Rennes University
263, avenue du Général Leclerc
35042 Rennes Cedex – France
☎ *+33.2.99.84.75.58*
✉ *Pierre-Alain.Fouque@ens.fr*
French citizenship, born 25 march 1974,
2 children (17 and 20 years)
http://www.di.ens.fr/~fouque

Pierre-Alain Fouque

Research areas

Post-Quantum Cryptography based on Lattices
Cryptanalysis in Symmetric Key Cryptography
Security of Cryptographic Implementations
Security Proof in Real-World Applications

The Post-Quantum Signature Scheme Falcon has been selected to be standardized by NIST

Work Experience

Since 2012 **Professor**, *Rennes University*, Responsible for the Master Cybersecurity.

Since 2021 **PI of PQ-TLS: Post-Quantum Cryptography project of the Quantum PEPR**, *13 research teams in cybersecurity*, 8.5 Meuros.

Since 2021 **Leader of the CAPSULE Team (IRISA / Inria)**, *Embedded Security and Cryptography*, 5 permanents researchers and 8 PhD Students, `https://www.irisa.fr/capsule/`.

Since 2020 **Leader of the EUR Cyberschool**, *Master in Cybersecurity*, 10 partners: INSA Rennes, Centrale-Supélec, IMTA, UR1, UR2, ENS Rennes, ENSAI, Science Po Rennes, Inria, CNRS, 5.75 Meuros, `https://cyberschool.univ-rennes.fr/en/`.

2015-20 **co-Leader of the EMSEC Team (IRISA – UMR 6074)**, *Embedded Security and Cryptography*, 8 permanents researchers and 8 PhD Students, `http://www.irisa.fr/emsec/`.

2013-2018 **Junior Member**, *Institut Universitaire de France*.

2011-2012 **Researcher**, *Inria*, Celtique Team, Security of cryptographic implementation using formal method.

2003-2012 **Assistant Professor in Computer Science**, *École normale supérieure (ÉNS)*, Paris, Member of the Educational Committee of the Master MPRI for ENS students.

2001 - 2003 **Cryptographic Researcher**, *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**, *Threshold Cryptography: Theory and Practice*, Supervisor: Jacques Stern, Université de Paris 7. Work done at École normale supérieure.

Sept.1998 **Master Degree**, *with Honors*, Université de Paris 7.
Dec. 1998 **Engineer Diploma**, *Télécom Paris*.

Professional Activities

Program Committees

Program Chair of CHES 2019.
Member of the PC of ATC USENIX 2018.
Member of the PC of ACM CCS 2015.
Member of the PC of Crypto 2012, Crypto 2014, Crypto 2016.
Member of the PC of Eurocrypt 2009, 2012 and 2014.
Member of the PC of CHES 2006, 2007, 2009, 2010, 2011, 2013, 2014, 2015, ...
Member of the PC of PKC 2006, 2009, 2013, 2016, 2017, 2018, and 2022.
Member of the PC of FSE 2011, 2018, 2020.
Member of the PC of CT-RSA 2012 and 2013.
Member of the PC of SCN 2012.

Invited Presentations

Workshop Japanese-French from April 2020 at Kyoto.
Presentation at NTT, Japan, April 2018.
Presentation at ENS, Paris, April 2017.
Workshop Japanese-French from April 2015 at Tokyo.
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 University of Rennes in January 2008.
Workshop Hash Function April 2007 at Barcelone (Espagne).
Workshop WOTE August 2003 at San Francisco (U.S.).

Visits

Simons Institute, USA – January / March 2020.
NTT, Japan – January / May 2018 .
IMDEA, Spain – April 2014.
Haifa-Weizmann Institute, Israël – October–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.

Grants

Prometheus	Participant to this European Project 2019–2022 "Security of post-quantum cryptography and anonymity property.
MobiS5	ANR Project since October 2019 to 2023 "Security of 5G communication". Length: 48 months.
SafeTLS	PI of the ANR Project SafeTLS since october 2016 to 2020 "Security of TLS 1.3". Length: 48 months.
Brutus	PI of the ANR Project Brutus since october 2014 to 2018 "Security of authenticated encryption". Length: 48 months.
Saphir2	Manager of the ANR project Saphir 2 for ENS since March 2009 to 2013 "Sécurité et Analyse des Primitives de Hachage Innovantes et Récentes". 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

25+ students have defensed their PhD. Currently I supervise 4 PhD.

