FranÃ§ois-Xavier Standaert

List of Publications by Year
in descending order

214 papers	6,780 citations	61857 43 h-index	91712 69 g-index
221 all docs	221 docs citations	221 times ranked	2068 citing authors

#	Article	IF	Citations
1	A Unified Framework for the Analysis of Side-Channel Key Recovery Attacks. Lecture Notes in Computer Science, 2009, , 443-461.	1.0	515
2	On the Energy Cost of Communication and Cryptography in Wireless Sensor Networks. , 2008, , .		205
3	Mutual Information Analysis: aÂComprehensive Study. Journal of Cryptology, 2011, 24, 269-291.	2.1	203
4	Univariate side channel attacks and leakage modeling. Journal of Cryptographic Engineering, 2011, 1, 123-144.	1.5	146
5	Power and electromagnetic analysis: Improved model, consequences and comparisons. The Integration VLSI Journal, 2007, 40, 52-60.	1.3	139
6	SEA: A Scalable Encryption Algorithm for Small Embedded Applications. Lecture Notes in Computer Science, 2006, , 222-236.	1.0	131
7	Using Subspace-Based Template Attacks to Compare and Combine Power and Electromagnetic Information Leakages. Lecture Notes in Computer Science, 2008, , 411-425.	1.0	128
8	The World Is Not Enough: Another Look on Second-Order DPA. Lecture Notes in Computer Science, 2010, , 112-129.	1.0	128
9	Introduction to Side-Channel Attacks. Integrated Circuits and Systems, 2010, , 27-42.	0.2	127
10	A Formalization of the Security Features of Physical Functions. , 2011, , .		112
11	Shuffling against Side-Channel Attacks: A Comprehensive Study with Cautionary Note. Lecture Notes in Computer Science, 2012, , 740-757.	1.0	110
12	A Formal Study of Power Variability Issues and Side-Channel Attacks for Nanoscale Devices. Lecture Notes in Computer Science, 2011, , 109-128.	1.0	101
13	Making Masking Security Proofs Concrete. Lecture Notes in Computer Science, 2015, , 401-429.	1.0	100
14	Efficient Implementation of Rijndael Encryption in Reconfigurable Hardware: Improvements and Design Tradeoffs. Lecture Notes in Computer Science, 2003, , 334-350.	1.0	100
15	Block Ciphers That Are Easier to Mask: How Far Can We Go?. Lecture Notes in Computer Science, 2013, , 383-399.	1.0	91
16	Key-Alternating Ciphers in a Provable Setting: Encryption Using a Small Number of Public Permutations. Lecture Notes in Computer Science, 2012, , 45-62.	1.0	90
17	The Swiss-Knife RFID Distance Bounding Protocol. Lecture Notes in Computer Science, 2009, , 98-115.	1.0	87
18	LS-Designs: Bitslice Encryption for Efficient Masked Software Implementations. Lecture Notes in Computer Science, 2015, , 18-37.	1.0	81

#	Article	IF	Citations
19	Mutual Information Analysis: How, When and Why?. Lecture Notes in Computer Science, 2009, , 429-443.	1.0	81
20	An Optimal Key Enumeration Algorithm and Its Application to Side-Channel Attacks. Lecture Notes in Computer Science, 2013, , 390-406.	1.0	80
21	Fresh Re-keying: Security against Side-Channel and Fault Attacks for Low-Cost Devices. Lecture Notes in Computer Science, 2010, , 279-296.	1.0	79
22	Compact Implementation and Performance Evaluation of Block Ciphers in ATtiny Devices. Lecture Notes in Computer Science, 2012, , 172-187.	1.0	78
23	Towards Stream Ciphers for Efficient FHE with Low-Noise Ciphertexts. Lecture Notes in Computer Science, 2016, , 311-343.	1.0	78
24	Algebraic Side-Channel Attacks on the AES: Why Time also Matters in DPA. Lecture Notes in Computer Science, 2009, , 97-111.	1.0	73
25	Template Attacks vs. Machine Learning Revisited (and the Curse of Dimensionality in Side-Channel) Tj ETQq1 1 0.784314 rgBT /Overlo	1.0	72
26	A Comparative Cost/Security Analysis of Fault Attack Countermeasures. Lecture Notes in Computer Science, 2006, , 159-172.	1.0	72
