LEDGER

DeepCover DS28C36: A Hardware Vulnerability Identification and Exploitation Using T-Test and Double Laser Fault Injection

Karim M. Abdellatif and Olivier Hériveaux

Motivation

- DeepCover is a **secure authenticator** circuit family developed by Analog Devices [1] (previously Maxim Integrated).
- DS28C36 has been recently used as a second secure element in Coldcard hardware wallet Mk4 [2].
  - This was done after attacking ATECC608B using LFI [3]
  - The secret is shared between the two secure elements and the MCU (STM32).
- Also, it has been widely used in secure boot and secure download for IoT.

Coldcard Mk4 (ref: Coinkite)

[1] https://www.analog.com/media/en/technical-documentation/tech-articles/deepcover-embedded-security.pdf

[2] https://coldcard.com/docs/coldcard-mk4

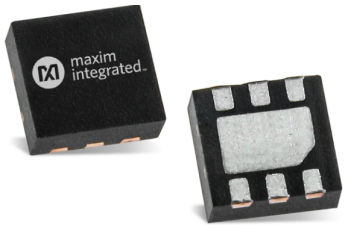
[3] Olivier Hériveaux, "Triple Exploit Chain with Laser Fault Injection on a Secure Element", FDTC 2022

Outline

FEATURES OF DS28C36

Security features [4]

- ECC-256 computation engine
- FIPS 180 SHA-256 computation engine
- TRNG with NIST SP 800-90B compliant entropy source with function to read out
- 17-Bit one-time settable, non-volatile decrement-only counter with authenticated read
- **8Kbit of EEPROM for user data, keys, and certificates**
- The full data sheet is not available and this required some reverse to find the available commands and their parameters.



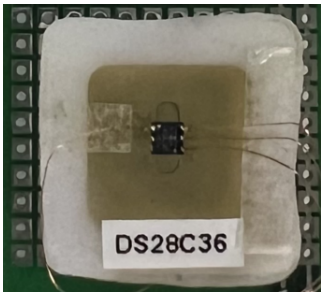
[4] https://www.analog.com/media/en/technical-documentation/data-sheets/DS28C36.pdf

Page	Description	Note
0 to 15	User pages	**Coldcard [5] uses pages 14 and 15**
16 to 21	Public keys (x and y)	N/A
22 to 24	Private keys	N/A
25 to 26	Secret pages	N/A
27	Counter	N/A
28 to 29	Random	N/A
30 to 31	RAM buffer	N/A

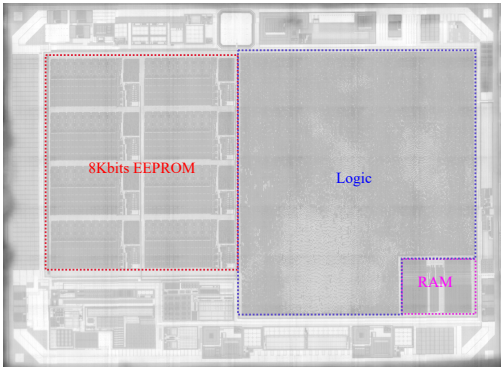
[5] https://github.com/Coldcard/firmware/blob/master/docs/mk4-secure-elements.md

ATTACK SETUP

Sample preparation



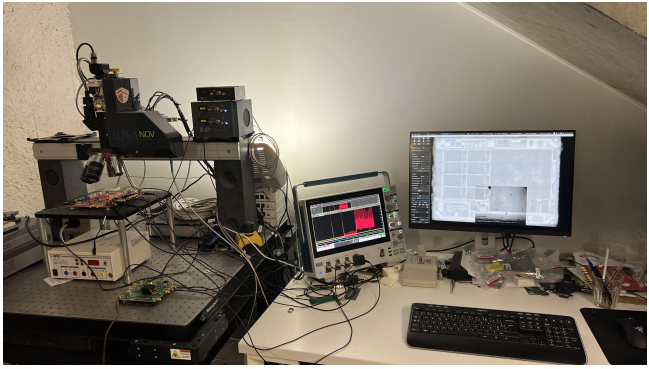
Decapped chip



Infrared backside image

Setup

- An infrared pulsed laser source and a microscope for focusing
- A Scaffold[6] board
- A Tektronix MSO44 oscilloscope
- DUT: DS28C36

