KU LEUVEN

Attacking Hardware Random Number Generators in a Multi-Tenant Scenario

Yrjo Koyen, Adriaan Peetermans, Vladimir Rožić and Ingrid Verbauwhede

Workshop on Fault Diagnosis and Tolerance in Cryptography
September 13, 2020

fwo

COSIC

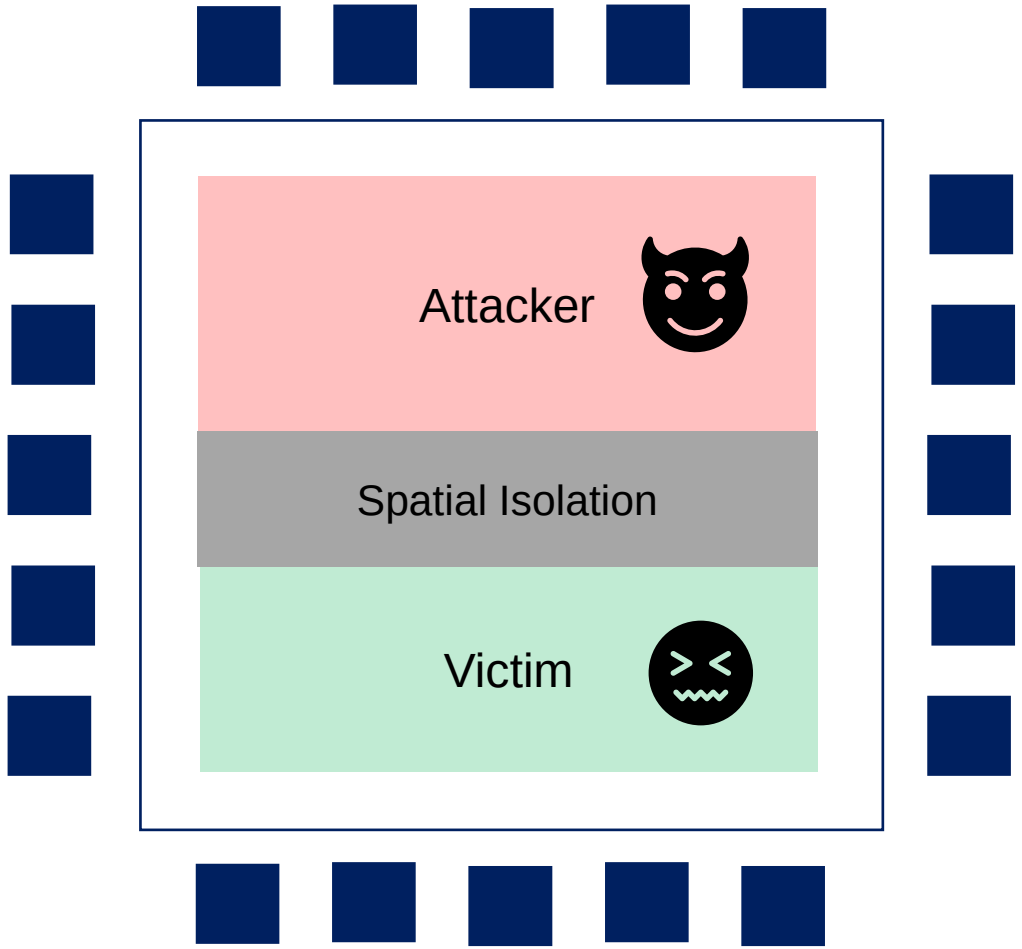
FPGAs in the Cloud

- Advantages
  - Low initial cost investment
  - Easy access
  - Easy dissemination
- Custom accelerators
  - Performance
  - Energy efficiency
  - Ability to modify accelerator functions
- Applications
  - Don’t require real-time access to I/O
  - Don’t have to push FPGA performance to a limit
- Sensitive data

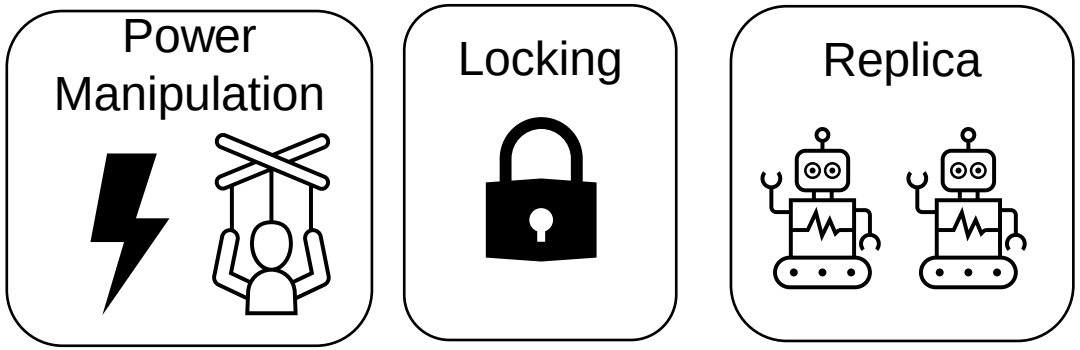
HUAWEI CLOUD

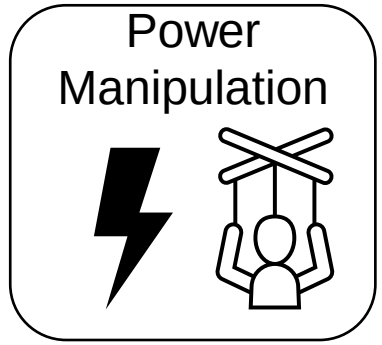
Threat Model

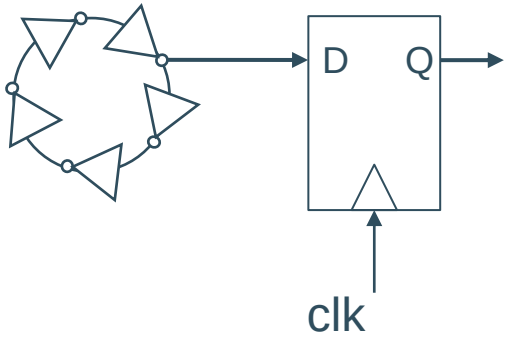
- Spatially isolated tenants
- Shared PDN
- No physical access to the device
- Secure Toolchain
- No restrictions on individual designs

