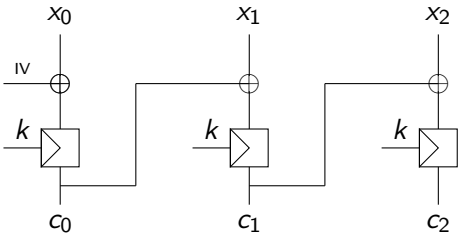
Simulatable Leakage, Revisited

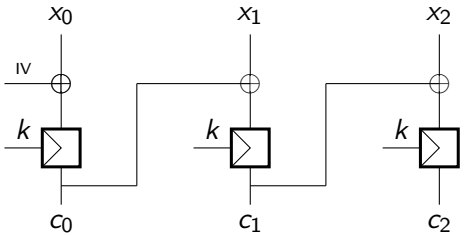
Emilie Deprez, Charles Momin, and François-Xavier Standaert

CASCADE 2026

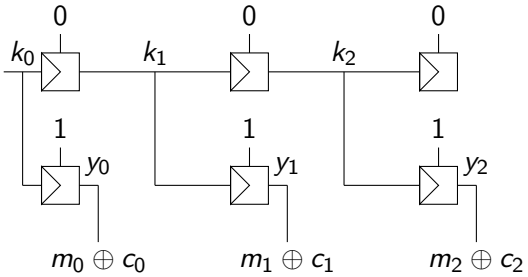
What is leakage-resilience ?



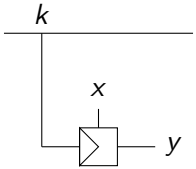
What is leakage-resilience ?



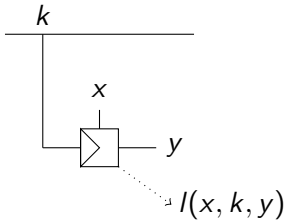
What is leakage-resilience ?



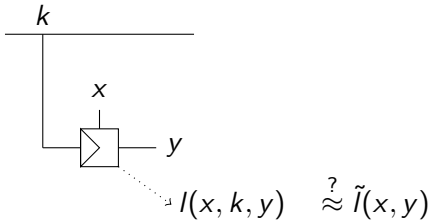
How to formalize SPA security ?



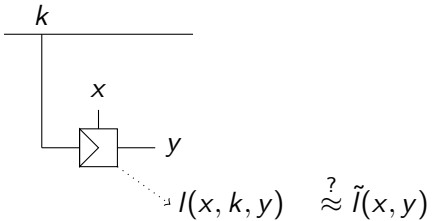
How to formalize SPA security ?



How to formalize SPA security ?

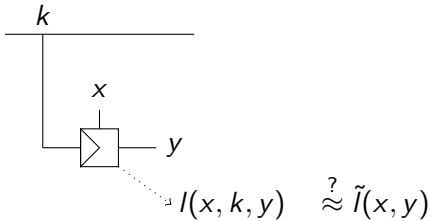


How to formalize SPA security ?



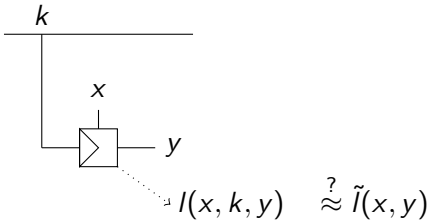
If we can efficiently simulate $l(x, k, y)$ without knowledge of k then the leakage can be viewed as independent of k.

How to formalize SPA security ?



If we can efficiently simulate $l(x, k, y)$ without knowledge of k then the leakage can be viewed as independent of k.
$\rightarrow$ 1-simulability game

How to formalize SPA security ?



If we can efficiently simulate $l(x, k, y)$ without knowledge of k then the leakage can be viewed as independent of k.

$\rightarrow$ 1-simulability game

$\rightarrow$ q-simulability game $=$ q block ciphers use k

How to formalize SPA security ?

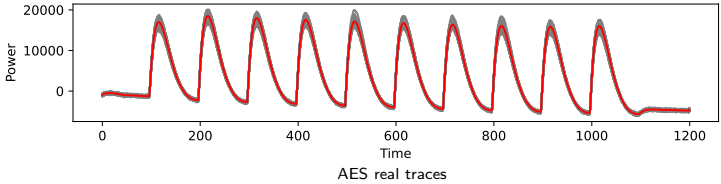
Question: How to efficiently and concretely simulate an indistinguishable leakage without key knowledge, but with the implementation ?

