

# Jean-Sébastien Coron

## Curriculum Vitae

10, rue Jean Engling, L-1466 Luxembourg, Luxembourg.

Phone: +352 26 43 10 87

Email: [coron@clipper.ens.fr](mailto:coron@clipper.ens.fr)

Web page: <http://www.eleves.ens.fr/home/coron/>

29 years old, French, married.

## Employment history

- Since October 2004, Assistant-Professor of Computer Science at University of Luxembourg, Luxembourg.

- 1998-2004, Research Scientist at Gemplus Card International, in the Information Security Group managed by Dr. D. Naccache. My main research areas were:

- *Cryptography* : analysis, optimization and implementation of cryptographic algorithms. Cryptanalysis of existing cryptographic algorithms. Design of new encryption algorithms and signature schemes with provable security.

- *Tamper resistance* : analysis of physical attacks against smart-cards, such as power attacks (DPA), electromagnetic attacks and fault attacks. Design of countermeasures against physical attacks.

- *Security protocols* : construction and evaluation of secure protocols around smart-cards. Security reviews.

## Education

- Ph.D. in Computer Science and Cryptography, Ecole Polytechnique, Paris, France, 2001. Title: *Cryptanalysis and security proofs for public-key schemes*. Areas of study: public-key encryption and signature, number theory, cryptanalysis and security proofs. Thesis supervisor: Prof. J. Stern. Jury: M. Bellare, M. Girault, D. Naccache, R. Rivest, A. Shamir, J. Stern, J.M. Steyaert and S. Vaudenay.

- Master in Computer Science, Ecole Normale Supérieure de Paris, 1998. Thesis title: Pseudo-random number generators and their security. Thesis supervisor: Prof. J. Stern.

- Student at the Ecole Normale Supérieure de Paris, France. Courses: Mathematics, Physics and Computer Science, 1995-1998.

- Scientific preparatory school, 1993-1995.

- Bachelor of Science, Mathematics, Physics, Computer Science, 1993.

## Research Summary

My research in information security has been concentrated in three areas: cryptanalysis of public-key schemes, security proofs for public-key schemes, and side-channel attacks.

For the cryptanalysis area, I have studied the security of encryption schemes and signature schemes based on the RSA algorithm, which are commonly used in real-world applications. My most significant contribution has been the cryptanalysis of the signature standards ISO 9796-1 and ISO 9796-2.

For the security proofs area, my most significant contribution is the first security proof for the signature standards ISO 9796-2 and PKCS#1 v1.5. I have also exhibited a message encoding scheme for RSA which can be used indifferently for encryption and signature, thereby simplifying the design of Public-Key Infrastructures.

For the side-channel area, I have studied how information leaks when a physical device (e.g., a smart card) performs cryptographic operations. I exhibited practical attacks based on measuring power-consumption. I designed countermeasures which have been patented and implemented in Gemplus smart-cards.

## Research Articles

These are my research articles which have appeared in conferences with program committee. These articles have all been published by Springer Verlag in the Lecture Notes in Computer Science volumes. They are available on my web page <http://www.eleves.ens.fr/home/coron/>.

1. J.S. Coron, D. Naccache and J.P. Stern. On the security of RSA padding. In *Advances in Cryptology - CRYPTO '99*, volume 1666, pages 1–18. Springer-Verlag, 1999. Lecture Notes in Computer Science.
2. J.S. Coron, H. Handschuh and D. Naccache. ECC: do we need to count ? In *Advances in Cryptology - ASIACRYPT '99*, volume 1716, pages 122–134. Springer-Verlag, 1999. Lecture Notes in Computer Science.
3. J.S. Coron, M. Joye, D. Naccache and P. Paillier. New attacks on PKCS#1 v1.5 encryption. In B. Preneel, editeur, *Proceedings of EUROCRYPT 2000*, volume 1807, pages 369–381. Springer Verlag, 2000. Lecture Notes in Computer Science.
4. J.S. Coron and D. Naccache. Security analysis of the Gennaro-Halevi-Rabin signature scheme. In B. Preneel, editeur, *Proceedings of EUROCRYPT 2000*, volume 1807, pages 91–101. Springer Verlag, 2000. Lecture Notes in Computer Science.
5. J.S. Coron. On the exact security of full domain hash. In M. Bellare, editeur, *Proceedings of CRYPTO 2000*, volume 1880, pages 229–235. Springer Verlag, 2000. Lecture Notes in Computer Science.
6. J.S. Coron, F. Koeune and D. Naccache. From fixed-length to arbitrary-length padding schemes. In *Advances in Cryptology - ASIACRYPT 2000*, volume 1976, pages 90–96. Springer-Verlag, 2000. Lecture Notes in Computer Science.
7. J.S. Coron, E. Brier, C. Clavier, and D. Naccache. Cryptanalysis of RSA signatures with fixed-pattern padding. In *CRYPTO 2001*. Springer-Verlag, 2001. Lecture Notes in Computer Science.
8. J.S. Coron. Optimal Security Proofs for PSS and Other Signature Schemes. In *EUROCRYPT 2002*. Springer-Verlag, 2002. Lecture Notes in Computer Science.

