High-Speed Ring Oscillator based Sensors for Remote Side-Channel Attacks on FPGAs

Joseph GRAVELLIER (EMSE)
Jean-Max DUTERTRE (EMSE)
Yannick TEGLIA (THALES)
Philippe LOUBET-MOUNDI (THALES)

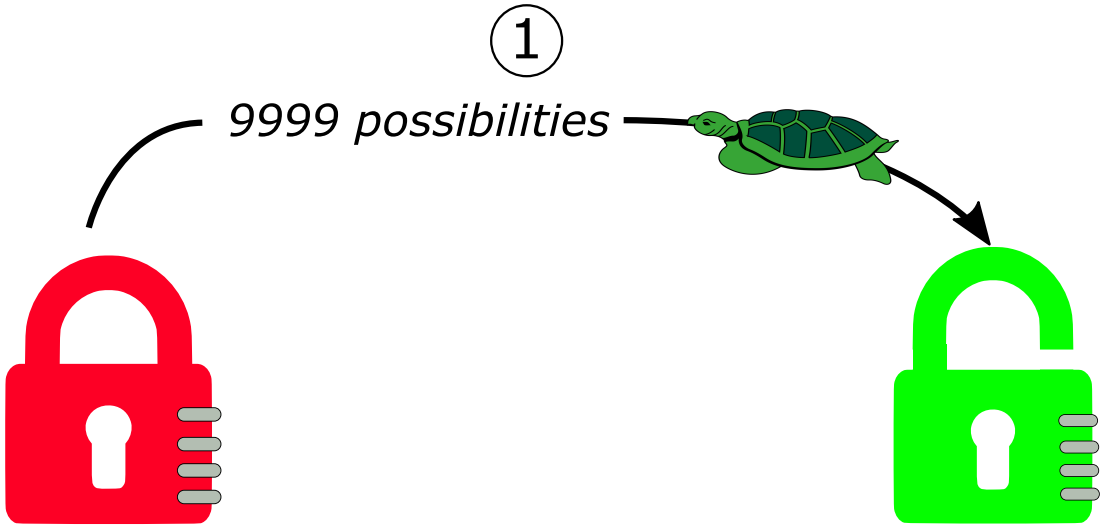
Laboratoire de Sécurité des Architectures et des Systèmes,
F-13541 Gardanne France
Thales - 13600 La Ciotat, France

December 2019

Context: What is side-channel ?

Example: Padlock

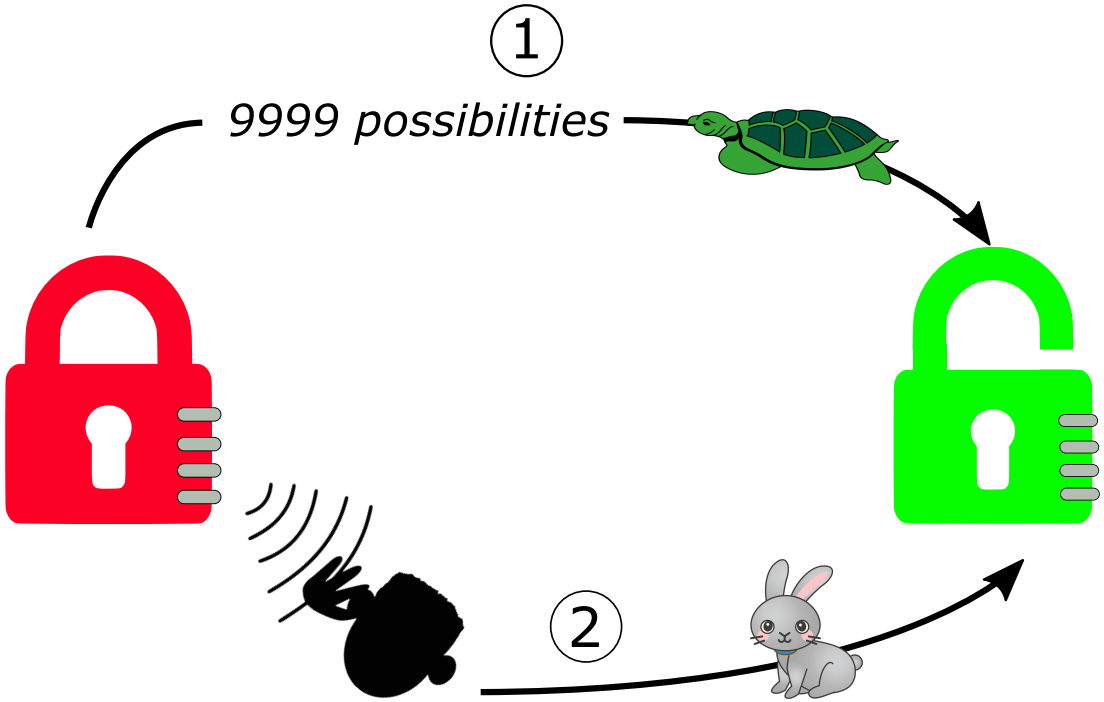
- Two ways to crack the padlock:
  1. Brute Force all the combinations.
  2. Listen to padlock clicks.



Context: What is side-channel ?

Example: Padlock

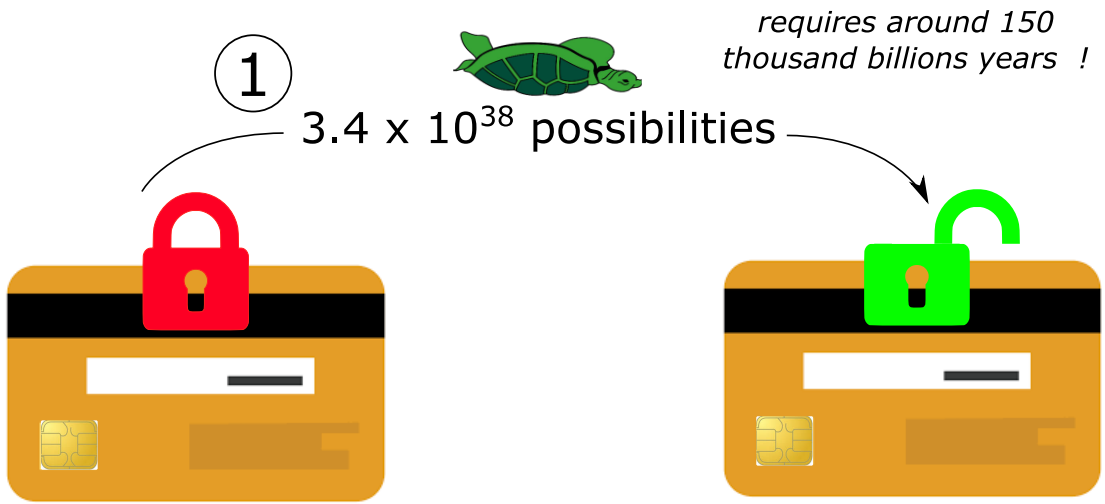
- Two ways to crack the padlock:
  1. Brute Force all the combinations.
  2. Listen to padlock clicks.



Context: What is side-channel ?

Use case: Smart Card

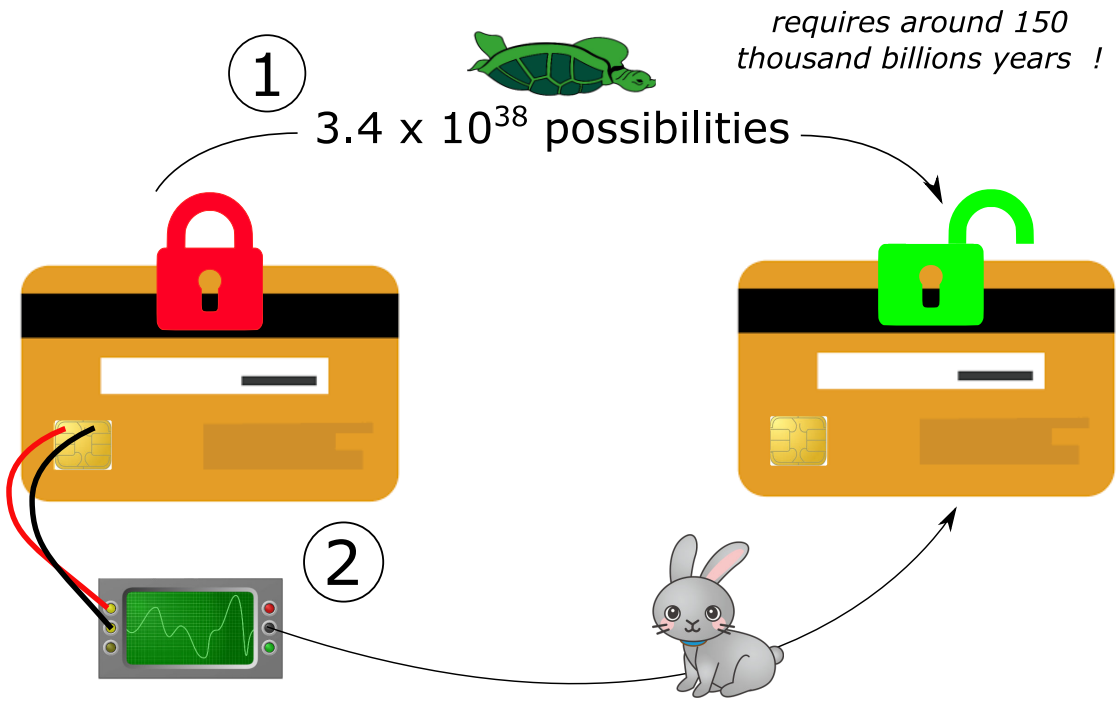
- Retrieve a credit card secret key ? :
  1. Using Brute Force → impossible.
  2. Using power measurement → Yes, because the secret leaks !



Context: What is side-channel ?

Use case: Smart Card

- Retrieve a credit card secret key ? :
  1. Using Brute Force → impossible.
  2. Using power measurement → Yes, because the secret leaks !



Context: What is side-channel ?

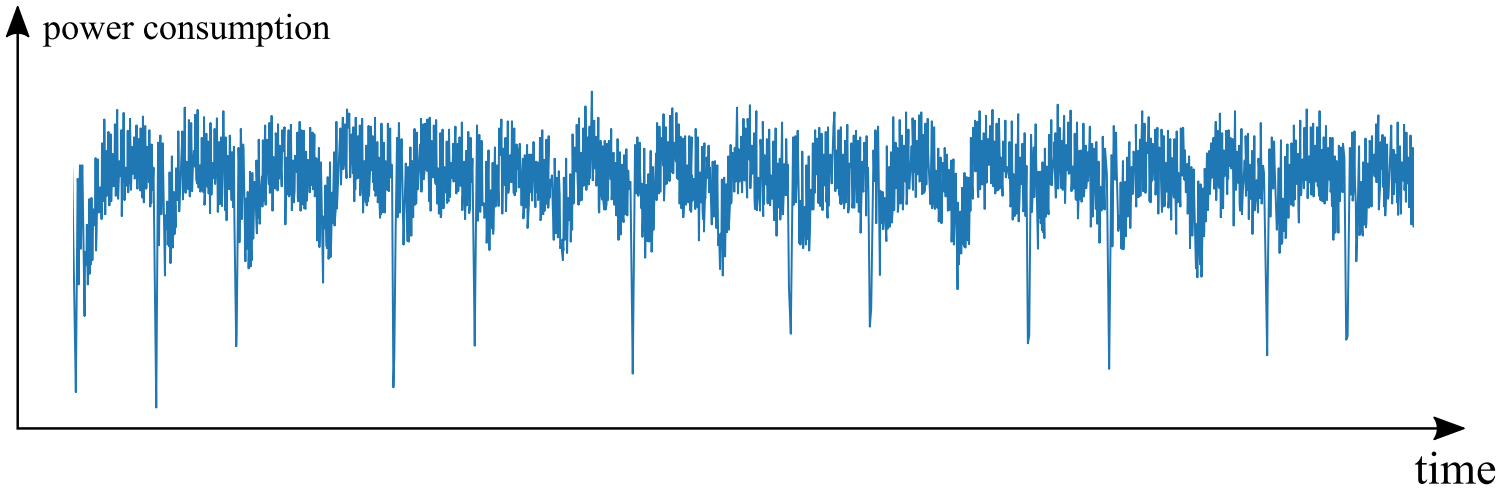
Application: Power side-channel on RSA

- Example on RSA algorithm: *if* $(Key[\mathrm{i}] = 1)$ $\{do\ something\}$.
- Attacker measures RSA power consumption.
- Knowing RSA algorithm & RSA power consumption, the attacker deduces RSA key bits.

Context: What is side-channel ?

Application: Power side-channel on RSA

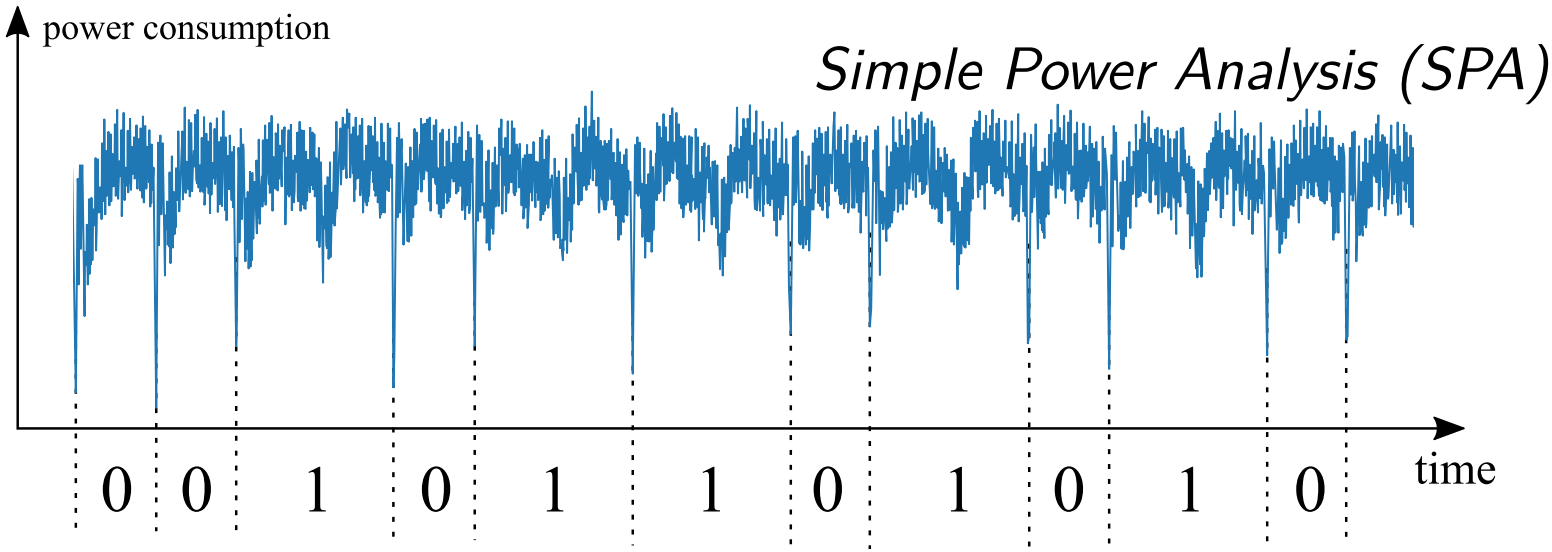
- Example on RSA algorithm: *if* $(Key[\mathrm{i}] = 1)$ $\{$*do something*$\}$.
- Attacker measures RSA power consumption.
- Knowing RSA algorithm & RSA power consumption, the attacker deduces RSA key bits.



