ENS - Département d'Informatique
45, rue d'Ulm
75005 Paris – France
☎ *+33.1.44.32.20.48*
✉ *Pierre-Alain.Fouque@ens.fr*
French citizenship, born 25 march 1974,
2 children (5 and 8 years)
`http://www.di.ens.fr/~fouque`

Pierre-Alain Fouque

Research areas

Cryptanalysis in symmetric-key cryptography

Cryptanalysis in public-key cryptography

Cryptanalysis with side-channels

Provable security

Work Experience

Since 2003 **Assistant Professor in Computer Science**, *École normale supérieure (ÉNS)*, Paris, (Délégation at INRIA Rennes – Celtique Team – in 2011/12).
Qualification Professeur since January 2011.

Since 2006 **Member of the Educational Committee of the Master MPRI**, *ENS Manager*.

Since 2006 **Member of the recruitment committee of the CS Department at ENS**.

2001 - 2003 **Cryptographic Researcher**, *PostDoc in the Cryptographic Lab of the DCSSI*, Paris, French Administration in charge of evaluating security products.

Education

Dec. 2010 **Habilitation Thesis**, *About Some Algebraic and Statistical Cryptanalysis*, Supervisor: Jacques Stern, École normale supérieure.

Oct. 2001 **PhD Thesis**, *Thresold Cryptography: Theory and Practice*, Supervisor: Jacques Stern, Université de Paris 7. Work done at École normale supérieure.

Sept.1999 **Master Degree**, *with Honors*, Université de Paris 7.

Teaching

Algorithms. Éns. Level L3, undergraduate, each year since 2003. 24h

C Programing. Éns and Énsta. Level L3, undergraduate, each year since 1999. 24h

Formal Languages and Automata. Éns. Level L3, undergraduate, each year since 2003. 12h

Calculability and Complexity. Éns. Level L3, undergraduate, each year since 2003. 12h

Introduction to Cryptography. Éns. MPRI. Master Level M1, 2005,2006,2007. 16h

Cryptanalysis. Éns. MPRI. Master Level M2, 2008, 2009,2010,2011. 12h

Professional Activities

Program Committees

Member of the PC of Crypto 2012.
Member of the PC of CT-RSA 2012.
Member of the PC of SCN 2012.
Member of the PC of FSE 2011.
Member of the PC of Eurocrypt 2009 and 2012.
Member of the PC of CHES 2006, 2007, 2009, 2010 and 2011.
Member of the PC of SAC 2011.
Member of the PC of PKC 2006 and 2009.

Editor

Member of the Editorial Board of the International Journal of Applied Cryptography (IJACT).

Invited Presentations

Haifa 2011 Theoretical Seminar in Computer Science – October 2011.
Weizmann 2011 Theoretical Seminar in Computer Science – November 2011.
Workshop Hash Function August 2010 at Santa Barbara (U.S.).
SuRI EPFL 2010 – June 2010.
ESC 2010 – January 2010.
Workshop Hash Function February 2008 at Leuven (Belgique).
ECRYPT Final Meeting – Mai 2008 at Anvers (Belgique).
Workshop Japanese-French from 13 to 14 May 2008 at LORIA Nancy.
Seminar University of Caen in May 2008.
Seminar at Uuniversity of Rennes in January 2008.
Workshop Hash Function April 2007 at Barcelone (Espagne).
Workshop WOTE August 2003 at San Francisco (U.S.).

Visits

Haifa-Weizmann 2011 – November 2011.
EPFL 2010 – June 2010.

Organisation of conferences

Conference PKC 2010 at ÉNS from 26 to 28 may 2010.
ECRYPT retreat on hash functions at ÉNS from 20 to 22 April 2010.
Conference ACNS 2009 at INRIA Rocquencourt from 2 to 5 June 2009.

PhD Defense Member

Sébastien Zimmer. *Key Generation and Authentication.* École polytechnique. Supervisor: David Pointcheval. September 2008.

Éric Leviel. *Contributions to the analysis of symmetric-key schemes and protocols.* Université Paris 7. Supervisor: Jacques Stern. September 2008.