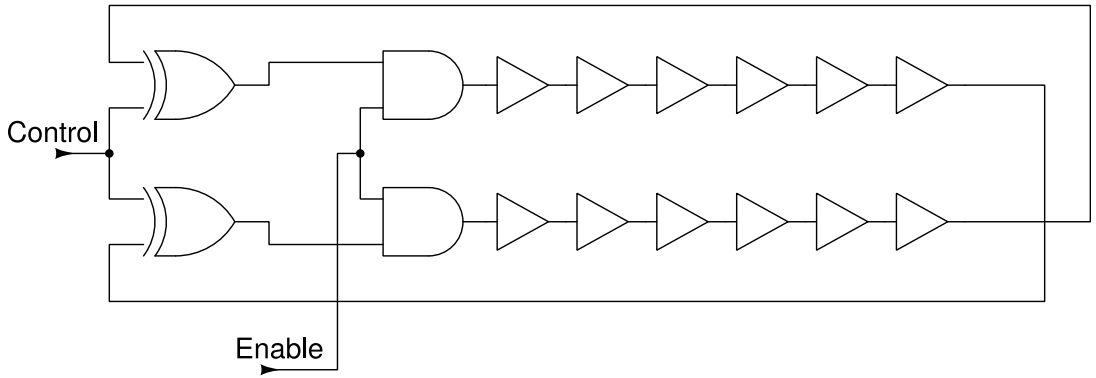


Our Contribution





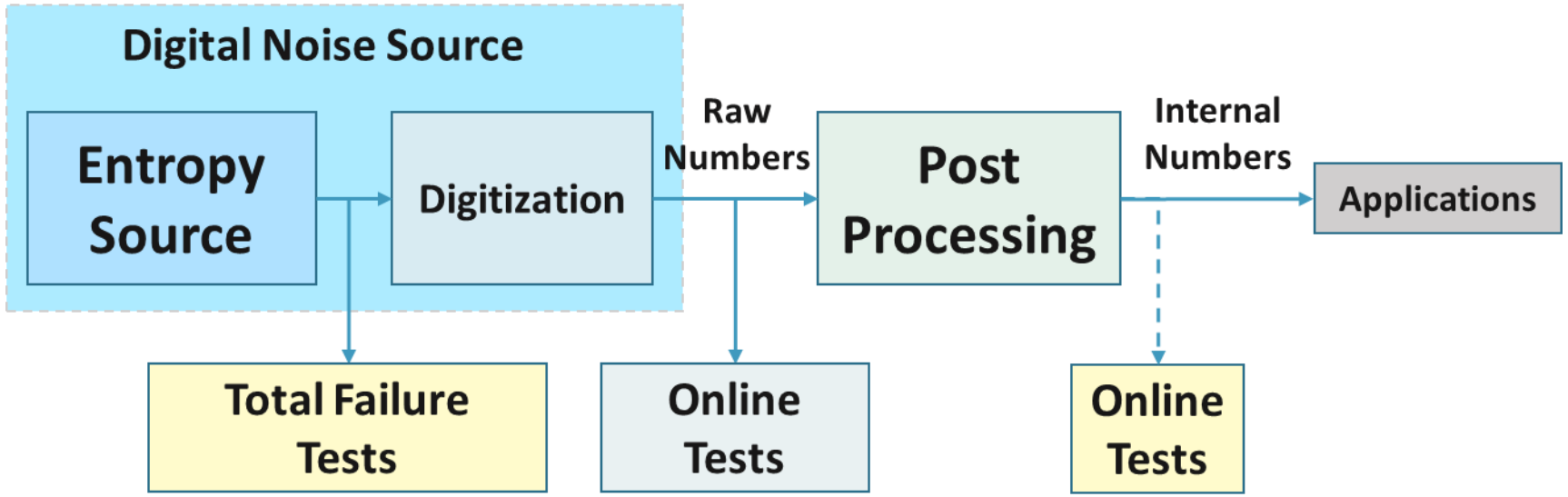




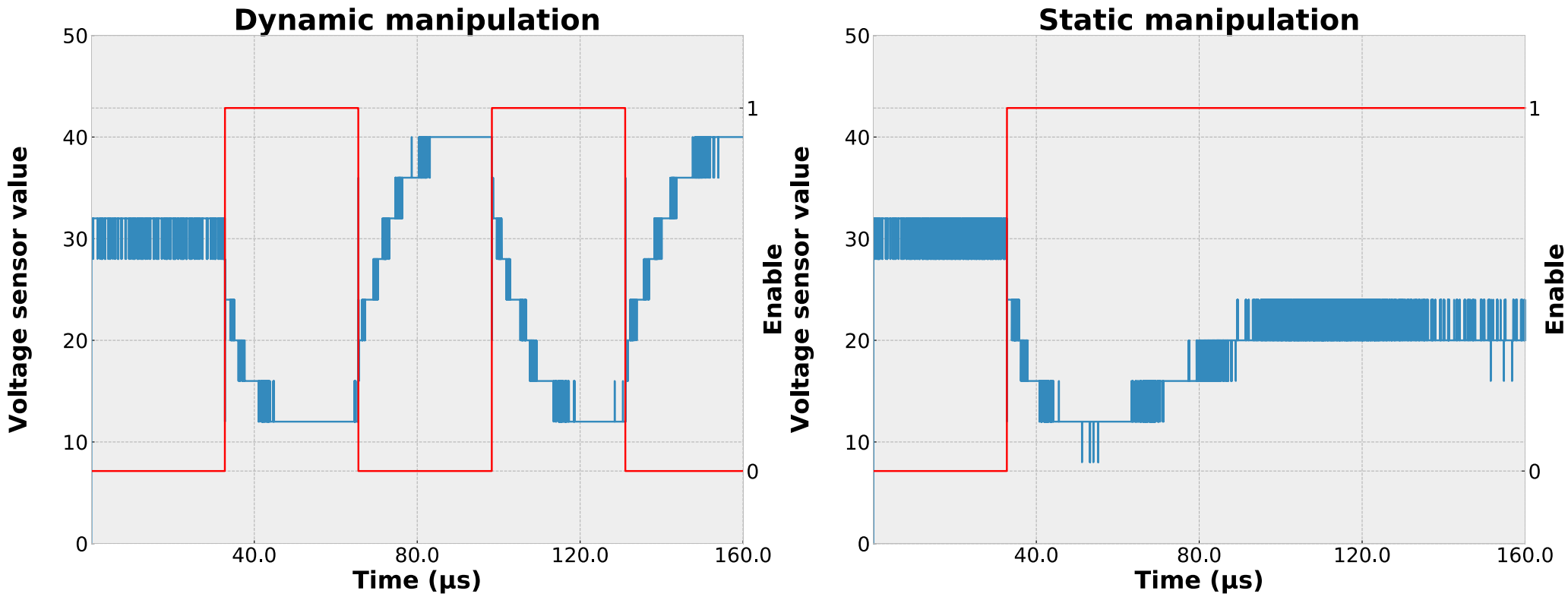
TRNG generic architecture

BSI AIS-31

NIST 800-90B

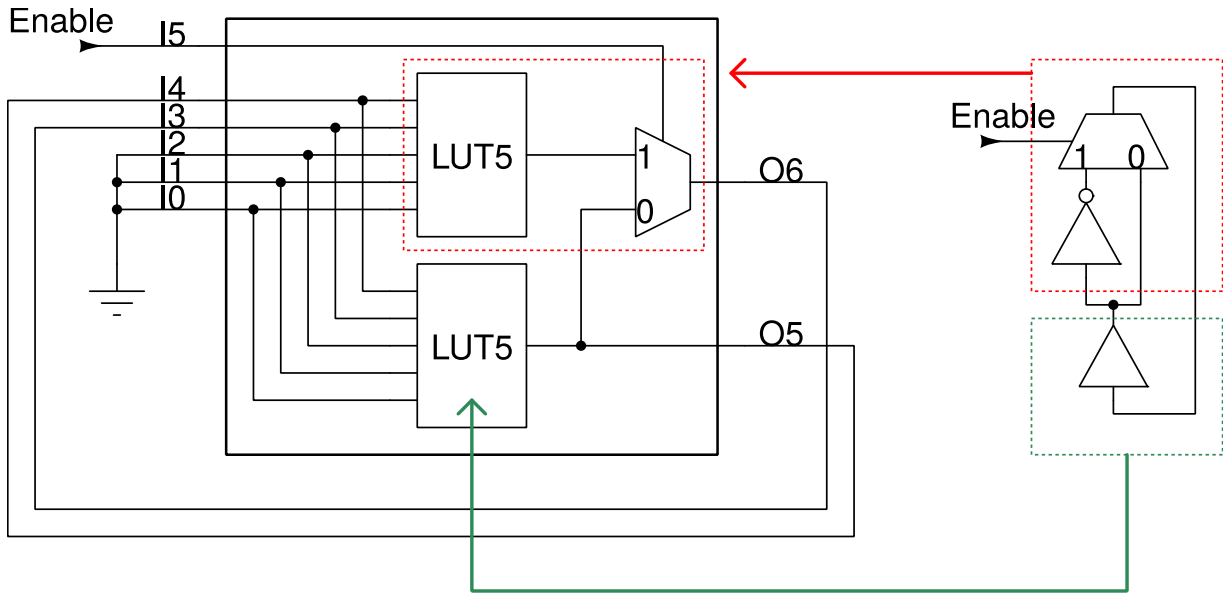


Attack scenario 1: Supply voltage manipulation



Attack scenario 1: Supply voltage manipulation

- Attack circuit: an array of 1-LUT ring oscillators
