Ingrid M Verbauwhede

List of Publications by Year
in descending order

411 papers	11,440 citations	53751 45 h-index	71651 76 g-index
423 all docs	423 docs citations	423 times ranked	4489 citing authors

#	Article	IF	Citations
1	TROT: A Three-Edge Ring Oscillator Based True Random Number Generator With Time-to-Digital Conversion. IEEE Transactions on Circuits and Systems I: Regular Papers, 2022, 69, 2435-2448.	3.5	15
2	Hardware Security: Physical Design versus Side-Channel and Fault Attacks. , 2022, , .		0
3	DATE 2022: Aiming for an Online/ Onsite Format and Finally Moving to Online Only. IEEE Design and Test, 2022, 39, 90-93.	1.1	0
4	Trust in FPGA-accelerated Cloud Computing. ACM Computing Surveys, 2021, 53, 1-28.	16.1	21
5	Exploring Micro-architectural Side-Channel Leakages through Statistical Testing. , 2021, , .		0
6	A Side-Channel-Resistant Implementation of SABER. ACM Journal on Emerging Technologies in Computing Systems, 2021, 17, 1-26.	1.8	30
7	Design and Analysis of Configurable Ring Oscillators for True Random Number Generation Based on Coherent Sampling. ACM Transactions on Reconfigurable Technology and Systems, 2021, 14, 1-20.	1.9	3
8	Prime+Scope. , 2021, , .		21
9	Lattice-Based Public-Key Cryptography in Hardware. Computer Architecture and Design Methodologies, 2020, , .	0.5	1
10	Design and Evaluation of a Spark Gap Based EM-fault Injection Setup. , 2020, , .		2
11	Sweeping for Leakage in Masked Circuit Layouts. , 2020, , .		1
12	Compact domain-specific co-processor for accelerating module lattice-based KEM. , 2020, , .		6
13	Attacking Hardware Random Number Generators in a Multi-Tenant Scenario. , 2020, , .		3
14	HEAWS: An Accelerator for Homomorphic Encryption on the Amazon AWS FPGA. IEEE Transactions on Computers, 2020, , 1-1.	2.4	39
15	Towards efficient and automated side-channel evaluations at design time. Journal of Cryptographic Engineering, 2020, 10, 305-319.	1.5	11
16	Coprocessor for Koblitz Curves. Computer Architecture and Design Methodologies, 2020, , 25-42.	0.5	0
17	Discrete Gaussian Sampling. Computer Architecture and Design Methodologies, 2020, , 43-63.	0.5	0
18	Design Considerations for EM Pulse FaultÂInjection. Lecture Notes in Computer Science, 2020, , 176-192.	1.0	3

#	Article	IF	Citations
19	Atlas: Application Confidentiality in Compromised Embedded Systems. IEEE Transactions on Dependable and Secure Computing, 2019, 16, 415-423.	3.7	3
20	EM Information Security Threats Against RO-Based TRNGs: The Frequency Injection Attack Based on IEMI and EM Information Leakage. IEEE Transactions on Electromagnetic Compatibility, 2019, 61, 1122-1128.	1.4	15
21	A Physically Unclonable Function Using Soft Oxide Breakdown Featuring 0% Native BER and 51.8 fJ/bit in 40-nm CMOS. IEEE Journal of Solid-State Circuits, 2019, 54, 2765-2776.	3.5	45
22	A Self-Calibrating True Random Number Generator. , 2019, , .		1
23	A Highly-Portable True Random Number Generator Based on Coherent Sampling. , 2019, , .		18
24	A Lightweight 1.16 pJ/bit Processor for the Authenticated Encryption Scheme KetjeSR. , 2019, , .		0
25	Pushing the speed limit of constant-time discrete Gaussian sampling. A case study on the Falcon signature scheme. , 2019, , .		17
26	Design Principles for True Random Number Generators for Security Applications. , 2019, , .		3
27	Compact and Flexible FPGA Implementation of Ed25519 and X25519. Transactions on Embedded Computing Systems, 2019, 18, 1-21.	2.1	23
28	Decryption Failure Attacks on IND-CCA Secure Lattice-Based Schemes. Lecture Notes in Computer Science, 2019, , 565-598.	1.0	26
29	FPGA-Based High-Performance Parallel Architecture for Homomorphic Computing on Encrypted Data. , 2019, , .		49
30	Security and reliability â€“ friend or foe. , 2019, , .		1
31	Hardware-Efficient Post-Processing Architectures for True Random Number Generators. IEEE Transactions on Circuits and Systems II: Express Briefs, 2019, 66, 1242-1246.	2.2	6
32	Single-Round Pattern Matching Key Generation Using Physically Unclonable Function. Security and Communication Networks, 2019, 2019, 1-13.	1.0	4
33	The Impact of Error Dependencies on Ring/Mod-LWE/LWR Based Schemes. Lecture Notes in Computer Science, 2019, , 103-115.	1.0	20
34	An In-Depth and Black-Box Characterization of the Effects of Laser Pulses on ATmega328P. Lecture Notes in Computer Science, 2019, , 156-170.	1.0	10
35	Propagating trusted execution through mutual attestation. , 2019, , .		2
36	Characterization of EM faults on ATmega328p. , 2019, , .		6

#	Article	IF	Citations
37	The Need for Hardware Roots of Trust. , 2019, , .		1
38	Arithmetic of $$au $$ ï„ -adic expansions for lightweight Koblitz curve cryptography. Journal of Cryptographic Engineering, 2018, 8, 285-300.	1.5	2
39	Private Mobile Pay-TV From Priced Oblivious Transfer. IEEE Transactions on Information Forensics and Security, 2018, 13, 280-291.	4.5	8
40	EE2: Workshop on circuits for social good. , 2018, , .		0
41	Towards inter-vendor compatibility of true random number generators for FPGAs. , 2018, , .		0
42	F1: Intelligent energy-efficient systems at the edge of IoT. , 2018, , .		1
43	X-Ray and Proton Radiation Effects on 40 nm CMOS Physically Unclonable Function Devices. IEEE Transactions on Nuclear Science, 2018, 65, 1519-1524.	1.2	9
44	HEPCloud: An FPGA-based Multicore Processor for FV Somewhat Homomorphic Function Evaluation. IEEE Transactions on Computers, 2018, , 1-1.	2.4	31
45	Constant-Time Discrete Gaussian Sampling. IEEE Transactions on Computers, 2018, 67, 1561-1571.	2.4	39
46	Hardware-Based Trusted Computing Architectures for Isolation and Attestation. IEEE Transactions on Computers, 2018, 67, 361-374.	2.4	91
47	A Physically Unclonable Function with 0% BER Using Soft Oxide Breakdown in 40nm CMOS. , 2018, , .		5
48	Teaching HW/SW codesign with a Zynq ARM/FPGA SoC. , 2018, , .		3
49	The Impact of Pulsed Electromagnetic Fault Injection on True Random Number Generators. , 2018, , .		6
50	A multi-bit/cell PUF using analog breakdown positions in CMOS. , 2018, , .		10
51	Design and testing methodologies for true random number generators towards industry certification. , 2018, , .		10
52	Introduction to EM information security for IoT devices. , 2018, , .		1
53	Detection of IEMI fault injection using voltage monitor constructed with fully digital circuit. , 2018, , .		5
54	Comparison of two setups for contactless power measurements for side-channel analysis. , 2018, , .		1

