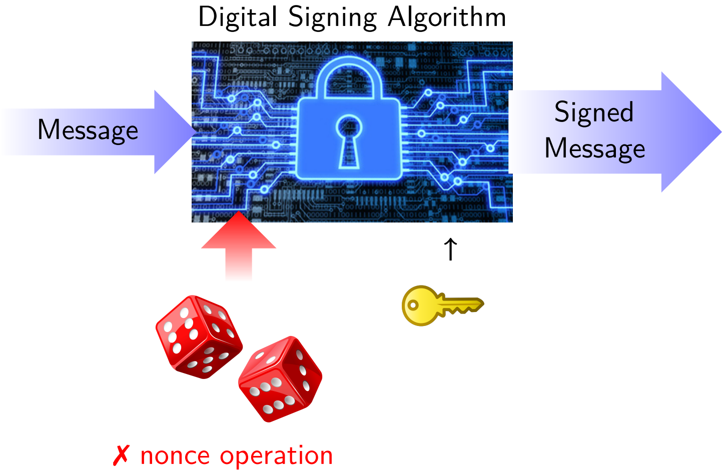
The impact of pulsed Electromagnetic Fault Injection on true random number generators

Maxime Madau, Michel Agoyan, Josep Balasch, Miloš Grujić, Patrick Haddad, Philippe Maurine, Vladimir Rožić, Dave Singelée, Bohan Yang, Ingrid Verbauwhede

Laboratoire d'Informatique de Robotique et de Microélectronique de Montpellier (LIRMM), Katolieke Universiteit Leuven, STMicroelectronics

FDTC 2018

Context


Digital Signing Algorithm

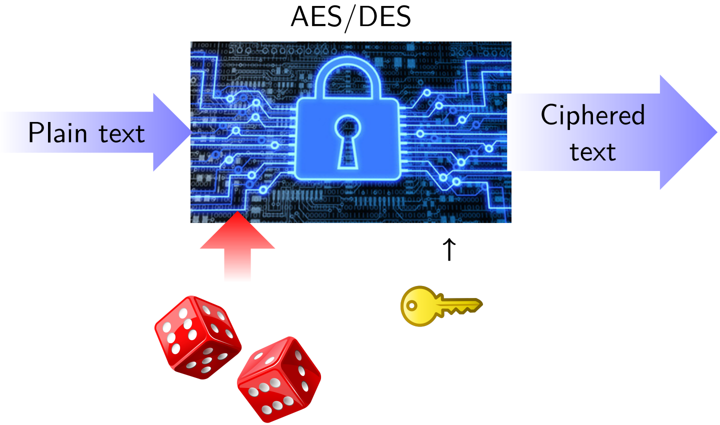
Message

Signed Message

↑

✗ nonce operation

Context



AES/DES

Plain text

Ciphered text

↑

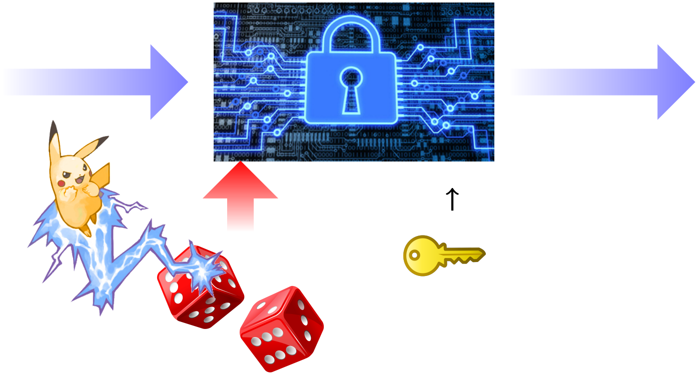
✗ Side Channel Countermeasure
(Example: masking)

What if... ?

Pulse Electromagnetic Fault Injection could:

- Craft pseudo random sequence.
- Stick random bit
  → DSA/ECDSA: [NNTW04], [NS03] and [NS02].

DSA/ECDSA

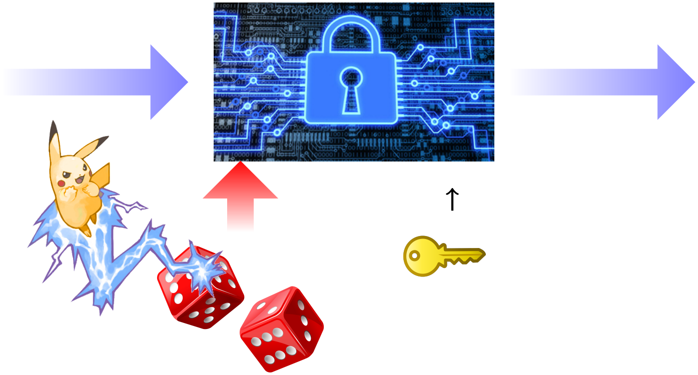


What if... ?

