Daniel Slamanig

List of Publications by Year
in descending order

75	1,256	643344 15	620720 26
papers	citations	h-index	g-index

80	80	80	557
all docs	docs citations	times ranked	citing authors

#	Article	IF	Citations
1	Updatable Signatures and Message Authentication Codes. Lecture Notes in Computer Science, 2021, , 691-723.	1.0	6
2	Versatile and Sustainable Timed-Release Encryption and Sequential Time-Lock Puzzles (Extended) Tj ETQq0 0 0 rgBT /Overlock 10 Tf 50 7	1.0	6
3	Bloom Filter Encryption and Applications to Efficient Forward-Secret 0-RTT Key Exchange. Journal of Cryptology, 2021, 34, 1.	2.1	13
4	Privacy-Preserving Authenticated Key Exchange: Stronger Privacy and Generic Constructions. Lecture Notes in Computer Science, 2021, , 676-696.	1.0	3
5	Fine-Grained Forward Secrecy: Allow-List/Deny-List Encryption and Applications. Lecture Notes in Computer Science, 2021, , 499-519.	1.0	6
6	Updatable Trapdoor SPHFs: Modular Construction of Updatable Zero-Knowledge Arguments and More. Lecture Notes in Computer Science, 2021, , 46-67.	1.0	0
7	With a Little Help from My Friends. , 2021, , .		14
8	Fully invisible protean signatures schemes. IET Information Security, 2020, 14, 266-285.	1.1	2
9	Policy-Based Sanitizable Signatures. Lecture Notes in Computer Science, 2020, , 538-563.	1.0	16
10	Privacy-Preserving Incentive Systems with Highly Efficient Point-Collection. , 2020, , .		9
11	Lift-and-Shift. , 2020, , .		19
12	CCA-Secure (Puncturable) KEMs from Encryption with Non-Negligible Decryption Errors. Lecture Notes in Computer Science, 2020, , 159-190.	1.0	6
13	Fully Collision-Resistant Chameleon-Hashes from Simpler and Post-quantum Assumptions. Lecture Notes in Computer Science, 2020, , 427-447.	1.0	2
14	Bringing Order to Chaos: The Case of Collision-Resistant Chameleon-Hashes. Lecture Notes in Computer Science, 2020, , 462-492.	1.0	9
15	Key-homomorphic signatures: definitions and applications to multiparty signatures and non-interactive zero-knowledge. Designs, Codes, and Cryptography, 2019, 87, 1373-1413.	1.0	13
16	Structure-Preserving Signatures on Equivalence Classes and Constant-Size Anonymous Credentials. Journal of Cryptology, 2019, 32, 498-546.	2.1	57
17	Fine-Grained and Controlled Rewriting in Blockchains: Chameleon-Hashing Gone Attribute-Based. , 2019, , .		95
18	Structure-Preserving Signatures onÂEquivalence Classes from Standard Assumptions. Lecture Notes in Computer Science, 2019, , 63-93.	1.0	3