#	Article	IF	Citations
55	Fundamental study on non-invasive frequency injection attack against RO-based TRNG. , 2018, , .		1
56	A Closer Look at the Delay-Chain based TRNG. , 2018, , .		5
57	SOFIA: Software and control flow integrity architecture. Computers and Security, 2017, 68, 16-35.	4.0	30
58	A 5.1Î¼J per pointâ€multiplication elliptic curve cryptographic processor. International Journal of Circuit Theory and Applications, 2017, 45, 170-187.	1.3	6
59	Dude, is my code constant time?. , 2017, , .		39
60	Hardware Assisted Fully Homomorphic Function Evaluation and Encrypted Search. IEEE Transactions on Computers, 2017, 66, 1562-1572.	2.4	21
61	Lightweight Prediction-Based Tests for On-Line Min-Entropy Estimation. IEEE Embedded Systems Letters, 2017, 9, 45-48.	1.3	2
62	High-Performance Ideal Lattice-Based Cryptography on 8-Bit AVR Microcontrollers. Transactions on Embedded Computing Systems, 2017, 16, 1-24.	2.1	14
63	Sancus 2.0. ACM Transactions on Privacy and Security, 2017, 20, 1-33.	2.2	61
64	STBC: Side Channel Attack Tolerant Balanced Circuit with Reduced Propagation Delay. , 2017, , .		4
65	LiBrA-CAN. Transactions on Embedded Computing Systems, 2017, 16, 1-28.	2.1	31
66	SCM. , 2017, , .		2
67	Elliptic Curve Cryptography with Efficiently Computable Endomorphisms and Its Hardware Implementations for the Internet of Things. IEEE Transactions on Computers, 2017, 66, 773-785.	2.4	49
68	Security Adds an Extra Dimension to IC Design: Future IC Design Must Focus on Security in Addition to Low Power and Energy. IEEE Solid-State Circuits Magazine, 2017, 9, 41-45.	0.5	9
69	The Monte Carlo PUF. , 2017, , .		1
70	Physically unclonable function using CMOS breakdown position. , 2017, , .		15
71	SSCS AdCom Member-at-Large Ingrid Verbauwhede Receives IEEE Computer Society 2017 Technical Achievement Award [IEEE News]. IEEE Solid-State Circuits Magazine, 2017, 9, 94-94.	0.5	0
72	On-chip jitter measurement for true random number generators. , 2017, , .		11

#	Article	IF	Citations
73	Fast Leakage Assessment. Lecture Notes in Computer Science, 2017, , 387-399.	1.0	15
74	Hold Your Breath, PRIMATEs Are Lightweight. Lecture Notes in Computer Science, 2017, , 197-216.	1.0	0
75	Providing security on demand using invasive computing. IT - Information Technology, 2016, 58, 281-295.	0.6	4
76	Iterating Von Neumann's post-processing under hardware constraints. , 2016, , .		8
77	Exploring active manipulation attacks on the TERO random number generator. , 2016, , .		12
78	On the Feasibility of Cryptography for a Wireless Insulin Pump System. , 2016, , .		23
79	Ring-LWE: Applications to Cryptography and Their Efficient Realization. Lecture Notes in Computer Science, 2016, , 323-331.	1.0	2
80	Binary decision diagram to design balanced secure logic styles. , 2016, , .		1
81	Upper bounds on the min-entropy of RO Sum, Arbiter, Feed-Forward Arbiter, and S-ArbRO PUFs. , 2016, , .		6
82	VLSI Design Methods for Low Power Embedded Encryption. , 2016, , .		4
83	Masking ring-LWE. Journal of Cryptographic Engineering, 2016, 6, 139-153.	1.5	24
84	A Lockdown Technique to Prevent Machine Learning on PUFs for Lightweight Authentication. IEEE Transactions on Multi-Scale Computing Systems, 2016, 2, 146-159.	2.5	142
85	A Fast and Compact FPGA Implementation of Elliptic Curve Cryptography Using Lambda Coordinates. Lecture Notes in Computer Science, 2016, , 63-83.	1.0	2
86	Hardware acceleration of a software-based VPN. , 2016, , .		4
87	IoT: Source of test challenges. , 2016, , .		21
88	A Tiny Coprocessor for Elliptic Curve Cryptography over the 256-bit NIST Prime Field. , 2016, , .		6
89	Embedded Security. , 2016, , .		1
90	Additively Homomorphic Ring-LWE Masking. Lecture Notes in Computer Science, 2016, , 233-244.	1.0	28

#	Article	IF	Citations
91	Single-Cycle Implementations of Block Ciphers. Lecture Notes in Computer Science, 2016, , 131-147.	1.0	19
92	Design and Implementation of a Waveform-Matching Based Triggering System. Lecture Notes in Computer Science, 2016, , 184-198.	1.0	11
93	Efficient Finite Field Multiplication for Isogeny Based Post Quantum Cryptography. Lecture Notes in Computer Science, 2016, , 193-207.	1.0	17
94	Efficient Fuzzy Extraction of PUF-Induced Secrets: Theory and Applications. Lecture Notes in Computer Science, 2016, , 412-431.	1.0	48
95	TOTAL: TRNG On-the-fly Testing for Attack Detection using Lightweight Hardware. , 2016, , .		20
96	Software Security: Vulnerabilities and Countermeasures for Two Attacker Models. , 2016, , .		6
97	On-the-fly tests for non-ideal true random number generators. , 2015, , .		9
98	Efficient Software Implementation of Ring-LWE Encryption. , 2015, , .		44
99	Embedded HW/SW Platform for On-the-Fly Testing of True Random Number Generators. , 2015, , .		9
100	Helper Data Algorithms for PUF-Based Key Generation: Overview and Analysis. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 2015, 34, 889-902.	1.9	189
101	RECTANGLE: a bit-slice lightweight block cipher suitable for multiple platforms. Science China Information Sciences, 2015, 58, 1-15.	2.7	115
102	A Survey on Lightweight Entity Authentication with Strong PUFs. ACM Computing Surveys, 2015, 48, 1-42.	16.1	133
103	Soteria. , 2015, , .		14
104	Practical feasibility evaluation and improvement of a pay-per-use licensing scheme for hardware IP cores in Xilinx FPGAs. Journal of Cryptographic Engineering, 2015, 5, 113-122.	1.5	8
105	High-Speed Polynomial Multiplication Architecture for Ring-LWE and SHE Cryptosystems. IEEE Transactions on Circuits and Systems I: Regular Papers, 2015, 62, 157-166.	3.5	94
106	Secure, Remote, Dynamic Reconfiguration of FPGAs. ACM Transactions on Reconfigurable Technology and Systems, 2015, 7, 1-19.	1.9	11
107	24.1 Circuit challenges from cryptography. , 2015, , .		15
108	Highly efficient entropy extraction for true random number generators on FPGAs. , 2015, , .		28

