Michel Abdalla

List of Publications by Year
in descending order

81 papers	3,808 citations	159525 30 h-index	128225 60 g-index
87 all docs	87 docs citations	87 times ranked	1414 citing authors

#	Article	IF	Citations
1	Password-Based Authenticated Key Exchange in the Three-Party Setting. Lecture Notes in Computer Science, 2005, , 65-84.	1.0	430
2	Searchable Encryption Revisited:ÂConsistency Properties, Relation to Anonymous IBE, and Extensions. Lecture Notes in Computer Science, 2005, , 205-222.	1.0	357
3	The Oracle Diffie-Hellman Assumptions and an Analysis of DHIES. Lecture Notes in Computer Science, 2001, , 143-158.	1.0	277
4	Searchable Encryption Revisited: Consistency Properties, Relation to Anonymous IBE, and Extensions. Journal of Cryptology, 2008, 21, 350-391.	2.1	247
5	Simple Password-Based Encrypted Key Exchange Protocols. Lecture Notes in Computer Science, 2005, , 191-208.	1.0	201
6	Simple Functional Encryption Schemes for Inner Products. Lecture Notes in Computer Science, 2015, , 733-751.	1.0	170
7	From Identification to Signatures via the Fiat-Shamir Transform: Minimizing Assumptions for Security and Forward-Security. Lecture Notes in Computer Science, 2002, , 418-433.	1.0	120
8	Robust Encryption. Lecture Notes in Computer Science, 2010, , 480-497.	1.0	82
9	Interactive Diffie-Hellman Assumptions with Applications to Password-Based Authentication. Lecture Notes in Computer Science, 2005, , 341-356.	1.0	78
10	Identity-Based Encryption Gone Wild. Lecture Notes in Computer Science, 2006, , 300-311.	1.0	76
11	Multi-input Inner-Product Functional Encryption from Pairings. Lecture Notes in Computer Science, 2017, , 601-626.	1.0	68
12	Password-Based Group Key Exchange in a Constant Number of Rounds. Lecture Notes in Computer Science, 2006, , 427-442.	1.0	65
13	One-Time Verifier-Based Encrypted Key Exchange. Lecture Notes in Computer Science, 2005, , 47-64.	1.0	60
14	Smooth Projective Hashing for Conditionally Extractable Commitments. Lecture Notes in Computer Science, 2009, , 671-689.	1.0	60
15	Multi-Input Functional Encryption for Inner Products: Function-Hiding Realizations and Constructions Without Pairings. Lecture Notes in Computer Science, 2018, , 597-627.	1.0	58
16	Tightly-Secure Signatures from Lossy Identification Schemes. Lecture Notes in Computer Science, 2012, , 572-590.	1.0	58
17	Key management for restricted multicast using broadcast encryption. IEEE/ACM Transactions on Networking, 2000, 8, 443-454.	2.6	57
18	Security of the J-PAKE Password-Authenticated Key Exchange Protocol. , 2015, , .		48

