David Pointcheval

List of Publications by Year
in descending order

154 papers	10,630 citations	57631 44 h-index	35952 97 g-index
162 all docs	162 docs citations	162 times ranked	2655 citing authors

#	Article	IF	Citations
1	Traceable Inner Product Functional Encryption. Lecture Notes in Computer Science, 2020, , 564-585.	1.0	7
2	Boosting Verifiable Computation onÂEncrypted Data. Lecture Notes in Computer Science, 2020, , 124-154.	1.0	19
3	Dynamic Decentralized Functional Encryption. Lecture Notes in Computer Science, 2020, , 747-775.	1.0	21
4	Multi-Client Inner-Product Functional Encryption in the Random-Oracle Model. Lecture Notes in Computer Science, 2020, , 525-545.	1.0	8
5	Linearly-Homomorphic Signatures and Scalable Mix-Nets. Lecture Notes in Computer Science, 2020, , 597-627.	1.0	6
6	Unbounded Inner-Product Functional Encryption with Succinct Keys. Lecture Notes in Computer Science, 2019, , 426-441.	1.0	15
7	On the Tightness of Forward-Secure Signature Reductions. Journal of Cryptology, 2019, 32, 84-150.	2.1	3
8	Divisible E-Cash from Constrained Pseudo-Random Functions. Lecture Notes in Computer Science, 2019, , 679-708.	1.0	8
9	Decentralized Evaluation of Quadratic Polynomials on Encrypted Data. Lecture Notes in Computer Science, 2019, , 87-106.	1.0	0
10	Fuzzy Password-Authenticated Key Exchange. Lecture Notes in Computer Science, 2018, , 393-424.	1.0	23
11	Decentralized Multi-Client Functional Encryption for Inner Product. Lecture Notes in Computer Science, 2018, , 703-732.	1.0	62
12	Reassessing Security of Randomizable Signatures. Lecture Notes in Computer Science, 2018, , 319-338.	1.0	21
13	Privacy-Preserving Plaintext-Equality of Low-Entropy Inputs. Lecture Notes in Computer Science, 2018, , 262-279.	1.0	3
14	Practical Strategy-Resistant Privacy-Preserving Elections. Lecture Notes in Computer Science, 2018, , 331-349.	1.0	6
15	Functional Encryption with Oblivious Helper. , 2017, , .		1
16	VTBPEKE. , 2017, , .		20
17	Human Computing for Handling Strong Corruptions in Authenticated Key Exchange. , 2017, , .		4
18	Removing the Strong RSA Assumption from Arguments over the Integers. Lecture Notes in Computer Science, 2017, , 321-350.	1.0	22

#	Article	IF	Citations
19	Cut Down the Tree to Achieve Constant Complexity in Divisible E-cash. Lecture Notes in Computer Science, 2017, , 61-90.	1.0	4
20	Removing Erasures with Explainable Hash Proof Systems. Lecture Notes in Computer Science, 2017, , 151-174.	1.0	5
21	Homomorphic-Policy Attribute-Based Key Encapsulation Mechanisms. Lecture Notes in Computer Science, 2017, , 155-172.	1.0	0
22	Divisible eâ€cash made practical. IET Information Security, 2016, 10, 332-347.	1.1	4
23	Publicâ€key encryption indistinguishable under plaintextâ€checkable attacks. IET Information Security, 2016, 10, 288-303.	1.1	11
24	Short Randomizable Signatures. Lecture Notes in Computer Science, 2016, , 111-126.	1.0	145
25	Secure Distributed Computation on Private Inputs. Lecture Notes in Computer Science, 2016, , 14-26.	1.0	3
26	Legally Fair Contract Signing Without Keystones. Lecture Notes in Computer Science, 2016, , 175-190.	1.0	7
27	Robust Password-Protected Secret Sharing. Lecture Notes in Computer Science, 2016, , 61-79.	1.0	14
28	Encryption Switching Protocols. Lecture Notes in Computer Science, 2016, , 308-338.	1.0	21
29	Robust Pseudo-Random Number Generators with Input Secure Against Side-Channel Attacks. Lecture Notes in Computer Science, 2015, , 635-654.	1.0	6
30	Scalable Divisible E-cash. Lecture Notes in Computer Science, 2015, , 287-306.	1.0	5
31	Public-Key Encryption Indistinguishable Under Plaintext-Checkable Attacks. Lecture Notes in Computer Science, 2015, , 332-352.	1.0	36
32	Simple Functional Encryption Schemes for Inner Products. Lecture Notes in Computer Science, 2015, , 733-751.	1.0	170
33	Divisible E-Cash Made Practical. Lecture Notes in Computer Science, 2015, , 77-100.	1.0	23
34	Disjunctions for Hash Proof Systems: New Constructions and Applications. Lecture Notes in Computer Science, 2015, , 69-100.	1.0	42
35	Implicit Zero-Knowledge Arguments and Applications to the Malicious Setting. Lecture Notes in Computer Science, 2015, , 107-129.	1.0	15
36	Forward Secure Non-Interactive Key Exchange. Lecture Notes in Computer Science, 2014, , 21-39.	1.0	12