#	Article	IF	Citations
109	Electromagnetic circuit fingerprints for Hardware Trojan detection. , 2015, , .		59
110	Accelerating Scalar Conversion for Koblitz Curve Cryptoprocessors on Hardware Platforms. IEEE Transactions on Very Large Scale Integration (VLSI) Systems, 2015, 23, 810-818.	2.1	3
111	How to Use Koblitz Curves on Small Devices?. Lecture Notes in Computer Science, 2015, , 154-170.	1.0	3
112	Consolidating Masking Schemes. Lecture Notes in Computer Science, 2015, , 764-783.	1.0	128
113	DPA, Bitslicing and Masking at 1 GHz. Lecture Notes in Computer Science, 2015, , 599-619.	1.0	47
114	Efficient Ring-LWE Encryption on 8-Bit AVR Processors. Lecture Notes in Computer Science, 2015, , 663-682.	1.0	45
115	A Masked Ring-LWE Implementation. Lecture Notes in Computer Science, 2015, , 683-702.	1.0	38
116	Lightweight Coprocessor for Koblitz Curves: 283-Bit ECC Including Scalar Conversion with only 4300 Gates. Lecture Notes in Computer Science, 2015, , 102-122.	1.0	9
117	Modular Hardware Architecture for Somewhat Homomorphic Function Evaluation. Lecture Notes in Computer Science, 2015, , 164-184.	1.0	16
118	Anonymous Split E-Cashâ€"Toward Mobile Anonymous Payments. Transactions on Embedded Computing Systems, 2015, 14, 1-25.	2.1	9
119	Hardware/software co-design flavors of elliptic curve scalar multiplication. , 2014, , .		0
120	A noise bifurcation architecture for linear additive physical functions. , 2014, , .		56
121	Software Only, Extremely Compact, Keccak-based Secure PRNG on ARM Cortex-M. , 2014, , .		9
122	Ultra Low-Power implementation of ECC on the ARM Cortex-M0+. , 2014, , .		29
123	Secure interrupts on low-end microcontrollers. , 2014, , .		9
124	Key-recovery attacks on various RO PUF constructions via helper data manipulation. , 2014, , .		9
125	Test Versus Security: Past and Present. IEEE Transactions on Emerging Topics in Computing, 2014, 2, 50-62.	3.2	77
126	BLAKE-512-Based 128-Bit CCA2 Secure Timing Attack Resistant McEliece Cryptoprocessor. IEEE Transactions on Computers, 2014, 63, 1124-1133.	2.4	17

#	Article	IF	Citations
127	Fault Injection Modeling Attacks on 65 nm Arbiter and RO Sum PUFs via Environmental Changes. IEEE Transactions on Circuits and Systems I: Regular Papers, 2014, 61, 1701-1713.	3.5	90
128	Novel RNS Parameter Selection for Fast Modular Multiplication. IEEE Transactions on Computers, 2014, 63, 2099-2105.	2.4	15
129	Attacking PUF-Based Pattern Matching Key Generators via Helper Data Manipulation. Lecture Notes in Computer Science, 2014, , 106-131.	1.0	34
130	Generic DPA Attacks: Curse or Blessing?. Lecture Notes in Computer Science, 2014, , 98-111.	1.0	9
131	Chaskey: An Efficient MAC Algorithm for 32-bit Microcontrollers. Lecture Notes in Computer Science, 2014, , 306-323.	1.0	113
132	High Precision Discrete Gaussian Sampling on FPGAs. Lecture Notes in Computer Science, 2014, , 383-401.	1.0	18
133	Compact Ring-LWE Cryptoprocessor. Lecture Notes in Computer Science, 2014, , 371-391.	1.0	125
134	Secure Lightweight Entity Authentication with Strong PUFs: Mission Impossible?. Lecture Notes in Computer Science, 2014, , 451-475.	1.0	44
135	Key-recovery attacks on various RO PUF constructions via helper data manipulation. , 2014, , .		7
136	A Note on the Use of Margins to Compare Distinguishers. Lecture Notes in Computer Science, 2014, , 1-8.	1.0	4
137	Secure JTAG Implementation Using Schnorr Protocol. Journal of Electronic Testing: Theory and Applications (JETTA), 2013, 29, 193-209.	0.9	32
138	Teaching HW/SW Co-Design With a Public Key Cryptography Application. IEEE Transactions on Education, 2013, 56, 478-483.	2.0	9
139	A New Model for Error-Tolerant Side-Channel Cube Attacks. Lecture Notes in Computer Science, 2013, , 453-470.	1.0	4
140	A single-chip solution for the secure remote configuration of FPGAs using bitstream compression. , 2013, , .		13
141	Core Based Architecture to Speed Up Optimal Ate Pairing on FPGA Platform. Lecture Notes in Computer Science, 2013, , 141-159.	1.0	10
142	Hardware Designer's Guide to Fault Attacks. IEEE Transactions on Very Large Scale Integration (VLSI) Systems, 2013, 21, 2295-2306.	2.1	128
143	Side channel modeling attacks on 65nm arbiter PUFs exploiting CMOS device noise. , 2013, , .		97
144	SPONGENT: The Design Space of Lightweight Cryptographic Hashing. IEEE Transactions on Computers, 2013, 62, 2041-2053.	2.4	74

