Physical Side-Channel Attacks and Covert Communication on FPGAs

Seyedeh Sharareh Mirzargar

and

Mirjana Stojilović

École polytechnique fédérale de Lausanne

Barcelona, Spain

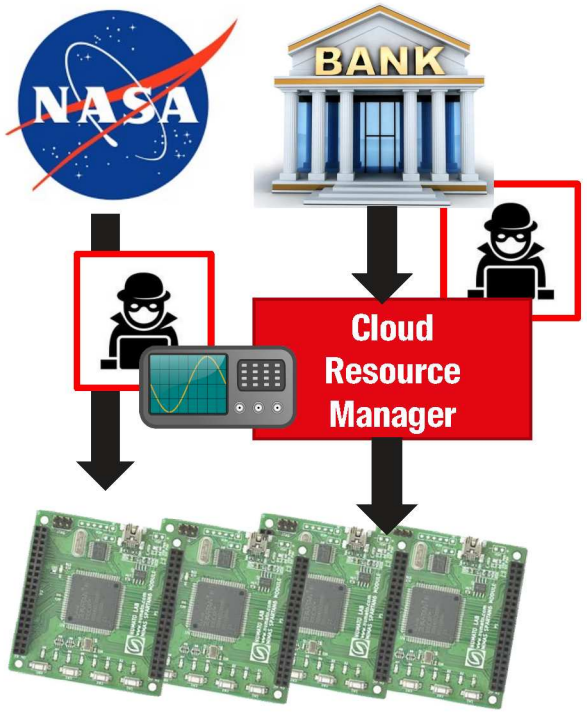
September 10, 2019

Introduction

- Application space keeps growing
- FPGAs run secure primitives and deal with sensitive data

Targets of security attacks since a while

Introduction



- Cloud providers now offer FPGAs
- Growth in FPGA application space inspires discovery of **new vulnerabilities**

Which of the vulnerabilities are due to FPGA physical properties?

Physical channels

- Several classifications
  - Transmission medium
  - Invasive or noninvasive
  - Require proximity
- Transmission medium as classifier
  - **Power** consumption
  - **Crosstalk** coupling
  - **Electromagnetic** emission
  - **Thermal** heating

Physical channels (ab)used for...

...stealing secrets, or so called side-channel attacks:

attacks based on **information** gained from
the **implementation** of a computer system, rather than
weaknesses in the implemented algorithm itself

Physical channels (ab)used for...

...covert communication

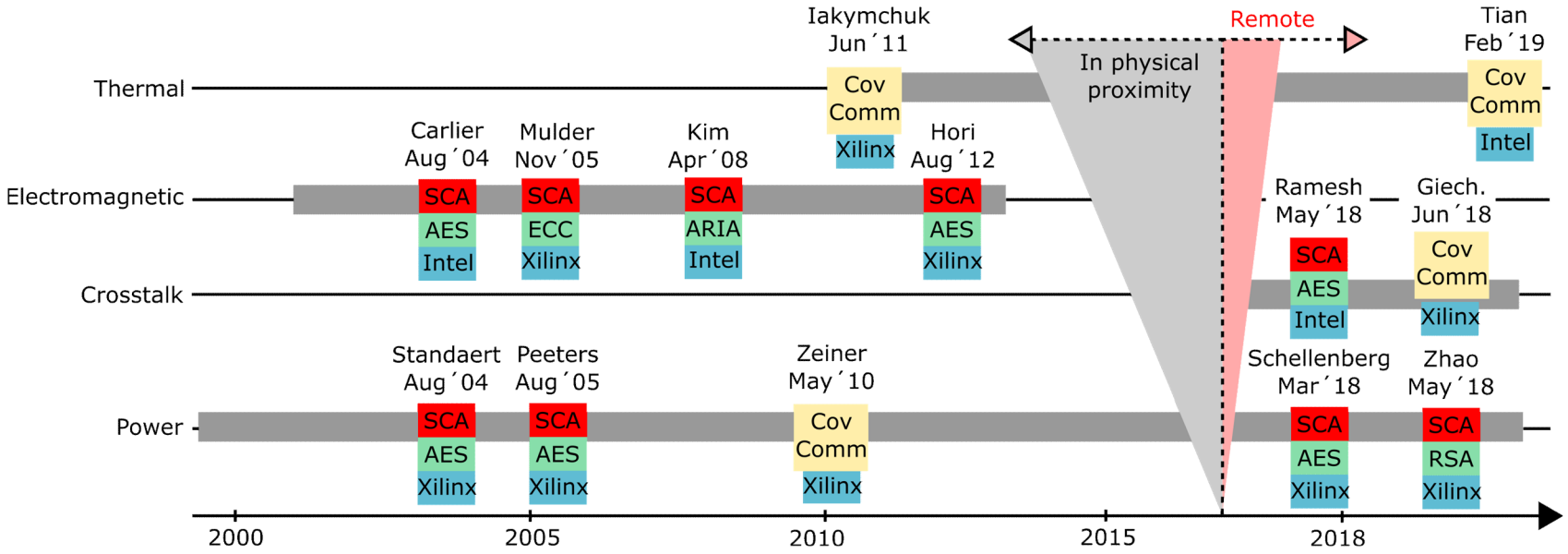
A **covert channel** is a communication channel not normally used in system communications and thus not protected by the system's security mechanisms.