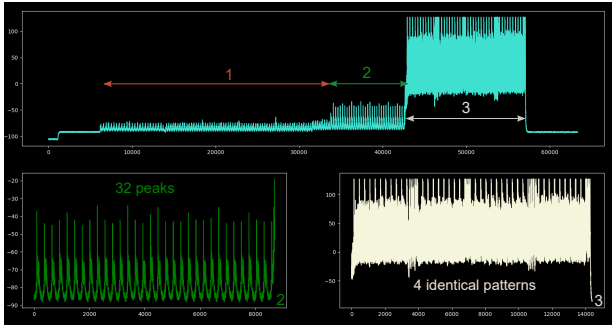


Setup

[6] O. Heriveaux. Scaffold. https://github.com/Ledger-Donjon/scaffold

Read page command

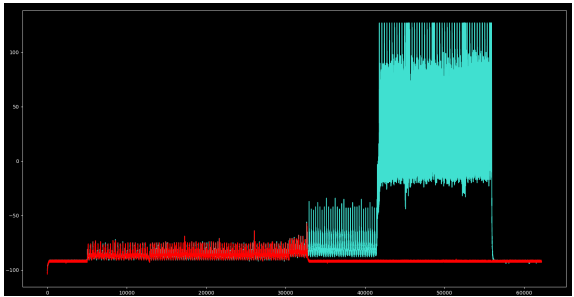
```
1 write_data(page_number, data)
2 read_page(page_number)
3 save_power_trace()
```



Power consumption in case of unprotected page

Unprotected and protected page

```
1 write_data(page_number, data)
2 read_page(page_number)
3 save_power_trace()
4 lock_page(page_number)
5 read_page(page_number)
6 save_power_trace()
```



Protected and unprotected

SINGLE FAULT PULSE

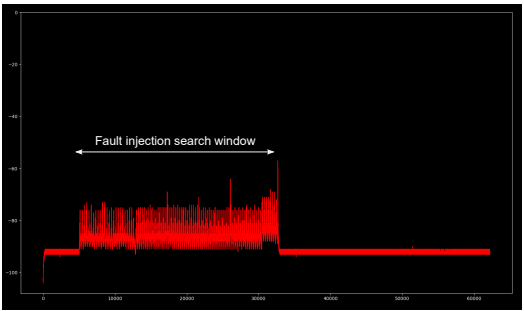
Attack scenario

Step 1:

```
write_data(page_number, data)
lock_page(page_number)
```

Step2:

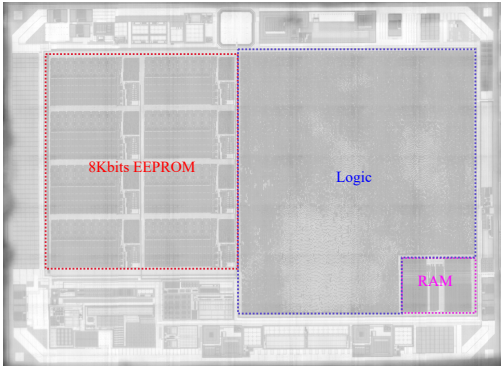
```
While True:
    prepare_fault() # single pulse
    chip_restart()
    read_page(page_number)
    save_log()
    move_laser()
```



Power consumption when the page is locked

Page configuration (bit or bits) can be:

- Stored in the EEPROM
- Stored in eFuses
- Manipulated in the logic
- Temporarily stored in RAM

