Ueli Maurer

List of Publications by Year
in descending order

55 papers	2,166 citations	279701 23 h-index	302012 39 g-index
55 all docs	55 docs citations	55 times ranked	864 citing authors

#	Article	IF	Citations
1	Non-malleable Encryption: Simpler, Shorter, Stronger. Journal of Cryptology, 2020, 33, 1984-2033.	2.1	1
2	Synchronous Constructive Cryptography. Lecture Notes in Computer Science, 2020, , 439-472.	1.0	6
3	Per-session security: Password-based cryptography revisited. Journal of Computer Security, 2019, 27, 75-111.	0.5	2
4	Composable and Finite Computational Security of Quantum Message Transmission. Lecture Notes in Computer Science, 2019, , 282-311.	1.0	1
5	Causal Boxes: Quantum Information-Processing Systems Closed under Composition. IEEE Transactions on Information Theory, 2017, , 1-1.	1.5	24
6	Per-Session Security: Password-Based Cryptography Revisited. Lecture Notes in Computer Science, 2017, , 408-426.	1.0	2
7	An information-theoretic approach to hardness amplification. , 2017, , .		1
8	Witness-hiding proofs of knowledge for cable locks. , 2017, , .		0
9	On the impossibility of information-theoretic composable coin toss extension. , 2016, , .		0
10	Quantum technology: from research to application. Applied Physics B: Lasers and Optics, 2016, 122, 1.	1.1	42
11	Breaking RSA Generically Is Equivalent to Factoring. IEEE Transactions on Information Theory, 2016, 62, 6251-6259.	1.5	19
12	A Definitional Framework for Functional Encryption. , 2015, , .		5
13	Zero-knowledge proofs of knowledge for group homomorphisms. Designs, Codes, and Cryptography, 2015, 77, 663-676.	1.0	17
14	Query-Complexity Amplification for Random Oracles. Lecture Notes in Computer Science, 2015, , 159-180.	1.0	3
15	From Single-Bit to Multi-bit Public-Key Encryption via Non-malleable Codes. Lecture Notes in Computer Science, 2015, , 532-560.	1.0	42
16	Idealizing Identity-Based Encryption. Lecture Notes in Computer Science, 2015, , 495-520.	1.0	8
17	Broadcast Amplification. Lecture Notes in Computer Science, 2014, , 419-439.	1.0	2
18	The one-time pad revisited. , 2013, , .		13

#	Article	IF	Citations
19	Conditional equivalence of random systems and indistinguishability proofs. , 2013, , .		8
20	Authentication amplification by synchronization. , 2013, , .		3
21	Unfair coin tossing. , 2013, , .		1
22	Common randomness amplification: A constructive view. , 2012, , .		1
23	Constructive Cryptography â€“ A New Paradigm for Security Definitions and Proofs. Lecture Notes in Computer Science, 2012, , 33-56.	1.0	90
24	Breaking RSA Generically Is Equivalent to Factoring. Lecture Notes in Computer Science, 2009, , 36-53.	1.0	47
25	Unifying Zero-Knowledge Proofs of Knowledge. Lecture Notes in Computer Science, 2009, , 272-286.	1.0	38
26	The Bare Bounded-Storage Model: The Tight Bound on the Storage Requirement for Key Agreement. IEEE Transactions on Information Theory, 2008, 54, 2790-2792.	1.5	9
27	Introduction to the Special Issue on Information Theoretic Security. IEEE Transactions on Information Theory, 2008, 54, 2405-2407.	1.5	7
28	MPC vs. SFE: Perfect Security in a Unified Corruption Model. , 2008, , 231-250.		12
29	MPC vs. SFE : Unconditional and Computational Security. Lecture Notes in Computer Science, 2008, , 1-18.	1.0	17
30	Small Accessible Quantum Information Does Not Imply Security. Physical Review Letters, 2007, 98, 140502.	2.9	95
31	Black-Box Extension Fields and the Inexistence of Field-Homomorphic One-Way Permutations. , 2007, , 427-443.		11
32	Secure multi-party computation made simple. Discrete Applied Mathematics, 2006, 154, 370-381.	0.5	72
33	Byzantine Agreement Given Partial Broadcast. Journal of Cryptology, 2005, 18, 191-217.	2.1	25
34	Efficient Proofs of Knowledge of Discrete Logarithms and Representations in Groups with Hidden Order. Lecture Notes in Computer Science, 2005, , 154-171.	1.0	26
35	Abstract Models of Computation in Cryptography. Lecture Notes in Computer Science, 2005, , 1-12.	1.0	127
36	The role of cryptography in database security. , 2004, , .		28

#	Article	IF	Citations
37	Optimal Randomizer Efficiency in the Bounded-Storage Model. Journal of Cryptology, 2004, 17, 5-26.	2.1	45
38	On Generating the Initial Key in the Bounded-Storage Model. Lecture Notes in Computer Science, 2004, , 126-137.	1.0	46
39	Towards a Theory of Consistency Primitives. Lecture Notes in Computer Science, 2004, , 379-389.	1.0	3
40	Secure Multi-party Computation Made Simple. Lecture Notes in Computer Science, 2003, , 14-28.	1.0	37
41	Unconditional Byzantine Agreement and Multi-party Computation Secure against Dishonest Minorities from Scratch. Lecture Notes in Computer Science, 2002, , 482-501.	1.0	24
42	Tight security proofs for the bounded-storage model. , 2002, , .		33
43	Indistinguishability of Random Systems. Lecture Notes in Computer Science, 2002, , 110-132.	1.0	129
44	Quantum Solution to the Byzantine Agreement Problem. Physical Review Letters, 2001, 87, 217901.	2.9	109
45	Cryptography 2000Â±10. Lecture Notes in Computer Science, 2001, , 63-85.	1.0	5
46	Robustness for Free in Unconditional Multi-party Computation. Lecture Notes in Computer Science, 2001, , 101-118.	1.0	43
47	Player Simulation and General Adversary Structures in Perfect Multiparty Computation. Journal of Cryptology, 2000, 13, 31-60.	2.1	169
48	General Secure Multi-party Computation from any Linear Secret-Sharing Scheme. Lecture Notes in Computer Science, 2000, , 316-334.	1.0	315
49	Efficient Secure Multi-party Computation. Lecture Notes in Computer Science, 2000, , 143-161.	1.0	79
50	General Adversaries in Unconditional Multi-party Computation. Lecture Notes in Computer Science, 1999, , 232-246.	1.0	29
51	Trading correctness for privacy in unconditional multi-party computation. Lecture Notes in Computer Science, 1998, , 121-136.	1.0	40
52	Complete characterization of adversaries tolerable in secure multi-party computation (extended) Tj ETQq0 0 0 rgBT /Overlock 10 Tf 50 1		102
53	Digital payment systems with passive anonymity-revoking trustees*. Journal of Computer Security, 1997, 5, 69-89.	0.5	33
54	Unconditional security against memory-bounded adversaries. Lecture Notes in Computer Science, 1997, , 292-306.	1.0	109

#	Article	IF	Citations
55	Cryptography and Computation after Turing. , 0, , 53-77.		11