

Tetsu Iwata

List of Publications by Year in descending order

Source: <https://exaly.com/author-pdf/4659546/publications.pdf>

Version: 2024-02-01

17
papers

402
citations

1170033

9
h-index

1113639

15
g-index

17
all docs

17
docs citations

17
times ranked

140
citing authors

#	ARTICLE	IF	CITATIONS
1	On the (im)possibility of improving the round diffusion of generalized Feistel structures. Information Processing Letters, 2022, 174, 106197.	0.4	2
2	Analyzing the Provable Security Bounds of GIFT-COFB and Photon-Beetle. Lecture Notes in Computer Science, 2022, , 67-84.	1.0	2
3	Matching attacks on Romulus. IET Information Security, 2022, 16, 459-469.	1.1	2
4	Blockcipher-Based Authenticated Encryption: How Small Can We Go?. Journal of Cryptology, 2020, 33, 703-741.	2.1	16
5	Cryptanalysis of OCB2: Attacks on Authenticity and Confidentiality. Journal of Cryptology, 2020, 33, 1871-1913.	2.1	4
6	Cryptanalysis of OCB2: Attacks on Authenticity and Confidentiality. Lecture Notes in Computer Science, 2019, , 3-31.	1.0	15
7	Quantum Chosen-Ciphertext Attacks Against Feistel Ciphers. Lecture Notes in Computer Science, 2019, , 391-411.	1.0	33
8	4-Round Luby-Rackoff Construction is a qPRP. Lecture Notes in Computer Science, 2019, , 145-174.	1.0	15
9	Quantum Attacks Against Type-1 Generalized Feistel Ciphers and Applications to CAST-256. Lecture Notes in Computer Science, 2019, , 433-455.	1.0	13
10	Integrity analysis of authenticated encryption based on stream ciphers. International Journal of Information Security, 2018, 17, 493-511.	2.3	3
11	Blockcipher-Based Authenticated Encryption: How Small Can We Go?. Lecture Notes in Computer Science, 2017, , 277-298.	1.0	24
12	CLOC: Authenticated Encryption for Short Input. Lecture Notes in Computer Science, 2015, , 149-167.	1.0	25
13	Attacks and Security Proofs of EAX-Prime. Lecture Notes in Computer Science, 2014, , 327-347.	1.0	7
14	Breaking and Repairing GCM Security Proofs. Lecture Notes in Computer Science, 2012, , 31-49.	1.0	45
15	OMAC: One-Key CBC MAC. Lecture Notes in Computer Science, 2003, , 129-153.	1.0	177
16	Duel of the Titans: The Romulus and Remus Families of Lightweight AEAD Algorithms. IACR Transactions on Symmetric Cryptology, 0, , 43-120.	0.0	18
17	New indifferentiability security proof of MDPH hash function. IET Information Security, 0, , .	1.1	1