A Key Update Scheme for Side-Channel Attack Mitigation

Yutian Gui, Suyash Mohan Tamore, Ali Shuja Siddiqui and Fareena Saqib
University of North Carolina at Charlotte, Charlotte, USA
ygui@uncc.edu, stamore@uncc.edu, asiddiq6@uncc.edu, fsaqib@uncc.edu

Abstract: In contrast to other attack models, the side-channel attack (SCA) utilizes various physical parameters to steal secret information non-invasively. As two typical representatives of Side-Channel Attack (SCA), power analysis attack and electromagnetic attack show a very high efficiency to extract cryptographic keys and other secret information from hardware devices. By applying the key update scheme which is presented in this DEMO, the risk of side-channel attacks based on power analysis and EM analysis can be reduced significantly.

Introduction

- Modern encryption algorithms, such as RSA and AES, have been proved efficient to defend brute-force attack and eavesdropping attack.
- Instead of targeting the algorithm itself, side-channel attacks focus on digging the correlated relationship between the leaked physical information and the real-time operation executed on the cryptographic device to reveal the secret information.
- The side-channel attack is passive and non-invasive (even non-contact) which brings a lot of difficulties for detection and defense.

AES Encryption

- For AES-128, there are 11 rounds in encryption with 11 round keys derived from the original key :
- Round 0: **AddRoundKey**: Combine each byte of the state with the corresponding byte of the round key by using bitwise XOR.
- Round 1 – Round 9: Each round has 4 operations: **SubBytes** (non-linear substitution based on look-up table named S-box), **ShiftRows** (cyclic shifting in each row by a certain offset), **MixColumns** (invertible linear transformation combing the bytes in each column), **AddRoundKey**
- Round 10: Consist of 3 operations: **SubBytes, ShiftRows** and **AddRoundKey**

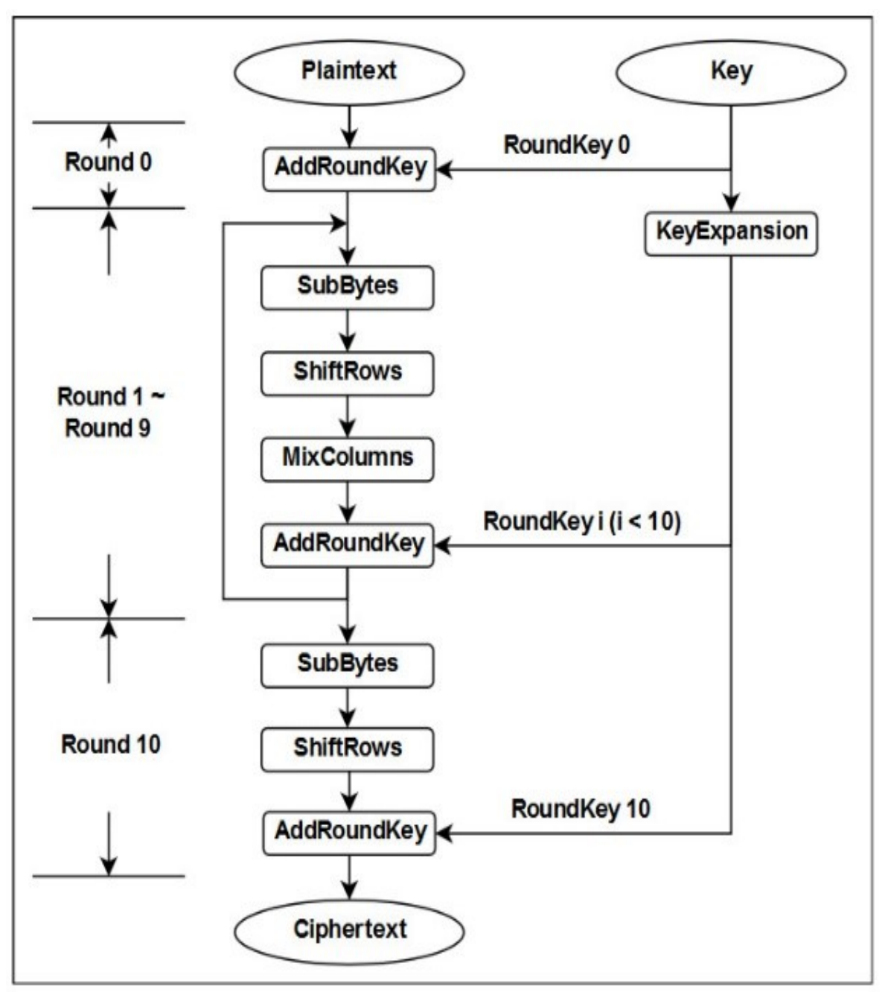

Fig.1: Encryption Process of AES-128

Side-Channel Attack

- In contrast to other attack models, the side-channel attack (SCA) utilizes various physical parameters to steal, such as power consumption, EM radiation, time delay [2] and sound.
- Extract secret information using leaked physical information based on the truth that the variation of leaked physical parameters is correlated to different operations executed on the hardware device during the run-time.
- Passive & non-invasive attack: The attacker only passively observes and utilizes leaked information and doesn't open up the chip or manipulate the packaging at all.