How to formalize SPA security ?

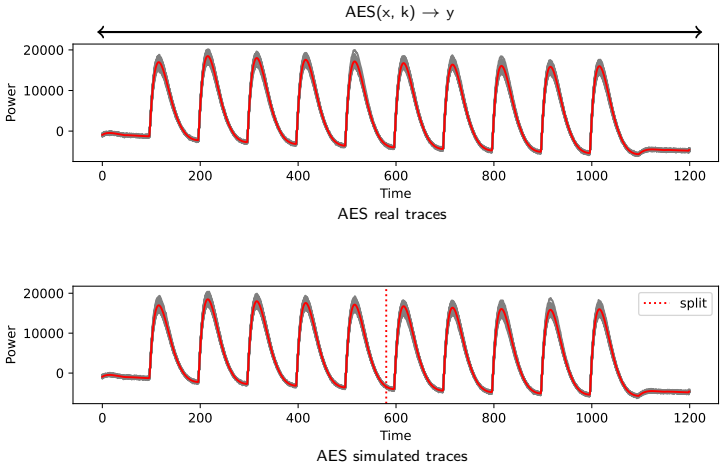
Question: How to efficiently and concretely simulate an indistinguishable leakage without key knowledge, but with the implementation ?

Attempt: the split-and-concatenate simulator

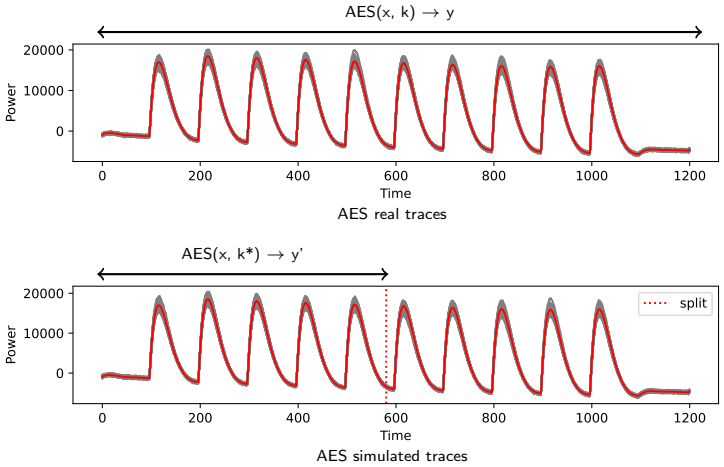
The split-and-concatenate simulator: principle



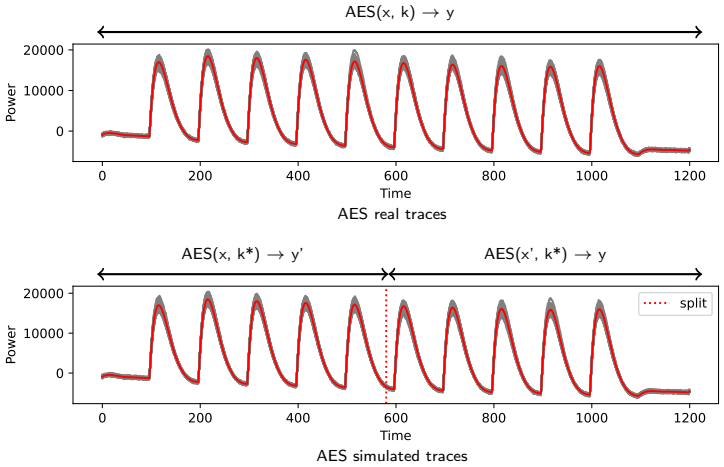
The split-and-concatenate simulator: principle