EPFL

- Introduction
- **Timeline**
- Physical channels
- Vulnerable platforms
- Discussion
- Conclusion

Physical Side-Channel Attacks and Covert Communication on FGPAs

Timeline of key research contributions



Focus shifts towards attacks performed remotely.

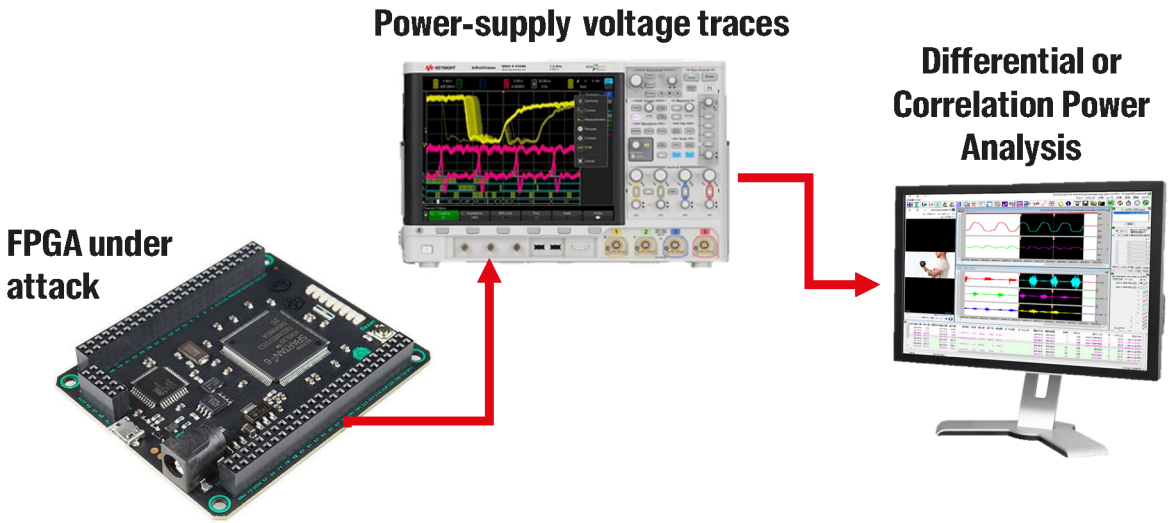
EPFL

- Introduction
- Timeline
- **Physical channels**
- Vulnerable platforms
- Discussion
- Conclusion

Physical Side-Channel Attacks and Covert Communication on FGPAs

Power analysis attacks

- If physical access is available:

