# Pierre-Alain Fouque

List of Publications by Year
in descending order



| 119 | 3,576 | 218381 | 214527 |
|---|---|---|---|
| papers | citations | 26 h-index | 47 g-index |

| 126 | 126 | 126 | 1459 |
|---|---|---|---|
| all docs | docs citations | times ranked | citing authors |

| # | Article | IF | Citations |
|---|---|---|---|
| 1 | Password-Based Authenticated Key Exchange in the Three-Party Setting. Lecture Notes in Computer Science, 2005, , 65-84. | 1.0 | 430 |
| 2 | Anomaly Detection in Streams with Extreme Value Theory. , 2017, , . | | 217 |
| 3 | Practical multi-candidate election system. , 2001, , . | | 178 |
| 4 | The Doubling Attack â€“ Why Upwards Is Better than Downwards. Lecture Notes in Computer Science, 2003, , 269-280. | 1.0 | 135 |
| 5 | Improved Key Recovery Attacks on Reduced-Round AES in the Single-Key Setting. Lecture Notes in Computer Science, 2013, , 371-387. | 1.0 | 115 |
| 6 | Practical Cryptanalysis of SFLASH. , 2007, , 1-12. | | 109 |
| 7 | An Improved LPN Algorithm. Lecture Notes in Computer Science, 2006, , 348-359. | 1.0 | 108 |
| 8 | Strong Non-Interference and Type-Directed Higher-Order Masking. , 2016, , . | | 102 |
| 9 | Verified Proofs of Higher-Order Masking. Lecture Notes in Computer Science, 2015, , 457-485. | 1.0 | 84 |
| 10 | Threshold Cryptosystems Secure against Chosen-Ciphertext Attacks. Lecture Notes in Computer Science, 2001, , 351-368. | 1.0 | 75 |
| 11 | Side-Channel Attacks on BLISS Lattice-Based Signatures. , 2017, , . | | 70 |
| 12 | Differential Cryptanalysis for Multivariate Schemes. Lecture Notes in Computer Science, 2005, , 341-353. | 1.0 | 68 |
| 13 | Revisiting Lattice Attacks on Overstretched NTRU Parameters. Lecture Notes in Computer Science, 2017, , 3-26. | 1.0 | 61 |
| 14 | Tightly-Secure Signatures from Lossy Identification Schemes. Lecture Notes in Computer Science, 2012, , 572-590. | 1.0 | 58 |
| 15 | An Improved BKW Algorithm for LWE with Applications to Cryptography and Lattices. Lecture Notes in Computer Science, 2015, , 43-62. | 1.0 | 55 |
| 16 | Fault Attack on Elliptic Curve Montgomery Ladder Implementation. , 2008, , . | | 54 |
| 17 | Improving Key Recovery to 784 and 799 Rounds of Trivium Using Optimized Cube Attacks. Lecture Notes in Computer Science, 2014, , 502-517. | 1.0 | 51 |
| 18 | Automatic Search of Attacks on Round-Reduced AES and Applications. Lecture Notes in Computer Science, 2011, , 169-187. | 1.0 | 50 |