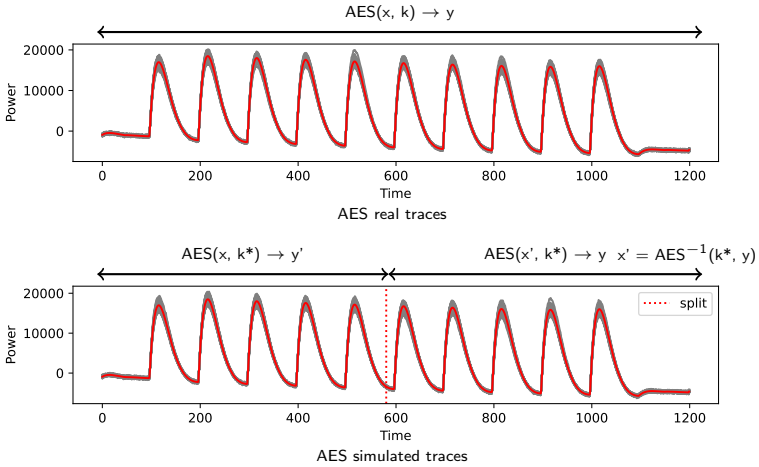
The split-and-concatenate simulator: principle



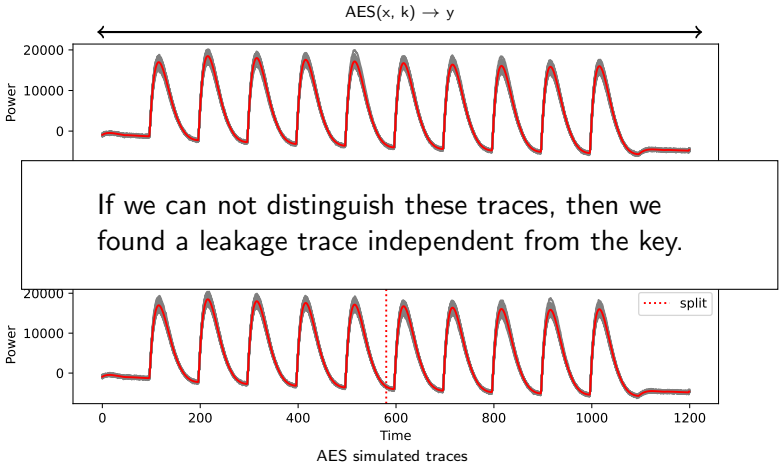
The split-and-concatenate simulator: principle



The split-and-concatenate simulator: principle



The split-and-concatenate simulator: principle

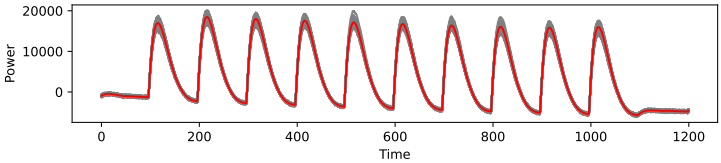


The S&C simulator: the correlation distinguisher

- In 2014 Longo et al. proposed a distinguisher by cross-correlation

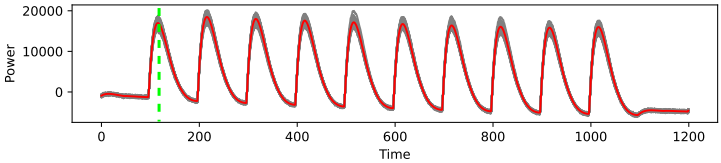
The S&C simulator: the correlation distinguisher

- In 2014 Longo et al. proposed a distinguisher by cross-correlation
- Idea:
  1. Take plenty of simulated traces with different plaintext, key and ciphertext



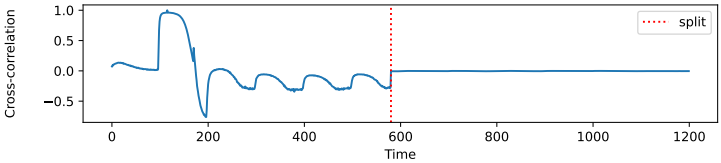
The S&C simulator: the correlation distinguisher

- In 2014 Longo et al. proposed a distinguisher by cross-correlation
- Idea:
  1. Take plenty of simulated traces with different plaintext, key and ciphertext
  2. Choose a time index

