Willy Susilo

List of Publications by Year in Descending Order

Source: https://exaly.com/author-pdf/3143554/willy-susilo-publications-by-year.pdf
Version: 2024-04-25

This document has been generated based on the publications and citations recorded by exaly.com. For the latest version of this publication list, visit the link given above.
The third column is the impact factor (IF) of the journal, and the fourth column is the number of citations of the article.

626	9,561	49	75
papers	citations	h-index	g-index
653	11,445	2.3	6.87
ext. papers	ext. citations	avg, IF	L-index

#	Paper	IF	Citations
626	Tight bound on NewHope failure probability. *IEEE Transactions on Emerging Topics in Computing*, **2022**, 1-1	4.1	
625	Trojan Attacks and Defense for Speech Recognition. *Communications in Computer and Information Science*, **2022**, 195-210	0.3	
624	Chosen-ciphertext lattice-based public key encryption with equality test in standard model. *Theoretical Computer Science*, **2022**, 905, 31-53	1.1	1
623	A model-driven approach to reengineering processes in cloud computing. *Information and Software Technology*, **2022**, 144, 106795	3.4	3
622	Wildcarded identity-based encryption from lattices. *Theoretical Computer Science*, **2022**, 902, 41-53	1.1	0
621	A survey of remote attestation in Internet of Things: Attacks, countermeasures, and prospects. *Computers and Security*, **2022**, 112, 102498	4.9	3
620	Mixed-protocol multi-party computation framework towards complex computation tasks with malicious security. *Computer Standards and Interfaces*, **2022**, 80, 103570	3.5	
619	Generic server-aided secure multi-party computation in cloud computing. *Computer Standards and Interfaces*, **2022**, 79, 103552	3.5	4
618	Efficient maliciously secure two-party mixed-protocol framework for data-driven computation tasks. *Computer Standards and Interfaces*, **2022**, 80, 103571	3.5	
617	ROSE: Robust Searchable Encryption With Forward and Backward Security. *IEEE Transactions on Information Forensics and Security*, **2022**, 17, 1115-1130	8	0
616	Secure and Efficient Communication in VANETs Using Level-Based Access Control. *Wireless Communications and Mobile Computing*, **2022**, 2022, 1-19	1.9	
615	FH-CFI: Fine-grained hardware-assisted control flow integrity for ARM-based IoT devices. *Computers and Security*, **2022**, 116, 102666	4.9	1
614	A fast and flexible attribute-based searchable encryption scheme supporting multi-search mechanism in cloud computing. *Computer Standards and Interfaces*, **2022**, 82, 103635	3.5	3
613	Functional Encryption for Pattern Matching with a Hidden String. *Cryptography*, **2022**, 6, 1	1.9	0
612	Attribute-based Hierarchical Access Control with Extendable Policy. *IEEE Transactions on Information Forensics and Security*, **2022**, 1-1	8	1
611	Optimal Tightness for Chain-Based Unique Signatures. *Lecture Notes in Computer Science*, **2022**, 553-583	0.9	
610	Practical Post-Quantum Signature Schemes from Isomorphism Problems of Trilinear Forms. *Lecture Notes in Computer Science*, **2022**, 582-612	0.9	0

609	Forward-Secure Group Encryptions from Lattices. *Lecture Notes in Computer Science*, **2021**, 610-629	0.9	
608	Lattice-Based Group Encryption with Full Dynamicity and Message Filtering Policy. *Lecture Notes in Computer Science*, **2021**, 156-186	0.9	
607	Puncturable Identity-Based Encryption from Lattices. *Lecture Notes in Computer Science*, **2021**, 571-589	0.9	2
606	Targeted Universal Adversarial Perturbations for Automatic Speech Recognition. *Lecture Notes in Computer Science*, **2021**, 358-373	0.9	1
605	Cryptanalysis of RSA Variants with Primes Sharing Most Significant Bits. *Lecture Notes in Computer Science*, **2021**, 42-53	0.9	1
604	Pattern Matching over Encrypted Data with a Short Ciphertext. *Lecture Notes in Computer Science*, **2021**, 132-143	0.9	
603	Secure Computation of Shared Secrets and Its Applications. *Lecture Notes in Computer Science*, **2021**, 119-131	0.9	
602	Functional signatures: new definition and constructions. *Science China Information Sciences*, **2021**, 64, 1	3.4	0
601	Efficient Unique Ring Signature for Blockchain Privacy Protection. *Lecture Notes in Computer Science*, **2021**, 391-407	0.9	2
600	Broadcast Authenticated Encryption with Keyword Search. *Lecture Notes in Computer Science*, **2021**, 193-213	0.9	3
599	Concise Mercurial Subvector Commitments: Definitions and Constructions. *Lecture Notes in Computer Science*, **2021**, 353-371	0.9	
598	Towards Visualizing and Detecting Audio Adversarial Examples for Automatic Speech Recognition. *Lecture Notes in Computer Science*, **2021**, 531-549	0.9	
597	An Efficient Post-quantum Identity-Based Signature. *Chinese Journal of Electronics*, **2021**, 30, 238-248	0.9	1
596	New proofs of ownership for efficient data deduplication in the adversarial conspiracy model. *International Journal of Intelligent Systems*, **2021**, 36, 2753-2766	8.4	2
595	Security and Privacy for Edge Intelligence in 5G and Beyond Networks: Challenges and Solutions. *IEEE Wireless Communications*, **2021**, 28, 63-69	13.4	8
594	Attribute-based proxy re-signature from standard lattices and its applications. *Computer Standards and Interfaces*, **2021**, 75, 103499	3.5	3
593	Introduction to the Special Section on Artificial Intelligence Security: Adversarial Attack and Defense. *IEEE Transactions on Network Science and Engineering*, **2021**, 8, 905-907	4.9	1
592	P2DPI: Practical and Privacy-Preserving Deep Packet Inspection **2021**,		3

591	Collusion-resistant identity-based Proxy Re-encryption: Lattice-based constructions in Standard Model. *Theoretical Computer Science*, **2021**, 871, 16-29	1.1	5
590	Lattice-based signcryption with equality test in standard model. *Computer Standards and Interfaces*, **2021**, 76, 103515	3.5	3
589	. *IEEE Transactions on Services Computing*, **2021**, 14, 683-694	4.8	
588	Efficient Server-Aided Secure Two-Party Computation in Heterogeneous Mobile Cloud Computing. *IEEE Transactions on Dependable and Secure Computing*, **2021**, 1-1	3.9	3
587	Beating Random Test Case Prioritization. *IEEE Transactions on Reliability*, **2021**, 70, 654-675	4.6	1
586	PPO-DFK: A Privacy-Preserving Optimization of Distributed Fractional Knapsack With Application in Secure Footballer Configurations. *IEEE Systems Journal*, **2021**, 15, 759-770	4.3	11
585	Traceable Monero: Anonymous Cryptocurrency with Enhanced Accountability. *IEEE Transactions on Dependable and Secure Computing*, **2021**, 18, 679-691	3.9	27
584	Ciphertext-policy attribute-based proxy re-encryption via constrained PRFs. *Science China Information Sciences*, **2021**, 64, 1	3.4	2
583	A cloud-aided privacy-preserving multi-dimensional data comparison protocol. *Information Sciences*, **2021**, 545, 739-752	7.7	22
582	Utilizing QR codes to verify the visual fidelity of image datasets for machine learning. *Journal of Network and Computer Applications*, **2021**, 173, 102834	7.9	3
581	Privacy-Preserving Multi-Keyword Searchable Encryption for Distributed Systems. *IEEE Transactions on Parallel and Distributed Systems*, **2021**, 32, 561-574	3.7	15
580	Lightweight Public Key Encryption With Equality Test Supporting Partial Authorization in Cloud Storage. *Computer Journal*, **2021**, 64, 1226-1238	1.3	2
579	Identity-Based Linkable Ring Signatures From Lattices. *IEEE Access*, **2021**, 9, 84739-84755	3.5	1
578	A Secure and Authenticated Mobile Payment Protocol Against Off-site Attack Strategy. *IEEE Transactions on Dependable and Secure Computing*, **2021**, 1-1	3.9	2
577	Robust Authentication Protocol for Dynamic Charging System of Electric Vehicles. *IEEE Transactions on Vehicular Technology*, **2021**, 1-1	6.8	4
576	Bestie: Very Practical Searchable Encryption with Forward and Backward Security. *Lecture Notes in Computer Science*, **2021**, 3-23	0.9	1
575	SyLPEnIoT: Symmetric Lightweight Predicate Encryption for Data Privacy Applications in IoT Environments. *Lecture Notes in Computer Science*, **2021**, 106-126	0.9	
574	Visual Analysis of Adversarial Examples in Machine Learning **2021**, 85-98		

