

Hwajeong Seo

List of Publications by Citations

Source: <https://exaly.com/author-pdf/7214375/hwajeong-seo-publications-by-citations.pdf>

Version: 2024-04-27

This document has been generated based on the publications and citations recorded by exaly.com. For the latest version of this publication list, visit the link given above.

The third column is the impact factor (IF) of the journal, and the fourth column is the number of citations of the article.

92
papers

670
citations

13
h-index

20
g-index

96
ext. papers

818
ext. citations

2.2
avg, IF

4.77
L-index

#	Paper	IF	Citations
92	Efficient Implementation of NIST-Compliant Elliptic Curve Cryptography for 8-bit AVR-Based Sensor Nodes. <i>IEEE Transactions on Information Forensics and Security</i> , 2016 , 11, 1385-1397	8	47
91	On Emerging Family of Elliptic Curves to Secure Internet of Things: ECC Comes of Age. <i>IEEE Transactions on Dependable and Secure Computing</i> , 2016 , 1-1	3.9	36
90	Efficient Ring-LWE Encryption on 8-Bit AVR Processors. <i>Lecture Notes in Computer Science</i> , 2015 , 663-682.	0.9	34
89	IoT-NUMS: Evaluating NUMS Elliptic Curve Cryptography for IoT Platforms. <i>IEEE Transactions on Information Forensics and Security</i> , 2019 , 14, 720-729	8	28
88	SIDH on ARM: Faster Modular Multiplications for Faster Post-Quantum Supersingular Isogeny Key Exchange. <i>Iacr Transactions on Cryptographic Hardware and Embedded Systems</i> , 1-20		25
87	Multi-precision Squaring for Public-Key Cryptography on Embedded Microprocessors. <i>Lecture Notes in Computer Science</i> , 2013 , 227-243	0.9	23
86	Secure IoT framework and 2D architecture for End-To-End security. <i>Journal of Supercomputing</i> , 2018 , 74, 3521-3535	2.5	21
85	Multi-precision Multiplication for Public-Key Cryptography on Embedded Microprocessors. <i>Lecture Notes in Computer Science</i> , 2012 , 55-67	0.9	20
84	Binary and prime field multiplication for public key cryptography on embedded microprocessors. <i>Security and Communication Networks</i> , 2014 , 7, 774-787	1.9	18
83	Performance enhancement of TinyECC based on multiplication optimizations. <i>Security and Communication Networks</i> , 2013 , 6, 151-160	1.9	16
82	Supersingular Isogeny Key Encapsulation (SIKE) Round 2 on ARM Cortex-M4. <i>IEEE Transactions on Computers</i> , 2020 , 1-1	2.5	16
81	Optimized Implementation of SIKE Round 2 on 64-bit ARM Cortex-A Processors. <i>IEEE Transactions on Circuits and Systems I: Regular Papers</i> , 2020 , 67, 2659-2671	3.9	14
80	Memory-Efficient Implementation of Elliptic Curve Cryptography for the Internet-of-Things. <i>IEEE Transactions on Dependable and Secure Computing</i> , 2019 , 16, 521-529	3.9	14
79	SIKE Round 2 Speed Record on ARM Cortex-M4. <i>Lecture Notes in Computer Science</i> , 2019 , 39-60	0.9	13
78	Efficient Software Implementation of Ring-LWE Encryption on IoT Processors. <i>IEEE Transactions on Computers</i> , 2020 , 69, 1424-1433	2.5	13
77	A fast ARX model-based image encryption scheme. <i>Multimedia Tools and Applications</i> , 2016 , 75, 14685-14706	1.7	12
76	Parallel Implementations of SIMON and SPECK 2016 ,		11

