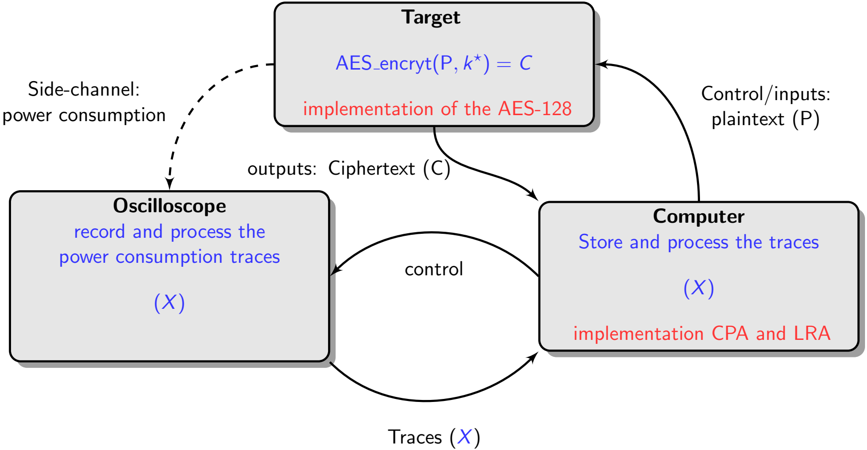
TOPIC VET: Correlation Power Analysis (CPA) and Linear Regression Analysis (LRA) Against AES-128 Traces

Advisor: Damien Marion

November 05, 2020

EMSEC

Overview



Target

$\mathrm{AES\_encryt}(\mathrm{P}, k^{\star}) = C$

implementation of the AES-128

Side-channel: power consumption

Control/inputs: plaintext (P)

outputs: Ciphertext (C)

Oscilloscope

record and process the power consumption traces

(X)

control

Computer

Store and process the traces

(X)

implementation CPA and LRA

Traces (X)

- Goal: understand and implement the CPA and LRA to recover the secret key $k^{\star}$ using the power traces X and the plaintext P (or the ciphertext C).

Project Organization

1. Understanding the two attacks: the CPA, the LRA and the target (AES-128):
    - *Behind the Scene of Side Channel Attacks* [8],
    - *Univariate side channel attacks and leakage modeling* [4],
    - *Correlation Power Analysis with a Leakage Model* [2],
    - *Specification for the Advanced Encryption Standard (AES)* [1],
    - *Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems* [6],
    - *DES and Differential Power Analysis (The ”Duplication” Method)* [5].
2. implementation of the AES-128 in python,
3. implementation of two leakage models,
4. implementation of the CPA and the LRA,
5. mount CPA and LRA against real world power traces from CTF (CHES-2016 [9], DPA-contest V2 [3])

Papers

- *Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems* [6]
  - first pulbished side-channel attack (timing attack).
- *DES and Differential Power Analysis (The "Duplication" Method)* [5]
  - seminal paper of the masking, one of the most powerful and used countermeasure against side-channel attacks
- *Correlation Power Analysis with a Leakage Model* [2]:
  - seminal paper of the CPA and first usage of a leakage model.
- *Univariate side channel attacks and leakage modeling* [4]:
  - seminal paper of the LRA with a learning step.
- *Behind the Scene of Side Channel Attacks* [8]:
  - practical paper, concrete evaluation and implementation of the CPA, LRA.
- *Specification for the Advanced Encryption Standard (AES)* [1].
  - full description of the Advanced Encryption Standard (AES).

Bibliographical references I

[1] Federal Information Processin Standards Publication 197, ed. *Specification for the Advanced Encryption Standard (AES)*. link to the document: http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf. 2001.

[2] Eric Brier, Christophe Clavier, and Francis Olivier. *Correlation Power Analysis with a Leakage Model*. Ed. by Marc Joye and Jean-Jacques Quisquater. eprint version https://www.iacr.org/archive/ches2004/31560016/31560016.pdf. 2004. DOI: 10.1007/978-3-540-28632-5_2. URL: http://dx.doi.org/10.1007/978-3-540-28632-5_2.

[3] Christophe Clavier et al. *Practical improvements of side-channel attacks on AES: feedback from the 2nd DPA contest*. link to the DPA-contest V2 website: http://www.dpacontest.org/v2/. 2014. DOI: 10.1007/s13389-014-0075-9.

Bibliographical references II

[4] Julien Doget et al. *Univariate side channel attacks and leakage modeling*. 2011. DOI: 10.1007/s13389-011-0010-2. URL: https://doi.org/10.1007/s13389-011-0010-2.

[5] Louis Goubin and Jacques Patarin. "DES and Differential Power Analysis (The "Duplication" Method)". In: *Cryptographic Hardware and Embedded Systems, First International Workshop, CHES'99, Worcester, MA, USA, August 12-13, 1999, Proceedings*. 1999, pp. 158–172. DOI: 10.1007/3-540-48059-5_15. URL: http://dx.doi.org/10.1007/3-540-48059-5_15.

[6] Paul C. Kocher. "Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems". In: *Advances in Cryptology - CRYPTO '96, 16th Annual International Cryptology Conference, Santa Barbara, California, USA, August 18-22, 1996, Proceedings*. 1996, pp. 104–113. DOI: 10.1007/3-540-68697-5_9.

Bibliographical references III

[7] Paul C. Kocher, Joshua Jaffe, and Benjamin Jun. "Differential Power Analysis". In: *Advances in Cryptology - CRYPTO '99, 19th Annual International Cryptology Conference, Santa Barbara, California, USA, August 15-19, 1999, Proceedings*. Ed. by Michael J. Wiener. Vol. 1666. Lecture Notes in Computer Science. Springer, 1999, pp. 388–397. ISBN: 3-540-66347-9. DOI: 10.1007/3-540-48405-1_25. URL: http://dx.doi.org/10.1007/3-540-48405-1_25.

[8] Victor Lomné, Emmanuel Prouff, and Thomas Roche. *Behind the Scene of Side Channel Attacks*. Ed. by Kazue Sako and Palash Sarkar. Extended version freely available: https://eprint.iacr.org/2013/794.pdf. 2013. DOI: 10.1007/978-3-642-42033-7_26. URL: https://doi.org/10.1007/978-3-642-42033-7_26.

Bibliographical references IV

[9] Colin O'Flynn. *CHES 2016 Capture the Flag - (NewAE)*. `http://ctf.newae.com/flags/`. 2016.