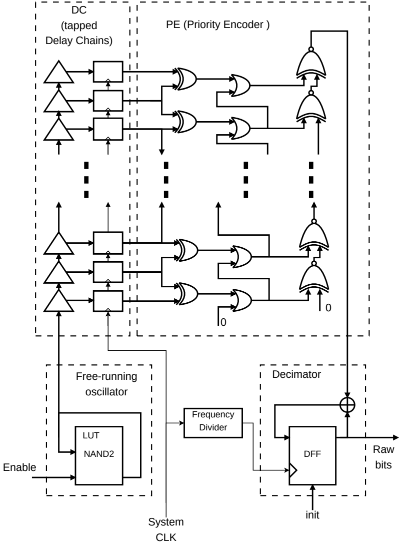
Pulse Electromagnetic Fault Injection could:

- Craft pseudo random sequence.
- Increasing the bias of the random output.

AES/DES



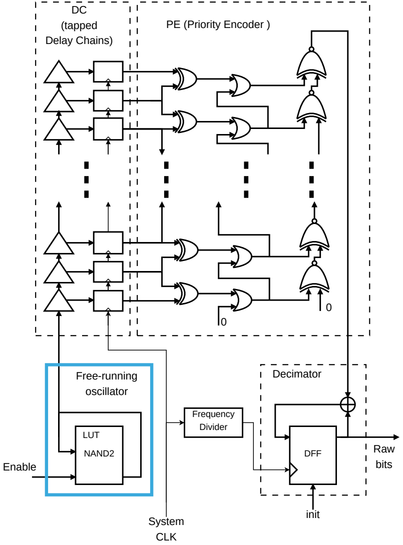
DC-TRNG's architecture [RYDV15]



Why this TRNG:

1. High speed for its space requirement (bitrate $4.5\mathit{MHz}$).
2. Common architecture, Ring Oscillators based.

DC-TRNG's Architecture [RYDV15]



Why this TRNG:

1. High speed for its space requirement (bitrate $4.5MHz$).
2. Common architecture, Ring Oscillators based.

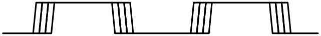
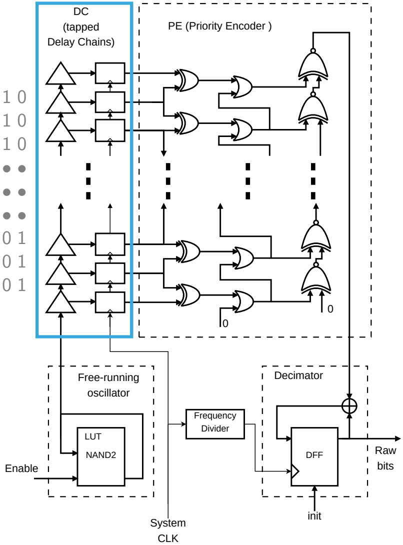


Figure: Ring Oscillator output (jitter on edges)

DC-TRNG's Architecture [RYDV15]



Why this TRNG:

1. High speed for its space requirement (bitrate $4.5 MHz$).
2. Common architecture, Ring Oscillators based.

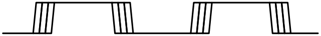
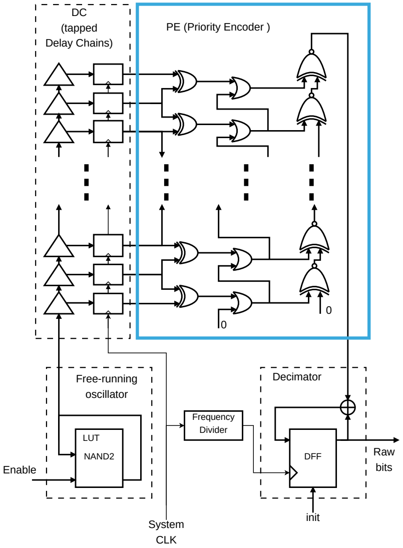


Figure: Ring Oscillator output (jitter on edges)

DC-TRNG's Architecture [RYDV15]



Why this TRNG:

1. High speed for its space requirement (bitrate $4.5\mathit{MHz}$).
2. Common architecture, Ring Oscillators based.

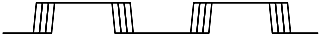
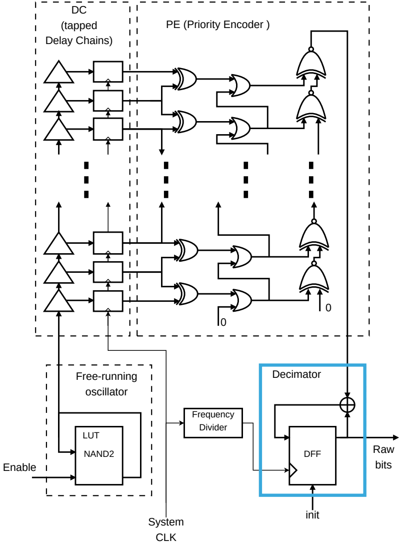


Figure: Ring Oscillator output (jitter on edges)

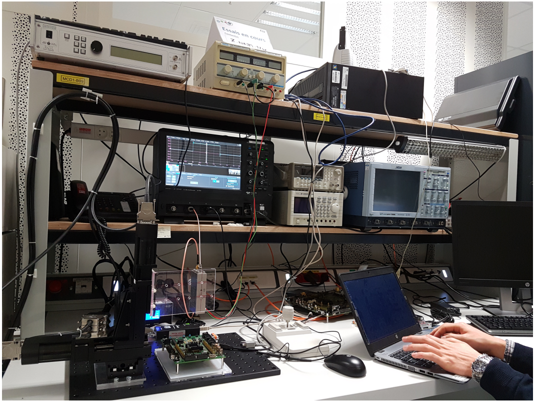
DC-TRNG's Architecture [RYDV15]



Why this TRNG:

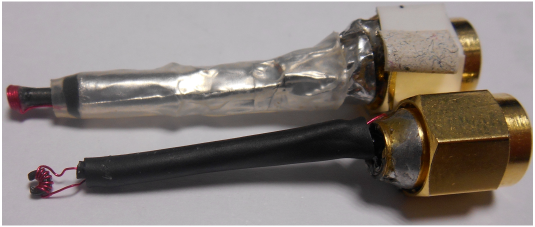
1. High speed for its space requirement (bitrate $4.5\mathit{MHz}$).
2. Common architecture, Ring Oscillators based.

Injection bench



	Amplitude	Pulse width	Pulse Repetition
Pulse	$\pm\ 0 - 400V$	$8 - 100ns$	$2kHz$
In practice	$290 - 350V$	$6 - 11ns$	

Injection bench (Probes)



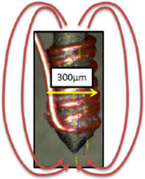


Figure: Plated probe's magnetic field line

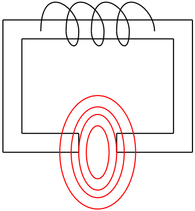
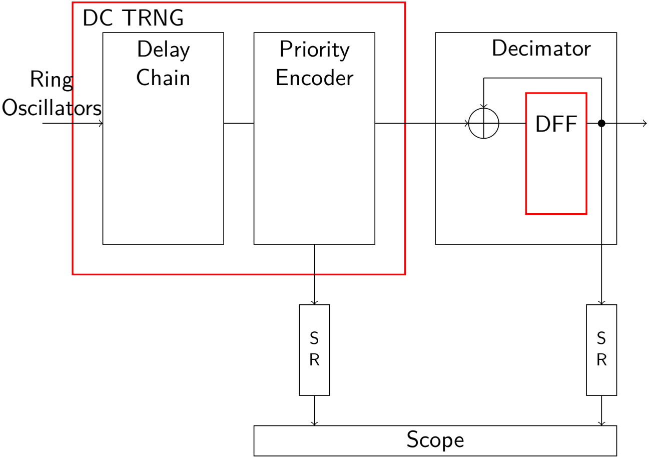