573	Sanitizable Access Control System for Secure Cloud Storage Against Malicious Data Publishers. *IEEE Transactions on Dependable and Secure Computing*, **2021**, 1-1	3.9	3
572	Group Encryption: Full Dynamicity, Message Filtering and Code-Based Instantiation. *Lecture Notes in Computer Science*, **2021**, 678-708	0.9	2
571	. *IEEE Access*, **2021**, 9, 70616-70627	3.5	1
570	Private Set Intersection With Authorization Over Outsourced Encrypted Datasets. *IEEE Transactions on Information Forensics and Security*, **2021**, 16, 4050-4062	8	2
569	Revocable Attribute-Based Encryption with Data Integrity in Clouds. *IEEE Transactions on Dependable and Secure Computing*, **2021**, 1-1	3.9	20
568	Data Security Storage Model of the Internet of Things Based on Blockchain. *Computer Systems Science and Engineering*, **2021**, 36, 213-224	3.9	6
567	Lattice-Based HRA-secure Attribute-Based Proxy Re-Encryption in Standard Model. *Lecture Notes in Computer Science*, **2021**, 169-191	0.9	1
566	A Verifiable and Fair Attribute-based Proxy Re-encryption Scheme for Data Sharing in Clouds. *IEEE Transactions on Dependable and Secure Computing*, **2021**, 1-1	3.9	16
565	Black-Box Audio Adversarial Example Generation Using Variational Autoencoder. *Lecture Notes in Computer Science*, **2021**, 142-160	0.9	1
564	Blockchain based Multi-Authority Fine-Grained Access Control System with Flexible Revocation. *IEEE Transactions on Services Computing*, **2021**, 1-1	4.8	1
563	An efficient multivariate threshold ring signature scheme. *Computer Standards and Interfaces*, **2021**, 74, 103489	3.5	4
562	Divide and capture: An improved cryptanalysis of the encryption standard algorithm RSA. *Computer Standards and Interfaces*, **2021**, 74, 103470	3.5	7
561	Privacy-Preserving Federated Learning in Medical Diagnosis with Homomorphic Re-Encryption. *Computer Standards and Interfaces*, **2021**, 103583	3.5	4
560	A Wiener-type attack on an RSA-like cryptosystem constructed from cubic Pell equations. *Theoretical Computer Science*, **2021**, 885, 125-130	1.1	3
559	Generic construction for tightly-secure signatures from discrete log. *Theoretical Computer Science*, **2021**, 888, 13-21	1.1	0
558	Optimal Verifiable Data Streaming Protocol with Data Auditing. *Lecture Notes in Computer Science*, **2021**, 296-312	0.9	2
557	Software Engineering for Internet of Things. *IEEE Transactions on Software Engineering*, **2021**, 1-1	3.5	4
556	Data Access Control in Cloud Computing: Flexible and Receiver Extendable. *IEEE Transactions on Services Computing*, **2021**, 1-1	4.8	1

555	Password Protected Secret Sharing from Lattices. *Lecture Notes in Computer Science*, **2021**, 442-459	0.9	
554	Blockchain-based secure deduplication and shared auditing in decentralized storage. *IEEE Transactions on Dependable and Secure Computing*, **2021**, 1-1	3.9	6
553	Harnessing Policy Authenticity for Hidden Ciphertext Policy Attribute Based Encryption. *IEEE Transactions on Dependable and Secure Computing*, **2020**, 1-1	3.9	3
552	PKE-MET: Public-Key Encryption with Multi-Ciphertext Equality Test in Cloud Computing. *IEEE Transactions on Cloud Computing*, **2020**, 1-1	3.3	3
551	Aggregatable Certificateless Designated Verifier Signature. *IEEE Access*, **2020**, 8, 95019-95031	3.5	4
550	A New Approach to Keep the Privacy Information of the Signer in a Digital Signature Scheme. *Information (Switzerland)*, **2020**, 11, 260	2.6	
549	A Blockchain-based Self-tallying Voting Protocol in Decentralized IoT. *IEEE Transactions on Dependable and Secure Computing*, **2020**, 1-1	3.9	10
548	On the General Construction of Tightly Secure Identity-Based Signature Schemes. *Computer Journal* , **2020**, 63, 1835-1848	1.3	1
547	A Noise Study of the PSW Signature Family: Patching DRS with Uniform Distribution □ *Information (Switzerland)*, **2020**, 11, 133	2.6	
546	DO-RA: Data-oriented runtime attestation for IoT devices. *Computers and Security*, **2020**, 97, 101945	4.9	5
545	Message-Locked Searchable Encryption: A New Versatile Tool for Secure Cloud Storage. *IEEE Transactions on Services Computing*, **2020**, 1-1	4.8	1
544	Publicly Verifiable Databases with All Efficient Updating Operations. *IEEE Transactions on Knowledge and Data Engineering*, **2020**, 1-1	4.2	8
543	Revocable identity-based encryption with server-aided ciphertext evolution. *Theoretical Computer Science*, **2020**, 815, 11-24	1.1	7
542	Blockchain-based fair payment smart contract for public cloud storage auditing. *Information Sciences*, **2020**, 519, 348-362	7.7	53
541	A Lightweight Privacy-Preserving Fair Meeting Location Determination Scheme. *IEEE Internet of Things Journal*, **2020**, 7, 3083-3093	10.7	14
540	Efficient Post-quantum Identity-based Encryption with Equality Test **2020**,		3
539	QR Code Watermarking for Digital Images. *Lecture Notes in Computer Science*, **2020**, 25-37	0.9	1
538	Efficient Anonymous Multi-group Broadcast Encryption. *Lecture Notes in Computer Science*, **2020**, 251-270	0.9	2

(2020-2020)