- Ring oscillators are enabled periodically

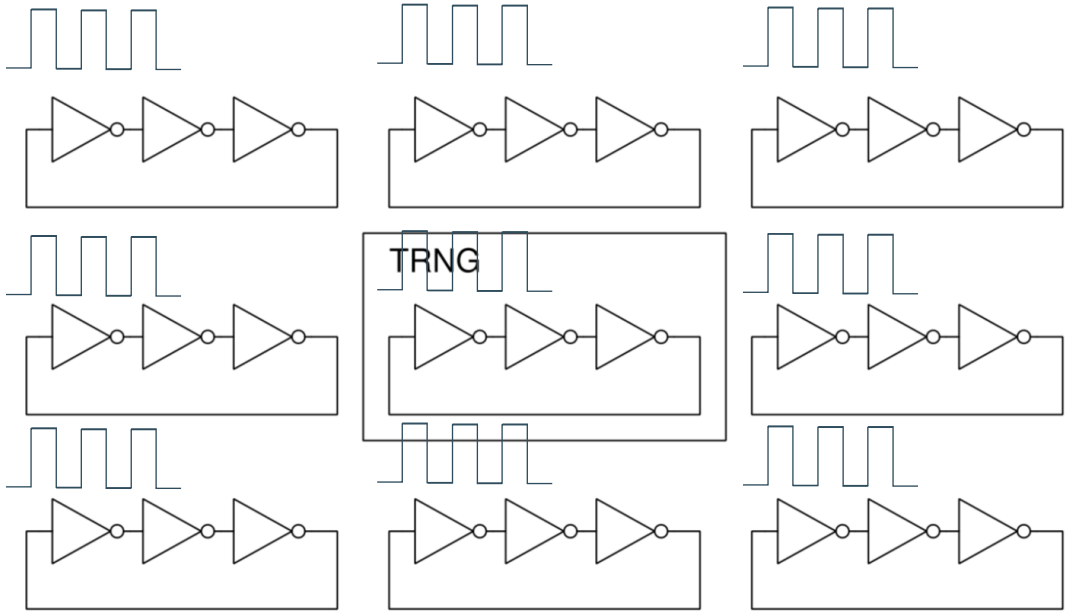


Attack scenario 2: Locking

- Entropy source contains ring oscillators
- Inject oscillating signal into entropy source
  - Oscillations with a fixed phase relative to the injected signal
  - Reduced entropy rate
- Two approaches:
  - Identical ring oscillators
  - Frequency matching

