On the Security of Off-the-Shelf Microcontrollers : Hardware is not enough

Balazs Udvarhelyi, Antoine van Wassenhove, Olivier Bronchain, François-Xavier Standaert

UCL Crypto Group

Content

Introduction

Side-channel attacks in academia:

- Mostly well understood and controlled environments

Attacks on real world targets are more sporadic:

- SIM cards [ZYSQ13, LYS+15]
- Xilinx bitstream [MKP12, MS16]
- Smart lamps [RSWO17]

Introduction

Reccuring in published black-box evaluations:

1. Heavy reverse engineering effort needed.
2. With sufficient understanding, attacks are relatively easy.

Research question : *How much does obscurity help for unprotected hardware co-processors?*

Introduction

How much does obscurity help for unprotected hardware co-processors?

1. Case study with two AES-128 coprocessors (from ST & NXP).
2. Simple attack vectors can be exhibited with limited initial understanding of their architecture.
3. Using mostly standard tools and some slightly less standard ones: one-hot TVLA and CWT.

Content

Measurement setup

Target caracteristics:

- NXP Kinetis K82
- ARM Cortex-M4
- LP Trusted Cryptography core
- SCA countermeasure?

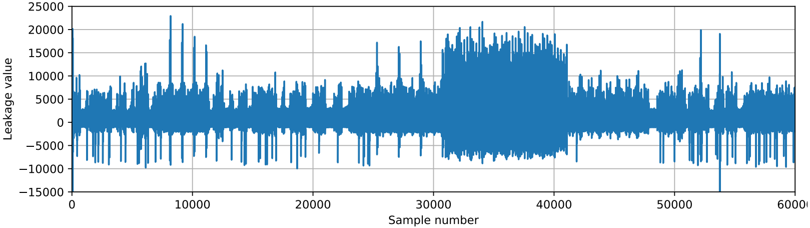
- STM 32 L4 Series
- ARM Cortex-M4
- AES peripheral
- No countermeasure

NXP Reference manual excerpt:

The DPA Mask Seed Register is used to reseed the mask that provides resistance against Differential Power Analysis attacks on AES keys.

Measurement setup

- Picoscope 5000 series
- 500 [MSamples/s], 8-bit
- H-field probe
- 10Ω shunt resistor
- MCU clock at 8MHz,80MHz and 100MHz



Content

Detection tools overview

Non-specific t-test

- Small number of classes to estimate
- Faster leakage detection

Specific tests (e.g. SNR)

- Using all classes to estimate
- POI detection is possible

Best of both worlds :

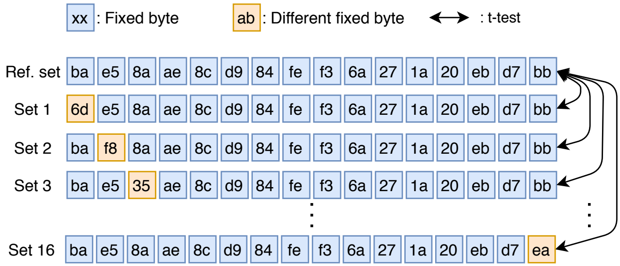
- Low number of classes to estimate
- While remaining specific

Some examples:

- Semi-fixed-vs-random t-test: Becomes more specific as the # of classes increases and model dependent
- We use the **One-hot TVLA**

One-hot TVLA

- Specific at some point, non-specific elsewhere with 2 classes/byte
- 16 well chosen fixed-vs-fixed *t*-tests
- Single byte difference in the first round of the AES
  - Specific for first AES round
- 17 sets of traces



One-hot TVLA and SNR combination

Comparison to other tools :