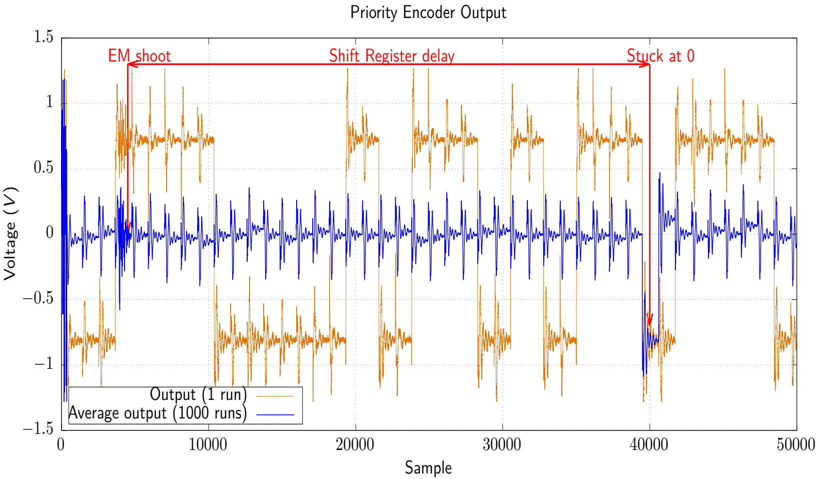
Figure: U-shaped probe's magnetic field line

Experiment 1

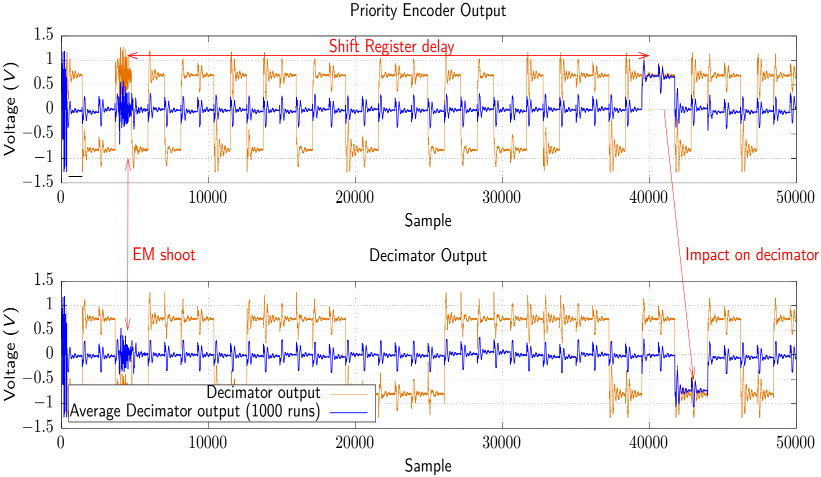


SR=Shift Register

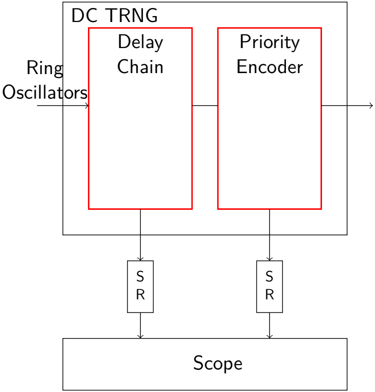
Stuck at 0


Priority Encoder Output
EM shoot
Shift Register delay
Stuck at 0
1.5
1
0.5
0
−0.5
−1
−1.5
Voltage (V)
0
10000
20000
30000
40000
50000
Sample
Output (1 run)
Average output (1000 runs)

Stuck at 11


Priority Encoder Output
Shift Register delay
Voltage (V)
1.5
1
0.5
0
−0.5
−1
−1.5
0
10000
20000
30000
40000
50000
Sample
EM shoot
Decimator Output
Impact on decimator
Decimator output
Average Decimator output (1000 runs)

Experiment 2



Results:

1. Control of PE output (stuck at 0 or 1).
2. DC chain or Ring Oscillators faulted in an uncontrol way.
   Normal output:

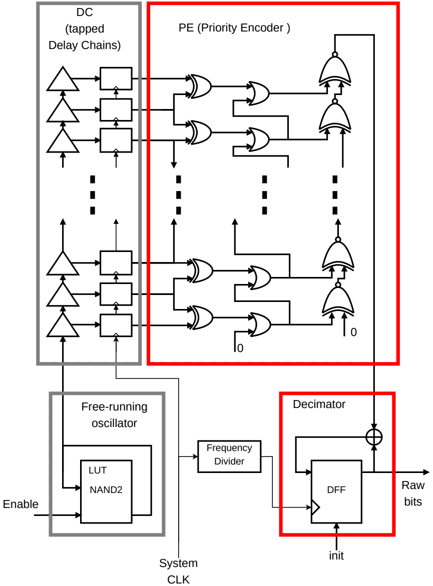
   $$...0000011111...$$

   Faulted Output:

   $$...01...10..11...0..10110...1111$$

SR=Shift Register

DC-TRNG Fault Injection entry point



Possible threat scenario (ECDSA/DSA)

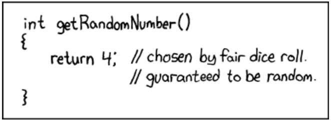
✗ Inject a known pseudo random sequence

→ EM bench too slow.