Thomas Peyrin. *Analysis of Cryptographic Hash Functions.* Université de Versailles Saint-Quentin-en-Yvelines. Supervisor: Antoine Joux. November 2008.

Yannick Seurin. *Provably Secure Building Blocks and Cryptographic Protocols.* Université Versailles Saint-Quentin-en-Yvelines. Supervisor: Jacques Patarin. July 2009.

Maria Naya-Plascencia. *Stream Cipher and Hash Function: design and analysis.* Université Pierre et Marie Curie. Supervisor: Anne Canteaut. November 2009.

Joana Treger. *Analysis of the Security of Block Cipher and Multivariate Cryptography.* Université of Versailles Saint-Quentin-en-Yvelines. Supervisor: Jacques Patarin. June 2010.

Gilles Macario-Rat. *Cryptanalysis of Multivariate Schemes and the Related Isomorphism Polynomial Problem.* Supervisor: Jacques Stern. June 2010.

Gaëtan Leurent. *Design and Analysis of Hash Functions.* Université Paris 7. Supervisor: David Pointcheval. September 2010.

Stéphane Manuel. *Analysis of hash function.* École polytechnique. Supervisor: Daniel Augot and Nicolas Sendrier. November 2010. Rapporteur.

Mehdi Tibouchi. *Hachage vers les courbes elliptiques et cryptanalyse de schémas RSA.* Université Paris 7. Supervisor: Jean-Sébastien Coron and David Naccache. September 2011.

Charles Bouillaguet. *Étude d'hypothèses algorithmiques et attaques de primitives cryptographiques.* Université Paris 7. Supervisor: David Pointcheval and Pierre-Alain Fouque. September 2011.

Luk Bettale. *Cryptanalyse algébrique : outils et applications.* Université Pierre et Marie Curie. Supervisor: Ludovic Perret and Jean-Charles Faugère. October 2011. Rapporteur.

Jean Martinelli. *Protection d'algorithmes de chiffrement par blocs contre les attaques par canaux auxiliaires d'ordre supérieur.* Université Versailles - Saint-Quentin. Supervisor: Louis Goubin. December 2011. Rapporteur.

Olivier Meynard. *Caractérisation et utilisation du rayonnement électromagnétique pour l'attaque de composants cryptographiques.* Télécom ParisTech. Supervisor: Jean-Luc Danger, Sylvain Guilley and Denis Réal. January 2012. Rapporteur.

Sylvain Heraud. *Vérification semi-automatique de primitives cryptographiques.* Université Nice - Sophia-Antipolis. Supervisor: Benjamin Grégoire. February 2012. Rapporteur.

Grants

Saphir2 Manager of the ANR project Saphir 2 since March 2009 "Sécurité et Analyse des Primitives de Hachage Innovantes et Récentes", for the Computer Science Department of the École normale supérieure. Length: 48 months. This project aims at studying attacks on hash functions and the design of these functions. It is also involved in supporting some SHA-3 candidates, like the SIMD hash functions (proposed by the ENS).

CELAR Project — How to build a hash function.

ECRYPT I and II — Participation to the european projects ECRYPT I and II. Organisation of the hash retreat.

Saphir1 — Manager of the ANR project Saphir 1 (March 2006 to March 2009) "Sécurité et Analyse des Primitives de Hachage Innovantes et Récentes", for the Computer Science Departement of the École normale supérieure. Length: 36 months. This project aims at studying hash functions. It allows us to build a hash function called SIMD that have been selected for the second round of the SHA-3 competition amongst 14 out of 51 initially proposed.

Crypto++ — Manager of the RNRT project (October 2003 to December 2006) The aim of this project was to study multi-agent protocols such as voting scheme and electronic payment.

Students

Past PhD Students

S. Zimmer — Key Generation and Authentication (Start september 2005 - Defense september 2008). With David Pointcheval (50%). Actually Defense Ministry in France.

