Shoichi Hirose

List of Publications by Year
in descending order

35	379	1163117 8	839539 18
papers	citations	h-index	g-index

41	41	41	102
all docs	docs citations	times ranked	citing authors

#	Article	IF	Citations
1	Provably Secure Double-Block-Length Hash Functions in a Black-Box Model. Lecture Notes in Computer Science, 2005, , 330-342.	1.3	51
2	A Simple Variant of the Merkle-DamgÃ¥rd Scheme with a Permutation. , 2007, , 113-129.		50
3	A Lightweight 256-Bit Hash Function for Hardware and Low-End Devices: Lesamnta-LW. Lecture Notes in Computer Science, 2011, , 151-168.	1.3	21
4	An AES Based 256-bit Hash Function for Lightweight Applications: Lesamnta-LW. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2012, E95-A, 89-99.	0.3	17
5	Non-adaptive Group-Testing Aggregate MAC Scheme. Lecture Notes in Computer Science, 2018, , 357-372.	1.3	11
6	A Simple Variant of the Merkleâ€“DamgÃ¥rd Scheme withÂaÂPermutation. Journal of Cryptology, 2012, 25, 271-309.	2.8	9
7	Hashing Mode Using a Lightweight Blockcipher. Lecture Notes in Computer Science, 2013, , 213-231.	1.3	9
8	Secure Block Ciphers Are Not Sufficient for One-Way Hash Functions in the Preneel-Govaerts-Vandewalle Model. Lecture Notes in Computer Science, 2003, , 339-352.	1.3	8
9	Forward-Secure Sequential Aggregate Message Authentication Revisited. Lecture Notes in Computer Science, 2014, , 87-102.	1.3	7
10	Re-Keying Scheme Revisited: Security Model and Instantiations. Applied Sciences (Switzerland), 2019, 9, 1002.	2.5	5
11	A Block-Cipher-Based Hash Function Using an MMO-Type Double-Block Compression Function. Lecture Notes in Computer Science, 2014, , 71-86.	1.3	5
12	Collision Resistance of Hash Functions in a Weak Ideal Cipher Model. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2012, E95-A, 252-255.	0.3	4
13	Lightweight Hashing Using Lesamnta-LW Compression Function Mode and MDP Domain Extension. , 2016, , .		4
14	Aggregate Message Authentication Code Capable of Non-Adaptive Group-Testing. IEEE Access, 2020, 8, 216116-216126.	4.2	4
15	A Pseudorandom-Function Mode Based on Lesamnta-LW and the MDP Domain Extension and Its Applications. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2018, E101.A, 110-118.	0.3	4
16	Generic Construction of Sequential Aggregate MACs from Any MACs. Lecture Notes in Computer Science, 2018, , 295-312.	1.3	4
17	Security Analysis of DRBG Using HMAC in NIST SP 800-90. Lecture Notes in Computer Science, 2009, , 278-291.	1.3	3
18	A Scheme to Base a Hash Function on a Block Cipher. Lecture Notes in Computer Science, 2009, , 262-275.	1.3	3

#	Article	IF	Citations
19	Efficient Pseudorandom-Function Modes of a Block-Cipher-Based Hash Function. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2009, E92-A, 2447-2453.	0.3	3
20	A Tweak for a PRF Mode of a Compression Function and Its Applications. Lecture Notes in Computer Science, 2016, , 103-114.	1.3	3
21	Compactly Committing Authenticated Encryption Using Tweakable Block Cipher. Lecture Notes in Computer Science, 2020, , 187-206.	1.3	3
22	A Collision Attack on a Double-Block-Length Compression Function Instantiated with 8-/9-Round AES-256. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2016, E99.A, 14-21.	0.3	2
23	Sequential Hashing with Minimum Padding. Cryptography, 2018, 2, 11.	2.3	2
24	Algebraic Fault Analysis of SHA-256 Compression Function and Its Application. Information (Switzerland), 2021, 12, 433.	2.9	2
25	Differentiability of four prefix-free PGV hash functions. IEICE Electronics Express, 2009, 6, 955-958.	0.8	1
26	Provable-Security Analysis of Authenticated Encryption Based on Lesamnta-LW in the Ideal Cipher Model. IEICE Transactions on Information and Systems, 2021, E104.D, 1894-1901.	0.7	1
27	Authenticated Encryption Based on Lesamnta-LW Hashing Mode. Lecture Notes in Computer Science, 2020, , 52-69.	1.3	1
28	Sequential Bitwise Sanitizable Signature Schemes. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2011, E94-A, 392-404.	0.3	0
29	Multilane Hashing Mode Suitable for Parallel Processing. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2013, E96.A, 2434-2442.	0.3	0
30	Provable Security of the Ma-Tsudik Forward-Secure Sequential Aggregate MAC Scheme. , 2019, , .		0
31	Another Algebraic Decomposition Method for Masked Implementation. Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, 2021, , 105-114.	0.3	0
32	Update on Analysis of Lesamnta-LW and New PRF Mode LRF. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2021, E104.A, 1304-1320.	0.3	0
33	A Note on Practical Key Derivation Functions. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2011, E94-A, 1764-1767.	0.3	0
34	History-Free Sequential Aggregate MAC Revisited. Lecture Notes in Computer Science, 2019, , 77-93.	1.3	0
35	The PRF Security of Compression-Function-Based MAC Functions in the Multi-User Setting. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2019, E102.A, 270-277.	0.3	0