Master research Internship

Bibliographic report

SCARE for Hardware SPN

Domain: Cryptography and Security

Author:
First_Name Name

Supervisor:
First_Name Name of your first supervisor
First_Name Name of your second supervisor
Name of the team in which you are doing your internship

CentraleSupélec

Abstract: write your abstract here

Contents

Introduction

Here start your document - Should be 15 pages long

Following Kerchoffs' principle, the security of a cryptographic device shall not rely on the secrecy of its mechanisms [Ker83]. However in some specific contexts, having a secret implementation can add a layer of security, by increasing the practical difficulty of the attack.

1 State of the art of Side Channel Attacks on SPNs

1.1 SPNs, Feistel schemes, DES and AES

Feistel scheme, DES

[ST01]

1.2 Side Channel Analysis classic attacks

SPA, DPA, CPA explanation (ref papers ?)

[CRR03] presents template attacks, "the strongest form of side channel attack possible in an information theoretic sense".

[PR70] presents the theory of Mutual Information Attacks (MIA) in side channels.

Machine Learning is very popular right now.

2 SCARE attacks

2.1 SCARE attacks on non AES ciphers

[Nov03] presents a side-channel attack on substitution blocks with a demonstration on a SIM card using COMP-128 cipher.

[Dau+05] presents a SCARE attack on DES and propose new methods to exploit the power measurement information.

[Gui+10] presents two SCARE attacks on the parameters of a LFSR and DES.

2.2 SCARE attacks on AES-like ciphers

[Tie+15] presents an integral cryptanalysis of an AES with a secret S-box and less rounds. It is not a SCA but is still closely related to our subject.

[RR13] presents a generic SCARE attack against a wide class of SPN block ciphers.

FIRE (injection fault attempts) and SCARE attacks to recover the full set of secret parameters of an AES-like software implementation, even with masking and shuffling [Cla+15].

3 Application to hardware implementations

[Réa+08] presents a SCARE attack on a general Feistel scheme with an hardware design.

SAKURA board reference

SCA attacks on FPGAs ([Pee+05] or more relevantly [SOP04] or something more recent)

4 Conclusion

References

References

[CRR03] Suresh Chari, Josyula R. Rao, and Pankaj Rohatgi. “Template Attacks”. en. In: *Cryptographic Hardware and Embedded Systems - CHES 2002*. Ed. by Burton S. Kaliski, çetin K. Koç, and Christof Paar. Vol. 2523. Lecture Notes in Computer Science. Berlin, Heidelberg: Springer Berlin Heidelberg, 2003, pp. 13–28. ISBN: 978-3-540-00409-7. DOI: 10.1007/3-540-36400-5_3. URL: http://link.springer.com/10.1007/3-540-36400-5_3.

[Cla+15] Christophe Clavier et al. “Complete reverse-engineering of AES-like block ciphers by SCARE and FIRE attacks”. en. In: *Cryptography and Communications* 7.1 (Mar. 2015), pp. 121–162. ISSN: 1936-2447, 1936-2455. DOI: 10.1007/s12095-014-0112-7.

[Dau+05] Rémy Daudigny et al. “SCARE of the DES: (Side Channel Analysis for Reverse Engineering of the Data Encryption Standard)”. en. In: *Applied Cryptography and Network Security*. Ed. by John Ioannidis, Angelos Keromytis, and Moti Yung. Vol. 3531. Lecture Notes in Computer Science. Berlin, Heidelberg: Springer Berlin Heidelberg, 2005, pp. 393–406. ISBN: 978-3-540-26223-7. DOI: 10.1007/11496137_27. URL: http://link.springer.com/10.1007/11496137_27.

[Gui+10] Sylvain Guilley et al. “Defeating Any Secret Cryptography with SCARE Attacks”. In: vol. 6212. Aug. 2010, pp. 273–293. ISBN: 978-3-642-14711-1. DOI: 10.1007/978-3-642-14712-8_17.

[Ker83] Auguste Kerckhoffs. “La cryptographie militaire”. In: *Journal des sciences militaires* (Jan. 1883), pp. 5–38.

[Nov03] Roman Novak. “Side-Channel Attack on Substitution Blocks”. en. In: *Applied Cryptography and Network Security*. Ed. by Jianying Zhou, Moti Yung, and Yongfei Han. Vol. 2846. Lecture Notes in Computer Science. Berlin, Heidelberg: Springer Berlin Heidelberg, 2003, pp. 307–318. ISBN: 978-3-540-20208-0. DOI: 10.1007/978-3-540-45203-4_24. URL: http://link.springer.com/10.1007/978-3-540-45203-4_24.

[Pee+05] Eric Peeters et al. “Improved Higher-Order Side-Channel Attacks with FPGA Experiments”. en. In: *Cryptographic Hardware and Embedded Systems – CHES 2005*. Ed. by Josyula R. Rao and Berk Sunar. Vol. 3659. Lecture Notes in Computer Science. Berlin, Heidelberg: Springer Berlin Heidelberg, 2005, pp. 309–323. ISBN: 978-3-540-28474-1. DOI: 10.1007/11545262_23. URL: http://link.springer.com/10.1007/11545262_23.

[PR70] Emmanuel Prouff and Matthieu Rivain. “Theoretical and Practical Aspects of Mutual Information Based Side Channel Analysis”. In: vol. 5536. Jan. 1970, pp. 499–518. ISBN: 978-3-642-01956-2. DOI: 10.1007/978-3-642-01957-9_31.

[Réa+08] Denis Réal et al. “SCARE of an Unknown Hardware Feistel Implementation”. en. In: *Smart Card Research and Advanced Applications*. Ed. by Gilles Grimaud and François-Xavier Standaert. Vol. 5189. Lecture Notes in Computer Science. Berlin, Heidelberg: Springer Berlin Heidelberg, 2008, pp. 218–227. ISBN: 978-3-540-85892-8. DOI: 10.1007/978-3-540-85893-5_16. URL: http://link.springer.com/10.1007/978-3-540-85893-5_16.

[RR13] Matthieu Rivain and Thomas Roche. “SCARE of Secret Ciphers with SPN Structures”. en. In: *Advances in Cryptology - ASIACRYPT 2013*. Ed. by Kazue Sako and Palash Sarkar. Vol. 8269. Lecture Notes in Computer Science. Berlin, Heidelberg: Springer Berlin Heidelberg, 2013, pp. 526–544. ISBN: 978-3-642-42032-0. DOI: 10.1007/978-3-642-42033-7_27. URL: http://link.springer.com/10.1007/978-3-642-42033-7_27.

[SOP04] François-Xavier Standaert, Berna Ors, and Bart Preneel. “Power Analysis of an FPGA: Implementation of Rijndael: Is Pipelining a DPA Countermeasure?” In: vol. 3156. Jan. 2004, pp. 30–44. DOI: 10.1007/b99451.

[ST01] National Institute of Standards and Technology. “Advanced Encryption Standard”. In: *NIST FIPS PUB 197* (2001).

[Tie+15] Tyge Tiessen et al. “Security of the AES with a Secret S-Box”. en. In: *Fast Software Encryption*. Ed. by Gregor Leander. Vol. 9054. Lecture Notes in Computer Science. Berlin, Heidelberg: Springer Berlin Heidelberg, 2015, pp. 175–189. ISBN: 978-3-662-48115-8. DOI: 10.1007/978-3-662-48116-5_9. URL: http://link.springer.com/10.1007/978-3-662-48116-5_9.