# Hwajeong Seo

## List of Publications by Year in Descending Order



| | | | |
|---|---|---|---|
| 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 | TensorCrypto: High Throughput Acceleration of Lattice-Based Cryptography Using Tensor Core on GPU. *IEEE Access*, **2022**, 10, 20616-20632 | 3.5 | 1 |
| 91 | Efficient Implementation of AES-CTR and AES-ECB on GPUs with Applications for High-speed FrodoKEM and Exhaustive Key Search. *IEEE Transactions on Circuits and Systems II: Express Briefs*, **2022**, 1-1 | 3.5 | 3 |
| 90 | Efficient Implementation of Lightweight Hash Functions on GPU and Quantum Computers for IoT Applications. *IEEE Access*, **2022**, 1-1 | 3.5 | 0 |
| 89 | DPCrypto: Acceleration of Post-Quantum Cryptography Using Dot-Product Instructions on GPUs. *IEEE Transactions on Circuits and Systems I: Regular Papers*, **2022**, 1-14 | 3.9 | |
| 88 | Quantum implementation and resource estimates for Rectangle and Knot. *Quantum Information Processing*, **2021**, 20, 1 | 1.6 | 6 |
| 87 | A New Method for Designing Lightweight S-Boxes With High Differential and Linear Branch Numbers, and its Application. *IEEE Access*, **2021**, 9, 150592-150607 | 3.5 | 0 |
| 86 | Masked Implementation of PIPO Block Cipher on 8-bit AVR Microcontrollers. *Lecture Notes in Computer Science*, **2021**, 171-182 | 0.9 | 4 |
| 85 | No Silver Bullet: Optimized Montgomery Multiplication on Various 64-Bit ARM Platforms. *Lecture Notes in Computer Science*, **2021**, 194-205 | 0.9 | |
| 84 | ARMed Frodo. *Lecture Notes in Computer Science*, **2021**, 206-217 | 0.9 | 2 |
| 83 | SIKE in 32-bit ARM Processors Based on Redundant Number System for NIST Level-II. *Transactions on Embedded Computing Systems*, **2021**, 20, 1-23 | 1.8 | 1 |
| 82 | Compact Implementation of ARIA on 16-Bit MSP430 and 32-Bit ARM Cortex-M3 Microcontrollers. *Electronics (Switzerland)*, **2021**, 10, 908 | 2.6 | 2 |
| 81 | Grover on PIPO. *Electronics (Switzerland)*, **2021**, 10, 1194 | 2.6 | 5 |
| 80 | Efficient Implementation of PRESENT and GIFT on Quantum Computers. *Applied Sciences (Switzerland)*, **2021**, 11, 4776 | 2.6 | 8 |
| 79 | Secure HIGHT Implementation on ARM Processors. *Mathematics*, **2021**, 9, 1044 | 2.3 | |
| 78 | Masked Implementation of Format Preserving Encryption on Low-End AVR Microcontrollers and High-End ARM Processors. *Mathematics*, **2021**, 9, 1294 | 2.3 | 2 |
| 77 | Curve448 on 32-Bit ARM Cortex-M4. *Lecture Notes in Computer Science*, **2021**, 125-139 | 0.9 | 1 |
| 76 | Generative Adversarial Networks-Based Pseudo-Random Number Generator for Embedded Processors. *Lecture Notes in Computer Science*, **2021**, 215-234 | 0.9 | |

