Yannick Seurin

List of Publications by Year
in descending order

Source: https://exaly.com/author-pdf/3807683/publications.pdf

Version: 2024-02-01

14
papers

589
citations

840776
11
h-index

1125743
13
g-index

14
all docs

14
docs citations

14
times ranked

193
citing authors

#	ARTICLE	IF	CITATIONS
1	MuSig2: Simple Two-Round Schnorr Multi-signatures. Lecture Notes in Computer Science, 2021, , 189-221.	1.3	42
2	Blind Schnorr Signatures and Signed ElGamal Encryption in the Algebraic Group Model. Lecture Notes in Computer Science, 2020, , 63-95.	1.3	48
3	MuSig-DN: Schnorr Multi-Signatures with Verifiably Deterministic Nonces. , 2020, , .		31
4	Simple Schnorr multi-signatures with applications to Bitcoin. Designs, Codes, and Cryptography, 2019, 87, 2139-2164.	1.6	138
5	Analysis of the single-permutation encrypted Daviesâ€“Meyer construction. Designs, Codes, and Cryptography, 2018, 86, 2703-2723.	1.6	12
6	Minimizing the Two-Round Evenâ€“Mansour Cipher. Journal of Cryptology, 2018, 31, 1064-1119.	2.8	11
7	Indifferentiability of Iterated Even-Mansour Ciphers with Non-idealized Key-Schedules: Five Rounds Are Necessary and Sufficient. Lecture Notes in Computer Science, 2017, , 524-555.	1.3	16
8	How to Build an Ideal Cipher: The Indifferentiability of the Feistel Construction. Journal of Cryptology, 2016, 29, 61-114.	2.8	32
9	EWCDM: An Efficient, Beyond-Birthday Secure, Nonce-Misuse Resistant MAC. Lecture Notes in Computer Science, 2016, , 121-149.	1.3	45
10	The Iterated Random Permutation Problem with Applications to Cascade Encryption. Lecture Notes in Computer Science, 2015, , 351-367.	1.3	4
11	Minimizing the Two-Round Even-Mansour Cipher. Lecture Notes in Computer Science, 2014, , 39-56.	1.3	59
12	How to Construct an Ideal Cipher from a Small Set of Public Permutations. Lecture Notes in Computer Science, 2013, , 444-463.	1.3	30
13	An Asymptotically Tight Security Analysis of the Iterated Even-Mansour Cipher. Lecture Notes in Computer Science, 2012, , 278-295.	1.3	57
14	The Random Oracle Model and the Ideal Cipher Model Are Equivalent. Lecture Notes in Computer Science, 2008, , 1-20.	1.3	64