G. Macario-Rat — Cryptanalysis of Multivariate Scheme (Start september 2006 - Defense 28 Juin 2010). PhD done in Orange Labs. With Jacques Stern (50%)

G. Leurent — Design and Analysis of Hash Functions (Start september 2007 - Defense 30 september 2010). PostDoc at Luxembourg with Alex Biruykov.

C. Bouillaguet — Multivariate Scheme, Hash Function and AES (Start september 2008 - september 2011). PostDoc at UVSQ with Antoine Joux.

Current PhD Students

D. Leresteux — Attaques par canaux auxiliaires (Start september 2008 - Expected Defense July 2012). PhD done in the Defense Ministry Labs (DGA).

J. Jean — Analysis of Hash Functions (Start october 2010 - Expected Defense september 2013).

P. Derbez — Automatic tools for AES (Start september 2010 - Expected Defense september 2013).

J.C. Zapalowicz — Side-Channel Attacks (Start december 2011 - Expected Defense december 2014).

Master Students

G. Leurent — Automatic Search of Differential Path on the MD4 hash function (2006).

A. Bernard — Analysis of algebraic hash functions (2006).

C. Bouillaguet — Analysis of Rivest mode of operation for hash functions (2007).

T. Chardin — Cache Attacks on RC4 (2007).

J.-G. Kammerer — Building block cipher of small size from a larger one (2008).

P. Derbez — Low Data Complexity Attacks on Round-Reduced Version of AES (2010).

J. Jean — Rebound Attacks on hash functions (2010).

Publications

More 50 publications in international conferences and 6 articles in journal.
Among the 50 most prolific cryptographers according to the IACR DB.

Venue	Number
1st class cryptographic conferences: Crypto, Eurocrypt, Asiacrypt	14
2nd class cryptographic conferences: FSE, FC, SAC, PKC, CT-RSA, CHES	30
Other cryptographic conferences: Pairing, SCN, FDTC, ...	6
Other conferences: ICALP, PODC ASIACCS	3

Books

PCS11 *Sommes-nous prisonniers des codes secrets ?*, with C. Bouillaguet, Éditions Le Pommier, Scientific Review for general public. ISBN:978-2-7465-0539-1.

ACNS09 *Applied Cryptography and Network Security, 7th International Conference, ACNS'09*, Paris-Rocquencourt, France, Juin 2-5, 2009, Proceedings. Springer-Verlag, LNCS 5536. ISBN:978-3-642-01956-2.

Articles in international journals

J. Math. Crypto *A Family of Weak Keys in HFE (and the Corresponding Practical Key-Recovery)*, with C. Bouillaguet, A. Joux and J. Treger. Accepted to *Journal of Mathematical Cryptology* in 2011.

IEEETIT *Low Data Complexity Attacks on AES*, with C. Bouillaguet, O. Dunkelman, P. Derbez, N. Keller and V. Rijmen. Accepted to *IEEE Transactions on Information Theory* in 2011.

MathComp *Indifferentiable Deterministic Hashing to Elliptic and Hyperelliptic Curves*, with R. R. Farashahi, I. Shparlinski, M. Tibouchi and F. Voloch, Accepted to *Journal of Math. Comp.* in 2011.

IEE *Password-Based Authenticated Key Exchange In The Three-Party Setting*, with M. Abdalla and D. Pointcheval. *IEE Proceedings Information Security*, 153(1):27–39, 2006.

IPL *Practical Hash Functions Constructions Resistant to Generic Second Preimage Attacks Beyond the Birthday Bound*, with C. Bouillaguet. Submitted to *Information Processing Letters (IPL)* in 2011.

JoC *New Second Preimage Attacks on Hash Function*, with E. Andreeva, C. Bouillaguet, O. Dunkelman, J.J. Hoch, J. Kelsey, A. Shamir and S. Zimmer. Submitted to*Journal of Cryptology* in 2011.

Articles in international conferences

Eurocrypt '12 *Tight Security Reductions for Lattice and Short Discrete Logarithm Signature Schemes*, with M. Abdalla, V. Lyubashevsky and M. Tibouchi. In *Eurocrypt '12*, volume of *Lecture Notes in Computer Science*, pages –. Springer-Verlag, Berlin, 2012.