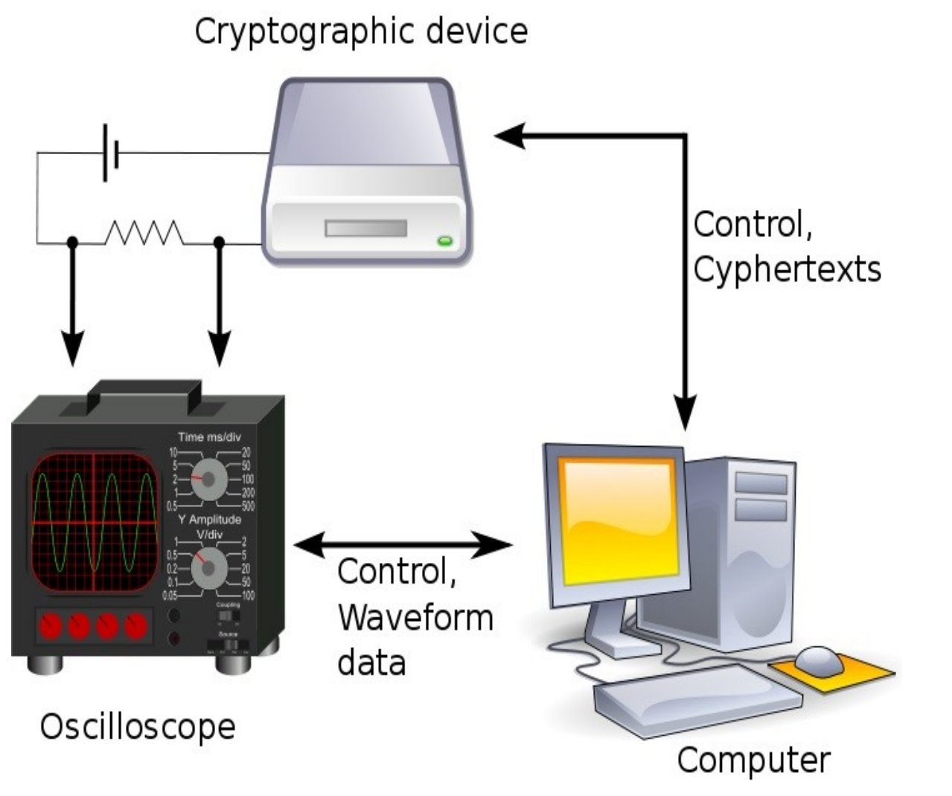

Fig.2: Attack process of Power/EM analysis.

Correlation Analysis

A more efficient attack which uses hamming weight to build the model and Pearson coefficient to evaluate the correlation between the hypothetical model and the actual power/EM traces [3]:

1. Collect Power/EM traces of the first/last round of AES-128 during the execution of the encryption process.
2. Build the leakage model. Most of the energy is consumed by the operation of SubBytes [4], so the output of the S-Box is the point to check the guessed value of the key.
3. Key guessing. The original key is divided into 16 bytes. For each subkey, guess every possible value.
4. Correlation Analysis. Evaluate the correlation between the modeled power and the actual power trace by using Pearson correlation coefficient ***ρ*** which is defined as:

$$\rho(A,B) = \frac{cov(A,B)}{\sigma_A\sigma_B} = \frac{\mathrm{E}[(A-\mu_A)(B-\mu_B)]}{\sqrt{\mathrm{E}[(A-\mu_A)^2]}\sqrt{\mathrm{E}[(B-\mu_B)^2]}}$$

A, B : Variables ***cov*** : Covariance
μ *: mean value* **E** : Expectation

In this work, two variables are the hypothetical value and the actual power/EM trace, so the Pearson correlation coefficient ***C*** is applied in this way:

$$C(h,t) = \frac{\sum_{d=1}^{D}[(\mathrm{h}_d-\overline{\mathrm{h}})(\mathrm{t}_d-\overline{\mathrm{t}})]}{\sqrt{\sum_{d=1}^{D}(\mathrm{h}_d-\overline{\mathrm{h}})^2\sum_{d=1}^{D}(\mathrm{t}_d-\overline{\mathrm{t}})^2}}$$

h : Hypothetical value of subkey
t : Power/EM trace
D *: total number of traces*

5. Key obtainment. The guessed subkey with the highest coefficient is considered as most likely the correct subkey used in the encryption.

