Sherman S M Chow

List of Publications by Year
in descending order

Source: https://exaly.com/author-pdf/1103928/publications.pdf

Version: 2024-02-01

138 papers	4,858 citations	212478 28 h-index	162838 57 g-index
143 all docs	143 docs citations	143 times ranked	2935 citing authors

#	Article	IF	Citations
1	Optimizing Privacy-Preserving Outsourced Convolutional Neural Network Predictions. IEEE Transactions on Dependable and Secure Computing, 2022, 19, 1592-1604.	3.7	25
2	Forward and Backward-Secure Range-Searchable Symmetric Encryption. Proceedings on Privacy Enhancing Technologies, 2022, 2022, 28-48.	2.3	10
3	Non-Malleable Functions and their Applications. Journal of Cryptology, 2022, 35, 1.	2.1	2
4	Secure-Computation-Friendly Private Set Intersection from Oblivious Compact Graph Evaluation. , 2022, , .		3
5	Donâ€™t Tamper withÂDual System Encryption. Lecture Notes in Computer Science, 2022, , 419-439.	1.0	1
6	Universal location referencing and homomorphic evaluation of geospatial query. Computers and Security, 2021, 102, 102137.	4.0	4
7	Simple Storage-Saving Structure for Volume-Hiding Encrypted Multi-maps. Lecture Notes in Computer Science, 2021, , 63-83.	1.0	4
8	Access Control Encryption from Group Encryption. Lecture Notes in Computer Science, 2021, , 417-441.	1.0	2
9	LDSP: Shopping with Cryptocurrency Privately and Quickly under Leadership. , 2021, , .		3
10	Sipster: Settling IOU Privately and Quickly with Smart Meters. , 2021, , .		3
11	Stargazing in the Dark: Secure Skyline Queries with SGX. Lecture Notes in Computer Science, 2020, , 322-338.	1.0	10
12	Multi-client Oblivious RAM with Poly-logarithmic Communication. Lecture Notes in Computer Science, 2020, , 160-190.	1.0	4
13	Another Look at Anonymous Communication. IEEE Transactions on Dependable and Secure Computing, 2019, 16, 731-742.	3.7	10
14	Updatable Block-Level Message-Locked Encryption. IEEE Transactions on Dependable and Secure Computing, 2019, , 1-1.	3.7	9
15	Fast-to-Finalize Nakamoto-Like Consensus. Lecture Notes in Computer Science, 2019, , 271-288.	1.0	3
16	Structure-Preserving Certificateless Encryption and Its Application. Lecture Notes in Computer Science, 2019, , 1-22.	1.0	5
17	Let a Non-barking Watchdog Bite: Cliptographic Signatures with an Offline Watchdog. Lecture Notes in Computer Science, 2019, , 221-251.	1.0	14
18	Fork-free hybrid consensus with flexible Proof-of-Activity. Future Generation Computer Systems, 2019, 96, 515-524.	4.9	30

#	Article	IF	Citations
19	Outsourced Biometric Identification With Privacy. IEEE Transactions on Information Forensics and Security, 2018, 13, 2448-2463.	4.5	41
20	Multi-authority fine-grained access control with accountability and its application in cloud. Journal of Network and Computer Applications, 2018, 112, 89-96.	5.8	110
21	Searchable Encryption over Feature-Rich Data. IEEE Transactions on Dependable and Secure Computing, 2018, 15, 496-510.	3.7	116
22	InstantCryptoGram: Secure Image Retrieval Service. , 2018, , .		23
23	Privacy-Preserving Machine Learning. Communications in Computer and Information Science, 2018, , 3-6.	0.4	2
24	Can You Find The One for Me?. , 2018, , .		15
25	Multi-key Homomorphic Signatures Unforgeable Under Insider Corruption. Lecture Notes in Computer Science, 2018, , 465-492.	1.0	10
26	Position Paper on Blockchain Technology: Smart Contract and Applications. Lecture Notes in Computer Science, 2018, , 474-483.	1.0	20
27	Systematic Market Control of Cryptocurrency Inflations. , 2018, , .		3
28	Sharding Blockchain. , 2018, , .		15
29	Geosocial query with user-controlled privacy. , 2017, , .		4
30	Privacy-Preserving Decision Trees Evaluation via Linear Functions. Lecture Notes in Computer Science, 2017, , 494-512.	1.0	56
31	Forward-Secure Searchable Encryption onÂLabeled Bipartite Graphs. Lecture Notes in Computer Science, 2017, , 478-497.	1.0	25
32	Updatable Block-Level Message-Locked Encryption. , 2017, , .		17
33	Secure Strategyproof Ascending-Price Spectrum Auction. , 2017, , .		3
34	Parallel and Dynamic Structured Encryption. Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, 2017, , 219-238.	0.2	4
35	Real Hidden Identity-Based Signatures. Lecture Notes in Computer Science, 2017, , 21-38.	1.0	6
36	Are you The One to Share? Secret Transfer with Access Structure. Proceedings on Privacy Enhancing Technologies, 2017, 2017, 149-169.	2.3	16