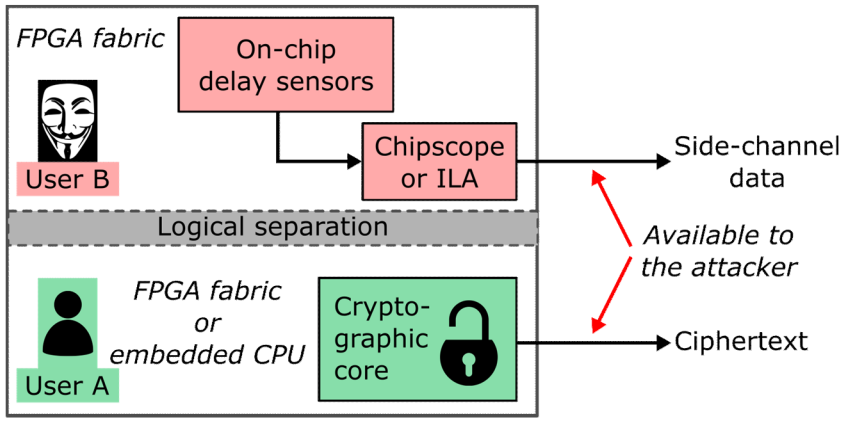


Kocher, Paul et al. "Differential power analysis." Annual International Cryptology Conference, 1999.

Örs, Sıddıka Berna, et al. "Power-analysis attacks on an FPGA First experimental results." International Workshop on Cryptographic Hardware and Embedded Systems., 2003.

Power analysis attacks

- Recently, demonstrated possible w/o an oscilloscope
- Vulnerable settings:
  - fabric-to-fabric, fabric-to-CPU, FPGA-to-FPGA



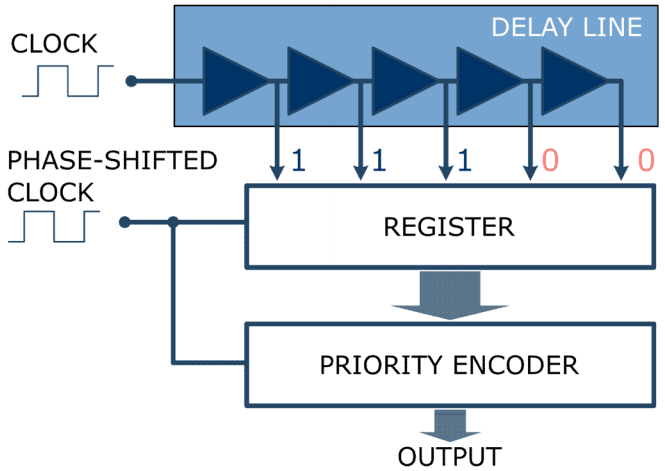
M. Zhao and G. E. Suh, "FPGA-based remote power side-channel attacks," IEEE Symposium on Security and Privacy, 2018