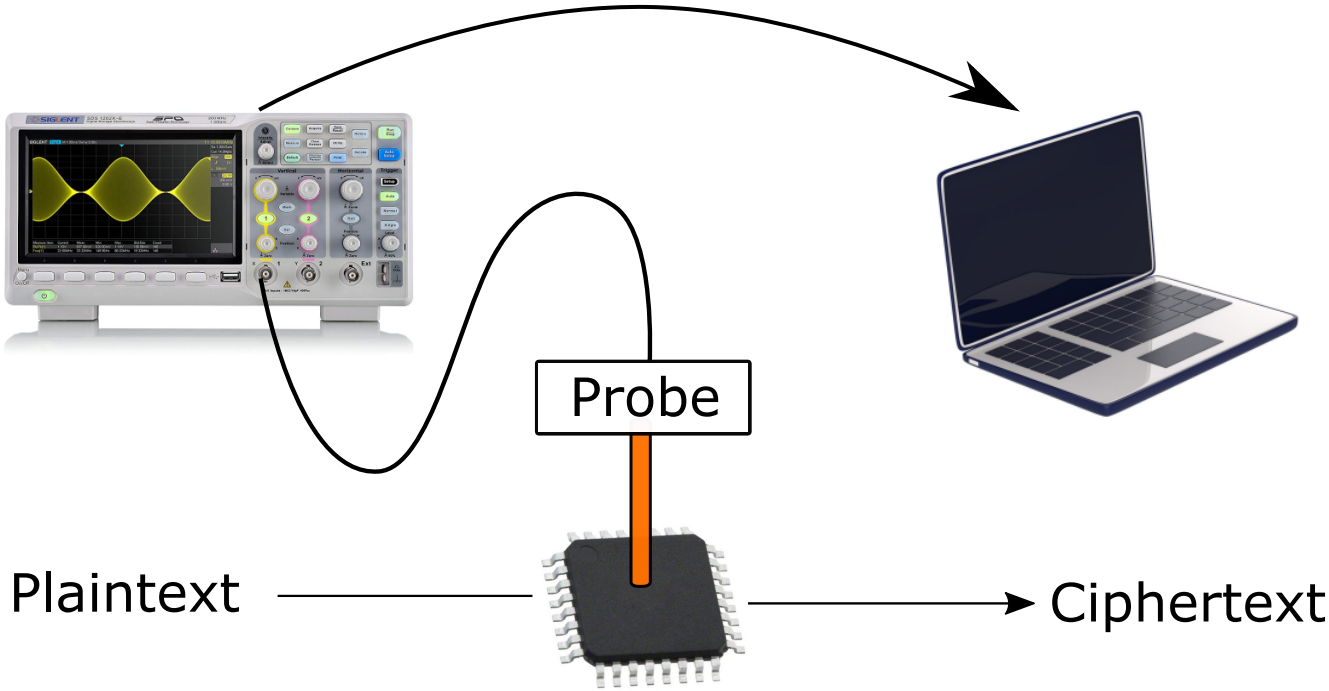
Context: What is side-channel ?

Application: Power side-channel on RSA

- Example on RSA algorithm: *if* $(Key[\mathrm{i}] = 1)$ $\{$*do something*$\}$.
- Attacker measures RSA power consumption.
- Knowing RSA algorithm & RSA power consumption, the attacker deduces RSA key bits.

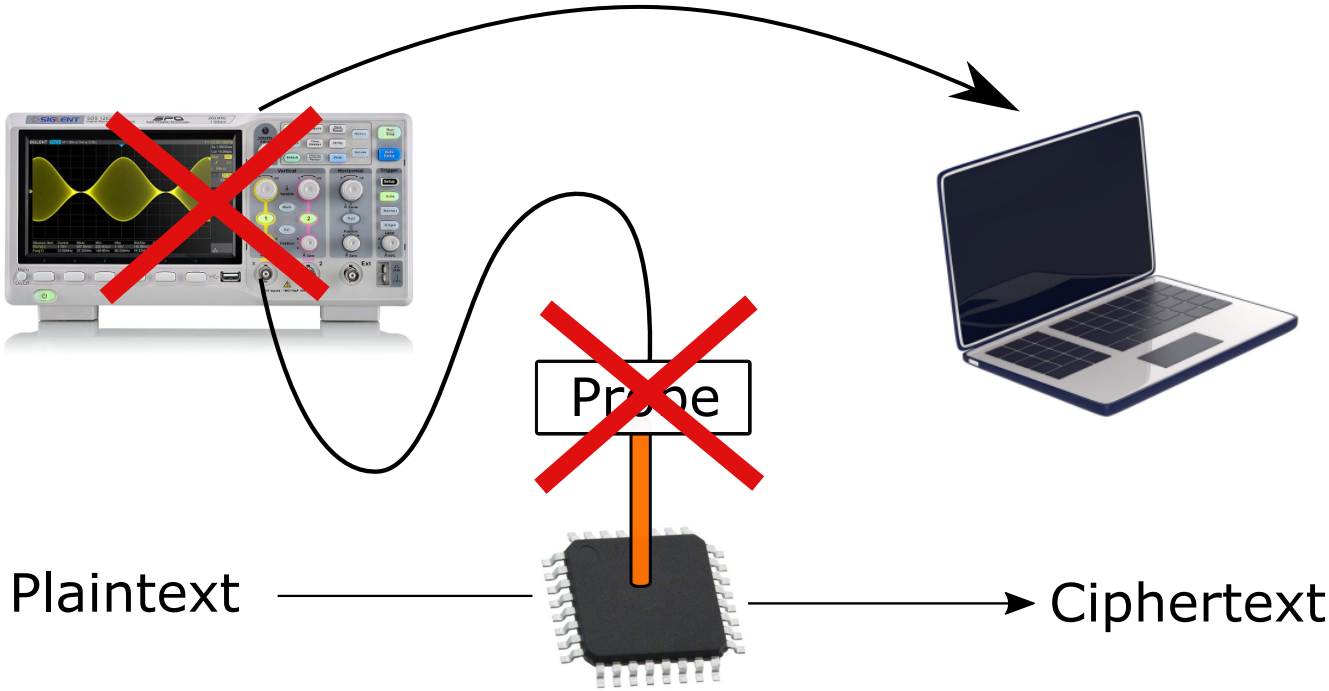


- Type: fault injection attack (FIA) & side-channel attack (SCA).
- Target: smart cards, microcontrollers, system on chip...
- Means: oscilloscope, power & EM probe...
- Range: **local**, direct physical access required.



Context: What is remote side-channel ?

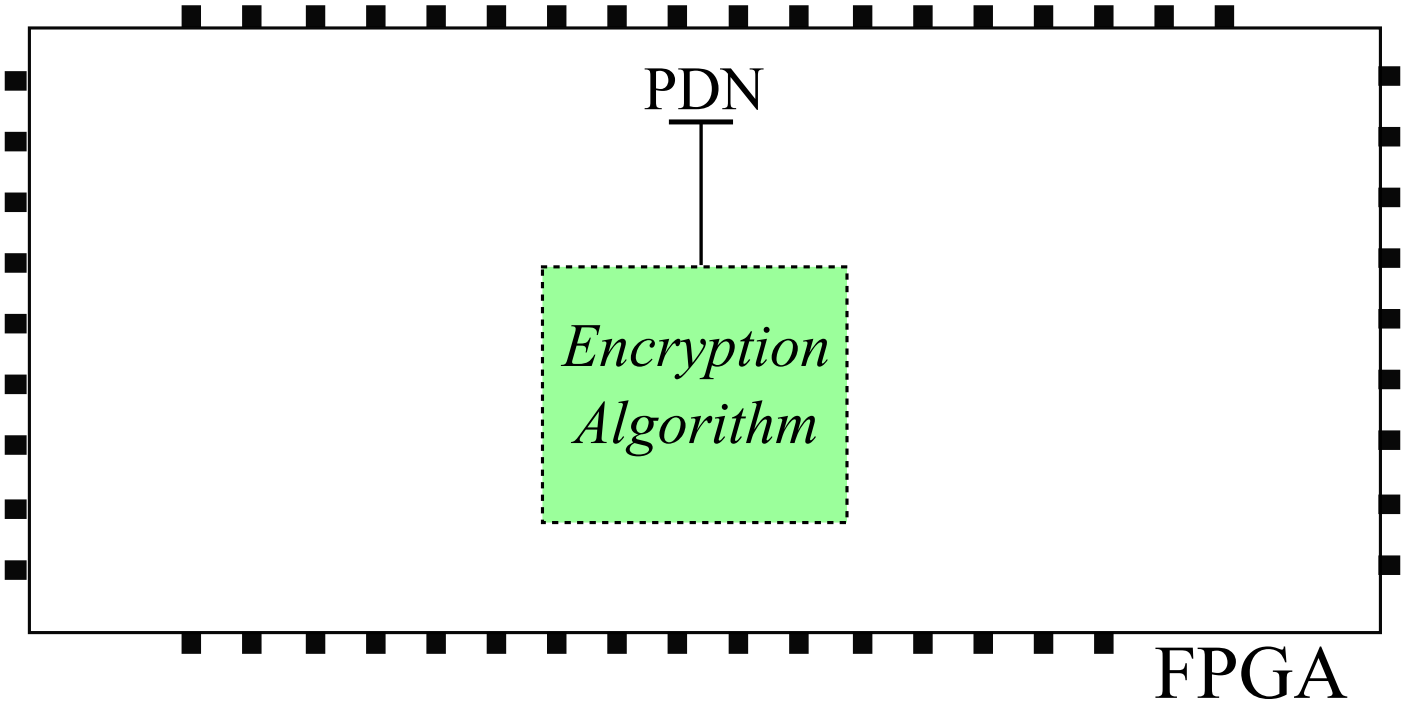
- Type: fault injection attack (FIA) & side-channel attack (SCA).
- Range: **remote, access to a network required.**
- Target: connected devices (IoT), data centers...
- Means: **resources available within the target**.



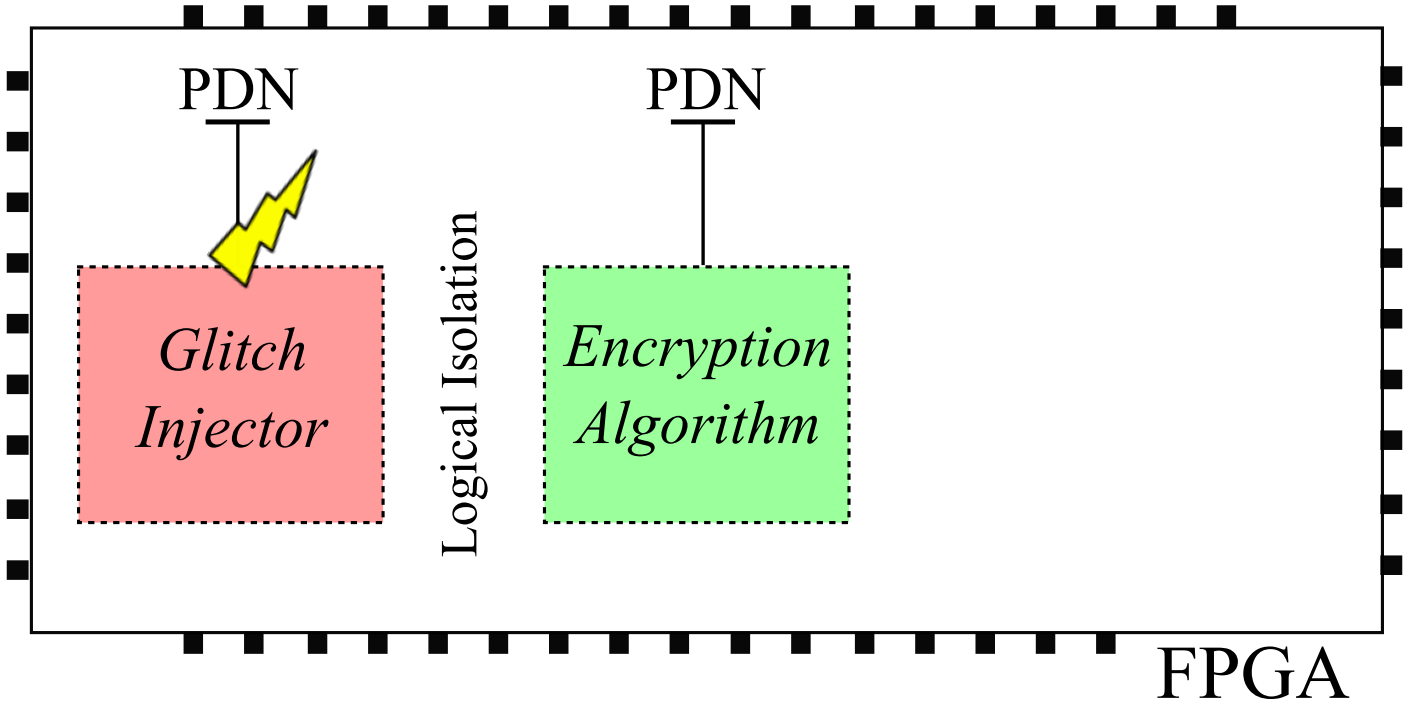
1. **Introduction** to remote FPGA-based hardware attacks.
2. Presentation of the proposed **RO-based sensor design**.
3. Experimental validation and SCA.
4. Comparison with other **SCA setups**.

1. **Introduction** to remote FPGA-based hardware attacks.
2. Presentation of the proposed **RO-based sensor design**.
3. Experimental validation and SCA.
4. Comparison with other **SCA setups**.

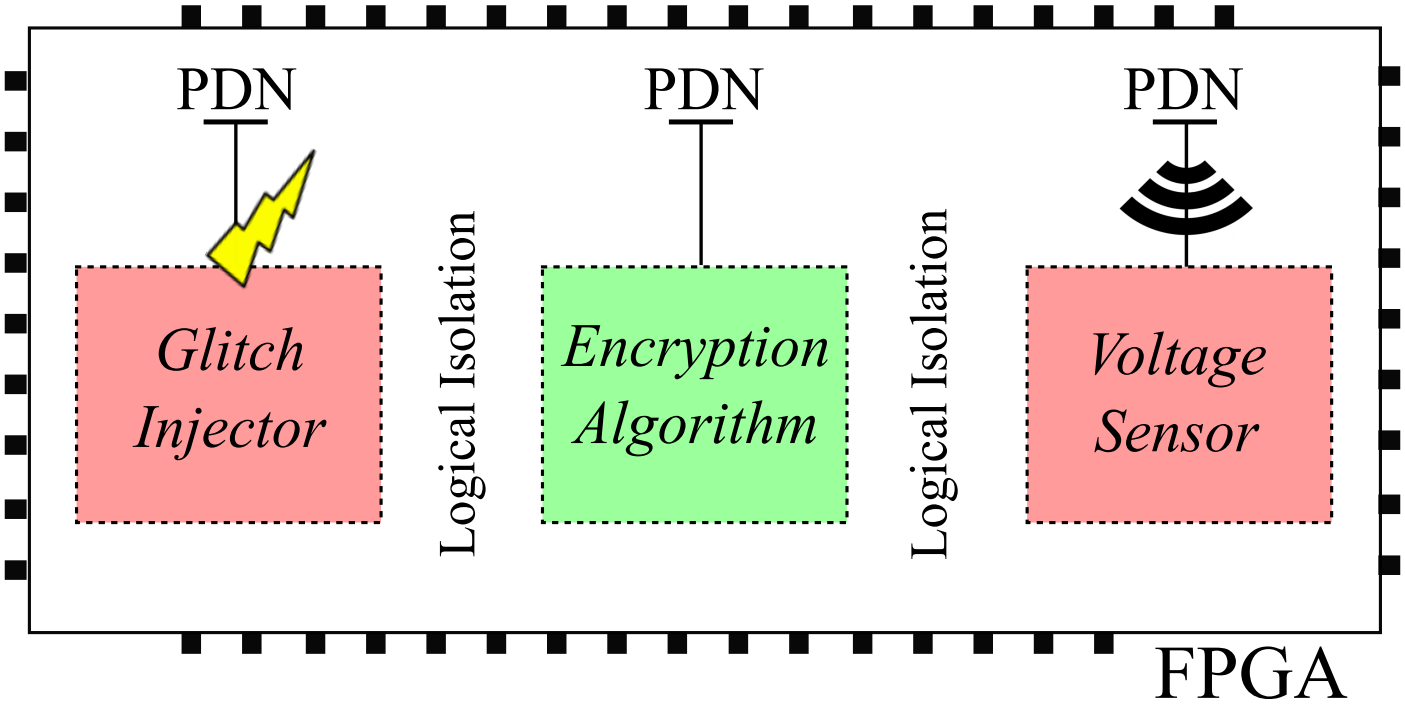
- Usual hardware attacks can be entirely reproduced within FPGA logic:
  - Encryption **algorithm** implementation.
  - Voltage glitch **injector** implementation (Krautter et al).
  - Voltage **sensor** implementation (Schellenberg et al).



