Jan Camenisch

List of Publications by Year
in descending order

Source: https://exaly.com/author-pdf/10535667/publications.pdf

Version: 2024-02-01

28 papers	4,328 citations	394286 19 h-index	526166 27 g-index
28 all docs	28 docs citations	28 times ranked	1085 citing authors

#	Article	IF	Citations
1	An Efficient System for Non-transferable Anonymous Credentials with Optional Anonymity Revocation. Lecture Notes in Computer Science, 2001, , 93-118.	1.0	707
2	Efficient group signature schemes for large groups. Lecture Notes in Computer Science, 1997, , 410-424.	1.0	645
3	Signature Schemes and Anonymous Credentials from Bilinear Maps. Lecture Notes in Computer Science, 2004, , 56-72.	1.0	565
4	A Practical and Provably Secure Coalition-Resistant Group Signature Scheme. Lecture Notes in Computer Science, 2000, , 255-270.	1.0	498
5	A Signature Scheme with Efficient Protocols. Lecture Notes in Computer Science, 2003, , 268-289.	1.0	358
6	Practical Verifiable Encryption and Decryption of Discrete Logarithms. Lecture Notes in Computer Science, 2003, , 126-144.	1.0	334
7	Compact E-Cash. Lecture Notes in Computer Science, 2005, , 302-321.	1.0	260
8	Proving in Zero-Knowledge that a Number is the Product of Two Safe Primes. Lecture Notes in Computer Science, 1999, , 107-122.	1.0	169
9	Simulatable Adaptive Oblivious Transfer. Lecture Notes in Computer Science, 2007, , 573-590.	1.0	139
10	Separability and Efficiency for Generic Group Signature Schemes. Lecture Notes in Computer Science, 1999, , 413-430.	1.0	112
11	A Public Key Encryption Scheme Secure against Key Dependent Chosen Plaintext and Adaptive Chosen Ciphertext Attacks. Lecture Notes in Computer Science, 2009, , 351-368.	1.0	112
12	Batch Verification of Short Signatures. Lecture Notes in Computer Science, 2007, , 246-263.	1.0	96
13	Batch Verification of Short Signatures. Journal of Cryptology, 2012, 25, 723-747.	2.1	48
14	Exploiting cryptography for privacy-enhanced access control: A result of the PRIME Project. Journal of Computer Security, 2010, 18, 123-160.	0.5	38
15	One TPM to Bind Them All: Fixing TPM 2.0 for Provably Secure Anonymous Attestation. , 2017, , .		34
16	Digital payment systems with passive anonymity-revoking trustees*. Journal of Computer Security, 1997, 5, 69-89.	0.5	33
17	Structure Preserving CCA Secure Encryption and Applications. Lecture Notes in Computer Science, 2011, , 89-106.	1.0	33
18	Oblivious Transfer with Hidden Access Control Policies. Lecture Notes in Computer Science, 2011, , 192-209.	1.0	32

#	Article	IF	Citations
19	Concepts and Languages for Privacy-Preserving Attribute-Based Authentication. International Federation for Information Processing, 2013, , 34-52.	0.4	30
20	Efficient Structure-Preserving Signature Scheme from Standard Assumptions. Lecture Notes in Computer Science, 2012, , 76-94.	1.0	21
21	Electronic Identities Need Private Credentials. IEEE Security and Privacy, 2012, 10, 80-83.	1.5	16
22	Accountable privacy supporting services. Identity in the Information Society, 2009, 2, 241-267.	0.8	9
23	Encrypting Keys Securely. IEEE Security and Privacy, 2010, 8, 66-69.	1.5	9
24	More efficient, provably-secure direct anonymous attestation from lattices. Future Generation Computer Systems, 2019, 99, 425-458.	4.9	9
25	Proving in Zero-Knowledge that a Number is the Product of Two Safe Primes. BRICS Report Series, 1998, 5, .	0.2	8
26	Information privacy?!. Computer Networks, 2012, 56, 3834-3848.	3.2	7
27	Concepts Around Privacy-Preserving Attribute-Based Credentials. IFIP Advances in Information and Communication Technology, 2014, , 53-63.	0.5	4
28	On the Impossibility of Structure-Preserving Deterministic Primitives. Journal of Cryptology, 2019, 32, 239-264.	2.1	2