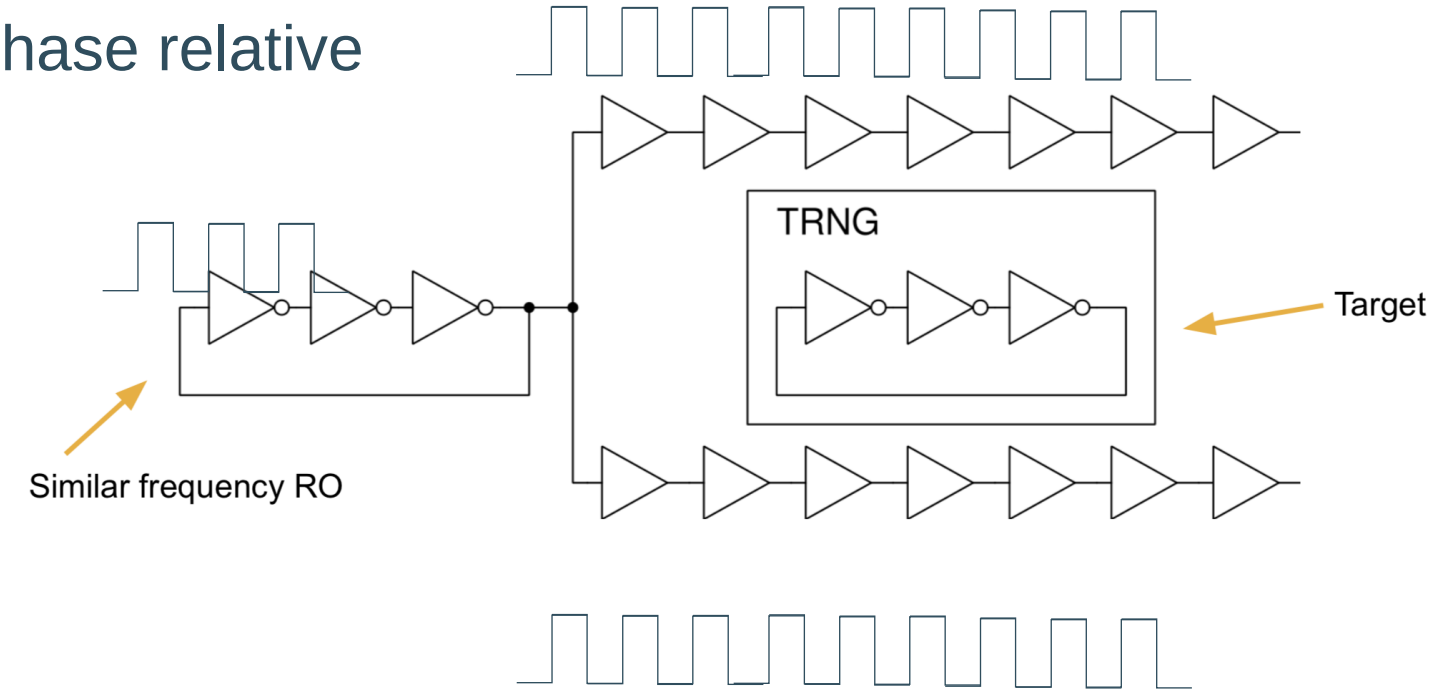
Attack scenario 2: Locking

- Entropy source contains ring oscillators
- Inject oscillating signal into entropy source
  - Oscillations with a fixed phase relative to the injected signal
  - Reduced entropy rate
- Two approaches:
  - Identical ring oscillators
  - Frequency matching