537	Trapdoor Delegation and HIBE from Middle-Product LWE in Standard Model. *Lecture Notes in Computer Science*, **2020**, 130-149	0.9	1
536	Chosen-Ciphertext Secure Homomorphic Proxy Re-Encryption. *IEEE Transactions on Cloud Computing*, **2020**, 1-1	3.3	0
535	Puncturable Encryption: A Generic Construction from Delegatable Fully Key-Homomorphic Encryption. *Lecture Notes in Computer Science*, **2020**, 107-127	0.9	5
534	Lattice Blind Signatures with Forward Security. *Lecture Notes in Computer Science*, **2020**, 3-22	0.9	1
533	Possibility and Impossibility Results for Receiver Selective Opening Secure PKE in the Multi-challenge Setting. *Lecture Notes in Computer Science*, **2020**, 191-220	0.9	2
532	Hierarchical Identity-Based Signature in Polynomial Rings. *Computer Journal*, **2020**, 63, 1490-1499	1.3	0
531	Inspecting TLS Anytime Anywhere: A New Approach to TLS Interception **2020**,		4
530	A Blind Ring Signature Based on the Short Integer Solution Problem. *Lecture Notes in Computer Science*, **2020**, 92-111	0.9	3
529	Short Principal Ideal Problem in multicubic fields. *Journal of Mathematical Cryptology*, **2020**, 14, 359-392	0.6	0
528	Efficient Decentralized Random Commitment Key Generation for Mixnet Shuffle Proof. *Lecture Notes in Computer Science*, **2020**, 206-216	0.9	
527	A Lattice-Based Certificateless Public Key Encryption with Equality Test in Standard Model. *Lecture Notes in Computer Science*, **2020**, 50-65	0.9	
526	Provably Secure Group Authentication in the Asynchronous Communication Model. *Lecture Notes in Computer Science*, **2020**, 324-340	0.9	1
525	A New Improved AES S-box with Enhanced Properties. *Lecture Notes in Computer Science*, **2020**, 125-141	0.9	2
524	Secure Cloud Auditing with Efficient Ownership Transfer. *Lecture Notes in Computer Science*, **2020**, 611-631	0.9	2
523	Lattice-Based IBE with Equality Test Supporting Flexible Authorization in the Standard Model. *Lecture Notes in Computer Science*, **2020**, 624-643	0.9	4
522	Identity-Based Unidirectional Proxy Re-encryption in Standard Model: A Lattice-Based Construction. *Lecture Notes in Computer Science*, **2020**, 245-257	0.9	3
521	A generalised bound for the Wiener attack on RSA. *Journal of Information Security and Applications*, **2020**, 53, 102531	3.5	3
520	Robust digital signature revisited. *Theoretical Computer Science*, **2020**, 844, 87-96	1.1	1

519	Leakage-resilient group signature: Definitions and constructions. *Information Sciences*, **2020**, 509, 119-132	7.7	3
518	A Multivariate Blind Ring Signature Scheme. *Computer Journal*, **2020**, 63, 1194-1202	1.3	4
517	Black-Box Accountable Authority Identity-Based Revocation System. *Computer Journal*, **2020**, 63, 525-535	1.3	0
516	Accountable authority identity-based broadcast encryption with constant-size private keys and ciphertexts. *Theoretical Computer Science*, **2020**, 809, 73-87	1.1	4
515	Certificateless aggregate signature scheme secure against fully chosen-key attacks. *Information Sciences*, **2020**, 514, 288-301	7.7	5
514	Blockchain-Based Dynamic Provable Data Possession for Smart Cities. *IEEE Internet of Things Journal*, **2020**, 7, 4143-4154	10.7	26
513	Secure Keyword Search and Data Sharing Mechanism for Cloud Computing. *IEEE Transactions on Dependable and Secure Computing*, **2020**, 1-1	3.9	36
512	A Secure Cloud Data Sharing Protocol for Enterprise Supporting Hierarchical Keyword Search. *IEEE Transactions on Dependable and Secure Computing*, **2020**, 1-1	3.9	4
511	AI-driven data security and privacy. *Journal of Network and Computer Applications*, **2020**, 172, 102842	7.9	2
510	PPO-CPQ: A Privacy-Preserving Optimization of Clinical Pathway Query for E-Healthcare Systems. *IEEE Internet of Things Journal*, **2020**, 7, 10660-10672	10.7	58
509	An Anonymous Authentication System for Pay-As-You-Go Cloud Computing. *IEEE Transactions on Dependable and Secure Computing*, **2020**, 1-1	3.9	2
508	Blockchain-based public auditing and secure deduplication with fair arbitration. *Information Sciences*, **2020**, 541, 409-425	7.7	26
507	Dual Access Control for Cloud-Based Data Storage and Sharing. *IEEE Transactions on Dependable and Secure Computing*, **2020**, 1-1	3.9	16
506	Attribute-Based Cloud Data Integrity Auditing for Secure Outsourced Storage. *IEEE Transactions on Emerging Topics in Computing*, **2020**, 8, 377-390	4.1	37
505	Secure Remote User Authenticated Key Establishment Protocol for Smart Home Environment. *IEEE Transactions on Dependable and Secure Computing*, **2020**, 17, 391-406	3.9	136
504	Interactive three-dimensional visualization of network intrusion detection data for machine learning. *Future Generation Computer Systems*, **2020**, 102, 292-306	7.5	23
503	Concise ID-based mercurial functional commitments and applications to zero-knowledge sets. *International Journal of Information Security*, **2020**, 19, 453-464	2.8	
502	Efficient chameleon hash functions in the enhanced collision resistant model. *Information Sciences*, **2020**, 510, 155-164	7.7	11

501	Cloud-based Outsourcing for Enabling Privacy-Preserving Large-scale Non-Negative Matrix Factorization. *IEEE Transactions on Services Computing*, **2019**, 1-1	4.8	16
500	Universal designated verifier signature scheme with non-delegatability in the standard model. *Information Sciences*, **2019**, 479, 321-334	7.7	8
499	Fine-grained information flow control using attributes. *Information Sciences*, **2019**, 484, 167-182	7.7	7
498	Strongly leakage resilient authenticated key exchange, revisited. *Designs, Codes, and Cryptography*, **2019**, 87, 2885-2911	1.2	5
497	A New Encoding Framework for Predicate Encryption with Non-linear Structures in Prime Order Groups. *Lecture Notes in Computer Science*, **2019**, 406-425	0.9	
496	A Secure and Efficient Data Sharing and Searching Scheme in Wireless Sensor Networks. *Sensors*, **2019**, 19,	3.8	3
495	. *IEEE Access*, **2019**, 7, 25936-25947	3.5	2
494	Efficient Certificateless Signcryption in the Standard Model: Revisiting Luo and Wan□ Scheme from Wireless Personal Communications (2018). *Computer Journal*, **2019**, 62, 1178-1193	1.3	6
493	Practical Multi-Keyword and Boolean Search Over Encrypted E-mail in Cloud Server. *IEEE Transactions on Services Computing*, **2019**, 1-1	4.8	23
492	Certificateless designated verifier signature revisited: achieving a concrete scheme in the standard model. *International Journal of Information Security*, **2019**, 18, 619-635	2.8	9
491	Optimally Efficient Secure Scalar Product With Applications in Cloud Computing. *IEEE Access*, **2019**, 7, 42798-42815	3.5	2
490	Security, Privacy, and Trust for Cyberphysical-Social Systems. *Security and Communication Networks*, **2019**, 2019, 1-2	1.9	
489	Privacy-Preserving Certificateless Cloud Auditing with Multiple Users. *Wireless Personal Communications*, **2019**, 106, 1161-1182	1.9	11
488	Authorized Equality Test on Identity-Based Ciphertexts for Secret Data Sharing via Cloud Storage. *IEEE Access*, **2019**, 7, 25409-25421	3.5	20
487	Subversion in Practice: How to Efficiently Undermine Signatures. *IEEE Access*, **2019**, 7, 68799-68811	3.5	4
486	Multi-designated verifiers signature schemes with threshold verifiability: generic pattern and a concrete scheme in the standard model. *IET Information Security*, **2019**, 13, 459-468	1.4	3
485	The code for securing web applications. *Journal of Information and Optimization Sciences*, **2019**, 40, 905-917	1.1	
484	Identity-Based Broadcast Encryption with Outsourced Partial Decryption for Hybrid Security Models in Edge Computing **2019**,		6