75	Optimized Multi-Precision Multiplication for Public-Key Cryptography on Embedded Microprocessors. <i>International Journal of Computer and Communication Engineering</i> , 2013 , 255-259	0.2	11
74	Grover on Korean Block Ciphers. <i>Applied Sciences (Switzerland)</i> , 2020 , 10, 6407	2.6	11
73	High-Performance Ideal Lattice-Based Cryptography on 8-Bit AVR Microcontrollers. <i>Transactions on Embedded Computing Systems</i> , 2017 , 16, 1-24	1.8	10
72	Compact Implementations of HIGHT Block Cipher on IoT Platforms. <i>Security and Communication Networks</i> , 2019 , 2019, 1-10	1.9	10
71	Four(\mathbb{Q}) on Embedded Devices with Strong Countermeasures Against Side-Channel Attacks. <i>Lecture Notes in Computer Science</i> , 2017 , 665-686	0.9	10
70	Efficient arithmetic on ARM-NEON and its application for high-speed RSA implementation. <i>Security and Communication Networks</i> , 2016 , 9, 5401-5411	1.9	10
69	Compact Implementations of ARX-Based Block Ciphers on IoT Processors. <i>Transactions on Embedded Computing Systems</i> , 2018 , 17, 1-16	1.8	9
68	Pseudo random number generator and Hash function for embedded microprocessors 2014 ,		9
67	Highly Efficient Implementation of NIST-Compliant Koblitz Curve for 8-bit AVR-Based Sensor Nodes. <i>IEEE Access</i> , 2018 , 6, 67637-67652	3.5	9
66	Efficient Elliptic Curve Cryptography for Embedded Devices. <i>Transactions on Embedded Computing Systems</i> , 2017 , 16, 1-18	1.8	8
65	Lightweight Implementations of NIST P-256 and SM2 ECC on 8-bit Resource-Constraint Embedded Device. <i>Transactions on Embedded Computing Systems</i> , 2019 , 18, 1-13	1.8	8
64	Efficient Implementation of ARX-Based Block Ciphers on 8-Bit AVR Microcontrollers. <i>Mathematics</i> , 2020 , 8, 1837	2.3	8
63	Implementing RSA for sensor nodes in smart cities. <i>Personal and Ubiquitous Computing</i> , 2017 , 21, 807-813	1.1	8
62	Efficient Implementation of PRESENT and GIFT on Quantum Computers. <i>Applied Sciences (Switzerland)</i> , 2021 , 11, 4776	2.6	8
61	Designing a CHAM Block Cipher on Low-End Microcontrollers for Internet of Things. <i>Electronics (Switzerland)</i> , 2020 , 9, 1548	2.6	7
60	Karatsuba-Block-Comb technique for elliptic curve cryptography over binary fields. <i>Security and Communication Networks</i> , 2015 , 8, 3121-3130	1.9	7
59	Zigbee security for visitors in home automation using attribute based proxy re-encryption 2011 ,		7
58	PIPO: A Lightweight Block Cipher with Efficient Higher-Order Masking Software Implementations. <i>Lecture Notes in Computer Science</i> , 2021 , 99-122	0.9	7