27	A first step towards automatic application of power analysis countermeasures. , 2011, , .		70
28	Algebraic Side-Channel Attacks. Lecture Notes in Computer Science, 2010, , 393-410.	1.0	68
29	ICEBERG : An Involutional Cipher Efficient for Block Encryption in Reconfigurable Hardware. Lecture Notes in Computer Science, 2004, , 279-298.	1.0	67
30	From Improved Leakage Detection to the Detection of Points of Interests in Leakage Traces. Lecture Notes in Computer Science, 2016, , 240-262.	1.0	67
31	Security Evaluations beyond Computing Power. Lecture Notes in Computer Science, 2013, , 126-141.	1.0	66
32	Implementation of the AES-128 on Virtex-5 FPGAs. , 2008, , 16-26.		65
33	Leakage Resilient Cryptography in Practice. Information Security and Cryptography, 2010, , 99-134.	0.2	65
34	Partition vs. Comparison Side-Channel Distinguishers: An Empirical Evaluation of Statistical Tests for Univariate Side-Channel Attacks against Two Unprotected CMOS Devices. Lecture Notes in Computer Science, 2009, , 253-267.	1.0	64
35	On the Cost of Lazy Engineering for Masked Software Implementations. Lecture Notes in Computer Science, 2015, , 64-81.	1.0	62
36	Leftover Hash Lemma, Revisited. Lecture Notes in Computer Science, 2011, , 1-20.	1.0	61

#	Article	IF	Citations
37	Soft Analytical Side-Channel Attacks. Lecture Notes in Computer Science, 2014, , 282-296.	1.0	58
38	Parallel Implementations of Masking Schemes and the Bounded Moment Leakage Model. Lecture Notes in Computer Science, 2017, , 535-566.	1.0	57
39	Towards Green Cryptography: A Comparison of Lightweight Ciphers from the Energy Viewpoint. Lecture Notes in Computer Science, 2012, , 390-407.	1.0	57
40	How to Certify the Leakage of a Chip?. Lecture Notes in Computer Science, 2014, , 459-476.	1.0	57
41	Improved Higher-Order Side-Channel Attacks with FPGA Experiments. Lecture Notes in Computer Science, 2005, , 309-323.	1.0	55
42	Simple Key Enumeration (and Rank Estimation) Using Histograms: An Integrated Approach. Lecture Notes in Computer Science, 2016, , 61-81.	1.0	52
43	A Framework for the Analysis and Evaluation of Algebraic Fault Attacks on Lightweight Block Ciphers. IEEE Transactions on Information Forensics and Security, 2016, 11, 1039-1054.	4.5	51
44	Gimli : A Cross-Platform Permutation. Lecture Notes in Computer Science, 2017, , 299-320.	1.0	51
45	Simpler and More Efficient Rank Estimation for Side-Channel Security Assessment. Lecture Notes in Computer Science, 2015, , 117-129.	1.0	49
46	Composable Masking Schemes in the Presence of Physical Defaults & the Robust Probing Model. Iacr Transactions on Cryptographic Hardware and Embedded Systems, 0, , 89-120.	0.0	48
47	How to Compare Profiled Side-Channel Attacks?. Lecture Notes in Computer Science, 2009, , 485-498.	1.0	44
48	A block cipher based pseudo random number generator secure against side-channel key recovery. , 2008, , .		43
49	The Myth of Generic DPAâ€¦and the Magic of Learning. Lecture Notes in Computer Science, 2014, , 183-205.	1.0	43
50	Information Theoretic Evaluation of Side-Channel Resistant Logic Styles. Lecture Notes in Computer Science, 2007, , 427-442.	1.0	43
51	Leakage-Resilient Authentication and Encryption from Symmetric Cryptographic Primitives. , 2015, , .		42
52	Power Analysis of an FPGA. Lecture Notes in Computer Science, 2004, , 30-44.	1.0	41
53	A Design Flow and Evaluation Framework for DPA-Resistant Instruction Set Extensions. Lecture Notes in Computer Science, 2009, , 205-219.	1.0	41
54	Compact FPGA Implementations of the Five SHA-3 Finalists. Lecture Notes in Computer Science, 2011, , 217-233.	1.0	40