#	Article	IF	Citations
37	Another Look at Anonymous Communication. Lecture Notes in Computer Science, 2017, , 56-82.	1.0	1
38	Privacy-Preserving Multi-pattern Matching. Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, 2017, , 199-218.	0.2	1
39	Privacy Preserving Credit Systems. Lecture Notes in Computer Science, 2016, , 184-199.	1.0	1
40	Efficient Sanitizable Signatures Without Random Oracles. Lecture Notes in Computer Science, 2016, , 363-380.	1.0	21
41	Faulty Instantiations of Threshold Ring Signature from Threshold Proof-of-Knowledge Protocol. Computer Journal, 2016, 59, 945-954.	1.5	2
42	Functional Credentials for Internet of Things. , 2016, , .		2
43	Password-Controlled Encryption with Accountable Break-Glass Access. , 2016, , .		6
44	Efficient Authenticated Multi-Pattern Matching. , 2016, , .		8
45	Cryptography for Parallel RAM from Indistinguishability Obfuscation. , 2016, , .		24
46	A Framework of Multi-Authority Attribute-Based Encryption with Outsourcing and Revocation. , 2016, , .		26
47	Secure Cloud Storage Meets with Secure Network Coding. IEEE Transactions on Computers, 2016, 65, 1936-1948.	2.4	54
48	Combiners for Chosen-Ciphertext Security. Lecture Notes in Computer Science, 2016, , 257-268.	1.0	5
49	Privacy-Preserving Wi-Fi Fingerprinting Indoor Localization. Lecture Notes in Computer Science, 2016, , 215-233.	1.0	10
50	Towards Proofs of Ownership Beyond Bounded Leakage. Lecture Notes in Computer Science, 2016, , 340-350.	1.0	7
51	Non-Malleable Functions and Their Applications. Lecture Notes in Computer Science, 2016, , 386-416.	1.0	12
52	Post-challenge leakage in public-key encryption. Theoretical Computer Science, 2015, 572, 25-49.	0.5	11
53	Practical (fully) distributed signatures provably secure in the standard model. Theoretical Computer Science, 2015, 595, 143-158.	0.5	1
54	Comments on 'Efficient Revocable Certificateless Encryption Secure in the Standard Model'. Computer Journal, 2015, 58, 779-781.	1.5	5

#	Article	IF	Citations
55	Structured Encryption with Non-interactive Updates and Parallel Traversal. , 2015, , .		12
56	Related Randomness Attacks for Public Key Cryptosystems. , 2015, , .		4
57	Time-Bound Anonymous Authentication for Roaming Networks. IEEE Transactions on Information Forensics and Security, 2015, 10, 178-189.	4.5	46
58	Trapdoors for Ideal Lattices with Applications. Lecture Notes in Computer Science, 2015, , 239-256.	1.0	10
59	Black-Box Separations of Hash-and-Sign Signatures in the Non-Programmable Random Oracle Model. Lecture Notes in Computer Science, 2015, , 435-454.	1.0	6
60	Privacy Preserving Collaborative Filtering from Asymmetric Randomized Encoding. Lecture Notes in Computer Science, 2015, , 459-477.	1.0	9
61	Security of Direct Anonymous Authentication Using TPM 2.0 Signature. Lecture Notes in Computer Science, 2015, , 37-48.	1.0	0
62	A tale of two clouds: Computing on data encrypted under multiple keys. , 2014, , .		41
63	Secure One-to-Group Communications Escrow-Free ID-Based Asymmetric Group Key Agreement. Lecture Notes in Computer Science, 2014, , 239-254.	1.0	3
64	Secure cloud storage meets with secure network coding. , 2014, , .		21
65	Key-Aggregate Cryptosystem for Scalable Data Sharing in Cloud Storage. IEEE Transactions on Parallel and Distributed Systems, 2014, 25, 468-477.	4.0	179
66	Cloud-Assisted Mobile-Access of Health Data With Privacy and Auditability. IEEE Journal of Biomedical and Health Informatics, 2014, 18, 419-429.	3.9	92
67	Tracing and revoking leaked credentials. , 2014, , .		18
68	Practical Distributed Signatures in the Standard Model. Lecture Notes in Computer Science, 2014, , 307-326.	1.0	6
69	Practical Dual-Receiver Encryption. Lecture Notes in Computer Science, 2014, , 85-105.	1.0	10
70	All-but-One Dual Projective Hashing and Its Applications. Lecture Notes in Computer Science, 2014, , 181-198.	1.0	3
71	Securely Outsourcing Exponentiations with Single Untrusted Program for Cloud Storage. Lecture Notes in Computer Science, 2014, , 326-343.	1.0	63
72	Multi-key leakage-resilient threshold cryptography. , 2013, , .		2