#	ARTICLE	IF	CITATIONS
37	Efficient Delegation of Zero-Knowledge Proofs of Knowledge in a Pairing-Friendly Setting. Lecture Notes in Computer Science, 2014, , 167-184.	1.0	2
38	Adaptive CCA broadcast encryption with constant-size secret keys and ciphertexts. International Journal of Information Security, 2013, 12, 251-265.	2.3	50
39	Black-Box Trace&Revoke Codes. Algorithmica, 2013, 67, 418-448.	1.0	2
40	Multi-channel broadcast encryption. , 2013, , .		8
41	Short blind signatures. Journal of Computer Security, 2013, 21, 627-661.	0.5	13
42	Security analysis of pseudo-random number generators with input. , 2013, , .		71
43	Efficient UC-Secure Authenticated Key-Exchange for Algebraic Languages. Lecture Notes in Computer Science, 2013, , 272-291.	1.0	27
44	Tighter Reductions for Forward-Secure Signature Schemes. Lecture Notes in Computer Science, 2013, , 292-311.	1.0	18
45	Analysis and Improvement of Lindell's UC-Secure Commitment Schemes. Lecture Notes in Computer Science, 2013, , 534-551.	1.0	21
46	New Techniques for SPHFs and Efficient One-Round PAKE Protocols. Lecture Notes in Computer Science, 2013, , 449-475.	1.0	82
47	SPHF-Friendly Non-interactive Commitments. Lecture Notes in Computer Science, 2013, , 214-234.	1.0	32
48	Verified security of redundancy-free encryption from Rabin and RSA. , 2012, , .		5
49	Traceable Signature with Stepping Capabilities. Lecture Notes in Computer Science, 2012, , 108-131.	1.0	5
50	Round-Optimal Privacy-Preserving Protocols with Smooth Projective Hash Functions. Lecture Notes in Computer Science, 2012, , 94-111.	1.0	26
51	Password-Based Authenticated Key Exchange. Lecture Notes in Computer Science, 2012, , 390-397.	1.0	23
52	Adaptive CCA Broadcast Encryption with Constant-Size Secret Keys and Ciphertexts. Lecture Notes in Computer Science, 2012, , 308-321.	1.0	15
53	Compact Round-Optimal Partially-Blind Signatures. Lecture Notes in Computer Science, 2012, , 95-112.	1.0	8
54	Decentralized Dynamic Broadcast Encryption. Lecture Notes in Computer Science, 2012, , 166-183.	1.0	8