Acknowledgements

This research is supported by the National Science Foundation NSF under grant No. 1814420

Proposed Key Update Scheme

Basic Idea: Obtain the Least Needed power/EM Traces (LNT) of the target cryptographic device by simulation experiments and update the key on each node synchronously before any subkey can be revealed:

1. Determine the LNT for Single key (LNTS) of the target hardware.
2. Generate a list of random secret keys for encryption/decryption on TPM, and shared with the receiver
3. Set the Update Period (UP) which is less than LNTS and share it with the receiver.
4. Start the encryption process with the first key and change the key following the order of the key list circularly when the value of the counter reaches the value of UP on both sender side and receiver side.

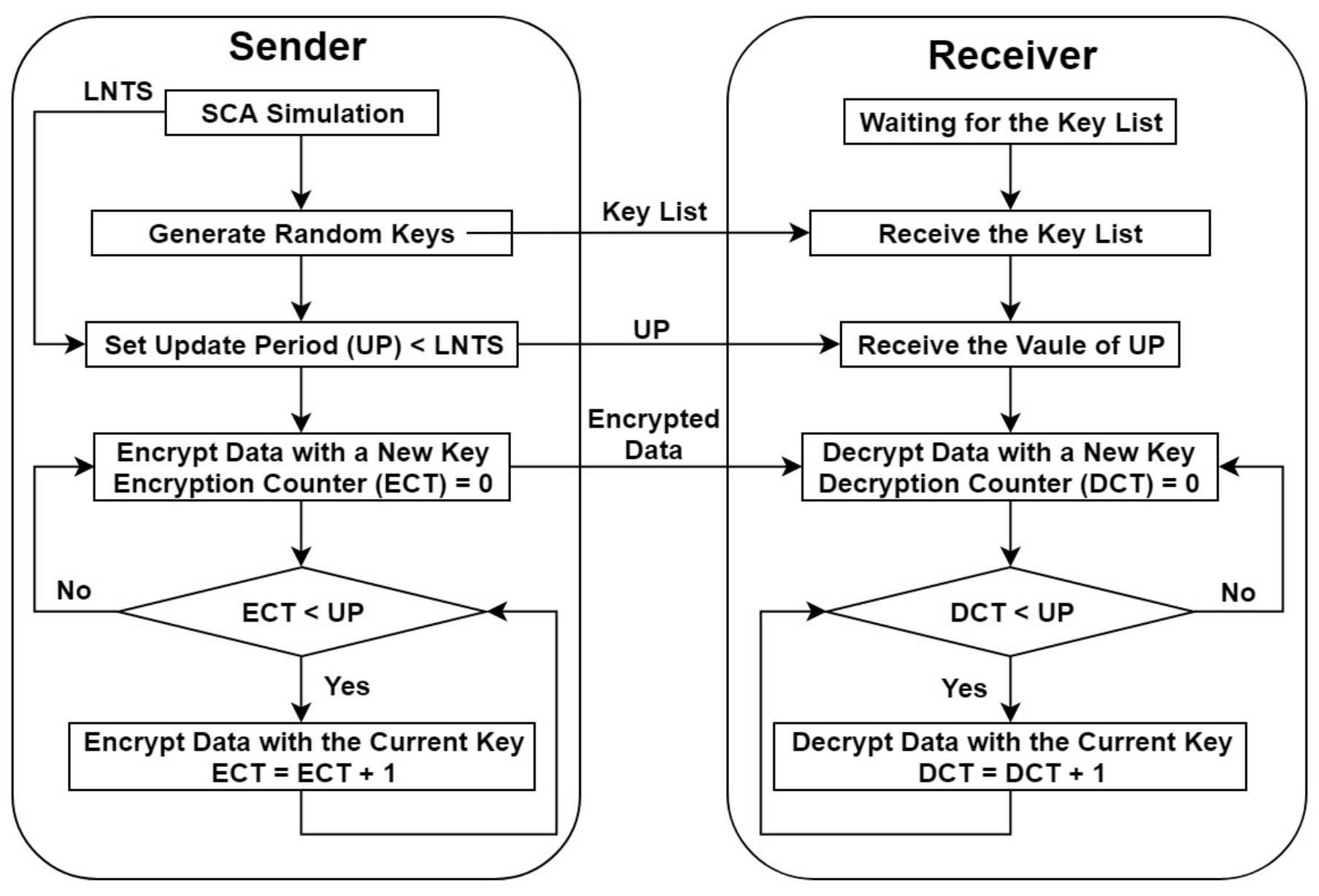
Sender
LNTS
SCA Simulation
Generate Random Keys
Set Update Period (UP) < LNTS
Encrypt Data with a New Key
Encryption Counter (ECT) = 0
No
ECT < UP
Yes
Encrypt Data with the Current Key
ECT = ECT + 1
Key List
UP
Encrypted Data
Receiver
Waiting for the Key List
Receive the Key List
Receive the Vaule of UP
Decrypt Data with a New Key
Decryption Counter (DCT) = 0
DCT < UP
No
Yes
Decrypt Data with the Current Key
DCT = DCT + 1

