Kazukuni Kobara

List of Publications by Year
in descending order

Source: https://exaly.com/author-pdf/4719690/publications.pdf

Version: 2024-02-01

75	633	840776 11	677142 22
papers	citations	h-index	g-index
77	77	77	333
all docs	docs citations	times ranked	citing authors

#	Article	IF	Citations
1	Semantically Secure McEliece Public-Key Cryptosystems -Conversions for McEliece PKC -. Lecture Notes in Computer Science, 2001, , 19-35.	1.3	103
2	Semantic security for the McEliece cryptosystem without random oracles. Designs, Codes, and Cryptography, 2008, 49, 289-305.	1.6	77
3	Cyber Physical Security for Industrial Control Systems and IoT. IEICE Transactions on Information and Systems, 2016, E99.D, 787-795.	0.7	43
4	A security framework for MQTT. , 2016, , .		40
5	Evaluation of Physical Unclonable Functions for 28-nm Process Field-Programmable Gate Arrays. Journal of Information Processing, 2014, 22, 344-356.	0.4	37
6	LR-AKE-Based AAA for Network Mobility (NEMO) Over Wireless Links. IEEE Journal on Selected Areas in Communications, 2006, 24, 1725-1737.	14.0	27
7	Leakage-Resilient Authenticated Key Establishment Protocols. Lecture Notes in Computer Science, 2003, , 155-172.	1.3	21
8	Sequential Key Derivation Patterns for Broadcast Encryption and Key Predistribution Schemes. Lecture Notes in Computer Science, 2003, , 374-391.	1.3	19
9	Modeling Bit Flipping Decoding Based on Nonorthogonal Check Sums With Application to Iterative Decoding Attack of McEliece Cryptosystem. IEEE Transactions on Information Theory, 2007, 53, 402-411.	2.4	17
10	A Secure Threshold Anonymous Password-Authenticated Key Exchange Protocol. , 2007, , 444-458.		16
11	Leakage-resilient security architecture for mobile IPv6 in wireless overlay networks. IEEE Journal on Selected Areas in Communications, 2005, 23, 2182-2193.	14.0	14
12	On the one-wayness against chosen-plaintext attacks of the Loidreau's modified McEliece PKC. IEEE Transactions on Information Theory, 2003, 49, 3160-3168.	2.4	13
13	Broadcast encryption with short keys and transmissions. , 2003, , .		13
14	Lightweight Asymmetric Privacy-Preserving Authentication Protocols Secure against Active Attack. , 2007, , .		13
15	A Simple Leakage-Resilient Authenticated Key Establishment Protocol, Its Extensions, and Applications. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2005, E88-A, 736-754.	0.3	13
16	Very-Efficient Anonymous Password-Authenticated Key Exchange and Its Extensions. Lecture Notes in Computer Science, 2009, , 149-158.	1.3	11
17	How to Strengthen the Security of RSA-OAEP. IEEE Transactions on Information Theory, 2010, 56, 5876-5886.	2.4	10
18	Coding-Based Oblivious Transfer. Lecture Notes in Computer Science, 2008, , 142-156.	1.3	9

#	Article	IF	Citations
19	An Efficient and Leakage-Resilient RSA-Based Authenticated Key Exchange Protocol with Tight Security Reduction. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2007, E90-A, 474-490.	0.3	8
20	A Secure Construction for Threshold Anonymous Password-Authenticated Key Exchange. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2008, E91-A, 3312-3324.	0.3	8
21	Anonymous Password-Authenticated Key Exchange: New Construction and Its Extensions. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2010, E93-A, 102-115.	0.3	8
22	Privacy Enhanced and Light Weight RFID System without Tag Synchronization and Exhaustive Search. , 2006, , .		7
23	Efficient and Leakage-Resilient Authenticated Key Transport Protocol Based on RSA. Lecture Notes in Computer Science, 2005, , 269-284.	1.3	6
24	Privacy Enhanced RFID Using Quasi-Dyadic Fix Domain Shrinking. , 2010, , .		6
25	Simple Anonymous Password-Based Authenticated Key Exchange (SAPAKE), Reconsidered. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2017, E100.A, 639-652.	0.3	6
26	IVs to Skip for Immunizing WEP against FMS Attack. IEICE Transactions on Communications, 2008, E91-B, 164-171.	0.7	6
27	Key-Dependent Weak IVs and Weak Keys in WEP -- How to Trace Conditions Back to Their Patterns --. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2006, E89-A, 2198-2206.	0.3	6
28	On the Channel Capacity of Narrow-Band Subliminal Channels. Lecture Notes in Computer Science, 1999, , 309-323.	1.3	6
29	An RSA-Based Leakage-Resilient Authenticated Key Exchange Protocol Secure against Replacement Attacks, and Its Extensions. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2010, E93-A, 1086-1101.	0.3	5
30	A New Variant for an Attack Against RSA Signature Verification Using Parameter Field. Lecture Notes in Computer Science, 2007, , 143-153.	1.3	5
31	Self-synchronized message randomization methods for subliminal channels. Lecture Notes in Computer Science, 1997, , 325-334.	1.3	4
32	A Generic Conversion with Optimal Redundancy. Lecture Notes in Computer Science, 2005, , 104-117.	1.3	4
33	Protocols for Authenticated Anonymous Communications. , 2007, , .		4
34	Comparative Studies in Key Disagreement Correction Process on Wireless Key Agreement System. Lecture Notes in Computer Science, 2007, , 173-187.	1.3	4
35	Lightweight Privacy-Preserving Authentication Protocols Secure against Active Attack in an Asymmetric Way. IEICE Transactions on Information and Systems, 2008, E91-D, 1457-1465.	0.7	4
36	RSA-Based Password-Authenticated Key Exchange, Revisited. IEICE Transactions on Information and Systems, 2008, E91-D, 1424-1438.	0.7	3