One-hot TVLA

- POIs can be identified
- Low memory needs
- Some false negatives

Signal to Noise Ratio

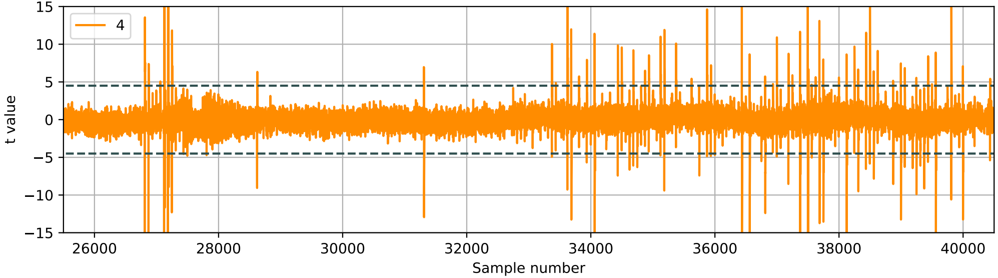
- SNR peaks have quantitative value
- 256 classes to estimate per byte
- Higher sampling complexity

One-hot TVLA and SNR complement each other

Content

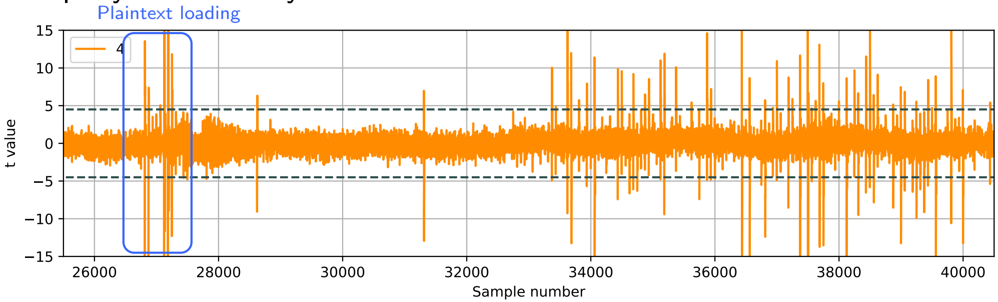
One-hot TVLA on NXP Kinetis

Exemplary t-test for byte 4



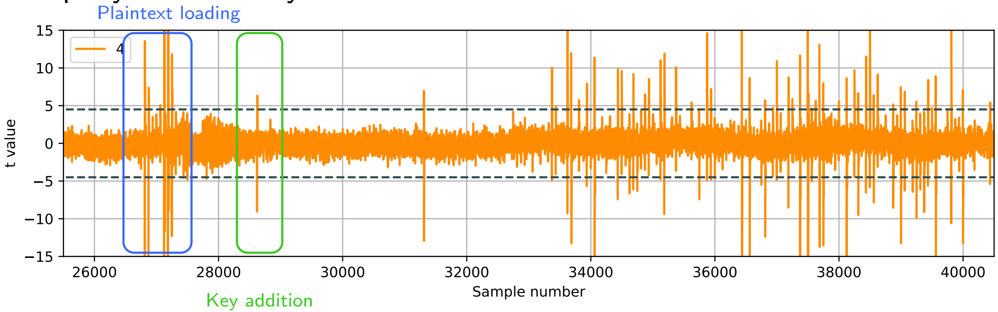
One-hot TVLA on NXP Kinetis

Exemplary t-test for byte 4



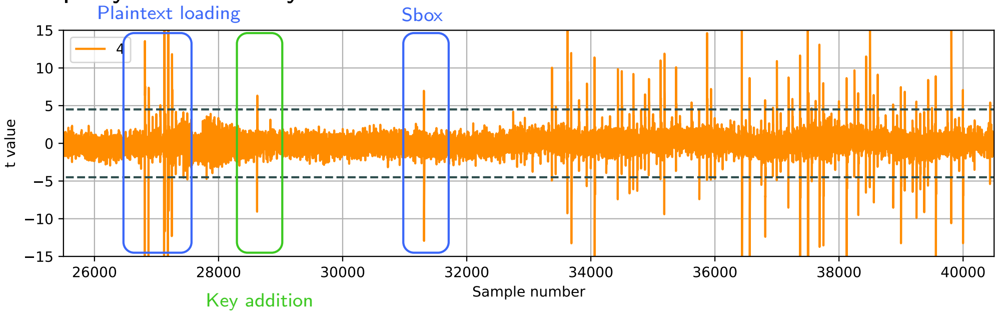
One-hot TVLA on NXP Kinetis

Exemplary t-test for byte 4



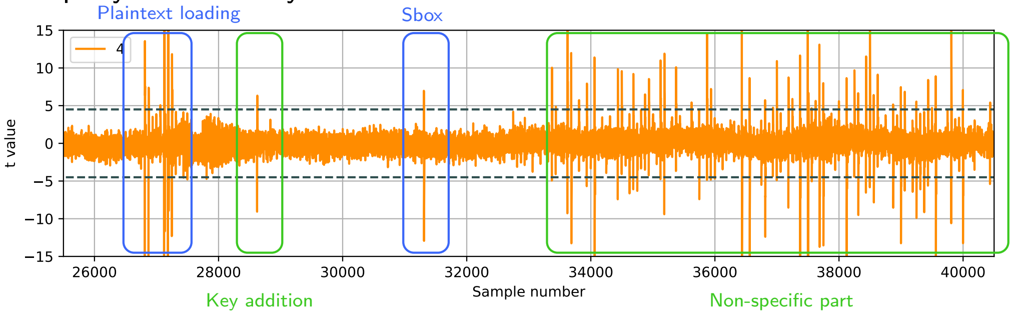
One-hot TVLA on NXP Kinetis

Exemplary t-test for byte 4



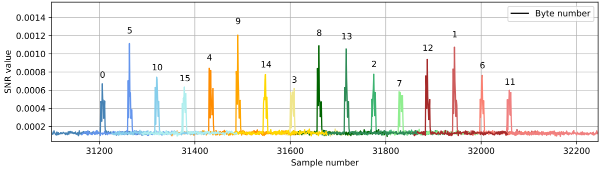
One-hot TVLA on NXP Kinetis

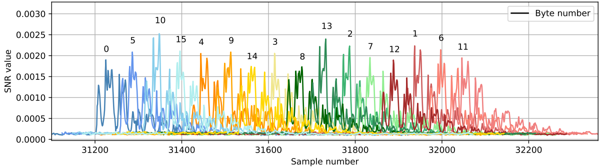
Exemplary t-test for byte 4



The t-test is indeed specific for the first round, and non-specific afterwards.

SNR on NXP Kinetis