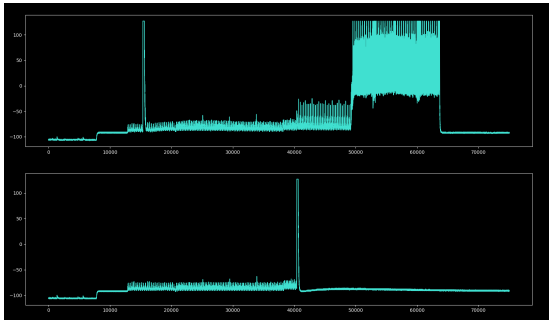


IR image

Results

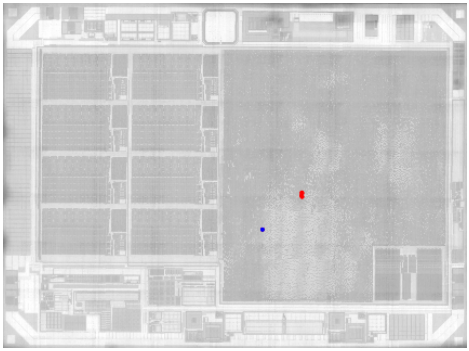
Number	Chip response	Note
0	2155ffffffffffffffffffffffffffffffff ffffffffffffffffffffffffffffffffffff	Locked
1	ffffffffffffffffffffffffffffffffffff ffffffffffffffffffffffffffffffffffff	Timeout
2	NACK	I2C communication error
3	21aab8289516978a7b25eb1d8a317f6c6a 71718b4d47de4754ac32a1d1c5adb7d324	Public key slot
4	21aa208cfc9a7dc7fcdb5437775fea79aa 2c95f5795ed2bfe883082a2ada0585694f	Needs to be investigated

- Correct read page trace for response 3
- In case of response 4, no EEPROM read
- It seems to be a RAM, or RNG content



Difference between response 3 (upper) and response 4 (below)

- The fault may change the page number.
- The two faults are in the logic area.



Response 3 and response 4 locations

Single fault effect

- Single laser pulse is not efficient (conclusion after several weeks of evaluation).
- Chip is protected against single fault attacks? (black box evaluation)
- Reverse-engineering the *Read Page* command is the only way to understand clearly.

LEAKAGE DETECTION AND MULTIPLE FAULTS

- A methodology to identify leakage moments which contain sensitive information
- It reduces the computation complexity of security evaluation and improves the efficiency of the SCAs.
- Several methods have been used to identify the amount of leakage such as SNR and NICV[7], and Welch's t-test[8].
- The Welch's t-test is calculated as shown in Eq. 1, where μ, S^2 and N are the mean, variance, and number of traces, respectively, for the two sets of data (0 and 1).

$$t = \frac{\mu_0 - \mu_1}{\sqrt{\frac{S_0^2}{N_0} + \frac{S_1^2}{N_1}}} \tag{1}$$

[7] S. Bhasin, J. Danger, and S. Guilley , "NICV: Normalized Inter-Class Variance for Detection of Side-Channel Leakage", SEC 2014

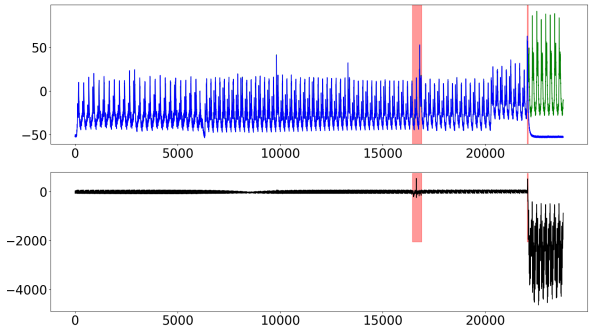
[8] Goodwill, Jaffe, and Rohatgi, "A testing methodology for side-channel resistance validation", 2011

T-test on read page command

- We will apply the t-test, which is used in SCAs to detect sensitive operations, in fault injection (FI).
- The main purpose is to detect when sensitive bits are processed.
- More precisely, we will try to locate on the power consumption trace, the manipulation of the page protection bit/bits.
- This can be done by performing the T-test between two. sets of data
  - The first set is collected when the page is unlocked (100K traces).
  - The second set is collected when the **same page** is locked (100K traces).