9. J.S. Coron. Security Proof for Partial-Domain Hash Signature Schemes. In *CRYPTO 2002*. Springer-Verlag, 2002. Lecture Notes in Computer Science.
10. J.S. Coron, M. Joye, D. Naccache, P. Paillier. Universal Padding Schemes for RSA. In *CRYPTO 2002*. Springer-Verlag, 2002. Lecture Notes in Computer Science.
11. J.S. Coron, D. Naccache. Boneh et al's  $k$ -Element Aggregate Extraction Assumption Is Equivalent to The Diffie-Hellman Assumption. In *ASIACRYPT 2003*. Springer-Verlag, 2003. Lecture Notes in Computer Science.
12. J.S. Coron. On finding small roots of bivariate polynomial equations revisited. In *EUROCRYPT 2004*. Springer-Verlag, 2004. Lecture Notes in Computer Science.
13. J.S. Coron and D. Naccache. An accurate evaluation of maurer's universal test. In *Selected Areas in Cryptography, SAC '98*, volume 1556, pages 57–71. Springer-Verlag, 1998. Lecture Notes in Computer Science.
14. J.S. Coron and D. Naccache. On the security of RSA screening. In *Proceedings of PKC '99*, volume 1560, pages 197–203. Springer-Verlag, 1999. Lecture Notes in Computer Science.
15. J.S. Coron. On the security of random sources. In *Proceedings of PKC '99*, volume 1560, pages 29–42. Springer-Verlag, 1999. Lecture Notes in Computer Science.
16. J.S. Coron. Resistance against differential power analysis for elliptic curve cryptosystems. In *Proceedings of CHES '99*, volume 1717, pages 292–302. Springer-Verlag, 1999. Lecture Notes in Computer Science.
17. C. Clavier, J.S. Coron and N. Dabbous. Differential power analysis in the presence of hardware countermeasures. In *CHES 2000*, volume 1965, pages 252–263. Springer-Verlag, 2000. Lecture Notes in Computer Science.
18. J.S. Coron and L. Goubin. On boolean and arithmetic masking against differential power analysis. In *CHES 2000*, volume 1965, pages 231–237. Springer-Verlag, 2000. Lecture Notes in Computer Science.
19. J.S. Coron, P. Kocher and D. Naccache. Statistics and secrand leakage. In *Financial Cryptography 2000*. Springer-Verlag, 2000. Lecture Notes in Computer Science.
20. J.S. Coron, D. M'Rahi and C. Tymen. Fast Generation of Pairs  $(k, [k]P)$  for Koblitz Elliptic Curves. In *SAC 2001*. Springer-Verlag, 2001. Lecture Notes in Computer Science.
21. J.S. Coron, H. Handschuh, M. Joye, P. Paillier, D. Pointcheval, C. Tymen. Optimal Chosen-Ciphertext Secure Encryption of Arbitrary-Length Messages. In *PKC 2002*. Springer-Verlag, 2002. Lecture Notes in Computer Science.
22. J.S. Coron, H. Handschuh, M. Joye, P. Paillier, D. Pointcheval, C. Tymen. GEM: A Generic Chosen-Ciphertext Secure Encryption Method. In *CT-RSA 2002*. Springer-Verlag, 2002. Lecture Notes in Computer Science.
23. J.S. Coron, A. Tchoulkine. A New Algorithm for Switching from Arithmetic to Boolean Masking In *CHES 2003*. Springer-Verlag, 2003. Lecture Notes in Computer Science.
24. J.S. Coron and D. Naccache. Cryptanalysis of a Zero-Knowledge Identification Protocol of Eurocrypt '95. In *CT-RSA 2004*. Springer-Verlag, 2004. Lecture Notes in Computer Science.
25. J.S. Coron. Cryptanalysis of a Public-key Encryption Scheme Based on the Polynomial Reconstruction Problem. In *PKC 2004*. Springer-Verlag, 2004. Lecture Notes in Computer Science.

This is the list of patents that I hold with Gemplus. Those patents can be divided in two areas: cryptography patents, and side-channel countermeasure patents.