| # | Article | IF | Citations |
|---|---|---|---|
| 19 | Low-Data Complexity Attacks on AES. IEEE Transactions on Information Theory, 2012, 58, 7002-7017. | 1.5 | 40 |
| 20 | Structural Evaluation of AES and Chosen-Key Distinguisher of 9-Round AES-128. Lecture Notes in Computer Science, 2013, , 183-203. | 1.0 | 39 |
| 21 | maskVerif: Automated Verification of Higher-Order Masking in Presence of Physical Defaults. Lecture Notes in Computer Science, 2019, , 300-318. | 1.0 | 35 |
| 22 | Indifferentiable deterministic hashing to elliptic and hyperelliptic curves. Mathematics of Computation, 2012, 82, 491-512. | 1.1 | 33 |
| 23 | Meet-in-the-Middle and Impossible Differential Fault Analysis on AES. Lecture Notes in Computer Science, 2011, , 274-291. | 1.0 | 33 |
| 24 | Automatic Search of Meet-in-the-Middle and Impossible Differential Attacks. Lecture Notes in Computer Science, 2016, , 157-184. | 1.0 | 33 |
| 25 | Exhausting Demirci-SelÃ§uk Meet-in-the-Middle Attacks Against Reduced-Round AES. Lecture Notes in Computer Science, 2014, , 541-560. | 1.0 | 32 |
| 26 | Masking the GLP Lattice-Based Signature Scheme at Any Order. Lecture Notes in Computer Science, 2018, , 354-384. | 1.0 | 31 |
| 27 | A Simple Threshold Authenticated Key Exchange from Short Secrets. Lecture Notes in Computer Science, 2005, , 566-584. | 1.0 | 31 |
| 28 | GALACTICS. , 2019, , . | | 30 |
| 29 | Achieving Better Privacy for the 3GPP AKA Protocol. Proceedings on Privacy Enhancing Technologies, 2016, 2016, 255-275. | 2.3 | 29 |
| 30 | The Twist-AUgmented Technique for Key Exchange. Lecture Notes in Computer Science, 2006, , 410-426. | 1.0 | 29 |
| 31 | Efficient and Provable White-Box Primitives. Lecture Notes in Computer Science, 2016, , 159-188. | 1.0 | 29 |
| 32 | CryptoComputing with Rationals. Lecture Notes in Computer Science, 2003, , 136-146. | 1.0 | 28 |
| 33 | Masking Dilithium. Lecture Notes in Computer Science, 2019, , 344-362. | 1.0 | 28 |
| 34 | Another Look at Complementation Properties. Lecture Notes in Computer Science, 2010, , 347-364. | 1.0 | 26 |
| 35 | Automated Identification of Cryptographic Primitives in Binary Code with Data Flow Graph Isomorphism. , 2015, , . | | 26 |
| 36 | Cryptanalysis of SFLASH with Slightly ModifiedÂParameters. Lecture Notes in Computer Science, 2007, , 264-275. | 1.0 | 26 |

| # | Article | IF | Citations |
|---|---|---|---|
| 37 | On Some Incompatible Properties of Voting Schemes. Lecture Notes in Computer Science, 2010, , 191-199. | 1.0 | 26 |
| 38 | The privacy of the TLS 1.3 protocol. Proceedings on Privacy Enhancing Technologies, 2019, 2019, 190-210. | 2.3 | 26 |
| 39 | One Round Threshold Discrete-Log Key Generation without Private Channels. Lecture Notes in Computer Science, 2001, , 300-316. | 1.0 | 25 |
| 40 | Authenticated On-Line Encryption. Lecture Notes in Computer Science, 2004, , 145-159. | 1.0 | 24 |
| 41 | Side-Channel Analysis of Weierstrass and Koblitz Curve ECDSA on Android Smartphones. Lecture Notes in Computer Science, 2016, , 236-252. | 1.0 | 23 |
| 42 | Improved Side-Channel Analysis of Finite-Field Multiplication. Lecture Notes in Computer Science, 2015, , 395-415. | 1.0 | 23 |
| 43 | LWE Without Modular Reduction and Improved Side-Channel Attacks Against BLISS. Lecture Notes in Computer Science, 2018, , 494-524. | 1.0 | 23 |
| 44 | Tightly Secure Signatures From Lossy Identification Schemes. Journal of Cryptology, 2016, 29, 597-631. | 2.1 | 22 |
| 45 | HMAC is a randomness extractor and applications to TLS. , 2008, , . | | 21 |
| 46 | Synthesis of Fault Attacks on Cryptographic Implementations. , 2014, , . | | 21 |
| 47 | Side-Channel Analysis of Multiplications in GF(2128). Lecture Notes in Computer Science, 2014, , 306-325. | 1.0 | 21 |
| 48 | GLV/GLS Decomposition, Power Analysis, and Attacks on ECDSA Signatures with Single-Bit Nonce Bias. Lecture Notes in Computer Science, 2014, , 262-281. | 1.0 | 21 |
| 49 | Key-Recovery Attacks on ASASA. Lecture Notes in Computer Science, 2015, , 3-27. | 1.0 | 20 |
| 50 | Estimating the Size of the Image of Deterministic Hash Functions to Elliptic Curves. Lecture Notes in Computer Science, 2010, , 81-91. | 1.0 | 19 |
| 51 | Deterministic Encoding and Hashing to Odd Hyperelliptic Curves. Lecture Notes in Computer Science, 2010, , 265-277. | 1.0 | 19 |
| 52 | Optimal Randomness Extraction from a Diffie-Hellman Element. Lecture Notes in Computer Science, 2009, , 572-589. | 1.0 | 19 |
| 53 | Indifferentiable Hashing to Barretoâ€“Naehrig Curves. Lecture Notes in Computer Science, 2012, , 1-17. | 1.0 | 18 |
| 54 | New Second-Preimage Attacks on Hash Functions. Journal of Cryptology, 2016, 29, 657-696. | 2.1 | 18 |

