The Fault Analysis & DFA on AES

Jérémy DRON

Summary

1. Injecting a fault…
2. … into the clock…
3. … allows the AES implementation to be broken…
4. …using the Piret attack.[1]

Injecting a fault...

What is a fault ? (Reminder)

Deliberate introduction of errors into the system to gain information about the secret

- 2 types of fault:
  - Permanent
  - transient
- Several methods
  - electromagnetic
  - illumination
  - temperature
  - glitch

How to inject an error into the clock with CW-lite ?

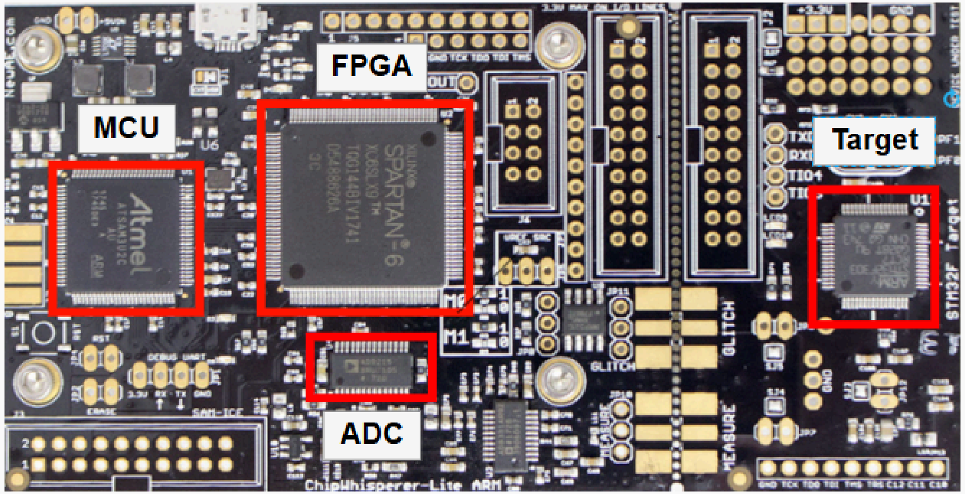


Figure 1: CW-lite board

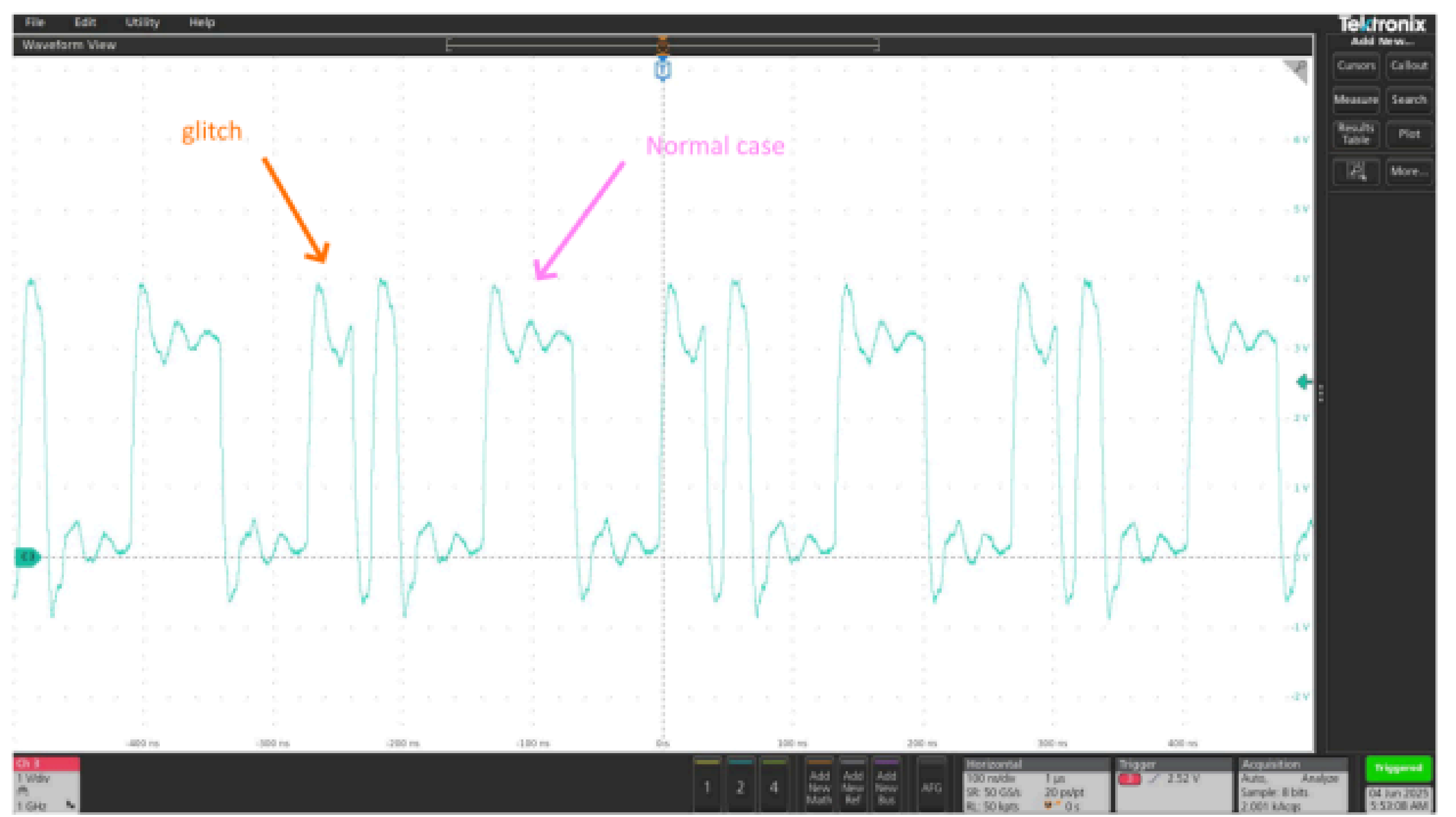
- MCU - controls the board
- FPGA - creates the fault signal
- ADC - captures traces
- Target - target of our attacks