57	A High-Speed Public-Key Signature Scheme for 8-b IoT-Constrained Devices. <i>IEEE Internet of Things Journal</i> , 2020 , 7, 3663-3677	10.7	6
56	Four \mathbb{Q} on Embedded Devices with Strong Countermeasures Against Side-Channel Attacks. <i>IEEE Transactions on Dependable and Secure Computing</i> , 2018 , 1-1	3.9	6
55	Performance evaluation of twisted Edwards-form elliptic curve cryptography for wireless sensor nodes. <i>Security and Communication Networks</i> , 2015 , 8, 3301-3310	1.9	6
54	Optimized Karatsuba squaring on 8-bit AVR processors. <i>Security and Communication Networks</i> , 2015 , 8, 3546-3554	1.9	6
53	Quantum implementation and resource estimates for Rectangle and Knot. <i>Quantum Information Processing</i> , 2021 , 20, 1	1.6	6
52	A Synthesis of Multi-Precision Multiplication and Squaring Techniques for 8-Bit Sensor Nodes: State-of-the-Art Research and Future Challenges. <i>Journal of Computer Science and Technology</i> , 2016 , 31, 284-299	1.7	6
51	Compact implementations of Curve Ed448 on low-end IoT platforms. <i>ETRI Journal</i> , 2019 , 41, 863-872	1.4	6
50	PAGE Practical AES-GCM Encryption for Low-End Microcontrollers. <i>Applied Sciences (Switzerland)</i> , 2020 , 10, 3131	2.6	5
49	Memory Efficient Implementation of Modular Multiplication for 32-bit ARM Cortex-M4. <i>Applied Sciences (Switzerland)</i> , 2020 , 10, 1539	2.6	5
48	Secure GCM implementation on AVR. <i>Discrete Applied Mathematics</i> , 2018 , 241, 58-66	1	5
47	Secure Data Encryption for Cloud-Based Human Care Services. <i>Journal of Sensors</i> , 2018 , 2018, 1-10	2	5
46	ZigBee security for Home automation using attribute-based cryptography 2011 ,		5
45	Low-Power Encryption Algorithm Block Cipher in JavaScript. <i>Journal of Information and Communication Convergence Engineering</i> , 2014 , 12, 252-256		5
44	ACE: ARIA-CTR Encryption for Low-End Embedded Processors. <i>Sensors</i> , 2020 , 20,	3.8	5
43	Grover on PIPO. <i>Electronics (Switzerland)</i> , 2021 , 10, 1194	2.6	5
42	Compact Software Implementation of Public-Key Cryptography on MSP430X. <i>Transactions on Embedded Computing Systems</i> , 2018 , 17, 1-12	1.8	5
41	Multi-precision squaring on MSP and ARM processors 2014 ,		4
40	Consecutive Operand-Caching Method for Multiprecision Multiplication, Revisited. <i>Journal of Information and Communication Convergence Engineering</i> , 2015 , 13, 27-35		4

39	Masked Implementation of PIPO Block Cipher on 8-bit AVR Microcontrollers. <i>Lecture Notes in Computer Science</i> , 2021 , 171-182	0.9	4
38	Small private key MQPKS on an embedded microprocessor. <i>Sensors</i> , 2014 , 14, 5441-58	3.8	3
37	Binary field multiplication on ARMv8. <i>Security and Communication Networks</i> , 2016 , 9, 2051-2058	1.9	3
36	Hybrid approach of parallel implementation on CPU+GPU for high-speed ECDSA verification. <i>Journal of Supercomputing</i> , 2019 , 75, 4329-4349	2.5	3
35	High-Speed Implementation of PRESENT on AVR Microcontroller. <i>Mathematics</i> , 2021 , 9, 374	2.3	3
34	Efficient Parallel Implementation of Matrix Multiplication for Lattice-Based Cryptography on Modern ARM Processor. <i>Security and Communication Networks</i> , 2018 , 2018, 1-10	1.9	3
33	Efficient Implementation of AES-CTR and AES-ECB on GPUs with Applications for High-speed FrodoKEM and Exhaustive Key Search. <i>IEEE Transactions on Circuits and Systems II: Express Briefs</i> , 2022 , 1-1	3.5	3
32	Fast Number Theoretic Transform for Ring-LWE on 8-bit AVR Embedded Processor. <i>Sensors</i> , 2020 , 20,	3.8	2
31	Hybrid Montgomery Reduction. <i>Transactions on Embedded Computing Systems</i> , 2016 , 15, 1-13	1.8	2
30	Montgomery multiplication and squaring for Optimal Prime Fields. <i>Computers and Security</i> , 2015 , 52, 276-291	4.9	2
29	ARMed Frodo. <i>Lecture Notes in Computer Science</i> , 2021 , 206-217	0.9	2
28	Lightweight Fault Attack Resistance in Software Using Intra-instruction Redundancy, Revisited. <i>Lecture Notes in Computer Science</i> , 2018 , 3-15	0.9	2
27	Compact Implementation of CHAM Block Cipher on Low-End Microcontrollers. <i>Lecture Notes in Computer Science</i> , 2020 , 127-141	0.9	2
26	Four Anchor Sensor Nodes Based Localization Algorithm over Three-Dimensional Space. <i>Journal of Information and Communication Convergence Engineering</i> , 2012 , 10, 349-358		2
25	Parallel Implementations of ARX-Based Block Ciphers on Graphic Processing Units. <i>Mathematics</i> , 2020 , 8, 1894	2.3	2
24	Compact Implementation of ARIA on 16-Bit MSP430 and 32-Bit ARM Cortex-M3 Microcontrollers. <i>Electronics (Switzerland)</i> , 2021 , 10, 908	2.6	2
23	Masked Implementation of Format Preserving Encryption on Low-End AVR Microcontrollers and High-End ARM Processors. <i>Mathematics</i> , 2021 , 9, 1294	2.3	2
22	Convolutional Neural Network-Based Cryptography Ransomware Detection for Low-End Embedded Processors. <i>Mathematics</i> , 2021 , 9, 705	2.3	2