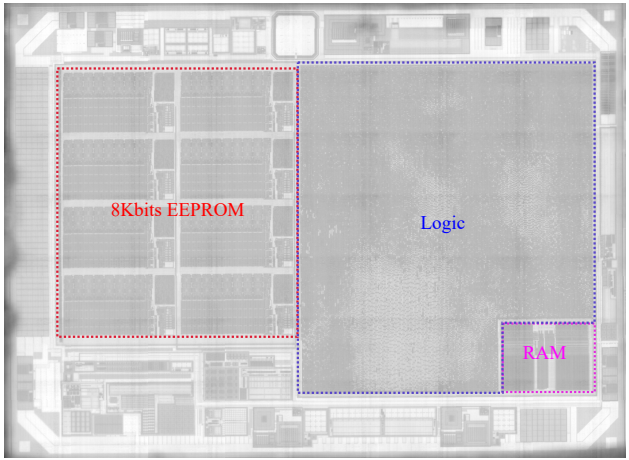
T-test on read page command

- Two zones of significant difference
- It hints that the chip is protected against single fault attacks.
- Multiple faults seem to be required.



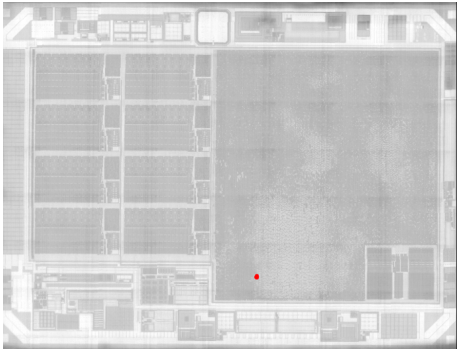
Upper: two traces protected and unprotected. Below: T-test result

- Injecting multiple pulses during and in-between the two windows
- Scanning the logic area

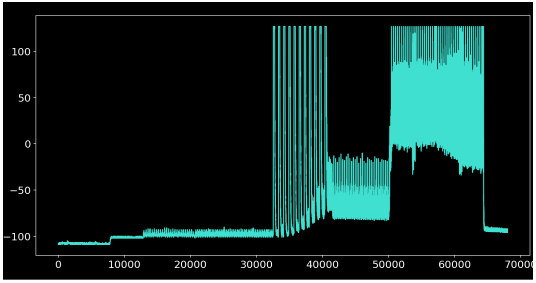


Infrared backside image

Successful faults



Successful fault position in red

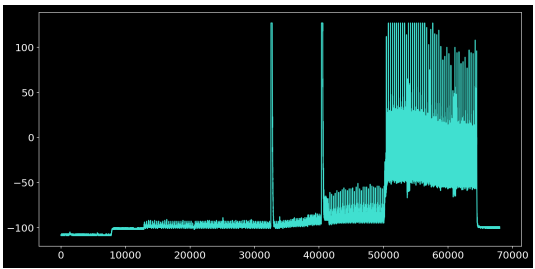


Power trace in case of a successful fault

Next step: Refining the number of faults.

Double fault attack

- Fixing the laser beam on the correct location
- Injecting double pulses related to the two peaks resulting from the T-test
- It needed to increase a little the laser power to obtain a successful fault.



Power trace in case of a successful fault

This confirms the t-test results.

User pages vs other pages

- The presented attack is applicable on all the user pages (Coldcard Mk4).
- It isn't applicable on permanent-protected pages used for P256 curve private keys.
    - The chip passed a fixed unidentified value for these pages.

RESPONSIBLE DISCLOSURE AND CONCLUSION

Disclosure

- The presented attack has been reported to Analog Devices before any publication.
- We also reported this work to the hardware wallet manufacturer Coinkite.

Conclusion and future work

- Side-channel techniques, such as Welch's t-test involved in this work, can be used when performing fault attack research in black box context.
- Using double verification against Fault Injection (FI) attacks is not efficient enough if it is used used alone.
- Manufacturers must at minimum combine it with hardware and/or software jitter as a countermeasure, to have unpredictable fault timings.
- For products that use DS28C36, we recommend splitting secrets into shares between different circuits to make the attack harder.
- Future work includes further research to investigate another attack path to extract the P256 curve private key pages.

THANK YOU. QUESTIONS?

Karim M. Abdellatif, PhD
e-mail: karim.abdellatif@ledger.fr