Tim GÃ¼neysu

List of Publications by Year
in descending order

Source: https://exaly.com/author-pdf/3972585/publications.pdf

Version: 2024-02-01

130	3,281	218592	197736
papers	citations	26 h-index	49 g-index

137	137	137	1668
all docs	docs citations	times ranked	citing authors

#	Article	IF	Citations
1	Folding BIKE: Scalable Hardware Implementation for Reconfigurable Devices. IEEE Transactions on Computers, 2022, 71, 1204-1215.	2.4	15
2	A Hard Crystal - Implementing Dilithium onÂReconfigurable Hardware. Lecture Notes in Computer Science, 2022, , 210-230.	1.0	16
3	Boolean Masking for Arithmetic Additions at Arbitrary Order in Hardware. Applied Sciences (Switzerland), 2022, 12, 2274.	1.3	2
4	Carry-Less toÂBIKE Faster. Lecture Notes in Computer Science, 2022, , 833-852.	1.0	5
5	Applications of machine learning techniques in side-channel attacks: a survey. Journal of Cryptographic Engineering, 2020, 10, 135-162.	1.5	54
6	Secure Implementation of Lattice-Based Encryption Schemes. , 2020, , 21-49.		0
7	Deep Learning Multi-Channel Fusion Attack Against Side-Channel Protected Hardware. , 2020, , .		1
8	Improved Side-Channel Resistance by Dynamic Fault-Injection Countermeasures. , 2020, , .		2
9	Towards Secure Composition of Integrated Circuits and Electronic Systems: On the Role of EDA. , 2020, , .		17
10	Lightweight Side-Channel Protection using Dynamic Clock Randomization. , 2020, , .		14
11	Deep Neural Network Attribution Methods for Leakage Analysis and Symmetric Key Recovery. Lecture Notes in Computer Science, 2020, , 645-666.	1.0	14
12	Efficient Microcontroller Implementation of BIKE. Lecture Notes in Computer Science, 2020, , 34-49.	1.0	0
13	Revisiting ECM on GPUs. Lecture Notes in Computer Science, 2020, , 299-319.	1.0	0
14	Concurrent error detection revisited. , 2020, , .		2
15	Securing Cryptographic Circuits by Exploiting Implementation Diversity and Partial Reconfiguration on FPGAs. , 2019, , .		11
16	Profiled Power Analysis Attacks Using Convolutional Neural Networks with Domain Knowledge. Lecture Notes in Computer Science, 2019, , 479-498.	1.0	14
17	Evaluation of (power) side-channels in cryptographic implementations. IT - Information Technology, 2019, 61, 15-28.	0.6	3
18	Efficiently Masking Binomial Sampling at Arbitrary Orders for Lattice-Based Crypto. Lecture Notes in Computer Science, 2019, , 534-564.	1.0	19

#	Article	IF	Citations
19	Implementing the NewHope-Simple Key Exchange on Low-Cost FPGAs. Lecture Notes in Computer Science, 2019, , 128-142.	1.0	15
20	Towards Practical Microcontroller Implementation of the Signature Scheme Falcon. Lecture Notes in Computer Science, 2019, , 65-80.	1.0	8
21	Confident leakage assessment â€" A side-channel evaluation framework based on confidence intervals. , 2018, , .		11
22	GliFreD: Glitch-Free Duplication Towards Power-Equalized Circuits on FPGAs. IEEE Transactions on Computers, 2018, 67, 375-387.	2.4	11
23	Exploring the Vulnerability of R-LWE Encryption to Fault Attacks. , 2018, , .		14
24	Evaluation of Lattice-Based Signature Schemes in Embedded Systems. , 2018, , .		7
25	Exploring RFC 7748 for Hardware Implementation: Curve25519 and Curve448 with Side-Channel Protection. Journal of Hardware and Systems Security, 2018, 2, 297-313.	0.8	10
26	Towards Self-Explaining Digital Systems: A Design Methodology for the Next Generation. , 2018, , .		5
27	Physical Protection of Lattice-Based Cryptography. , 2018, , .		11
28	Hiding Higher-Order Side-Channel Leakage. Lecture Notes in Computer Science, 2017, , 131-146.	1.0	8
29	Compact Constant Weight Coding Engines for the Code-Based Cryptography. IEEE Transactions on Circuits and Systems II: Express Briefs, 2017, 64, 1092-1096.	2.2	3
30	Towards lightweight Identity-Based Encryption for the post-quantum-secure Internet of Things. , 2017, , .		25
31	LWE-based lossless computational fuzzy extractor for the Internet of Things. , 2017, , .		5
32	Securing Systems With Indispensable Entropy: LWE-Based Lossless Computational Fuzzy Extractor for the Internet of Things. IEEE Access, 2017, 5, 11909-11926.	2.6	14
33	Strong 8-bit Sboxes with efficient masking in hardware extended version. Journal of Cryptographic Engineering, 2017, 7, 149-165.	1.5	13
34	Cryptography for Next Generation TLS. , 2017, , .		7
35	High-Performance Ideal Lattice-Based Cryptography on 8-Bit AVR Microcontrollers. Transactions on Embedded Computing Systems, 2017, 16, 1-24.	2.1	14
36	CAKE: Code-Based Algorithm for Key Encapsulation. Lecture Notes in Computer Science, 2017, , 207-226.	1.0	13