483	Generalized public-key cryptography with tight security. *Information Sciences*, **2019**, 504, 561-577	7.7	2
482	Improving the Security of the DRS Scheme with Uniformly Chosen Random Noise. *Lecture Notes in Computer Science*, **2019**, 119-137	0.9	2
481	A Lattice-Based Public Key Encryption with Equality Test in Standard Model. *Lecture Notes in Computer Science*, **2019**, 138-155	0.9	8
480	Programmable logic controllers based systems (PLC-BS): vulnerabilities and threats. *SN Applied Sciences*, **2019**, 1, 1	1.8	4
479	Accountable identity-based encryption with distributed private key generators. *Information Sciences*, **2019**, 505, 352-366	7.7	2
478	Location Based Encryption. *Lecture Notes in Computer Science*, **2019**, 21-38	0.9	0
477	The Wiener Attack on RSA Revisited: A Quest for the Exact Bound. *Lecture Notes in Computer Science*, **2019**, 381-398	0.9	1
476	Dimensionality Reduction and Visualization of Network Intrusion Detection Data. *Lecture Notes in Computer Science*, **2019**, 441-455	0.9	2
475	RS-HABE: Revocable-Storage and Hierarchical Attribute-Based Access Scheme for Secure Sharing of e-Health Records in Public Cloud. *IEEE Transactions on Dependable and Secure Computing*, **2019**, 1-1	3.9	24
474	Public Key Authenticated Encryption With Designated Equality Test and its Applications in Diagnostic Related Groups. *IEEE Access*, **2019**, 7, 135999-136011	3.5	6
473	Stateful Public-Key Encryption: A Security Solution for Resource-Constrained Environment **2019**, 1-22		3
472	Using Freivalds□Algorithm to Accelerate Lattice-Based Signature Verifications. *Lecture Notes in Computer Science*, **2019**, 401-412	0.9	1
471	Protecting the Visual Fidelity of Machine Learning Datasets Using QR Codes. *Lecture Notes in Computer Science*, **2019**, 320-335	0.9	
470	Puncturable Proxy Re-Encryption Supporting to Group Messaging Service. *Lecture Notes in Computer Science*, **2019**, 215-233	0.9	5
469	Improved Cryptanalysis of the KMOV Elliptic Curve Cryptosystem. *Lecture Notes in Computer Science*, **2019**, 206-221	0.9	0
468	Towards Enhanced Security for Certificateless Public-Key Authenticated Encryption with Keyword Search. *Lecture Notes in Computer Science*, **2019**, 113-129	0.9	7
467	Ciphertext-Delegatable CP-ABE for a Dynamic Credential: A Modular Approach. *Lecture Notes in Computer Science*, **2019**, 3-20	0.9	1
466	Cloud-Based Data-Sharing Scheme Using Verifiable and CCA-Secure Re-encryption from Indistinguishability Obfuscation. *Lecture Notes in Computer Science*, **2019**, 240-259	0.9	

465	Lattice-Based IBE with Equality Test in Standard Model. *Lecture Notes in Computer Science*, **2019**, 19-40	0.9	7
464	Toward Privacy and Regulation in Blockchain-Based Cryptocurrencies. *IEEE Network*, **2019**, 33, 111-117	11.4	73
463	Leakage-resilient ring signature schemes. *Theoretical Computer Science*, **2019**, 759, 1-13	1.1	5
462	A Blind Signature from Module Latices **2019**,		3
461	Enhancing Goldreich, Goldwasser and Halevi□ scheme with intersecting lattices. *Journal of Mathematical Cryptology*, **2019**, 13, 169-196	0.6	
460	Tightly Secure Public-Key Cryptographic Schemes from One-More Assumptions. *Journal of Computer Science and Technology*, **2019**, 34, 1366-1379	1.7	1
459	Identity-based revocation system: Enhanced security model and scalable bounded IBRS construction with short parameters. *Information Sciences*, **2019**, 472, 35-52	7.7	1
458	Designated-server identity-based authenticated encryption with keyword search for encrypted emails. *Information Sciences*, **2019**, 481, 330-343	7.7	43
457	DABKE: Secure deniable attribute-based key exchange framework. *Journal of Computer Security*, **2019**, 27, 259-275	0.8	
456	Threshold privacy-preserving cloud auditing with multiple uploaders. *International Journal of Information Security*, **2019**, 18, 321-331	2.8	3
455	CAPTCHA Design and Security Issues **2019**, 69-92		8
454	Fuzzy Identity-Based Data Integrity Auditing for Reliable Cloud Storage Systems. *IEEE Transactions on Dependable and Secure Computing*, **2019**, 16, 72-83	3.9	109
453	Privacy-preserving Naive Bayes classifiers secure against the substitution-then-comparison attack. *Information Sciences*, **2018**, 444, 72-88	7.7	111
452	A Secure and Efficient Authentication Technique for Vehicular Ad-Hoc Networks. *IEEE Transactions on Vehicular Technology*, **2018**, 67, 5409-5423	6.8	38
451	Witness-based searchable encryption. *Information Sciences*, **2018**, 453, 364-378	7.7	10
450	Multirate DelPHI to secure multirate ad hoc networks against wormhole attacks. *Journal of Information Security and Applications*, **2018**, 39, 31-40	3.5	10
449	A CCA-secure key-policy attribute-based proxy re-encryption in the adaptive corruption model for dropbox data sharing system. *Designs, Codes, and Cryptography*, **2018**, 86, 2587-2603	1.2	33
448	Secure Message Communication Protocol Among Vehicles in Smart City. *IEEE Transactions on Vehicular Technology*, **2018**, 67, 4359-4373	6.8	99

447	. *IEEE Transactions on Industrial Informatics*, **2018**, 14, 3712-3723	11.9	61
446	Anonymous and Traceable Group Data Sharing in Cloud Computing. *IEEE Transactions on Information Forensics and Security*, **2018**, 13, 912-925	8	144
445	Privacy-enhanced attribute-based private information retrieval. *Information Sciences*, **2018**, 454-455, 275-291	7.7	7
444	Ciphertext-policy attribute-based encryption against key-delegation abuse in fog computing. *Future Generation Computer Systems*, **2018**, 78, 720-729	7.5	64
443	Flexible ciphertext-policy attribute-based encryption supporting AND-gate and threshold with short ciphertexts. *International Journal of Information Security*, **2018**, 17, 463-475	2.8	11
442	Functional encryption for computational hiding in prime order groups via pair encodings. *Designs, Codes, and Cryptography*, **2018**, 86, 97-120	1.2	1
441	Criteria-Based Encryption. *Computer Journal*, **2018**, 61, 512-525	1.3	1
440	Man-in-the-middle attacks on Secure Simple Pairing in Bluetooth standard V5.0 and its countermeasure. *Personal and Ubiquitous Computing*, **2018**, 22, 55-67	2.1	29
439	A cost-effective software testing strategy employing online feedback information. *Information Sciences*, **2018**, 422, 318-335	7.7	5
438	Leakage-Resilient Dual-Form Signatures. *Computer Journal*, **2018**, 61, 1216-1227	1.3	1
437	A System Model for Personalized Medication Management (MyMediMan)▯The Consumers▯Point of View. *Information (Switzerland)*, **2018**, 9, 69	2.6	0
436	Cooperative Secret Sharing Using QR Codes and Symmetric Keys. *Symmetry*, **2018**, 10, 95	2.7	12
435	Cryptanalysis of RSA-type cryptosystems based on Lucas sequences, Gaussian integers and elliptic curves. *Journal of Information Security and Applications*, **2018**, 40, 193-198	3.5	8
434	Policy controlled system with anonymity. *Theoretical Computer Science*, **2018**, 745, 87-113	1.1	2
433	Improved Threat Models for the Security of Encrypted and Deniable File Systems. *Lecture Notes in Electrical Engineering*, **2018**, 223-230	0.2	1
432	Constant-size ciphertexts in threshold attribute-based encryption without dummy attributes. *Information Sciences*, **2018**, 429, 349-360	7.7	13
431	A Generic Scheme of plaintext-checkable database encryption. *Information Sciences*, **2018**, 429, 88-101	7.7	12
430	Ciphertext-policy attribute-based encryption supporting access policy update and its extension with preserved attributes. *International Journal of Information Security*, **2018**, 17, 533-548	2.8	14