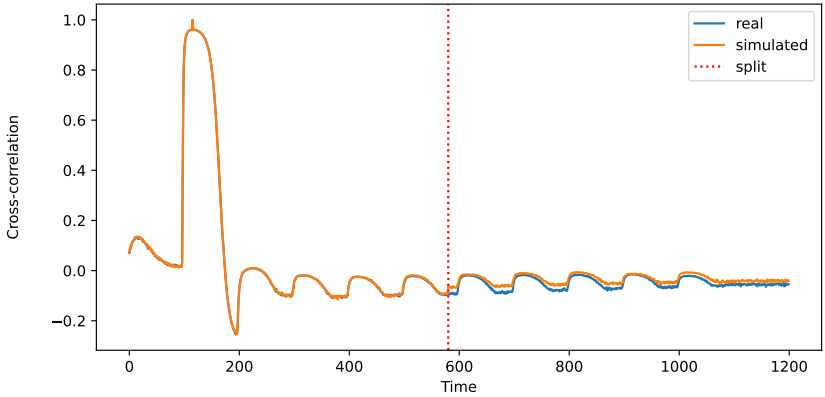


The S&C simulator: the correlation distinguisher

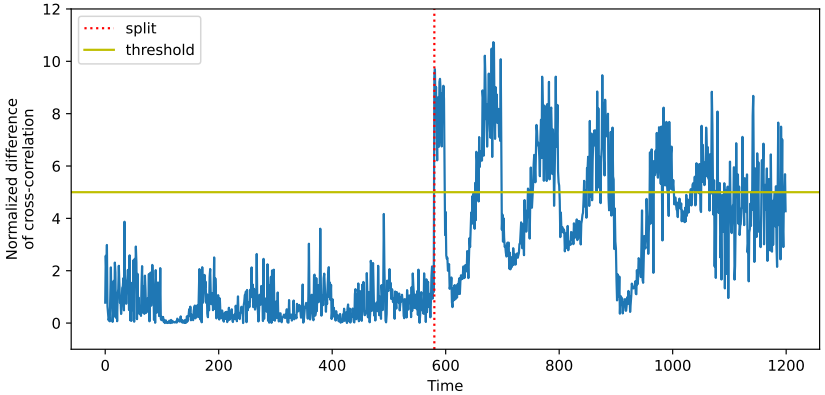
- In 2014 Longo et al. proposed a distinguisher by cross-correlation
- Idea:
  1. Take plenty of simulated traces with different plaintext, key and ciphertext
  2. Choose a time index
  3. Perform the correlation with the remaining time indexes



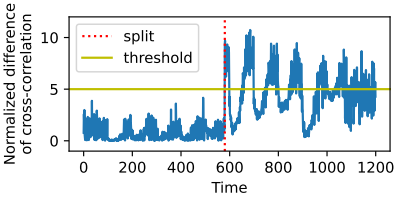
The S&C simulator: the correlation distinguisher



The S&C simulator: the correlation distinguisher

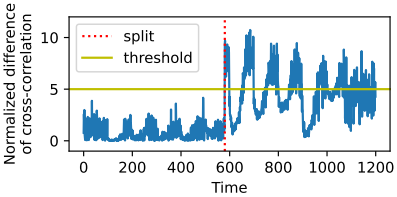


The S&C simulator: the correlation distinguisher

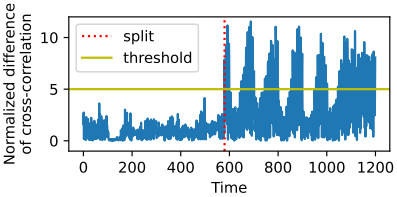


Spartan-6

The S&C simulator: the correlation distinguisher



Spartan-6



Artix-7

The S&C simulator: discussion

The concrete simulator:

The S&C simulator: discussion

The concrete simulator:

- based exclusively on manipulating traces

The S&C simulator: discussion

The concrete simulator:

- based exclusively on manipulating traces
- unlikely to provide confident security guarantees

The S&C simulator: discussion

The concrete simulator:

- based exclusively on manipulating traces
- unlikely to provide confident security guarantees
- a perfect simulation would require an extremely accurate modeling of the leakage function

Theoretical simulator

Theorem[ORR+24,BMO+26]: $L(x) = \delta(x) + n$ can be efficiently simulated from T bits of bounded leakage.