#	Article	IF	Citations
37	A fair and comprehensive large-scale analysis of oscillation-based PUFs for FPGAs. , 2017, , .		18
38	Secure and Private, yet Lightweight, Authentication for the IoT via PUF and CBKA. Lecture Notes in Computer Science, 2017, , 28-48.	1.0	2
39	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
40	On the problems of realizing reliable and efficient ring oscillator PUFs on FPGAs. , 2016, , .		8
41	On the Energy Cost of Channel Based Key Agreement. , 2016, , .		4
42	ParTI. , 2016, , .		5
43	Sixth International Workshop on Trustworthy Embedded Devices (TrustED 2016). , 2016, , .		0
44	A grain in the silicon: SCA-protected AES in less than 30 slices. , 2016, , .		5
45	Lattice-based cryptography: From reconfigurable hardware to ASIC. , 2016, , .		11
46	Secure software update and IP protection for untrusted devices in the Internet of Things via physically unclonable functions. , 2016, , .		14
47	Lattice-based Encryption Over Standard Lattices In Hardware. , 2016, , .		19
48	ParTI â€“ Towards Combined Hardware Countermeasures Against Side-Channel and Fault-Injection Attacks. Lecture Notes in Computer Science, 2016, , 302-332.	1.0	67
49	White-Box Cryptography in the Gray Box. Lecture Notes in Computer Science, 2016, , 185-203.	1.0	15
50	Strong 8-bit Sboxes with Efficient Masking in Hardware. Lecture Notes in Computer Science, 2016, , 171-193.	1.0	10
51	Secure architectures of future emerging cryptography SAFEcrypto. , 2016, , .		3
52	High-Performance and Lightweight Lattice-Based Public-Key Encryption. , 2016, , .		59
53	Affine Equivalence and Its Application to Tightening Threshold Implementations. Lecture Notes in Computer Science, 2016, , 263-276.	1.0	7
54	Information reconciliation schemes in physical-layer security: A survey. Computer Networks, 2016, 109, 84-104.	3.2	51

#	Article	IF	Citations
55	Introduction to the CHES 2015 special issue. Journal of Cryptographic Engineering, 2016, 6, 83-84.	1.5	0
56	IND-CCA Secure Hybrid Encryption from QC-MDPC Niederreiter. Lecture Notes in Computer Science, 2016, , 1-17.	1.0	13
57	New ASIC/FPGA Cost Estimates for SHA-1 Collisions. , 2015, , .		5
58	Securing systems on the Internet of Things via physical properties of devices and communications. , 2015, , .		26
59	Implementing QC-MDPC McEliece Encryption. Transactions on Embedded Computing Systems, 2015, 14, 1-27.	2.1	29
60	High-Performance Ideal Lattice-Based Cryptography on 8-Bit ATxmega Microcontrollers. Lecture Notes in Computer Science, 2015, , 346-365.	1.0	74
61	Practical Lattice-Based Digital Signature Schemes. Transactions on Embedded Computing Systems, 2015, 14, 1-24.	2.1	31
62	Security analysis of index-based syndrome coding for PUF-based key generation. , 2015, , .		18
63	Achieving side-channel protection with dynamic logic reconfiguration on modern FPGAs. , 2015, , .		27
64	Implementing Curve25519 for Side-Channel--Protected Elliptic Curve Cryptography. ACM Transactions on Reconfigurable Technology and Systems, 2015, 9, 1-15.	1.9	29
65	Lattice-Based Signatures: Optimization and Implementation on Reconfigurable Hardware. IEEE Transactions on Computers, 2015, 64, 1954-1967.	2.4	15
66	High-Speed Signatures from Standard Lattices. Lecture Notes in Computer Science, 2015, , 84-103.	1.0	15
67	Evaluating the Duplication of Dual-Rail Precharge Logics on FPGAs. Lecture Notes in Computer Science, 2015, , 81-94.	1.0	11
68	Arithmetic Addition over Boolean Masking. Lecture Notes in Computer Science, 2015, , 559-578.	1.0	30
69	Area optimization of lightweight lattice-based encryption on reconfigurable hardware. , 2014, , .		61
70	A hardware-assisted proof-of-concept for secure VoIP clients on untrusted operating systems. , 2014, , .		1
71	Fault Sensitivity Analysis Meets Zero-Value Attack. , 2014, , .		7
72	Enhanced Lattice-Based Signatures on Reconfigurable Hardware. Lecture Notes in Computer Science, 2014, , 353-370.	1.0	70