429	A 3D Approach for the Visualization of Network Intrusion Detection Data **2018**,		2
428	PPFilter: Provider Privacy-aware Encrypted Filtering System. *IEEE Transactions on Services Computing*, **2018**, 1-1	4.8	1
427	A Two-Stage Classifier Approach for Network Intrusion Detection. *Lecture Notes in Computer Science*, **2018**, 329-340	0.9	12
426	. *IEEE Access*, **2018**, 6, 56977-56983	3.5	5
425	PLC Code-Level Vulnerabilities **2018**,		8
424	Introduction to Security Reduction **2018**,		7
423	. *IEEE Transactions on Dependable and Secure Computing*, **2017**, 14, 211-220	3.9	18
422	Online/Offline Provable Data Possession. *IEEE Transactions on Information Forensics and Security*, **2017**, 12, 1182-1194	8	24
421	Securely Reinforcing Synchronization for Embedded Online Contests. *Transactions on Embedded Computing Systems*, **2017**, 16, 1-21	1.8	1
420	An efficient and provably secure RFID grouping proof protocol **2017**,		8
419	An Efficient KP-ABE with Short Ciphertexts in Prime OrderGroups under Standard Assumption **2017** ,		5
418	Cloud computing security and privacy: Standards and regulations. *Computer Standards and Interfaces*, **2017**, 54, 1-2	3.5	16
417	An Efficient Public Auditing Protocol With Novel Dynamic Structure for Cloud Data. *IEEE Transactions on Information Forensics and Security*, **2017**, 12, 2402-2415	8	231
416	A QR Code Watermarking Approach Based on the DWT-DCT Technique. *Lecture Notes in Computer Science*, **2017**, 314-331	0.9	16
415	A general framework for secure sharing of personal health records in cloud system. *Journal of Computer and System Sciences*, **2017**, 90, 46-62	1	45
414	Strong authenticated key exchange with auxiliary inputs. *Designs, Codes, and Cryptography*, **2017**, 85, 145-173	1.2	26
413	Identity-based conditional proxy re-encryption with fine grain policy. *Computer Standards and Interfaces*, **2017**, 52, 1-9	3.5	22
412	A generalized attack on RSA type cryptosystems. *Theoretical Computer Science*, **2017**, 704, 74-81	1.1	12

411	Cooperative Learning in Information Security Education: Teaching Secret Sharing Concepts. *Lecture Notes in Computer Science*, **2017**, 65-72	0.9	
410	Towards Multi-user Searchable Encryption Supporting Boolean Query and Fast Decryption. *Lecture Notes in Computer Science*, **2017**, 24-38	0.9	13
409	An Efficient Key-Policy Attribute-Based Searchable Encryption in Prime-Order Groups. *Lecture Notes in Computer Science*, **2017**, 39-56	0.9	3
408	Fuzzy Extractors for Biometric Identification **2017**,		6
407	A note on the strong authenticated key exchange with auxiliary inputs. *Designs, Codes, and Cryptography*, **2017**, 85, 175-178	1.2	5
406	Privacy-Preserving Mutual Authentication in RFID with Designated Readers. *Wireless Personal Communications*, **2017**, 96, 4819-4845	1.9	4
405	Dirichlet product for boolean functions. *Journal of Applied Mathematics and Computing*, **2017**, 55, 293-312	1.8	
404	. *IEEE Transactions on Information Forensics and Security*, **2017**, 12, 3110-3122	8	14
403	Optimal Security Reductions for Unique Signatures: Bypassing Impossibilities with a Counterexample. *Lecture Notes in Computer Science*, **2017**, 517-547	0.9	8
402	Covert QR Codes: How to Hide in the Crowd. *Lecture Notes in Computer Science*, **2017**, 678-693	0.9	1
401	Sequence aware functional encryption and its application in searchable encryption. *Journal of Information Security and Applications*, **2017**, 35, 106-118	3.5	5
400	Fully privacy-preserving and revocable ID-based broadcast encryption for data access control in smart city. *Personal and Ubiquitous Computing*, **2017**, 21, 855-868	2.1	13
399	Secure and Efficient Cloud Data Deduplication With Randomized Tag. *IEEE Transactions on Information Forensics and Security*, **2017**, 12, 532-543	8	51
398	Policy-controlled signatures and their applications. *Computer Standards and Interfaces*, **2017**, 50, 26-41	3.5	4
397	Publicly verifiable databases with efficient insertion/deletion operations. *Journal of Computer and System Sciences*, **2017**, 86, 49-58	1	15
396	Identity-Based Remote Data Integrity Checking With Perfect Data Privacy Preserving for Cloud Storage. *IEEE Transactions on Information Forensics and Security*, **2017**, 12, 767-778	8	246
395	Obfuscating Re-encryption Algorithm With Flexible and Controllable Multi-Hop on Untrusted Outsourcing Server. *IEEE Access*, **2017**, 5, 26419-26434	3.5	7
394	Dynamic Provable Data Possession Protocols with Public Verifiability and Data Privacy. *Lecture Notes in Computer Science*, **2017**, 485-505	0.9	6

393	Dynamic Searchable Symmetric Encryption with Physical Deletion and Small Leakage. *Lecture Notes in Computer Science*, **2017**, 207-226	0.9	6
392	Mergeable and Revocable Identity-Based Encryption. *Lecture Notes in Computer Science*, **2017**, 147-167	0.9	
391	Defeating Plausible Deniability of VeraCrypt Hidden Operating Systems. *Communications in Computer and Information Science*, **2017**, 3-13	0.3	1
390	Hidden Ciphertext Policy Attribute-Based Encryption Under Standard Assumptions. *IEEE Transactions on Information Forensics and Security*, **2016**, 11, 35-45	8	94
389	Efficient dynamic threshold identity-based encryption with constant-size ciphertext. *Theoretical Computer Science*, **2016**, 609, 49-59	1.1	2
388	Broadcast encryption with dealership. *International Journal of Information Security*, **2016**, 15, 271-283	2.8	7
387	Generalized closest substring encryption. *Designs, Codes, and Cryptography*, **2016**, 80, 103-124	1.2	
386	A short ID-based proxy signature scheme. *International Journal of Communication Systems*, **2016**, 29, 859-873	1.7	9
385	Multi-authority security framework for scalable EHR systems. *International Journal of Medical Engineering and Informatics*, **2016**, 8, 390	0.5	2
384	A Tag Based Encoding: An Efficient Encoding for Predicate Encryption in Prime Order Groups. *Lecture Notes in Computer Science*, **2016**, 3-22	0.9	6
383	Identifying malicious web domains using machine learning techniques with online credibility and performance data **2016**,		14
382	Are the most popular users always trustworthy? The case of Yelp. *Electronic Commerce Research and Applications*, **2016**, 20, 30-41	4.6	12
381	Public Cloud Data Auditing with Practical Key Update and Zero Knowledge Privacy. *Lecture Notes in Computer Science*, **2016**, 389-405	0.9	6
380	Ciphertext-Policy Attribute Based Encryption Supporting Access Policy Update. *Lecture Notes in Computer Science*, **2016**, 39-60	0.9	2
379	ABKS-CSC: attribute-based keyword search with constant-size ciphertexts. *Security and Communication Networks*, **2016**, 9, 5003-5015	1.9	5
378	Anonymous Announcement System (AAS) for Electric Vehicle in VANETs. *Computer Journal*, **2016**,	1.3	1
377	Generally Hybrid Proxy Re-Encryption **2016**,		7
376	Faulty Instantiations of Threshold Ring Signature from Threshold Proof-of-Knowledge Protocol. *Computer Journal*, **2016**, 59, 945-954	1.3	2

