Side-channel analysis of SipHash in FPGA

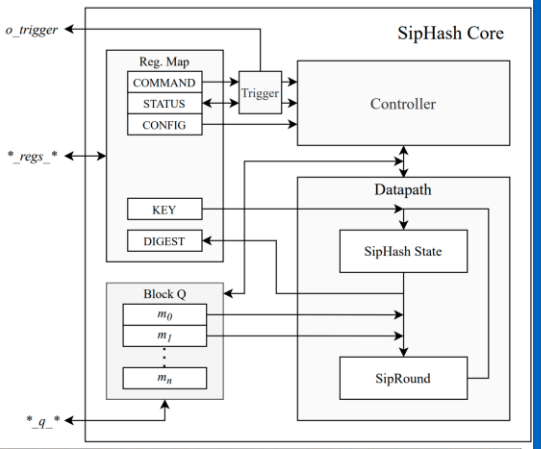
Ing. Vít Mašek
Faculty of Information Technology, Czech Technical University in Prague
Supervisor: Ing, Vojtěch Miškovský, Ph.D.

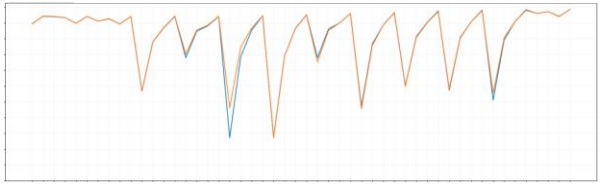
Motivation and Problem

- Modern cryptographic algorithms are often assessed only mathematically. In practice, hardware implementations can unintentionally leak sensitive data through physical channels such as power consumption or electromagnetic emissions.
- SipHash, a lightweight ARX-based cryptographic function, is widely used for authentication in network protocols and data structures. Although widely believed to resist side-channel attacks, recent research has challenged this assumption.
- This thesis investigates how a hardware implementation of SipHash behaves under power analysis attacks when deployed on an FPGA platform. The aim is to reveal potential weaknesses and assess the need for countermeasures.

SipHash Implementation in FPGA

- Artix-7 FPGA
- Modular and highly configurable
- 3.55 Gbps throughput
- Outperforms current designs in speed-area efficiency
- Automated power trace collection using ChipWhisperrer





Leakage Assessment of the power consumption

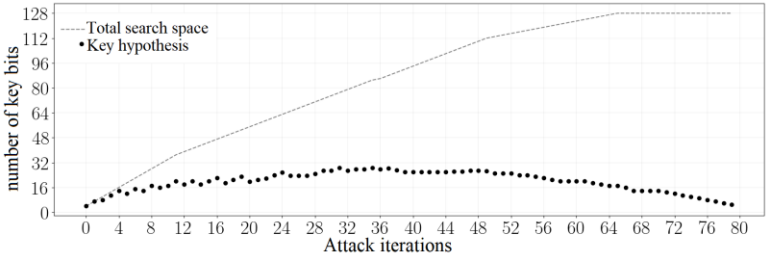
- Use statistical methods (Welch's t-test and χ^2 test)
- Non-specific – tests for general leakage of information
- Specific – tests the potential quality of a specific leakage model

Results: Information leakage in power consumption was detected

Side-channel Attack

- **Leakage Model:** Hamming Distance and Full-state models based on leakage patterns.
- **Target Selection**: Identified SipRound steps where specific key bits influence intermediate values most strongly.
- **Iterative Key Recovery:**
  - Recover "weak bits" first using low-complexity subkey guesses.
  - Use overlap between rounds to progressively reveal remaining bits without exponential search growth.

Results: First DPA-based attack on SipHash targeting FPGA implementation was created.



Conclusion

- This work presents the first DPA-based attack on a SipHash implementation in FPGA hardware.
- The findings support the development of more secure cryptographic hardware, with applications from secure network communications to embedded IoT systems.
- The results of this attack were showcased in an academic paper presented at the DSD 2025 conference.