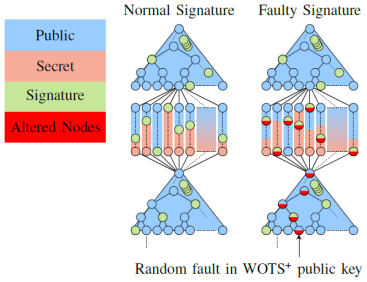
Hardware Security Modules (HSM) from Securosys



Architecture of the New-Hope FPGA implementation



Side channel attack on New Hope



Fault attack on SPHINCS

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