Victor Shoup

List of Publications by Year in descending order

29 papers	2,560 citations	430874 18 h-index	580821 25 g-index
31 all docs	31 docs citations	31 times ranked	792 citing authors

#	Article	IF	Citations
1	Design and Analysis of Practical Public-Key Encryption Schemes Secure against Adaptive Chosen Ciphertext Attack. SIAM Journal on Computing, 2003, 33, 167-226.	1.0	685
2	Signature schemes based on the strong RSA assumption. ACM Transactions on Information and System Security, 2000, 3, 161-185.	4.5	216
3	Random Oracles in Constantinople: Practical Asynchronous Byzantine Agreement Using Cryptography. Journal of Cryptology, 2005, 18, 219-246.	2.8	177
4	The Twin Diffie-Hellman Problem and Applications. , 2008, , 127-145.		162
5	Computing Frobenius maps and factoring polynomials. Computational Complexity, 1992, 2, 187-224.	0.3	137
6	New algorithms for finding irreducible polynomials over finite fields. Mathematics of Computation, 1990, 54, 435-447.	2.1	127
7	Securing Threshold Cryptosystems against Chosen Ciphertext Attack. Journal of Cryptology, 2002, 15, 75-96.	2.8	121
8	Subquadratic-time factoring of polynomials over finite fields. Mathematics of Computation, 1998, 67, 1179-1198.	2.1	102
9	Fast Construction of Irreducible Polynomials over Finite Fields. Journal of Symbolic Computation, 1994, 17, 371-391.	0.8	100
10	Tag-KEM/DEM: A New Framework for Hybrid Encryption and A New Analysis of Kurosawa-Desmedt KEM. Lecture Notes in Computer Science, 2005, , 128-146.	1.3	94
11	A New Polynomial Factorization Algorithm and its Implementation. Journal of Symbolic Computation, 1995, 20, 363-397.	0.8	78
12	Searching for primitive roots in finite fields. Mathematics of Computation, 1992, 58, 369-380.	2.1	76
13	Algorithms for Exponentiation in Finite Fields. Journal of Symbolic Computation, 2000, 29, 879-889.	0.8	71
14	On the deterministic complexity of factoring polynomials over finite fields. Information Processing Letters, 1990, 33, 261-267.	0.6	67
15	The Twin Diffieâ€“Hellman Problem and Applications. Journal of Cryptology, 2009, 22, 470-504.	2.8	58
16	Simple and Efficient Public-Key Encryption from Computational Diffie-Hellman in the Standard Model. Lecture Notes in Computer Science, 2010, , 1-18.	1.3	47
17	GNUC: A New Universal Composability Framework. Journal of Cryptology, 2015, 28, 423-508.	2.8	36
18	Stateful public-key cryptosystems. , 2006, , .		33

#	Article	IF	Citations
19	A fast deterministic algorithm for factoring polynomials over finite fields of small characteristic. , 1991, , .		27
20	Practical Chosen Ciphertext Secure Encryption from Factoring. Journal of Cryptology, 2013, 26, 102-118.	2.8	26
21	Fast polynomial factorization over high algebraic extensions of finite fields. , 1997, , .		23
22	Credential Authenticated Identification and Key Exchange. Lecture Notes in Computer Science, 2010, , 255-276.	1.3	21
23	Factoring polynomials using fewer random bits. Journal of Symbolic Computation, 1990, 9, 229-239.	0.8	18
24	Smoothness and factoring polynomials over finite fields. Information Processing Letters, 1991, 38, 39-42.	0.6	18
25	A New and Improved Paradigm for Hybrid Encryption Secure Against Chosen-Ciphertext Attack. Journal of Cryptology, 2010, 23, 91-120.	2.8	15
26	Primality testing with fewer random bits. Computational Complexity, 1993, 3, 355-367.	0.3	10
27	Counting the number of points on elliptic curves over finite fields of characteristic greater than three. Lecture Notes in Computer Science, 1994, , 60-70.	1.3	10
28	Constructing nonresidues in finite fields and the extended Riemann hypothesis. Mathematics of Computation, 1996, 65, 1311-1327.	2.1	4
29	Security Analysis of $$extit{SPAKE2}+$$. Lecture Notes in Computer Science, 2020, , 31-60.	1.3	1