Past PhD Students

S. Zimmer	Key Generation and Authentication (Sept. 2005 - Defense Sept. 2008). With David Pointcheval (50%). Actually Defense Ministry in France.
G. Macario-Rat	Cryptanalysis of Multivariate Scheme (Sept. 2006 - Defense June 2010). PhD done in Orange Labs. With Jacques Stern (50%)
G. Leurent	Design and Analysis of Hash Functions (Sept. 2007 - Defense Sept. 2010). Postdoc in Luxembourg with Alex Biryukov and in UCL with François-Xavier Standaert. Junior Researcher at Inria.
C. Bouillaguet	Multivariate Scheme, Hash Function and AES (Sept. 2008 - Defense Sept. 2011). Postdoc in Lille with Louis Goubin. Assistant Professor at Lille.
D. Leresteux	Attaques par canaux auxiliaires (Sept. 2008 - Defense July 2012). PhD done in the Defense Ministry Labs (DGA).
J. Jean	Analysis of Hash Functions (Oct. 2010 - Defense Sept. 2013). Postdoc in Singapore with Thomas Peyrin. ANSSI.
P. Derbez	Automatic tools for AES (Sept. 2010 - Defense Dec. 2013). Postdoc in Luxembourg with Alex Biryukov. Assistant Professor at Rennes.
J.C. Zapalowicz	Side-Channel Attacks (Dec. 2011 - Defense Nov. 2014). Thalès.
S. Belaid	Side-Channel Masking (Sept. 2012 - Defense Oct. 2015). CryptoExperts. **Prix de Trophée des ingénieurs du futur** pour sa thèse effectuée entre l'ENS et Thalès.
P. Belgarric	Smartphone Security (Dec. 2014 - Defense July 2017). HP Labs Bristol.
P. Lestringant	Automatic Analysis of Binary Code (Sept. 2013 - Defense Sept. 2016). Cifre Amossys. ANSSI.
B. Richard	Security Proof of Authenticated Key Exchange (Dec. 2013 - Defense December. 2017). CapGemini Bordeaux.
P. Karpman	Analysis of Hash Functions (Oct. 2013 - Defense Nov. 2016). Postdoc in CWI with Marc Stevens. Assistant Professor at Grenoble University.
B. Minaud	Cryptanalysis of Block Ciphers (Sept. 2014 - Defense oct. 2016). PostDoc RHUL with K. Paterson and now Inria Junior Researcher at ENS.
R. Bost	Symmetric Searchable Encryption (Start Sept. 2014 - Defense January. 2018). **Best thesis Award by the GDR Security 2018** DGA.
C. Delaplace	Lattice-Based Cryptography (Start Sept. 2015 - Defense Sept. 2018). PostDoc in Bochum with Alexander May. Assistant Professor at Amiens.
Q. Chen	Lattice Zero-Knowledge Proof (Start Sept. 2016 - Oct. 2019). PostDoc in Norway NTNU
B. Lambin	Symmetric Cryptography (Start Sept. 2016 - Defense Oct. 2019). PostDoc in Bochum with Gregor Leander
P. Bert	Lattice-Based Signature (Start Sept. 2016 - Defense Nov. 2019). PostDoc in Orange Labs with Olivier Sanders
A. Siffer	Data Mining and Anomaly Detection (Start Sept. 2016 - Defense Dec. 2019). Cifre Amossys.

T. Espitau	Cryptanalysis of lattice schemes (Start sept. 2016 - Defense Jan. 2020). PostDoc in NTT Japan with Mehdi Tibouchi
A. Bossuat	Provable Security of Real-World Protocols (Start sept. 2017 - Defense Sept. 2020). Engineer Quarkslab
C. Duguey	On the Security of Instant Messaging (Start sept. 2016 - Defense Dec. 2021). DGA–MI
V. Mollimard	Algorithmes pour la cryptanalyse différentielle (Start sept. 2018 - Defense January. 2022). PostDoc Haida, Israël with Orr Dunkelman
K. Boudgoust	Theoretical Hardness of Algebraically Structured Learning With Errors (Start sept. 2018 - Defense Nov. 2021). PostDoc Åarhus, Danemark with Peter Scholl
A. Nedelcu	On the Security of Instant Messaging (Start sept. 2018 - Defense January. 2022). Cifre with Orange Labs.

Publications

136 publications in international conferences and 24 articles in journal: DBLP `http://dblp.uni-trier.de/pers/hd/f/Fouque:Pierre=Alain`.
Among the 20 most prolific cryptographers according to the IACR DB and **first French cryptographer:** `https://www.iacr.org/cryptodb/data/stats.php`. 74 publications.
Conferences in bold are A^* ranked in CORE. I have 45 A^* ranked papers in journal and conferences and 45 in ranked A journal and conferences.

Venues	**Numbers**
1st class cryptographic conferences: **Crypto**, **Eurocrypt**, Asiacrypt	42
2nd class cryptographic conferences: FSE, FC, SAC, PKC, CT-RSA, ACNS, CHES	51
Other cryptographic conferences: Pairing, SCN, FDTC, ...	9
Conferences in Security and Algorithms (first-class ranked): ICALP, COCOON, **PODC**, **CCS**, CSF, EuroSP, ESORICS, **SP**, **KDD**, PETS, ASIACCS	30

Publications

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

C. Bouillaguet, P. A. Fouque, A. Joux and J. Treger. *A Family of Weak Keys in HFE (and the Corresponding Practical Key-Recovery)*. **Journal of Mathematical Cryptology**, 2011. Available at `http://www.di.ens.fr/~fouque/jmc11.pdf`.

E. Andreeva, C. Bouillaguet, O. Dunkelman, P. A. Fouque, J.J. Hoch, J. Kelsey, A. Shamir and S. Zimmer. *New Second Preimage Attacks on Hash Function*. **Journal of Cryptology**, 2016. Available at `http://www.di.ens.fr/~fouque/pub/joc11.pdf`.

C. Bouillaguet, P. Derbez, O. Dunkelman, P. A. Fouque, and N. Keller. *Low Data Complexity Attacks on AES*. **ACM Transactions on Information and System Security (TISSEC)**, 2012. Available at `http://www.di.ens.fr/~fouque/pub/tissec11.pdf`.