| # | Article | IF | Citations |
|---|---|---|---|
| 55 | Computing Generator in Cyclotomic Integer Rings. Lecture Notes in Computer Science, 2017, , 60-88. | 1.0 | 18 |
| 56 | Mitaka: A Simpler, Parallelizable, Maskable Variant ofÂFalcon. Lecture Notes in Computer Science, 2022, , 222-253. | 1.0 | 18 |
| 57 | Pattern Matching on Encrypted Streams. Lecture Notes in Computer Science, 2018, , 121-148. | 1.0 | 17 |
| 58 | Practical Symmetric On-Line Encryption. Lecture Notes in Computer Science, 2003, , 362-375. | 1.0 | 17 |
| 59 | Total Break of the â„“-IC Signature Scheme. , 2008, , 1-17. | | 17 |
| 60 | Graph-Theoretic Algorithms for the â€œIsomorphism of Polynomialsâ€•Problem. Lecture Notes in Computer Science, 2013, , 211-227. | 1.0 | 17 |
| 61 | FasterÂEnumeration-BasedÂLatticeÂReduction: RootÂHermiteÂFactorÂ$$k^{1/(2k)}$$ÂTimeÂ$$k^{k/8+o(k)}$$. Lecture Notes in Computer Science, 2020, , 186-212. | 1.0 | 16 |
| 62 | Defeating Countermeasures Based on Randomized BSD Representations. Lecture Notes in Computer Science, 2004, , 312-327. | 1.0 | 16 |
| 63 | Attacking Unbalanced RSA-CRT Using SPA. Lecture Notes in Computer Science, 2003, , 254-268. | 1.0 | 15 |
| 64 | The Carry Leakage on the Randomized Exponent Countermeasure. Lecture Notes in Computer Science, 2008, , 198-213. | 1.0 | 15 |
| 65 | Practical Cryptanalysis of the Identification Scheme Based on the Isomorphism of Polynomial with One Secret Problem. Lecture Notes in Computer Science, 2011, , 473-493. | 1.0 | 15 |
| 66 | Key-Recovery Attacks on ASASA. Journal of Cryptology, 2018, 31, 845-884. | 2.1 | 13 |
| 67 | A Cryptographic Analysis of UMTS/LTE AKA. Lecture Notes in Computer Science, 2016, , 18-35. | 1.0 | 13 |
| 68 | Loop-Abort Faults on Lattice-Based Fiat-Shamir and Hash-and-Sign Signatures. Lecture Notes in Computer Science, 2017, , 140-158. | 1.0 | 13 |
| 69 | On the Security of the CCM Encryption Mode and of a Slight Variant. Lecture Notes in Computer Science, 2008, , 411-428. | 1.0 | 12 |
| 70 | Cryptanalysis of reduced versions of the Camellia block cipher. IET Information Security, 2012, 6, 228-238. | 1.1 | 12 |
| 71 | SSE and SSD: Page-Efficient Searchable Symmetric Encryption. Lecture Notes in Computer Science, 2021, , 157-184. | 1.0 | 12 |
| 72 | Binary Elligator Squared. Lecture Notes in Computer Science, 2014, , 20-37. | 1.0 | 12 |