#	ARTICLE	IF	CITATIONS
55	A Tutorial on Physical Security and Side-Channel Attacks. Lecture Notes in Computer Science, 2005, , 78-108.	1.0	40
56	Leakage-Resilient Symmetric Cryptography under Empirically Verifiable Assumptions. Lecture Notes in Computer Science, 2013, , 335-352.	1.0	38
57	FPGA Implementation(s) of a Scalable Encryption Algorithm. IEEE Transactions on Very Large Scale Integration (VLSI) Systems, 2008, 16, 212-216.	2.1	37
58	Leakage Detection with the x2-Test. Iacr Transactions on Cryptographic Hardware and Embedded Systems, 0, , 209-237.	0.0	37
59	Power Analysis of FPGAs: How Practical Is the Attack?. Lecture Notes in Computer Science, 2003, , 701-710.	1.0	35
60	Trivially and Efficiently Composing Masked Gadgets With Probe Isolating Non-Interference. IEEE Transactions on Information Forensics and Security, 2020, 15, 2542-2555.	4.5	35
61	maskVerif: Automated Verification of Higher-Order Masking in Presence of Physical Defaults. Lecture Notes in Computer Science, 2019, , 300-318.	1.0	35
62	Side-Channel Attacks from Static Power: When Should We Care?. , 2015, , .		34
63	Power Analysis Attacks Against FPGA Implementations of the DES. Lecture Notes in Computer Science, 2004, , 84-94.	1.0	33
64	Generic Side-Channel Distinguishers: Improvements and Limitations. Lecture Notes in Computer Science, 2011, , 354-372.	1.0	32
65	TemplateÂattacksÂversusÂmachineÂlearningÂrevisited andÂtheÂcurseÂofÂdimensionalityÂinÂside-channelÂanalysis: extended version. Journal of Cryptographic Engineering, 2018, 8, 301-313.	1.5	32
66	Automatic Application of Power Analysis Countermeasures. IEEE Transactions on Computers, 2015, 64, 329-341.	2.4	31
67	A methodology to implement block ciphers in reconfigurable hardware and its application to fast and compact AES RIJNDAEL. , 2003, , .		30
68	How to strongly link data and its medium: the paper case. IET Information Security, 2010, 4, 125.	1.1	29
69	Harvesting the potential of nano-CMOS for lightweight cryptography: an ultra-low-voltage 65Ânm AES coprocessor for passive RFID tags. Journal of Cryptographic Engineering, 2011, 1, 79-86.	1.5	29
70	Moments-Correlating DPA. , 2016, , .		29
71	Making Masking Security Proofs Concrete (Or How to Evaluate the Security of Any Leaking Device), Extended Version. Journal of Cryptology, 2019, 32, 1263-1297.	2.1	29
72	Hardware Private Circuits: From Trivial Composition to Full Verification. IEEE Transactions on Computers, 2021, 70, 1677-1690.	2.4	29

#	Article	IF	Citations
73	Algebraic Side-Channel Attacks Beyond the Hamming Weight Leakage Model. Lecture Notes in Computer Science, 2012, , 140-154.	1.0	29
74	Very High Order Masking: Efficient Implementation and Security Evaluation. Lecture Notes in Computer Science, 2017, , 623-643.	1.0	28
75	Small Tweaks Do Not Help: Differential Power Analysis of MILENAGE Implementations in 3G/4G USIM Cards. Lecture Notes in Computer Science, 2015, , 468-480.	1.0	27
76	Towards Super-Exponential Side-Channel Security with Efficient Leakage-Resilient PRFs. Lecture Notes in Computer Science, 2012, , 193-212.	1.0	27
77	Efficient Removal of Random Delays from Embedded Software Implementations Using Hidden Markov Models. Lecture Notes in Computer Science, 2013, , 123-140.	1.0	27
78	Glitch-Resistant Masking Revisited. Iacr Transactions on Cryptographic Hardware and Embedded Systems, 0, , 256-292.	0.0	27
79	Efficient uses of FPGAs for implementations of DES and its experimental linear cryptanalysis. IEEE Transactions on Computers, 2003, 52, 473-482.	2.4	25
80	Ridge-Based DPA: Improvement of Differential Power Analysis For Nanoscale Chips. IEEE Transactions on Information Forensics and Security, 2018, 13, 1301-1316.	4.5	25