Fig.3: Proposed key update scheme

Experimental Setup

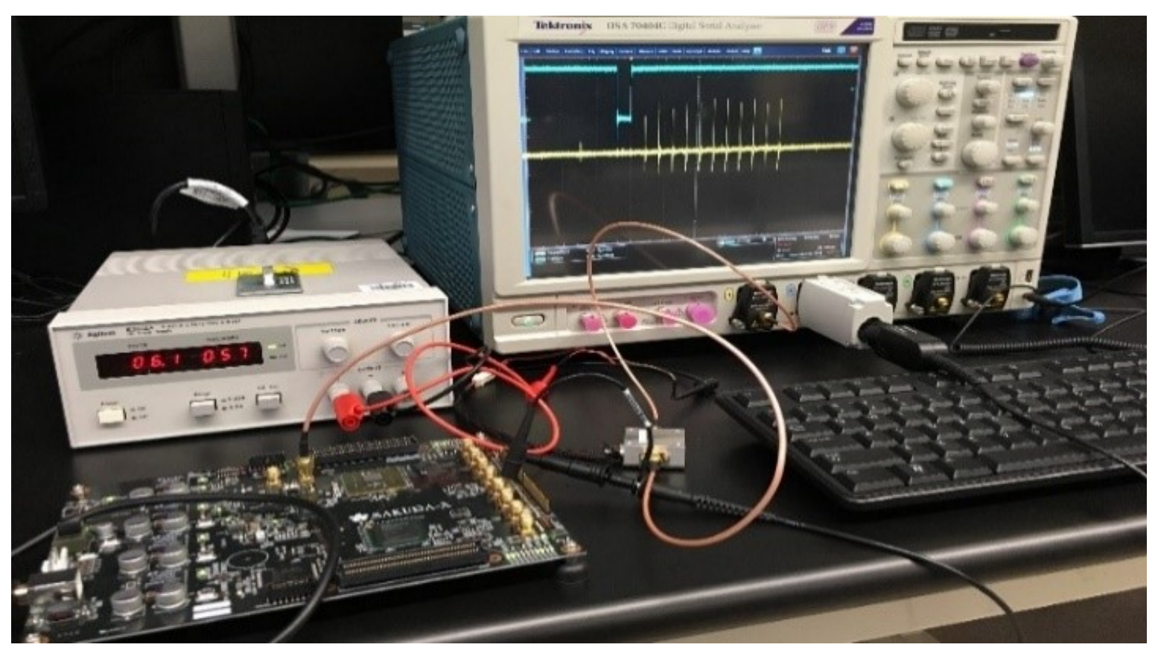

Fig.4: Setup of Power Capture

Hardware:

- Sakura-X experimental board
- LNA-1050 low noise amplifier
- Oscilloscope
- Passive Probe (For Power Consumption)
- CW505 Planar H-field EM probe (For EM)

