Mehran Mozaffari-Kermani

List of Publications by Year
in descending order

Source: https://exaly.com/author-pdf/9342303/publications.pdf

Version: 2024-02-01

87

papers

1,925

citations

218677

26

h-index

315739

38

g-index

90

all docs

90

docs citations

90

times ranked

966

citing authors

#	Article	IF	Citations
1	Reliable Constructions for the Key Generator of Code-based Post-quantum Cryptosystems on FPGA. ACM Journal on Emerging Technologies in Computing Systems, 2023, 19, 1-20.	2.3	1
2	Hardware Constructions for Lightweight Cryptographic Block Cipher QARMA With Error Detection Mechanisms. IEEE Transactions on Emerging Topics in Computing, 2022, 10, 514-519.	4.6	9
3	Hardware Constructions for Error Detection in Lightweight Authenticated Cipher ASCON Benchmarked on FPGA. IEEE Transactions on Circuits and Systems II: Express Briefs, 2022, 69, 2276-2280.	3.0	6
4	Efficient Error Detection Architectures for Postquantum Signature Falconâ€™s Sampler and KEM SABER. IEEE Transactions on Very Large Scale Integration (VLSI) Systems, 2022, 30, 794-802.	3.1	13
5	Accelerated RISC-V for Post-Quantum SIKE. IEEE Transactions on Circuits and Systems I: Regular Papers, 2022, 69, 2490-2501.	5.4	4
6	Error Detection Architectures for Ring Polynomial Multiplication and Modular Reduction of Ring-LWE in $oldsymbol{rac{mathbb{Z}}/pmathbb{Z}[x]}{x^{n}+1}}$ Benchmarked on ASIC. IEEE Transactions on Reliability, 2021, 70, 362-370.	4.6	20
7	Fault Detection Architectures for Inverted Binary Ring-LWE Construction Benchmarked on FPGA. IEEE Transactions on Circuits and Systems II: Express Briefs, 2021, 68, 1403-1407.	3.0	12
8	Reliable Architectures for Composite-Field-Oriented Constructions of McEliece Post-Quantum Cryptography on FPGA. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 2021, 40, 999-1003.	2.7	11
9	Hardware Constructions for Error Detection in Lightweight Welch-Gong (WG)-Oriented Streamcipher WAGE Benchmarked on FPGA. IEEE Transactions on Emerging Topics in Computing, 2021, , 1-1.	4.6	1
10	High-Performance FPGA Accelerator for SIKE. IEEE Transactions on Computers, 2021, , 1-1.	3.4	8
11	A Monolithic Hardware Implementation of Kyber: Comparing Apples to Apples inÂPQC Candidates. Lecture Notes in Computer Science, 2021, , 108-126.	1.3	8
12	Reliable CRC-Based Error Detection Constructions for Finite Field Multipliers With Applications in Cryptography. IEEE Transactions on Very Large Scale Integration (VLSI) Systems, 2021, 29, 232-236.	3.1	16
13	CRC-Based Error Detection Constructions for FLT and ITA Finite Field Inversions Over GF(2<sup>) Tj ETQq1 1 0.784314 rgBT /Overlock 1	3.1	8
14	Cryptographic Accelerators for Digital Signature Based on Ed25519. IEEE Transactions on Very Large Scale Integration (VLSI) Systems, 2021, 29, 1297-1305.	3.1	53
15	Area-Time Efficient Hardware Architecture for Signature Based on Ed448. IEEE Transactions on Circuits and Systems II: Express Briefs, 2021, 68, 2942-2946.	3.0	6
16	Fast Strategies for the Implementation of SIKE Round 3 on ARM Cortex-M4. IEEE Transactions on Circuits and Systems I: Regular Papers, 2021, 68, 4129-4141.	5.4	48
17	Instruction-Set Accelerated Implementation of CRYSTALS-Kyber. IEEE Transactions on Circuits and Systems I: Regular Papers, 2021, 68, 4648-4659.	5.4	38
18	High-Speed NTT-based Polynomial Multiplication Accelerator for Post-Quantum Cryptography. , 2021, , .		39