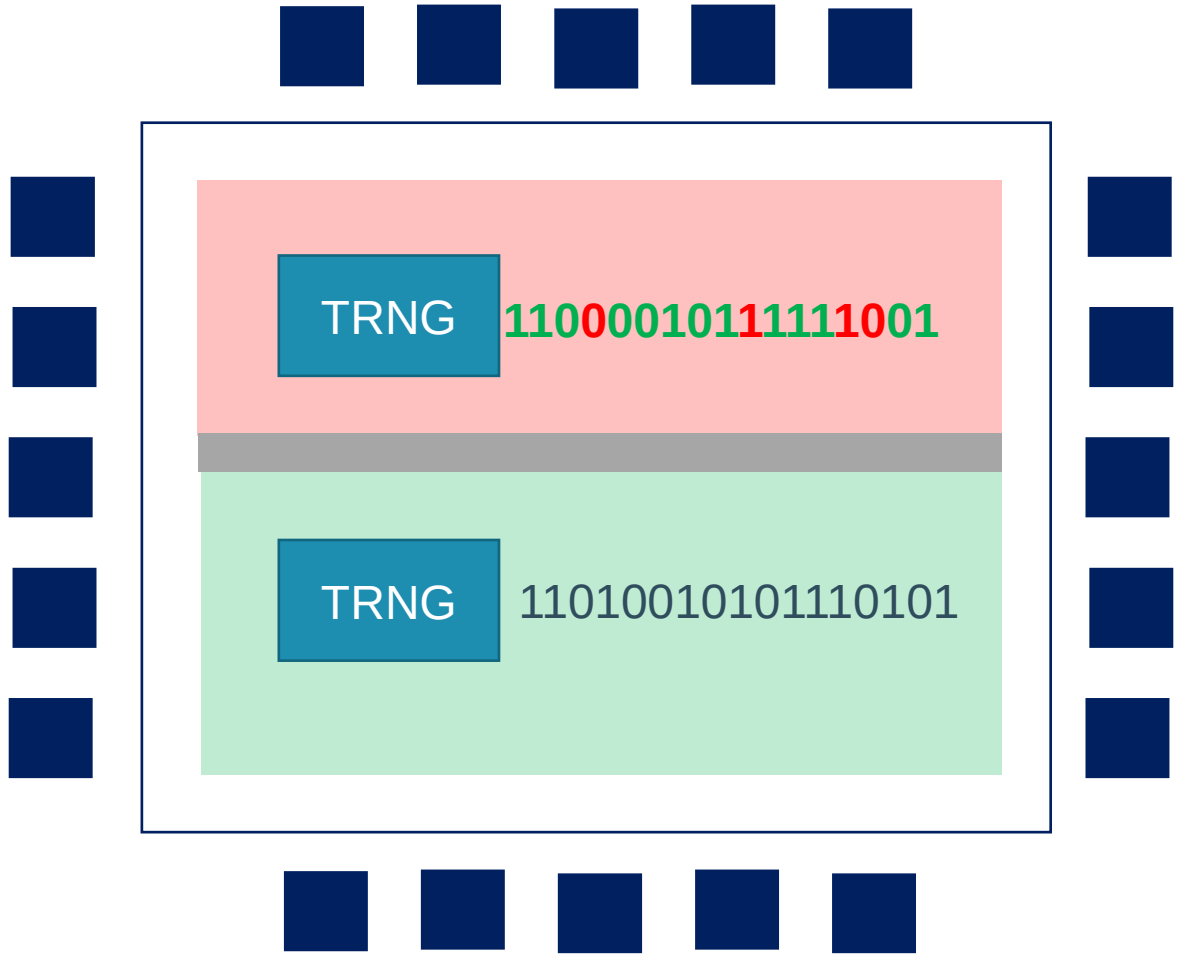
Attack scenario 2: Locking

- Entropy source contains ring oscillators
- Inject oscillating signal into entropy source
  - Oscillations with a fixed phase relative to the injected signal
  - Reduced entropy rate
- Two approaches:
  - Identical ring oscillators
  - Frequency matching

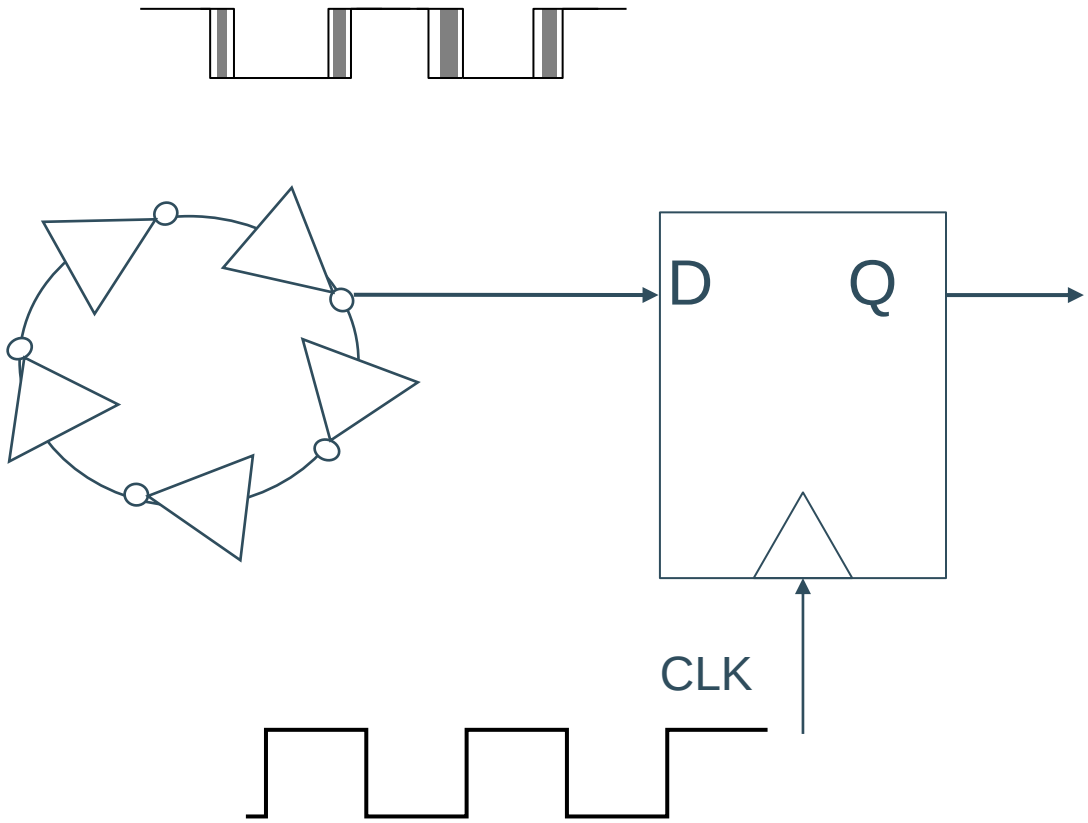


Attack scenario 3: Replica observation

- Identical design close to the target
- Observe the output for differences
- Additionally inject a similar oscillating signal into both entropy sources to increase the coupling



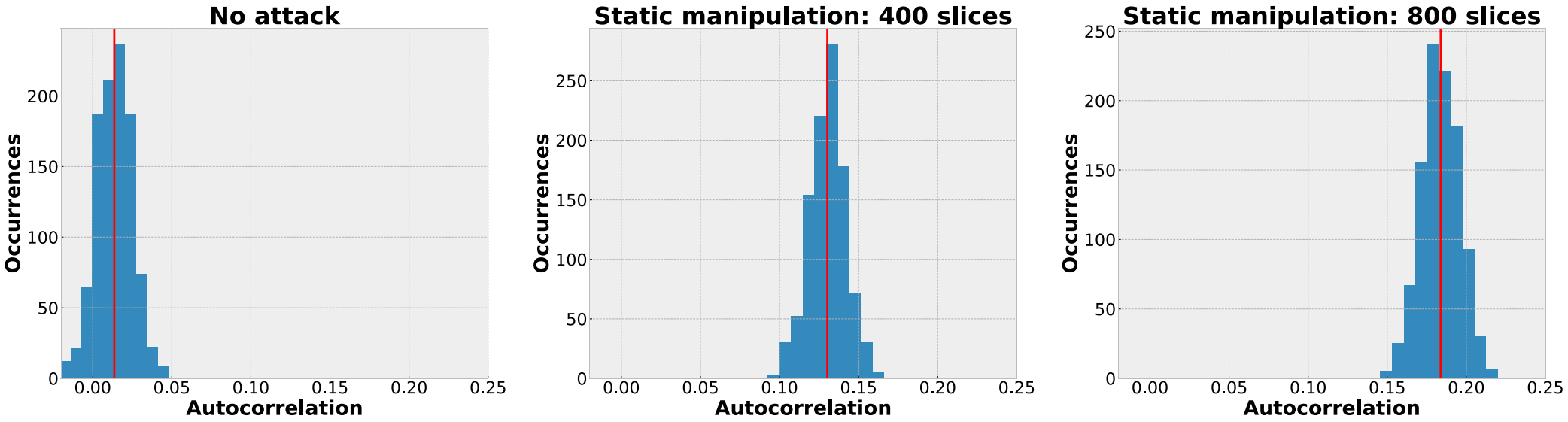
Case study 1: Elementary Ring Oscillator (ERO)