| | | | |
|---|---|---|---|
| 75 | High-Speed Implementation of PRESENT on AVR Microcontroller. *Mathematics*, **2021**, 9, 374 | 2.3 | 3 |
| 74 | Convolutional Neural Network-Based Cryptography Ransomware Detection for Low-End Embedded Processors. *Mathematics*, **2021**, 9, 705 | 2.3 | 2 |
| 73 | PIPO: A Lightweight Block Cipher with Efficient Higher-Order Masking Software Implementations. *Lecture Notes in Computer Science*, **2021**, 99-122 | 0.9 | 7 |
| 72 | Designing a CHAM Block Cipher on Low-End Microcontrollers for Internet of Things. *Electronics (Switzerland)*, **2020**, 9, 1548 | 2.6 | 7 |
| 71 | Efficient Implementation of ARX-Based Block Ciphers on 8-Bit AVR Microcontrollers. *Mathematics*, **2020**, 8, 1837 | 2.3 | 8 |
| 70 | PAGEPractical AES-GCM Encryption for Low-End Microcontrollers. *Applied Sciences (Switzerland)*, **2020**, 10, 3131 | 2.6 | 5 |
| 69 | 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 | 3.9 | 14 |
| 68 | Memory Efficient Implementation of Modular Multiplication for 32-bit ARM Cortex-M4. *Applied Sciences (Switzerland)*, **2020**, 10, 1539 | 2.6 | 5 |
| 67 | Fast Number Theoretic Transform for Ring-LWE on 8-bit AVR Embedded Processor. *Sensors*, **2020**, 20, | 3.8 | 2 |
| 66 | A High-Speed Public-Key Signature Scheme for 8-b IoT-Constrained Devices. *IEEE Internet of Things Journal*, **2020**, 7, 3663-3677 | 10.7 | 6 |
| 65 | Montgomery Multiplication for Public Key Cryptography on MSP430X. *Transactions on Embedded Computing Systems*, **2020**, 19, 1-15 | 1.8 | |
| 64 | Ring-LWE on 8-Bit AVR Embedded Processor. *Lecture Notes in Computer Science*, **2020**, 315-327 | 0.9 | |
| 63 | Compact Implementation of CHAM Block Cipher on Low-End Microcontrollers. *Lecture Notes in Computer Science*, **2020**, 127-141 | 0.9 | 2 |
| 62 | Parallel Implementations of ARX-Based Block Ciphers on Graphic Processing Units. *Mathematics*, **2020**, 8, 1894 | 2.3 | 2 |
| 61 | ACE: ARIA-CTR Encryption for Low-End Embedded Processors. *Sensors*, **2020**, 20, | 3.8 | 5 |
| 60 | ASIC-Resistant Proof of Work Based on Power Analysis of Low-End Microcontrollers. *Mathematics*, **2020**, 8, 1343 | 2.3 | 1 |
| 59 | Grover on Korean Block Ciphers. *Applied Sciences (Switzerland)*, **2020**, 10, 6407 | 2.6 | 11 |
| 58 | Supersingular Isogeny Key Encapsulation (SIKE) Round 2 on ARM Cortex-M4. *IEEE Transactions on Computers*, **2020**, 1-1 | 2.5 | 16 |

| | | | |
|---|---|---|---|
| 57 | Efficient Software Implementation of Ring-LWE Encryption on IoT Processors. *IEEE Transactions on Computers*, **2020**, 69, 1424-1433 | 2.5 | 13 |
| 56 | Lightweight Implementations of NIST P-256 and SM2 ECC on 8-bit Resource-Constraint Embedded Device. *Transactions on Embedded Computing Systems*, **2019**, 18, 1-13 | 1.8 | 8 |
| 55 | Parallel Implementations of CHAM. *Lecture Notes in Computer Science*, **2019**, 93-104 | 0.9 | |
| 54 | IoT-NUMS: Evaluating NUMS Elliptic Curve Cryptography for IoT Platforms. *IEEE Transactions on Information Forensics and Security*, **2019**, 14, 720-729 | 8 | 28 |
| 53 | Compact Implementations of HIGHT Block Cipher on IoT Platforms. *Security and Communication Networks*, **2019**, 2019, 1-10 | 1.9 | 10 |
| 52 | SIKE Round 2 Speed Record on ARM Cortex-M4. *Lecture Notes in Computer Science*, **2019**, 39-60 | 0.9 | 13 |
| 51 | Compact implementations of Curve Ed448 on low-end IoT platforms. *ETRI Journal*, **2019**, 41, 863-872 | 1.4 | 6 |
| 50 | Hybrid approach of parallel implementation on CPU□GPU for high-speed ECDSA verification. *Journal of Supercomputing*, **2019**, 75, 4329-4349 | 2.5 | 3 |
| 49 | Memory-Efficient Implementation of Elliptic Curve Cryptography for the Internet-of-Things. *IEEE Transactions on Dependable and Secure Computing*, **2019**, 16, 521-529 | 3.9 | 14 |
| 48 | Secure IoT framework and 2D architecture for End-To-End security. *Journal of Supercomputing*, **2018**, 74, 3521-3535 | 2.5 | 21 |
| 47 | Four$mathbb {Q}$Q on Embedded Devices with Strong Countermeasures Against Side-Channel Attacks. *IEEE Transactions on Dependable and Secure Computing*, **2018**, 1-1 | 3.9 | 6 |
| 46 | Compact Implementations of ARX-Based Block Ciphers on IoT Processors. *Transactions on Embedded Computing Systems*, **2018**, 17, 1-16 | 1.8 | 9 |
| 45 | Secure GCM implementation on AVR. *Discrete Applied Mathematics*, **2018**, 241, 58-66 | 1 | 5 |
| 44 | Secure Data Encryption for Cloud-Based Human Care Services. *Journal of Sensors*, **2018**, 2018, 1-10 | 2 | 5 |
| 43 | Lightweight Fault Attack Resistance in Software Using Intra-instruction Redundancy, Revisited. *Lecture Notes in Computer Science*, **2018**, 3-15 | 0.9 | 2 |
| 42 | Secure Number Theoretic Transform and□Speed Record for Ring-LWE Encryption on Embedded Processors. *Lecture Notes in Computer Science*, **2018**, 175-188 | 0.9 | 1 |
| 41 | Highly Efficient Implementation of NIST-Compliant Koblitz Curve for 8-bit AVR-Based Sensor Nodes. *IEEE Access*, **2018**, 6, 67637-67652 | 3.5 | 9 |
| 40 | Efficient Parallel Implementation of Matrix Multiplication for Lattice-Based Cryptography on Modern ARM Processor. *Security and Communication Networks*, **2018**, 2018, 1-10 | 1.9 | 3 |