F. Schellenberg et al. "An inside job: Remote power analysis attacks on FPGAs," DATE 2018

F. Schellenberg et al. "Remote inter-chip power analysis side-channel attacks at board-level," ICCAD 2018

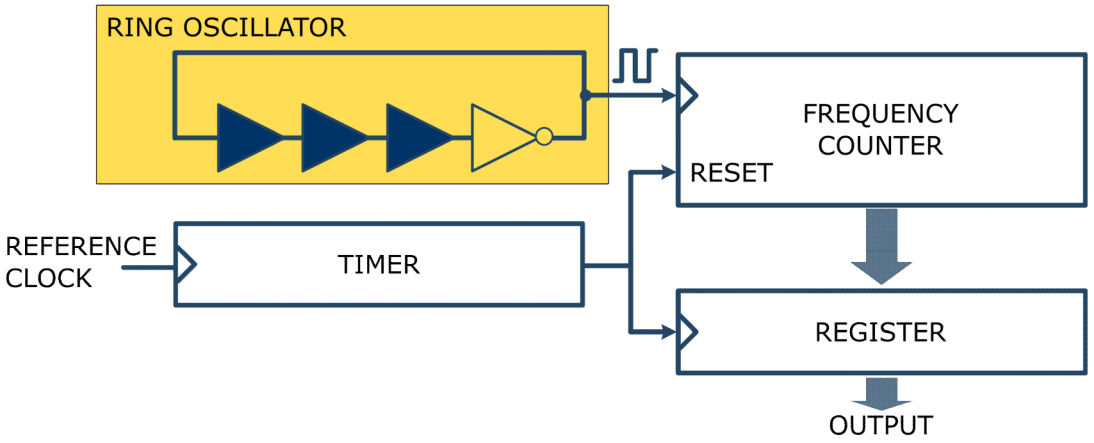
On-chip voltage measurements: How-To?

- Not measuring voltage directly, but **indirectly**
- Change in voltage creates change in **delay**
  - **Measure delay**



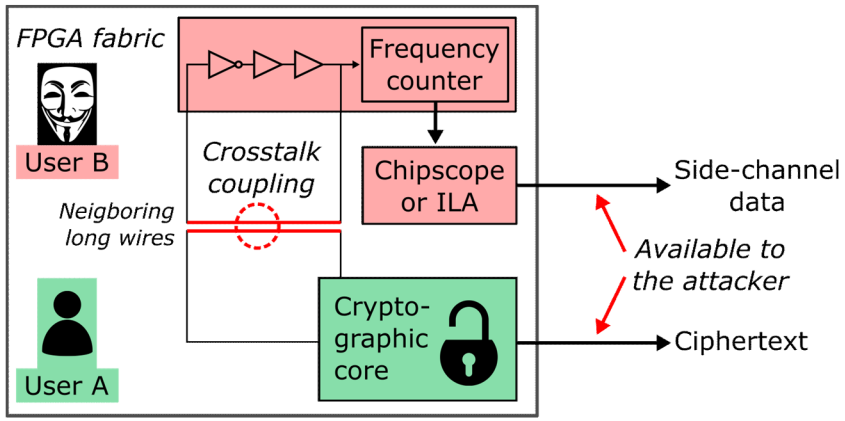
On-chip voltage measurements: How-To?

- Not measuring voltage directly, but **indirectly**
- Change in voltage creates change in **delay**
  - **Measure delay**



Crosstalk coupling

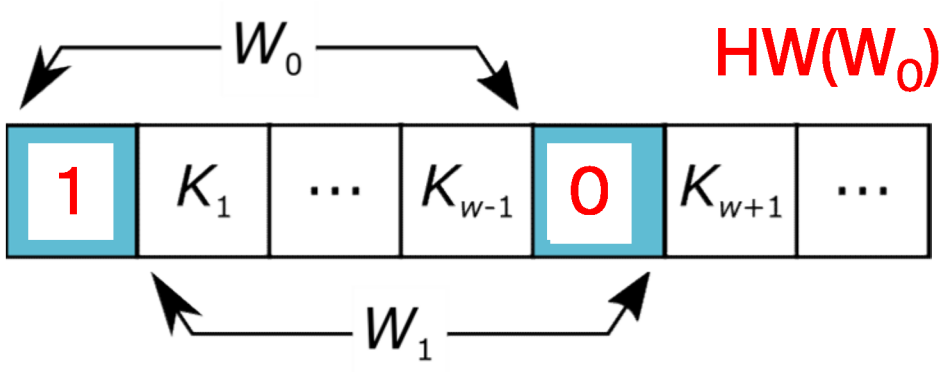
- Long wire carrying **1** reduces the propagation delay of the unconnected adjacent long wire
- Measurable if the wires are adjacent, or with at most one wire between
- Used as side channel or covert communication channel



Giechaskiel et al.
"Leaky wires: Information leakage and covert communication between FPGA long wires." Asia Conference on Computer and Communications Security. 2018.