… into the clock…

Glitch on the clock

- The hardware is clocked by a clock
- The glitch creates a rising edge
- Execution of the erroneous instruction

Observation of a fault on a scope



Ch 3
1 V/div
1 GHz

Horizontal
100 ns/div 1 µs
SR: 50 GS/s 20 ps/pt
RL: 50 kpts 0 s

Trigger
3 2.52 V

Acquisition
Auto, Analyze
Sample: 8 bits
2.001 kAcqs

04 Jun 2025
5:53:08 AM

Figure 2: Screenshot of a scope

… allows the AES implementation to be broken…

AES 128-bits - 10 rounds (Reminder)

- Each round uses a round key (derived from the key scheduler)
- The key schedule can be reversed

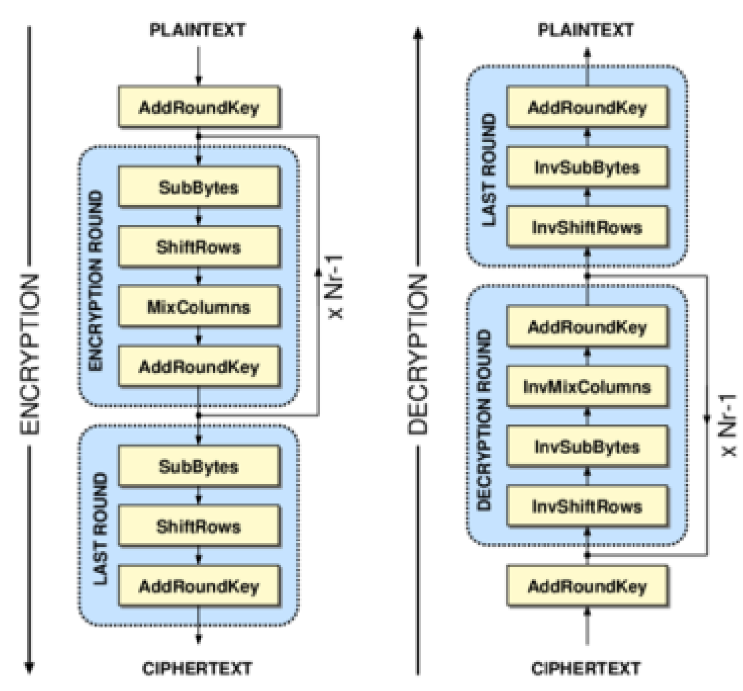


Figure 3: AES schema

How to break AES with fault analysis ?

- $C_i = k_i^{10} \oplus C_i^{10_{\text{before\_last\_ARK}}}$
- $k_i^{10} = C_i \oplus C_i^{10_{\text{before\_last\_ARK}}}$
- $k_i^{10} = C_i \oplus 0$