| # | Article | IF | Citations |
|---|---|---|---|
| 73 | Loop-Abort Faults on Lattice-Based Signatures and Key Exchange Protocols. IEEE Transactions on Computers, 2018, , 1-1. | 2.4 | 11 |
| 74 | Key Recovery on Hidden Monomial Multivariate Schemes. , 2008, , 19-30. | | 11 |
| 75 | Attacks on Hash Functions Based on Generalized Feistel: Application to Reduced-Round Lesamnta and SHAvite-3 512. Lecture Notes in Computer Science, 2011, , 18-35. | 1.0 | 11 |
| 76 | Making RSAâ€“PSS Provably Secure against Non-random Faults. Lecture Notes in Computer Science, 2014, , 206-222. | 1.0 | 11 |
| 77 | Blockwise Adversarial Model for On-line Ciphers and Symmetric Encryption Schemes. Lecture Notes in Computer Science, 2004, , 212-226. | 1.0 | 11 |
| 78 | Security-Efficiency Tradeoffs in Searchable Encryption. Proceedings on Privacy Enhancing Technologies, 2019, 2019, 132-151. | 2.3 | 11 |
| 79 | Dragonblood is Still Leaking: Practical Cache-based Side-Channel in the Wild. , 2020, , . | | 10 |
| 80 | On Recovering Affine Encodings in White-Box Implementations. Iacr Transactions on Cryptographic Hardware and Embedded Systems, 0, , 121-149. | 0.0 | 10 |
| 81 | Attacking RSAâ€“CRT signatures with faults on montgomery multiplication. Journal of Cryptographic Engineering, 2013, 3, 59-72. | 1.5 | 9 |
| 82 | Linearly equivalent S-boxes and the division property. Designs, Codes, and Cryptography, 2020, 88, 2207-2231. | 1.0 | 9 |
| 83 | Cryptanalysis of Tweaked Versions of SMASH and Reparation. Lecture Notes in Computer Science, 2009, , 136-150. | 1.0 | 9 |
| 84 | Practical Key-Recovery for All Possible Parameters of SFLASH. Lecture Notes in Computer Science, 2011, , 667-685. | 1.0 | 9 |
| 85 | Attacking RSAâ€“CRT Signatures with Faults on Montgomery Multiplication. Lecture Notes in Computer Science, 2012, , 447-462. | 1.0 | 9 |
| 86 | Higher-Order Differential Meet-in-the-middle Preimage Attacks on SHA-1 and BLAKE. Lecture Notes in Computer Science, 2015, , 683-701. | 1.0 | 9 |
| 87 | Increasing Precision of Division Property. IACR Transactions on Symmetric Cryptology, 0, , 173-194. | 0.0 | 9 |
| 88 | Content delivery over TLS: a cryptographic analysis of keyless SSL. , 2017, , . | | 8 |
| 89 | Hardness of Distinguishing the MSB or LSB of Secret Keys in Diffie-Hellman Schemes. Lecture Notes in Computer Science, 2006, , 240-251. | 1.0 | 8 |
| 90 | Practical Near-Collisions and Collisions on Round-Reduced ECHO-256 Compression Function. Lecture Notes in Computer Science, 2011, , 107-127. | 1.0 | 8 |