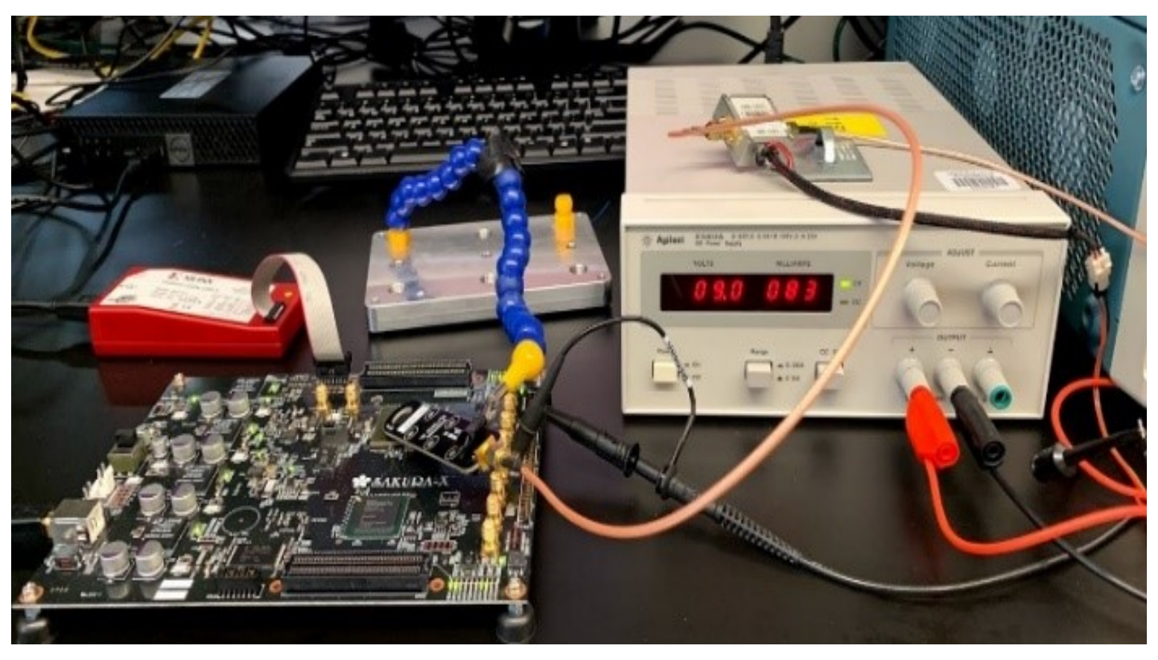

Fig.5: Setup of EM Capture

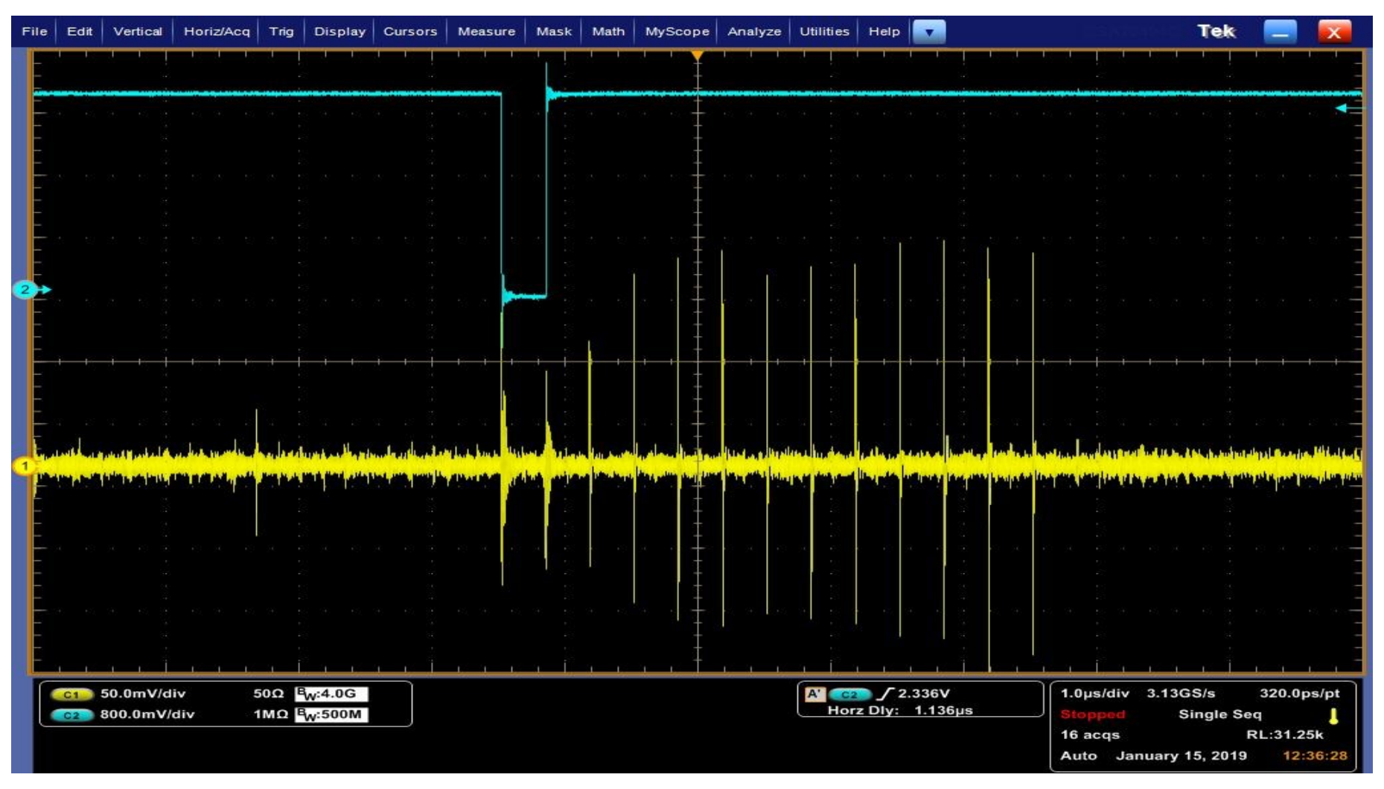

Fig.6: EM Trace of AES Encryption

Experimental Result

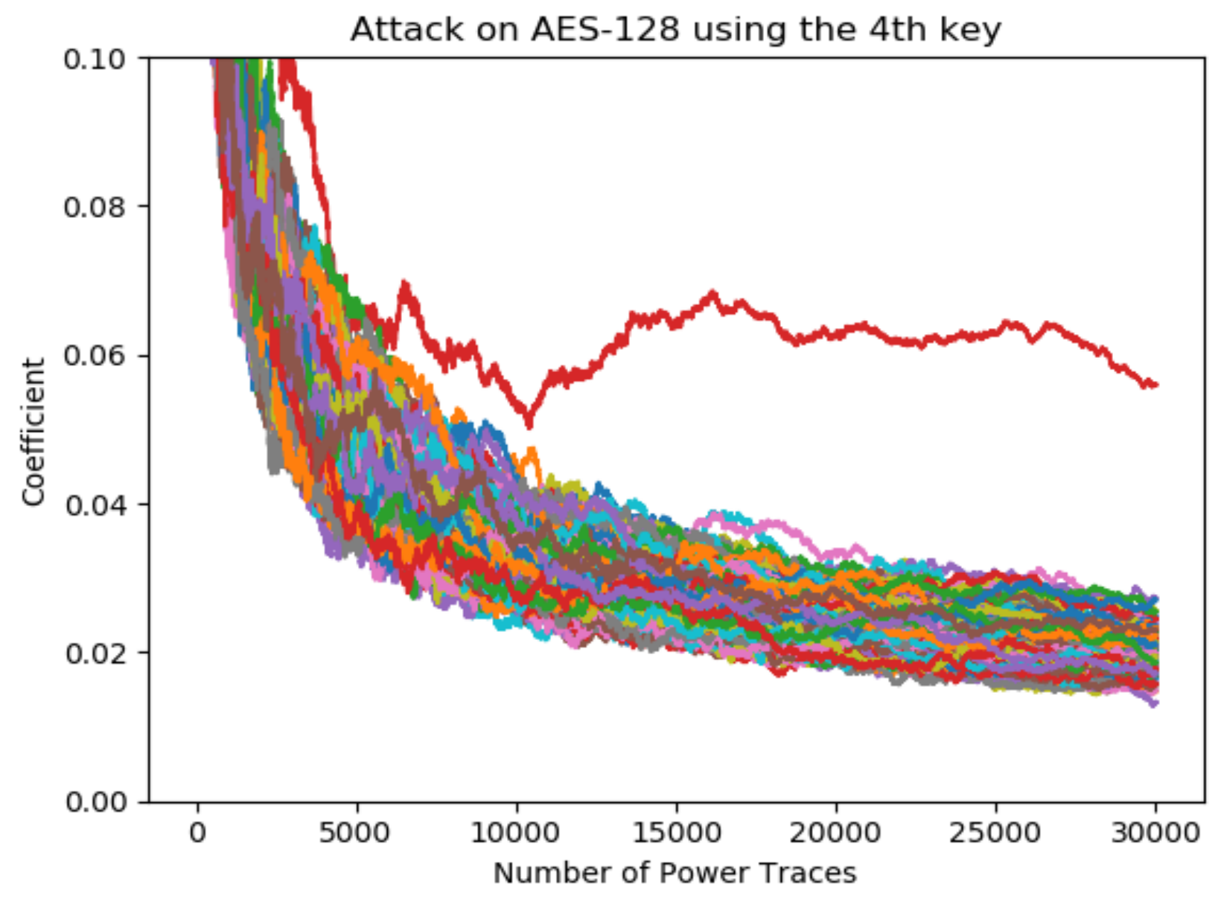

Fig 7.: The result of CPA attack on the first subkey

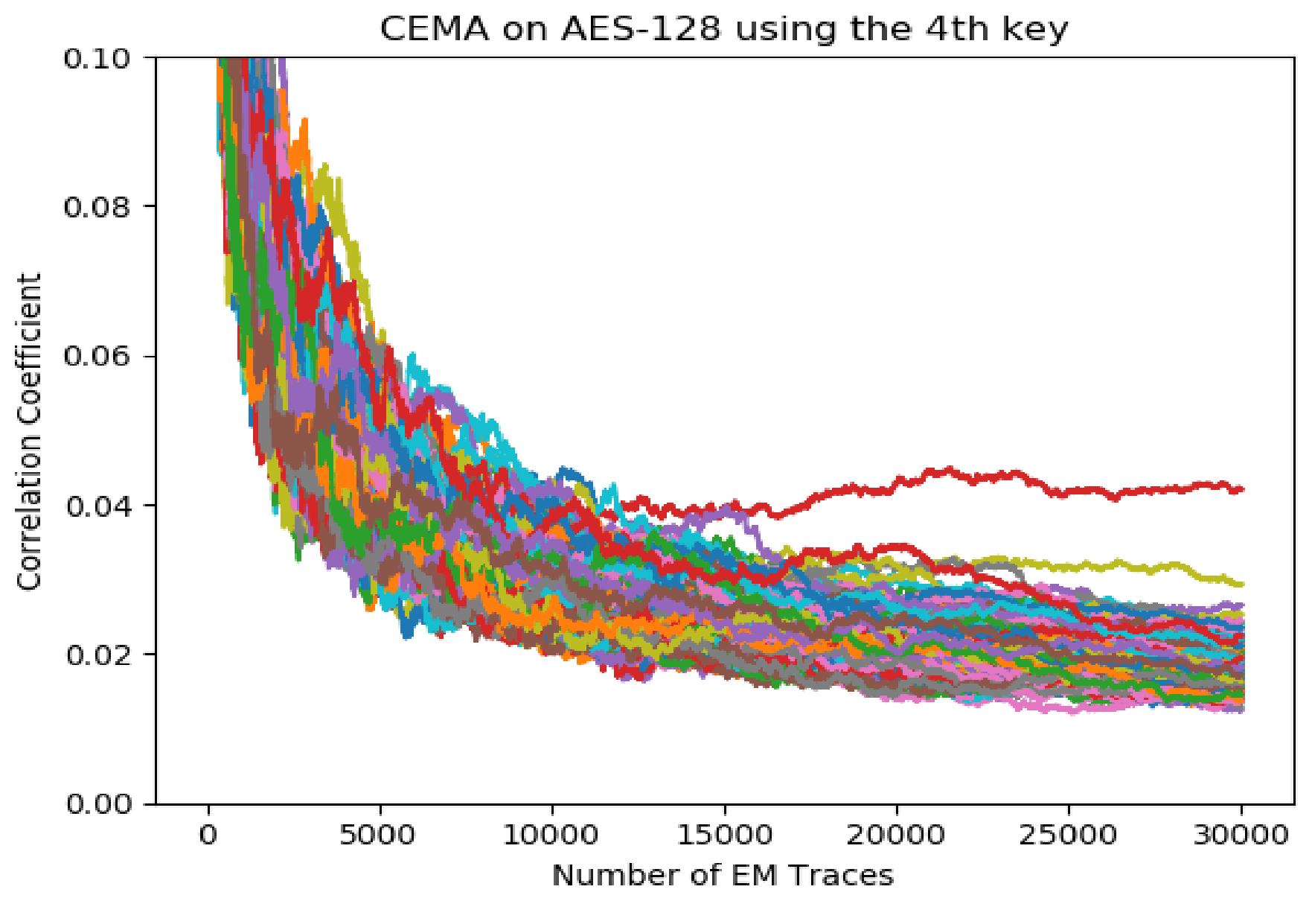

Fig.8: The result of CEMA attack on the first subkey

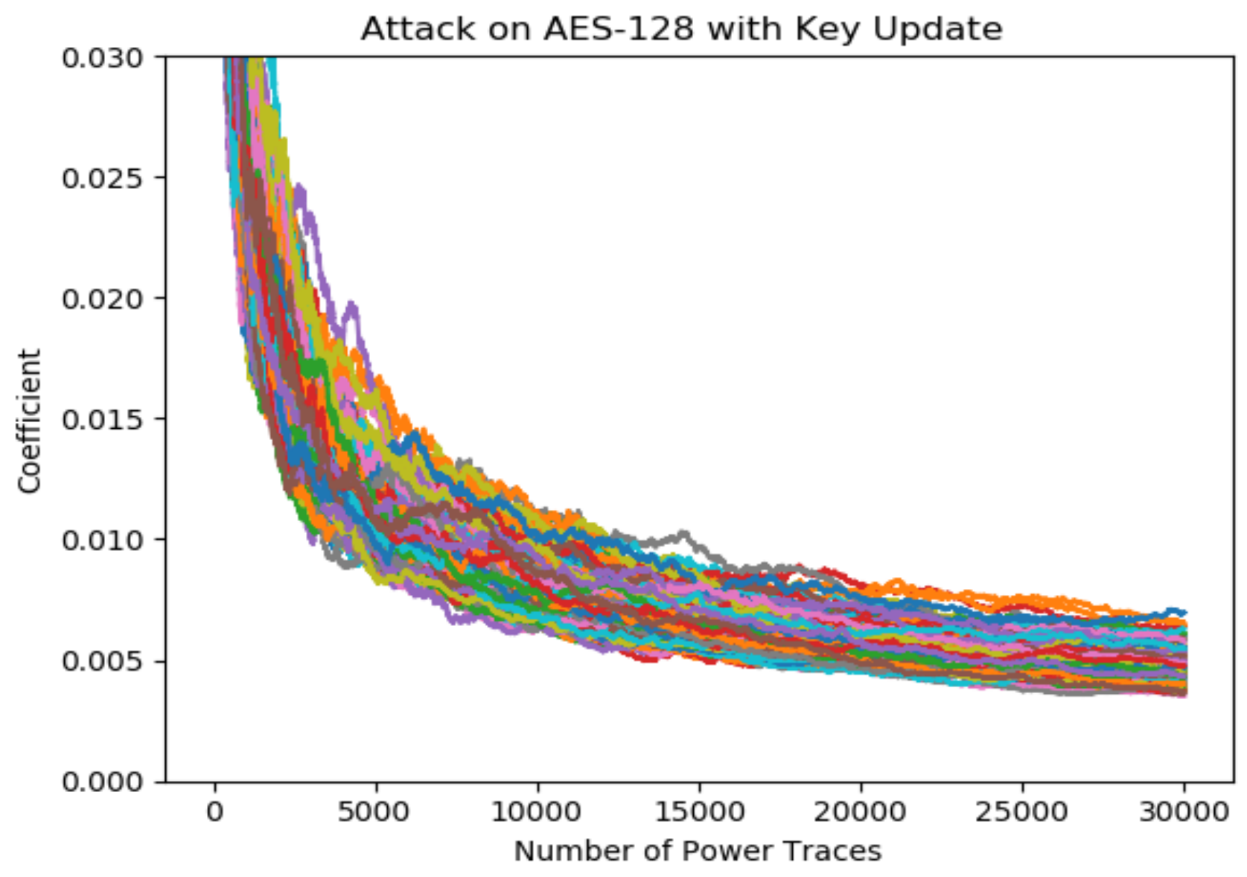

