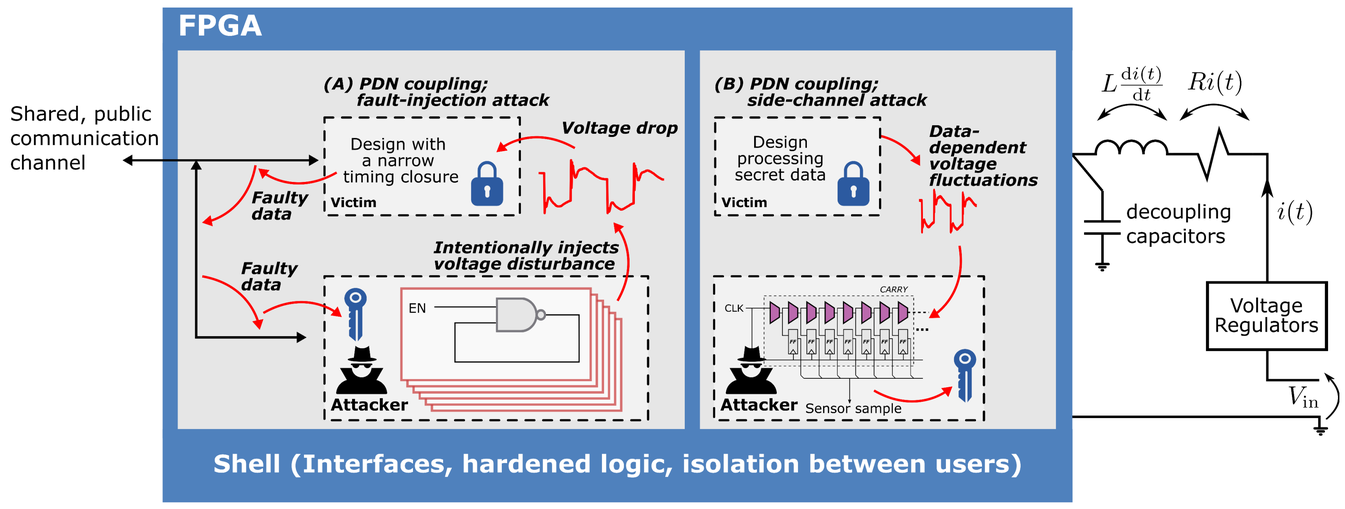
Remote Electrical-Level Attacks on Cloud FPGAs

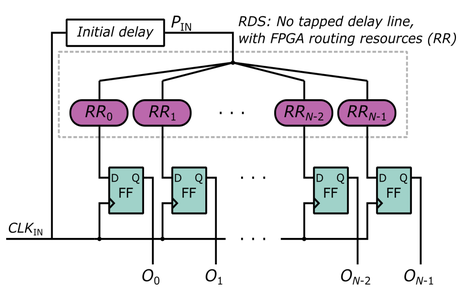
Dina G. Mahmoud, Ognjen Glamočanin, and Mirjana Stojilović

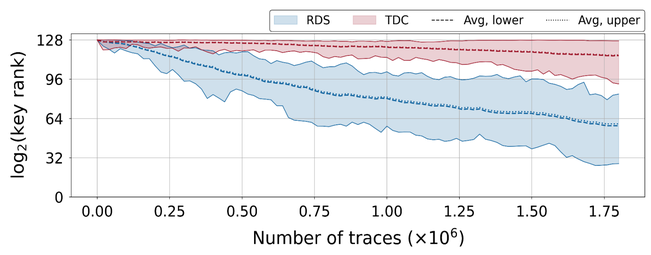
- Cloud providers (AWS, Azure, Alibaba) deploy FPGAs in servers
- FPGAs allow access to **low-level logic** (LUTs, FFs)
  - To build voltage-drop sensors (time-to-digital converters (TDCs))
  - To build power wasters
- Remote FPGA access creates security risks
  - Remote **power side-channel** attacks (SCAs)
  - Remote **fault injection** (FI) attacks
- In a multitenant user scenario
  - Tenants **logically** and **physically** separated
  - Connected through the power delivery network (PDN)



Routing Delay Sensors (RDS) [TCHES'23]

- TDC sensors use CARRY elements detectable by bitstream scanners
- We present the first voltage-drop sensor that leverages routing resources
  - The observable delay line replaced with routing for a stealthier sensor
- RDS also **outperforms the state-of-the-art** TDC
  - 4× larger peak-to-peak ratio and 2× larger SNR
  - Breaks 3× more key bits on a datacenter-scale FPGAs (Alveo U200)

