

Jan Camenisch

List of Publications by Citations

Source: <https://exaly.com/author-pdf/10535667/jan-camenisch-publications-by-citations.pdf>

Version: 2024-04-29

This document has been generated based on the publications and citations recorded by exaly.com. For the latest version of this publication list, visit the link given above.

The third column is the impact factor (IF) of the journal, and the fourth column is the number of citations of the article.

28

papers

3,361

citations

19

h-index

28

g-index

28

ext. papers

3,615

ext. citations

1.4

avg, IF

5.31

L-index

#	Paper	IF	Citations
28	An Efficient System for Non-transferable Anonymous Credentials with Optional Anonymity Revocation. <i>Lecture Notes in Computer Science</i> , 2001 , 93-118	0.9	531
27	Efficient group signature schemes for large groups. <i>Lecture Notes in Computer Science</i> , 1997 , 410-424	0.9	502
26	Signature Schemes and Anonymous Credentials from Bilinear Maps. <i>Lecture Notes in Computer Science</i> , 2004 , 56-72	0.9	444
25	A Practical and Provably Secure Coalition-Resistant Group Signature Scheme. <i>Lecture Notes in Computer Science</i> , 2000 , 255-270	0.9	364
24	A Signature Scheme with Efficient Protocols. <i>Lecture Notes in Computer Science</i> , 2003 , 268-289	0.9	281
23	Practical Verifiable Encryption and Decryption of Discrete Logarithms. <i>Lecture Notes in Computer Science</i> , 2003 , 126-144	0.9	268
22	Compact E-Cash. <i>Lecture Notes in Computer Science</i> , 2005 , 302-321	0.9	213
21	Proving in Zero-Knowledge that a Number is the Product of Two Safe Primes. <i>Lecture Notes in Computer Science</i> , 1999 , 107-122	0.9	135
20	Simulatable Adaptive Oblivious Transfer. <i>Lecture Notes in Computer Science</i> , 2007 , 573-590	0.9	112
19	A Public Key Encryption Scheme Secure against Key Dependent Chosen Plaintext and Adaptive Chosen Ciphertext Attacks. <i>Lecture Notes in Computer Science</i> , 2009 , 351-368	0.9	95
18	Separability and Efficiency for Generic Group Signature Schemes. <i>Lecture Notes in Computer Science</i> , 1999 , 413-430	0.9	87
17	Batch Verification of Short Signatures. <i>Lecture Notes in Computer Science</i> , 2007 , 246-263	0.9	77
16	Batch Verification of Short Signatures. <i>Journal of Cryptology</i> , 2012 , 25, 723-747	2.1	36
15	Structure Preserving CCA Secure Encryption and Applications. <i>Lecture Notes in Computer Science</i> , 2011 , 89-106	0.9	31
14	Exploiting cryptography for privacy-enhanced access control: A result of the PRIME Project. <i>Journal of Computer Security</i> , 2010 , 18, 123-160	0.8	27
13	Oblivious Transfer with Hidden Access Control Policies. <i>Lecture Notes in Computer Science</i> , 2011 , 192-209	0.9	27
12	One TPM to Bind Them All: Fixing TPM 2.0 for Provably Secure Anonymous Attestation 2017 ,		23

11	Concepts and Languages for Privacy-Preserving Attribute-Based Authentication. <i>International Federation for Information Processing</i> , 2013 , 34-52		22
10	Digital payment systems with passive anonymity-revoking trustees*. <i>Journal of Computer Security</i> , 1997 , 5, 69-89	0.8	20
9	Efficient Structure-Preserving Signature Scheme from Standard Assumptions. <i>Lecture Notes in Computer Science</i> , 2012 , 76-94	0.9	19
8	Electronic Identities Need Private Credentials. <i>IEEE Security and Privacy</i> , 2012 , 10, 80-83	2	14
7	Accountable privacy supporting services. <i>Identity in the Information Society</i> , 2009 , 2, 241-267		7
6	Information privacy?!. <i>Computer Networks</i> , 2012 , 56, 3834-3848	5.4	6
5	. <i>IEEE Security and Privacy</i> , 2010 , 8, 66-69	2	6
4	Proving in Zero-Knowledge that a Number is the Product of Two Safe Primes. <i>BRICS Report Series</i> , 1998 , 5,		6
3	More efficient, provably-secure direct anonymous attestation from lattices. <i>Future Generation Computer Systems</i> , 2019 , 99, 425-458	7.5	4
2	Concepts Around Privacy-Preserving Attribute-Based Credentials. <i>IFIP Advances in Information and Communication Technology</i> , 2014 , 53-63	0.5	3
1	On the Impossibility of Structure-Preserving Deterministic Primitives. <i>Journal of Cryptology</i> , 2019 , 32, 239-264	2.1	1