SaTC: CORE: Small: Finding and Mitigating Side-channel Leakage in Embedded Architectures

VIRGINIA TECH

WPI

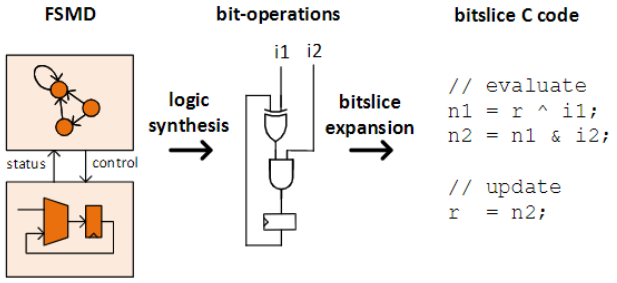
Challenge:

- Side-channel Leakage in software is hard to predict because hardware is unknown
- Countermeasures against implementation attacks hard to compose and verify

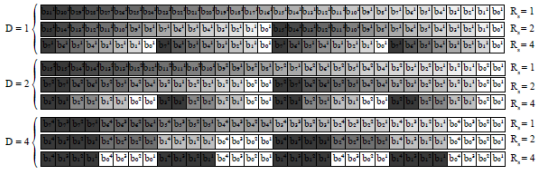
Solution:

- Use bit-slice representation to create a redundant representation of a program in Boolean logic
- Automatic conversion of Programs into bitsliced form using *Parallel Synchronous Programming*
- Demonstrated combined masking countermeasures and fault countermeasures on bitsliced software
- Demonstrated SKIVA: Bitslice-redundant RISC-V
- Built protected version of Dilithium Post Quantum Signature Algorithm

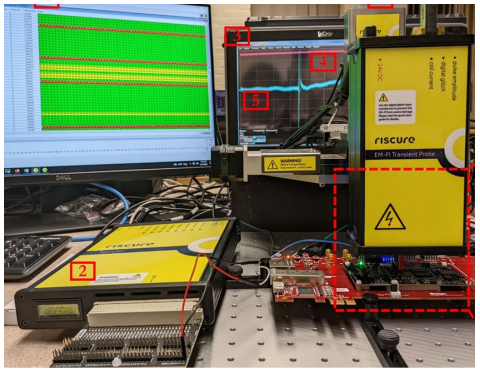
Bitslice Generation Principle



SKIVA-V Processor redundant slices on 32-bit



FI Prototype for Dilithium



Scientific Impact:

- Demonstrates that countermeasures and functionality (software) can be developed and verified separately
- Demonstrates a processor-independent countermeasure for implementation attacks
- Highlights open problems in bitslice programming

Broader Impact and Broader Participation:

- PSP Compiler is open source
- Supported 2 PhD, 2 MS
- Automatic generation of Boolean programs from PSP may be very useful for Homomorphic Encryption
- Demonstrated Saidoyoki Board
- Talks: Sabanci U (Turkey), FAU (Germany), UK RISE (UK), SOCC21
- 10 Conference Articles, 4 Journal Articles

Patrick Schaumont, William Diehl, Paul Ampadu
Award 1931639
October 2019 – September 2022