375	Metamorphic Testing for Cybersecurity. *Computer*, **2016**, 49, 48-55	1.6	38
374	Recipient Revocable Identity-Based Broadcast Encryption **2016**,		17
373	A Key-Policy Attribute-Based Proxy Re-Encryption Without Random Oracles: Table 1.. *Computer Journal*, **2016**, 59, 970-982	1.3	22
372	SAKE: scalable authenticated key exchange for mobile e-health networks. *Security and Communication Networks*, **2016**, 9, 2754-2765	1.9	3
371	Solutions to the anti-piracy problem in oblivious transfer. *Journal of Computer and System Sciences*, **2016**, 82, 466-476	1	0
370	Logarithmic size ring signatures without random oracles. *IET Information Security*, **2016**, 10, 1-7	1.4	4
369	Comments on Public Integrity Auditing for Dynamic Data Sharing With Multiuser Modification *IEEE Transactions on Information Forensics and Security*, **2016**, 11, 658-659	8	24
368	Strongly Leakage-Resilient Authenticated Key Exchange. *Lecture Notes in Computer Science*, **2016**, 19-36	0.9	19
367	Cloud data integrity checking with an identity-based auditing mechanism from RSA. *Future Generation Computer Systems*, **2016**, 62, 85-91	7.5	77
366	Efficient Privacy-Preserving Charging Station Reservation System for Electric Vehicles. *Computer Journal*, **2016**, 59, 1040-1053	1.3	9
365	Distance-Based Encryption: How to Embed Fuzziness in Biometric-Based Encryption. *IEEE Transactions on Information Forensics and Security*, **2016**, 11, 247-257	8	31
364	. *IEEE Transactions on Computers*, **2016**, 65, 1992-2004	2.5	40
363	RFID Ownership Transfer with Positive Secrecy Capacity Channels. *Sensors*, **2016**, 17,	3.8	3
362	Towards Efficient Fully Randomized Message-Locked Encryption. *Lecture Notes in Computer Science* , **2016**, 361-375	0.9	7
361	Exploiting the Error Correction Mechanism in QR Codes for Secret Sharing. *Lecture Notes in Computer Science*, **2016**, 409-425	0.9	28
360	A New Attack on Three Variants of the RSA Cryptosystem. *Lecture Notes in Computer Science*, **2016**, 258-268	0.9	7
359	Authentication and Transaction Verification Using QR Codes with a Mobile Device. *Lecture Notes in Computer Science*, **2016**, 437-451	0.9	7
358	Privacy-Preserving Cloud Auditing with Multiple Uploaders. *Lecture Notes in Computer Science*, **2016** , 224-237	0.9	9

357	Cryptographic Reverse Firewall via Malleable Smooth Projective Hash Functions. *Lecture Notes in Computer Science*, **2016**, 844-876	0.9	27
356	Iterated Random Oracle: A Universal Approach for Finding Loss in Security Reduction. *Lecture Notes in Computer Science*, **2016**, 745-776	0.9	1
355	Securing Shared Systems. *Lecture Notes in Computer Science*, **2016**, 194-201	0.9	
354	Ciphertext-Policy Attribute-Based Encryption with Key-Delegation Abuse Resistance. *Lecture Notes in Computer Science*, **2016**, 477-494	0.9	1
353	Anonymous Identity-Based Broadcast Encryption with Revocation for File Sharing. *Lecture Notes in Computer Science*, **2016**, 223-239	0.9	20
352	One-Round Strong Oblivious Signature-Based Envelope. *Lecture Notes in Computer Science*, **2016**, 3-20	0.9	2
351	Edit Distance Based Encryption and Its Application. *Lecture Notes in Computer Science*, **2016**, 103-119	0.9	3
350	A semantic web vision for an intelligent community transport service brokering system **2016**,		2
349	Improving Privacy and Security in Decentralized Ciphertext-Policy Attribute-Based Encryption. *IEEE Transactions on Information Forensics and Security*, **2015**, 10, 665-678	8	87
348	Adaptively Secure Identity-Based Broadcast Encryption With a Constant-Sized Ciphertext. *IEEE Transactions on Information Forensics and Security*, **2015**, 10, 679-693	8	44
347	Revisiting Security Against the Arbitrator in Optimistic Fair Exchange. *Computer Journal*, **2015**, 58, 2665-2676	1.3	1
346	Identity-based quotable ring signature. *Information Sciences*, **2015**, 321, 71-89	7.7	6
345	Privacy-preserving encryption scheme using DNA parentage test. *Theoretical Computer Science*, **2015**, 580, 1-13	1.1	1
344	A New Biocryptosystem-Oriented Security Analysis Framework and Implementation of Multibiometric Cryptosystems Based on Decision Level Fusion. *IEEE Transactions on Information Forensics and Security*, **2015**, 10, 1193-1206	8	44
343	Privacy-Preserving Ciphertext Multi-Sharing Control for Big Data Storage. *IEEE Transactions on Information Forensics and Security*, **2015**, 10, 1578-1589	8	59
342	Secure sharing and searching for real-time video data in mobile cloud. *IEEE Network*, **2015**, 29, 46-50	11.4	47
341	Secure Delegation of Signing Power from Factorization. *Computer Journal*, **2015**, 58, 867-877	1.3	1
340	Asymmetric Cross-cryptosystem Re-encryption Applicable to Efficient and Secure Mobile Access to Outsourced Data **2015**,		7

339	Efficient and Fully CCA Secure Conditional Proxy Re-Encryption from Hierarchical Identity-Based Encryption. *Computer Journal*, **2015**, 58, 2778-2792	1.3	11
338	Attribute Based Broadcast Encryption with Short Ciphertext and Decryption Key. *Lecture Notes in Computer Science*, **2015**, 252-269	0.9	11
337	AAC-OT: Accountable Oblivious Transfer With Access Control. *IEEE Transactions on Information Forensics and Security*, **2015**, 10, 2502-2514	8	10
336	Anonymous Yoking-Group Proofs **2015**,		2
335	Provably Secure Identity Based Provable Data Possession. *Lecture Notes in Computer Science*, **2015**, 310-325	0.9	14
334	A Visual One-Time Password Authentication Scheme Using Mobile Devices. *Lecture Notes in Computer Science*, **2015**, 243-257	0.9	4
333	Collusion-resistant convertible ring signature schemes. *Science China Information Sciences*, **2015**, 58, 1-16	5.4	
332	A short identity-based proxy ring signature scheme from RSA. *Computer Standards and Interfaces*, **2015**, 38, 144-151	3.5	5
331	A provably secure identity-based proxy ring signature based on RSA. *Security and Communication Networks*, **2015**, 8, 1223-1236	1.9	3
330	Enhanced privacy of a remote data integrity-checking protocol for secure cloud storage. *International Journal of Information Security*, **2015**, 14, 307-318	2.8	53
329	A secure and efficient Ciphertext-Policy Attribute-Based Proxy Re-Encryption for cloud data sharing. *Future Generation Computer Systems*, **2015**, 52, 95-108	7.5	94
328	Optimistic fair exchange in the enhanced chosen-key model. *Theoretical Computer Science*, **2015**, 562, 57-74	1.1	2
327	Ambiguous optimistic fair exchange: Definition and constructions. *Theoretical Computer Science*, **2015**, 562, 177-193	1.1	4
326	Analysis and Improvement on a Biometric-Based Remote User Authentication Scheme Using Smart Cards. *Wireless Personal Communications*, **2015**, 80, 1747-1760	1.9	27
325	k -Times Attribute-Based Anonymous Access Control for Cloud Computing. *IEEE Transactions on Computers*, **2015**, 64, 2595-2608	2.5	35
324	A ciphertext-policy attribute-based proxy re-encryption scheme for data sharing in public clouds. *Concurrency Computation Practice and Experience*, **2015**, 27, 2004-2027	1.4	17
323	An Identity-Based Multi-Proxy Multi-Signature Scheme Without Bilinear Pairings and its Variants. *Computer Journal*, **2015**, 58, 1021-1039	1.3	3
322	Efficient algorithms for secure outsourcing of bilinear pairings. *Theoretical Computer Science*, **2015**, 562, 112-121	1.1	53