#	Article	IF	Citations
145	Low-energy encryption for medical devices. , 2013, , .		7
146	DEMO: Inherent PUFs and secure PRNGs on commercial off-the-shelf microcontrollers. , 2013, , .		5
147	Secure PRNG seeding on commercial off-the-shelf microcontrollers. , 2013, , .		15
148	The exponential impact of creativity in computer engineering education. , 2013, , .		3
149	Security Analysis of Industrial Test Compression Schemes. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 2013, 32, 1966-1977.	1.9	33
150	Signal Processing for Cryptography and Security Applications. , 2013, , 223-241.		3
151	Faster Pairing Coprocessor Architecture. Lecture Notes in Computer Science, 2013, , 160-176.	1.0	16
152	On the Implementation of Unified Arithmetic on Binary Huff Curves. Lecture Notes in Computer Science, 2013, , 349-364.	1.0	11
153	Dietary Recommendations for Lightweight Block Ciphers: Power, Energy and Area Analysis of Recently Developed Architectures. Lecture Notes in Computer Science, 2013, , 103-112.	1.0	34
154	Protected Software Module Architectures. , 2013, , 241-251.		14
155	PUF-based secure test wrapper design for cryptographic SoC testing. , 2012, , .		33
156	Fair and Consistent Hardware Evaluation of Fourteen Round Two SHA-3 Candidates. IEEE Transactions on Very Large Scale Integration (VLSI) Systems, 2012, 20, 827-840.	2.1	35
157	Low-cost implementations of on-the-fly tests for random number generators. , 2012, , .		12
158	Experimental evaluation of Physically Unclonable Functions in 65 nm CMOS. , 2012, , .		85
159	Guest Editorial - Integrated Circuit and System Security. IEEE Transactions on Information Forensics and Security, 2012, 7, 1-2.	4.5	3
160	Scan attacks on side-channel and fault attack resistant public-key implementations. Journal of Cryptographic Engineering, 2012, 2, 207-219.	1.5	3
161	Machine learning attacks on 65nm Arbiter PUFs: Accurate modeling poses strict bounds on usability. , 2012, , .		98
162	Design solutions for securing SRAM cell against power analysis. , 2012, , .		12

#	Article	IF	Citations
163	A Pay-per-Use Licensing Scheme for Hardware IP Cores in Recent SRAM-Based FPGAs. IEEE Transactions on Information Forensics and Security, 2012, 7, 98-108.	4.5	55
164	A systematic M safe-error detection in hardware implementations of cryptographic algorithms. , 2012, , .		3
165	A Speed Area Optimized Embedded Co-processor for McEliece Cryptosystem. , 2012, , .		18
166	Tiny application-specific programmable processor for BCH decoding. , 2012, , .		4
167	A scan-based attack on Elliptic Curve Cryptosystems in presence of industrial Design-for-Testability structures. , 2012, , .		14
168	Differential Scan Attack on AES with X-tolerant and X-masked Test Response Compactor. , 2012, , .		20
169	PUFs: Myth, Fact or Busted? A Security Evaluation of Physically Unclonable FunctionsÂ(PUFs) Cast in Silicon. Lecture Notes in Computer Science, 2012, , 283-301.	1.0	148
170	Efficient and secure hardware. Datenschutz Und Datensicherheit - DuD, 2012, 36, 872-875.	0.4	0
171	Interface Design for Mapping a Variety of RSA Exponentiation Algorithms on a HW/SW Co-design Platform. , 2012, , .		4
172	Theory and Practice of a Leakage Resilient Masking Scheme. Lecture Notes in Computer Science, 2012, , 758-775.	1.0	30
173	Extending ECC-based RFID authentication protocols to privacy-preserving multi-party grouping proofs. Personal and Ubiquitous Computing, 2012, 16, 323-335.	1.9	36
174	Efficient Hardware Implementation of Fp-Arithmetic for Pairing-Friendly Curves. IEEE Transactions on Computers, 2012, 61, 676-685.	2.4	22
175	A Practical Attack on KeeLoq. Journal of Cryptology, 2012, 25, 136-157.	2.1	14
176	Hierarchical ECC-Based RFID Authentication Protocol. Lecture Notes in Computer Science, 2012, , 183-201.	1.0	14
177	Power Analysis of Atmel CryptoMemory â€“ Recovering Keys from Secure EEPROMs. Lecture Notes in Computer Science, 2012, , 19-34.	1.0	34
178	An Updated Survey on Secure ECC Implementations: Attacks, Countermeasures and Cost. Lecture Notes in Computer Science, 2012, , 265-282.	1.0	60
179	A New Scan Attack on RSA in Presence of Industrial Countermeasures. Lecture Notes in Computer Science, 2012, , 89-104.	1.0	20
180	Reverse Fuzzy Extractors: Enabling Lightweight Mutual Authentication for PUF-Enabled RFIDs. Lecture Notes in Computer Science, 2012, , 374-389.	1.0	115

#	Article	IF	Citations
181	Selecting Time Samples for Multivariate DPA Attacks. Lecture Notes in Computer Science, 2012, , 155-174.	1.0	31
182	PUFKY: A Fully Functional PUF-Based Cryptographic Key Generator. Lecture Notes in Computer Science, 2012, , 302-319.	1.0	147
183	Performance and Security Evaluation of AES S-Box-Based Glitch PUFs on FPGAs. Lecture Notes in Computer Science, 2012, , 45-62.	1.0	6
184	LiBrA-CAN: A Lightweight Broadcast Authentication Protocol for Controller Area Networks. Lecture Notes in Computer Science, 2012, , 185-200.	1.0	118
185	Three Phase Dynamic Current Mode Logic: A More Secure DyCML to Achieve a More Balanced Power Consumption. Lecture Notes in Computer Science, 2012, , 68-81.	1.0	10
186	Systematic security evaluation method against C safe-error attacks. , 2011, , .		1
187	The Fault Attack Jungle - A Classification Model to Guide You. , 2011, , .		39
188	An In-depth and Black-box Characterization of the Effects of Clock Glitches on 8-bit MCUs. , 2011, , .		104
189	The cost of cryptography: Is low budget possible?. , 2011, , .		5
190	spongent: A Lightweight Hash Function. Lecture Notes in Computer Science, 2011, , 312-325.	1.0	185
191	Secure remote reconfiguration of an FPGA-based embedded system. , 2011, , .		15
192	Machine learning in side-channel analysis: a first study. Journal of Cryptographic Engineering, 2011, 1, 293-302.	1.5	211
193	Tripartite modular multiplication. The Integration VLSI Journal, 2011, 44, 259-269.	1.3	21
194	Design and design methods for unified multiplier and inverter and its application for HECC. The Integration VLSI Journal, 2011, 44, 280-289.	1.3	12
195	Physically unclonable functions. , 2011, , .		29
196	The communication and computation cost of wireless security. , 2011, , .		14
197	Low-cost fault detection method for ECC using Montgomery powering ladder. , 2011, , .		9
198	FPGA Implementation of Pairings Using Residue Number System and Lazy Reduction. Lecture Notes in Computer Science, 2011, , 421-441.	1.0	48