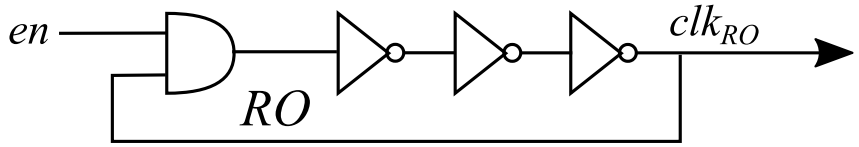
- Usual hardware attacks can be entirely reproduced within FPGA logic:
  - Encryption **algorithm** implementation.
  - Voltage glitch **injector** implementation (Krautter et al).
  - Voltage **sensor** implementation (Schellenberg et al).



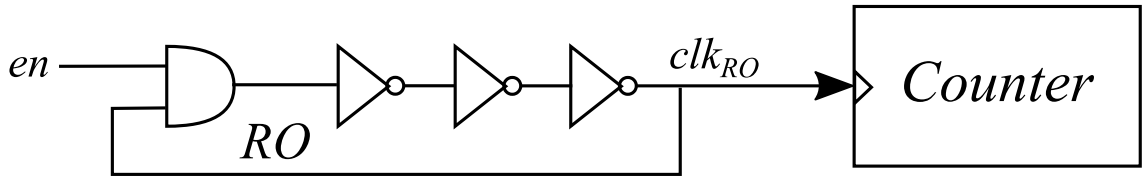
- Usual hardware attacks can be entirely reproduced within FPGA logic:
  - Encryption **algorithm** implementation.
  - Voltage glitch **injector** implementation (Krautter et al).
  - Voltage **sensor** implementation (Schellenberg et al).



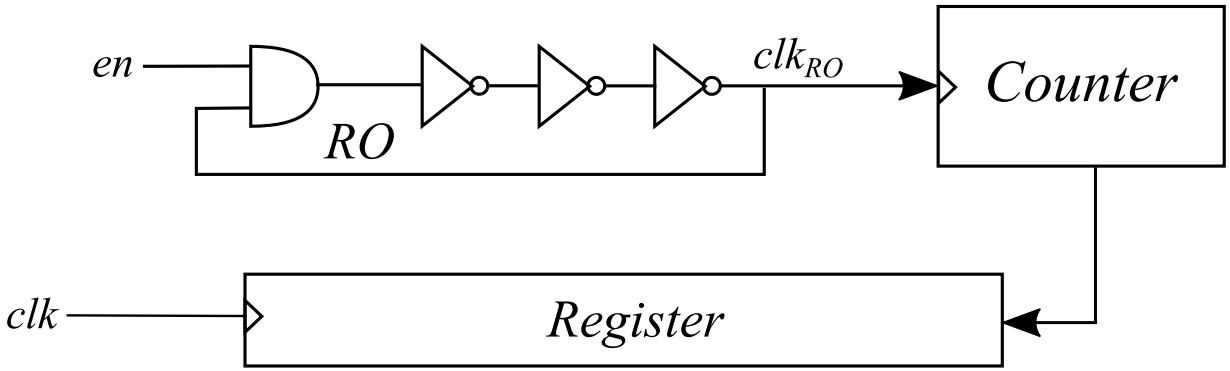
- Ring-oscillator based sensor basics:
  - A **RO** generates an oscillation clk_{RO} at a frequency f_{RO}.



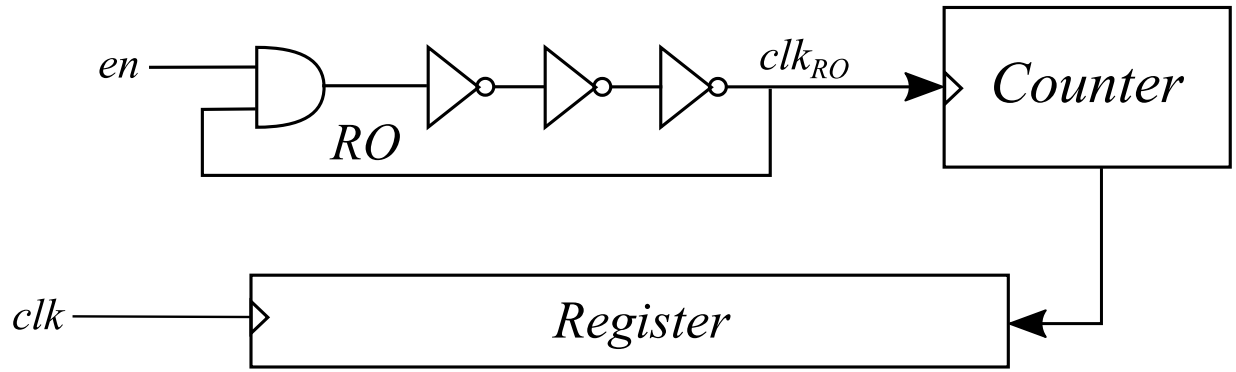
- Ring-oscillator based sensor basics:
  - A **RO** generates an oscillation clk_{RO} at a frequency f_{RO}.
  - A **counter** is incremented by one each clk_{RO} period.



- Ring-oscillator based sensor basics:
  - A **RO** generates an oscillation clk_{RO} at a frequency f_{RO}.
  - A **counter** is incremented by one each clk_{RO} period.
  - A **register** reads the **counter** value at a fixed rate clk.

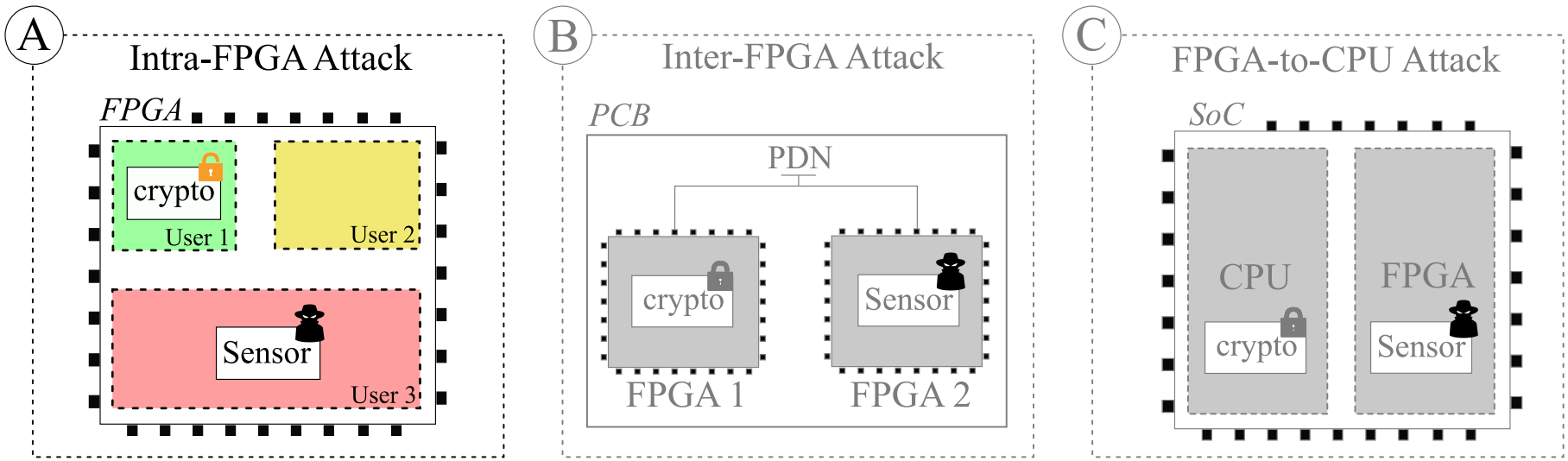


- Ring-oscillator based sensor basics:
  - A **RO** generates an oscillation clk_{RO} at a frequency f_{RO}.
  - A **counter** is incremented by one each clk_{RO} period.
  - A **register** reads the **counter** value at a fixed rate clk.

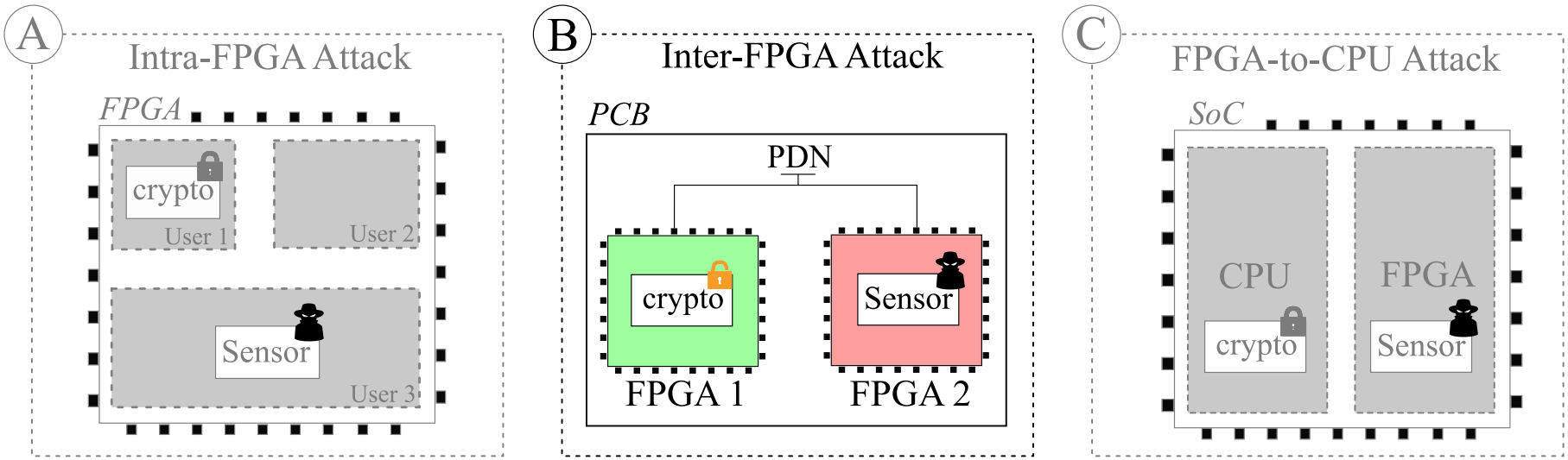


- f_{RO} fluctuates with temperature and voltage variations.
  - if $V \nearrow$ or $T \searrow$ then $f_{RO} \nearrow$: bigger values are sampled
  - if $V \searrow$ or $T \nearrow$ then $f_{RO} \searrow$: smaller values are sampled

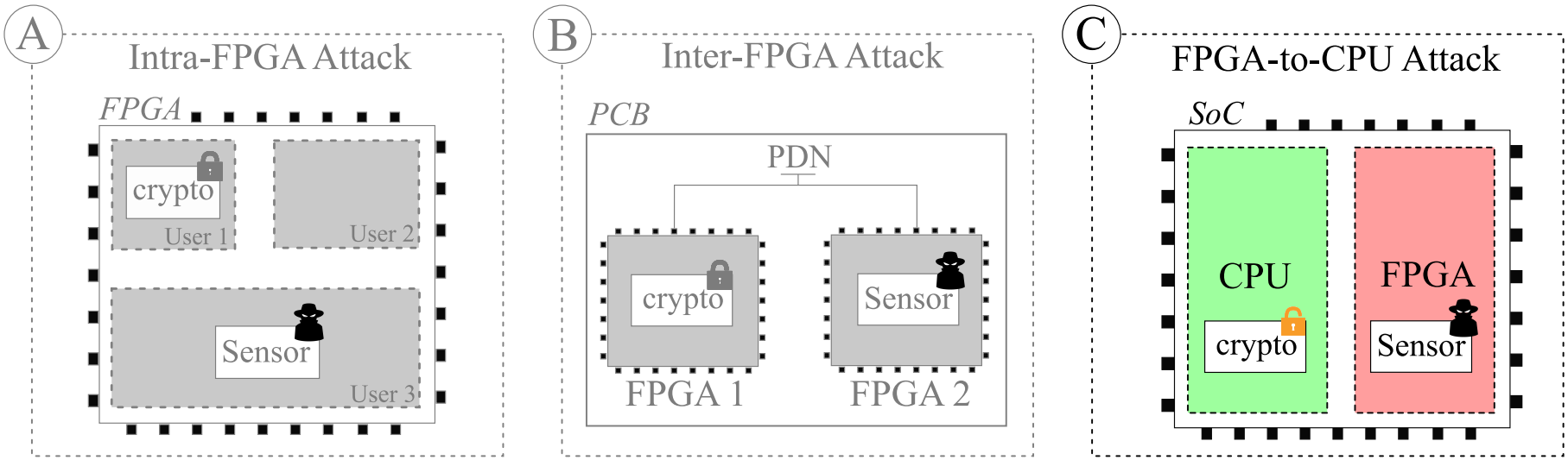
- Target: connected devices that embeds FPGAs.
  - A Multi-user FPGAs in **cloud datacenters** (Schellenberg et al).
  - B Printed circuit boards **PCB** (Schellenberg et al).
  - C **Heterogeneous** connected **SoCs** (Zhao et al).



- Target: connected devices that embeds FPGAs.
  - A Multi-user FPGAs in **cloud datacenters** (Schellenberg et al).
  - B Printed circuit boards **PCB** (Schellenberg et al).
  - C **Heterogeneous** connected **SoCs** (Zhao et al).



- Target: connected devices that embeds FPGAs.
  - A Multi-user FPGAs in **cloud datacenters** (Schellenberg et al).
  - B Printed circuit boards **PCB** (Schellenberg et al).
  - C **Heterogeneous** connected **SoCs** (Zhao et al).



- **Supposed** RO-based sensors limitations

  "The measurement through ROs requires a counting mechanism. Because of that, even with multiple ROs, a sampling rate of only 8 MHz was achieved [...], making them too slow to sense variations at circuit speed" (Gnad et al. 2018)

- **Supposed** RO-based sensors limitations

  "The measurement through ROs requires a counting mechanism. Because of that, even with multiple ROs, a sampling rate of only 8 MHz was achieved [...], making them too slow to sense variations at circuit speed" (Gnad et al. 2018)

- For this reason:
  - RO were **only used for SPA** side-channel attacks.
  - RO are **not considered as a threat** for CPA attacks.

- **Supposed** RO-based sensors limitations

  "The measurement through ROs requires a counting mechanism. Because of that, even with multiple ROs, a sampling rate of only 8 MHz was achieved [...], making them too slow to sense variations at circuit speed" (Gnad et al. 2018)

- For this reason:
  - RO were **only used for SPA** side-channel attacks.
  - RO are **not considered as a threat** for CPA attacks.

- **We refute this assumption:**

- **Supposed** RO-based sensors limitations

  "The measurement through ROs requires a counting mechanism. Because of that, even with multiple ROs, a sampling rate of only 8 MHz was achieved [...], making them too slow to sense variations at circuit speed" (Gnad et al. 2018)

- For this reason:
  - RO were **only used for SPA** side-channel attacks.
  - RO are **not considered as a threat** for CPA attacks.