Cryptography patents describe new cryptographic primitives or improve existing ones:

1. J.S. Coron, D. Naccache, J. Stern, "Signature schemes based on discrete logarithm with partial or total message recovery". Patent Number: FR2797127. Publication date: 2001-02-02. International Publication Number: WO0110078.
2. J.S. Coron, C. Tymen, "Cryptography method on elliptic curves", Patent Number: FR2807898. Publication date: 2001-10-19. International Publication Number: WO0180481.
3. J.S. Coron, D. Naccache, "Method for encoding long messages for RSA electronic signature schemes", Patent Number: FR2814619. Publication date: 2002-03-29. International Publication Number: WO0228010.
4. J.S. Coron, M. Joye and P. Paillier, "Method for enhancing security of public key encryption scheme". Patent Number: FR2818471. Publication date: 2002-06-21. International Publication Number: WO0251065
5. J.S. Coron, "Method for determining the size of a random variable for an electronic signature scheme". Patent Number: FR2828353. Publication date: 2003-02-07. International Publication Number: WO03013053.
6. J.S. Coron, D. Naccache, "Method for accelerated transmission of electronic signature". Patent Number: US2002188850. Publication date: 2002-12-12. International Publication Number: WO0228011.

Side-channel countermeasure patents describe countermeasures against side-channel attacks for smart-cards. This includes countermeasures for secret-key cryptosystems such as DES and AES, and public-key cryptosystems such as RSA and ECC.

1. J.S. Coron, C. Clavier, "Countermeasure method in an electronic component using a secret key cryptographic algorithm". Patent Number: EP1125394. Publication date: 2000-05-05. International Publication Number: WO0027068.
2. J.S. Coron, O. Benoit, N. Feyt, D. Naccache, "Method for countermeasure in an electronic component using a secret key algorithm". Patent Number: EP1198921; Publication date: 2000-08-18. International Publication Number: WO0049765.
3. J.S. Coron, "Countermeasure method in an electric component implementing an elliptical curve type public key cryptography algorithm". Patent Number: FR2791496. Publication date: 2000-09-29. International Publication Number: WO0059157.
4. J.S. Coron, "Countermeasure procedures in an electronic component implementing an elliptical curve type public key encryption algorithm". Patent Number: FR2791497. Publication date: 2000-09-29. International Publication Number: WO0059156.
5. J.S. Coron, D. Naccache, "Method for improving a random number generator to make it more resistant against attacks by current measuring". Patent Number: FR2796477. Publication date: 2001-01-19. International Publication Number: WO0106350.
6. J.S. Coron, P. Paillier, "Countermeasure method in an electronic component which uses an RSA-type public key cryptographic algorithm". Patent Number: FR2799851. Publication date: 2001-04-20. International Publication Number: WO0128153.
7. J.S. Coron, "countermeasure methods in an electronic component using a Koblitz elliptic curve public key cryptographic algorithm", Patent Number: FR2810821. Publication date: 2001-12-28. International Publication Number: WO0201343.

8. J.S. Coron, “Counter-measure method in an electronic component using a secret key encryption algorithm” Patent Number: FR2818472. Publication date: 2002-06-21. International Publication Number: WO0251064.
9. J.S. Coron, “Countermeasure methods in an electronic component using an rsa-type public key encryption algorithm”, Patent Number: FR2818473. Publication date: 2002-06-21. International Publication Number: WO0250658.
10. J.S. Coron, M. Joye and P. Paillier, “Execution of cryptographic algorithms based on the Chinese Remainder theorem, CRT, for use with chip cards, etc., which by changing the order of calculation runs faster than existing CRT algorithms” Patent Number: FR2819663. Publication date: 2002-07-19. International Publication Number: WO02058321.

### Publication summary

Publication:	Number
Top cryptography conferences (Eurocrypt, Crypto, Asiacrypt)	12
Other cryptography conferences	13
Patents	16

### Invited lectures and invited participation at workshops

*Cryptanalysis of ISO 9796-1 and ISO 9796-2 standards*, Royal Holloway, University of London. Cryptography seminar, March 1999.

*Optimal security proofs for signature schemes*, Monte Verita Workshop, Switzerland, March 2001.

*Optimal security proofs for PSS*, Ecole Normale Supérieure de Paris, Cryptography seminar, April 2002.

*Equivalence between the random oracle model and the random cipher model*, Dagstuhl Workshop, Germany, September 2002.

*Cryptanalysis of Augot and Finiasz Cryptosystem of Eurocrypt 2003*, Ecole Normale Supérieure de Paris, Cryptography seminar, March 2003.

*How to use RSA in practice ?*, Quo vadis cryptology international workshop, Warsaw, Poland, May 2003.

*Finding small roots of bivariate integer polynomial equations revisited*, Royal Holloway, University of London. Cryptography seminar, April 2004.

## Academic Services

Program Committee member of the following conferences: CHES 2001, 2002 and 2003, CRYPTO 2003, EUROCRYPT 2004, CRYPTO 2005, CT-RSA 2005.

## Teaching experience

- *Introduction to programming languages*, University of Luxembourg, fall 2004.
- *Introduction to operating systems*, University of Luxembourg, fall 2004.
- *Introduction to cryptography*, University of Luxembourg, fall 2004.