#	Article	IF	Citations
73	Enabling SRAM-PUFs on Xilinx FPGAs. , 2014, , .		14
74	THOR - The hardware onion router. , 2014, , .		2
75	Cryptographic Algorithms on the GA144 Asynchronous Multi-Core Processor. Journal of Signal Processing Systems, 2014, 77, 151.	1.4	2
76	Beyond ECDSA and RSA. , 2014, , .		23
77	Beyond ECDSA and RSA: Lattice-based digital signatures on constrained devices. , 2014, , .		15
78	Efficient Elliptic-Curve Cryptography Using Curve25519 on Reconfigurable Devices. Lecture Notes in Computer Science, 2014, , 25-36.	1.0	33
79	Towards Side-Channel Resistant Implementations of QC-MDPC McEliece Encryption on Constrained Devices. Lecture Notes in Computer Science, 2014, , 266-282.	1.0	24
80	Towards Practical Lattice-Based Public-Key Encryption on Reconfigurable Hardware. Lecture Notes in Computer Science, 2014, , 68-85.	1.0	57
81	Lightweight code-based cryptography: QC-MDPC McEliece encryption on reconfigurable devices. , 2014, , .		19
82	High-Performance Cryptanalysis on RIVYERA and COPACOBANA Computing Systems. , 2013, , 335-366.		10
83	Efficient implementation of cryptographic primitives on the GA144 multi-core architecture. , 2013, , .		2
84	Code-based cryptography on reconfigurable hardware: tweaking Niederreiter encryption for performance. Journal of Cryptographic Engineering, 2013, 3, 29-43.	1.5	7
85	Smaller Keys for Code-Based Cryptography: QC-MDPC McEliece Implementations on Embedded Devices. Lecture Notes in Computer Science, 2013, , 273-292.	1.0	56
86	Compact Implementation and Performance Evaluation of Hash Functions in ATtiny Devices. Lecture Notes in Computer Science, 2013, , 158-172.	1.0	24
87	Software Speed Records for Lattice-Based Signatures. Lecture Notes in Computer Science, 2013, , 67-82.	1.0	37
88	Attacking Atmelâ€™s CryptoMemory EEPROM with Special-Purpose Hardware. Lecture Notes in Computer Science, 2013, , 389-404.	1.0	0
89	Embedded Syndrome-Based Hashing. Lecture Notes in Computer Science, 2012, , 339-357.	1.0	3
90	Side channels as building blocks. Journal of Cryptographic Engineering, 2012, 2, 143-159.	1.5	19