SAComp '12 *Fault Attacks like Buffer Overflow*, with D. Leresteux and F. Valette. In *Symposium on Applied Computing '12*, volume of *Lecture Notes in Computer Science*, pages –. Springer-Verlag, Berlin, 2012.

Asiacrypt '11 *Practical Key-Recovery for All Possible Parameters of SFLASH*, with C. Bouillaguet and G.Macario-Rat. In *Asiacrypt '11*, volume 7073 of *Lecture Notes in Computer Science*, pages 667–685. Springer-Verlag, Berlin, 2011.

CHES '11 *Meet-in-the-Middle and Impossible Differential Fault Analysis on AES*, with P. Derbez and D. Leresteux. In *CHES '11*, volume 6917 of *Lecture Notes in Computer Science*, pages 274–291. Springer-Verlag, Berlin, 2011.

Crypto '11 *Automatic Search of Attacks on Round-Reduced AES and Applications*, with C. Bouillaguet and P. Derbez. In *CRYPTO '11*, volume 6841 of *Lecture Notes in Computer Science*, pages 169–187. Springer-Verlag, Berlin, 2011.

SAC '11 *Attacks on Hash Functions Based on Generalized Feistel: Application to Reduced-Round Lesamnta and SHAvite-3$_{512}$*, with C. Bouillaguet, O. Dunkelman and G. Leurent. In *SAC '11*, volume of *Lecture Notes in Computer Science*, pages –. Springer-Verlag, Berlin, 2011.

ACNS '11 *Cache Timing Analysis of RC4*, with T. Chardin and D. Leresteux. In *ACNS '11*, volume 6715 of *Lecture Notes in Computer Science*, pages 110–129. Springer-Verlag, Berlin, 2011.

PKC '11 *Practical Cryptanalysis of the Identification Scheme Based on the Isomorphism of Polynomial With One Secret Problem*, with C. Bouillaguet, J.C. Faugère and L. Perret. In *PKC '11*, volume 6571 of *Lecture Notes in Computer Science*, pages 473–493. Springer-Verlag, Berlin, 2011.

FSE '11 *Practical Near-Collisions and Collisions on Round-Reduced ECHO-256 Compression Function*, with J. Jean. In *FSE '11*, volume 6733 of *Lecture Notes in Computer Science*, pages –. Springer-Verlag, Berlin, 2011.

Pairing '10 *Deterministic encoding and hashing to odd hyperelliptic curves*, with M. Tibouchi. In *PAIRING '10*, volume of *Lecture Notes in Computer Science*, pages –. Springer-Verlag, Berlin, 2010.

Latincrypt '10 *Estimating the Size of the Image of Deterministic Hash Functions to Elliptic Curves*, with M. Tibouchi. In *LATINCRYPT '10*, volume of *Lecture Notes in Computer Science*, pages –. Springer-Verlag, Berlin, 2010.

SCC '10 *A Family of Weak Keys in HFE (and the Corresponding Practical Key-Recovery)*, with C. Bouillaguet, A. Joux and J. Treger. In *SCC'10*.

SAC '10 *Security of SIMD*, with C. Bouillaguet and G. Leurent. In *Selected Areas in Cryptography '10*, volume of 6544 *Lecture Notes in Computer Science*, pages 351–368. Springer-Verlag, Berlin, 2010.

SAC '10 *Attacks on Hash Functions based on Generalized Feistel - Application to Reduced-Round Lesamnta and SHAvite-3*, and C. Bouillaguet, O. Dunkelman et G. Leurent. In *Selected Areas in Cryptography '10*, volume 6544 of *Lecture Notes in Computer Science*, pages 18–35. Springer-Verlag, Berlin, 2010.

FSE '10 *Another Look at the Complementation Property*, with C. Bouillaguet, O. Dunkelman and G. Leurent. In *FSE '10*, volume of *Lecture Notes in Computer Science*, pages –. Springer-Verlag, Berlin, 2010.

CHES '09 *Practical Electromagnetic Template Attack on HMAC*, with G. Leurent, D. Réal and F. Valette. In *CHES '09*, volume 5747 of *Lecture Notes in Computer Science*, pages 66–80. Springer-Verlag, Berlin, 2009.