#	Article	IF	Citations
199	Constructing Application-Specific Memory Hierarchies on FPGAs. Lecture Notes in Computer Science, 2011, , 201-216.	1.0	1
200	FO4-based models for area, delay and energy of polynomial multiplication over binary fields. , 2010, , .		0
201	Low Cost Built in Self Test for Public Key Crypto Cores. , 2010, , .		5
202	An embedded platform for privacy-friendly road charging applications. , 2010, , .		4
203	Physically Unclonable Functions: A Study on the State of the Art and Future Research Directions. Information Security and Cryptography, 2010, , 3-37.	0.2	294
204	Low-cost untraceable authentication protocols for RFID. , 2010, , .		70
205	Wideâ€“Weak Privacyâ€“Preserving RFID Authentication Protocols. Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, 2010, , 254-267.	0.2	12
206	A compact FPGA-based architecture for elliptic curve cryptography over prime fields. , 2010, , .		43
207	Faster Interleaved Modular Multiplication Based on Barrett and Montgomery Reduction Methods. IEEE Transactions on Computers, 2010, 59, 1715-1721.	2.4	52
208	Implementation of binary edwards curves for very-constrained devices. , 2010, , .		20
209	State-of-the-art of secure ECC implementations: a survey on known side-channel attacks and countermeasures. , 2010, , .		101
210	A Hybrid Scheme for Concurrent Error Detection of Multiplication over Finite Fields. , 2010, , .		3
211	Breaking Elliptic Curve Cryptosystems Using Reconfigurable Hardware. , 2010, , .		14
212	Prototyping platform for performance evaluation of SHA-3 candidates. , 2010, , .		12
213	Compact Public-Key Implementations for RFID and Sensor Nodes. Integrated Circuits and Systems, 2010, , 179-195.	0.2	1
214	Privacy Challenges in RFID Systems. , 2010, , 397-407.		12
215	Revisiting Higher-Order DPA Attacks:. Lecture Notes in Computer Science, 2010, , 221-234.	1.0	45
216	Speeding Up Bipartite Modular Multiplication. Lecture Notes in Computer Science, 2010, , 166-179.	1.0	11

#	Article	IF	Citations
217	Anti-counterfeiting, Untraceability and Other Security Challenges for RFID Systems: Public-Key-Based Protocols and Hardware. Information Security and Cryptography, 2010, , 237-257.	0.2	12
218	Hardware design for Hash functions. Integrated Circuits and Systems, 2010, , 79-104.	0.2	2
219	Signal Processing for Cryptography and Security Applications. , 2010, , 161-177.		0
220	Practical Mitigations for Timing-Based Side-Channel Attacks on Modern x86 Processors. , 2009, , .		133
221	Analysis and design of active IC metering schemes. , 2009, , .		29
222	Light-weight implementation options for curve-based cryptography: HECC is also ready for RFID. , 2009, , .		1
223	Empirical comparison of side channel analysis distinguishers on DES in hardware. , 2009, , .		3
224	FPGA-based testing strategy for cryptographic chips: A case study on Elliptic Curve Processor for RFID tags. , 2009, , .		2
225	Modular reduction without precomputational phase. , 2009, , .		9
226	Practical DPA attacks on MDPL. , 2009, , .		13
227	A soft decision helper data algorithm for SRAM PUFs. , 2009, , .		125
228	Efficient implementation of anonymous credentials on Java Card smart cards. , 2009, , .		31
229	Untraceable RFID authentication protocols: Revision of EC-RAC. , 2009, , .		16
230	Random numbers generation: Investigation of narrowtransitions suppression on FPGA. , 2009, , .		3
231	Case Study : A class E power amplifier for ISO-14443A. , 2009, , .		3
232	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
233	Faster $mathbb{F}_p$ -Arithmetic for Cryptographic Pairings on Barreto-Naehrig Curves. Lecture Notes in Computer Science, 2009, , 240-253.	1.0	29
234	Programmable and Parallel ECC Coprocessor Architecture: Tradeoffs between Area, Speed and Security. Lecture Notes in Computer Science, 2009, , 289-303.	1.0	7

#	Article	IF	Citations
235	Low-Overhead Implementation of a Soft Decision Helper Data Algorithm for SRAM PUFs. Lecture Notes in Computer Science, 2009, , 332-347.	1.0	115
236	HECC Goes Embedded: An Area-Efficient Implementation of HECC. Lecture Notes in Computer Science, 2009, , 387-400.	1.0	5
237	Hardware evaluation of the Luffa hash family. , 2009, , .		5
238	Design Methodology for Throughput Optimum Architectures of Hash Algorithms of the MD4-class. Journal of Signal Processing Systems, 2008, 53, 89-102.	1.4	8
239	Elliptic curve cryptography on embedded multicore systems. Design Automation for Embedded Systems, 2008, 12, 231-242.	0.7	23
240	Dependence of RFID Reader Antenna Design on Read Out Distance. IEEE Transactions on Antennas and Propagation, 2008, 56, 3829-3837.	3.1	39
241	EC-RAC (ECDLP Based Randomized Access Control): Provably Secure RFID authentication protocol. , 2008, , .		84
242	Elliptic-Curve-Based Security Processor for RFID. IEEE Transactions on Computers, 2008, 57, 1514-1527.	2.4	181
243	A Cost-Effective Latency-Aware Memory Bus for Symmetric Multiprocessor Systems. IEEE Transactions on Computers, 2008, 57, 1714-1719.	2.4	7
244	Extended abstract: Unified digit-serial multiplier/inverter in finite field GF(2^m). , 2008, , .		2
245	A digit-serial architecture for inversion and multiplication in GF(2^M). , 2008, , .		3
246	On the high-throughput implementation of RIPEMD-160 hash algorithm. , 2008, , .		5
247	Low-cost implementations of NTRU for pervasive security. , 2008, , .		29
248	FPGA Design for Algebraic Tori-Based Public-Key Cryptography. , 2008, , .		0
249	Demonstration of Uncoordinated Multiple Access in Optical Communications. IEEE Transactions on Circuits and Systems I: Regular Papers, 2008, 55, 3259-3269.	3.5	1
250	Exploiting Hardware Performance Counters. , 2008, , .		50
251	Cover and Frontmatter. , 2008, , .		0
252	Public-Key Cryptography for RFID Tags and Applications. , 2008, , 317-348.		4