#	Article	IF	Citations
55	Autotomic Signatures. Lecture Notes in Computer Science, 2012, , 143-155.	1.0	0
56	Message-Based Traitor Tracing with Optimal Ciphertext Rate. Lecture Notes in Computer Science, 2012, , 56-77.	1.0	5
57	Contributory Password-Authenticated Group Key Exchange with Join Capability. Lecture Notes in Computer Science, 2011, , 142-160.	1.0	15
58	Signatures on Randomizable Ciphertexts. Lecture Notes in Computer Science, 2011, , 403-422.	1.0	44
59	Security Notions for Broadcast Encryption. Lecture Notes in Computer Science, 2011, , 377-394.	1.0	17
60	Strong Cryptography from Weak Secrets. Lecture Notes in Computer Science, 2010, , 297-315.	1.0	10
61	Flexible Group Key Exchange with On-demand Computation of Subgroup Keys. Lecture Notes in Computer Science, 2010, , 351-368.	1.0	10
62	Mediated Traceable Anonymous Encryption. Lecture Notes in Computer Science, 2010, , 40-60.	1.0	9
63	Parallel Signcryption. Information Security and Cryptography, 2010, , 175-192.	0.2	1
64	Distributed Public-Key Cryptography from Weak Secrets. Lecture Notes in Computer Science, 2009, , 139-159.	1.0	16
65	Optimal Randomness Extraction from a Diffie-Hellman Element. Lecture Notes in Computer Science, 2009, , 572-589.	1.0	19
66	Anonymous Consecutive Delegation of Signing Rights: Unifying Group and Proxy Signatures. Lecture Notes in Computer Science, 2009, , 95-115.	1.0	9
67	New Anonymity Notions for Identity-Based Encryption. Lecture Notes in Computer Science, 2009, , 138-157.	1.0	5
68	Password-Authenticated Group Key Agreement with Adaptive Security and Contributiveness. Lecture Notes in Computer Science, 2009, , 254-271.	1.0	12
69	Proofs on Encrypted Values in Bilinear Groups and an Application to Anonymity of Signatures. Lecture Notes in Computer Science, 2009, , 132-149.	1.0	24
70	Smooth Projective Hashing for Conditionally Extractable Commitments. Lecture Notes in Computer Science, 2009, , 671-689.	1.0	60
71	Transferable Constant-Size Fair E-Cash. Lecture Notes in Computer Science, 2009, , 226-247.	1.0	40
72	HMAC is a randomness extractor and applications to TLS. , 2008, , .		21

#	ARTICLE	IF	CITATIONS
73	A Formal Study of the Privacy Concerns in Biometric-Based Remote Authentication Schemes. Lecture Notes in Computer Science, 2008, , 56-70.	1.0	25
74	Multi-factor Authenticated Key Exchange. Lecture Notes in Computer Science, 2008, , 277-295.	1.0	60
75	Efficient Two-Party Password-Based Key Exchange Protocols in the UC Framework. Lecture Notes in Computer Science, 2008, , 335-351.	1.0	38
76	Dynamic Threshold Public-Key Encryption. Lecture Notes in Computer Science, 2008, , 317-334.	1.0	69
77	New Anonymity Notions for Identity-Based Encryption. Lecture Notes in Computer Science, 2008, , 375-391.	1.0	9
78	An Application of the Boneh and Shacham Group Signature Scheme to Biometric Authentication. Lecture Notes in Computer Science, 2008, , 219-230.	1.0	15
79	Anonymous and Transparent Gateway-Based Password-Authenticated Key Exchange. Lecture Notes in Computer Science, 2008, , 133-148.	1.0	23
80	An Application of the Goldwasser-Micali Cryptosystem to Biometric Authentication. Lecture Notes in Computer Science, 2007, , 96-106.	1.0	79
81	Provably secure authenticated group Diffie-Hellman key exchange. ACM Transactions on Information and System Security, 2007, 10, 10.	4.5	60
82	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
83	A security solution for IEEE 802.11's ad hoc mode: password-authentication and group Diffie Hellman key exchange. International Journal of Wireless and Mobile Computing, 2007, 2, 4.	0.1	13
84	Trapdoor Hard-to-Invert Group Isomorphisms and Their Application to Password-Based Authentication. Journal of Cryptology, 2007, 20, 115-149.	2.1	17
85	Fully Collusion Secure Dynamic Broadcast Encryption with Constant-Size Ciphertexts or Decryption Keys. Lecture Notes in Computer Science, 2007, , 39-59.	1.0	144
86	Extended Private Information Retrieval and Its Application in Biometrics Authentications. Lecture Notes in Computer Science, 2007, , 175-193.	1.0	27
87	Automated Security Proofs with Sequences of Games. Lecture Notes in Computer Science, 2006, , 537-554.	1.0	51
88	A Scalable Password-Based Group Key Exchange Protocol in the Standard Model. Lecture Notes in Computer Science, 2006, , 332-347.	1.0	37
89	Provably secure password-based authentication in TLS. , 2006, , .		31
90	Encoding-Free ElGamal Encryption Without Random Oracles. Lecture Notes in Computer Science, 2006, , 91-104.	1.0	22