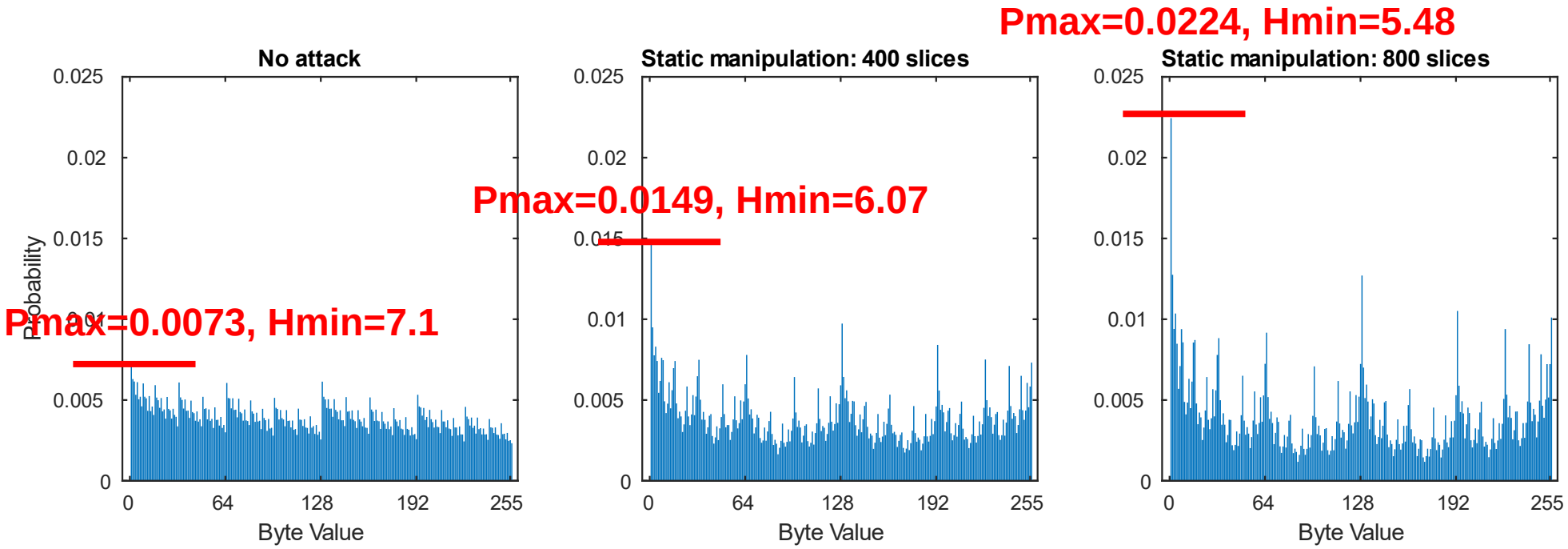
Case study 1: Power manipulation

- Supply voltage manipulation
  - Dynamic: no observed effect on generated bits
  - Static: increased autocorrelation