#	Article	IF	Citations
253	Modular Reduction in GF(2 n) without Pre-computational Phase. Lecture Notes in Computer Science, 2008, , 77-87.	1.0	14
254	Perfect Matching Disclosure Attacks. Lecture Notes in Computer Science, 2008, , 2-23.	1.0	33
255	Fault Analysis Study of IDEA. Lecture Notes in Computer Science, 2008, , 274-287.	1.0	19
256	Power and Fault Analysis Resistance in Hardware through Dynamic Reconfiguration. Lecture Notes in Computer Science, 2008, , 346-362.	1.0	38
257	Revisiting a combinatorial approach toward measuring anonymity. , 2008, , .		33
258	Computer Architecture and Design. , 2008, , .		0
259	Public-Key Cryptography on the Top of a Needle. , 2007, , .		24
260	Side-channel resistant system-level design flow for public-key cryptography. , 2007, , .		0
261	Efficient pipelining for modular multiplication architectures in prime fields. , 2007, , .		16
262	Design of an Interconnect Architecture and Signaling Technology for Parallelism in Communication. IEEE Transactions on Very Large Scale Integration (VLSI) Systems, 2007, 15, 881-894.	2.1	35
263	Design methods for Security and Trust. , 2007, , .		18
264	Transforming Signal Processing Applications into Parallel Implementations. Eurasip Journal on Advances in Signal Processing, 2007, 2007, .	1.0	0
265	Public-Key Cryptography for RFID-Tags. , 2007, , .		158
266	Multicore Curve-Based Cryptoprocessor with Reconfigurable Modular Arithmetic Logic Units over GF(2^n). IEEE Transactions on Computers, 2007, 56, 1269-1282.	2.4	46
267	Reconfigurable modular arithmetic logic unit supporting high-performance RSA and ECC over GF(p). International Journal of Electronics, 2007, 94, 501-514.	0.9	20
268	Montgomery Modular Multiplication Algorithm on Multi-Core Systems. Signal Processing Systems Design and Implementation (siPS), IEEE Workshop on, 2007, , .	0.0	17
269	A Side-channel Attack Resistant Programmable PKC Coprocessor for Embedded Applications. , 2007, , .		7
270	Secure IRIS Verification. , 2007, , .		42

#	Article	IF	Citations
271	HW/SW co-design of a hyperelliptic curve cryptosystem using a microcode instruction set coprocessor. The Integration VLSI Journal, 2007, 40, 45-51.	1.3	11
272	HW/SW co-design for public-key cryptosystems on the 8051 micro-controller. Computers and Electrical Engineering, 2007, 33, 324-332.	3.0	4
273	Differential power and electromagnetic attacks on a FPGA implementation of elliptic curve cryptosystems. Computers and Electrical Engineering, 2007, 33, 367-382.	3.0	42
274	High-performance Public-key Cryptoprocessor for Wireless Mobile Applications. Mobile Networks and Applications, 2007, 12, 245-258.	2.2	16
275	Iteration Bound Analysis and Throughput Optimum Architecture of SHA-256 (384,512) for Hardware Implementations. Lecture Notes in Computer Science, 2007, , 102-114.	1.0	17
276	A Compact Architecture for Montgomery Elliptic Curve Scalar Multiplication Processor. Lecture Notes in Computer Science, 2007, , 115-127.	1.0	11
277	Side-Channel Analysis Attacks on Hardware Implementations of Cryptographic Algorithms. , 2007, , .		6
278	Throughput Optimized SHA-1 Architecture Using Unfolding Transformation. , 2006, , .		19
279	Side-Channel Leakage Tolerant Architectures. , 2006, , .		3
280	Cross Layer Design to Multi-thread a Data-Pipelining Application on a Multi-processor on Chip. , 2006, , .		1
281	FPGA Vendor Agnostic True Random Number Generator. , 2006, , .		83
282	Fpga-Oriented Secure Data Path Design: Implementation of a Public Key Coprocessor. , 2006, , .		6
283	Reconfigurable Architectures for Curve-Based Cryptography on Embedded Micro-Controllers. , 2006, , .		6
284	A digital design flow for secure integrated circuits. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 2006, 25, 1197-1208.	1.9	117
285	Clock-skew-optimization methodology for substrate-noise reduction with supply-current folding. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 2006, 25, 1146-1154.	1.9	12
286	AES-Based Security Coprocessor IC in 0.18-<tex>$muhbox m$</tex>CMOS With Resistance to Differential Power Analysis Side-Channel Attacks. IEEE Journal of Solid-State Circuits, 2006, 41, 781-792.	3.5	126
287	Area-throughput trade-offs for fully pipelined 30 to 70 Gbits/s AES processors. IEEE Transactions on Computers, 2006, 55, 366-372.	2.4	146
288	Multilevel Design Validation in a Secure Embedded System. IEEE Transactions on Computers, 2006, 55, 1380-1390.	2.4	5

#	Article	IF	Citations
289	A Component-Based Design Environment for ESL Design. IEEE Design and Test of Computers, 2006, 23, 338-347.	1.4	11
290	Circuits and design techniques for secure ICs resistant to side-channel attacks. , 2006, , .		2
291	Differential Electromagnetic Attack on an FPGA Implementation of Elliptic Curve Cryptosystems. , 2006, , .		20
292	Design with race-free hardware semantics. , 2006, , .		20
293	Efficient and Secure Fingerprint Verification for Embedded Devices. Eurasip Journal on Advances in Signal Processing, 2006, 2006, 1.	1.0	10
294	An interactive codesign environment for domain-specific coprocessors. ACM Transactions on Design Automation of Electronic Systems, 2006, 11, 70-87.	1.9	21
295	Securing embedded systems. IEEE Security and Privacy, 2006, 4, 40-49.	1.5	66
296	High Speed Channel Coding Architectures for the Uncoordinated OR Channel. , 2006, , .		4
297	HW/SW Co-design for Accelerating Public-Key Cryptosystems over GF(p) on the 8051 ?-controller. , 2006, , .		3
298	Trellis Codes with Low Ones Density for the OR Multiple Access Channel. , 2006, , .		5
299	Time-Memory Trade-Off Attack on FPGA Platforms: UNIX Password Cracking. Lecture Notes in Computer Science, 2006, , 323-334.	1.0	15
300	Reconfigurable Modular Arithmetic Logic Unit for High-Performance Public-Key Cryptosystems. Lecture Notes in Computer Science, 2006, , 347-357.	1.0	17
301	Superscalar Coprocessor for High-Speed Curve-Based Cryptography. Lecture Notes in Computer Science, 2006, , 415-429.	1.0	20
302	A scalable and high performance elliptic curve processor with resistance to timing attacks. , 2005, , .		4
303	Integrated modelling and generation of a reconfigurable network-on-chip. International Journal of Embedded Systems, 2005, 1, 218.	0.2	1
304	Advanced RF/Baseband Interconnect Schemes for Inter- and Intra-ULSI Communications. IEEE Transactions on Electron Devices, 2005, 52, 1271-1285.	1.6	61
305	Microcoded coprocessor for embedded secure biometric authentication systems. , 2005, , .		1
306	A side-channel leakage free coprocessor IC in 0.18Âµm CMOS for embedded AES-based cryptographic and biometric processing. , 2005, , .		39