#	Article	IF	Citations
91	The Twist-AUgmented Technique for Key Exchange. Lecture Notes in Computer Science, 2006, , 410-426.	1.0	29
92	Password-Based Group Key Exchange in a Constant Number of Rounds. Lecture Notes in Computer Science, 2006, , 427-442.	1.0	65
93	Hardness of Distinguishing the MSB or LSB of Secret Keys in Diffie-Hellman Schemes. Lecture Notes in Computer Science, 2006, , 240-251.	1.0	8
94	About the Security of MTI/C0 and MQV. Lecture Notes in Computer Science, 2006, , 156-172.	1.0	22
95	A New Key Exchange Protocol Based on MQV Assuming Public Computations. Lecture Notes in Computer Science, 2006, , 186-200.	1.0	3
96	Public Traceability in Traitor Tracing Schemes. Lecture Notes in Computer Science, 2005, , 542-558.	1.0	72
97	Optimal Asymmetric Encryption and Signature Paddings. Lecture Notes in Computer Science, 2005, , 254-268.	1.0	10
98	Password-Based Authenticated Key Exchange in the Three-Party Setting. Lecture Notes in Computer Science, 2005, , 65-84.	1.0	430
99	Simple Password-Based Encrypted Key Exchange Protocols. Lecture Notes in Computer Science, 2005, , 191-208.	1.0	201
100	Interactive Diffie-Hellman Assumptions with Applications to Password-Based Authentication. Lecture Notes in Computer Science, 2005, , 341-356.	1.0	78
101	Provable Security for Public Key Schemes. , 2005, , 133-190.		17
102	A Simple Threshold Authenticated Key Exchange from Short Secrets. Lecture Notes in Computer Science, 2005, , 566-584.	1.0	31
103	One-Time Verifier-Based Encrypted Key Exchange. Lecture Notes in Computer Science, 2005, , 47-64.	1.0	60
104	On the Security Notions for Public-Key Encryption Schemes. Lecture Notes in Computer Science, 2005, , 33-46.	1.0	6
105	New Security Results on Encrypted Key Exchange. Lecture Notes in Computer Science, 2004, , 145-158.	1.0	111
106	RSA-OAEP Is Secure under the RSA Assumption. Journal of Cryptology, 2004, 17, 81-104.	2.1	104
107	Mutual authentication and group key agreement for low-power mobile devices. Computer Communications, 2004, 27, 1730-1737.	3.1	57
108	IPAKE: Isomorphisms for Password-Based Authenticated Key Exchange. Lecture Notes in Computer Science, 2004, , 477-493.	1.0	15

#	Article	IF	Citations
109	How to Disembed a Program?. Lecture Notes in Computer Science, 2004, , 441-454.	1.0	4
110	OAEP 3-Round:A Generic and Secure Asymmetric Encryption Padding. Lecture Notes in Computer Science, 2004, , 63-77.	1.0	32
111	A New (mathcal{N}mathcal{P})-Complete Problem and Public-Key Identification. Designs, Codes, and Cryptography, 2003, 28, 5-31.	1.0	10
112	The One-More-RSA-Inversion Problems and the Security of Chaum's Blind Signature Scheme. Journal of Cryptology, 2003, 16, 185-215.	2.1	266
113	The Impact of Decryption Failures on the Security of NTRU Encryption. Lecture Notes in Computer Science, 2003, , 226-246.	1.0	70
114	Security proofs for an efficient password-based key exchange. , 2003, , .		111
115	A Simple Public-Key Cryptosystem with a Double Trapdoor Decryption Mechanism and Its Applications. Lecture Notes in Computer Science, 2003, , 37-54.	1.0	191
116	MUTUAL AUTHENTICATION AND GROUP KEY AGREEMENT FOR LOW-POWER MOBILE DEVICES. , 2003, , .		41
117	The Group Diffie-Hellman Problems. Lecture Notes in Computer Science, 2003, , 325-338.	1.0	20
118	Chosen-Ciphertext Security without Redundancy. Lecture Notes in Computer Science, 2003, , 1-18.	1.0	26
119	Dynamic Group Diffie-Hellman Key Exchange under Standard Assumptions. Lecture Notes in Computer Science, 2002, , 321-336.	1.0	140
120	Group Diffie-Hellman Key Exchange Secure against Dictionary Attacks. Lecture Notes in Computer Science, 2002, , 497-514.	1.0	75
121	Optimal Chosen-Ciphertext Secure Encryption of Arbitrary-Length Messages. Lecture Notes in Computer Science, 2002, , 17-33.	1.0	12
122	Analysis and Improvements of NTRU Encryption Paddings. Lecture Notes in Computer Science, 2002, , 210-225.	1.0	25
123	Flaws in Applying Proof Methodologies to Signature Schemes. Lecture Notes in Computer Science, 2002, , 93-110.	1.0	50
124	Practical Security in Public-Key Cryptography. Lecture Notes in Computer Science, 2002, , 1-17.	1.0	2
125	Mutual Authentication for Low-Power Mobile Devices. Lecture Notes in Computer Science, 2002, , 178-195.	1.0	56
126	The Power of RSA Inversion Oracles and the Security of Chaum's RSA-Based Blind Signature Scheme. Lecture Notes in Computer Science, 2002, , 319-338.	1.0	49