321	LLL for ideal lattices: re-evaluation of the security of Gentry�Halevi� FHE scheme. *Designs, Codes, and Cryptography*, **2015**, 76, 325-344	1.2	8
320	A systematic literature review on security and privacy of electronic health record systems: technical perspectives. *Health Information Management Journal*, **2015**, 44, 23-38	2.6	32
319	Achieving fairness by sequential equilibrium in rational two-party computation under incomplete information. *Security and Communication Networks*, **2015**, 8, 3690-3700	1.9	
318	Vulnerabilities of an ECC-based RFID authentication scheme. *Security and Communication Networks*, **2015**, 8, 3262-3270	1.9	4
317	File sharing in cloud computing using win stay lose shift strategy. *International Journal of High Performance Computing and Networking*, **2015**, 8, 154	1	5
316	Searchable Attribute-Based Mechanism With Efficient Data Sharing for Secure Cloud Storage. *IEEE Transactions on Information Forensics and Security*, **2015**, 10, 1981-1992	8	122
315	Generating Searchable Public-Key Ciphertexts With Hidden Structures for Fast Keyword Search. *IEEE Transactions on Information Forensics and Security*, **2015**, 10, 1993-2006	8	34
314	Shared RFID ownership transfer protocols. *Computer Standards and Interfaces*, **2015**, 42, 95-104	3.5	6
313	How to protect privacy in Optimistic Fair Exchange of digital signatures. *Information Sciences*, **2015**, 325, 300-315	7.7	1
312	Protecting peer-to-peer-based massively multiplayer online games. *International Journal of Computational Science and Engineering*, **2015**, 10, 293	0.4	2
311	A resilient identity-based authenticated key exchange protocol. *Security and Communication Networks*, **2015**, 8, 2279-2290	1.9	7
310	An Efficient Variant of Boneh-Gentry-Hamburg� Identity-Based Encryption Without Pairing. *Lecture Notes in Computer Science*, **2015**, 257-268	0.9	3
309	Improved Identity-Based Online/Offline Encryption. *Lecture Notes in Computer Science*, **2015**, 160-173	0.9	9
308	Efficient Dynamic Provable Data Possession with Public Verifiability and Data Privacy. *Lecture Notes in Computer Science*, **2015**, 395-412	0.9	10
307	Fair Multi-signature. *Lecture Notes in Computer Science*, **2015**, 244-256	0.9	1
306	A New Payment System for Enhancing Location Privacy of Electric Vehicles. *IEEE Transactions on Vehicular Technology*, **2014**, 63, 3-18	6.8	55
305	A robust smart card-based anonymous user authentication protocol for wireless communications. *Security and Communication Networks*, **2014**, 7, 987-993	1.9	22
304	Identity based identification from algebraic coding theory. *Theoretical Computer Science*, **2014**, 520, 51-61	1.1	6

303	Improvements on an authentication scheme for vehicular sensor networks. *Expert Systems With Applications*, **2014**, 41, 2559-2564	7.8	88
302	Subset Membership Encryption and Its Applications to Oblivious Transfer. *IEEE Transactions on Information Forensics and Security*, **2014**, 9, 1098-1107	8	16
301	Security pitfalls of an efficient threshold proxy signature scheme for mobile agents. *Information Processing Letters*, **2014**, 114, 5-8	0.8	2
300	Collusion-Resistance in Optimistic Fair Exchange. *IEEE Transactions on Information Forensics and Security*, **2014**, 9, 1227-1239	8	1
299	. *IEEE Transactions on Computers*, **2014**, 63, 941-953	2.5	6
298	CP-ABE With Constant-Size Keys for Lightweight Devices. *IEEE Transactions on Information Forensics and Security*, **2014**, 9, 763-771	8	98
297	A DFA-Based Functional Proxy Re-Encryption Scheme for Secure Public Cloud Data Sharing. *IEEE Transactions on Information Forensics and Security*, **2014**, 9, 1667-1680	8	61
296	Attribute-based optimistic fair exchange: How to restrict brokers with policies. *Theoretical Computer Science*, **2014**, 527, 83-96	1.1	2
295	Two-Party (Blind) Ring Signatures and Their Applications. *Lecture Notes in Computer Science*, **2014**, 403-417	0.9	
294	On the security of text-based 3D CAPTCHAs. *Computers and Security*, **2014**, 45, 84-99	4.9	15
293	On the security of auditing mechanisms for secure cloud storage. *Future Generation Computer Systems*, **2014**, 30, 127-132	7.5	30
292	Linkable Ring Signature with Unconditional Anonymity. *IEEE Transactions on Knowledge and Data Engineering*, **2014**, 26, 157-165	4.2	49
291	Attribute-Based Data Transfer with Filtering Scheme in Cloud Computing. *Computer Journal*, **2014**, 57, 579-591	1.3	3
290	PPDCP-ABE: Privacy-Preserving Decentralized Ciphertext-Policy Attribute-Based Encryption. *Lecture Notes in Computer Science*, **2014**, 73-90	0.9	22
289	Towards a cryptographic treatment of publish/subscribe systems1. *Journal of Computer Security*, **2014**, 22, 33-67	0.8	6
288	Efficient public key encryption with revocable keyword search. *Security and Communication Networks*, **2014**, 7, 466-472	1.9	23
287	Revisiting Optimistic Fair Exchange Based on Ring Signatures. *IEEE Transactions on Information Forensics and Security*, **2014**, 9, 1883-1892	8	1
286	(Strong) multidesignated verifiers signatures secure against rogue key attack. *Concurrency Computation Practice and Experience*, **2014**, 26, 1574-1592	1.4	3

285	Privacy-Preserving Authorized RFID Authentication Protocols. *Lecture Notes in Computer Science*, **2014**, 108-122	0.9	6
284	Server-Aided Signature Verification for Lightweight Devices. *Computer Journal*, **2014**, 57, 481-493	1.3	4
283	Identity-based chameleon hashing and signatures without key exposure. *Information Sciences*, **2014** , 265, 198-210	7.7	47
282	Deniability and forward secrecy of one-round authenticated key exchange. *Journal of Supercomputing*, **2014**, 67, 671-690	2.5	3
281	Cryptanalysis on Two Certificateless Signature Schemes. *International Journal of Computers, Communications and Control*, **2014**, 5, 586	3.6	4
280	P2OFE: Privacy-Preserving Optimistic Fair Exchange of Digital Signatures. *Lecture Notes in Computer Science*, **2014**, 367-384	0.9	8
279	Efficient Semi-static Secure Broadcast Encryption Scheme. *Lecture Notes in Computer Science*, **2014**, 62-76	0.9	5
278	An Adaptively CCA-Secure Ciphertext-Policy Attribute-Based Proxy Re-Encryption for Cloud Data Sharing. *Lecture Notes in Computer Science*, **2014**, 448-461	0.9	21
277	A CAPTCHA Scheme Based on the Identification of Character Locations. *Lecture Notes in Computer Science*, **2014**, 60-74	0.9	8
276	An Efficient Cloud-Based Revocable Identity-Based Proxy Re-encryption Scheme for Public Clouds Data Sharing. *Lecture Notes in Computer Science*, **2014**, 257-272	0.9	67
275	Efficient Hidden Vector Encryption with Constant-Size Ciphertext. *Lecture Notes in Computer Science*, **2014**, 472-487	0.9	6
274	New Insight to Preserve Online Survey Accuracy and Privacy in Big Data Era. *Lecture Notes in Computer Science*, **2014**, 182-199	0.9	5
273	Jhanwar-Barua□ Identity-Based Encryption Revisited. *Lecture Notes in Computer Science*, **2014**, 271-284	0.9	5
272	Attribute-Based Signature with Message Recovery. *Lecture Notes in Computer Science*, **2014**, 433-447	0.9	1
271	A Secure and Effective Anonymous User Authentication Scheme for Roaming Service in Global Mobility Networks. *Wireless Personal Communications*, **2013**, 73, 993-1004	1.9	66
270	Cryptanalaysis of an EPCC1G2 Standard Compliant Ownership Transfer Scheme. *Wireless Personal Communications*, **2013**, 72, 245-258	1.9	9
269	Fully Homomorphic Encryption Using Hidden Ideal Lattice. *IEEE Transactions on Information Forensics and Security*, **2013**, 8, 2127-2137	8	29
268	Server-aided signatures verification secure against collusion attack. *Information Security Technical Report*, **2013**, 17, 46-57		12