- **We refute this assumption:**
  - Through the introduction of a **novel RO-based sensor design**.

- **Supposed** RO-based sensors limitations

  "The measurement through ROs requires a counting mechanism. Because of that, even with multiple ROs, a sampling rate of only 8 MHz was achieved [...], making them too slow to sense variations at circuit speed" (Gnad et al. 2018)

- For this reason:
  - RO were **only used for SPA** side-channel attacks.
  - RO are **not considered as a threat** for CPA attacks.

- **We refute this assumption:**
  - Through the introduction of a **novel RO-based sensor design**.
  - Capable of a **250 MHz** sampling frequency.

- **Supposed** RO-based sensors limitations

  "The measurement through ROs requires a counting mechanism. Because of that, even with multiple ROs, a sampling rate of only 8 MHz was achieved [...], making them too slow to sense variations at circuit speed" (Gnad et al. 2018)

- For this reason:
  - RO were **only used for SPA** side-channel attacks.
  - RO are **not considered as a threat** for CPA attacks.

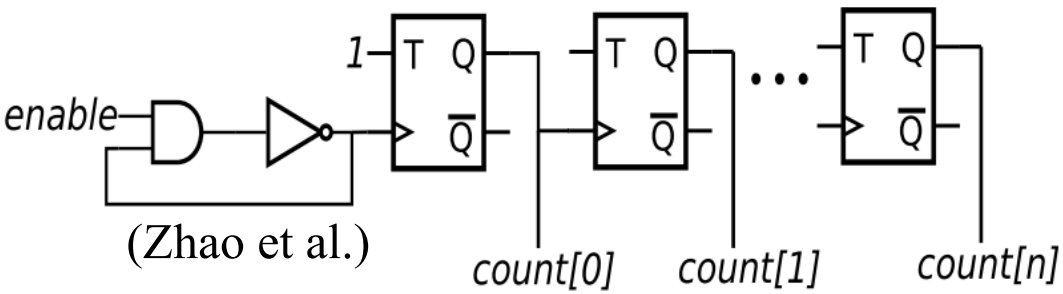
- **We refute this assumption:**
  - Through the introduction of a **novel RO-based sensor design**.
  - Capable of a **250 MHz** sampling frequency.
  - Suitable for **CPA side-channel attacks**.

1. **Introduction** to remote FPGA-based hardware attacks.
2. Presentation of the proposed **RO-based sensor design**.
3. Experimental validation and SCA.
4. Comparison with other **SCA setups**.

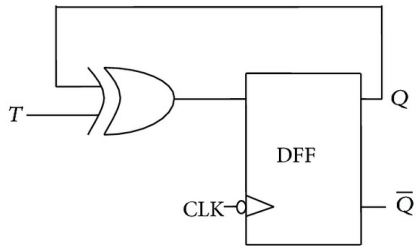
- Recipe for a speed efficient sensor:
  - Implement the **fastest RO achievable** with the available logic.

- Recipe for a speed efficient sensor:
  - Implement the **fastest RO achievable** with the available logic.
  - Implement a counter **capable of handling RO speed**.

- Recipe for a speed efficient sensor:
  - Implement the **fastest RO achievable** with the available logic.
  - Implement a counter **capable of handling RO speed**.
- Problem with existing sensors:
  - They use binary counters made of **complex** flip-flops JK, Toggle, etc and additional **logic**.

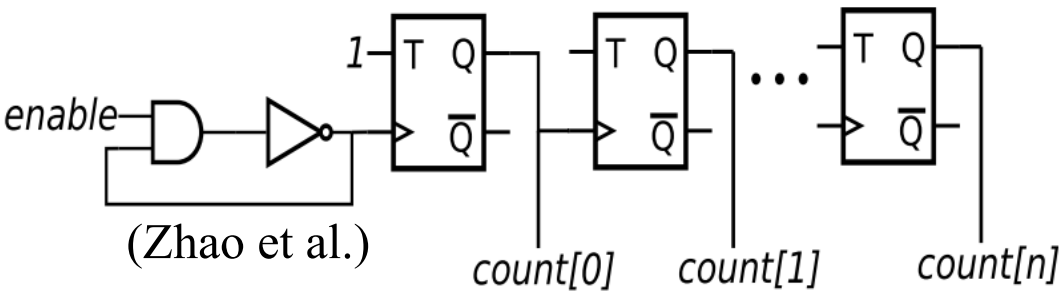


(Zhao et al.)

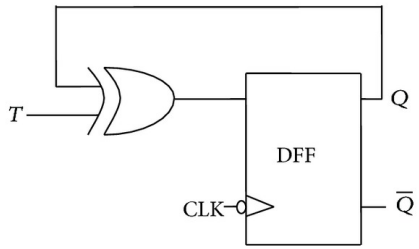


DFF-based TFF

- Recipe for a speed efficient sensor:
  - Implement the **fastest RO achievable** with the available logic.
  - Implement a counter **capable of handling RO speed**.
- Problem with existing sensors:
  - They use binary counters made of **complex** flip-flops JK, Toggle, etc and additional **logic**.
  - These designs struggle to **meet timing requirement**.

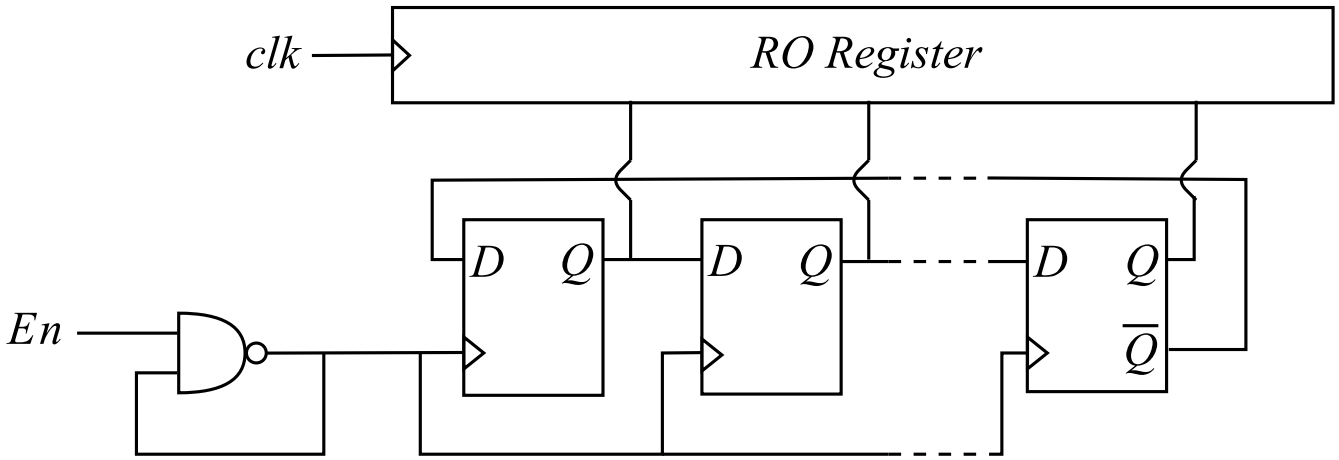


(Zhao et al.)

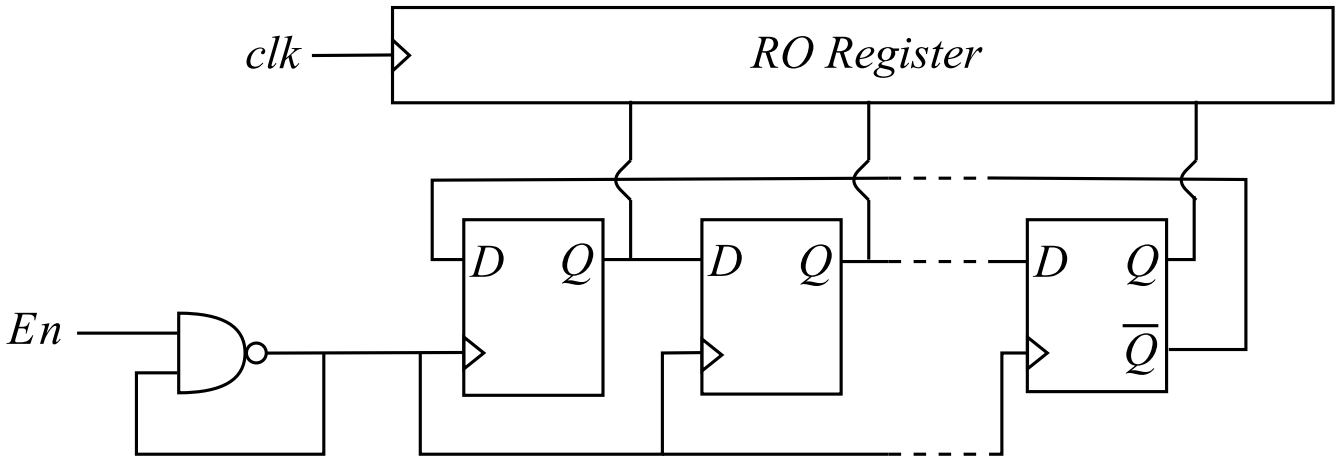


DFF-based TFF

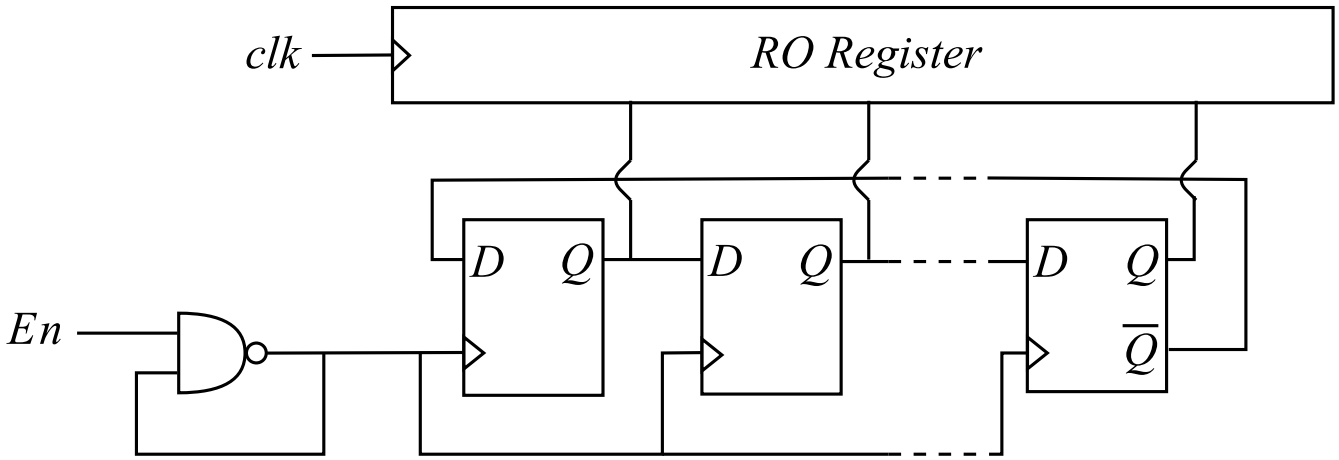
- We propose an ultra-light/speed optimized design:
  - A unique NAND gate for the **RO**.(1 LUT)
  - A synchronous Johnson Ring **Counter**. (8 flip-flops + 1 LUT)
  - A 8-bit sampling **Register**. (8 flip-flops)



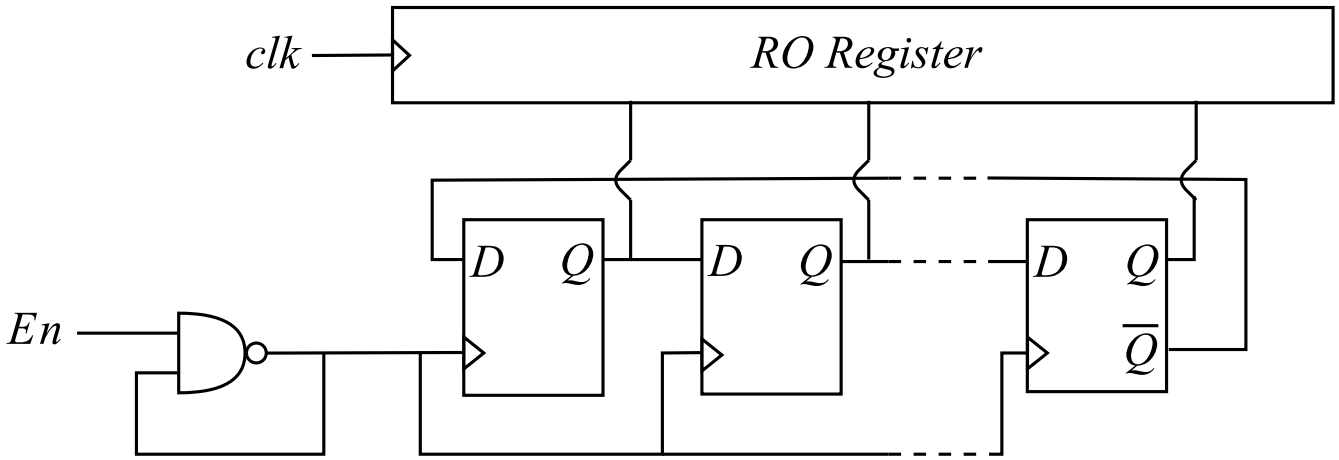
- We propose an ultra-light/speed optimized design:
  - A unique NAND gate for the **RO**.(1 LUT)
  - A synchronous Johnson Ring **Counter**. (8 flip-flops + 1 LUT)
  - A 8-bit sampling **Register**. (8 flip-flops)



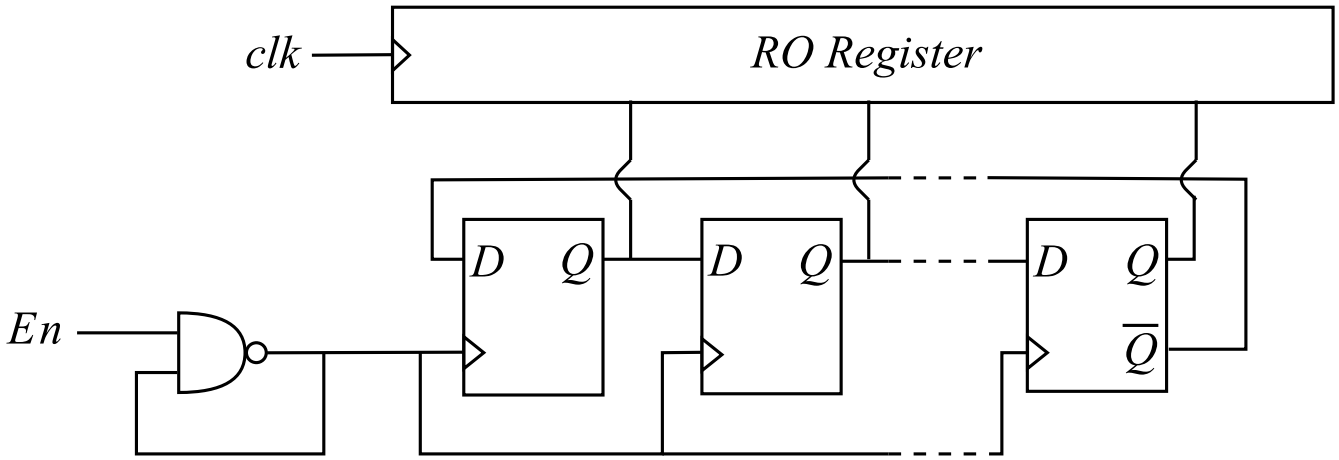
- We propose an ultra-light/speed optimized design:
  - A unique NAND gate for the **RO**.(1 LUT)
  - A synchronous Johnson Ring **Counter**. (8 flip-flops + 1 LUT)
  - A 8-bit sampling **Register**. (8 flip-flops)