#	Article	IF	Citations
73	Storing Shared Data on the Cloud via Security-Mediator. , 2013, , .		67
74	Server-aided signatures verification secure against collusion attack. Information Security Technical Report, 2013, 17, 46-57.	1.3	13
75	Towards auditable cloud-assisted access of encrypted health data. , 2013, , .		5
76	Privacy-Preserving Public Auditing for Secure Cloud Storage. IEEE Transactions on Computers, 2013, 62, 362-375.	2.4	980
77	Double-trapdoor anonymous tags for traceable signatures. International Journal of Information Security, 2013, 12, 19-31.	2.3	15
78	Computing encrypted cloud data efficiently under multiple keys. , 2013, , .		12
79	Constant-Size Dynamic k-Times Anonymous Authentication. IEEE Systems Journal, 2013, 7, 249-261.	2.9	26
80	Accumulators and U-Prove Revocation. Lecture Notes in Computer Science, 2013, , 189-196.	1.0	19
81	Towards Anonymous Ciphertext Indistinguishability with Identity Leakage. Lecture Notes in Computer Science, 2013, , 139-153.	1.0	5
82	Identity-Based Encryption Resilient to Continual Auxiliary Leakage. Lecture Notes in Computer Science, 2012, , 117-134.	1.0	64
83	Dynamic Secure Cloud Storage with Provenance. Lecture Notes in Computer Science, 2012, , 442-464.	1.0	37
84	SPICEÂâ€“ Simple Privacy-Preserving Identity-Management for Cloud Environment. Lecture Notes in Computer Science, 2012, , 526-543.	1.0	59
85	Zero-Knowledge Argument for Simultaneous Discrete Logarithms. Algorithmica, 2012, 64, 246-266.	1.0	5
86	PE(AR)2: Privacy-Enhanced Anonymous Authentication with Reputation and Revocation. Lecture Notes in Computer Science, 2012, , 679-696.	1.0	17
87	Multi-authority ciphertext-policy attribute-based encryption with accountability. , 2011, , .		106
88	Identity-based online/offline key encapsulation and encryption. , 2011, , .		32
89	Secure mobile subscription of sensor-encrypted data. , 2011, , .		4
90	Exclusion-intersection encryption. International Journal of Security and Networks, 2011, 6, 136.	0.1	7

#	Article	IF	Citations
91	Optimal Sybil-resilient node admission control. , 2011, , .		95
92	Server-aided signatures verification secure against collusion attack. , 2011, , .		7
93	Efficient Secure Two-Party Exponentiation. Lecture Notes in Computer Science, 2011, , 17-32.	1.0	7
94	Non-interactive Confirmer Signatures. Lecture Notes in Computer Science, 2011, , 49-64.	1.0	1
95	Double-Trapdoor Anonymous Tags for Traceable Signatures. Lecture Notes in Computer Science, 2011, , 183-200.	1.0	13
96	Practical leakage-resilient identity-based encryption from simple assumptions. , 2010, , .		96
97	An efficient signcryption scheme with key privacy and its extension to ring signcryption*. Journal of Computer Security, 2010, 18, 451-473.	0.5	28
98	Efficient Unidirectional Proxy Re-Encryption. Lecture Notes in Computer Science, 2010, , 316-332.	1.0	132
99	Zero-Knowledge Argument for Simultaneous Discrete Logarithms. Lecture Notes in Computer Science, 2010, , 520-529.	1.0	6
100	Blind signature and ring signature schemes: Rehabilitation and attack. Computer Standards and Interfaces, 2009, 31, 707-712.	3.8	9
101	Partial decryption attacks in security-mediated certificateless encryption. IET Information Security, 2009, 3, 148-151.	1.1	4
102	Improving privacy and security in multi-authority attribute-based encryption. , 2009, , .		505
103	Removing Escrow from Identity-Based Encryption. Lecture Notes in Computer Science, 2009, , 256-276.	1.0	83
104	Conditional Proxy Broadcast Re-Encryption. Lecture Notes in Computer Science, 2009, , 327-342.	1.0	76
105	Real Traceable Signatures. Lecture Notes in Computer Science, 2009, , 92-107.	1.0	44
106	General Certificateless Encryption and Timed-Release Encryption. Lecture Notes in Computer Science, 2008, , 126-143.	1.0	29
107	Proxy Re-signatures in the Standard Model. Lecture Notes in Computer Science, 2008, , 260-276.	1.0	12
108	Timed-Release Encryption Revisited. Lecture Notes in Computer Science, 2008, , 38-51.	1.0	13