FDTC '09 *Fault Attack on Schnorr-based Identification and Signature Schemes*, with D. Masgana and V. Valette. In *FTDC '09*, pages 32–38. IEEE-CS Press, 2009.

Eurocrypt '09 *Optimal Randomness Extraction from a Diffie-Hellman Element*, with C. Chevalier, D. Pointcheval and S. Zimmer. In *Eurocrypt '09*, volume 5479 of *Lecture Notes in Computer Science*, pages 411–428. Springer-Verlag, Berlin, 2009.

CHES '08 *The Carry Leakage on the Randomized Exponent Countermeasure*, with D. Réal, F. Valette and M. Drissi. In *CHES '08*, volume 5154 of *Lecture Notes in Computer Science*, pages 198–213. Springer-Verlag, Berlin, 2008.

FDTC '08 *Fault Attack on Elliptic Curve with Montgomery Ladder Implementation*, with R. Lercier, D. Réal and V. Valette. In *FTDC '08*, pages –. IEEE-CS Press, 2008.

Eurocrypt '08 *Key Recovery on Hidden Monomial Multivariate Schemes*, with G. Macario-Rat and J. Stern. In *Advances in Cryptology – Proceedings of EUROCRYPT '08*, volume 4965 of *Lecture Notes in Computer Science*, pages 19–30. Springer-Verlag, Berlin, 2007.

Eurocrypt '08 *Second Preimage Attacks on Dithered Hash Functions*, avec E. Andreeva, C. Bouillaguet, J. J. Hoch, J. Kelsey, A. Shamir et S. Zimmer. Dans *Advances in Cryptology – Proceedings of EUROCRYPT '08*, volume 4965 of *Lecture Notes in Computer Science*, pages 270–288. Springer-Verlag, Berlin, 2008.

SAC '08 *Analysis of the Collision Resistance of Radiogatùn using Algebraic Technique*, avec C. Bouillaguet. Dans *Selected Areas in Cryptography '08*, volume 5381 of *Lecture Notes in Computer Science*, pages 245–261. Springer-Verlag, Berlin, 2008.

SAC '08 *Cryptanalysis of Tweaked Versions of SMASH and Reparation*, avec J. Stern et S. Zimmer. Dans *Selected Areas in Cryptography '08*, volume 5381 of *Lecture Notes in Computer Science*, pages 136–150. Springer-Verlag, Berlin, 2008.

AsiaCCS '08 *HMAC is a Randomness Extractor and Applications to TLS*, with D. Pointcheval, and S. Zimmer. In *AsiaCCS '08*, pages 1–17. ACM Press, 2008.

ACNS '08 *On the Security of the CCM Encryption Mode and of a Slight Variant*, with G. Martinet, F. Valette and S. Zimmer. In *ACNS '08*, volume 5037 of *Lecture Notes in Computer Science*, pages 411–428. Springer-Verlag, Berlin, 2008.

CT RSA '08 *Cryptanalysis of a Hash Function Based on Quasi-Cyclic Codes*, with G. Leurent. In *CT RSA '08*, volume of *Lecture Notes in Computer Science*, pages 1–17. Springer-Verlag, Berlin, 2008.

PKC '08 *Key Recovery on Hidden Monomial Multivariate Schemes*, with G. Macario-Rat, L. Perret and J. Stern. In *PKC '08*, volume 4939 of *Lecture Notes in Computer Science*, pages 1–17. Springer-Verlag, Berlin, 2008.

Crypto '07 *Full Key-Recovery Attacks on HMAC/NMAC-MD4 and NMAC-MD5*, with G. Leurent and P. Q. Nguyen. In *Advances in Cryptology – Proceedings of CRYPT0 '07*, volume 4965 of *Lecture Notes in Computer Science*, pages 13–30. Springer-Verlag, Berlin, 2007.