#	Article	IF	Citations
19	Generalized Key Delegation for Hierarchical Identity-Based Encryption. Lecture Notes in Computer Science, 2007, , 139-154.	1.0	46
20	Forward-Secure Threshold Signature Schemes. Lecture Notes in Computer Science, 2001, , 441-456.	1.0	42
21	Disjunctions for Hash Proof Systems: New Constructions and Applications. Lecture Notes in Computer Science, 2015, , 69-100.	1.0	42
22	Efficient Two-Party Password-Based Key Exchange Protocols in the UC Framework. Lecture Notes in Computer Science, 2008, , 335-351.	1.0	38
23	A Scalable Password-Based Group Key Exchange Protocol in the Standard Model. Lecture Notes in Computer Science, 2006, , 332-347.	1.0	37
24	Public-Key Encryption Indistinguishable Under Plaintext-Checkable Attacks. Lecture Notes in Computer Science, 2015, , 332-352.	1.0	36
25	Decentralizing Inner-Product Functional Encryption. Lecture Notes in Computer Science, 2019, , 128-157.	1.0	35
26	Identity-Based Traitor Tracing. Lecture Notes in Computer Science, 2007, , 361-376.	1.0	34
27	SPHF-Friendly Non-interactive Commitments. Lecture Notes in Computer Science, 2013, , 214-234.	1.0	32
28	Provably secure password-based authentication in TLS. , 2006, , .		31
29	A Simple Threshold Authenticated Key Exchange from Short Secrets. Lecture Notes in Computer Science, 2005, , 566-584.	1.0	31
30	From Single-Input to Multi-client Inner-Product Functional Encryption. Lecture Notes in Computer Science, 2019, , 552-582.	1.0	31
31	Verifiable Random Functions from Identity-Based Key Encapsulation. Lecture Notes in Computer Science, 2009, , 554-571.	1.0	30
32	Inner-Product Functional Encryption with Fine-Grained Access Control. Lecture Notes in Computer Science, 2020, , 467-497.	1.0	29
33	Securing wireless sensor networks against aggregator compromises. , 2008, 46, 134-141.		27
34	From Identification to Signatures Via the Fiatâ€“Shamir Transform: Necessary and Sufficient Conditions for Security and Forward-Security. IEEE Transactions on Information Theory, 2008, 54, 3631-3646.	1.5	26
35	Related-Key Security for Pseudorandom Functions Beyond the Linear Barrier. Lecture Notes in Computer Science, 2014, , 77-94.	1.0	26
36	Wildcarded Identity-Based Encryption. Journal of Cryptology, 2011, 24, 42-82.	2.1	25

#	Article	IF	Citations
37	Verifiable Random Functions: Relations to Identity-Based Key Encapsulation and New Constructions. Journal of Cryptology, 2014, 27, 544-593.	2.1	25
38	(Password) Authenticated Key Establishment: From 2-Party to Group. Lecture Notes in Computer Science, 2007, , 499-514.	1.0	25
39	Strong password-based authentication in TLS using the three-party group Diffie Hellman protocol. International Journal of Security and Networks, 2007, 2, 284.	0.1	24
40	Anonymous and Transparent Gateway-Based Password-Authenticated Key Exchange. Lecture Notes in Computer Science, 2008, , 133-148.	1.0	23
41	Leakage-Resilient Symmetric Encryption via Re-keying. Lecture Notes in Computer Science, 2013, , 471-488.	1.0	22
42	Tightly Secure Signatures From Lossy Identification Schemes. Journal of Cryptology, 2016, 29, 597-631.	2.1	22
43	On the Minimal Assumptions of Group Signature Schemes. Lecture Notes in Computer Science, 2004, , 1-13.	1.0	21
44	Somewhat homomorphic encryption scheme for arithmetic operations on large integers. , 2012, , .		20
45	On the (Im)possibility of Blind Message Authentication Codes. Lecture Notes in Computer Science, 2006, , 262-279.	1.0	20
46	Tighter Reductions for Forward-Secure Signature Schemes. Lecture Notes in Computer Science, 2013, , 292-311.	1.0	18
47	Universally Composable Relaxed Password Authenticated Key Exchange. Lecture Notes in Computer Science, 2020, , 278-307.	1.0	17
48	Functional Encryption for Attribute-Weighted Sums from k-Lin. Lecture Notes in Computer Science, 2020, , 685-716.	1.0	17
49	Distributed Public-Key Cryptography from Weak Secrets. Lecture Notes in Computer Science, 2009, , 139-159.	1.0	16
50	Contributory Password-Authenticated Group Key Exchange with Join Capability. Lecture Notes in Computer Science, 2011, , 142-160.	1.0	15
51	Generalised key delegation for hierarchical identity-based encryption. IET Information Security, 2008, 2, 67.	1.1	14
52	Towards Making Broadcast Encryption Practical. Lecture Notes in Computer Science, 1999, , 140-157.	1.0	14
53	Robust Password-Protected Secret Sharing. Lecture Notes in Computer Science, 2016, , 61-79.	1.0	14
54	Generalized Key Delegation for Wildcarded Identity-Based and Inner-Product Encryption. IEEE Transactions on Information Forensics and Security, 2012, 7, 1695-1706.	4.5	13