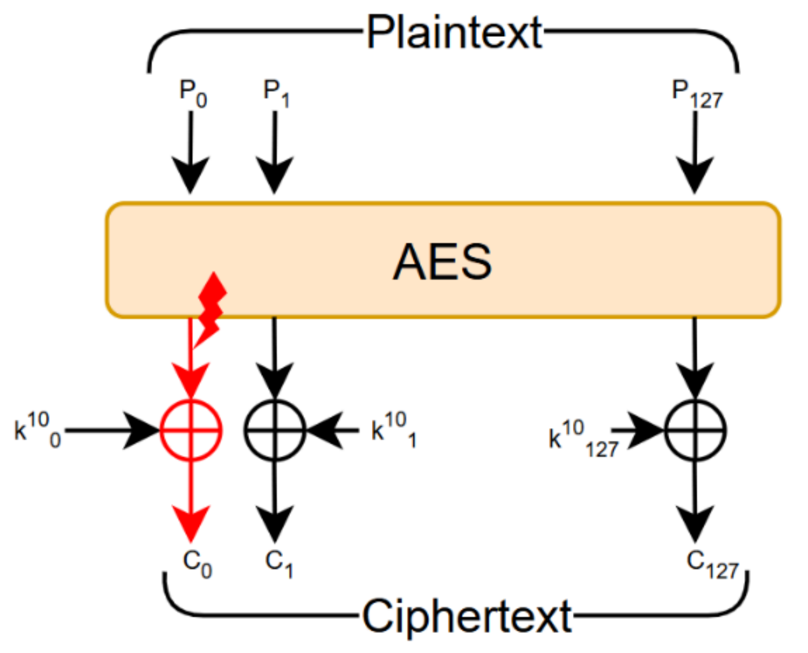


Figure 4: Basic attack on the last round of AES

Is the attack realistic ?

- Require precision equipment
- Impossible with basic CW equipment
- What attacks can we perform with our equipment?

…using the Piret attack.[1]

Piret's attack is based on DFA (Reminder)

- Principle of DFA
  - Execution of a cryptographic algorithm (C)
  - Faulty execution of a cryptographic algorithm ($C^\star$)
- Exploitation of the difference between C and $C^\star$ to find the secret

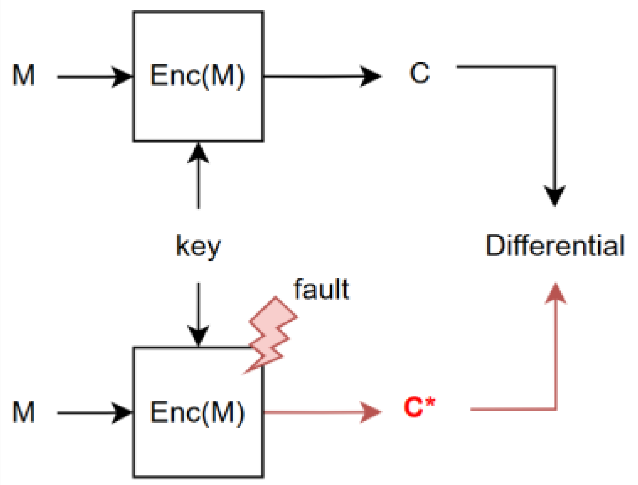


Figure 5: DFA schema

How does Piret's attack work?

1. Calculate D-set: set of all possible differences
   - Compute all possible differences (4-byte $*$ 255 errors = 1020)
   - Compute each possible into the MixColumn
2. Creation of a (C,$C^\star$)
3. We go back up the AES to the SB of the last round, testing key hypotheses.
   - $\Delta_i = \mathrm{SB}^{-1}(C_i \oplus k_i^r) \oplus \mathrm{SB}^{-1}(C_i^\star \oplus k_i^r)$ with $r = 10$
4. If Δ_i exists in D-set, then put k_i^r in L-set (Liar set)
5. Start again with a new (C,$C^\star$) (goto step 2)
6. $W = \{L_{\text{pair}_1} \cap L_{\text{pair}_2}\}$
   - If $|W| = 1$ then you win
   - Else start again with a new (C,$C^\star$) (goto step 2)
7. Reverse the Key Schedule operation with K^{10} to find the master key.

Faults propagations r-1 & r

- Piret's attack works columns by columns
- The propagation of faults is known
- 2 faults per columns to attack
- 4 cols $*$ 2^{1} faults $=$ 8 faults