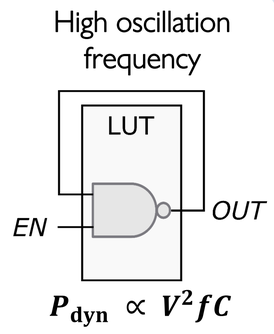


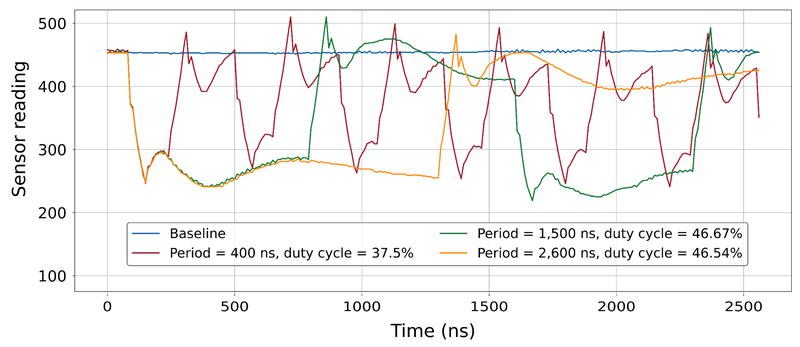


Stealthy routing-based voltage sensor, outperforming state-of-the-art TDCs

Fault Injection Attacker [DATE'22]

- Remote fault injection relies on violating timing constraints
  - Undervolting increases the delays in the circuit
  - High power consumption → undervolting
- Limit the duration to avoid denial-of-service
- Divide the attacker into independently-controlled blocks
- Carefully choose the period and the duty cycle of the enable signals



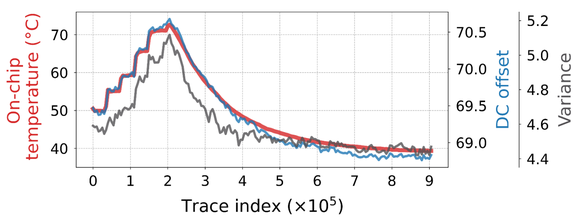


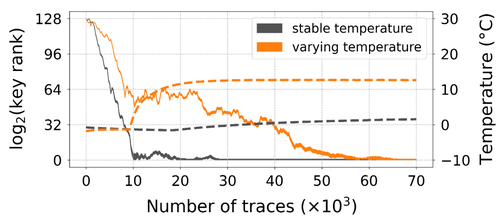
217 blocks of 124 LUTs each

Shape and amplitude of voltage drop controlled by activation pattern of attacker

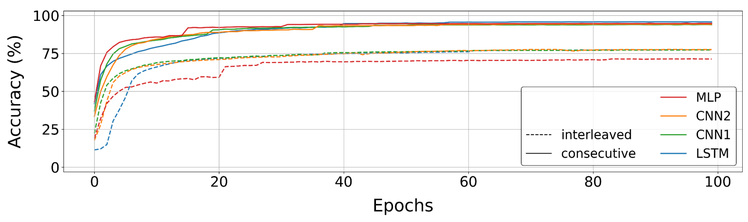
Temperature Impact on Remote Power Analysis Attacks [DATE'23]

- On shared FPGAs, we present the first analysis of temperature impact on voltage-drop sensors and statistical and ML-based power analysis attacks
- TDC sensors are impacted by temperature, affecting power SCA results





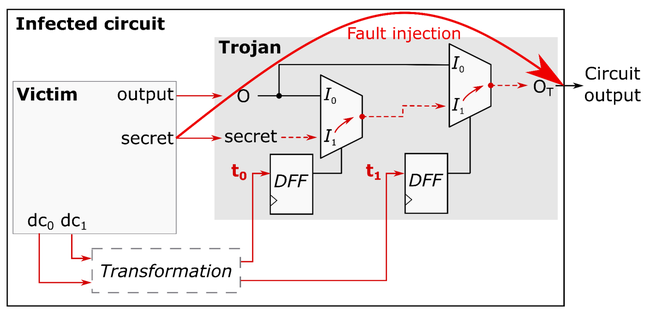
- We quantify the impact of trace acquisition techniques on ML attacks
  - Correct trace acquisition is important even in shared FPGAs
  - Consecutively recorded traces can show a **misleadingly high accuracy**