#	Article	IF	Citations
109	Security Mediated Certificateless Signatures. Lecture Notes in Computer Science, 2007, , 459-477.	1.0	22
110	An Efficient Signcryption Scheme with Key Privacy. Lecture Notes in Computer Science, 2007, , 78-93.	1.0	19
111	Strongly-Secure Identity-Based Key Agreement and Anonymous Extension. Lecture Notes in Computer Science, 2007, , 203-220.	1.0	35
112	Batch Pairing Delegation. , 2007, , 74-90.		28
113	Running on Karma â€“ P2P Reputation and Currency Systems. , 2007, , 146-158.		5
114	Anonymous Identification and Designated-Verifiers Signatures from Insecure Batch Verification. Lecture Notes in Computer Science, 2007, , 203-219.	1.0	6
115	Token-Controlled Public Key Encryption in the Standard Model. Lecture Notes in Computer Science, 2007, , 315-332.	1.0	4
116	Short Linkable Ring Signatures Revisited. Lecture Notes in Computer Science, 2006, , 101-115.	1.0	51
117	Practical electronic lotteries with offline TTP. Computer Communications, 2006, 29, 2830-2840.	3.1	13
118	Ring signatures without random oracles. , 2006, , .		63
119	Identity-Based Strong Multi-Designated Verifiers Signatures. Lecture Notes in Computer Science, 2006, , 257-259.	1.0	15
120	Escrowed Linkability of Ring Signatures and Its Applications. Lecture Notes in Computer Science, 2006, , 175-192.	1.0	30
121	A generic anti-spyware solution by access control list at kernel level. Journal of Systems and Software, 2005, 75, 227-234.	3.3	10
122	Forward-secure multisignature and blind signature schemes. Applied Mathematics and Computation, 2005, 168, 895-908.	1.4	14
123	Signcryption in Hierarchical Identity Based Cryptosystem. IFIP Advances in Information and Communication Technology, 2005, , 443-457.	0.5	6
124	Identity Based Threshold Ring Signature. Lecture Notes in Computer Science, 2005, , 218-232.	1.0	46
125	Two Improved Partially Blind Signature Schemes from Bilinear Pairings. Lecture Notes in Computer Science, 2005, , 316-328.	1.0	74
126	Role Activation Management in Role Based Access Control. Lecture Notes in Computer Science, 2005, , 358-369.	1.0	4

#	Article	IF	Citations
127	An e-Lottery Scheme Using Verifiable Random Function. Lecture Notes in Computer Science, 2005, , 651-660.	1.0	13
128	Efficient Identity Based Ring Signature. Lecture Notes in Computer Science, 2005, , 499-512.	1.0	120
129	Identity Based Ring Signature: Why, How and What Next. Lecture Notes in Computer Science, 2005, , 144-161.	1.0	22
130	Short E-Cash. Lecture Notes in Computer Science, 2005, , 332-346.	1.0	14
131	Generic Construction of (Identity-Based) Perfect Concurrent Signatures. Lecture Notes in Computer Science, 2005, , 194-206.	1.0	31
132	Verifiable Pairing and Its Applications. Lecture Notes in Computer Science, 2005, , 170-187.	1.0	11
133	Identity Based Delegation Network. Lecture Notes in Computer Science, 2005, , 99-115.	1.0	4
134	Security Analysis of Three Cryptographic Schemes from Other Cryptographic Schemes. Lecture Notes in Computer Science, 2005, , 290-301.	1.0	0
135	Efficient Forward and Provably Secure ID-Based Signcryption Scheme with Public Verifiability and Public Ciphertext Authenticity. Lecture Notes in Computer Science, 2004, , 352-369.	1.0	99
136	Secure Hierarchical Identity Based Signature and Its Application. Lecture Notes in Computer Science, 2004, , 480-494.	1.0	42
137	Supporting E.cient Authorization in Delegation with Supervision. , 0, , .		1
138	Separable and Anonymous Identity-Based Key Issuing. , 0, , .		21