Crosstalk coupling

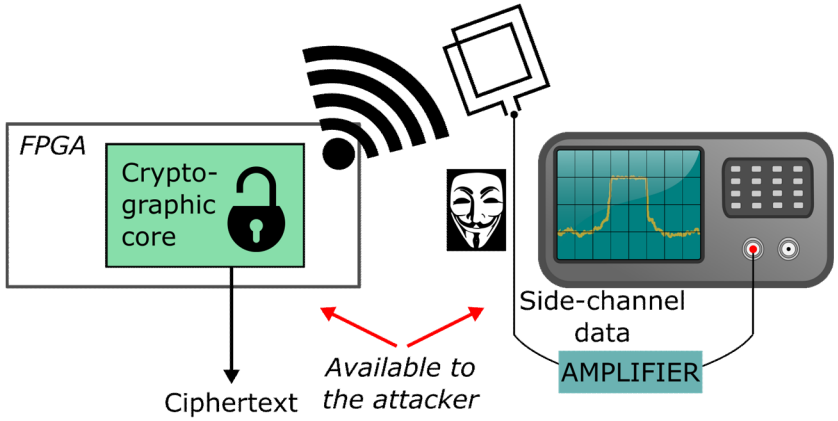
- Delay of adjacent long wire
  - depends on how long the transmitter carries one
  - independent from the switching frequency
- Sequence of bits can be extracted by
  - sliding window approach
  - comparing Hamming weight of overlapping windows



$HW(W_0) - HW(W_1) = +1$

Electromagnetic emission

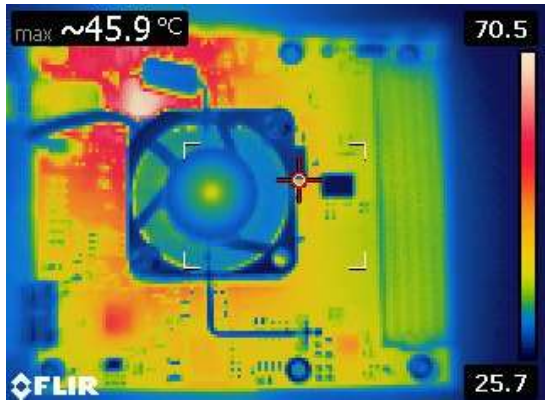
- Current flowing through a conductor creates EM signals
  - Radiation
  - Conduction
- Multiple view of events: more powerful than power side channel
- Impossible to attack remotely?



Carlier et al. "Generalizing square attack using side-channels of an AES implementation on an FPGA", FPL 2005

Thermal channel

- Some physical channels keep their state longer
  - Temperature-based covert communication
    - Transmitter and receiver use, for instance, **ring oscillators**
  - Possible to transmit (very slowly!) data in cloud FPGAs
    - Transmitter heats to send **1**
    - Receiver lands on the same FPGA and checks the temperature



Iakymchuk et al. "Temperature-based covert channel in FPGA systems." 6th Intl. Workshop on Reconfig. Communication-centric SoC (ReCoSoC), 2011.

Tian et al. "Temporal Thermal Covert Channels in Cloud FPGAs." FPGA 2019.

