

Dooho Choi

List of Publications by Year in descending order

Source: <https://exaly.com/author-pdf/299144/publications.pdf>

Version: 2024-02-01

25
papers

176
citations

1307594

7
h-index

1281871

11
g-index

26
all docs

26
docs citations

26
times ranked

164
citing authors

#	ARTICLE	IF	CITATIONS
1	Tâ€depth reduction method for efficient SHAâ€256 quantum circuit construction. IET Information Security, 2023, 17, 46-65.	1.7	2
2	Wireless Transceiver Aided Run-Time Secret Key Extraction for IoT Device Security. IEEE Transactions on Consumer Electronics, 2020, 66, 11-21.	3.6	12
3	Deep Neural Networks Based Key Concealment Scheme. IEEE Access, 2020, 8, 204214-204225.	4.2	2
4	Quantum Modular Multiplication. IEEE Access, 2020, 8, 213244-213252.	4.2	5
5	Design of Resistor-Capacitor Physically Unclonable Function for Resource-Constrained IoT Devices. Sensors, 2020, 20, 404.	3.8	6
6	Is It Possible to Hide My Key into Deep Neural Network?. Lecture Notes in Computer Science, 2020, , 259-272.	1.3	1
7	PUF-based Authentication Scheme for IoT Devices. , 2020, , .		12
8	Secure IoT Device Authentication Scheme using Key Hiding Technology. , 2020, , .		2
9	Two-Factor Fuzzy Commitment for Unmanned IoT Devices Security. IEEE Internet of Things Journal, 2019, 6, 335-348.	8.7	23
10	PUF based IoT Device Authentication Scheme. , 2019, , .		13
11	Implementing a phase detection ring oscillator PUF on FPGA. , 2018, , .		6
12	Rapid Run-Time DRAM PUF Based on Bit-Flip Position for Secure IoT Devices. , 2018, , .		5
13	Secure Key Extraction for IoT Devices Integrating IEEE 802.15.4g/k Transceiver. , 2018, , .		2
14	An Improved Square-always Exponentiation Resistant to Side-channel Attacks on RSA Implementation. Intelligent Automation and Soft Computing, 2016, 22, 353-363.	2.1	7
15	Conditional Re-encoding Method for Cryptanalysis-Resistant White-Box AES. ETRI Journal, 2015, 37, 1012-1022.	2.0	12
16	A distributed file system over unreliable network storages. , 2015, , .		0
17	Improved Shamir's CRT-RSA Algorithm: Revisit with the Modulus Chaining Method. ETRI Journal, 2014, 36, 469-478.	2.0	8
18	Comments on an Improved RFID Security Protocol for ISO/IEC WD 29167-6. ETRI Journal, 2013, 35, 170-172.	2.0	8

#	ARTICLE	IF	CITATIONS
19	Ghost key patterns with Equidistant Chosen Message attack on RSA-CRT. , 2011, , .		3
20	Fault attack for the iterative operation of AES S-Box. , 2010, , .		1
21	Fault resistant CRT-RSA scheme adopting a small exponent. , 2010, , .		2
22	Convolutive Noise Filtering in Power Analysis on Smartcards Using the Cepstrum. , 2009, , .		2
23	Improved Computation of Square Roots in Specific Finite Fields. IEEE Transactions on Computers, 2009, 58, 188-196.	3.4	17
24	Efficient Implementation of Pairing-Based Cryptography on a Sensor Node. IEICE Transactions on Information and Systems, 2009, E92-D, 909-917.	0.7	23
25	RFID Stamp with RFID Passive Reader. , 2008, , .		0