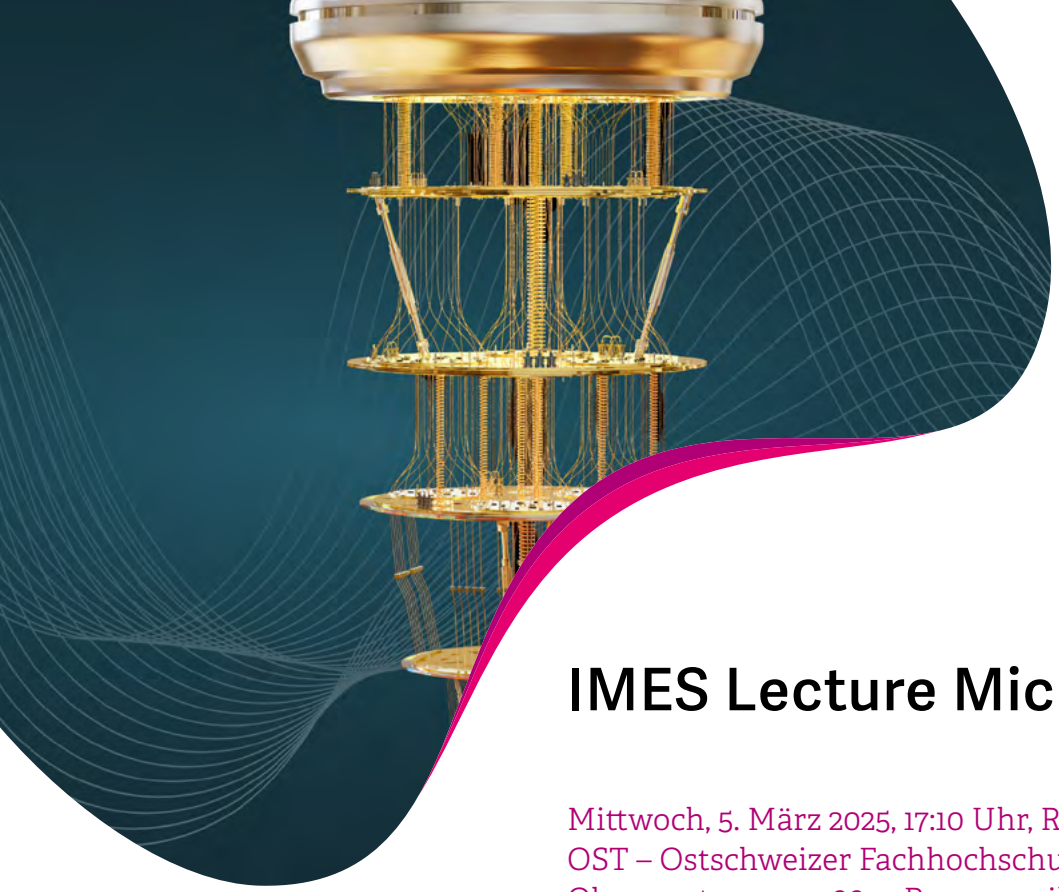

OST
Ostschweizer
Fachhochschule

WO WISSEN WIRKT.

IMES Lecture Microelectronics

Mittwoch, 5. März 2025, 17:10 Uhr, Raum 4.006a
OST – Ostschweizer Fachhochschule
Oberseestrasse 10, 8640 Rapperswil-Jona

IMES | Institut für Mikroelektronik,
Embedded Systems und Sensorik

IMES Lecture Microelectronics

PQC Kryptographie, State-of-Art und Herausforderungen

PQ-Kryptographie ist mit ihren veränderten Eigenschaften nicht einfach ein Algorithmus-Update, sondern eine disruptive Technologie in der digitalen Sicherheitslandschaft. Die Herausforderungen sind vielfältig und allgegenwärtig: Basistechnologien wie TLS und IKE sind betroffen, ebenso wie Authentifizierung, Datenbanken, Dateispeicherung und erst kürzlich in der Industrie etablierte Systeme, die auf MPC basieren. Für die PQC-Transition haben Gremien wie NIST und NSA Handlungsempfehlungen erlassen. Der Vortrag beleuchtet die praktischen Herausforderungen und Wege, diese in einem vernetzten Umfeld zu meistern.

Eine Strommessung knackt den quantencomputersicheren Schlüsseltausch

Im Vortrag wird zunächst ein von NIST standardisiertes, quantensicheres Schlüsselaustauschverfahren und dessen Umsetzung auf einem FPGA gezeigt. Diese wird auf Seitenkanalresistenz geprüft. Dabei wird zum Beispiel die Stromaufnahme während der Ausführung gemessen und so Rückschlüsse auf die verarbeiteten Daten gezogen. Diese Analyse offenbarte ein Seitenkanalproblem im Algorithmus.

Programm:

Mittwoch, 5. März 2025

17:10 Uhr — PQC Kryptographie, State-of-Art und Herausforderungen
Marcel Dasen, VP Engineering, Securosys SA

17:55 Uhr — Eine Strommessung knackt den quantencomputersicheren Schlüsseltausch
Dorian Amiet, Senior Research Engineer IMES Institut für Mikroelektronik, Embedded Systems und Sensorik

18:15 Uhr — Apéro