21	Personal identification number entry for Google glass. <i>Computers and Electrical Engineering</i> , 2017 , 63, 160-167	4.3	1
20	Multiprecision Multiplication on ARMv8 2017 ,		1
19	Implementation of an RFID Key Management System for DASH7. <i>Journal of Information and Communication Convergence Engineering</i> , 2014 , 12, 19-25		1
18	Secure Number Theoretic Transform and Speed Record for Ring-LWE Encryption on Embedded Processors. <i>Lecture Notes in Computer Science</i> , 2018 , 175-188	0.9	1
17	Multi-precision Squaring for Public-Key Cryptography on Embedded Microprocessors, a Step Forward. <i>Lecture Notes in Computer Science</i> , 2017 , 331-340	0.9	1
16	ASIC-Resistant Proof of Work Based on Power Analysis of Low-End Microcontrollers. <i>Mathematics</i> , 2020 , 8, 1343	2.3	1
15	SIKE in 32-bit ARM Processors Based on Redundant Number System for NIST Level-II. <i>Transactions on Embedded Computing Systems</i> , 2021 , 20, 1-23	1.8	1
14	Curve448 on 32-Bit ARM Cortex-M4. <i>Lecture Notes in Computer Science</i> , 2021 , 125-139	0.9	1
13	TensorCrypto: High Throughput Acceleration of Lattice-Based Cryptography Using Tensor Core on GPU. <i>IEEE Access</i> , 2022 , 10, 20616-20632	3.5	1
12	A New Method for Designing Lightweight S-Boxes With High Differential and Linear Branch Numbers, and its Application. <i>IEEE Access</i> , 2021 , 9, 150592-150607	3.5	0
11	Efficient Implementation of Lightweight Hash Functions on GPU and Quantum Computers for IoT Applications. <i>IEEE Access</i> , 2022 , 1-1	3.5	0
10	Parallel Implementations of CHAM. <i>Lecture Notes in Computer Science</i> , 2019 , 93-104	0.9	
9	Fixed-base comb with window-non-adjacent form (NAF) method for scalar multiplication. <i>Sensors</i> , 2013 , 13, 9483-512	3.8	
8	Montgomery Multiplication for Public Key Cryptography on MSP430X. <i>Transactions on Embedded Computing Systems</i> , 2020 , 19, 1-15	1.8	
7	No Silver Bullet: Optimized Montgomery Multiplication on Various 64-Bit ARM Platforms. <i>Lecture Notes in Computer Science</i> , 2021 , 194-205	0.9	
6	Ring-LWE on 8-Bit AVR Embedded Processor. <i>Lecture Notes in Computer Science</i> , 2020 , 315-327	0.9	
5	Secure Message Transmission against Remote Control System. <i>Journal of Information and Communication Convergence Engineering</i> , 2016 , 14, 233-239		
4	Comprehensive PEP Performance Analysis of MCIK-OFDM with a Low-Complexity Detector in Fading Channels. <i>Advanced Science Letters</i> , 2017 , 23, 10255-10258	0.1	

- | | | |
|---|---|-----|
| 3 | Secure HIGHT Implementation on ARM Processors. <i>Mathematics</i> , 2021 , 9, 1044 | 2.3 |
| 2 | Generative Adversarial Networks-Based Pseudo-Random Number Generator for Embedded Processors. <i>Lecture Notes in Computer Science</i> , 2021 , 215-234 | 0.9 |
| 1 | DPCrypto: Acceleration of Post-Quantum Cryptography Using Dot-Product Instructions on GPUs. <i>IEEE Transactions on Circuits and Systems I: Regular Papers</i> , 2022 , 1-14 | 3.9 |