Crypto '07 *Practical Cryptanalysis of SFLASH*, with V. Dubois, A. Shamir and J. Stern. In *Advances in Cryptology – Proceedings of CRYPT0 '07*, volume 4622 of *Lecture Notes in Computer Science*, pages 1–12. Springer-Verlag, Berlin, 2007.

Eurocrypt '07 *Cryptanalysis of SFLASH with Slightly Modified Parameters*, with V. Dubois and J. Stern. In *Advances in Cryptology – Proceedings of EUROCRYPT '07*, volume of *Lecture Notes in Computer Science*, pages 264–275. Springer-Verlag, Berlin, 2007.

Inscrypt '07 *Cryptanalysis of the SFLASH Signature Scheme*, avec V. Dubois, A. Shamir et J. Stern. Dans *Inscrypt '07*, volume 4990 of *Lecture Notes in Computer Science*, pages 1–4. Springer-Verlag, Berlin, 2007.

ICALP '06 *Hardness of Distinguishing the MSB or LSB of Secrete Keys in Diffie-Hellman Schemes*, with D. Pointcheval, J. Stern and S. Zimmer. In *Proc. of the 33rd International Colloquium on Automata, Languages and Programming, Part II (ICALP '06)*, volume 4052 of *Lecture Notes in Computer Science*, pages 240–251. Springer-Verlag, Berlin, 2006.

SCN '06 *An Improved LPN Algorithm*, with E. Levieil. In *SCN '06*, volume 4116 of *Lecture Notes in Computer Science*, pages 348–359. Springer-Verlag, Berlin, 2006.

CHES '06 *Power Attack on Small RSA Public Exponent*, with S. Kunz-Jacques, G. Martinet, F. Muller and F. Valette. In *Cryptographic Hardware and Embedded Systems (CHES '06)*, volume 4249 of *Lecture Notes in Computer Science*, pages 339–353. Springer-Verlag, Berlin, 2006.

PKC '06 *The Twist-Augmented Technique for Key Exchange*, with O. Chevassut, P. Gaudry and D. Pointcheval. In *Conference on Practice and Theory in Public-Key Cryptography (PKC '06)*, volume 3958 of *Lecture Notes in Computer Science*, pages 410–426. Springer-Verlag, Berlin, 2006.

Eurocrypt '05 *Differential Cryptanalysis for Multivariate Schemes*, with L. Granboulan and J. Stern. In *Advances in Cryptology – Proceedings of EUROCRYPT '05*, volume 3494 of *Lecture Notes in Computer Science*, pages 341–353. Springer-Verlag, Berlin, 2005.

Asiacrypt '05 *A Simple Threshold Authenticated Key Exchange from Short Secrets*, with M. Abdalla, O. Chevassut and D. Pointcheval. In *Conference ASIACRYPT 2005*, volume 3788 of *Lecture Notes in Computer Science*, pages 566–584. Springer-Verlag, Berlin, 2005.

PKC '05 *Password-Based Authenticated Key Exchange in the Three-Party Setting*, with M. Abdalla and D. Pointcheval. In *Conference on Practice and Theory in Public-Key Cryptography (PKC '05)*, volume 3386 of *Lecture Notes in Computer Science*, pages 65–84. Springer-Verlag, Berlin, 2005.

SAC '04 *Blockwise Adversarial Model for On-line Ciphers and Symmetric Encryption Schemes*, with A. Joux and G. Poupard. In *Selected Areas in Cryptography '04*, volume 3357 of *Lecture Notes in Computer Science*, pages 212–226. Springer-Verlag, Berlin, 2004.

CHES '04 *Defeating Countermeasures Based on Randomized BSD Representations*, with F. Muller, G. Poupard and F. Valette. In *Cryptographic Hardware and Embedded Systems (CHES '04)*, volume 3156 of *Lecture Notes in Computer Science*, pages 312–327. Springer-Verlag, Berlin, 2004.

Asiacrypt '03 *The Insecurity of Esign in Practical Implementations*, with N. Howgrave-Graham, G. Martinet and G. Poupard. In *Conference ASIACRYPT 2003*, volume 2894 of *Lecture Notes in Computer Science*, pages 492–506. Springer-Verlag, Berlin, 2003.