First analysis of the temperature impact on remote power analysis attacks

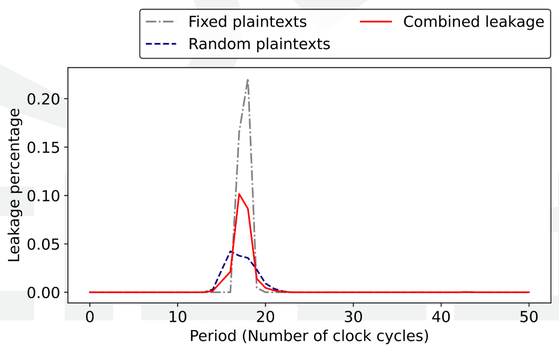
Fault Injection Victim [FPL'20]

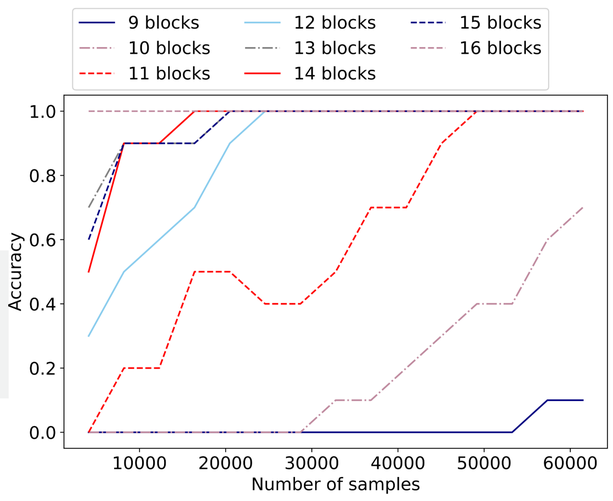
- Satisfiability don't-cares (SDCs): Internal design states which are never reached
  - e.g., two signals cannot both be logic '1' at the same time
- Use SDC signals as Trojan activation signals
  - **Stealthy Trojan only activated in faulting conditions**
- Hide Trojan into in the Sbox of an AES circuit to leak AES key



Fault Injection Results

- Using blocks of 4,096 ROs each
- Tested on commercially available cloud FPGA instances
- Success of the attack is measured by the leakage of the AES key
  - Percentage of ciphertexts at the output that are actually the key
- The optimal activation frequency is centered around a specific frequency
  - Most likely the resonance frequency of the PDN
- With enough samples, the key is the most occurring value (accuracy = 100%) at the output when the plaintexts are pseudorandom

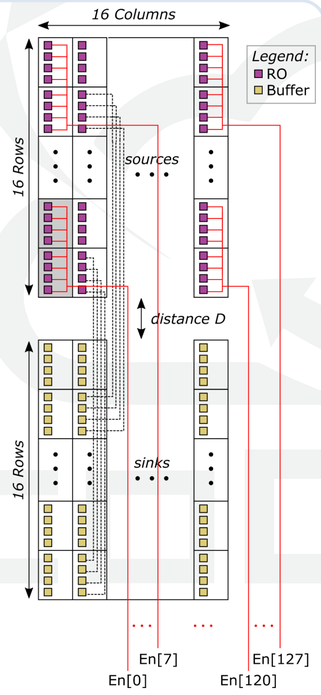


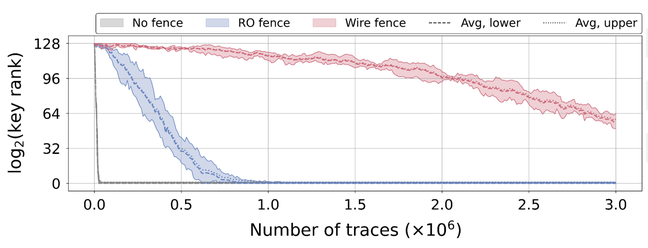


Controlled fault injection is a threat to cloud FPGAs

Active Wire Fences [DDECS'23]

- We propose novel wire-based power wasters
  - Sources (ROs) drive wires ending in sinks (buffers)
- Wire-based wasters consume more power than ROs
  - 2× voltage drop without extra resource overhead
- Active wire fences **protect better** from power SCAs
  - Surpassing RO fences when activated with a PRNG





New active wire fences for 6× improved power side-channel security