Reza Azarderakhsh

List of Publications by Year
in descending order

75	1,435	331538	434063
papers	citations	21 h-index	31 g-index

78	78	78	540
all docs	docs citations	times ranked	citing authors

#	Article	IF	Citations
1	Post-Quantum Cryptography on FPGA Based on Isogenies on Elliptic Curves. IEEE Transactions on Circuits and Systems I: Regular Papers, 2017, 64, 86-99.	3.5	83
2	Key Compression for Isogeny-Based Cryptosystems. , 2016, , .		62
3	A Post-quantum Digital Signature Scheme Based on Supersingular Isogenies. Lecture Notes in Computer Science, 2017, , 163-181.	1.0	59
4	Cryptographic Accelerators for Digital Signature Based on Ed25519. IEEE Transactions on Very Large Scale Integration (VLSI) Systems, 2021, 29, 1297-1305.	2.1	53
5	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.	3.5	48
6	Low-Complexity Multiplier Architectures for Single and Hybrid-Double Multiplications in Gaussian Normal Bases. IEEE Transactions on Computers, 2013, 62, 744-757.	2.4	47
7	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.	1.9	44
8	A High-Performance and Scalable Hardware Architecture for Isogeny-Based Cryptography. IEEE Transactions on Computers, 2018, 67, 1594-1609.	2.4	44
9	NEON-SIDH: Efficient Implementation of Supersingular Isogeny Diffie-Hellman Key Exchange Protocol on ARM. Lecture Notes in Computer Science, 2016, , 88-103.	1.0	41
10	Supersingular Isogeny Diffie-Hellman Key Exchange on 64-Bit ARM. IEEE Transactions on Dependable and Secure Computing, 2019, 16, 902-912.	3.7	41
11	High-Speed NTT-based Polynomial Multiplication Accelerator for Post-Quantum Cryptography. , 2021, , .		39
12	Parallel and High-Speed Computations of Elliptic Curve Cryptography Using Hybrid-Double Multipliers. IEEE Transactions on Parallel and Distributed Systems, 2015, 26, 1668-1677.	4.0	38
13	Instruction-Set Accelerated Implementation of CRYSTALS-Kyber. IEEE Transactions on Circuits and Systems I: Regular Papers, 2021, 68, 4648-4659.	3.5	38
14	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.	2.1	36
15	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.	5.2	31
16	Fault-Resilient Lightweight Cryptographic Block Ciphers for Secure Embedded Systems. IEEE Embedded Systems Letters, 2014, 6, 89-92.	1.3	31
17	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.	2.1	29
18	Reliable Concurrent Error Detection Architectures for Extended Euclidean-Based Division Over <inline-formula> <tex-math notation="TeX">${m GF}(2^{m})$ </tex-math></inline-formula>. IEEE Transactions on Very Large Scale Integration (VLSI) Systems, 2014, 22, 995-1003.	2.1	28

#	Article	IF	Citations
19	SIKEâ€™d Up: Fast Hardware Architectures for Supersingular Isogeny Key Encapsulation. IEEE Transactions on Circuits and Systems I: Regular Papers, 2020, 67, 4842-4854.	3.5	28
20	Fast Hardware Architectures for Supersingular Isogeny Diffie-Hellman Key Exchange on FPGA. Lecture Notes in Computer Science, 2016, , 191-206.	1.0	28
21	Emerging Embedded and Cyber Physical System Security Challenges and Innovations. IEEE Transactions on Dependable and Secure Computing, 2017, 14, 235-236.	3.7	26
22	Supersingular Isogeny Key Encapsulation (SIKE) Round 2 on ARM Cortex-M4. IEEE Transactions on Computers, 2021, 70, 1705-1718.	2.4	25
23	Fault Detection Architectures for Post-Quantum Cryptographic Stateless Hash-Based Secure Signatures Benchmarked on ASIC. Transactions on Embedded Computing Systems, 2017, 16, 1-19.	2.1	24
24	Reliable hash trees for post-quantum stateless cryptographic hash-based signatures. , 2015, , .		21
25	Towards Optimized and Constant-Time CSIDH on Embedded Devices. Lecture Notes in Computer Science, 2019, , 215-231.	1.0	20
26	Efficient Software Implementation of Ring-LWE Encryption on IoT Processors. IEEE Transactions on Computers, 2020, 69, 1424-1433.	2.4	20
27	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.	3.5	20
28	Fast Inversion in <formula formulatype="inline"><tex Notation="TeX">${schmi{GF(2^m)}}$</tex></formula> with Normal Basis Using Hybrid-Double Multipliers. IEEE Transactions on Computers, 2014, 63, 1041-1047.	2.4	19
29	Optimized Implementation of SIKE Round 2 on 64-bit ARM Cortex-A Processors. IEEE Transactions on Circuits and Systems I: Regular Papers, 2020, 67, 2659-2671.	3.5	18
30	Fast, Small, and Area-Time Efficient Architectures for Key-Exchange on Curve25519. , 2020, , .		17
31	Reliable Architecture-Oblivious Error Detection Schemes for Secure Cryptographic GCM Structures. IEEE Transactions on Reliability, 2019, 68, 1347-1355.	3.5	16
32	Highly Optimized Montgomery Multiplier for SIKE Primes on FPGA. , 2020, , .		16
33	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.	2.1	16
34	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.	2.1	14
35	A New Double Point Multiplication Algorithm and Its Application to Binary Elliptic Curves with Endomorphisms. IEEE Transactions on Computers, 2014, 63, 2614-2619.	2.4	13
36	Fast Software Implementations of Bilinear Pairings. IEEE Transactions on Dependable and Secure Computing, 2017, 14, 605-619.	3.7	13