#	Article	IF	Citations
37	Purpose-restricted Anonymous Mobile Communications Using Anonymous Signatures in Online Credential Systems. Wireless Personal Communications, 2010, 54, 225-236.	2.7	3
38	How to distinguish on-line dictionary attacks and password mis-typing in two-factor authentication. , 2010, , .		3
39	Comparison of tools and simulators for control system security studies. , 2012, , .		3
40	On the Key-Privacy Issue of McEliece Public-Key Encryption. , 2007, , 168-177.		3
41	A Lower-Bound of Complexity for RSA-Based Password-Authenticated Key Exchange. Lecture Notes in Computer Science, 2005, , 191-205.	1.3	3
42	A Secure Authenticated Key Exchange Protocol for Credential Services. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2008, E91-A, 139-149.	0.3	3
43	Secure AAA and Mobility for Nested Mobile Networks. , 2007, , .		2
44	Protocols for purpose-restricted anonymous communications in IP-based wireless networks. Computer Communications, 2008, 31, 3662-3671.	5.1	2
45	Threshold Anonymous Password-Authenticated Key Exchange Secure against Insider Attacks. IEICE Transactions on Information and Systems, 2011, E94-D, 2095-2110.	0.7	2
46	On Finding Secure Domain Parameters Resistant to Cheon's Algorithm. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2015, E98.A, 2456-2470.	0.3	2
47	Kernel Memory Protection by an Insertable Hypervisor Which Has VM Introspection and Stealth Breakpoints. Lecture Notes in Computer Science, 2014, , 48-61.	1.3	2
48	Compact Conversion Schemes for the Probabilistic OW-PCA Primitives. Lecture Notes in Computer Science, 2003, , 269-279.	1.3	1
49	How to Establish Secure Channels for Wireless Communications. IETE Journal of Research, 2006, 52, 229-238.	2.6	1
50	New security layer for overlay networks. Journal of Communications and Networks, 2009, 11, 211-228.	2.6	1
51	On Unlinkability of Password-Based Anonymous Authentication. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2015, E98.A, 1320-1324.	0.3	1
52	Key Establishment Using Physically Unclonable Functions. , 2015, , .		1
53	An Authentication and Key Exchange Protocol for Secure Credential Services. Lecture Notes in Computer Science, 2006, , 443-458.	1.3	1
54	Security Analysis of Two Augmented Password-Authenticated Key Exchange Protocols. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2010, E93.A, 2092-2095.	0.3	1

#	Article	IF	Citations
55	Security against peeping attacks of challenge-response type direct human identification schemes using uniform mapping. Electronics and Communications in Japan, Part III: Fundamental Electronic Science (English Translation of Denshi Tsushin Gakkai Ronbunshi), 1999, 82, 79-86.	0.1	0
56	An error-control method for narrow-band subliminal channels: How to embed more bits in a carrier. Electronics and Communications in Japan, Part III: Fundamental Electronic Science (English) Tj ETQq0 0 0 rgBT /Overlock 10 Tf 50 697 Td	0.1	0
57	Application of trust-metrics for evaluating performance system in ad-hoc networks with privacy. , 0, , .		0
58	Dynamic Fingerprinting over Broadcast Using Revocation Scheme. Lecture Notes in Computer Science, 2005, , 251-263.	1.3	0
59	A Simplified Leakage-Resilient Authenticated Key Exchange Protocol with Optimal Memory Size. Lecture Notes in Computer Science, 2005, , 944-952.	1.3	0
60	Elliptic Curve based Authenticated Key Agreement Protocol for Wireless Security. , 2006, , .		0
61	Next Wireless Security Architecture for MJPv6. , 2006, , .		0
62	An Elliptic Curve Based Authenticated Key Agreement Protocol for Wireless Security. Lecture Notes in Computer Science, 2007, , 767-777.	1.3	0
63	A study on a key establishment scheme with QC LDPC codes and UH-protocols. , 2008, , .		0
64	A note on the error of optimized LFC Private Information Retrieval scheme. , 2008, , .		0
65	A security framework for personal networks. , 2008, , .		0
66	RSA-based Password-Authenticated Key Retrieval using multiple servers. , 2013, , .		0
67	How to Preserve User Anonymity in Password-Based Anonymous Authentication Scheme. IEICE Transactions on Information and Systems, 2018, E101.D, 803-807.	0.7	0
68	Efficient Shared-Key Authentication Scheme from Any Weak Pseudorandom Function. Lecture Notes in Computer Science, 2006, , 303-316.	1.3	0
69	On Achieving Chosen Ciphertext Security with Decryption Errors. Lecture Notes in Computer Science, 2006, , 173-182.	1.3	0
70	Anonymous Pay-TV System with Secure Revenue Sharing. Lecture Notes in Computer Science, 2007, , 984-991.	1.3	0
71	A New Security Architecture for Personal Networks and Its Performance Evaluation. IEICE Transactions on Communications, 2008, E91-B, 2255-2264.	0.7	0
72	A Note on a Fatal Error of Optimized LFC Private Information Retrieval Scheme and Its Corrected Results. Lecture Notes in Computer Science, 2010, , 47-56.	1.3	0

#	Article	IF	Citations
73	Code-Based Public-Key Cryptosystems and Their Applications. Lecture Notes in Computer Science, 2010, , 45-55.	1.3	0
74	About Validity Checks of Augmented PAKE in IEEE 1363.2 and ISO/IEC 11770-4. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2014, E97.A, 413-417.	0.3	0
75	Hidden Credential Retrieval, Revisited. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2015, E98.A, 428-433.	0.3	0