| | | | |
|---|---|---|---|
| 39 | Compact Software Implementation of Public-Key Cryptography on MSP430X. *Transactions on Embedded Computing Systems*, **2018**, 17, 1-12 | 1.8 | 5 |
| 38 | Personal identification number entry for Google glass. *Computers and Electrical Engineering*, **2017**, 63, 160-167 | 4.3 | 1 |
| 37 | Efficient Elliptic Curve Cryptography for Embedded Devices. *Transactions on Embedded Computing Systems*, **2017**, 16, 1-18 | 1.8 | 8 |
| 36 | Multiprecision Multiplication on ARMv8 **2017**, | | 1 |
| 35 | High-Performance Ideal Lattice-Based Cryptography on 8-Bit AVR Microcontrollers. *Transactions on Embedded Computing Systems*, **2017**, 16, 1-24 | 1.8 | 10 |
| 34 | Implementing RSA for sensor nodes in smart cities. *Personal and Ubiquitous Computing*, **2017**, 21, 807-813 | 2.1 | 8 |
| 33 | Multi-precision Squaring for Public-Key Cryptography on Embedded Microprocessors, a Step Forward. *Lecture Notes in Computer Science*, **2017**, 331-340 | 0.9 | 1 |
| 32 | Four(mathbb {Q}) on Embedded Devices with Strong Countermeasures Against Side-Channel Attacks. *Lecture Notes in Computer Science*, **2017**, 665-686 | 0.9 | 10 |
| 31 | Comprehensive PEP Performance Analysis of MCIK-OFDM with a Low-Complexity Detector in □ Fading Channels. *Advanced Science Letters*, **2017**, 23, 10255-10258 | 0.1 | |
| 30 | On Emerging Family of Elliptic Curves to Secure Internet of Things: ECC Comes of Age. *IEEE Transactions on Dependable and Secure Computing*, **2016**, 1-1 | 3.9 | 36 |
| 29 | Hybrid Montgomery Reduction. *Transactions on Embedded Computing Systems*, **2016**, 15, 1-13 | 1.8 | 2 |
| 28 | Parallel Implementations of SIMON and SPECK **2016**, | | 11 |
| 27 | A fast ARX model-based image encryption scheme. *Multimedia Tools and Applications*, **2016**, 75, 14685-14706 | 1.9 | 12 |
| 26 | Efficient Implementation of NIST-Compliant Elliptic Curve Cryptography for 8-bit AVR-Based Sensor Nodes. *IEEE Transactions on Information Forensics and Security*, **2016**, 11, 1385-1397 | 8 | 47 |
| 25 | Secure Message Transmission against Remote Control System. *Journal of Information and Communication Convergence Engineering*, **2016**, 14, 233-239 | | |
| 24 | Binary field multiplication on ARMv8. *Security and Communication Networks*, **2016**, 9, 2051-2058 | 1.9 | 3 |
| 23 | Efficient arithmetic on ARM-NEON and its application for high-speed RSA implementation. *Security and Communication Networks*, **2016**, 9, 5401-5411 | 1.9 | 10 |
| 22 | A Synthesis of Multi-Precision Multiplication and Squaring Techniques for 8-Bit Sensor Nodes: State-of-the-Art Research and Future Challenges. *Journal of Computer Science and Technology*, **2016**, 31, 284-299 | 1.7 | 6 |