$$\sum_{i=1}^{n-1} \frac{(-1)^{b_i+b_{i+1}}}{n-1}$$

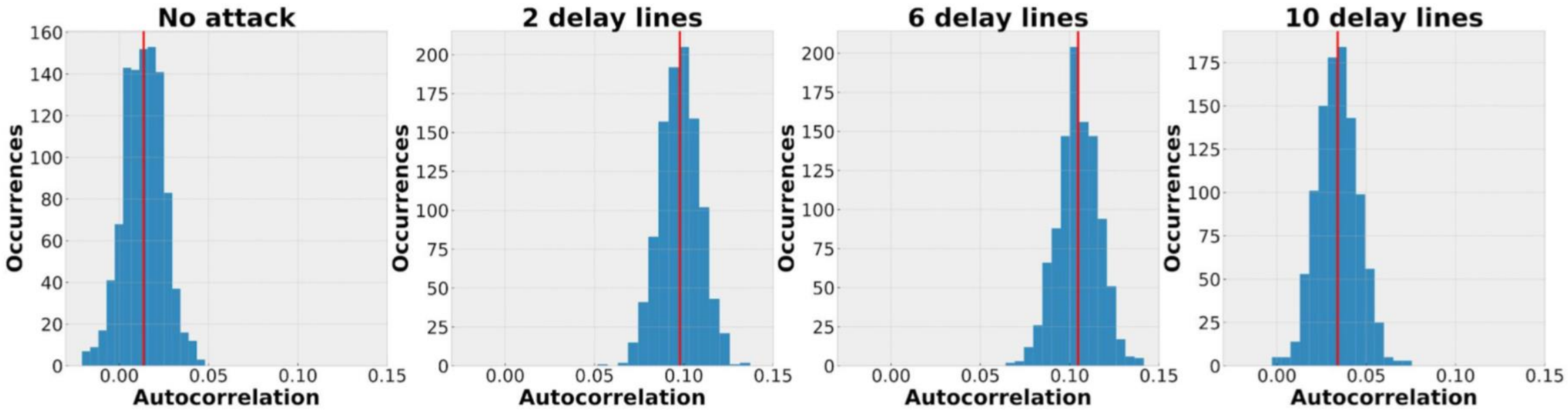


Case study 1: Power manipulation

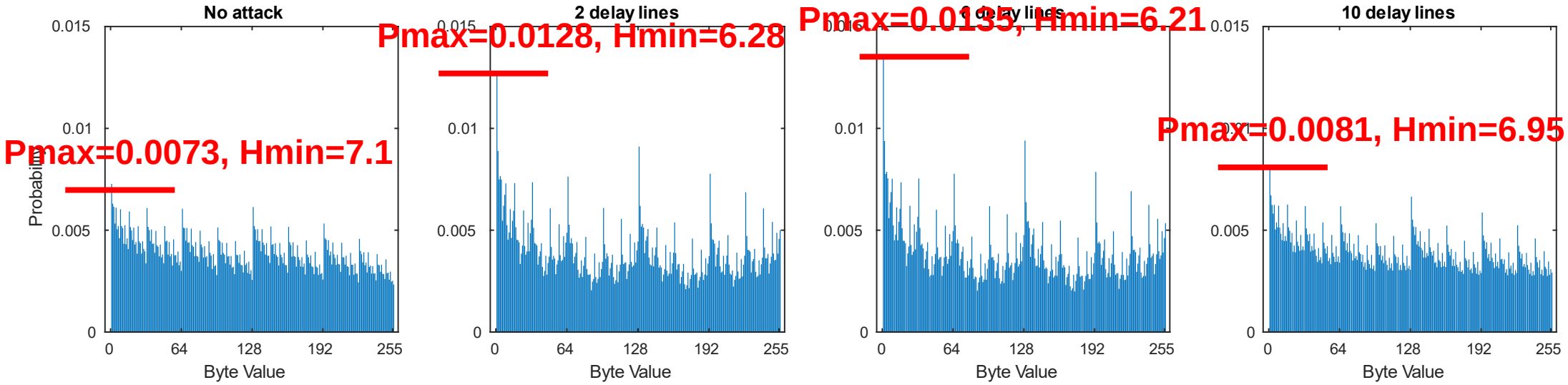


Case study 1: Locking

- Identical ring oscillators: no observed effect
- Frequency matching: increased autocorrelation