#	Article	IF	Citations
19	A Framework for UC-Secure Commitments from Publicly Computable Smooth Projective Hashing. Lecture Notes in Computer Science, 2019, , 1-21.	1.0	1
20	Post-Quantum Zero-Knowledge Proofs for Accumulators with Applications to Ring Signatures from Symmetric-Key Primitives. Lecture Notes in Computer Science, 2018, , 419-440.	1.0	30
21	Bloom Filter Encryption and Applications to Efficient Forward-Secret 0-RTT Key Exchange. Lecture Notes in Computer Science, 2018, , 425-455.	1.0	53
22	Protean Signature Schemes. Lecture Notes in Computer Science, 2018, , 256-276.	1.0	4
23	Practical witness encryption for algebraic languages or how to encrypt under Grothâ€“Sahai proofs. Designs, Codes, and Cryptography, 2018, 86, 2525-2547.	1.0	5
24	Short Double- and N-Times-Authentication-Preventing Signatures from ECDSA and More. , 2018, , .		14
25	Highly-Efficient Fully-Anonymous Dynamic Group Signatures. , 2018, , .		31
26	Chameleon-Hashes with Dual Long-Term Trapdoors and Their Applications. Lecture Notes in Computer Science, 2018, , 11-32.	1.0	11
27	Generic Double-Authentication Preventing Signatures and a Post-quantum Instantiation. Lecture Notes in Computer Science, 2018, , 258-276.	1.0	12
28	Revisiting Proxy Re-encryption: Forward Secrecy, Improved Security, and Applications. Lecture Notes in Computer Science, 2018, , 219-250.	1.0	31
29	Secure and Privacy-Friendly Storage and Data Processing in the Cloud. IFIP Advances in Information and Communication Technology, 2018, , 153-169.	0.5	0
30	Post-Quantum Zero-Knowledge and Signatures from Symmetric-Key Primitives. , 2017, , .		149
31	Practical Strongly Invisible and Strongly Accountable Sanitizable Signatures. Lecture Notes in Computer Science, 2017, , 437-452.	1.0	15
32	Linking-Based Revocation for Group Signatures: A Pragmatic Approach for Efficient Revocation Checks. Lecture Notes in Computer Science, 2017, , 364-388.	1.0	5
33	Homomorphic Proxy Re-Authenticators and Applications to Verifiable Multi-User Data Aggregation. Lecture Notes in Computer Science, 2017, , 124-142.	1.0	15
34	Chameleon-Hashes with Ephemeral Trapdoors. Lecture Notes in Computer Science, 2017, , 152-182.	1.0	68
35	PRISMACLOUD Tools: A Cryptographic Toolbox for Increasing Security in Cloud Services. , 2016, , .		8
36	Towards Authenticity and Privacy Preserving Accountable Workflows. IFIP Advances in Information and Communication Technology, 2016, , 170-186.	0.5	1

#	Article	IF	Citations
37	Practical Round-Optimal Blind Signatures in the Standard Model from Weaker Assumptions. Lecture Notes in Computer Science, 2016, , 391-408.	1.0	20
38	Signatures for Privacy, Trust and Accountability in the Cloud: Applications and Requirements. IFIP Advances in Information and Communication Technology, 2016, , 79-96.	0.5	2
39	The Austrian eID ecosystem in the public cloud: How to obtain privacy while preserving practicality. Journal of Information Security and Applications, 2016, 27-28, 35-53.	1.8	4
40	Non-Interactive Plaintext (In-)Equality Proofs and Group Signatures with Verifiable Controllable Linkability. Lecture Notes in Computer Science, 2016, , 127-143.	1.0	17
41	A General Framework for Redactable Signatures and New Constructions. Lecture Notes in Computer Science, 2016, , 3-19.	1.0	25
42	Signer-Anonymous Designated-Verifier Redactable Signatures for Cloud-Based Data Sharing. Lecture Notes in Computer Science, 2016, , 211-227.	1.0	9
43	Blank Digital Signatures: Optimization and Practical Experiences. IFIP Advances in Information and Communication Technology, 2015, , 201-215.	0.5	4
44	Design strategies for a privacy-friendly Austrian eID system in the public cloud. Computers and Security, 2015, 52, 178-193.	4.0	3
45	ARCHISTAR: Towards Secure and Robust Cloud Based Data Sharing. , 2015, , .		25
46	Towards a New Paradigm for Privacy andÂSecurity in Cloud Services. Communications in Computer and Information Science, 2015, , 14-25.	0.4	8
47	Privacy-Aware Authentication in the Internet of Things. Lecture Notes in Computer Science, 2015, , 32-39.	1.0	11
48	Revisiting Cryptographic Accumulators, Additional Properties and Relations to Other Primitives. Lecture Notes in Computer Science, 2015, , 127-144.	1.0	55
49	Rethinking Privacy for Extended Sanitizable Signatures and a Black-Box Construction of Strongly Private Schemes. Lecture Notes in Computer Science, 2015, , 455-474.	1.0	17
50	A New Approach to Efficient Revocable Attribute-Based Anonymous Credentials. Lecture Notes in Computer Science, 2015, , 57-74.	1.0	11
51	Practical Round-Optimal Blind Signatures in the Standard Model. Lecture Notes in Computer Science, 2015, , 233-253.	1.0	48
52	User-centric identity as a service-architecture for eIDs with selective attribute disclosure. , 2014, , .		13
53	Adding Controllable Linkability to Pairing-Based Group Signatures for Free. Lecture Notes in Computer Science, 2014, , 388-400.	1.0	19
54	Privacy-Enhancing Proxy Signatures from Non-interactive Anonymous Credentials. Lecture Notes in Computer Science, 2014, , 49-65.	1.0	4