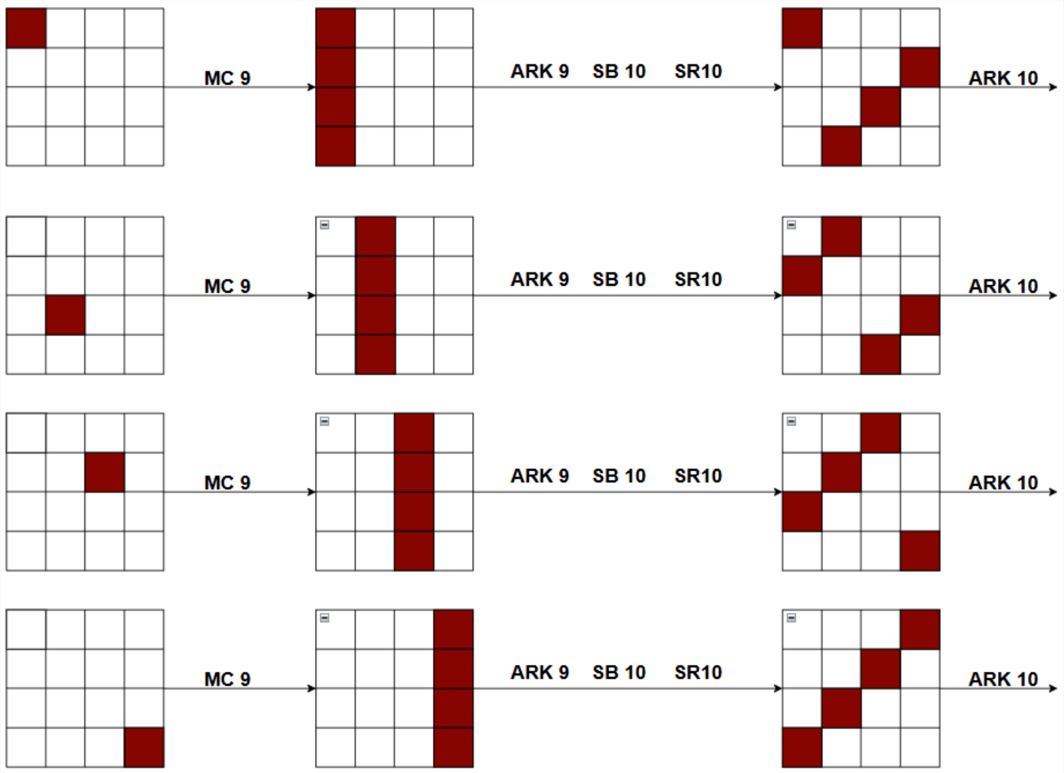


Figure 6: Faults propagation

[1] In 92% of cases

Fault propagation & Piret's attack round 9

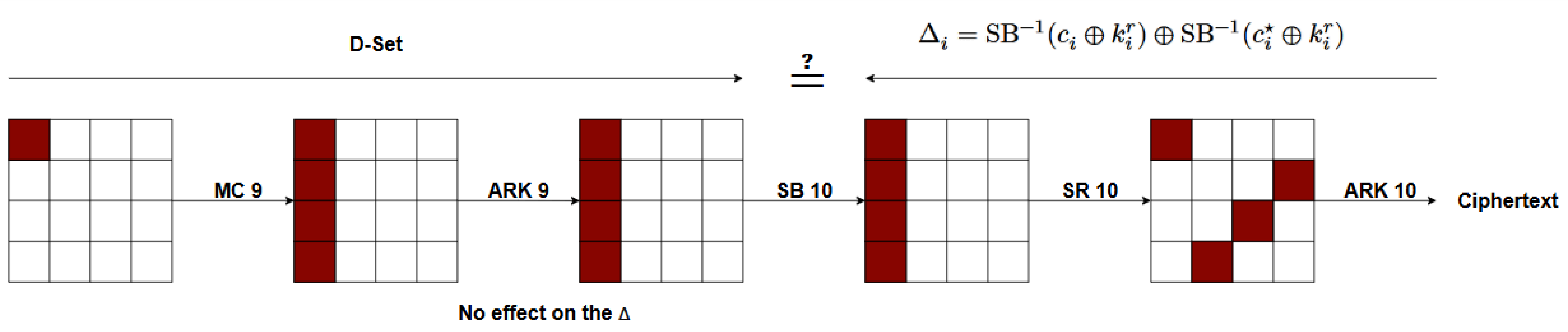

D-Set
$\Delta_i = \mathrm{SB}^{-1}(c_i \oplus k_i^r) \oplus \mathrm{SB}^{-1}(c_i^\star \oplus k_i^r)$
$\overset{?}{=}$
MC 9
ARK 9
SB 10
SR 10
ARK 10
Ciphertext
No effect on the Δ

Figure 7: Schematization of the attack

Suggested sequence of attack

1. Identify rounds 9 & 10 of AES-128
2. Set the Glitch controller to tap on each column
3. Create pairs $(C, C^\star)$ and identify the faulty column
4. Use the crack_bytes function from phoenixAES to find k^{10}.
5. Reverse the Key schedule[2] to find the master key.

[2] It's possible to use key_schedule_rounds function included in the CW library

Bibliography

[1] G. Piret and J.-J. Quisquater, “A Differential Fault Attack Technique against SPN Structures, with Application to the AES and KHAZAD,” in *Cryptographic Hardware and Embedded Systems - CHES 2003, 5th International Workshop, Cologne, Germany, September 8-10, 2003, Proceedings*, in Lecture Notes in Computer Science, vol. 2779. Springer, 2003, pp. 77–88. doi: 10.1007/978-3-540-45238-6_7.

[2] J. Francq, J.-B. Rigaud, P. Manet, J.-C. Bajard, and A. Tisserand, “Amélioration de la sécurité des circuits intégrés par codage de l'information.”