#	Article	IF	Citations
19	Accelerated RISC-V for SIKE. , 2021, , .		5
20	Highly Optimized Montgomery Multiplier for SIKE Primes on FPGA. , 2020, , .		16
21	SIKEâ€™d Up: Fast Hardware Architectures for Supersingular Isogeny Key Encapsulation. IEEE Transactions on Circuits and Systems I: Regular Papers, 2020, 67, 4842-4854.	5.4	28
22	Fast, Small, and Area-Time Efficient Architectures for Key-Exchange on Curve25519. , 2020, , .		17
23	High-Performance Fault Diagnosis Schemes for Efficient Hash Algorithm BLAKE. , 2019, , .		2
24	ARMv8 SIKE: Optimized Supersingular Isogeny Key Encapsulation on ARMv8 Processors. IEEE Transactions on Circuits and Systems I: Regular Papers, 2019, 66, 4209-4218.	5.4	13
25	Towards Optimized and Constant-Time CSIDH on Embedded Devices. Lecture Notes in Computer Science, 2019, , 215-231.	1.3	20
26	Reliable Architecture-Oblivious Error Detection Schemes for Secure Cryptographic GCM Structures. IEEE Transactions on Reliability, 2019, 68, 1347-1355.	4.6	16
27	Hardware Constructions for Error Detection of Number-Theoretic Transform Utilized in Secure Cryptographic Architectures. IEEE Transactions on Very Large Scale Integration (VLSI) Systems, 2019, 27, 738-741.	3.1	14
28	Supersingular Isogeny Diffie-Hellman Key Exchange on 64-Bit ARM. IEEE Transactions on Dependable and Secure Computing, 2019, 16, 902-912.	5.4	41
29	Optimized Algorithms and Architectures for Montgomery Multiplication for Post-quantum Cryptography. Lecture Notes in Computer Science, 2019, , 83-98.	1.3	7
30	Reliable Inversion in GF(2<sup>8</sup>) With Redundant Arithmetic for Secure Error Detection of Cryptographic Architectures. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 2018, 37, 696-704.	2.7	8
31	A High-Performance and Scalable Hardware Architecture for Isogeny-Based Cryptography. IEEE Transactions on Computers, 2018, 67, 1594-1609.	3.4	44
32	Reliable and Fault Diagnosis Architectures for Hardware and Software-Efficient Block Cipher KLEIN Benchmarked on FPGA. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 2018, 37, 901-905.	2.7	13
33	Design-for-Error-Detection in Implementations of Cryptographic Nonlinear Substitution Boxes Benchmarked on ASIC. , 2018, , .		0
34	Lightweight Error Detection Architectures through Swapping the Shares for a Subset of S-boxes. , 2018, , .		0
35	NEON SIKE: Supersingular Isogeny Key Encapsulation on ARMv7. Lecture Notes in Computer Science, 2018, , 37-51.	1.3	12
36	Reliable hardware architectures for efficient secure hash functions ECHO and fugue. , 2018, , .		0

