Atsuko Miyaji

List of Publications by Year
in descending order

49	512	1163117 8	713466 21
papers	citations	h-index	g-index

51	51	51	312
all docs	docs citations	times ranked	citing authors

#	Article	IF	Citations
1	Efficient Elliptic Curve Exponentiation Using Mixed Coordinates. Lecture Notes in Computer Science, 1998, , 51-65.	1.3	215
2	Scalar multiplication on WeierstraÃŸ elliptic curves from Co-Z arithmetic. Journal of Cryptographic Engineering, 2011, 1, 161-176.	1.8	50
3	Generic constructions of secureâ€channel free searchable encryption with adaptive security. Security and Communication Networks, 2015, 8, 1547-1560.	1.5	32
4	Privacy-Preserving Integration of Medical Data. Journal of Medical Systems, 2017, 41, 37.	3.6	27
5	Co-Z Addition FormulÃ¦ and Binary Ladders on Elliptic Curves. Lecture Notes in Computer Science, 2010, , 65-79.	1.3	23
6	A Timed-Release Proxy Re-Encryption Scheme. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2011, E94-A, 1682-1695.	0.3	17
7	A Dynamic Attribute-Based Group Signature Scheme and its Application in an Anonymous Survey for the Collection of Attribute Statistics. , 2009, , .		15
8	Selfâ€healing wireless sensor networks. Concurrency Computation Practice and Experience, 2015, 27, 2547-2568.	2.2	9
9	A New (n, 2n) Double Block Length Hash Function Based on Single Key Scheduling. , 2015, , .		8
10	Adaptive Secure-Channel Free Public-Key Encryption with Keyword Search Implies Timed Release Encryption. Lecture Notes in Computer Science, 2011, , 102-118.	1.3	8
11	A Secure and Private RFID Authentication Protocol under SLPN Problem. Lecture Notes in Computer Science, 2012, , 476-489.	1.3	8
12	A Secure RFID Authentication Protocol with Low Communication Cost. , 2009, , .		7
13	A Dynamic Attribute-Based Group Signature Scheme and Its Application in an Anonymous Survey for the Collection of Attribute Statistics. Journal of Information Processing, 2009, 17, 216-231.	0.4	6
14	A privacy-preserving efficient RFID authentication protocol from SLPN assumption. International Journal of Computational Science and Engineering, 2015, 10, 234.	0.5	6
15	Recursive Matrix Oblivious RAM: An ORAM Construction for Constrained Storage Devices. IEEE Transactions on Information Forensics and Security, 2017, 12, 3024-3038.	6.9	6
16	A Fully-Secure RFID Authentication Protocol from Exact LPN Assumption. , 2013, , .		5
17	SupAUTH: A new approach to supply chain authentication for the IoT. Computational Intelligence, 2018, 34, 582-602.	3.2	5
18	SIT: Supersingular Isogeny Tree-based Group Key Exchange. , 2020, , .		5

#	Article	IF	Citations
19	Security and Access Control for Vehicular Communications. , 2008, , .		4
20	A Matrix Based ORAM: Design, Implementation and Experimental Analysis. IEICE Transactions on Information and Systems, 2016, E99.D, 2044-2055.	0.7	4
21	A lightweight multi-party authentication in insecure reader-server channel in RFID-based IoT. Peer-to-Peer Networking and Applications, 2021, 14, 708-721.	3.9	4
22	Verifiable M+1st-Price Auction without Manager. , 2021, , .		4
23	How to Enhance the Security on the Least Significant Bit. Lecture Notes in Computer Science, 2012, , 263-279.	1.3	4
24	Privacy-Preserving Set Operations in the Presence of Rational Parties. , 2012, , .		3
25	Authenticated logarithmic-order supersingular isogeny group key exchange. International Journal of Information Security, 2022, 21, 207-221.	3.4	3
26	Bidder Scalable M+1st-Price Auction with Public Verifiability. , 2021, , .		3
27	A Certificate Revocable Anonymous Authentication Scheme with Designated Verifier. , 2009, , .		2
28	Generalized Analysis on Key Collisions of Stream Cipher RC4. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2011, E94-A, 2194-2206.	0.3	2
29	Novel strategies for searching RC4 key collisions. Computers and Mathematics With Applications, 2013, 66, 81-90.	2.7	2
30	A Scalable and Secure RFID Ownership Transfer Protocol. , 2014, , .		2
31	A simple authentication encryption scheme. Concurrency Computation Practice and Experience, 2017, 29, e4058.	2.2	2
32	A simple construction of encryption for a tiny domain message. , 2017, , .		2
33	Probably Secure Keyed-Function Based Authenticated Encryption Schemes for Big Data. International Journal of Foundations of Computer Science, 2017, 28, 661-682.	1.1	2
34	OTP-IoT: An ownership transfer protocol for the Internet of Things. Journal of Information Security and Applications, 2018, 43, 73-82.	2.5	2
35	String commitment scheme with low output locality. , 2019, , .		2
36	Compact Elliptic Curve Scalar Multiplication with a Secure Generality. Journal of Information Processing, 2020, 28, 464-472.	0.4	2

#	Article	IF	Citations
37	Variable message encryption through blockcipher compression function. Concurrency Computation Practice and Experience, 2017, 29, e3956.	2.2	1
38	Theoretical and Practical Possibilities of Elliptic Curves : From Elliptic Curve Cryptosystems to Post-Quantum Cryptosystems. Ieice Ess Fundamentals Review, 2021, 14, 329-336.	0.1	1
39	An Experimental Analysis on Lattice Attacks against Ring-LWE over Decomposition Fields. , 2018, , .		1
40	Secure and Compact Elliptic Curve LR Scalar Multiplication. Lecture Notes in Computer Science, 2020, , 605-618.	1.3	1
41	A Practical Privacy-Preserving Algorithm for Document Data. , 2020, , .		1
42	Privacy Risk of Document Data and a Countermeasure Framework. Journal of Information Processing, 2021, 29, 778-786.	0.4	1
43	Homomorphic commitment scheme with constant output locality. , 2020, , .		1
44	Revocable Policy-Based Chameleon Hash for Blockchain Rewriting. Computer Journal, 0, , .	2.4	1
45	Simple Certificateless Signature with Smart Cards. , 2008, , .		0
46	APRAP: Another privacy preserving RFID authentication protocol. , 2010, , .		0
47	POND: A Novel Protocol for Network Coding Based on Hybrid Cryptographic Scheme. , 2014, , .		0
48	SKENO: Secret key encryption with non-interactive opening. Journal of Mathematical Cryptology, 2015, 9, .	0.7	0
49	A Practical Parallel Computation in a Scalable Multiparty Private Set Intersection. , 2021, , .		0