81	Efficient Masked S-Boxes Processing â€" A Step Forward â€". Lecture Notes in Computer Science, 2014, , 251-266.	1.0	25
82	Information Theoretic and Security Analysis of a 65-Nanometer DDSLL AES S-Box. Lecture Notes in Computer Science, 2011, , 223-239.	1.0	25
83	On Leakage-Resilient Authenticated Encryption with Decryption Leakages. IACR Transactions on Symmetric Cryptology, 0, , 271-293.	0.0	25
84	Stealthy Compromise of Wireless Sensor Nodes with Power Analysis Attacks. Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, 2010, , 229-242.	0.2	24
85	Compact Implementation and Performance Evaluation of Hash Functions in ATtiny Devices. Lecture Notes in Computer Science, 2013, , 158-172.	1.0	24
86	How (Not) to Use Welchâ€™s T-Test in Side-Channel Security Evaluations. Lecture Notes in Computer Science, 2019, , 65-79.	1.0	23
87	Deep learning mitigates but does not annihilate the need of aligned traces and a generalized ResNet model for side-channel attacks. Journal of Cryptographic Engineering, 2020, 10, 85-95.	1.5	23
88	Towards Fresh and Hybrid Re-Keying Schemes with Beyond Birthday Security. Lecture Notes in Computer Science, 2016, , 225-241.	1.0	23
89	Fresh Re-keying II: Securing Multiple Parties against Side-Channel and Fault Attacks. Lecture Notes in Computer Science, 2011, , 115-132.	1.0	23
90	Consolidating Inner Product Masking. Lecture Notes in Computer Science, 2017, , 724-754.	1.0	22

#	Article	IF	Citations
91	Leakage Certification Revisited: Bounding Model Errors in Side-Channel Security Evaluations. Lecture Notes in Computer Science, 2019, , 713-737.	1.0	22
92	Blind Source Separation from Single Measurements Using Singular Spectrum Analysis. Lecture Notes in Computer Science, 2015, , 42-59.	1.0	21
93	Practical Leakage-Resilient Pseudorandom Objects with Minimum Public Randomness. Lecture Notes in Computer Science, 2013, , 223-238.	1.0	21
94	Masking and leakage-resilient primitives: One, the other(s) or both?. Cryptography and Communications, 2015, 7, 163-184.	0.9	20
95	Low Entropy Masking Schemes, Revisited. Lecture Notes in Computer Science, 2014, , 33-43.	1.0	20
96	Unified and Optimized Linear Collision Attacks and Their Application in a Non-profiled Setting. Lecture Notes in Computer Science, 2012, , 175-192.	1.0	20
97	Masking vs. Multiparty Computation: How Large Is the Gap for AES?. Lecture Notes in Computer Science, 2013, , 400-416.	1.0	19
98	Improving the security and efficiency of block ciphers based on LS-designs. Designs, Codes, and Cryptography, 2017, 82, 495-509.	1.0	19
99	Improved Filter Permutators for Efficient FHE: Better Instances and Implementations. Lecture Notes in Computer Science, 2019, , 68-91.	1.0	19
100	Adaptive Chosen-Message Side-Channel Attacks. Lecture Notes in Computer Science, 2010, , 186-199.	1.0	19
101	Spook: Sponge-Based Leakage-Resistant Authenticated Encryption with a Masked Tweakable Block Cipher. IACR Transactions on Symmetric Cryptology, 0, , 295-349.	0.0	19
102	Masking vs. multiparty computation: how large is the gap for AES?. Journal of Cryptographic Engineering, 2014, 4, 47-57.	1.5	17
103	Private Circuits III. , 2016, , .		17
104	Towards Sound and Optimal Leakage Detection Procedure. Lecture Notes in Computer Science, 2018, , 105-122.	1.0	17
105	Efficient Selection of Time Samples for Higher-Order DPA with Projection Pursuits. Lecture Notes in Computer Science, 2015, , 34-50.	1.0	17
106	Experiments on the Multiple Linear Cryptanalysis of Reduced Round Serpent. Lecture Notes in Computer Science, 2008, , 382-397.	1.0	17
107	ASCA, SASCA and DPA with Enumeration: Which One Beats the Other and When?. Lecture Notes in Computer Science, 2015, , 291-312.	1.0	17