R. R. Farashahi, P. A. Fouque, I. Shparlinski, M. Tibouchi and F. Voloch. *Indifferentiability deterministic hashing to elliptic curve and hyperelliptic curves*. **Math. Comp.**, 2012. Available at `http://www.di.ens.fr/~fouque/pub/mathcomp11.pdf`.

M. Abdalla, P. A. Fouque, V. Lyubashevsky and M. Tibouchi. *Tightly-Secure Signatures From Lossy Identification Schemes*. **Journal of Cryptology**, 2016. Available at `http://eprint.iacr.org/2013/856.pdf`.

P. A. Fouque, N. Guillermin, D. Leresteux, M. Tibouchi and J. C. Zapalowicz. *Attacking RSA-CRT Signatures with Faults on Montgomery Multiplication*. **Journal of Cryptographic ENgineering**, 2013. Available at `http://www.irisa.fr/celtique/zapalowicz/papers/jcen2013.pdf`

J. Plut, P. A. Fouque and G. Macario-Rat. *Solving the "Isomorphism of Polynomials with Two Secrets" Problem for All Pairs of Quadratic Forms*. **Soumis au Journal Math. Comp.** Available at `http://arxiv.org/pdf/1406.3163.pdf`

Charles Bouillaguet, Claire Delaplace, and Pierre-Alain Fouque. *Revisiting and Improving Algorithms for the 3XOR Problem.* **IACR Trans. Symmetric Cryptol. 2018**, pp. 254–276, 2018.

Patrick Derbez, Pierre-Alain Fouque, Baptiste Lambin, and Brice Minaud. *On Recovering Affine Encodings in White-Box Implementations.* **IACR Trans. Cryptogr. Hardw. Embed. Syst. 2018**, pp. 121–149, 2018.

Thomas Espitau, Pierre-Alain Fouque, Benoît Gérard, and Mehdi Tibouchi. *Loop-Abort Faults on Lattice-Based Signature Schemes and Key Exchange Protocols.* **IEEE Trans. Computers 67(11)**, pp. 1535–1549, 2018.

Brice Minaud, Patrick Derbez, Pierre-Alain Fouque, and Pierre Karpman. *Key-Recovery Attacks on ASASA.* **J. Cryptology 31(3)**, pp. 845–884, 2018.

Patrick Derbez, Pierre-Alain Fouque, Baptiste Lambin, and Victor Mollimard. *Efficient Search for Optimal Diffusion Layers of Generalized Feistel Networks.* **IACR Trans. Symmetric Cryptol. 2019(2)**, pp. 218–240, 2020.

Pierre-Alain Fouque and Mehdi Tibouchi. *Close to Uniform Prime Number Generation With Fewer Random Bits.* **IEEE Trans. Information Theory 65(2)**, pp. 1307–1317, 2019.

Ghada Arfaoui, Pierre-Alain Fouque, Adina Nedelcu and Cristina Onete. *The privacy of the TLS 1.3 protocol.* **PETS 2019**, pp. 190–210, 2019.

Raphael Bost and Pierre-Alain Fouque. *Security-Efficiency Tradeoffs in Searchable Encryption - Lower Bounds and Optimal Constructions.* **PETS 2019**, pp. 232–151, 2019.

Patrick Derbez and Pierre-Alain Fouque. *Increasing Precision of Division Property.* **IACR Trans. Symmetric Cryptol. 2020(4)**, pp. 173–194, 2020.

Patrick Derbez, Pierre-Alain Fouque, and Victor Mollimard. *Fake Near Collisions Attacks.* **IACR Trans. Symmetric Cryptol. 2020(4)**, pp. 88–103, 2020.

Gilles Barthe, Sonia Belaïd, François Dupressoir, Pierre-Alain Fouque, Benjamin Grégoire, François-Xavier Standaert, Pierre-Yves Strub. *Improved parallel mask refreshing algorithms: generic solutions with parametrized non-interference and automated optimizations.* **J. Cryptogr. Eng. 10(1)**, pp. 17–26, 2020.

Daniel De Almeida Braga, Pierre-Alain Fouque, and Mohamed Sabt. *The Long and Winding Path to Secure Implementation of GlobalPlatform SCP10.* **IACR Trans. Cryptogr. Hardw. Embed. Syst. 2020(3)**, pp. 196–218, 2020.

Baptiste Lambin, Patrick Derbez, and Pierre-Alain Fouque. *Linearly equivalent S-boxes and the division property.* **Des. Codes Cryptogr. 88(10)**, pp. 2207–2231, 2020.

Pierre-Alain Fouque, Paul Kirchner, Thomas Pornin, and Yang Yu. *BAT: Small and Fast KEM over NTRU Lattices.* **IACR Trans. Cryptogr. Hardw. Embed. Syst. 2022(2)**, pp. 240–265, 2022.

Gwendal Patat, Mohamed Sabt, Pierre-Alain Fouque: *Your DRM Can Watch You Too: Exploring the Privacy Implications of Browsers (mis)Implementations of Widevine EME.* **Proc. Priv. Enhancing Technol. 2023(4).** pp. 306–321, 2023.

International Conferences

Daniel De Almeida Braga, Natalia Kulatova, Mohamed Sabt, Pierre-Alain Fouque and Karthikeyan Bhargavan. *From Dragondoom to Dragonstar: Side-channel Attacks and Formally Verified Implementation of WPA3 Dragonfly Handshake.* **EuroS&P 2023**, pp. 707–723, 2023.

