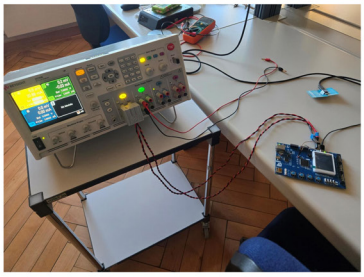
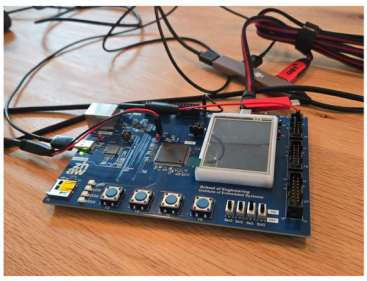
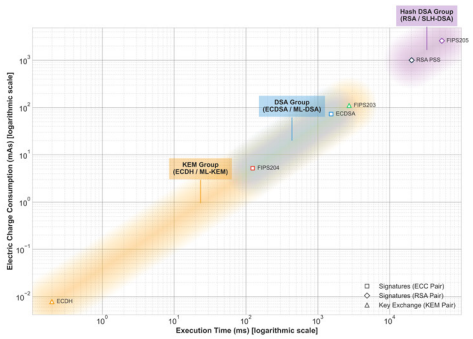
School of Engineering

Institute of Embedded Systems

Post Quantum Cryptography on Microcontrollers







- Quantum computers can break asymmetric cryptography
- Comparing new NIST post-quantum standards against classical algorithms
- Hardware-level benchmarking on an STM32
- Profiling of execution time, energy, and memory footprint
- Post-quantum is feasible, but demands hardware trade-offs

Bachelor Thesis FS26
Authors: Julien Wyss, Levin Hofer
Supervisor: Dr. Simon Künzli
www.zhaw.ch/ines