#	Article	IF	Citations
307	A Systematic Evaluation of Compact Hardware Implementations for the Rijndael S-Box. Lecture Notes in Computer Science, 2005, , 323-333.	1.0	61
308	Wireless Wednesday at DAC. IEEE Solid-State Circuits Society Newsletter, 2005, 10, 11-11.	0.1	0
309	A 3.84 gbits/s AES crypto coprocessor with modes of operation in a 0.18-Î¼m CMOS technology. , 2005, , .		46
310	A 5.6-mW 1-Gb/s/pair pulsed signaling transceiver for a fully AC coupled bus. IEEE Journal of Solid-State Circuits, 2005, 40, 1331-1340.	3.5	12
311	Platform-based design for an embedded-fingerprint-authentication device. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 2005, 24, 1929-1936.	1.9	9
312	Cooperative multithreading on embedded multiprocessor architectures enables energy-scalable design. , 2005, , .		12
313	Side-channel issues for designing secure hardware implementations. , 2005, , .		15
314	Prototype IC with WDDL and Differential Routing â€“ DPA Resistance Assessment. Lecture Notes in Computer Science, 2005, , 354-365.	1.0	99
315	Electromagnetic Analysis Attack on an FPGA Implementation of an Elliptic Curve Cryptosystem. , 2005, , .		56
316	A side-channel leakage free coprocessor IC in 0.18/spl mu/m CMOS for embedded AES-based cryptographic and biometric processing. , 2005, , .		9
317	Skiing the embedded systems mountain. Transactions on Embedded Computing Systems, 2005, 4, 529-548.	2.1	6
318	Simulation models for side-channel information leaks. , 2005, , .		39
319	Hardware/Software Co-design for Hyperelliptic Curve Cryptography (HECC) on the 8051 Î¼P. Lecture Notes in Computer Science, 2005, , 106-118.	1.0	12
320	Security for Ambient Intelligent Systems. , 2005, , 199-221.		7
321	Balanced point operations for side-channel protection of elliptic curve cryptography. IEE Proceedings - Information Security, 2005, 152, 57.	1.9	15
322	Low-Power DSPs. , 2005, , 2-1-2-15.		0
323	Architectures and Design Techniques for Energy Efficient Embedded DSP and Multimedia Processing. , 2004, , 141-155.		0
324	Reducing radio energy consumption of key management protocols for wireless sensor networks. , 2004, , .		41

#	Article	IF	Citations
325	The happy marriage of architecture and application in next-generation reconfigurable systems. , 2004, , .		6
326	Streaming encryption for a secure wavelength and time domain hopped optical network. , 2004, , .		1
327	Place and Route for Secure Standard Cell Design. International Federation for Information Processing, 2004, , 143-158.	0.4	70
328	Architectural design features of a programmable high throughput AES coprocessor. , 2004, , .		12
329	Digital circuit capacitance and switching analysis for ground bounce in ICs with a high-ohmic substrate. IEEE Journal of Solid-State Circuits, 2004, 39, 1119-1130.	3.5	25
330	Java cryptography on KVM and its performance and security optimization using HW/SW co-design techniques. , 2004, , .		11
331	High-throughput programmable cryptocoprocessor. IEEE Micro, 2004, 24, 34-45.	1.8	41
332	Design of portable biometric authenticators - energy, performance, and security tradeoffs. IEEE Transactions on Consumer Electronics, 2004, 50, 1222-1231.	3.0	20
333	E09: An FPGA implementation of Rijndael: Trade-offs for side-channel security. IFAC Postprint Volumes IPPV / International Federation of Automatic Control, 2004, 37, 493-498.	0.4	2
334	Secure Logic Synthesis. Lecture Notes in Computer Science, 2004, , 1052-1056.	1.0	17
335	Low- Power DSPs. Computer Engineering Series, 2004, , 19-1-19-15.	0.1	0
336	Domain-specific codesign for embedded security. Computer, 2003, 36, 68-74.	1.2	43
337	Design and performance testing of a 2.29-GB/s rijndael processor. IEEE Journal of Solid-State Circuits, 2003, 38, 569-572.	3.5	166
338	Design flow for HW / SW acceleration transparency in the thumbpod secure embedded system. , 2003, , .		7
339	A secure fingerprint matching technique. , 2003, , .		35
340	Finding the best system design flow for a high-speed JPEG encoder. , 2003, , .		12
341	Securing Encryption Algorithms against DPA at the Logic Level: Next Generation Smart Card Technology. Lecture Notes in Computer Science, 2003, , 125-136.	1.0	100
342	Unlocking the design secrets of a 2.29 Gb/s Rijndael processor. , 2002, , .		11

#	Article	IF	Citations
343	Unlocking the design secrets of a 2.29 Gb/s Rijndael processor. Proceedings - Design Automation Conference, 2002, , .	0.0	19
344	Clock tree optimization in synchronous CMOS digital circuits for substrate noise reduction using folding of supply current transients. , 2002, , .		10
345	Guest editorial: low-power electronics and design. IEEE Transactions on Very Large Scale Integration (VLSI) Systems, 2002, 10, 69-70.	2.1	0
346	Domain Specific Tools and Methods for Application in Security Processor Design. Design Automation for Embedded Systems, 2002, 7, 365-383.	0.7	8
347	Reconfigurable interconnect for next generation systems. , 2002, , .		12
348	Architectural Optimization for a 1.82Gbits/sec VLSI Implementation of the AES Rijndael Algorithm. Lecture Notes in Computer Science, 2001, , 51-64.	1.0	78
349	A reconfiguration hierarchy for elliptic curve cryptography. , 2001, , .		4
350	A quick safari through the reconfiguration jungle. , 2001, , .		63
351	Low power DSP's for wireless communications. , 2000, , .		13
352	Low power DSP's for wireless communications (embedded tutorial session). , 2000, , .		8
353	A Low Power DSP Engine for Wireless Communications. Journal of Signal Processing Systems, 1998, 18, 177-186.	1.0	24
354	Analysis of multidimensional DSP specifications. IEEE Transactions on Signal Processing, 1996, 44, 3169-3174.	3.2	3
355	Guest editor's introduction design environments for DSP. Journal of Signal Processing Systems, 1995, 9, 5-6.	1.0	0
356	Synthesis for real time systems: Solutions and challenges. Journal of Signal Processing Systems, 1995, 9, 67-88.	1.0	6
357	Memory estimation for high level synthesis. , 1994, , .		49
358	ASIC cryptographical processor based on DES. , 1991, , .		9
359	In-place memory management of algebraic algorithms on application specific ICs. Journal of Signal Processing Systems, 1991, 3, 193-200.	1.0	22
360	Security and performance optimization of a new DES data encryption chip. IEEE Journal of Solid-State Circuits, 1988, 23, 647-656.	3.5	26