Pierre-Alain Fouque, Adela Georgescu, Chen Qian, Adeline Roux-Langlois, and Weiqiang Wen. *A Generic Transform from Multi-round Interactive Proof to NIZK.* **Public Key Cryptography (2) 2023**, pp. 461–481, 2023.

Charles Bouillaguet, Ambroise Fleury, Pierre-Alain Fouque, and Paul Kirchner. *We Are on the Same Side. Alternative Sieving Strategies for the Number Field Sieve.* **ASIACRYPT 2023**, pp. –, 2023.

Ghada Arfaoui, Pierre-Alain Fouque, Thibaut Jacques, Pascal Lafourcade, Adina Nedelcu, Cristina Onete, Léo Robert. *A Cryptographic View of Deep-Attestation, or How to Do Provably-Secure Layer-Linking.* **ACNS 2022**, pp. 399–418, 2022.

Patrick Derbez, Marie Euler, Pierre-Alain Fouque, and Phuong Hoa Nguyen. *Revisiting Related-Key Boomerang Attacks on AES Using Computer-Aided Tool.* **ASIACRYPT (3) 2022**, pp. 68–88, 2022.

Gwendal Patat, Mohamed Sabt, and Pierre-Alain Fouque. *WideLeak: How Over-the-Top Platforms Fail in Android.* **DSN 2022**, pp. 501–508, 2022.

Thomas Espitau, Pierre-Alain Fouque, FranÁois GÈrard, Mélissa Rossi, Akira Takahashi, Mehdi Tibouchi, Alexandre Wallet, and Yang Yu. *Mitaka: A Simpler, Parallelizable, Maskable Variant of Falcon.* **EUROCRYPT (3) 2022**, pp. 222–253, 2022.

Olivier Blazy, Pierre-Alain Fouque, Thibaut Jacques, Pascal Lafourcade, Cristina Onete, and Léo Robert. *MARSHAL: messaging with asynchronous ratchets and signatures for faster HeALing.* **SAC 2022**, pp. 1666–1673, 2022.

Gwendal Patat, Mohamed Sabt, and Pierre-Alain Fouque. *Exploring Widevine for Fun and Profit.* **SP Workshops 2022**, pp. 277–288, 2022.

Jan Jancar, Marcel Fourné, Daniel De Almeida Braga, Mohamed Sabt, Peter Schwabe, Gilles Barthe, Pierre-Alain Fouque, and Yasemin Acar. *"They're not that hard to mitigate": What Cryptographic Library Developers Think About Timing Attacks.* newblock **IEEE Symposium on Security and Privacy 2022**, pp. 632–649, 2022.

Daniel De Almeida Braga, Pierre-Alain Fouque, and Mohamed Sabt. *PARASITE: PAssword Recovery Attack against Srp Implementations in ThE wild.* **CCS 2021**, pp. 2497–2512, 2021.

Angéle Bossuat, Raphaël Bost, Pierre-Alain Fouque, Brice Minaud, and Michael Reichle. *SSE and SSD: Page-Efficient Searchable Symmetric Encryption.* **CRYPTO (3) 2021**, pp. 157–184, 2021.

Paul Kirchner, Thomas Espitau, and Pierre-Alain Fouque. *Towards Faster Polynomial-Time Lattice Reduction.* **CRYPTO (2) 2021**, pp. 760–790, 2021.

Ghada Arfaoui, Olivier Blazy, Xavier Bultel, Pierre-Alain Fouque, Thibaut Jacques, Adina Nedelcu, and Cristina Onete. *How to (Legally) Keep Secrets from Mobile Operators.* **ESORICS (1) 2021**, pp. 23–43, 2021.

Julien Devigne, Céline Duguey, and Pierre-Alain Fouque. *MLS Group Messaging: How Zero-Knowledge Can Secure Updates.* **ESORICS (2) 2021**, pp. 587–607.

Sébastien Campion, Julien Devigne, Céline Duguey, and Pierre-Alain Fouque. *Multi-Device for Signal.* **ACNS (2) 2020**, pp. 167–187, 2020.

Daniel De Almeida Braga, Pierre-Alain Fouque, and Mohamed Sabt. *Dragonblood is Still Leaking: Practical Cache-based Side-Channel in the Wild.* **ACSAC 2020**, pp. 291–303, 2020.

Paul Kirchner, Thomas Espitau, and Pierre-Alain Fouque. *Fast Reduction of Algebraic Lattices over Cyclotomic Fields.* **CRYPTO (2) 2020**, pp. 155–185, 2020.

Martin R. Albrecht, Shi Bai, Pierre-Alain Fouque, Paul Kirchner, Damien Stehlé, and Weiqiang Wen. *Faster Enumeration-Based Lattice Reduction: Root Hermite Factor $k^{1/(2k)}$ Time $k^{k/8+o(k)}$.* **CRYPTO (2) 2020**, pp. 186–212, 2020.

Angèle Bossuat, Xavier Bultel, Pierre-Alain Fouque, Cristina Onete, and Thyla van der Merwe. *Designing Reverse Firewalls for the Real World.* **ESORICS (1) 2020**, pp. 193–213, 2020.

Pierre-Alain Fouque, Paul Kirchner, Mehdi Tibouchi, Alexandre Wallet, and Yang Yu. *Key Recovery from Gram-Schmidt Norm Leakage in Hash-and-Sign Signatures over NTRU Lattices.* **EUROCRYPT (3) 2020**, pp. 34–63, 2020.