#	Article	IF	Citations
37	Comparative realization of error detection schemes for implementations of mixcolumns in lightweight cryptography. , 2018, , .		0
38	Efficient and Reliable Error Detection Architectures of Hash-Counter-Hash Tweakable Enciphering Schemes. Transactions on Embedded Computing Systems, 2018, 17, 1-19.	2.9	9
39	Reliable Hardware Architectures for Cryptographic Block Ciphers LED and HIGHT. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 2017, 36, 1750-1758.	2.7	44
40	Lightweight Architectures for Reliable and Fault Detection Simon and Speck Cryptographic Algorithms on FPGA. Transactions on Embedded Computing Systems, 2017, 16, 1-17.	2.9	19
41	Emerging Embedded and Cyber Physical System Security Challenges and Innovations. IEEE Transactions on Dependable and Secure Computing, 2017, 14, 235-236.	5.4	26
42	Fault Diagnosis Schemes for Low-Energy Block Cipher Midori Benchmarked on FPGA. IEEE Transactions on Very Large Scale Integration (VLSI) Systems, 2017, 25, 1528-1536.	3.1	29
43	Fault Detection Architectures for Post-Quantum Cryptographic Stateless Hash-Based Secure Signatures Benchmarked on ASIC. Transactions on Embedded Computing Systems, 2017, 16, 1-19.	2.9	24
44	Reliable Low-Latency Viterbi Algorithm Architectures Benchmarked on ASIC and FPGA. IEEE Transactions on Circuits and Systems I: Regular Papers, 2017, 64, 208-216.	5.4	14
45	Post-Quantum Cryptography on FPGA Based on Isogenies on Elliptic Curves. IEEE Transactions on Circuits and Systems I: Regular Papers, 2017, 64, 86-99.	5.4	83
46	Reliable Hardware Architectures of the CORDIC Algorithm With a Fixed Angle of Rotations. IEEE Transactions on Circuits and Systems II: Express Briefs, 2017, 64, 972-976.	3.0	8
47	FPGA Realization of Low Register Systolic All-One-Polynomial Multipliers Over $GF(2^{m})$ and Their Applications in Trinomial Multipliers. IEEE Transactions on Very Large Scale Integration (VLSI) Systems, 2017, 25, 725-734.	3.1	11
48	On Fast Calculation of Addition Chains for Isogeny-Based Cryptography. Lecture Notes in Computer Science, 2017, , 323-342.	1.3	4
49	Guest Editorial: Introduction to the Special Section on Emerging Security Trends for Biomedical Computations, Devices, and Infrastructures. IEEE/ACM Transactions on Computational Biology and Bioinformatics, 2016, 13, 399-400.	3.0	3
50	Fault diagnosis schemes for secure lightweight cryptographic block cipher RECTANGLE benchmarked on FPGA. , 2016, , .		11
51	Guest Editorial: Introduction to the Special Issue on Emerging Security Trends for Deeply-Embedded Computing Systems. IEEE Transactions on Emerging Topics in Computing, 2016, 4, 318-320.	4.6	4
52	Error detection reliable architectures of Camellia block cipher applicable to different variants of its substitution boxes. , 2016, , .		4
53	Efficient error detection architectures for CORDIC through recomputing with encoded operands. , 2016, , .		4
54	NEON-SIDH: Efficient Implementation of Supersingular Isogeny Diffie-Hellman Key Exchange Protocol on ARM. Lecture Notes in Computer Science, 2016, , 88-103.	1.3	41

#	Article	IF	Citations
55	Fast Hardware Architectures for Supersingular Isogeny Diffie-Hellman Key Exchange on FPGA. Lecture Notes in Computer Science, 2016, , 191-206.	1.3	28
56	Low-Resource and Fast Binary Edwards Curves Cryptography. Lecture Notes in Computer Science, 2015, , 347-369.	1.3	9
57	Energy-Efficient Long-term Continuous Personal Health Monitoring. IEEE Transactions on Multi-Scale Computing Systems, 2015, 1, 85-98.	2.4	78
58	Reliable hash trees for post-quantum stateless cryptographic hash-based signatures. , 2015, , .		21
59	Secure and Efficient Architectures for Single Exponentiations in Finite Fields Suitable for High-Performance Cryptographic Applications. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 2015, 34, 332-340.	2.7	5
60	Reliable Radix-4 Complex Division for Fault-Sensitive Applications. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 2015, 34, 656-667.	2.7	8
61	Generalized parallel CRC computation on FPGA. , 2015, , .		3
62	Reliable and Error Detection Architectures of Pomaranch for False-Alarm-Sensitive Cryptographic Applications. IEEE Transactions on Very Large Scale Integration (VLSI) Systems, 2015, 23, 2804-2812.	3.1	36
63	High-Performance Two-Dimensional Finite Field Multiplication and Exponentiation for Cryptographic Applications. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 2015, 34, 1569-1576.	2.7	5
64	Systolic Gaussian Normal Basis Multiplier Architectures Suitable for High-Performance Applications. IEEE Transactions on Very Large Scale Integration (VLSI) Systems, 2015, 23, 1969-1972.	3.1	12
65	Systematic Poisoning Attacks on and Defenses for Machine Learning in Healthcare. IEEE Journal of Biomedical and Health Informatics, 2015, 19, 1893-1905.	6.3	140
66	Efficient algorithm and architecture for elliptic curve cryptography for extremely constrained secure applications. IEEE Transactions on Circuits and Systems I: Regular Papers, 2014, 61, 1144-1155.	5.4	53
67	Reliable Concurrent Error Detection Architectures for Extended Euclidean-Based Division Over &lt;inline-formula&gt; &lt;tex-math notation="TeX"&gt;${m GF}(2^{m})$ &lt;/tex-math&gt;&lt;/inline-formula&gt;. IEEE Transactions on Very Large Scale Integration (VLSI) Systems, 2014, 22, 995-1003.	3.1	28
68	Fault-Resilient Lightweight Cryptographic Block Ciphers for Secure Embedded Systems. IEEE Embedded Systems Letters, 2014, 6, 89-92.	1.9	31
69	Low-Latency Digit-Serial Systolic Double Basis Multiplier over &lt;formula formulatype="inline"&gt; &lt;tex Notation="TeX"&gt;$mbi GF{(2^m})$&lt;/tex&gt; &lt;/formula&gt; Using Subquadratic Toeplitz Matrix-Vector Product Approach. IEEE Transactions on Computers, 2014, 63, 1169-1181.	3.4	30
70	Efficient and Concurrent Reliable Realization of the Secure Cryptographic SHA-3 Algorithm. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 2014, 33, 1105-1109.	2.7	43
71	Dual-Basis Superserial Multipliers for Secure Applications and Lightweight Cryptographic Architectures. IEEE Transactions on Circuits and Systems II: Express Briefs, 2014, 61, 125-129.	3.0	22
72	Efficient Fault Diagnosis Schemes for Reliable Lightweight Cryptographic ISO/IEC Standard CLEFIA Benchmarked on ASIC and FPGA. IEEE Transactions on Industrial Electronics, 2013, 60, 5925-5932.	7.9	31