#	Article	IF	Citations
37	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.	1.9	13
38	ARMv8 SIKE: Optimized Supersingular Isogeny Key Encapsulation on ARMv8 Processors. IEEE Transactions on Circuits and Systems I: Regular Papers, 2019, 66, 4209-4218.	3.5	13
39	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.	2.1	13
40	Systolic Gaussian Normal Basis Multiplier Architectures Suitable for High-Performance Applications. IEEE Transactions on Very Large Scale Integration (VLSI) Systems, 2015, 23, 1969-1972.	2.1	12
41	NEON SIKE: Supersingular Isogeny Key Encapsulation on ARMv7. Lecture Notes in Computer Science, 2018, , 37-51.	1.0	12
42	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.	2.2	12
43	Fault diagnosis schemes for secure lightweight cryptographic block cipher RECTANGLE benchmarked on FPGA. , 2016, , .		11
44	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.	2.1	11
45	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.	1.9	11
46	Efficient Hardware Implementations for Elliptic Curve Cryptography over Curve448. Lecture Notes in Computer Science, 2020, , 228-247.	1.0	11
47	A Generalization of Addition Chains and Fast Inversions in Binary Fields. IEEE Transactions on Computers, 2015, 64, 2421-2432.	2.4	10
48	Side-Channel Attacks on Quantum-Resistant Supersingular Isogeny Diffie-Hellman. Lecture Notes in Computer Science, 2018, , 64-81.	1.0	10
49	Efficient and Reliable Error Detection Architectures of Hash-Counter-Hash Tweakable Enciphering Schemes. Transactions on Embedded Computing Systems, 2018, 17, 1-19.	2.1	9
50	Hardware Constructions for Lightweight Cryptographic Block Cipher QARMA With Error Detection Mechanisms. IEEE Transactions on Emerging Topics in Computing, 2022, 10, 514-519.	3.2	9
51	Common Subexpression Algorithms for Space-Complexity Reduction of Gaussian Normal Basis Multiplication. IEEE Transactions on Information Theory, 2015, 61, 2357-2369.	1.5	8
52	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.	2.2	8
53	Reliable Inversion in GF(2⁸) 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.	1.9	8
54	High-Performance FPGA Accelerator for SIKE. IEEE Transactions on Computers, 2021, , 1-1.	2.4	8

#	Article	IF	Citations
55	A Monolithic Hardware Implementation of Kyber: Comparing Apples to Apples inÂPQC Candidates. Lecture Notes in Computer Science, 2021, , 108-126.	1.0	8
56	CRC-Based Error Detection Constructions for FLT and ITA Finite Field Inversions Over GF(2<sup>) Tj ETQq0 0 0 rgBT /Overlock 10 Tf 50 7	2.1	8
57	Optimized Algorithms and Architectures for Montgomery Multiplication for Post-quantum Cryptography. Lecture Notes in Computer Science, 2019, , 83-98.	1.0	7
58	Area-Time Efficient Hardware Architecture for Signature Based on Ed448. IEEE Transactions on Circuits and Systems II: Express Briefs, 2021, 68, 2942-2946.	2.2	6
59	How Not to Create an Isogeny-Based PAKE. Lecture Notes in Computer Science, 2020, , 169-186.	1.0	6
60	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.	2.2	6
61	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.	1.9	5
62	An Exposure Model for Supersingular Isogeny Diffie-Hellman Key Exchange. Lecture Notes in Computer Science, 2018, , 452-469.	1.0	5
63	Accelerated RISC-V for SIKE. , 2021, , .		5
64	Error detection reliable architectures of Camellia block cipher applicable to different variants of its substitution boxes. , 2016, , .		4
65	Efficient error detection architectures for CORDIC through recomputing with encoded operands. , 2016, , .		4
66	Accelerated RISC-V for Post-Quantum SIKE. IEEE Transactions on Circuits and Systems I: Regular Papers, 2022, 69, 2490-2501.	3.5	4
67	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.	1.9	3
68	SIKE in 32-bit ARM Processors Based on Redundant Number System for NIST Level-II. Transactions on Embedded Computing Systems, 2021, 20, 1-23.	2.1	3
69	High-Performance Fault Diagnosis Schemes for Efficient Hash Algorithm BLAKE. , 2019, , .		2
70	Hardware Deployment of Hybrid PQC: SIKE+ECDH. Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, 2021, , 475-491.	0.2	2
71	Faster Isogenies for Post-quantum Cryptography: SIKE. Lecture Notes in Computer Science, 2022, , 49-72.	1.0	1
72	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.	1.8	1

#	Article	IF	Citations
73	Design-for-Error-Detection in Implementations of Cryptographic Nonlinear Substitution Boxes Benchmarked on ASIC. , 2018, , .		0
74	Parallelism strategies for the tuneable golden-claw finding problem. International Journal of Computer Mathematics: Computer Systems Theory, 2021, 6, 337-363.	0.7	0
75	No Silver Bullet: Optimized Montgomery Multiplication on Various 64-Bit ARM Platforms. Lecture Notes in Computer Science, 2021, , 194-205.	1.0	0