#	Article	IF	Citations
55	Robust Encryption. Journal of Cryptology, 2018, 31, 307-350.	2.1	12
56	Password-Authenticated Group Key Agreement with Adaptive Security and Contributiveness. Lecture Notes in Computer Science, 2009, , 254-271.	1.0	12
57	An Algebraic Framework for Pseudorandom Functions and Applications to Related-Key Security. Lecture Notes in Computer Science, 2015, , 388-409.	1.0	12
58	Publicâ€key encryption indistinguishable under plaintextâ€checkable attacks. IET Information Security, 2016, 10, 288-303.	1.1	11
59	Flexible Group Key Exchange with On-demand Computation of Subgroup Keys. Lecture Notes in Computer Science, 2010, , 351-368.	1.0	10
60	Security Analysis ofÂCPace. Lecture Notes in Computer Science, 2021, , 711-741.	1.0	9
61	Password-Based Authenticated Key Exchange: An Overview. Lecture Notes in Computer Science, 2014, , 1-9.	1.0	8
62	Multi-Client Inner-Product Functional Encryption in the Random-Oracle Model. Lecture Notes in Computer Science, 2020, , 525-545.	1.0	8
63	From Selective to Full Security: Semi-generic Transformations in the Standard Model. Lecture Notes in Computer Science, 2012, , 316-333.	1.0	8
64	Robust Pseudo-Random Number Generators with Input Secure Against Side-Channel Attacks. Lecture Notes in Computer Science, 2015, , 635-654.	1.0	6
65	Lattice-Based Hierarchical Inner Product Encryption. Lecture Notes in Computer Science, 2012, , 121-138.	1.0	6
66	Algebraic Adversaries inÂtheÂUniversal Composability Framework. Lecture Notes in Computer Science, 2021, , 311-341.	1.0	6
67	Removing Erasures with Explainable Hash Proof Systems. Lecture Notes in Computer Science, 2017, , 151-174.	1.0	5
68	Practical dynamic group signature with efficient concurrent joins and batch verifications. Journal of Information Security and Applications, 2021, 63, 103003.	1.8	5
69	Pairing-Based Cryptography â€“ Pairing 2012. Lecture Notes in Computer Science, 2013, , .	1.0	4
70	Progress in Cryptology â€“ LATINCRYPT 2010. Lecture Notes in Computer Science, 2010, , .	1.0	4
71	Secure architectures of future emerging cryptography SAFEcrypto. , 2016, , .		3
72	Related-Key Security for Pseudorandom Functions Beyond the Linear Barrier. Journal of Cryptology, 2018, 31, 917-964.	2.1	3

#	Article	IF	Citations
73	New technique for chosen-ciphertext security based on non-interactive zero-knowledge. Information Sciences, 2019, 490, 18-35.	4.0	3
74	On the Tightness of Forward-Secure Signature Reductions. Journal of Cryptology, 2019, 32, 84-150.	2.1	3
75	Leakage-Resilient Spatial Encryption. Lecture Notes in Computer Science, 2012, , 78-99.	1.0	2
76	Algebraic XOR-RKA-Secure Pseudorandom Functions from Post-Zeroizing Multilinear Maps. Lecture Notes in Computer Science, 2019, , 386-412.	1.0	2
77	A Study of Blind Message Authentication Codes. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2007, E90-A, 75-82.	0.2	1
78	Multilinear and Aggregate Pseudorandom Functions: New Constructions and Improved Security. Lecture Notes in Computer Science, 2015, , 103-120.	1.0	1
79	Resisting against aggregator compromises in sensor networks. , 2006, , .		0
80	Improving Thomlinson-Walkerâ€™s Software Patching Scheme Using Standard Cryptographic and Statistical Tools. Lecture Notes in Computer Science, 2014, , 8-14.	1.0	0
81	Cryptology and Network Security. Lecture Notes in Computer Science, 2013, , .	1.0	0