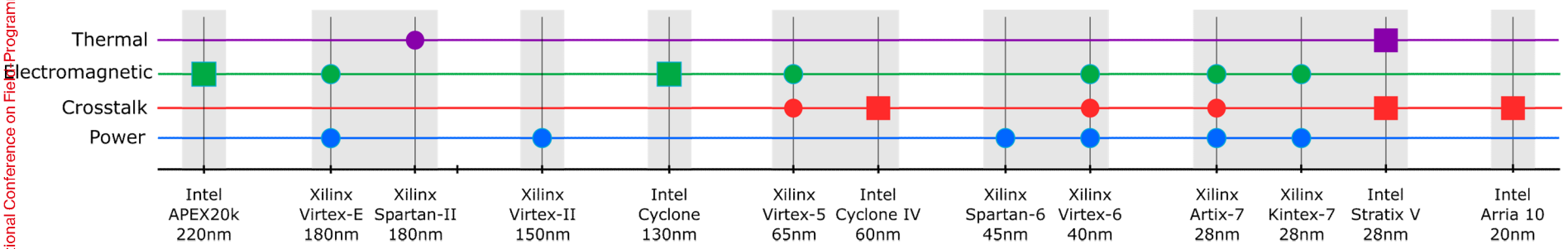
EPFL

- Introduction
- Timeline
- Physical channels
- **Vulnerable platforms**
- Discussion
- Conclusion

Physical Side-Channel Attacks and Covert Communication on FGPAs

Comprehensive list of vulnerable platforms

- **Experimentally** shown vulnerable
- All technology nodes sensitive
- Crosstalk coupling stronger in newer technology nodes



EPFL

- Introduction
- Timeline
- Physical channels
- Vulnerable platforms
- **Discussion**
- Conclusion

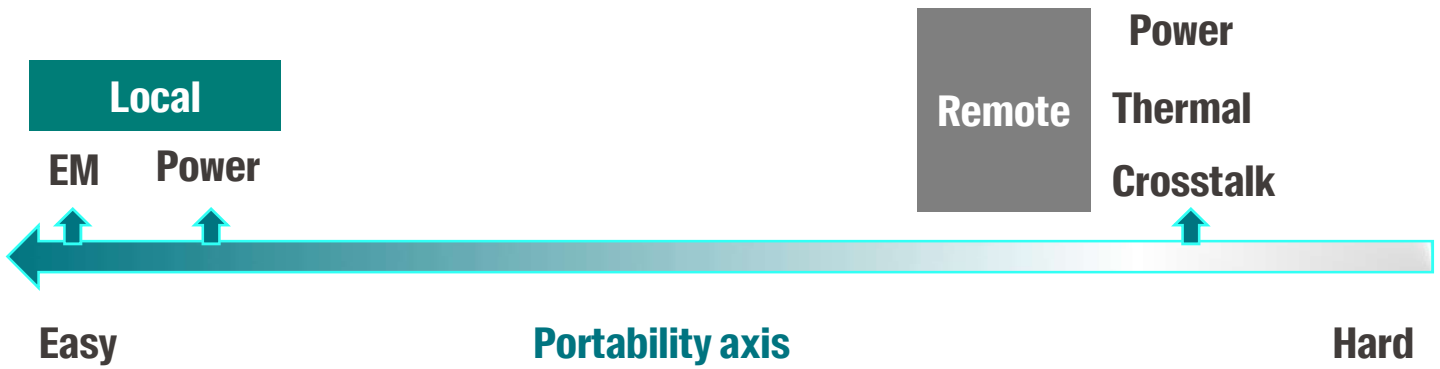
Physical Side-Channel Attacks and Covert Communication on FGPAs

Equipment cost and complexity

- EM attack most complex and costly
- Local power analysis attack is comparably complex but less costly
- Remote attack has the least complexity and cost

Portability

- How much one needs to change the methodology or experimental set-up when the target changes?



Prevention and protection

- **Prevention**
  - Local: restricting the access to the device
  - Remote: not allow FPGA sharing nor (even) board sharing
- **Protection**
  - Local
    - Design countermeasures (hiding, masking)
  - Remote
    - Power: detect special primitives (e.g., bitstream analysis)
    - Crosstalk: add space between two circuits
    - Thermal: enforce idle periods between users

Conclusions

- FPGAs **vulnerable** to side-channel attacks and covert communication
- No perfect countermeasure exits, let alone a universal one
- Can we **design** FPGAs to be less vulnerable?
- Can we **write code** for more robust FPGAs?
- Attack space still not exhausted
- Methods to prevent/protect still largely unexplored

Thank you!

mirjana.stojilovic@epfl.ch