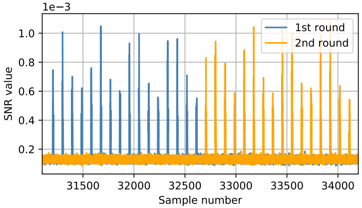




- Every byte is detected
- 1 cycle per byte
- EM leakage is more precise in time

NXP Kinetis Architecture

SNR on the first and second round:

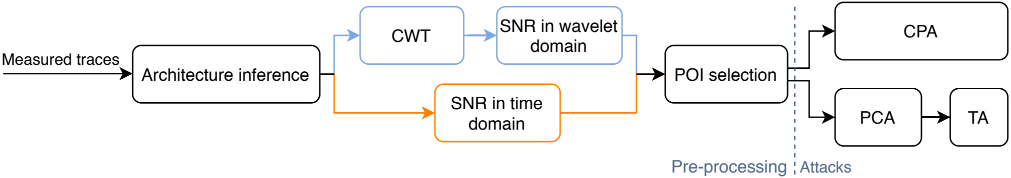


Conclusions :

- 16 Sboxes identified
- 1 cycle for each Sbox
- Serialized on 8-bit Sboxes
- Other operations parallel to Sboxes

Content

Attack strategies



- 2 attacks : CPA and Template attack
- Both TA and CPA are showed with profiled leakage model
- HW and HD CPA attacks were tested
  - Successful
  - Outperformed by profiled attacks

Attack results on NXP Kinetis

Device		2^{32} key rank		Full key recovery	
		CPA	TA	CPA	TA
NXP 8MHz	EM	27800	5200	N.A.	27400
	EM with CWT	3800	2400	7400	8800
	Power	6400	2000	15600	6200
	Power with CWT	12600	1200	27600	5400
NXP 100MHz	EM	26000	N.A.	N.A.	N.A.
	EM with CWT	4200	4400	11000	26600
	Power	N.A.	N.A.	N.A.	N.A.
	Power with CWT	10000	N.A.	N.A.	N.A.