108	Exploiting the Incomplete Diffusion Feature: A Specialized Analytical Side-Channel Attack Against the AES and Its Application to Microcontroller Implementations. IEEE Transactions on Information Forensics and Security, 2014, 9, 999-1014.	4.5	16

#	Article	IF	Citations
109	Mode-Level vs. Implementation-Level Physical Security in Symmetric Cryptography. Lecture Notes in Computer Science, 2020, , 369-400.	1.0	16
110	Comparing Approaches to Rank Estimation for Side-Channel Security Evaluations. Lecture Notes in Computer Science, 2016, , 125-142.	1.0	16
111	On the Need of Physical Security for Small Embedded Devices: A Case Study with COMP128-1 Implementations in SIM Cards. Lecture Notes in Computer Science, 2013, , 230-238.	1.0	16
112	Towards Sound Fresh Re-keying with Hard (Physical) Learning Problems. Lecture Notes in Computer Science, 2016, , 272-301.	1.0	16
113	Reducing a Masked Implementationâ€™s Effective Security Order with Setup Manipulations. Iacr Transactions on Cryptographic Hardware and Embedded Systems, 0, , 293-317.	0.0	16
114	Scaling trends of the AES S-box low power consumption in 130 and 65 nm CMOS technology nodes. , 2009, , .		15
115	Design Strategies and Modified Descriptions to Optimize Cipher FPGA Implementations: Fast and Compact Results for DES and Triple-DES. Lecture Notes in Computer Science, 2003, , 181-193.	1.0	15
116	Exploring the Feasibility of Low Cost Fault Injection Attacks on Sub-threshold Devices through an Example of a 65nm AES Implementation. Lecture Notes in Computer Science, 2012, , 48-60.	1.0	14
117	Analysis and experimental evaluation of image-based PUFs. Journal of Cryptographic Engineering, 2012, 2, 189-206.	1.5	14
118	Intellectual property protection for FPGA designs with soft physical hash functions: First experimental results. , 2013, , .		14
119	A Systematic Approach to the Side-Channel Analysis of ECC Implementations with Worst-Case Horizontal Attacks. Lecture Notes in Computer Science, 2017, , 534-554.	1.0	14
120	Unified and optimized linear collision attacks and their application in a non-profiled setting: extended version. Journal of Cryptographic Engineering, 2013, 3, 45-58.	1.5	13
121	Masking Proofs Are Tight and How to Exploit it in Security Evaluations. Lecture Notes in Computer Science, 2018, , 385-412.	1.0	13
122	Ask Less, Get More: Side-Channel Signal Hiding, Revisited. IEEE Transactions on Circuits and Systems I: Regular Papers, 2020, 67, 4904-4917.	3.5	13
123	A Design Methodology for Secured ICs Using Dynamic Current Mode Logic. Lecture Notes in Computer Science, 2005, , 550-560.	1.0	13
124	Hardware Implementation and Side-Channel Analysis of Lapin. Lecture Notes in Computer Science, 2014, , 206-226.	1.0	12
125	Towards fresh re-keying with leakage-resilient PRFs: cipher design principles and analysis. Journal of Cryptographic Engineering, 2014, 4, 157.	1.5	12
126	Towards Easy Leakage Certification. Lecture Notes in Computer Science, 2016, , 40-60.	1.0	12

#	Article	IF	Citations
127	A Combined Design-Time/Test-Time Study of the Vulnerability of Sub-Threshold Devices to Low Voltage Fault Attacks. IEEE Transactions on Emerging Topics in Computing, 2014, 2, 107-118.	3.2	11
128	Breaking Masked Implementations with Many Shares on 32-bit Software Platforms. Iacr Transactions on Cryptographic Hardware and Embedded Systems, 0, , 202-234.	0.0	11
129	A Systematic Appraisal of Side Channel Evaluation Strategies. Lecture Notes in Computer Science, 2020, , 46-66.	1.0	11
130	Connecting and Improving Direct Sum Masking and Inner Product Masking. Lecture Notes in Computer Science, 2018, , 123-141.	1.0	10