Alban Siffer, Pierre-Alain Fouque, Alexandre Termier, and Christine Largouët. *Netspot: a simple Intrusion Detection System with statistical learning.* **TrustCom 2020**, pp. 911-918, 2020.

Gilles Barthe, Sonia Belaid, Thomas Espitau, Pierre-Alain Fouque, Mélissa Rossi and Mehdi Tibouchi. *GALACTICS: Gaussian Sampling for Lattice-Based Constant-Time Implementation of Cryptographic Signatures, Revisited.* **CCS 2019**, pp. 2147–2164, 2019.

Gilles Barthe, Sonia Belaid, Gaetan Cassiers, Pierre-Alain Fouque, Benjamin Grégoire and François-Xavier Standaert. *maskVerif: Automated Verification of Higher-Order Masking in Presence of Physical Defaults.* **ESORICS 2019**, pp. 300–318, 2019.

Olivier Blazy, Angèle Bossuat, Xavier Bultel, Pierre-Alain Fouque, Cristina Onete, and Elena Pagnin. *SAID: Reshaping Signal into an Identity-Based Asynchronous Messaging Protocol with Authenticated Ratcheting.* **EuroSP 2019**, pp. 294–309, 2019.

Vincent Migliore, Benoît Gérard, Mehdi Tibouchi, and Pierre-Alain Fouque. *Masking Dilithium - Efficient Implementation and Side-Channel Evaluation.* **ACNS 2019**, pp. 344–362, 2019.

Nicolas Desmoulins, Pierre-Alain Fouque, Cristina Onete, and Olivier Sanders. *Pattern Matching on Encrypted Streams.* **ASIACRYPT 2018**, pp. 121–148, 2018.

Jonathan Bootle, Claire Delaplace, Thomas Espitau, Pierre-Alain Fouque, and Mehdi Tibouchi. *LWE Without Modular Reduction and Improved Side-Channel Attacks Against BLISS.* **ASIACRYPT 2018**, pp. 494–524, 2018.

Cécile Baritel-Ruet, François Dupressoir, Pierre-Alain Fouque, and Benjamin Grégoire. *Formal Security Proof of CMAC and Its Variants.* **CSF 2018**, pp. 91–104, 2018.

Gilles Barthe, Sonia Belaïd, Thomas Espitau, Pierre-Alain Fouque, Benjamin Grégoire, Mélissa Rossi, and Mehdi Tibouchi. *Masking the GLP Lattice-Based Signature Scheme at Any Order.* **EUROCRYPT 2018**, pp. 354–384, 2018.

Alban Siffer, Pierre-Alain Fouque, Alexandre Termier, and Christine Largouët. *Are your data gathered ?* **KDD 2018**, pp. 2210–2218, 2018.

Pauline Bert, Pierre-Alain Fouque, Adeline Roux-Langlois, and Mohamed Sabt. *Practical Implementation of Ring-SIS/LWE Based Signature and IBE.* **PQCrypto 2018**, pp. 271–291, 2018.

Patrick Derbez, Pierre-Alain Fouque, Jérémy Jean, and Baptiste Lambin. *Variants of the AES Key Schedule for Better Truncated Differential Bounds.* **SAC 2018**, pp.27–49, 2018.

Karthikeyan Bhargavan, Ioana Boureanu, Antoine Delignat-Lavaud, Pierre-Alain Fouque, and Cristina Onete. *A Formal Treatment of Accountable Proxying Over TLS.* **IEEE Symposium on Security and Privacy 2018**, pp. 799–816, 2018.

Thomas Espitau, Pierre-Alain Fouque, Benoît Gérard and Mehdi Tibouchi. *Side-channel attacks on BLISS lattice-based signatures.* **ACM CCS 2017**, pp. 1857–1874, ACM, 2017.

Alban Siffer, Pierre-Alain Fouque, Alexandre Termier and Christine Largouët. *Anomaly Detection in Streams with Extreme Value Theory.* **KDD 2017**, pp. 1067–1075, 2017.

Charles Bouillaguet, Claire Delaplace, Pierre-Alain Fouque and Paul Kirchner. *Fast Lattice-Based Encryption: Stretching Spring.* **PQCrypto 2017**, pp. 125–142, 2017.

Karthikeyan Bhargavan, Ioana Bureanu, Pierre-Alain Fouque, Cristina Onete and Benjamin Richard. *Content delivery and TLS: a cryptographic analysis of keyless SSL*. **EuroSP 2017**, pp. 1–16, IEEE, 2017.

Jean-François Biasse, Thomas Espitau, Pierre-Alain Fouque, Alexandre Gélin and Paul Kirchner. *Computing generator in cyclotomic integer rings - A subfield algorithm for the Principal Ideal Problem in $L_{|\Delta_K|}(1/2)$ and application to cryptanalysis of a FHE scheme*. **EUROCRYPT 2017**, pp. 60–88, Springer-Verlag, 2017.

Paul Kirchner and Pierre-Alain Fouque. *Revisiting Lattice Attacks on overstretched NTRU parameters*. **EUROCRYPT 2017**, pp. 3–26, Springer-Verlag, 2017.

Pierre-Alain Fouque, Pierre Karpman, Paul Kirchner and Brice Minaud. *Efficient and Provable White-Box Primitives*. **ASIACRYPT (1) 2016**, pp. 159–188, Springer-Verlag, 2016.