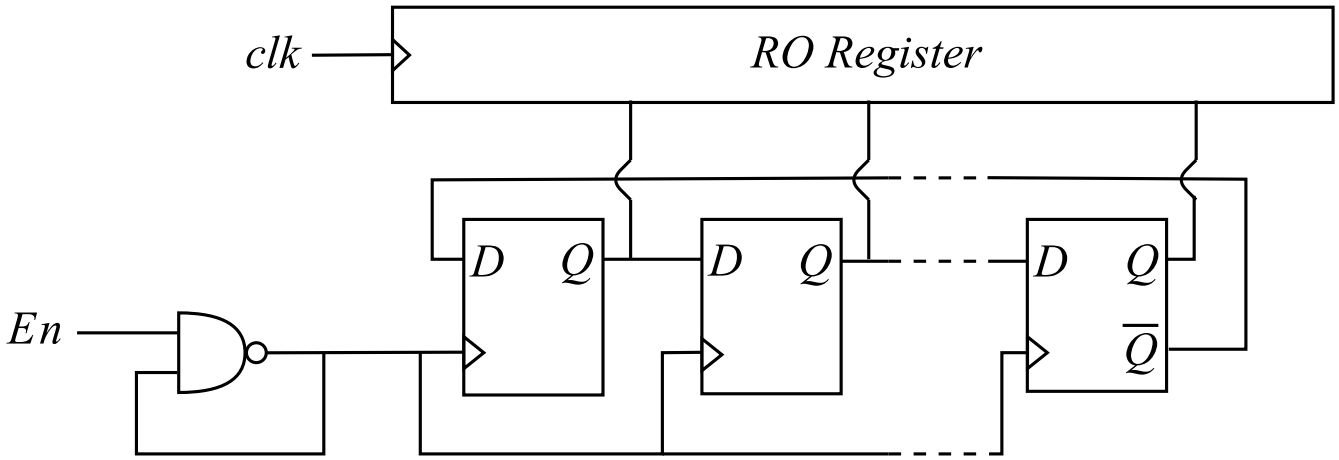
- We propose an ultra-light/speed optimized design:
  - A unique NAND gate for the **RO**.(1 LUT)
  - A synchronous Johnson Ring **Counter**. (8 flip-flops + 1 LUT)
  - A 8-bit sampling **Register**. (8 flip-flops)
- The overall sensor consumes 2 Artix-7 slices.



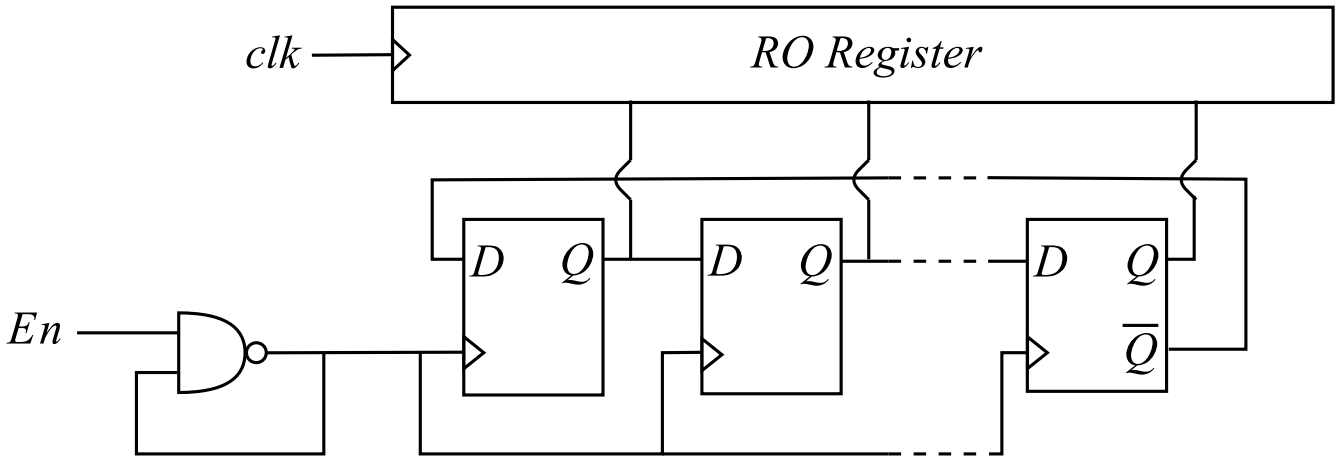
- A speed optimized design:
  - RO frequency reaches around **1.2 GHz**.
  - Johnson Ring-Counter provides **16 distinct states**.
  - Sampling register is cadenced at **250 MHz**



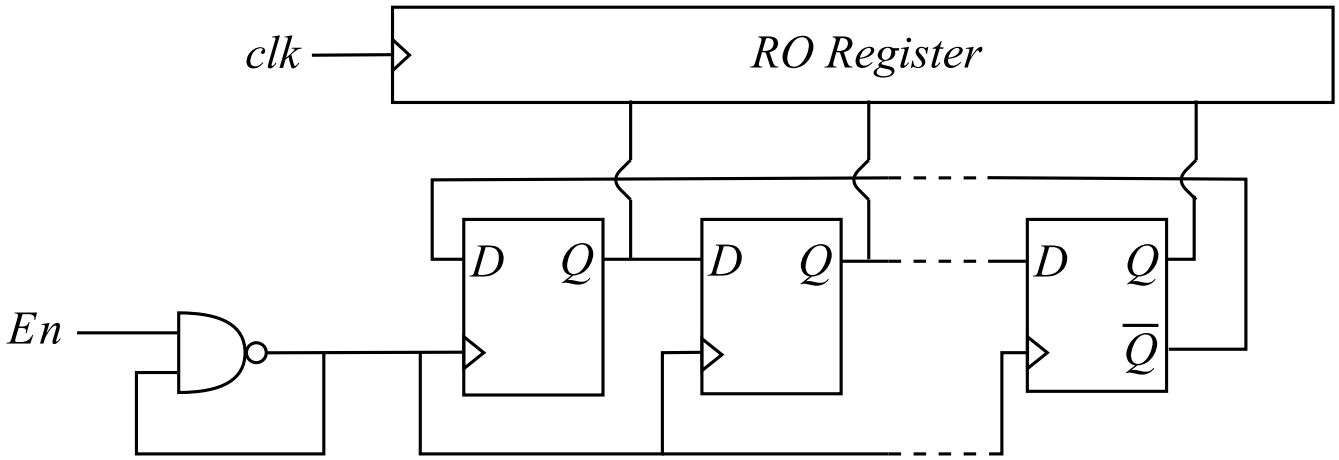
- A speed optimized design:
  - RO frequency reaches around **1.2 GHz**.
  - Johnson Ring-Counter provides **16 distinct states**.
  - Sampling register is cadenced at **250 MHz**



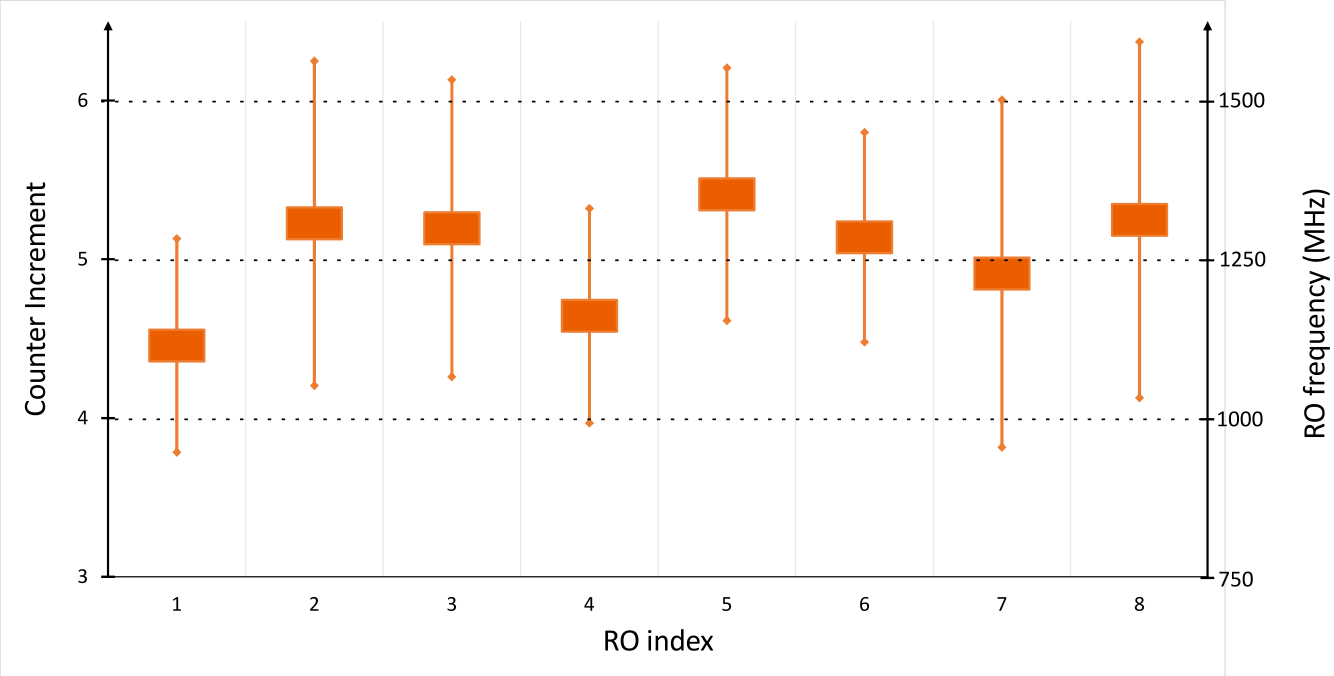
- A speed optimized design:
  - RO frequency reaches around **1.2 GHz**.
  - Johnson Ring-Counter provides **16 distinct states**.
  - Sampling register is cadenced at **250 MHz**



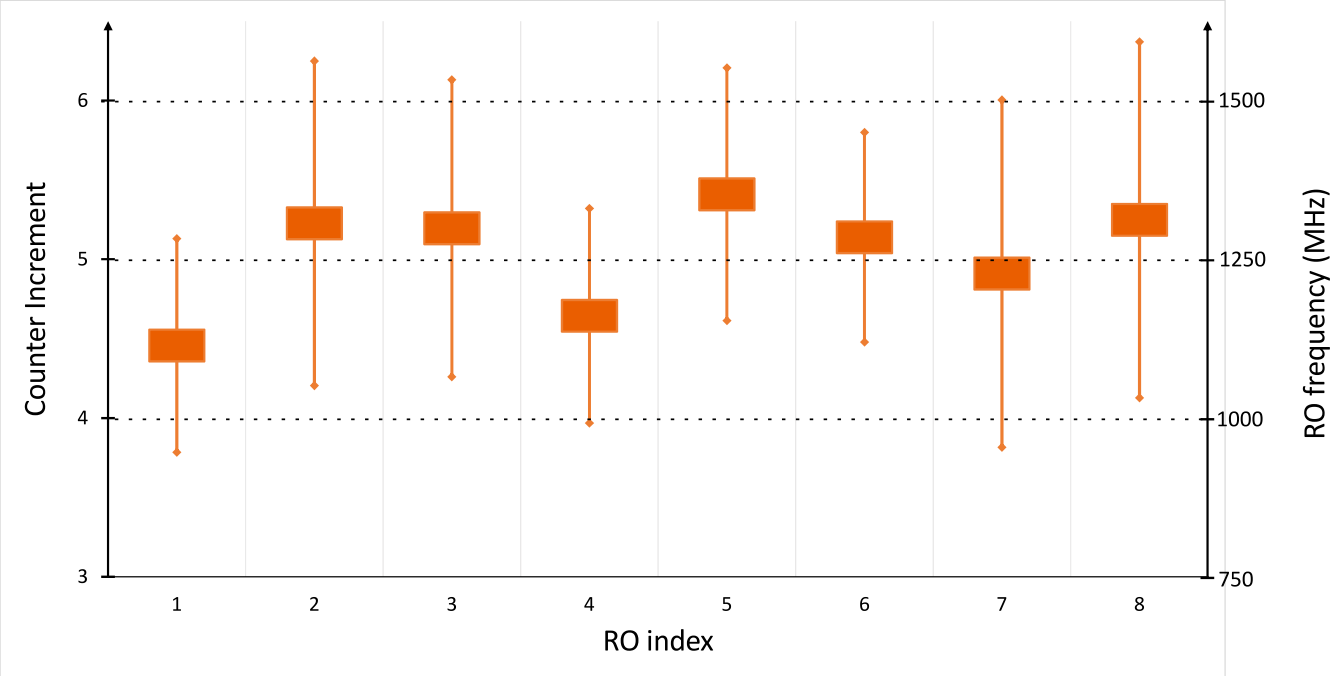
- A speed optimized design:
  - RO frequency reaches around **1.2 GHz**.
  - Johnson Ring-Counter provides **16 distinct states**.
  - Sampling register is cadenced at **250 MHz**
- Only 4-5 counter increments between each sampling !



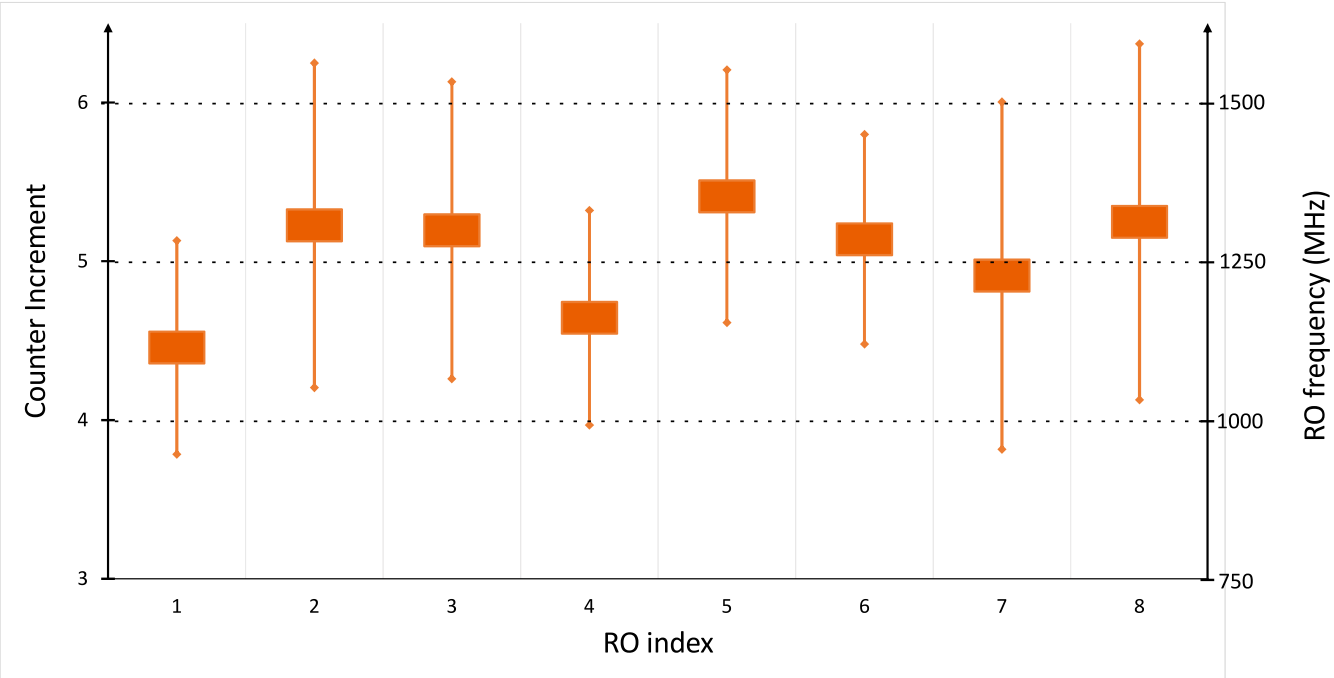
- Resolution relies on the number of RO-based sensor instances.
  - **Different ROs** run at **Different frequencies**.