131	Inner Product Masking for Bitslice Ciphers and Security Order Amplification for Linear Leakages. Lecture Notes in Computer Science, 2017, , 174-191.	1.0	10
132	Towards Low-Energy Leakage-Resistant Authenticated Encryption from the Duplex Sponge Construction. IACR Transactions on Symmetric Cryptology, 0, , 6-42.	0.0	10
133	Extractors against side-channel attacks: weak or strong?. Journal of Cryptographic Engineering, 2011, 1, 231-241.	1.5	9
134	Understanding the limitations and improving the relevance of SPICE simulations in side-channel security evaluations. Journal of Cryptographic Engineering, 2014, 4, 187-195.	1.5	9
135	Ciphertext Integrity with Misuse and Leakage. , 2018, , .		9
136	Authenticated Encryption with Nonce Misuse and Physical Leakage: Definitions, Separation Results and First Construction. Lecture Notes in Computer Science, 2019, , 150-172.	1.0	9
137	Systematic Construction and Comprehensive Evaluation of Kolmogorov-Smirnov Test Based Side-Channel Distinguishers. Lecture Notes in Computer Science, 2013, , 336-352.	1.0	9
138	Multi-Tuple Leakage Detection and the Dependent Signal Issue. Iacr Transactions on Cryptographic Hardware and Embedded Systems, 0, , 318-345.	0.0	9
139	TEDT, a Leakage-Resist AEAD Mode for High Physical Security Applications. Iacr Transactions on Cryptographic Hardware and Embedded Systems, 0, , 256-320.	0.0	9
140	FPGA Implementations of SPRING. Lecture Notes in Computer Science, 2014, , 414-432.	1.0	8
141	Scaling Trends for Dual-Rail Logic Styles Against Side-Channel Attacks: A Case-Study. Lecture Notes in Computer Science, 2017, , 19-33.	1.0	8
142	Start Simple and then Refine: Bias-Variance Decomposition as a Diagnosis Tool for Leakage Profiling. IEEE Transactions on Computers, 2018, 67, 268-283.	2.4	8
143	Score-Based vs. Probability-Based Enumeration â€“ A Cautionary Note. Lecture Notes in Computer Science, 2016, , 137-152.	1.0	8
144	Secure Multiplication for Bitslice Higher-Order Masking: Optimisation andÂComparison. Lecture Notes in Computer Science, 2018, , 3-22.	1.0	8

#	Article	IF	Citations
145	Intellectual Property Protection for Integrated Systems Using Soft Physical Hash Functions. Lecture Notes in Computer Science, 2012, , 208-225.	1.0	8
146	Design strategies and modified descriptions to optimize cipher FPGA implementations. , 2003, , .		7
147	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
148	Automated news recommendation in front of adversarial examples and the technical limits of transparency in algorithmic accountability. AI and Society, 2022, 37, 67-80.	3.1	7
149	Masking with Randomized Look Up Tables. Lecture Notes in Computer Science, 2012, , 283-299.	1.0	7
150	Taylor Expansion of Maximum Likelihood Attacks for Masked and Shuffled Implementations. Lecture Notes in Computer Science, 2016, , 573-601.	1.0	7
151	Towards Globally Optimized Masking: From Low Randomness to Low Noise Rate. Iacr Transactions on Cryptographic Hardware and Embedded Systems, 0, , 162-198.	0.0	7
152	Randomly driven fuzzy key extraction of unclonable images. , 2010, , .		6
153	Glitch-induced within-die variations of dynamic energy in voltage-scaled nano-CMOS circuits. , 2010, , .		6
154	Ridge-Based Profiled Differential Power Analysis. Lecture Notes in Computer Science, 2017, , 347-362.	1.0	6
155	Towards easy leakage certification: extended version. Journal of Cryptographic Engineering, 2017, 7, 129-147.	1.5	6
156	Side-channel attacks against the human brain: the PIN code case study (extended version). Brain Informatics, 2018, 5, 12.	1.8	6
157	Beyond algorithmic noise or how to shuffle parallel implementations?. International Journal of Circuit Theory and Applications, 2020, 48, 674-695.	1.3	6