Gilles Barthe, Sonia Belaïd, François Dupressoir, Pierre-Alain Fouque, Benjamin Grégoire, Pierre-Yves Strub and Rébecca Zucchini. *Strong Non-Interference and Type-Directed Higher-Order Masking*. **ACM Conference on Computer and Communications Security 2016**, pp. 116–129, ACM, 2016.

P. A. Fouque, C. Onete and B. Richard. *Achieving Better Privacy for the 3GPP AKA Protocol*. In **PETS 2016**, pp. 255–275, De Gruyter Open, 2016.

P. Derbez and P. A. Fouque. *Automatic Search of Meet-in-the-Middle and Impossible Differential Attacks*. In **CRYPTO 2016**, pp. 157–184, Springer-Verlag, 2016.

Thomas Espitau, Pierre-Alain Fouque, Benoît Gérard and Mehdi Tibouchi. *Loop abort Faults on Lattice-Based Fiat-Shamir & Hash n Sign signatures*. **SAC 2016**, pp. 140–158, Springer-Verlag, 2016.

P. A. Fouque, B. Hadjibeyli and P. Kirchner. *Homomorphic Evaluation of Lattice-Based Symmetric Encryption Schemes*. In **COCOON 2016**, pp. 269–280, Springer-Verlag, 2016.

P. Lestringant, P. A. Fouque and F. Guihéry. *Assisted Identification of Mode of Operation in Binary Code with Dynamic Data Flow Slicing*. In **ACNS 2016**, pp. 561–579, Springer-Verlag, 2016.

S. Alt, P. A. Fouque, G. Macario-Rat, C. Onete and B. Richard. *A Cryptographic Analysis of UMTS/LTE AKA*. In **ACNS 2016**, pp. 18–35, Springer-Verlag, 2016.

J. H. Cheon, P. A. Fouque, C. Lee, B. Minaud and H. Ryu. *Cryptanalysis of the New CLT Multilinear Maps over the Integers*. In **EUROCRYPT 2016**, pp. 509–536, Springer-Verlag, 2016.

Q. Chen and P. A. Fouque. *Fault Attacks on Efficient Pairing Implementations*. In **ASIACCS 2016**, pp. 641–650, ACM, 2016.

P. Belgarric, P. A. Fouque, G. Macario-Rat and M. Tibouchi. *Side-Channel Analysis of Weierstrass and Koblitz Curve ECDSA on Android Smartphones*. In **CT-RSA 2016**, pp. 236–252, Springer-Verlag, 2016.

B. Minaud, P. Derbez, P. A. Fouque, and P. Karpman. *Key-Recovery Attacks on ASASA*. In **ASIACRYPT 2015**, pp. 3–27, Springer-Verlag, 2015.

S. Belaid, J.-S. Coron, P. A. Fouque, B. Gérard, J.-G. Kammerer and E. Prouff. *Improved Side-Channel Analysis of Finite-Field Multiplication*. In **CHES 2015**, pp. 395–415, Springer-Verlag, 2015.

T. Espitau, P. A. Fouque and P. Karpman. *Higher-Order Differential Meet-in-The-Middle Preimage Attacks on SHA-1 and BLAKE*. In **CRYPTO 2015**, pp. 683–701, Springer-Verlag, 2015.

P. Kirchner and P. A. Fouque. *An Improved BKW Algorithm for LWE with Applications to Cryptography and Lattices*. In **CRYPTO 2015**, pp. 43–62, Springer-Verlag, 2015.

P.-A. Fouque, M.S. Lee; T. Lepoint and M. Tibouchi. *Cryptanalysis of the Co-ACD Assumption*. In **CRYPTO 2015**, pp. 561–580, Springer-Verlag, 2015.

G. Barthe, S. Belaid, F. Dupressoir, P. A. Fouque, B. Grégoire and P. Y. Strub. *Verified Proofs of Higher-Order Masking*. In **EUROCRYPT 2015**, pp. 457–485, Springer-Verlag, 2015.

P. Lestringant, P. A. Fouque and F. Guihléry. *Automated Identification of Cryptographic Primitives in Binary Code with Data Flow Graph Isomorphism*. In **ACM ASIACCS 2015**, pp. 203–214, ACM, 2015.

P. A. Fouque and M. Tibouchi. *Close to Uniform Prime Number Generation With Fewer Random Bits*. In **ICALP 2014**, pp. 991–1002, Springer-Verlag, 2014.

G. Barthe, F. Dupressoir, P. A. Fouque, B. Grégoire and J. C. Zapalowicz. *Synthesis of Fault Attacks on Cryptographic Implementations*. In **ACM CCS 2014**, pp. 1016–1027, ACM, 2014.

D. F. Aranha, P. A. Fouque, B. Gérard, J. G. Kammerer, M. Tibouchi and J. C. Zapalowicz. *GLV/GLS Decomposition, Power Analysis, and Attacks on ECDSA Signatures With Single-Bit Nonce Bias*. In **Asiacrypt 2014**, pp. 262–281, Springer-Verlag, 2014.

S. Belaid, P. A. Fouque and B. Gérard. *Side-Channel Analysis of the authentication of AES-GCM*. In **Asiacrypt 2014**, pp. 306–325, Springer-Verlag, 2014.