- Resolution relies on the number of RO-based sensor instances.
  - **Different ROs** run at **Different frequencies**.
  - Each RO provide a peculiar information!

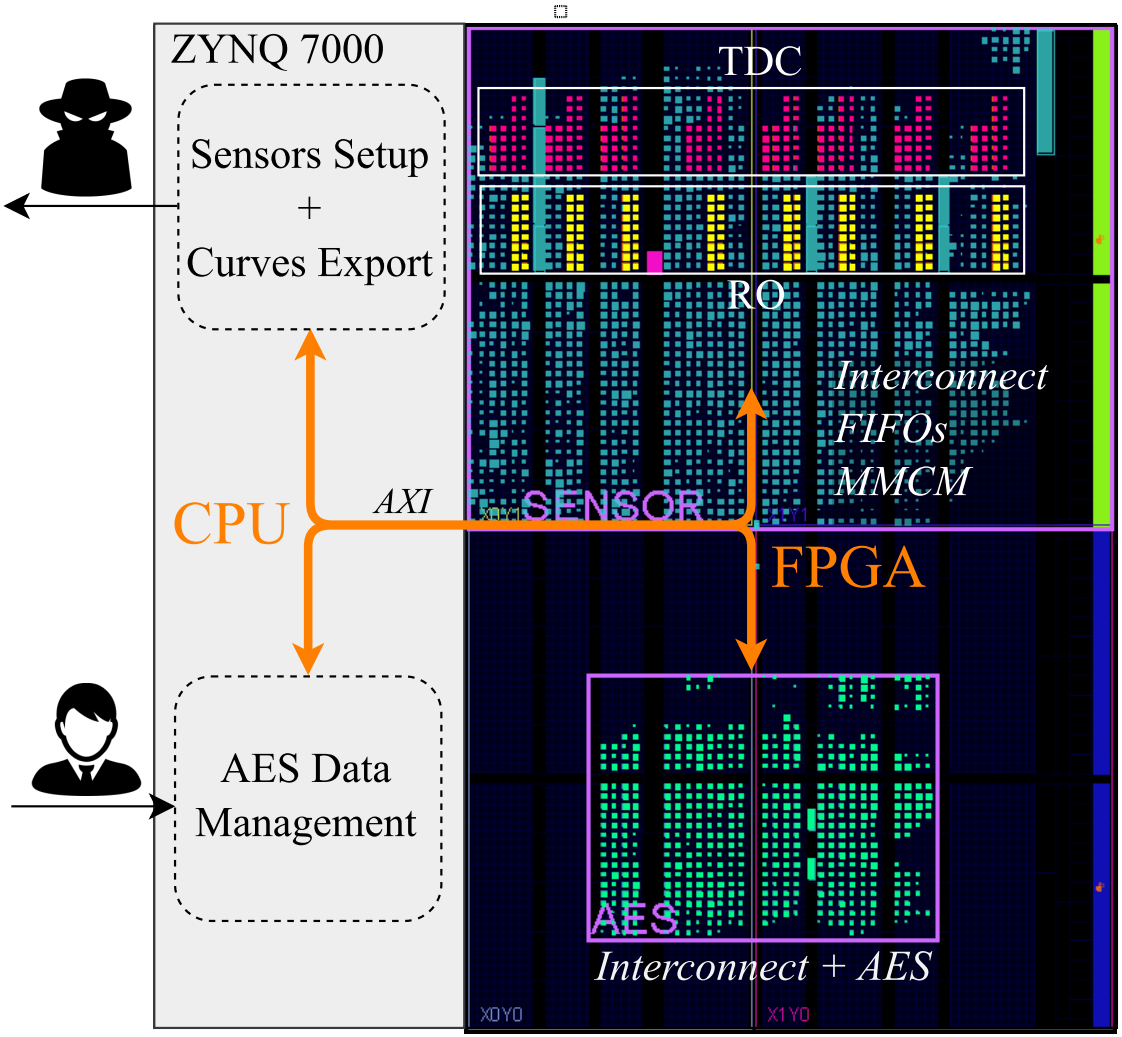


- Resolution relies on the number of RO-based sensor instances.
  - **Different ROs** run at **Different frequencies**.
  - Each RO provide a peculiar information!
  - **Multiplying ROs** enhances the **overall granularity**.

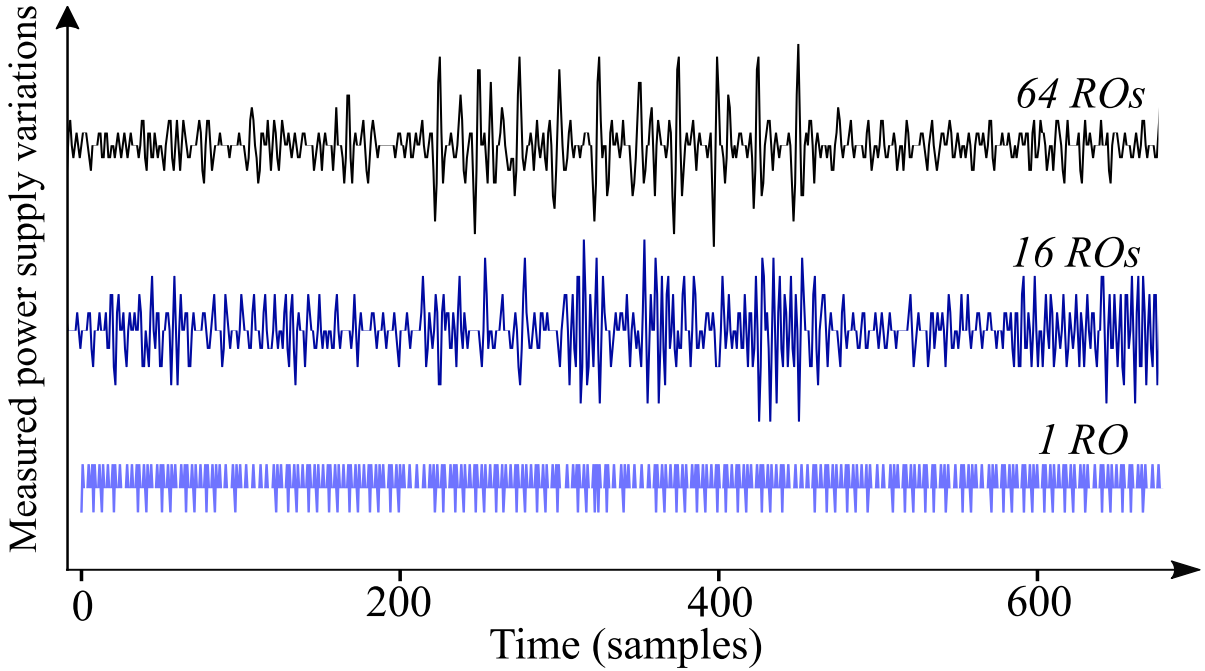


1. **Introduction** to remote FPGA-based hardware attacks.
2. Presentation of the proposed **RO-based sensor design**.
3. Experimental validation and SCA.
4. Comparison with other **SCA setups**.

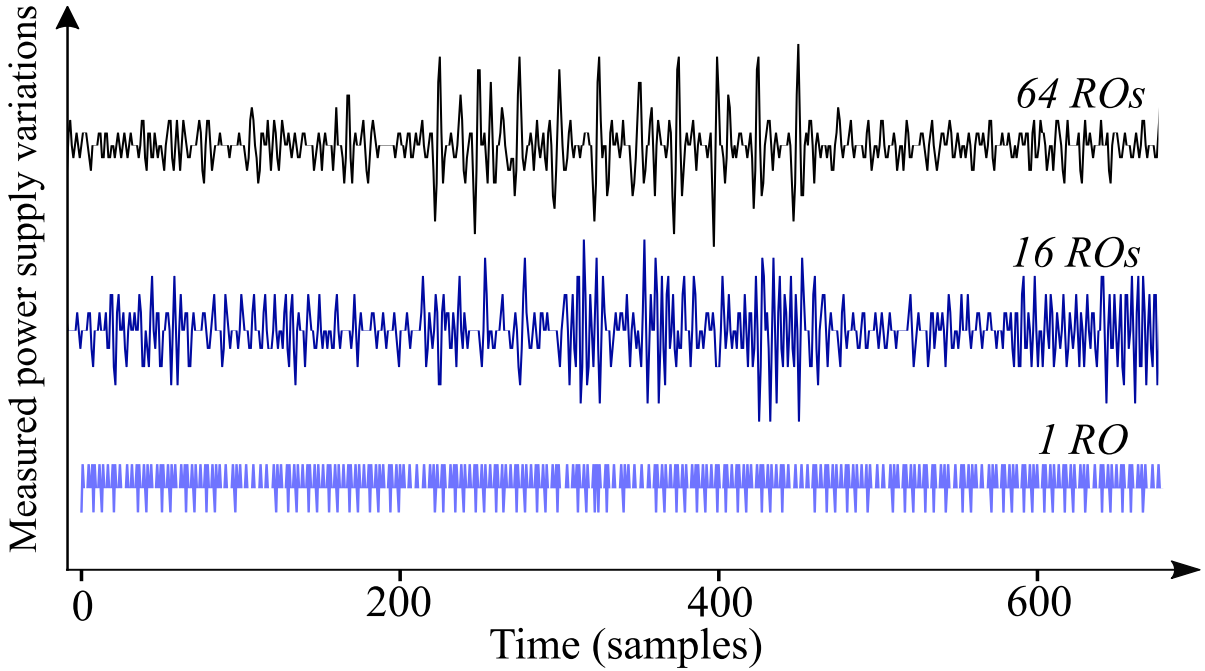
- Target: Xilinx Zynq 7000 heterogeneous SoC
- FPGA (Xilinx Artix-7): 64 RO-based sensors and AES algorithm
- CPU (ARM Cortex-A9): Traces export and AES management



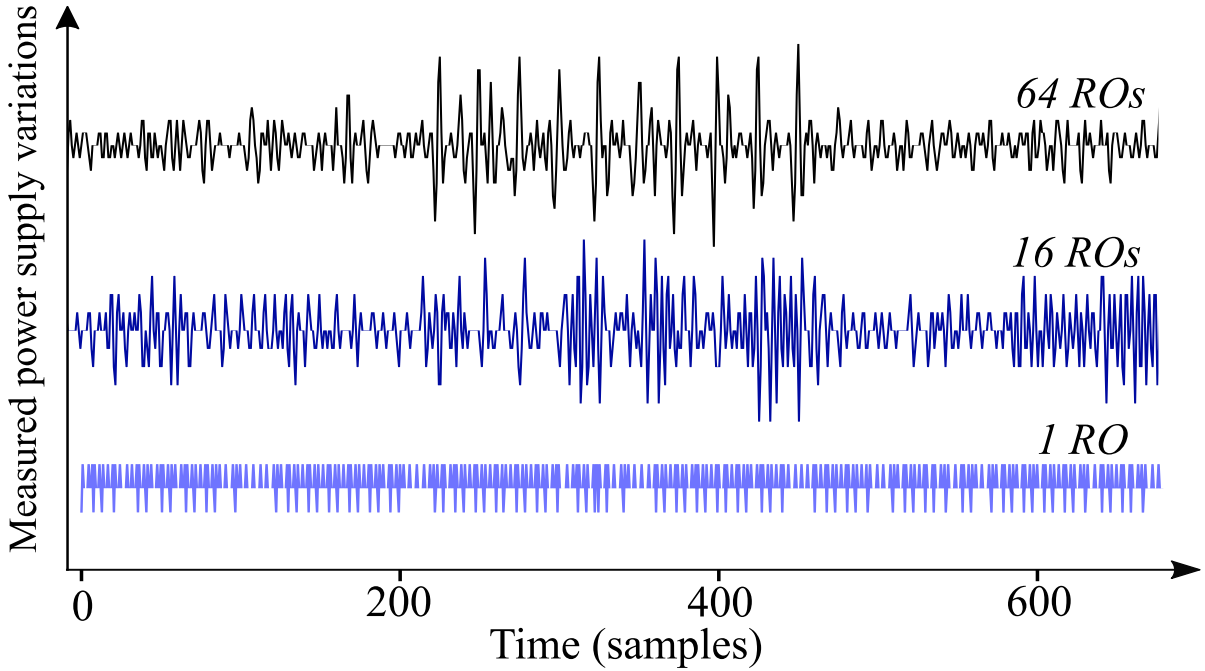
- Experiment on AES encryption @10MHz:
  - 1 acquisition using **1, 16 and 64 ROs** @250MHz.



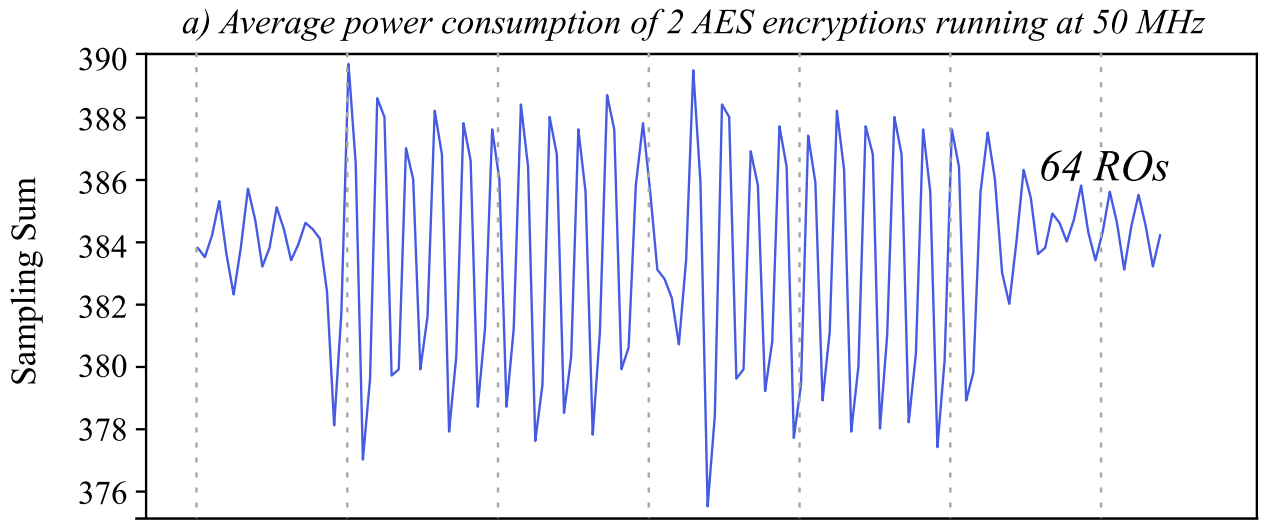
- Experiment on AES encryption @10MHz:
  - 1 acquisition using **1, 16 and 64 ROs** @250MHz.
  - RO contributions are **summed** and **averaged**.