✓ Defeating DSA and ECDSA.

→ “stuck at” faults on up to 2 bits.

→ but private key’s length: 512 to 1024 bits and public key’s length 160 bits



```
int getRandomNumber()
{
    return 4;  // chosen by fair dice roll.
               // guaranteed to be random.
}
```

Figure: www.xkcd.com

Possible threat scenario (AES/DES)

✗ Inject a known pseudo random sequence

→ EM bench too slow.

? Injected bias sufficient to lower masking robustness.

Simulated bias injected by our Injection bench

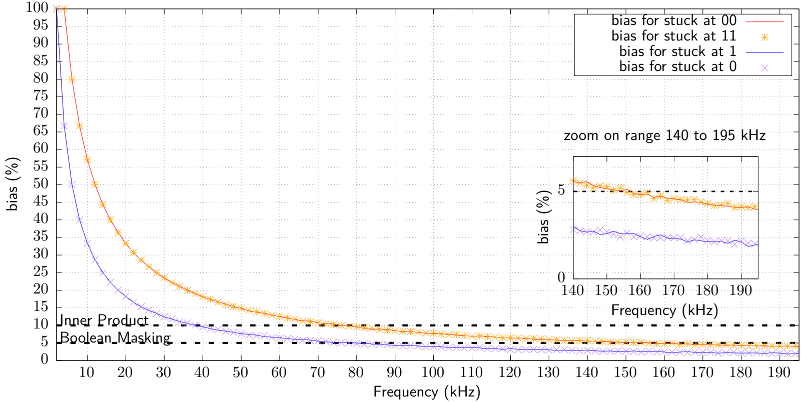
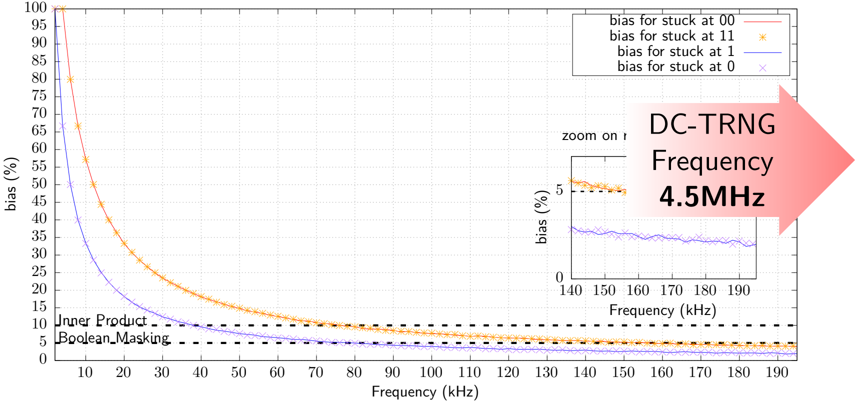


Figure: Bias on the TRNG random output against functionning frequency.

Simulated bias injected by our Injection bench



DC-TRNG Frequency **4.5MHz**

Figure: Bias on the TRNG random output against functionning frequency.

Conclusion

- Entropy source is not the only target for fault injection.
- The use High speed TRNG is an asset to protect against fault injection.
- Pulsed EMFI effect on Ring Oscillators based TRNG seems to be uncontrollable but digitizing part can be problematic.

Thanks,
Any Questions ?

Acknowledgments

This work is partly supported by Horizon 2020 research and innovation programme under grant agreement No 644052 HECTOR and Cathedral ERC Advanced Grant 695305.

Bibliography I

- David Naccache, Phong Q. Nguyen, Michael Tunstall, and Claire Whelan, *Experimenting with faults, lattices and the DSA*, IACR Cryptology ePrint Archive **2004** (2004), 277.

- Phong Q. Nguyen and Igor E. Shparlinski, *The insecurity of the digital signature algorithm with partially known nonces*, J. Cryptology **15** (2002), no. 3, 151–176.

- ______, *The insecurity of the elliptic curve digital signature algorithm with partially known nonces*, Des. Codes Cryptography **30** (2003), no. 2, 201–217.

- Vladimir Rozic, Bohan Yang, Wim Dehaene, and Ingrid Verbauwhede, *Highly efficient entropy extraction for true random number generators on fpgas*, Design Automation Conference DAC'15 (2015).