158	Towards Tight Random Probing Security. Lecture Notes in Computer Science, 2021, , 185-214.	1.0	6
159	Low Entropy Masking Schemes, Revisited. Lecture Notes in Computer Science, 2014, , 33-43.	1.0	6
160	Unknown-Input Attacks in the Parallel Setting: Improving the Security of the CHES 2012 Leakage-Resilient PRF. Lecture Notes in Computer Science, 2016, , 602-623.	1.0	6
161	Efficient Profiled Side-Channel Analysis of Masked Implementations, Extended. IEEE Transactions on Information Forensics and Security, 2022, 17, 574-584.	4.5	6
162	Implementing Trojan-Resilient Hardware from (Mostly) Untrusted Components Designed by Colluding Manufacturers. , 2018, , .		5

#	Article	IF	Citations
163	Multi-trail Statistical Saturation Attacks. Lecture Notes in Computer Science, 2010, , 123-138.	1.0	5
164	Analysis of Dynamic Differential Swing Limited Logic for Low-Power Secure Applications. Journal of Low Power Electronics and Applications, 2012, 2, 98-126.	1.3	4
165	A Survey of Recent Results in FPGA Security and Intellectual Property Protection. , 2014, , 201-224.		4
166	Provable Order Amplification for Code-Based Masking: How to Avoid Non-Linear Leakages Due to Masked Operations. IEEE Transactions on Information Forensics and Security, 2019, 14, 3069-3082.	4.5	4
167	Towards Securing Low-Power Digital Circuits with Ultra-Low-Voltage Vdd Randomizers. Lecture Notes in Computer Science, 2016, , 233-248.	1.0	4
168	Side-Channel Attacks Against the Human Brain: The PIN Code Case Study. Lecture Notes in Computer Science, 2017, , 171-189.	1.0	4
169	Bridging the Gap: Advanced Tools for Side-Channel Leakage Estimation Beyond Gaussian Templates and Histograms. Lecture Notes in Computer Science, 2017, , 58-78.	1.0	4
170	Security Analysis of Image-Based PUFs for Anti-counterfeiting. Lecture Notes in Computer Science, 2012, , 26-38.	1.0	4
171	Evaluation and Improvement of Generic-Emulating DPA Attacks. Lecture Notes in Computer Science, 2015, , 416-432.	1.0	4
172	Extractors against Side-Channel Attacks: Weak or Strong?. Lecture Notes in Computer Science, 2011, , 256-272.	1.0	4
173	Combining Leakage-Resilient PRFs and Shuffling. Lecture Notes in Computer Science, 2015, , 122-136.	1.0	4
174	Reducing the Cost of Authenticity with Leakages: a $$mathsf {CIML2}$$ -Secure $$mathsf {AE}$$ Scheme with One Call to a Strongly Protected Tweakable Block Cipher. Lecture Notes in Computer Science, 2019, , 229-249.	1.0	4
175	Side-Channel Countermeasuresâ€™ Dissection and the Limits of Closed Source Security Evaluations. Iacr Transactions on Cryptographic Hardware and Embedded Systems, 0, , 1-25.	0.0	4
176	Security Analysis of Deterministic Re-keying with Masking and Shuffling: Application to ISAP. Lecture Notes in Computer Science, 2021, , 168-183.	1.0	4
177	Demonstrating an LPPN Processor. , 2018, , .		3
178	A security oriented transient-noise simulation methodology: Evaluation of intrinsic physical noise of cryptographic designs. The Integration VLSI Journal, 2019, 68, 71-79.	1.3	3
179	Learning with Physical Noise or Errors. IEEE Transactions on Dependable and Secure Computing, 2020, 17, 957-971.	3.7	3
180	How to fool a black box machine learning based side-channel security evaluation. Cryptography and Communications, 2021, 13, 573-585.	0.9	3

#	Article	IF	Citations
181	An Analysis of the Learning Parity with Noise Assumption Against Fault Attacks. Lecture Notes in Computer Science, 2017, , 245-264.	1.0	3
182	Secure and Efficient Implementation of Symmetric Encryption Schemes using FPGAs. , 2009, , 295-320.		2
183	Letâ€™s make it Noisy: A Simulation Methodology for adding Intrinsic Physical Noise to Cryptographic Designs. , 2018, , .		2