#	Article	IF	Citations
73	Emerging Frontiers in Embedded Security. , 2013, , .		24
74	Energy-efficient and Secure Sensor Data Transmission Using Encompression. , 2013, , .		18
75	Efficient and High-Performance Parallel Hardware Architectures for the AES-GCM. IEEE Transactions on Computers, 2012, 61, 1165-1178.	3.4	58
76	Reliable Hardware Architectures for the Third-Round SHA-3 Finalist Grostl Benchmarked on FPGA Platform. , 2011, , .		18
77	A High-Performance Fault Diagnosis Approach for the AES SubBytes Utilizing Mixed Bases. , 2011, , .		15
78	A Lightweight High-Performance Fault Detection Scheme for the Advanced Encryption Standard Using Composite Fields. IEEE Transactions on Very Large Scale Integration (VLSI) Systems, 2011, 19, 85-91.	3.1	69
79	A Low-Power High-Performance Concurrent Fault Detection Approach for the Composite Field S-Box and Inverse S-Box. IEEE Transactions on Computers, 2011, 60, 1327-1340.	3.4	23
80	Concurrent Structure-Independent Fault Detection Schemes for the Advanced Encryption Standard. IEEE Transactions on Computers, 2010, 59, 608-622.	3.4	99
81	Fault Detection Structures of the S-boxes and the Inverse S-boxes for the Advanced Encryption Standard. Journal of Electronic Testing: Theory and Applications (JETTA), 2009, 25, 225-245.	1.2	31
82	A low-cost S-box for the Advanced Encryption Standard using normal basis. , 2009, , .		12
83	A Lightweight Concurrent Fault Detection Scheme for the AES S-Boxes Using Normal Basis. Lecture Notes in Computer Science, 2008, , 113-129.	1.3	18
84	A Structure-independent Approach for Fault Detection Hardware Implementations of the Advanced Encryption Standard. , 2007, , .		10
85	A Structure-independent Approach for Fault Detection Hardware Implementations of the Advanced Encryption Standard. , 2007, , .		0
86	Parity-Based Fault Detection Architecture of S-box for Advanced Encryption Standard. Defect and Fault Tolerance in VLSI Systems, Proceedings of the IEEE International Symposium on, 2006, , .	0.0	32
87	Parity Prediction of S-Box for AES. , 2006, , .		7