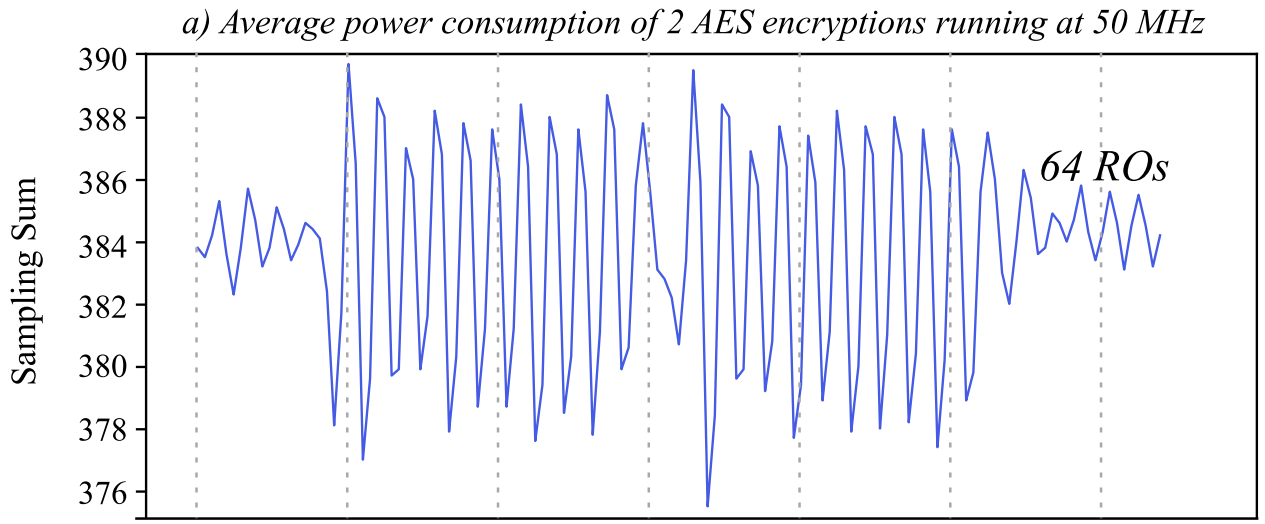
- Experiment on AES encryption @10MHz:
  - 1 acquisition using **1, 16 and 64 ROs** @250MHz.
  - RO contributions are **summed** and **averaged**.
  - The 10 AES rounds **gradually** appears.



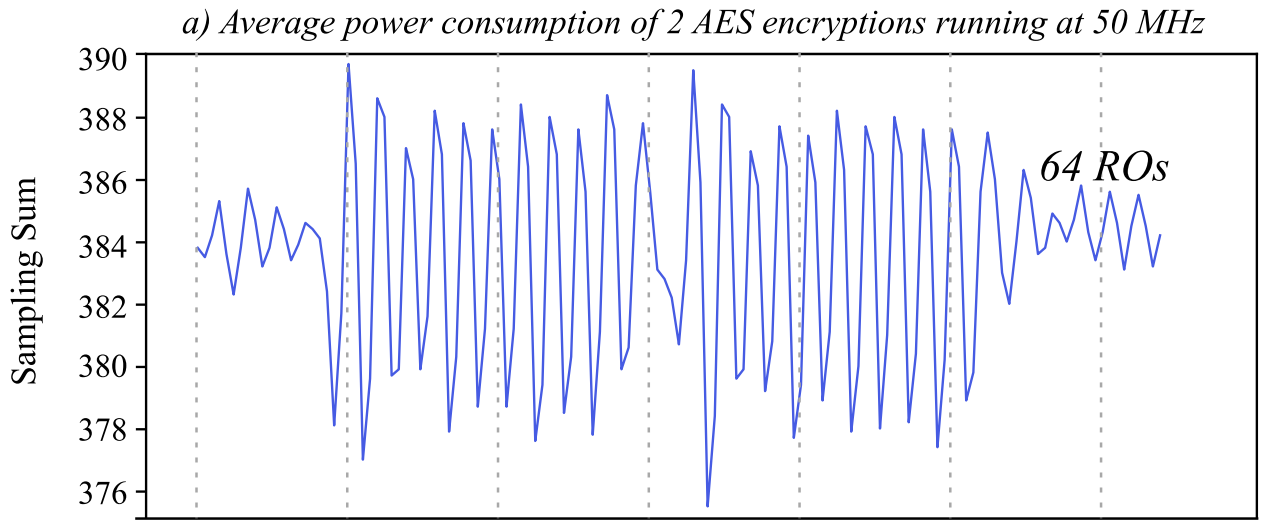
- Custom VHDL AES designed for the attack.
  - Key size **128 bit**, Datapath **128 bit**.



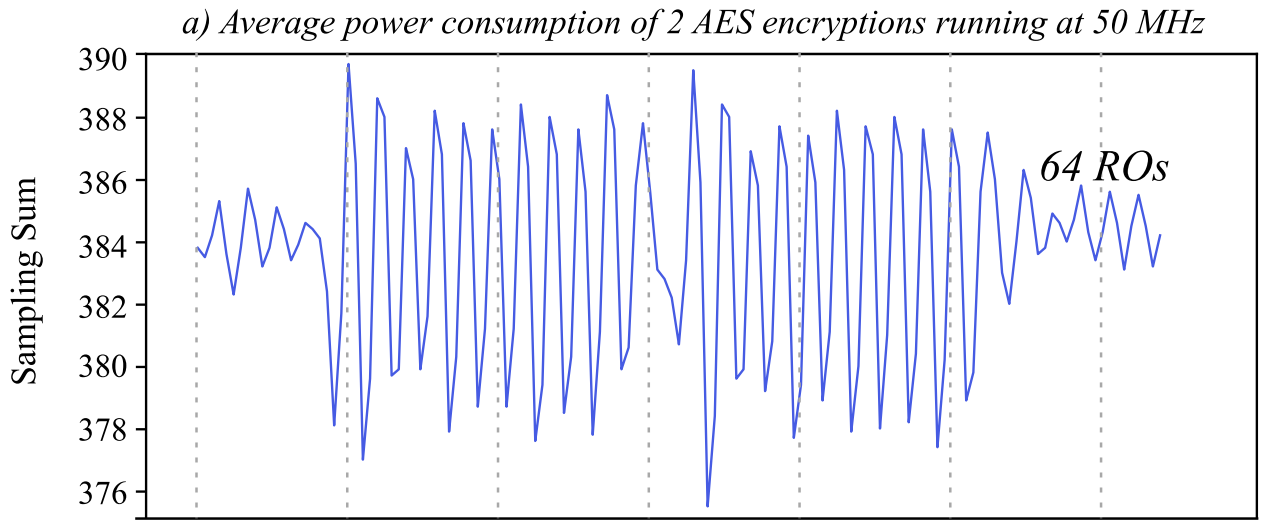
- Custom VHDL AES designed for the attack.
  - Key size **128 bit**, Datapath **128 bit**.
  - AES encryption time @50MHz $\Rightarrow$ **220***ns*



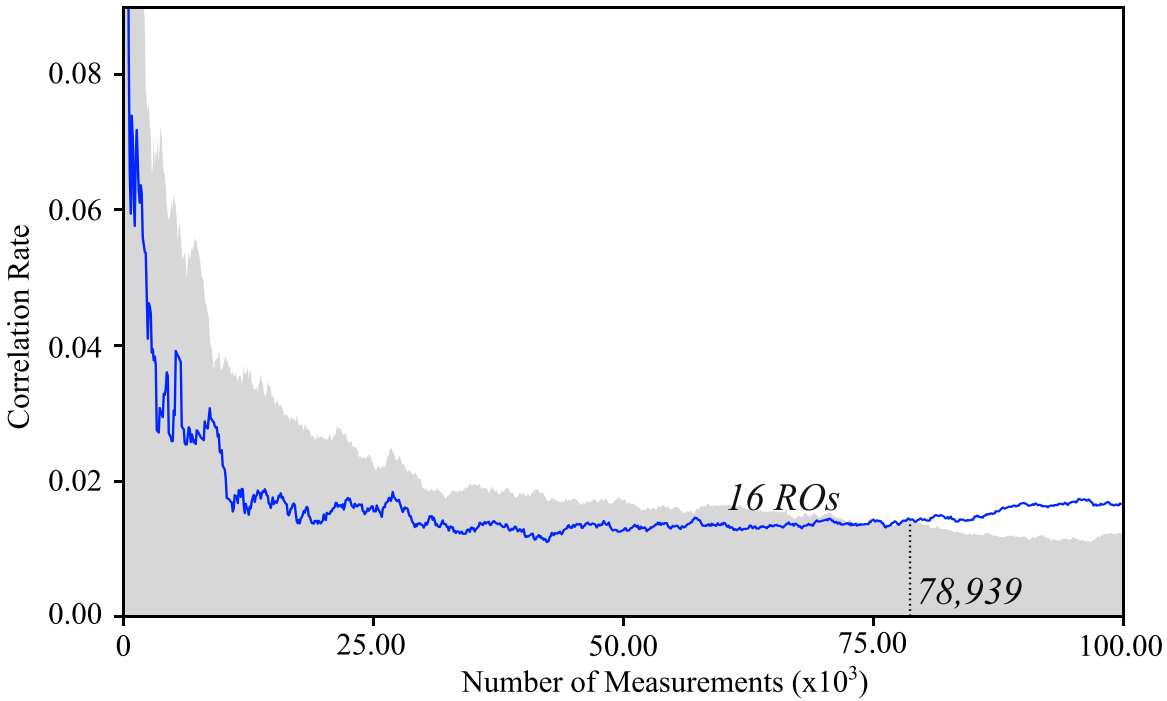
- Custom VHDL AES designed for the attack.
  - Key size **128 bit**, Datapath **128 bit**.
  - AES encryption time @50MHz $\Rightarrow$ **220***ns*
  - Synchronisation $\Rightarrow$ Encryption and measurement launched **simultaneously**.



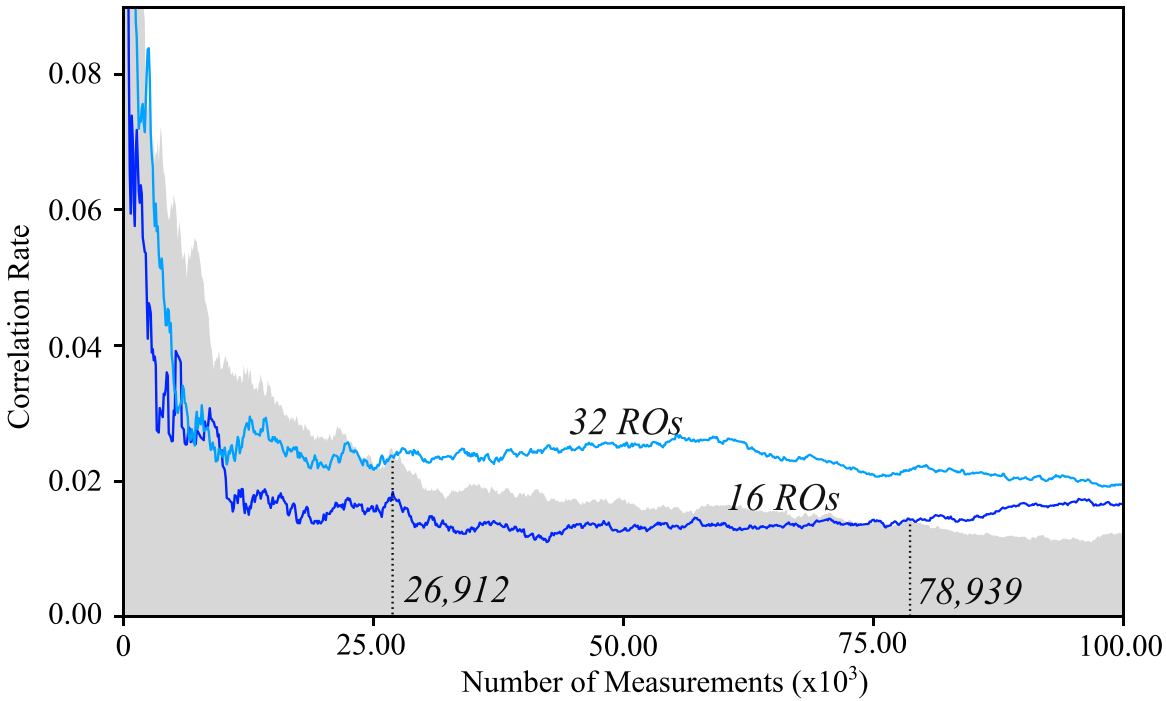
- Custom VHDL AES designed for the attack.
  - Key size **128 bit**, Datapath **128 bit**.
  - AES encryption time @50MHz $\Rightarrow$ **220***ns*
  - Synchronisation $\Rightarrow$ Encryption and measurement launched **simultaneously**.
  - CPA model $\Rightarrow$ AES Last round $HW[ARK_9 \oplus ARK_{10}]$



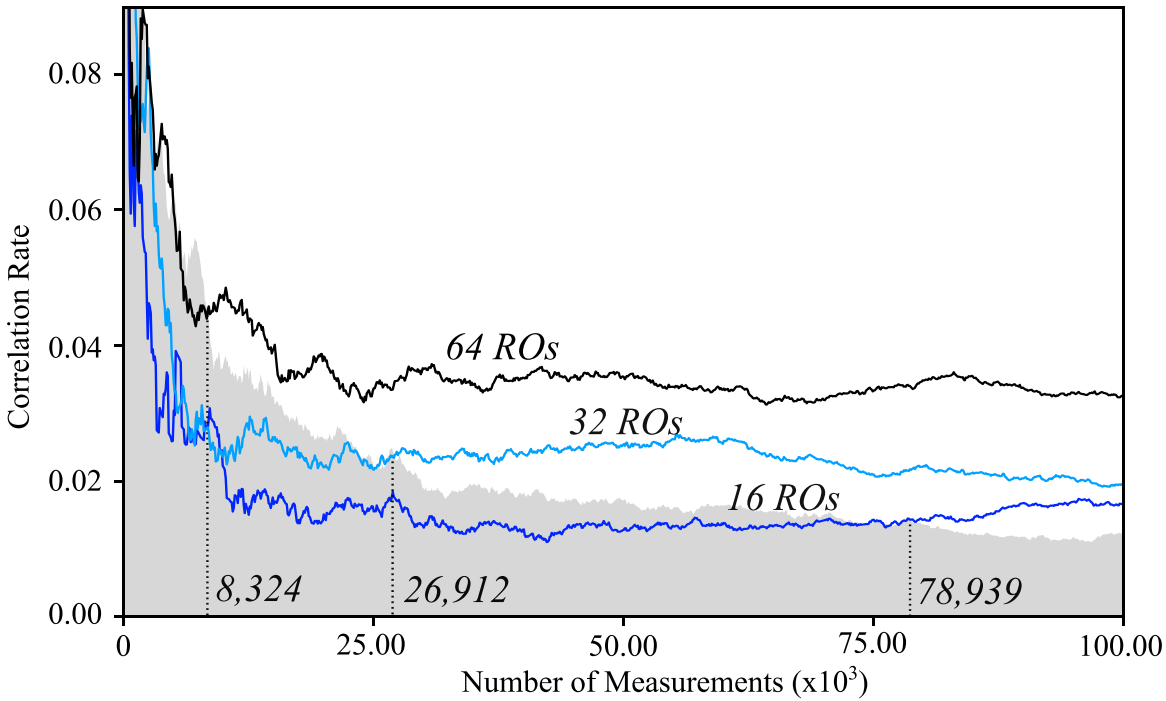
- **100,000 AES encryptions** are measured using 16, 32 and 64 ROs.
  - Using **16 ROs** $\rightarrow$ **78,939 traces** per AES key byte



- **100,000 AES encryptions** are measured using 16, 32 and 64 ROs.
  - Using **16 ROs** $\rightarrow$ **78,939 traces** per AES key byte
  - Using **32 ROs** $\rightarrow$ **26,912 traces** per AES key byte

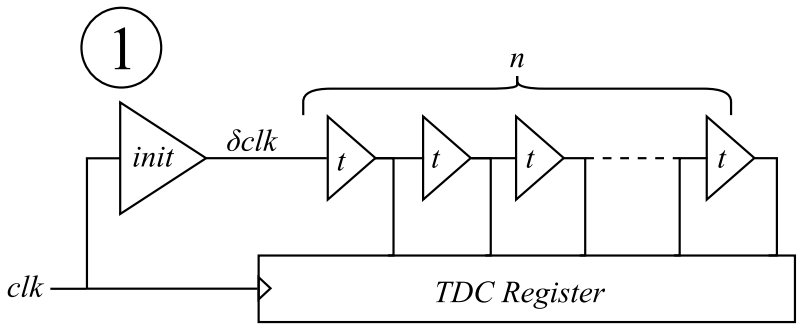


- **100,000 AES encryptions** are measured using 16, 32 and 64 ROs.
  - Using **16 ROs** → **78,939 traces** per AES key byte
  - Using **32 ROs** → **26,912 traces** per AES key byte
  - Using **64 ROs** → **8,324 traces** per AES key byte

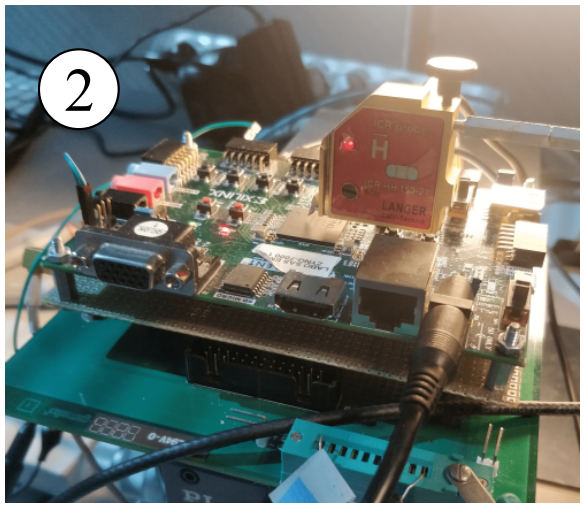


1. **Introduction** to remote FPGA-based hardware attacks.
2. Presentation of the proposed **RO-based sensor design**.
3. Experimental validation and SCA.
4. Comparison with other **SCA setups**.