Theoretical simulator

Theorem[ORR+24,BMO+26]: $L(x) = \delta(x) + n$ can be efficiently simulated from T bits of bounded leakage.

- Assume a perfect distribution knowledge

Theoretical simulator

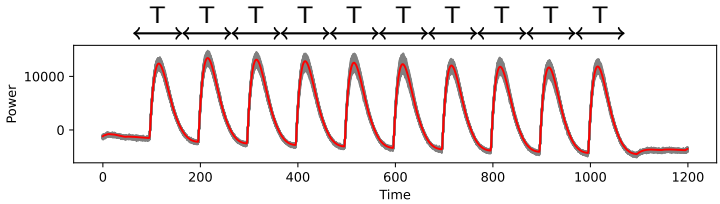
Theorem[ORR+24,BMO+26]: $L(x) = \delta(x) + n$ can be efficiently simulated from T bits of bounded leakage.

- Assume a perfect distribution knowledge
- T depends on the information

Theoretical simulator

Theorem[ORR+24,BMO+26]: $L(x) = \delta(x) + n$ can be efficiently simulated from T bits of bounded leakage.

- Assume a perfect distribution knowledge
- T depends on the information
- Apply the theorem to each round of AES $\rightarrow$ needs 10x Tbits

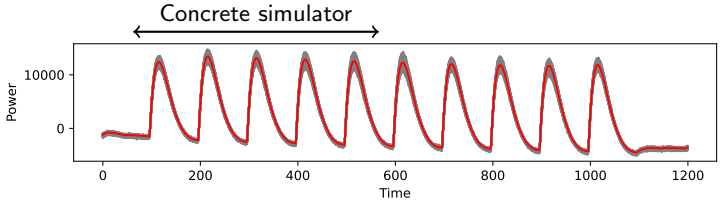


Hybrid simulator

Idea: Combine the pros and cons of concrete and theoretical simulator

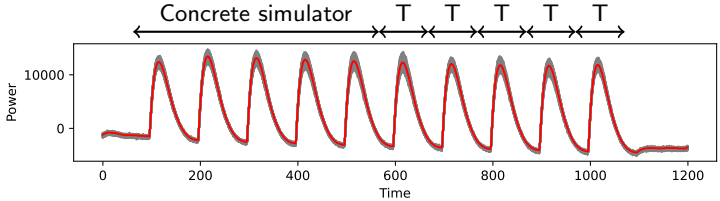
Hybrid simulator

Idea: Combine the pros and cons of concrete and theoretical simulator



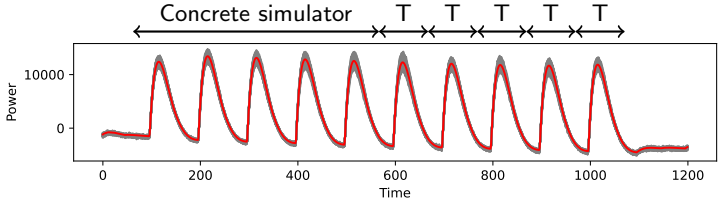
Hybrid simulator

Idea: Combine the pros and cons of concrete and theoretical simulator



Hybrid simulator

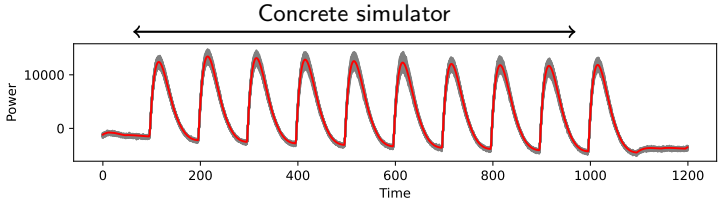
Idea: Combine the pros and cons of concrete and theoretical simulator



Can we do better ?