#	Article	IF	Citations
127	Monotone Signatures. Lecture Notes in Computer Science, 2002, , 305-318.	1.0	4
128	Practical multi-candidate election system. , 2001, , .		178
129	Provably Authenticated Group Diffie-Hellman Key Exchange â€" The Dynamic Case. Lecture Notes in Computer Science, 2001, , 290-309.	1.0	141
130	Self-Scrambling Anonymizers. Lecture Notes in Computer Science, 2001, , 259-275.	1.0	32
131	Twin signatures. , 2001, , .		25
132	Provably authenticated group Diffie-Hellman key exchange. , 2001, , .		223
133	The Gap-Problems: A New Class of Problems for the Security of Cryptographic Schemes. Lecture Notes in Computer Science, 2001, , 104-118.	1.0	272
134	RSA-OAEP Is Secure under the RSA Assumption. Lecture Notes in Computer Science, 2001, , 260-274.	1.0	116
135	Secure Mobile Gambling. Lecture Notes in Computer Science, 2001, , 110-125.	1.0	4
136	Threshold Cryptosystems Secure against Chosen-Ciphertext Attacks. Lecture Notes in Computer Science, 2001, , 351-368.	1.0	75
137	Key-Privacy in Public-Key Encryption. Lecture Notes in Computer Science, 2001, , 566-582.	1.0	276
138	NUMBER THEORY AND PUBLIC-KEY CRYPTOGRAPHY. , 2001, , .		0
139	Security Arguments for Digital Signatures and Blind Signatures. Journal of Cryptology, 2000, 13, 361-396.	2.1	1,611
140	REACT: Rapid Enhanced-Security Asymmetric Cryptosystem Transform. Lecture Notes in Computer Science, 2000, , 159-174.	1.0	131
141	Extended Notions of Security for Multicast Public Key Cryptosystems. Lecture Notes in Computer Science, 2000, , 499-511.	1.0	37
142	Authenticated Key Exchange Secure against Dictionary Attacks. Lecture Notes in Computer Science, 2000, , 139-155.	1.0	893
143	Chosen-Ciphertext Security for Any One-Way Cryptosystem. Lecture Notes in Computer Science, 2000, , 129-146.	1.0	70
144	Design Validations for Discrete Logarithm Based Signature Schemes. Lecture Notes in Computer Science, 2000, , 276-292.	1.0	55

#	Article	IF	Citations
145	The Composite Discrete Logarithm and Secure Authentication. Lecture Notes in Computer Science, 2000, , 113-128.	1.0	25
146	Efficient Public-Key Cryptosystems Provably Secure Against Active Adversaries. Lecture Notes in Computer Science, 1999, , 165-179.	1.0	96
147	Computational Alternatives to Random Number Generators. Lecture Notes in Computer Science, 1999, , 72-80.	1.0	16
148	Relations among notions of security for public-key encryption schemes. Lecture Notes in Computer Science, 1998, , 26-45.	1.0	514
149	Distributed Trustees and revocability: A framework for internet payment. Lecture Notes in Computer Science, 1998, , 28-42.	1.0	3
150	Strengthened security for blind signatures. Lecture Notes in Computer Science, 1998, , 391-405.	1.0	39
151	New blind signatures equivalent to factorization (extended abstract). , 1997, , .		31
152	Security Proofs for Signature Schemes. Lecture Notes in Computer Science, 1996, , 387-398.	1.0	619
153	Provably secure blind signature schemes. Lecture Notes in Computer Science, 1996, , 252-265.	1.0	126
154	A New Identification Scheme Based on the Perceptrons Problem. Lecture Notes in Computer Science, 1995, , 319-328.	1.0	42