#	Article	IF	Citations
91	IPSecco: A lightweight and reconfigurable IPSec core. , 2012, , .		15
92	Two IP protection schemes for multi-FPGA systems. , 2012, , .		7
93	Practical Lattice-Based Cryptography: A Signature Scheme for Embedded Systems. Lecture Notes in Computer Science, 2012, , 530-547.	1.0	154
94	Using Data Contention in Dual-ported Memories for Security Applications. Journal of Signal Processing Systems, 2012, 67, 15-29.	1.4	14
95	Securely Sealing Multi-FPGA Systems. Lecture Notes in Computer Science, 2012, , 276-289.	1.0	3
96	Compact Implementation and Performance Evaluation of Block Ciphers in ATtiny Devices. Lecture Notes in Computer Science, 2012, , 172-187.	1.0	78
97	Towards One Cycle per Bit Asymmetric Encryption: Code-Based Cryptography on Reconfigurable Hardware. Lecture Notes in Computer Science, 2012, , 340-355.	1.0	22
98	Evaluation of Standardized Password-Based Key Derivation against Parallel Processing Platforms. Lecture Notes in Computer Science, 2012, , 716-733.	1.0	14
99	Towards Efficient Arithmetic for Lattice-Based Cryptography on Reconfigurable Hardware. Lecture Notes in Computer Science, 2012, , 139-158.	1.0	100
100	PRINCE â€“ A Low-Latency Block Cipher for Pervasive Computing Applications. Lecture Notes in Computer Science, 2012, , 208-225.	1.0	440
101	Full Lattice Basis Reduction on Graphics Cards. Lecture Notes in Computer Science, 2012, , 30-44.	1.0	1
102	Decrypting HDCP-protected Video Streams Using Reconfigurable Hardware. , 2011, , .		4
103	MicroECC: A Lightweight Reconfigurable Elliptic Curve Crypto-processor. , 2011, , .		26
104	Utilizing hard cores of modern FPGA devices for high-performance cryptography. Journal of Cryptographic Engineering, 2011, 1, 37-55.	1.5	25
105	The future of high-speed cryptography. , 2011, , .		1
106	Generic Side-Channel Countermeasures for Reconfigurable Devices. Lecture Notes in Computer Science, 2011, , 33-48.	1.0	67
107	An Experimentally Verified Attack on Full Grain-128 Using Dedicated Reconfigurable Hardware. Lecture Notes in Computer Science, 2011, , 327-343.	1.0	52
108	DSPs, BRAMs, and a Pinch of Logic. ACM Transactions on Reconfigurable Technology and Systems, 2010, 3, 1-27.	1.9	35

#	Article	IF	Citations
109	High-Performance Integer Factoring with Reconfigurable Devices. , 2010, , .		5
110	True random number generation in block memories of reconfigurable devices. , 2010, , .		12
111	Breaking Elliptic Curve Cryptosystems Using Reconfigurable Hardware. , 2010, , .		14
112	Modular Integer Arithmetic for Public Key Cryptography. Integrated Circuits and Systems, 2010, , 3-26.	0.2	1
113	Transforming write collisions in block RAMs into security applications. , 2009, , .		10
114	Secure IP-block distribution for hardware devices. , 2009, , .		6
115	Trojan Side-Channels: Lightweight Hardware Trojans through Side-Channel Engineering. Lecture Notes in Computer Science, 2009, , 382-395.	1.0	112
116	MicroEliece: McEliece for Embedded Devices. Lecture Notes in Computer Science, 2009, , 49-64.	1.0	50
117	Cryptanalysis with COPACOBANA. IEEE Transactions on Computers, 2008, 57, 1498-1513.	2.4	98
118	Exploiting the Power of GPUs for Asymmetric Cryptography. Lecture Notes in Computer Science, 2008, , 79-99.	1.0	98
119	Enhancing COPACOBANA for advanced applications in cryptography and cryptanalysis. , 2008, , .		9
120	DSPs, BRAMs and a Pinch of Logic: New Recipes for AES on FPGAs. , 2008, , .		24
121	Special-Purpose Hardware for Solving the Elliptic Curve Discrete Logarithm Problem. ACM Transactions on Reconfigurable Technology and Systems, 2008, 1, 1-21.	1.9	9
122	Ultra High Performance ECC over NIST Primes on Commercial FPGAs. Lecture Notes in Computer Science, 2008, , 62-78.	1.0	88
123	Breaking Legacy Banking Standards with Special-Purpose Hardware. Lecture Notes in Computer Science, 2008, , 128-140.	1.0	2
124	Efficient Hash Collision Search Strategies on Special-Purpose Hardware. Lecture Notes in Computer Science, 2008, , 39-51.	1.0	2
125	Reconfigurable trusted computing in hardware. , 2007, , .		47
126	Dynamic Intellectual Property Protection for Reconfigurable Devices. , 2007, , .		31

#	Article	IF	Citations
127	New Protection Mechanisms for Intellectual Property in Reconfigurable Logic. , 2007, , .		4
128	Establishing Chain of Trust in Reconfigurable Hardware. , 2007, , .		1
129	Efficient Hardware Implementation of Finite Fields with Applications to Cryptography. Acta Applicandae Mathematicae, 2006, 93, 75-118.	0.5	32
130	Practical CCA2-Secure and Masked Ring-LWE Implementation. Iacr Transactions on Cryptographic Hardware and Embedded Systems, 0, , 142-174.	0.0	46