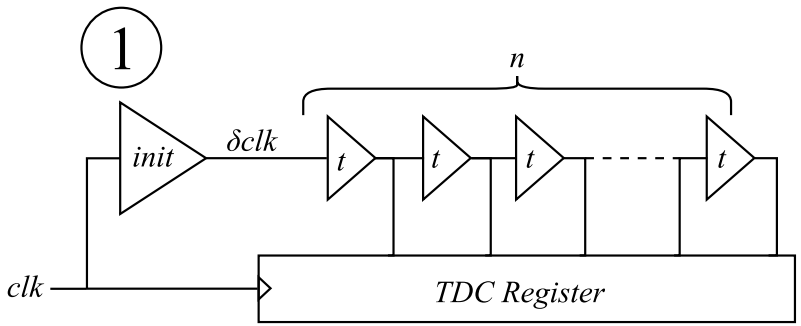
- Goal: **challenge** our sensor results regarding other SCA setups.
- Experimental Setup ① (internal remote):
  - Time-to-digital converter (delay line)
  - TDC Sampling Rate: **250MHz**
- Experimental Setup ② (external local):
  - EM Probe: Langer ICR HH 150
  - Oscilloscope Sampling Rate: **5GS/s**



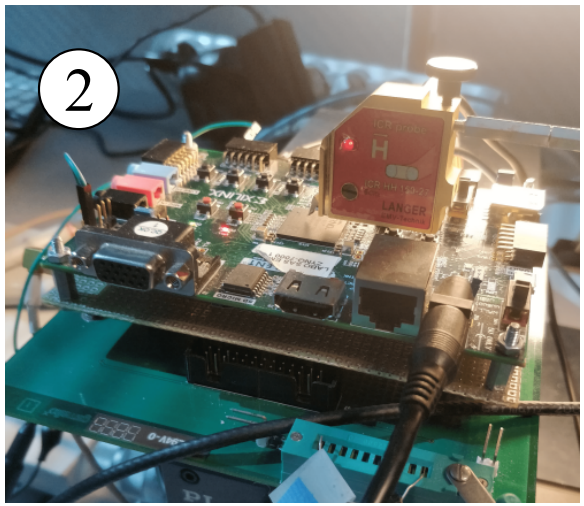
Time-to-Digital Converter



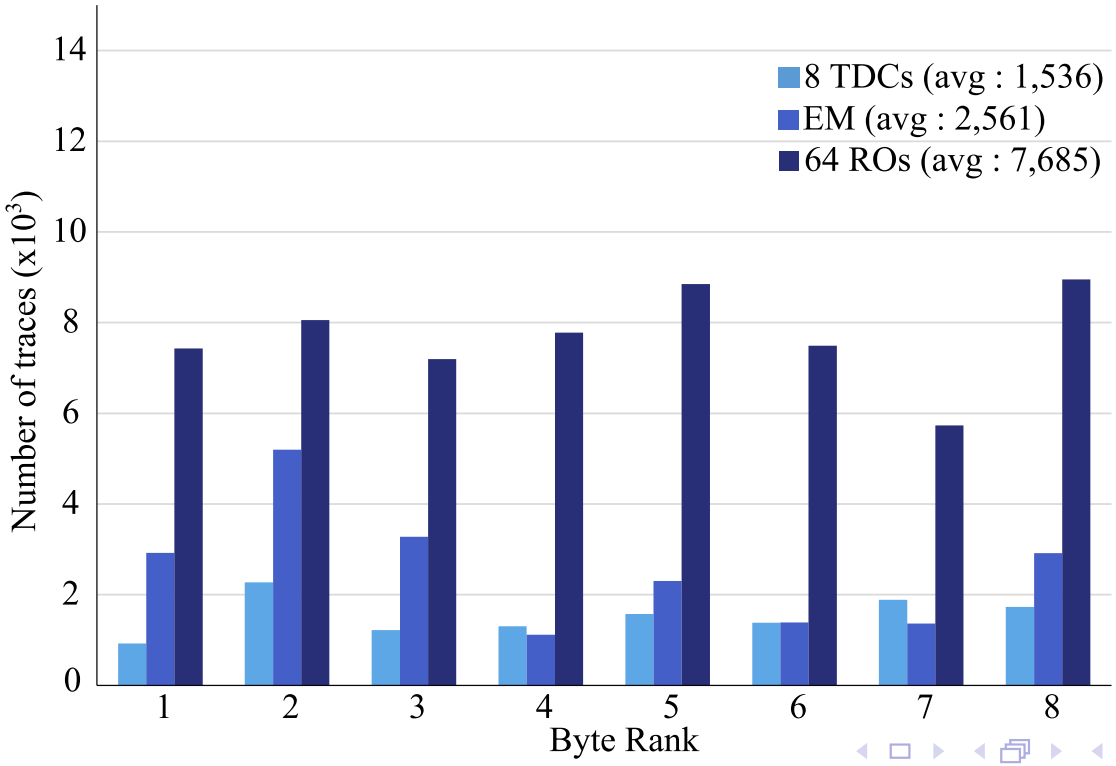
- Goal: **challenge** our sensor results regarding other SCA setups.
- Experimental Setup ① (internal remote):
  - Time-to-digital converter (delay line)
  - TDC Sampling Rate: **250MHz**
- Experimental Setup ② (external local):
  - EM Probe: Langer ICR HH 150
  - Oscilloscope Sampling Rate: **5GS/s**



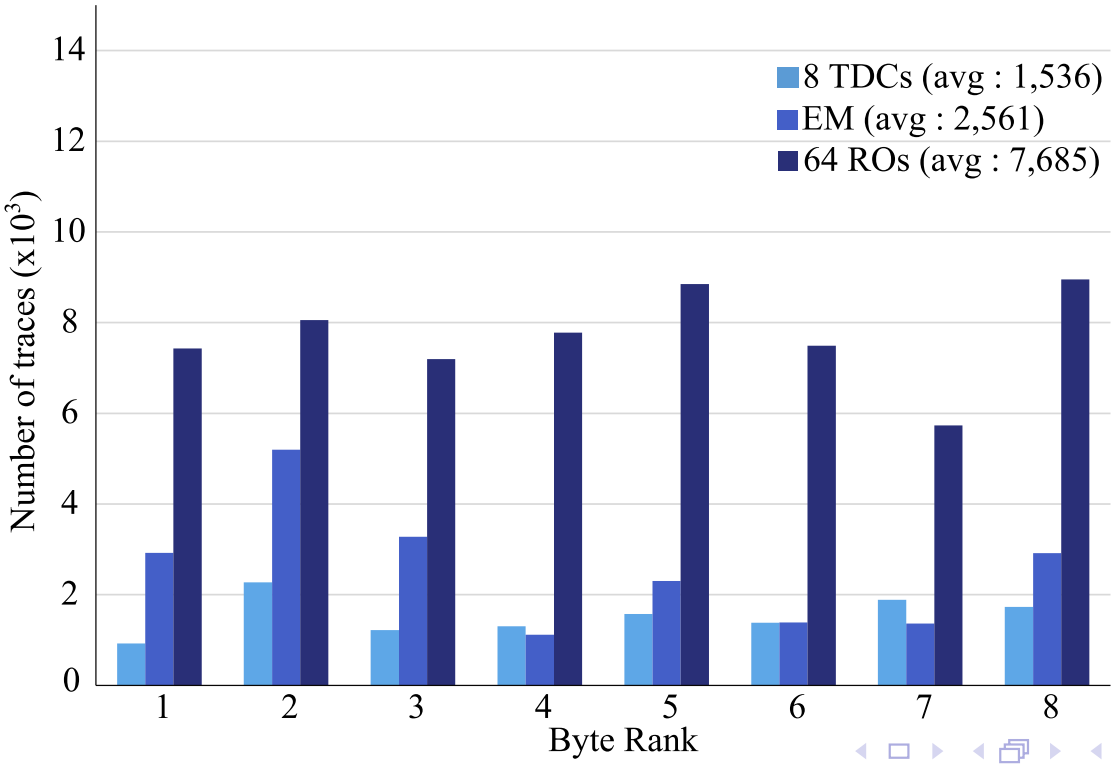
Time-to-Digital Converter



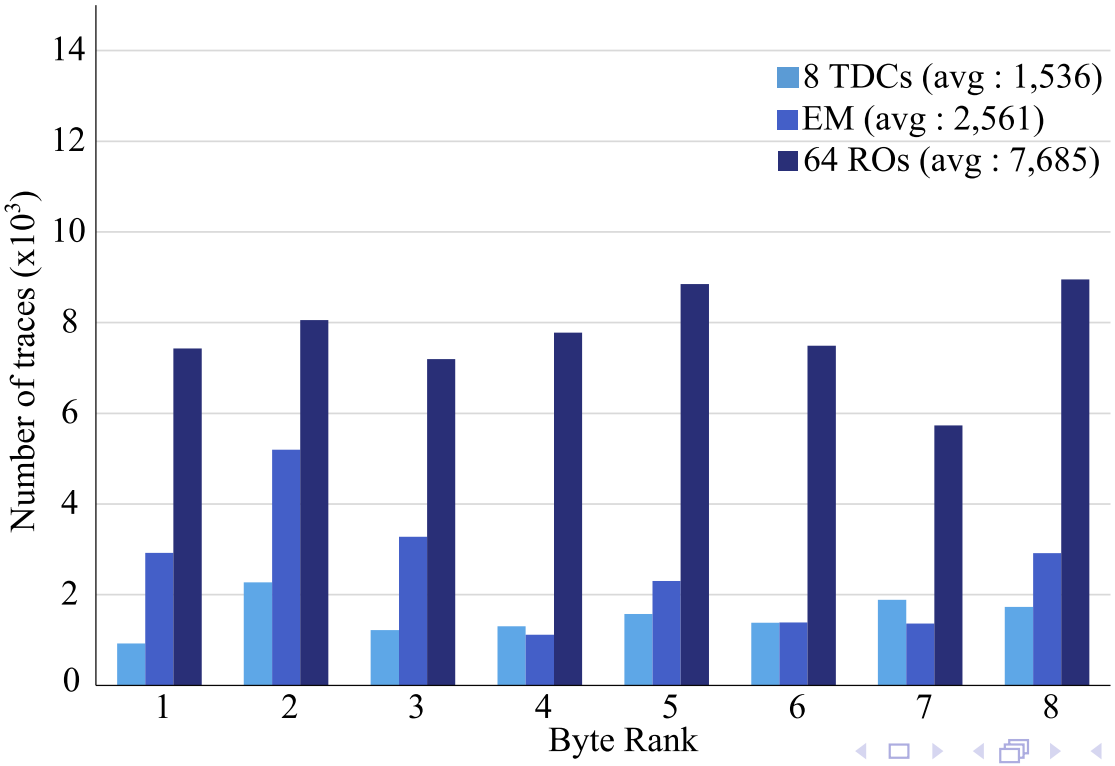
- Goal: **challenge** our sensor results with TDC-based sensor.
- RO provides "similar" results to other setups.
  - Using **RO** $\rightarrow$ **7,685 traces** per AES key byte



- Goal: **challenge** our sensor results with TDC-based sensor.
- RO provides "similar" results to other setups.
  - Using **RO** $\rightarrow$ **7,685 traces** per AES key byte
  - Using **EM** $\rightarrow$ **2,561 traces** per AES key byte



- Goal: **challenge** our sensor results with TDC-based sensor.
- RO provides "similar" results to other setups.
  - Using **RO** $\rightarrow$ **7,685 traces** per AES key byte
  - Using **EM** $\rightarrow$ **2,561 traces** per AES key byte
  - Using **TDC** $\rightarrow$ **1,536 traces** per AES key byte



Conclusion

- Our main contribution is a new RO-based sensor capable of:
  - Reaching **high sampling frequencies** with decent resolution.

Conclusion

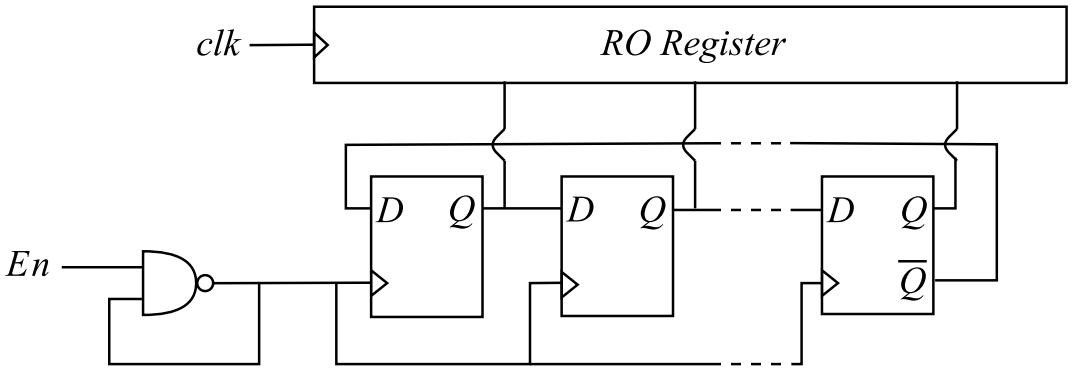
- Our main contribution is a new RO-based sensor capable of:
  - Reaching **high sampling frequencies** with decent resolution.
  - **Performing remote CPA attacks** on secret key algorithms (AES).

Conclusion

- Our main contribution is a new RO-based sensor capable of:
  - Reaching **high sampling frequencies** with decent resolution.
  - **Performing remote CPA attacks** on secret key algorithms (AES).
  - Providing similar results to existing SCA setups.

Conclusion

- Our main contribution is a new RO-based sensor capable of:
  - Reaching **high sampling frequencies** with decent resolution.
  - **Performing remote CPA attacks** on secret key algorithms (AES).
  - Providing similar results to existing SCA setups.
- It's an ideal alternative for monitoring fine-grained high-speed voltage fluctuations in SoCs



Thank you! Questions?

joseph.gravellier@emse.fr