P. A. Fouque, A. Joux and C. Mavromati. *Multi-user collisions: Applications to Discrete-Logs, Even-Mansour and Prince*. In **Asiacrypt 2014**, pp. 420–438, Springer-Verlag, 2014.

G. Barthe, F. Dupressoir, P. A. Fouque, B. Grégoire, M. Tibouchi and J. C. Zapalowicz. *Making RSA-PSS Provably Secure Against Non-Random Faults*. In **CHES 2014**, pp. 206–222, Springer-Verlag, 2014.

P. A. Fouque and J. C. Zapalowicz. *Statistical Properties of Short RSA Distribution and their Cryptographic Applications*. In **COCOON 2014**, pp. 525–536, Springer-Verlag, 2014.

D. Augot, P. A. Fouque and P. Karpman. *Diffusion matrices from algebraic-geometry codes with efficient constant-time software implementation*. In **SAC 2014**, pp. 243–260, Springer-Verlag, 2014.

D. F. Aranha, Q. Chen, P. A. Fouque, M. Tibouchi and J. C. Zapalowicz. *Binary Elligator Squared*. In **SAC 2014**, pp. 20–37, Springer-Verlag, 2014.

P. A. Fouque and P. Karpman. *Security Amplification against Meet-in-the-Middle Attacks using Whitening*. In **IMACC 2013**, pp. 252–269, Springer-Verglag, 2013.

P. A. Fouque, M. Tibouchi and J. C. Zapalowicz. *Recovering Private Keys Generated with Weak PRNGs*. In **IMACC 2013**, pp. 158–172, Springer-Verlag, 2013.

P. A. Fouque, J. Jean and T. Peyrin. *Structural Evaluation of AES and Chosen-Key Distinguisher of 9-round AES-128*. In **CRYPTO 2013**, pp. 183–203, Springer-Verlag, 2013.

M. Abdalla, S. Belaid and P. A. Fouque. *Leakage-Resilient Symmetric Encryption via Re-Keying*. In **CHES 2013**, pp. 471–488, Springer-Verlag, 2013.

P. A. Fouque, A. Joux and M. Tibouchi. *Injective Encodings to Elliptic Curves*. In **ACISP 2013**, pp. 203–218, Springer-Verlag, 2013.

P. A. Fouque, D. Vergnaud and J. C. Zapalowicz. *Time/Memory/Data Tradeoffs for Variants of the RSA Problem*. In **COCOON 2013**, pp. 651–662, Springer-Verlag, 2013.

P. A. Fouque and T. Vannet. *Improving Key Recovery to 784 and 799 rounds of Trivium using Optimized Cube Attacks*. In **FSE 2013**, pp. 502–517, Springer-Verlag, 2013.

P. Derbez and P. A. Fouque. *Exhausting Demirci-Selcuk Meet-in-the-Middle Attacks against Reduced-Round AES*. In **FSE 2013**, pp. 541–560, Springer-Verlag, 2013.

P. Derbez, P. A. Fouque and J. Jean. *Improved Key Recovery Attacks on Reduced-Round AES in the Single-Key Setting*. In **EUROCRYPT 2013**, pp. 371–387, Springer-Verlag, 2013.

C. Bouillaguet, P. A. Fouque et A. Veber. *Graph-Theoretic Algorithms for the "Isomorphism of Polynomials" Problem*. In **EUROCRYPT 2013**, pp. 211–227, Springer-Verlag, 2013.

C. Arnaud and P. A. Fouque. *Timing Attack against protected RSA-CRT implementation used in PolarSSL*. In **CT RSA 2013**, pp. 18–33, Springer-Verlag, 2013.

J. Lu, Wei, P. A. Fouque and E. Pasalic. *Meet-in-the-Middle Attack on Reduced Versions of the Camellia Block Cipher*. In **IWSEC 2012**, pp. 197–215, Springer-Verlag, 2012.

P. A. Fouque and M. Tibouchi. *Indifferentiable Hashing to Barreto-Naehrig Curves*. In **Latincrypt 2012**, LNCS, pp. 1–17, Springer-Verlag, 2012.

M. Daubignard, P. A. Fouque and Y. Lakhnech. *Generic Indifferentiability Proofs of Hash Designs*. In **CSF 2012**, pp. 340–353, ACM, 2012.

P. A. Fouque, N. Guillermin, D. Leresteux, M. Tibouchi and J. C. Zapalowicz. *Attacking RSA-CRT Signatures with Faults on Montgomery Multiplication*. In **CHES 2012**, LNCS , pp. 447–462, Springer-Verlag, 2012.

M. Abdalla, P. A. Fouque, V. Lyubashevsky and M. Tibouchi. *Tightly-Secure Signatures from Lossy ID Schemes*. In **Advances in Cryptology – Proceedings of EUROCRYPT '12**, volume of *Lecture Notes in Computer Science*, pages 667–685. Springer-Verlag, Berlin, 2012.

D. Leresteux, P. A. Fouque and F. Valette. *Fault Attack like Buffer Overflow*. In **Symposium on Applied Computing '12**, *ACM Press*, pages –. 2012.

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

P. Derbez, P. A. Fouque and D. Leresteux. *Meet-in-the-Middle and Impossible Differential Fault Analysis on AES*. In **Crytographic Hardware and Embedded Systems (CHES) '11**, volume 6917 of *Lecture Notes in Computer Science*, pages 667–685. Springer-Verlag, Berlin, 2011.