CHES '03 *Attacking Unbalanced RSA-CRT Using SPA*, with G. Martinet and G. Poupard. In *Cryptographic Hardware and Embedded Systems (CHES '03)*, volume 2779 of *Lecture Notes in Computer Science*, pages 254–268. Springer-Verlag, Berlin, 2003.

CHES '03 *The Doubling Attack – Why Upwards is Better than Downwards*, with F. Valette. In *Cryptographic Hardware and Embedded Systems (CHES '03)*, volume 2779 of *Lecture Notes in Computer Science*, pages 269–280. Springer-Verlag, Berlin, 2003.

FSE '03 *Practical Symmetric On-Line Encryption*, with G. Martinet and G. Poupard. In *Advances in Cryptology – Proceedings of FSE '03*, volume 2887 of *Lecture Notes in Computer Science*, pages 362–375. Springer-Verlag, Berlin, 2003.

SAC '03 *Authenticated On-Line Encryption*, with A. Joux, G. Martinet and F. Valette. In *Selected Areas in Cryptography '03*, volume 3006 of *Lecture Notes in Computer Science*, pages 145–159. Springer-Verlag, Berlin, 2003.

Eurocrypt '03 *On the Security of RDSA*, with G. Poupard. In *Advances in Cryptology – Proceedings of EUROCRYPT '03*, volume 2656 of *Lecture Notes in Computer Science*, pages 462–476. Springer-Verlag, Berlin, 2003.

FC '02 *CryptoComputing with Rationals*, with J. Stern and J. G. Wackers. In *Financial Cryptography '02*, volume 2357 of *Lecture Notes in Computer Science*, pages 136–146. Springer-Verlag, Berlin, 2002.

Asiacrypt '01 *Fully Distributed Threshold RSA under Standard Assumptions*, with J. Stern. In *Conference ASIACRYPT '01*, volume 2248 of *Lecture Notes in Computer Science*, pages 310–330. Springer-Verlag, Berlin, 2001.

Asiacrypt '01 *Threshold Cryptosystems Secure against Chosen-Ciphertext Attacks*, with D. Pointcheval. In *Conference ASIACRYPT '01*, volume 2248 of *Lecture Notes in Computer Science*, pages 351–368. Springer-Verlag, Berlin, 2001.

PODC '01 *Practical multi-candidate election system*, avec O. Baudron, D. Pointcheval, G. Poupard and J. Stern. In *ACM Symposium on Principles of Distributed Computing PODC '01*, pages 274–283. ACM, 2001.

PKC '01 *One Round Threshold Discrete-Log Key Generation without Private Channels*, with J. Stern. In *Conference on Practice and Theory in Public-Key Cryptography (PKC '01)*, volume 1992 of *Lecture Notes in Computer Science*, pages 300–316. Springer-Verlag, Berlin, 2001.

FC '00 *Sharing Decryption in the Context of Voting or Lotteries*, avec G. Poupard and J. Stern. In *Financial Cryptography '00*, volume 1962 of *Lecture Notes in Computer Science*, pages 90–104. Springer-Verlag, Berlin, 2000.

Preprints

- *Close to Uniform Prime Number Generation with Fewer Random Bits*, with M. Tibouchi.
- *Chosen-Key Attacks on AES*, with P.Derbez and J. Jean.
- *Meet-in-the-middle attack on reduced versions of the Camellia block cipher*, with J. Lu, Y. Wei and E. Pasalic.
- *Probabilistic Algorithms for the Equivalence of Quadratic Maps*, with C. Bouillaguet and A.Véber.
- *Injective Encodings to Elliptic Curves*, with A. Joux and M. Tibouchi.
- *Attacking RSA-CRT Signatures with Faults on Montgomery Multiplication*, with N. Guillermin, D. Leresteux, M. Tibouchi and J.C. Zapalowicz.
- *Generic Indifferentiability Proofs of Hash Designs*, with M. Daubignard and Y. Lakhnech.
- *A Generic Differential Characteristic Search Algorithm to Evaluate the Security of SPN Ciphers*, with J. Jean and T. Peyrin.