| | | | |
|---|---|---|---|
| 21 | Montgomery multiplication and squaring for Optimal Prime Fields. *Computers and Security*, **2015**, 52, 276-291 | 4.9 | 2 |
| 20 | Performance evaluation of twisted Edwards-form elliptic curve cryptography for wireless sensor nodes. *Security and Communication Networks*, **2015**, 8, 3301-3310 | 1.9 | 6 |
| 19 | Optimized Karatsuba squaring on 8-bit AVR processors. *Security and Communication Networks*, **2015**, 8, 3546-3554 | 1.9 | 6 |
| 18 | Karatsuba-Block-Comb technique for elliptic curve cryptography over binary fields. *Security and Communication Networks*, **2015**, 8, 3121-3130 | 1.9 | 7 |
| 17 | Consecutive Operand-Caching Method for Multiprecision Multiplication, Revisited. *Journal of Information and Communication Convergence Engineering*, **2015**, 13, 27-35 | | 4 |
| 16 | Efficient Ring-LWE Encryption on 8-Bit AVR Processors. *Lecture Notes in Computer Science*, **2015**, 663-682 | 0.9 | 34 |
| 15 | Pseudo random number generator and Hash function for embedded microprocessors **2014**, | | 9 |
| 14 | Small private key MQPKS on an embedded microprocessor. *Sensors*, **2014**, 14, 5441-58 | 3.8 | 3 |
| 13 | Binary and prime field multiplication for public key cryptography on embedded microprocessors. *Security and Communication Networks*, **2014**, 7, 774-787 | 1.9 | 18 |
| 12 | Multi-precision squaring on MSP and ARM processors **2014**, | | 4 |
| 11 | Implementation of an RFID Key Management System for DASH7. *Journal of Information and Communication Convergence Engineering*, **2014**, 12, 19-25 | | 1 |
| 10 | Low-Power Encryption Algorithm Block Cipher in JavaScript. *Journal of Information and Communication Convergence Engineering*, **2014**, 12, 252-256 | | 5 |
| 9 | Performance enhancement of TinyECC based on multiplication optimizations. *Security and Communication Networks*, **2013**, 6, 151-160 | 1.9 | 16 |
| 8 | Fixed-base comb with window-non-adjacent form (NAF) method for scalar multiplication. *Sensors*, **2013**, 13, 9483-512 | 3.8 | |
| 7 | Optimized Multi-Precision Multiplication for Public-Key Cryptography on Embedded Microprocessors. *International Journal of Computer and Communication Engineering*, **2013**, 255-259 | 0.2 | 11 |
| 6 | Multi-precision Squaring for Public-Key Cryptography on Embedded Microprocessors. *Lecture Notes in Computer Science*, **2013**, 227-243 | 0.9 | 23 |
| 5 | Multi-precision Multiplication for Public-Key Cryptography on Embedded Microprocessors. *Lecture Notes in Computer Science*, **2012**, 55-67 | 0.9 | 20 |
| 4 | Four Anchor Sensor Nodes Based Localization Algorithm over Three-Dimensional Space. *Journal of Information and Communication Convergence Engineering*, **2012**, 10, 349-358 | | 2 |

# List of Publications

| | | |
|---|---|---|
| 3 | Zigbee security for visitors in home automation using attribute based proxy re-encryption **2011**, | 7 |
| 2 | ZigBee security for Home automation using attribute-based cryptography **2011**, | 5 |
| 1 | SIDH on ARM: Faster Modular Multiplications for Faster Post-Quantum Supersingular Isogeny Key Exchange. *Iacr Transactions on Cryptographic Hardware and Embedded Systems*,1-20 | 25 |