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

C. Bouillaguet, O. Dunkelman, P. A. Fouque and G. Leurent. *New Insights on Impossible Differential Cryptanalysis*. In **Selected Areas in Cryptography (SAC) '11**, volume of *Lecture Notes in Computer Science*, pages –. Springer-Verlag, Berlin, 2011.

T. Chardin, P. A. Fouque and D. Leresteux. *Cache Timing Analysis of RC4*. In **Applied Cryptography and Network Security (ACNS) '11**, volume 6715 of *Lecture Notes in Computer Science*, pages 110–129. Springer-Verlag, Berlin, 2011.

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

P. A. Fouque and J. Jean. *Practical Near-Collisions and Collisions on Round-Reduced ECHO-256 Compression Function*. In **Fast Software Encryption (FSE) '11**, volume of *Lecture Notes in Computer Science*, pages 107–127. Springer-Verlag, Berlin, 2011.

P. A. Fouque and M. Tibouchi. *Deterministic encoding and hashing to odd hyperelliptic curves*. In **PAIRING '10**, volume 6487 of *Lecture Notes in Computer Science*, pages 265–277. Springer-Verlag, Berlin, 2010.

P. A. Fouque and M. Tibouchi. *Estimating the Size of the Image of Deterministic Hash Functions to Elliptic Curves*. In **LATINCRYPT '10**, volume 6212 of *Lecture Notes in Computer Science*, pages 81–91. Springer-Verlag, Berlin, 2010.

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

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

C. Bouillaguet, O. Dunkelman, P. A. Fouque and G. Leurent. *Another Look at the Complementation Property*. In **Fast Software Encryption (FSE) '10**, volume 6147 of *Lecture Notes in Computer Science*, pages 347–364. Springer-Verlag, Berlin, 2010.

P. A. Fouque, G. Leurent, D. Réal and F. Valette. *Practical Electromagnetic Template Attack on HMAC*. In **Cryptographic Hardware and Embedded Systems (CHES) '09**, volume 5747 of *Lecture Notes in Computer Science*, pages 66–80. Springer-Verlag, Berlin, 2009.

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

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

P. A. Fouque, D. Réal, F. Valette and M. Drissi. *The Carry Leakage on the Randomized Exponent Countermeasure*. In **Cryptographic Hardware and Embedded Systems (CHES) '08**, volume 5154 of *Lecture Notes in Computer Science*, pages 198–213. Springer-Verlag, Berlin, 2008.

P. A. Fouque, R. Lercier, D. Réal and V. Valette. *Fault Attack on Elliptic Curve with Montgomery Ladder Implementation*. In **FTDC '08**, pages 92–98. IEEE-CS Press, 2008.

C. Bouillaguet and P. A. Fouque. *Analysis of the Collision Resistance of Radiogatuun using Algebraic Technique*. In **Selected Areas in Cryptography (SAC) '08**, volume 5381 of *Lecture Notes in Computer Science*, pages 245–261. Springer-Verlag, Berlin, 2008.

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

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

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

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

P. A. Fouque, G. Macario-Rat, L. Perret and J. Stern. *Total Break of the ℓ-IC Signature Scheme*. In **Conference on Practice and Theory in Public-Key Cryptography (PKC) '08**, volume 4939 of *Lecture Notes in Computer Science*, pages 1–17. Springer-Verlag, Berlin, 2008.

P. A. Fouque, G. Macario-Rat and J. Stern. *Key Recovery on Hidden Monomial Multivariate Schemes*. In **Advances in Cryptology – Proceedings of EUROCRYPT '08**, volume 4965 of *Lecture Notes in Computer Science*, pages 19–30. Springer-Verlag, Berlin, 2008.

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

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

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

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

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

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

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

, O. Chevassut, P. A. Fouque, P. Gaudry and D. Pointcheval. *The Twist-Augmented Technique for Key Exchange*. 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.

P. A. Fouque, D. Pointcheval, J. Stern and S. Zimmer. *Hardness of Distinguishing the MSB or LSB of Secrete Keys in Diffie-Hellman Schemes*. 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.

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

M. Abdalla, O. Chevassut, P. A. Fouque and D. Pointcheval. *A Simple Threshold Authenticated Key Exchange from Short Secrets*. In **Advances in Cryptology – Proceedings of ASIACRYPT 2005**, volume 3788 of *Lecture Notes in Computer Science*, pages 566–584. Springer-Verlag, Berlin, 2005.

M. Abdalla, P. A. Fouque and D. Pointcheval. *Password-Based Authenticated Key Exchange in the Three-Party Setting*. Dans **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.

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

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

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

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

P. A. Fouque, G. Martinet and G. Poupard. *Practical Symmetric On-Line Encryption*. In **Fast Software Encryption (FSE) '03**, volume 2887 of *Lecture Notes in Computer Science*, pages 362–375. Springer-Verlag, Berlin, 2003.

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

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

P. A. Fouque and G. Poupard. *On the Security of RDSA*. In **EUROCRYPT '03**, volume 2656 of *Lecture Notes in Computer Science*, pages 462–476. Springer-Verlag, Berlin, 2003.

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

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

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

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

P. A. Fouque and J. Stern. *One Round Threshold Discrete-Log Key Generation without Private Channels*. In **PKC '01**, volume 1992 of *Lecture Notes in Computer Science*, pages 300–316. Springer-Verlag, Berlin, 2001.

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