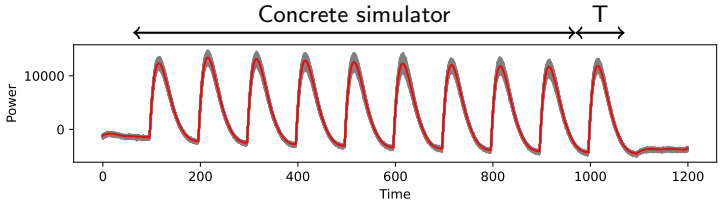
Hybrid simulator

Idea: Combine the pros and cons of concrete and theoretical simulator



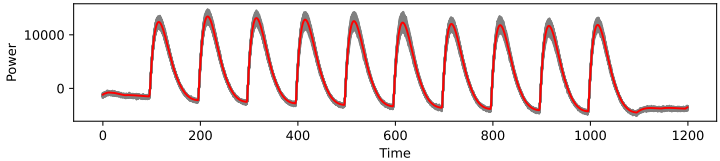
Hybrid simulator

Idea: Combine the pros and cons of concrete and theoretical simulator



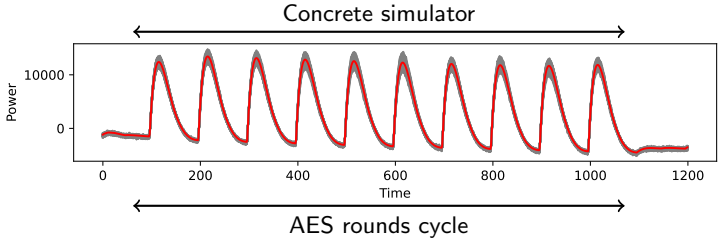
Hybrid simulator

Idea: Combine the pros and cons of concrete and theoretical simulator



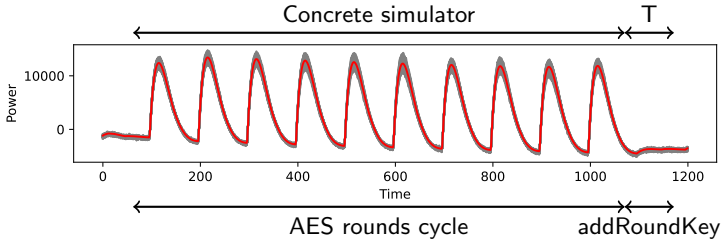
Hybrid simulator

Idea: Combine the pros and cons of concrete and theoretical simulator



Hybrid simulator

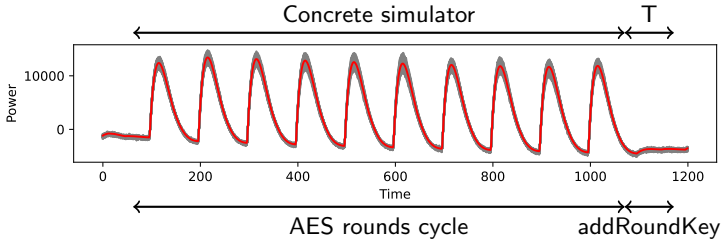
Idea: Combine the pros and cons of concrete and theoretical simulator



- Last addRoundKey in an extra clock cycle

Hybrid simulator

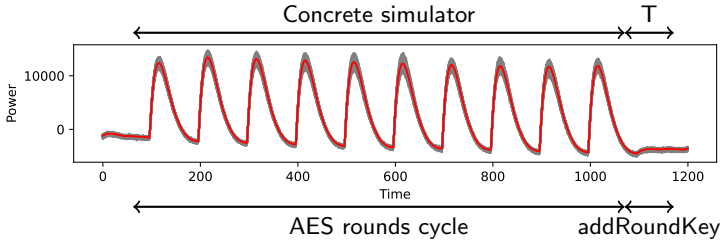
Idea: Combine the pros and cons of concrete and theoretical simulator



- Last addRoundKey in an extra clock cycle
- T decreases when SNR and/or MI decrease

Hybrid simulator

Idea: Combine the pros and cons of concrete and theoretical simulator



- Last addRoundKey in an extra clock cycle
- T decreases when SNR and/or MI decrease
- Our goal: Reducing key dependency in the last cycle to reduce the need of bounded leakage

The hybrid simulator: theoretical simulation

Simulate the last cycle:

The hybrid simulator: theoretical simulation

Simulate the last cycle:

- Assume leakage mostly depends on public ciphertext

The hybrid simulator: theoretical simulation

Simulate the last cycle:

- Assume leakage mostly depends on public ciphertext
- Masking the final cycle to be independent as possible from the secret key

The hybrid simulator: theoretical simulation

Simulate the last cycle:

- Assume leakage mostly depends on public ciphertext
- Masking the final cycle to be independent as possible from the secret key
  - $y_0 = k'_9 \oplus r$

The hybrid simulator: theoretical simulation

Simulate the last cycle:

- Assume leakage mostly depends on public ciphertext
- Masking the final cycle to be independent as possible from the secret key
  - $y_0 = k'_9 \oplus r$
  - $y_1 = SB_9 \oplus r$

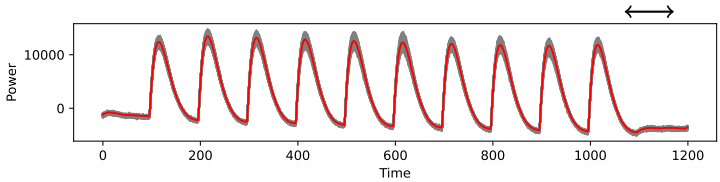
The hybrid simulator: theoretical simulation

Simulate the last cycle:

- Assume leakage mostly depends on public ciphertext
- Masking the final cycle to be independent as possible from the secret key
  - $y_0 = k'_9 \oplus r$
  - $y_1 = SB_9 \oplus r$
  - $y = y_0 \oplus y_1$

The hybrid simulator: residual leakage analysis

- Power consumption:
  $\rightarrow$ The final cycle consumes significantly less power.



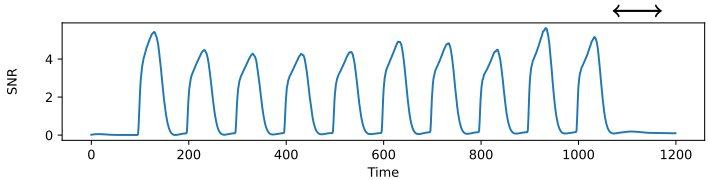
The hybrid simulator: residual leakage analysis

Quantifying residual key dependency

The hybrid simulator: residual leakage analysis

Quantifying residual key dependency

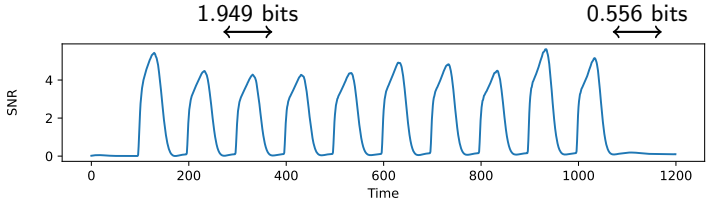
- SNR of the full AES state:
  $\rightarrow$ Drop (but still present) for final cycle.



The hybrid simulator: residual leakage analysis

Quantifying residual key dependency

- SNR of the full AES state:
  $\rightarrow$ Drop (but still present) for final cycle.
- Quantifying the information:
  $\rightarrow$ Third cycle $\approx$ 4x more informative than the last cycle.



Conclusion

- **q-sim game** goal: formalize the notion of SPA security
- **Concrete simulator** (split-and-concatenate): hard to achieve in practice
- **Theoretical simulator**: a lot (too much ?) information required
- **Hybrid simulator**: concatenate concrete + theoretical simulator
  - take advantage of both
  - bounded leakage only for the last cycle
  - goal: reducing key dependency in the last cycle
- **Further work**: better formalizing these findings, non-hermetic approaches

Thank you for listening

References

- **[ORR+24]** Obremski, M., Ribeiro, J., Roy, L., Standaert, F. X., & Venturi, D. (2024, August). Improved reductions from noisy to bounded and probing leakages via hockey-stick divergences. In Annual International Cryptology Conference (pp. 461-491). Cham: Springer Nature Switzerland.
- **[BMO+26]** Béguinot, J., Mukherjee, A., Obresmki, M., Ribeiro, J., Roy, L., Standaert, F.X., Venturi, D.: Simulating noisy leakage with bounded leakage: Simpler, better, faster. Cryptology ePrint Archive, Paper 2026/357 (2026), https://eprint.iacr.org/2026/357