Jan Camenisch

List of Publications by Year in Descending Order

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	More efficient, provably-secure direct anonymous attestation from lattices. *Future Generation Computer Systems*, **2019**, 99, 425-458	7.5	4
27	On the Impossibility of Structure-Preserving Deterministic Primitives. *Journal of Cryptology*, **2019**, 32, 239-264	2.1	1
26	One TPM to Bind Them All: Fixing TPM 2.0 for Provably Secure Anonymous Attestation **2017**,		23
25	Concepts Around Privacy-Preserving Attribute-Based Credentials. *IFIP Advances in Information and Communication Technology*, **2014**, 53-63	0.5	3
24	Concepts and Languages for Privacy-Preserving Attribute-Based Authentication. *International Federation for Information Processing*, **2013**, 34-52		22
23	Electronic Identities Need Private Credentials. *IEEE Security and Privacy*, **2012**, 10, 80-83	2	14
22	Batch Verification of Short Signatures. *Journal of Cryptology*, **2012**, 25, 723-747	2.1	36
21	Information privacy?!. *Computer Networks*, **2012**, 56, 3834-3848	5.4	6
20	Efficient Structure-Preserving Signature Scheme from Standard Assumptions. *Lecture Notes in Computer Science*, **2012**, 76-94	0.9	19
19	Structure Preserving CCA Secure Encryption and Applications. *Lecture Notes in Computer Science*, **2011**, 89-106	0.9	31
18	Oblivious Transfer with Hidden Access Control Policies. *Lecture Notes in Computer Science*, **2011**, 192-209	0.9	27
17	Exploiting cryptography for privacy-enhanced access control: A result of the PRIME Project. *Journal of Computer Security*, **2010**, 18, 123-160	0.8	27
16	. *IEEE Security and Privacy*, **2010**, 8, 66-69	2	6
15	Accountable privacy supporting services. *Identity in the Information Society*, **2009**, 2, 241-267		7
14	A Public Key Encryption Scheme Secure against Key Dependent Chosen Plaintext and Adaptive Chosen Ciphertext Attacks. *Lecture Notes in Computer Science*, **2009**, 351-368	0.9	95
13	Batch Verification of Short Signatures. *Lecture Notes in Computer Science*, **2007**, 246-263	0.9	77
12	Simulatable Adaptive Oblivious Transfer. *Lecture Notes in Computer Science*, **2007**, 573-590	0.9	112

11	Compact E-Cash. *Lecture Notes in Computer Science*, **2005**, 302-321	0.9	213
10	Signature Schemes and Anonymous Credentials from Bilinear Maps. *Lecture Notes in Computer Science*, **2004**, 56-72	0.9	444
9	Practical Verifiable Encryption and Decryption of Discrete Logarithms. *Lecture Notes in Computer Science*, **2003**, 126-144	0.9	268
8	A Signature Scheme with Efficient Protocols. *Lecture Notes in Computer Science*, **2003**, 268-289	0.9	281
7	An Efficient System for Non-transferable Anonymous Credentials with Optional Anonymity Revocation. *Lecture Notes in Computer Science*, **2001**, 93-118	0.9	531
6	A Practical and Provably Secure Coalition-Resistant Group Signature Scheme. *Lecture Notes in Computer Science*, **2000**, 255-270	0.9	364
5	Separability and Efficiency for Generic Group Signature Schemes. *Lecture Notes in Computer Science* , **1999**, 413-430	0.9	87
4	Proving in Zero-Knowledge that a Number is the Product of Two Safe Primes. *Lecture Notes in Computer Science*, **1999**, 107-122	0.9	135
3	Proving in Zero-Knowledge that a Number is the Product of Two Safe Primes. *BRICS Report Series*, **1998**, 5,		6
2	Digital payment systems with passive anonymity-revoking trustees*. *Journal of Computer Security*, **1997**, 5, 69-89	0.8	20
1	Efficient group signature schemes for large groups. *Lecture Notes in Computer Science*, **1997**, 410-424	0.9	502