#	Article	IF	Citations
55	A Federated Cloud Identity Broker-Model for Enhanced Privacy via Proxy Re-Encryption. Lecture Notes in Computer Science, 2014, , 92-103.	1.0	6
56	Structure-Preserving Signatures on Equivalence Classes and Their Application to Anonymous Credentials. Lecture Notes in Computer Science, 2014, , 491-511.	1.0	42
57	Scalable and Privacy-Preserving Variants of the Austrian Electronic Mandate System in the Public Cloud. , 2013, , .		2
58	Blank digital signatures. , 2013, , .		23
59	Warrant-Hiding Delegation-by-Certificate Proxy Signature Schemes. Lecture Notes in Computer Science, 2013, , 60-77.	1.0	3
60	On Privacy-Preserving Ways to Porting the Austrian eID System to the Public Cloud. IFIP Advances in Information and Communication Technology, 2013, , 300-314.	0.5	9
61	A Framework for Privacy-Preserving Mobile Payment on Security Enhanced ARM TrustZone Platforms. , 2012, , .		23
62	Efficient Schemes for Anonymous Yet Authorized and Bounded Use of Cloud Resources. Lecture Notes in Computer Science, 2012, , 73-91.	1.0	8
63	Practical Privacy Preserving Cloud Resource-Payment for Constrained Clients. Lecture Notes in Computer Science, 2012, , 201-220.	1.0	7
64	Dynamic Accumulator Based Discretionary Access Control for Outsourced Storage with Unlinkable Access. Lecture Notes in Computer Science, 2012, , 215-222.	1.0	8
65	Selectively Traceable Anonymous and Unlinkable Token-Based Transactions. Communications in Computer and Information Science, 2012, , 289-303.	0.4	0
66	Health Records and the Cloud Computing Paradigm from a Privacy Perspective. Journal of Healthcare Engineering, 2011, 2, 487-508.	1.1	5
67	Anonymous Authentication from Public-Key Encryption Revisited. Lecture Notes in Computer Science, 2011, , 247-249.	1.0	1
68	Electronic Health Records: An Enhanced Security Paradigm to Preserve Patientâ€™s Privacy. Communications in Computer and Information Science, 2010, , 369-380.	0.4	4
69	Generalizations and Extensions of Redactable Signatures with Applications to Electronic Healthcare. Lecture Notes in Computer Science, 2010, , 201-213.	1.0	19
70	Privacy Enhancing Technologies in Electronic Health Records. , 2010, , 275-295.		0
71	Disclosing verifiable partial information of signed CDA documents using generalized redactable signatures. , 2009, , .		3
72	Anonymity and Application Privacy in Context of Mobile Computing in eHealth. Lecture Notes in Computer Science, 2009, , 148-157.	1.0	3

#	Article	IF	Citations
73	Investigating Anonymity in Group Based Anonymous Authentication. IFIP Advances in Information and Communication Technology, 2009, , 268-281.	0.5	4
74	Privacy-enhancing methods for e-health applications: how to prevent statistical analyses and attacks. International Journal of Business Intelligence and Data Mining, 2008, 3, 236.	0.2	13
75	Privacy Aspects of eHealth. , 2008, , .		38