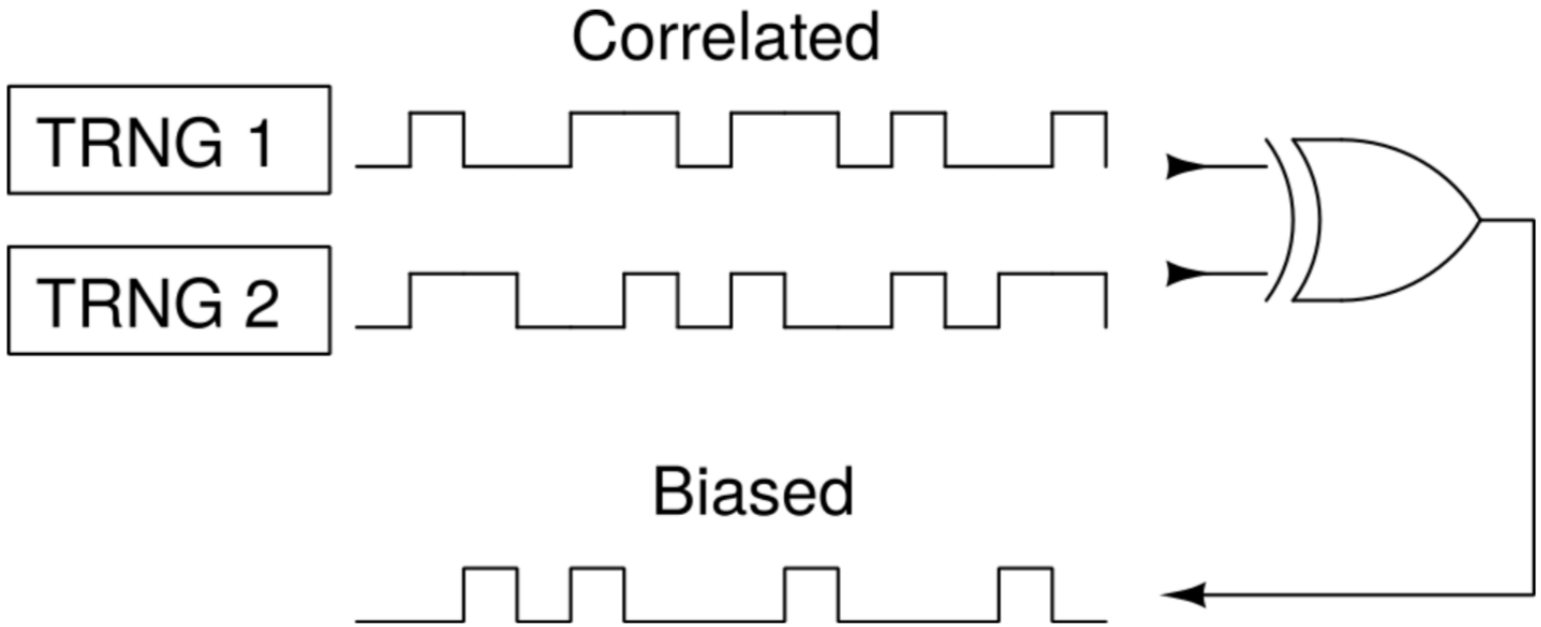


Case study 1: Locking



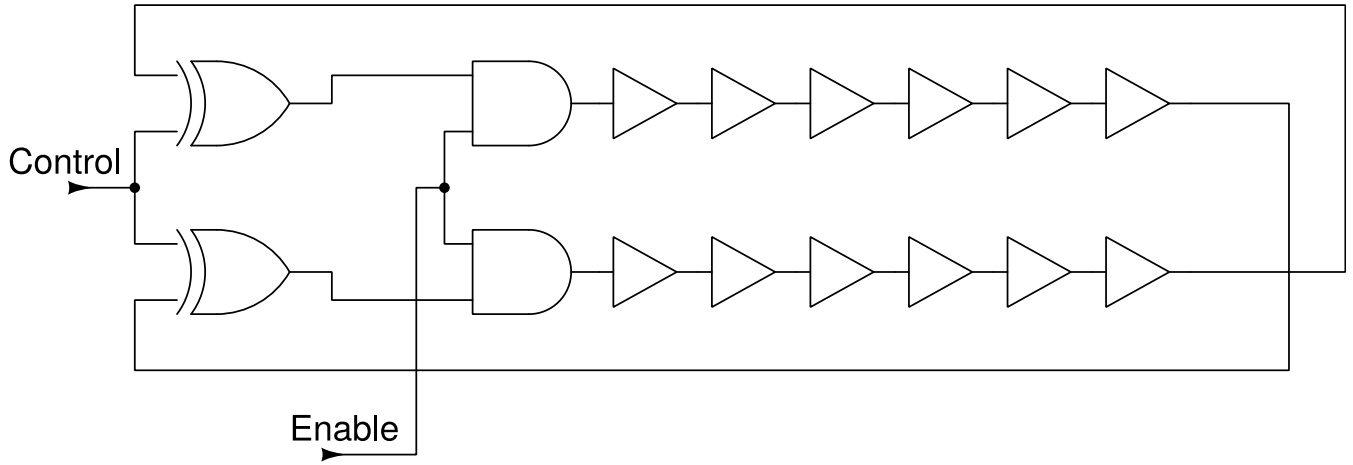
Case study 1: Replica Observation

- Attack scenario 3: Replica observation
  - No correlation observed

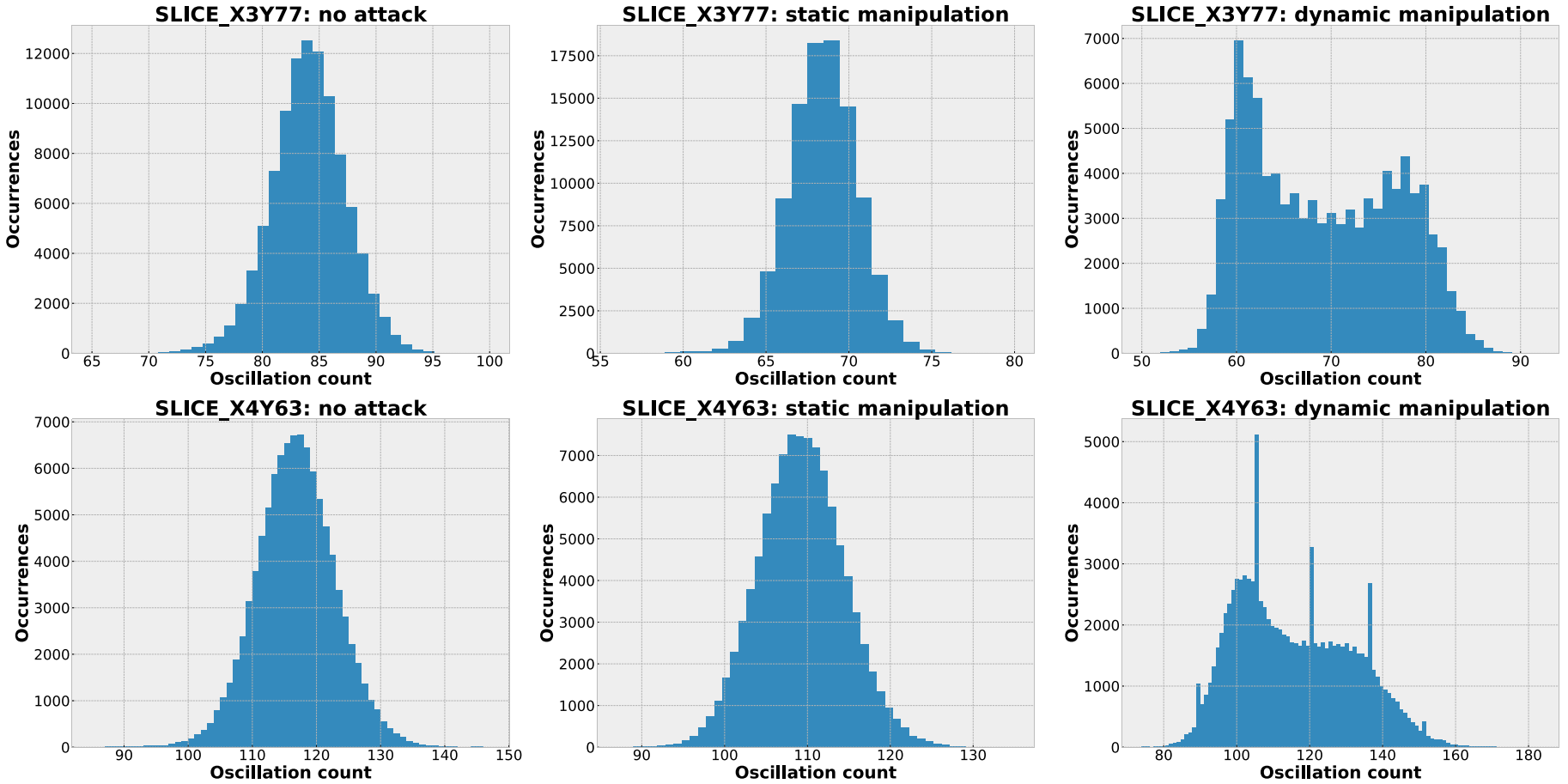


Case study 2: Transition Effect Ring Oscillator (TERO)

- Two edges injected in a non inverting delay loop
  - Edges start racing around the loop
- Output oscillates until edges collide
  - Number of oscillations is random due to jitter



Case study 2: Power manipulation



Case study 2: Borderline implementation

- Attack scenario 1: Supply voltage manipulation
  - TERO characteristics are highly dependent on FPGA placement
  - Supply voltage manipulation affects a poorly chosen TERO location

Test name	Pass rate standard	Pass rate attack
Frequency	97/100	97/100
Block frequency	98/100	3/100
Cumulative sums	97/100	95/100
Runs	93/100	1/100
Longest run	100/100	58/100
Rank	98/100	100/100
FFT	99/100	97/100
Serial	99/100	0/100

Conclusion

Architecture	Scenario 1	Scenario 2	Scenario 3
ERO	✓	✓	✗
TERO	✓	-	-

- Remote entropy source manipulation in a multi-tenant scenario is possible
  - Key entropy is reduced
- Careless entropy source design can make it more vulnerable to these attacks
- ERO TRNG is more vulnerable than TERO
- Complying to the TRNG design and evaluation standards is a sufficient countermeasure

Questions?