Phillip Rogaway

List of Publications by Year in descending order

Source: https://exaly.com/author-pdf/11564850/publications.pdf

Version: 2024-02-01

22 papers	3,307 citations	448610 19 h-index	685536 24 g-index
26 all docs	26 docs citations	26 times ranked	1065 citing authors

#	Article	IF	Citations
1	The Design and Evolution of OCB. Journal of Cryptology, 2021, 34, 1.	2.1	3
2	Deterministic Encryption with the Thorp Shuffle. Journal of Cryptology, 2018, 31, 521-536.	2.1	3
3	Onion-AE: Foundations of Nested Encryption. Proceedings on Privacy Enhancing Technologies, 2018, 2018, 85-104.	2.3	4
4	Practice-Oriented Provable Security and the Social Construction of Cryptography. IEEE Security and Privacy, 2016, 14, 10-17.	1.5	2
5	Efficient Garbling from a Fixed-Key Blockcipher. , 2013, , .		202
6	Authentication without Elision: Partially Specified Protocols, Associated Data, and Cryptographic Models Described by Code. , 2009, , .		11
7	Formalizing Human Ignorance. Lecture Notes in Computer Science, 2006, , 211-228.	1.0	75
8	CBC MACs for Arbitrary-Length Messages: The Three-Key Constructions. Journal of Cryptology, 2005, 18, 111-131.	2.1	48
9	Improved Security Analyses for CBCÂMACs. Lecture Notes in Computer Science, 2005, , 527-545.	1.0	43
10	Efficient Instantiations of Tweakable Blockciphers and Refinements to Modes OCB and PMAC. Lecture Notes in Computer Science, 2004, , 16-31.	1.0	248
11	A Parallelizable Enciphering Mode. Lecture Notes in Computer Science, 2004, , 292-304.	1.0	114
12	The EAX Mode of Operation. Lecture Notes in Computer Science, 2004, , 389-407.	1.0	153
13	Encryption-Scheme Security in the Presence of Key-Dependent Messages. Lecture Notes in Computer Science, 2003, , 62-75.	1.0	155
14	OCB. ACM Transactions on Information and System Security, 2003, 6, 365-403.	4.5	227
15	A Tweakable Enciphering Mode. Lecture Notes in Computer Science, 2003, , 482-499.	1.0	144
16	Ciphers with Arbitrary Finite Domains. Lecture Notes in Computer Science, 2002, , 114-130.	1.0	126
17	Black-Box Analysis of the Block-Cipher-Based Hash-Function Constructions from PGV. Lecture Notes in Computer Science, 2002, , 320-335.	1.0	214
18	Reconciling Two Views of Cryptography (The Computational Soundness of Formal Encryption)*. Journal of Cryptology, 2002, 15, 103-127.	2.1	235

#	Article	IF	Citations
19	How to Protect DES Against Exhaustive Key Search (an Analysis of DESX). Journal of Cryptology, 2001, 14, 17-35.	2.1	100
20	The Security of the Cipher Block Chaining Message Authentication Code. Journal of Computer and System Sciences, 2000, 61, 362-399.	0.9	357
21	Bucket Hashing and Its Application to Fast Message Authentication. Journal of Cryptology, 1999, 12, 91-115.	2.1	34
22	A Software-Optimized Encryption Algorithm. Journal of Cryptology, 1998, 11, 273-287.	2.1	35