Fig.9: The result of CPA attack on the first subkey after applying the key update scheme

Least needed power traces for a successful CPA attack on the first subkey (2B) of AES-128: ≈ **5000 (Fig.7)**

Least needed EM traces for a successful CEMA attack on the first subkey (2B) of AES-128: ≈ **15000 (Fig.8)**

Least needed power traces for a successful CPA attack on the first subkey of AES-128 after applying key update scheme with 4 random keys: **> 30000 (Fig.9)**

Reference

[1] United States National Institute of Standards and Technology (NIST). "Announcing the ADVANCED ENCRYPTION STANDARD (AES)," in *Federal Information Processing Standards Publication 197*, November 2001.
[2] Paul C. Kocher. "Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems," in *Koblitz N. (eds) Advances in Cryptology — CRYPTO '96*, vol. 1109, pp.104-113, 1996.
[3] E. Brier, C. Clavier, and F. Olivier. "Correlation power analysis with a leakage model," in *Joye M., Quisquater JJ. (eds) Cryptographic Hardware and Embedded Systems - CHES 2004*, vol. 3156, pp.16-29, 2004.
[4] Sumio Morioka and Akashi Satoh. "An Optimized S-Box Circuit Architecture for Low PowerAES Design," in *In: Kaliski B.S., Koç .K., Paar C. (eds) Cryptographic Hardware and Embedded Systems - CHES 2002.*, vol 2523, pp. 172-186