Attack results on STM 32 L4

Device		2^{32} key rank		Full key recovery	
		CPA	TA	CPA	TA
STM32 8MHz	EM	16800	N.A.	N.A.	N.A.
	EM with CWT	3800	N.A.	11000	N.A.
	Power	4200	N.A.	17400	N.A.
	Power with CWT	1800	38000	5400	N.A.
STM32 80MHz	EM	30000	N.A.	N.A.	N.A.
	EM with CWT	2200	N.A.	7200	N.A.
	Power	1600	N.A.	7400	N.A.
	Power with CWT	1600	N.A.	6200	N.A.

Discussion : Attack strategies

Attacks, Template vs CPA:

- Best results obtained with CPA
- Device dependent
- Multiple dimensions of the TA $\rightarrow$ higher profiling effort
- TA should at least reach efficiency of CPA with more profiling effort

Discussion : Attack strategies

Attacks, Template vs CPA:

- Best results obtained with CPA
- Device dependent
- Multiple dimensions of the TA $\rightarrow$ higher profiling effort
- TA should at least reach efficiency of CPA with more profiling effort

Continuous wavelet transform:

- Almost always improving attacks for our setup
- Higher gain for EM attacks

Discussion : Targets

Clock speed:

- Impact of higher clock speed:
  - Slightly harder for NXP
  - No particular effect on STM
- No particular challenge at these clock speeds

Discussion : Targets

Clock speed:

- Impact of higher clock speed:
  - Slightly harder for NXP
  - No particular effect on STM
- No particular challenge at these clock speeds

NXP Countermeasure:

- Multiple tests performed
- No noticeable difference in attack results
- Confirmed by independent teams

Content

Conclusion

- Obscurity did not prevent side-channel attacks
- Yet attacks are also non trivial and require more than 1000 traces to succeed
- Natural direction is to investigate their integration into leakage-resilient modes of operation [BBC+20, USS+20]

Thank you!

Bibliography I

- Davide Bellizia, Olivier Bronchain, Gaëtan Cassiers, Vincent Grosso, Chun Guo, Charles Momin, Olivier Pereira, Thomas Peters, and François-Xavier Standaert, *Mode-level vs. implementation-level physical security in symmetric cryptography - A practical guide through the leakage-resistance jungle*, CRYPTO (1), Lecture Notes in Computer Science, vol. 12170, Springer, 2020, pp. 369–400.

- Junrong Liu, Yu Yu, François-Xavier Standaert, Zheng Guo, Dawu Gu, Wei Sun, Yijie Ge, and Xinjun Xie, *Small tweaks do not help: Differential power analysis of MILENAGE implementations in 3g/4g USIM cards*, ESORICS (1), Lecture Notes in Computer Science, vol. 9326, Springer, 2015, pp. 468–480.

Bibliography II

Amir Moradi, Markus Kasper, and Christof Paar, *Black-box side-channel attacks highlight the importance of countermeasures - an analysis of the xilinx virtex-4 and virtex-5 bitstream encryption mechanism*, CT-RSA, Lecture Notes in Computer Science, vol. 7178, Springer, 2012, pp. 1–18.

Amir Moradi and Tobias Schneider, *Improved side-channel analysis attacks on xilinx bitstream encryption of 5, 6, and 7 series*, COSADE, Lecture Notes in Computer Science, vol. 9689, Springer, 2016, pp. 71–87.

Bibliography III

- Eyal Ronen, Adi Shamir, Achi-Or Weingarten, and Colin O'Flynn, *Iot goes nuclear: Creating a zigbee chain reaction*, IEEE Symposium on Security and Privacy, IEEE Computer Society, 2017, pp. 195–212.
- Florian Unterstein, Marc Schink, Thomas Schamberger, Lars Tebelmann, Manuel Ilg, and Johann Heyszl, *Retrofitting leakage resilient authenticated encryption to microcontrollers*, IACR Trans. Cryptogr. Hardw. Embed. Syst. **2020** (2020), no. 4, 365–388.

Bibliography IV

Yuanyuan Zhou, Yu Yu, François-Xavier Standaert, and Jean-Jacques Quisquater, *On the need of physical security for small embedded devices: A case study with COMP128-1 implementations in SIM cards*, Financial Cryptography, Lecture Notes in Computer Science, vol. 7859, Springer, 2013, pp. 230–238.