#	Article	IF	Citations
361	Security Considerations in the Design and Implementation of a new DES chip. Lecture Notes in Computer Science, 1988, , 287-300.	1.0	6
362	A Micropower CMOS-Instrumentation Amplifier. IEEE Journal of Solid-State Circuits, 1985, 20, 805-807.	3.5	106
363	Micropower high-performance SC building block for integrated low-level signal processing. IEEE Journal of Solid-State Circuits, 1985, 20, 837-844.	3.5	30
364	A low power DSP engine for wireless communications. , 0, , .		7
365	Turbo codes on the fixed point DSP TMS320C55x. , 0, , .		3
366	Benchmarking DSP Architectures for Low Power Applications. , 0, , 287-298.		0
367	Low power showdown: comparison of five DSP platforms implementing an LPC speech codec. , 0, , .		7
368	Hardware/software co-design of an elliptic curve public-key cryptosystem. , 0, , .		11
369	A 2.29 Gbits/sec, 56 mW non-pipelined Rijndael AES encryption IC in a 1.8 V, 0.18 Î¼m CMOS technology. , 0, , .		7
370	A hardware implementation in FPGA of the Rijndael algorithm. , 0, , .		15
371	Gigabit simultaneous bi-directional signaling using DS-CDMA. , 0, , .		0
372	A compact and efficient fingerprint verification system for secure embedded devices. , 0, , .		16
373	Teaching trade-offs in system-level design methodologies. , 0, , .		3
374	Speed-area trade-off for 10 to 100 Gbits/s throughput AES processor. , 0, , .		26
375	Testing ThumbPod: Softcore bugs are hard to find. , 0, , .		4
376	Interfacing a high speed crypto accelerator to an embedded CPU. , 0, , .		30
377	Charge recycling sense amplifier based logic: securing low power security ICs against DPA [differential power analysis]. , 0, , .		22
378	Interactive cosimulation with partial evaluation. , 0, , .		14

#	Article	IF	Citations
379	Secure fuzzy vault based fingerprint verification system. , 0, , .		13
380	Architectures and design techniques for energy efficient embedded DSP and multimedia processing. , 0, , .		5
381	Integrated modeling and generation of a reconfigurable network-on-chip. , 0, , .		14
382	A realtime, memory efficient fingerprint verification system. , 0, , .		3
383	A low power capacitive coupled bus interface based on pulsed signaling. , 0, , .		8
384	Minimum area cost for a 30 to 70 Gbits/s AES processor. , 0, , .		51
385	A logic level design methodology for a secure DPA resistant ASIC or FPGA implementation. , 0, , .		396
386	A 21.54 Gbits/s Fully Pipelined AES Processor on FPGA. , 0, , .		133
387	Embedded software integration for coarse-grain reconfigurable systems. , 0, , .		16
388	Design Method for Constant Power Consumption of Differential Logic Circuits. , 0, , .		39
389	A Light-Weight Cooperative Multi-threading with Hardware Supported Thread-Management on an Embedded Multi-Processor System. , 0, , .		1
390	A VLSI Design Flow for Secure Side-Channel Attack Resistant ICs. , 0, , .		60
391	A hyperelliptic curve crypto coprocessor for an 8051 microcontroller. , 0, , .		6
392	Fast Dynamic Memory Integration in Co-Simulation Frameworks for Multiprocessor System on-Chip. , 0, , .		2
393	Energy and performance analysis of mapping parallel multi-threaded tasks for an on-chip multi-processor system. , 0, , .		0
394	Side-channel aware design: Algorithms and Architectures for Elliptic Curve Cryptography over GF(2^n) Tj ETQq0 0 0 rgBT /Overlock 10 Tf		0
395	Extended abstract: a race-free hardware modeling language. , 0, , .		1
396	Multi-level design validation in a secure embedded system. , 0, , .		3

#	Article	IF	Citations
397	AES-Based Cryptographic and Biometric Security Coprocessor IC in 0.18-Î¼m CMOS Resistant to Side-Channel Power Analysis Attacks. , 0, , .		15
398	Automatic Secure Fingerprint Verification System Based on Fuzzy Vault Scheme. , 0, , .		59
399	A Fast Dual-Field Modular Arithmetic Logic Unit and Its Hardware Implementation. , 0, , .		13
400	A Parallel Processing Hardware Architecture for Elliptic Curve Cryptosystems. , 0, , .		20
401	Network Security. , 0, , 509-585.		1
402	Circuits and design techniques for secure ICs resistant to side-channel attacks. , 0, , .		2
403	Flexible Hardware Architectures for Curve-based Cryptography. , 0, , .		4
404	Scabbard: a suite of efficient learning with rounding key-encapsulation mechanisms. Iacr Transactions on Cryptographic Hardware and Embedded Systems, 0, , 474-509.	0.0	6
405	Towards Efficient and Automated Side Channel Evaluations at Design Time. , 0, , .		9
406	Saber on ARM. Iacr Transactions on Cryptographic Hardware and Embedded Systems, 0, , 243-266.	0.0	31
407	ES-TRNG: A High-throughput, Low-area True Random Number Generator based on Edge Sampling. Iacr Transactions on Cryptographic Hardware and Embedded Systems, 0, , 267-292.	0.0	39
408	Design flow for HW/SW acceleration transparency in the thumbpod secure embedded system. , 0, , .		1
409	Polynomial multiplication on embedded vector architectures. Iacr Transactions on Cryptographic Hardware and Embedded Systems, 0, , 482-505.	0.0	3
410	A quick safari through the reconfiguration jungle. , 0, , .		0
411	Low power DSP's for wireless communications. , 0, , .		0