| # | Article | IF | Citations |
|---|---|---|---|
| 91 | Close to Uniform Prime Number Generation with Fewer Random Bits. Lecture Notes in Computer Science, 2014, , 991-1002. | 1.0 | 8 |
| 92 | Improved parallel mask refreshing algorithms: generic solutions with parametrized non-interference and automated optimizations. Journal of Cryptographic Engineering, 2020, 10, 17-26. | 1.5 | 7 |
| 93 | Efficient Search for Optimal Diffusion Layers of Generalized Feistel Networks. IACR Transactions on Symmetric Cryptology, 0, , 218-240. | 0.0 | 7 |
| 94 | Using faults for buffer overflow effects. , 2012, , . | | 6 |
| 95 | Designing Reverse Firewalls for the Real World. Lecture Notes in Computer Science, 2020, , 193-213. | 1.0 | 6 |
| 96 | Faster Chosen-Key Distinguishers on Reduced-Round AES. Lecture Notes in Computer Science, 2012, , 225-243. | 1.0 | 6 |
| 97 | BAT: Small and Fast KEM over NTRU Lattices. Iacr Transactions on Cryptographic Hardware and Embedded Systems, 0, , 240-265. | 0.0 | 6 |
| 98 | Variants of the AES Key Schedule for Better Truncated Differential Bounds. Lecture Notes in Computer Science, 2019, , 27-49. | 1.0 | 5 |
| 99 | Recovering Private Keys Generated with Weak PRNGs. Lecture Notes in Computer Science, 2013, , 158-172. | 1.0 | 5 |
| 100 | Security Amplification against Meet-in-the-Middle Attacks Using Whitening. Lecture Notes in Computer Science, 2013, , 252-269. | 1.0 | 4 |
| 101 | Close to Uniform Prime Number Generation With Fewer Random Bits. IEEE Transactions on Information Theory, 2019, 65, 1307-1317. | 1.5 | 4 |
| 102 | SAID: Reshaping Signal into an Identity-Based Asynchronous Messaging Protocol with Authenticated Ratcheting. , 2019, , . | | 4 |
| 103 | MLS Group Messaging: How Zero-Knowledge Can Secure Updates. Lecture Notes in Computer Science, 2021, , 587-607. | 1.0 | 4 |
| 104 | Fast Reduction of Algebraic Lattices over Cyclotomic Fields. Lecture Notes in Computer Science, 2020, , 155-185. | 1.0 | 4 |
| 105 | A family of weak keys in HFE and the corresponding practical key-recovery. Journal of Mathematical Cryptology, 2012, 5, . | 0.4 | 3 |
| 106 | The Insecurity of Esign in Practical Implementations. Lecture Notes in Computer Science, 2003, , 492-506. | 1.0 | 3 |
| 107 | Cryptanalysis of the Co-ACD Assumption. Lecture Notes in Computer Science, 2015, , 561-580. | 1.0 | 3 |
| 108 | Safe-Errors on SPA Protected Implementations with the Atomicity Technique. Lecture Notes in Computer Science, 2016, , 479-493. | 1.0 | 3 |

| # | Article | IF | Citations |
|---|---|---|---|
| 109 | Fake Near Collisions Attacks. IACR Transactions on Symmetric Cryptology, 0, , 88-103. | 0.0 | 3 |
| 110 | Towards Faster Polynomial-Time Lattice Reduction. Lecture Notes in Computer Science, 2021, , 760-790. | 1.0 | 2 |
| 111 | Multi-Device for Signal. Lecture Notes in Computer Science, 2020, , 167-187. | 1.0 | 2 |
| 112 | Netspot: A Simple Intrusion Detection System with Statistical Learning. , 2020, , . | | 2 |
| 113 | PARASITE: PAssword Recovery Attack against Srp Implementations in ThE wild. , 2021, , . | | 2 |
| 114 | Time/Memory/Data Tradeoffs for Variants of the RSA Problem. Lecture Notes in Computer Science, 2013, , 651-662. | 1.0 | 1 |
| 115 | Assisted Identification of Mode of Operation in Binary Code with Dynamic Data Flow Slicing. Lecture Notes in Computer Science, 2016, , 561-579. | 1.0 | 1 |
| 116 | Fault Attacks on Efficient Pairing Implementations. , 2016, , . | | 0 |
| 117 | Statistical Properties of Short RSA Distribution and Their Cryptographic Applications. Lecture Notes in Computer Science, 2014, , 525-536. | 1.0 | 0 |
| 118 | The Long and Winding Path to Secure Implementation of GlobalPlatform SCP10. Iacr Transactions on Cryptographic Hardware and Embedded Systems, 0, , 196-218. | 0.0 | 0 |
| 119 | Cryptanalysis of the SFLASH Signature Scheme. Lecture Notes in Computer Science, 2007, , 1-4. | 1.0 | 0 |