184	Fast Side-Channel Security Evaluation of ECC Implementations. Lecture Notes in Computer Science, 2019, , 25-42.	1.0	2
185	On the Security of Off-the-Shelf Microcontrollers: Hardware IsÂNotÂEnough. Lecture Notes in Computer Science, 2021, , 103-118.	1.0	2
186	SpookChain: Chaining a Sponge-Based AEAD with Beyond-Birthday Security. Lecture Notes in Computer Science, 2019, , 67-85.	1.0	2
187	Towards Fair and Efficient Evaluations of Leaking Cryptographic Devices. Lecture Notes in Computer Science, 2016, , 353-362.	1.0	2
188	Getting the Most Out of Leakage Detection. Lecture Notes in Computer Science, 2017, , 264-281.	1.0	2
189	Packed Multiplication: How to Amortize the Cost of Side-Channel Masking?. Lecture Notes in Computer Science, 2020, , 851-880.	1.0	2
190	Strong Authenticity with Leakage Under Weak and Falsifiable Physical Assumptions. Lecture Notes in Computer Science, 2020, , 517-532.	1.0	2
191	Efficient Leakage-Resilient MACs Without Idealized Assumptions. Lecture Notes in Computer Science, 2021, , 95-123.	1.0	2
192	Fully-Digital Randomization Based Side-Channel Securityâ€"Toward Ultra-Low Cost-per-Security. IEEE Access, 2022, 10, 68440-68449.	2.6	2
193	Provable security of block ciphers against linear cryptanalysis: a mission impossible?. Designs, Codes, and Cryptography, 2009, 50, 325-338.	1.0	1
194	Fidelity Leakages: Applying Membership Inference Attacks to Preference Data. , 2020, , .		1
195	Side-channel analysis of a learning parity with physical noise processor. Journal of Cryptographic Engineering, 2021, 11, 171-179.	1.5	1
196	Reducing risks through simplicity: high side-channel security for lazy engineers. Journal of Cryptographic Engineering, 2021, 11, 39-55.	1.5	1
197	MOE: Multiplication Operated Encryption with Trojan Resilience. IACR Transactions on Symmetric Cryptology, 0, , 78-129.	0.0	1
198	Support Vector Machines for Improved IP Detection with Soft Physical Hash Functions. Lecture Notes in Computer Science, 2014, , 112-128.	1.0	1

#	Article	IF	Citations
199	Key Enumeration from the Adversarial Viewpoint. Lecture Notes in Computer Science, 2020, , 252-267.	1.0	1
200	On the Worst-Case Side-Channel Security of ECC Point Randomization in Embedded Devices. Lecture Notes in Computer Science, 2020, , 205-227.	1.0	1
201	Time-memory tradeoffs. , 2005, , 614-616.		1
202	Towards a Better Understanding of Side-Channel Analysis Measurements Setups. Lecture Notes in Computer Science, 2022, , 64-79.	1.0	1
203	Automatic and Manual Detection of Generated News: Case Study, Limitations and Challenges. , 2022, , .		1
204	On a Particular Case of the Bisymmetric Equation for Quasigroups. Acta Mathematica Hungarica, 2014, 143, 330-336.	0.3	0
205	A Transient Noise Analysis of Secured Dual-Rail Based Logic Style. , 2018, , .		0
206	A stealthy Hardware Trojan based on a Statistical Fault Attack. Cryptography and Communications, 2021, 13, 587-600.	0.9	0
207	Scatter: a Missing Case?. Lecture Notes in Computer Science, 2021, , 90-103.	1.0	0
208	Post-Quantum Cryptography: Challenges and Opportunities for Robust and Secure HW Design. , 2021, , .		0
209	On The Security of the DeKaRT Primitive. International Federation for Information Processing, 2004, , 241-254.	0.4	0
210	Physical Security. , 2011, , 928-929.		0
211	Time-Memory Trade-offs. , 2011, , 1297-1299.		0
212	From New Technologies to New Solutions. Lecture Notes in Computer Science, 2014, , 16-29.	1.0	0
213	On the Impacts of Mathematical Realization over Practical Security of Leakage Resilient Cryptographic Schemes. Lecture Notes in Computer Science, 2015, , 469-484.	1.0	0
214	Tight-ES-TRNG: Improved Construction and Robustness Analysis. SN Computer Science, 2022, 3, .	2.3	0