267	Fully secure hidden vector encryption under standard assumptions. *Information Sciences*, **2013**, 232, 188-207	7.7	11
266	Realizing Fully Secure Unrestricted ID-Based Ring Signature in the Standard Model Based on HIBE. *IEEE Transactions on Information Forensics and Security*, **2013**, 8, 1909-1922	8	11
265	Anonymous Single Sign-On Schemes Transformed from Group Signatures **2013**,		3
264	The construction of ambiguous optimistic fair exchange from designated confirmer signature without random oracles. *Information Sciences*, **2013**, 228, 222-238	7.7	8
263	Securing DSR against wormhole attacks in multirate ad hoc networks. *Journal of Network and Computer Applications*, **2013**, 36, 582-592	7.9	35
262	Public key encryption with keyword search secure against keyword guessing attacks without random oracle. *Information Sciences*, **2013**, 238, 221-241	7.7	133
261	Secure ID-based linkable and revocable-iff-linked ring signature with constant-size construction. *Theoretical Computer Science*, **2013**, 469, 1-14	1.1	46
260	Identity-based data storage in cloud computing. *Future Generation Computer Systems*, **2013**, 29, 673-681	7.5	50
259	Secure RFID Ownership Transfer Protocols. *Lecture Notes in Computer Science*, **2013**, 189-203	0.9	0
258	Membership Encryption and Its Applications. *Lecture Notes in Computer Science*, **2013**, 219-234	0.9	9
257	Leakage Resilient Authenticated Key Exchange Secure in the Auxiliary Input Model. *Lecture Notes in Computer Science*, **2013**, 204-217	0.9	13
256	Efficient Linkable and/or Threshold Ring Signature Without Random Oracles. *Computer Journal*, **2013**, 56, 407-421	1.3	31
255	A Ciphertext-Policy Attribute-Based Proxy Re-encryption with Chosen-Ciphertext Security **2013**,		64
254	Privacy-Enhanced Keyword Search in Clouds **2013**,		1
253	Constant-Size Dynamic K-Times Anonymous Authentication. *IEEE Systems Journal*, **2013**, 7, 249-261	4.3	17
252	Identity-Based Mediated RSA Revisited **2013**,		1
251	Lattice Reduction for Modular Knapsack. *Lecture Notes in Computer Science*, **2013**, 275-286	0.9	2
250	Threshold-Oriented Optimistic Fair Exchange. *Lecture Notes in Computer Science*, **2013**, 424-438	0.9	1

249	Fairness in Concurrent Signatures Revisited. *Lecture Notes in Computer Science*, **2013**, 318-329	0.9	2
248	Secure Exchange of Electronic Health Records **2013**, 1059-1079		
247	Identity-Based Multisignature with Message Recovery. *Lecture Notes in Computer Science*, **2013**, 91-104	0.9	
246	Relations among Privacy Notions for Signcryption and Key Invisible Sign-then-Encrypt *Lecture Notes in Computer Science*, **2013**, 187-202	0.9	4
245	Generic Mediated Encryption. *Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering*, **2013**, 154-168	0.2	0
244	Adaptive Precision Floating Point LLL. *Lecture Notes in Computer Science*, **2013**, 104-117	0.9	1
243	Hierarchical conditional proxy re-encryption. *Computer Standards and Interfaces*, **2012**, 34, 380-389	3.5	9
242	Privacy enhanced data outsourcing in the cloud. *Journal of Network and Computer Applications*, **2012**, 35, 1367-1373	7.9	27
241	Strongly secure certificateless short signatures. *Journal of Systems and Software*, **2012**, 85, 1409-1417	3.3	44
240	Provably secure proxy signature scheme from factorization. *Mathematical and Computer Modelling*, **2012**, 55, 1160-1168		15
239	A new efficient optimistic fair exchange protocol without random oracles. *International Journal of Information Security*, **2012**, 11, 53-63	2.8	9
238	Efficient Fair Conditional Payments for Outsourcing Computations. *IEEE Transactions on Information Forensics and Security*, **2012**, 7, 1687-1694	8	85
237	New constructions of OSBE schemes and their applications in oblivious access control. *International Journal of Information Security*, **2012**, 11, 389-401	2.8	1
236	Privacy-Preserving Decentralized Key-Policy Attribute-Based Encryption. *IEEE Transactions on Parallel and Distributed Systems*, **2012**, 23, 2150-2162	3.7	95
235	Chosen-ciphertext secure anonymous conditional proxy re-encryption with keyword search. *Theoretical Computer Science*, **2012**, 462, 39-58	1.1	40
234	Forward Secure Attribute-Based Signatures. *Lecture Notes in Computer Science*, **2012**, 167-177	0.9	6
233	Privacy preserving protocol for service aggregation in cloud computing. *Software - Practice and Experience*, **2012**, 42, 467-483	2.5	
232	Efficient oblivious transfers with access control. *Computers and Mathematics With Applications*, **2012**, 63, 827-837	2.7	5

231	Efficient and secure stored-value cards with leakage resilience. *Computers and Electrical Engineering* , **2012**, 38, 370-380	4.3	
230	Attribute-Based Oblivious Access Control. *Computer Journal*, **2012**, 55, 1202-1215	1.3	14
229	Certificateless Signatures: New Schemes and Security Models. *Computer Journal*, **2012**, 55, 457-474	1.3	63
228	On the Fault-Detection Capabilities of Adaptive Random Test Case Prioritization: Case Studies with Large Test Suites **2012**,		12
227	A Provably Secure Construction of Certificate-Based Encryption from Certificateless Encryption. *Computer Journal*, **2012**, 55, 1157-1168	1.3	11
226	Enhanced STE3D-CAP: A Novel 3D CAPTCHA Family. *Lecture Notes in Computer Science*, **2012**, 170-181	0.9	1
225	Fault Analysis of the KATAN Family of Block Ciphers. *Lecture Notes in Computer Science*, **2012**, 319-336	0.9	4
224	On the CCA-1 Security of Somewhat Homomorphic Encryption over the Integers. *Lecture Notes in Computer Science*, **2012**, 353-368	0.9	8
223	Breaking an Animated CAPTCHA Scheme. *Lecture Notes in Computer Science*, **2012**, 12-29	0.9	11
222	Breaking a 3D-Based CAPTCHA Scheme. *Lecture Notes in Computer Science*, **2012**, 391-405	0.9	7
221	Reaction Attack on Outsourced Computing with Fully Homomorphic Encryption Schemes. *Lecture Notes in Computer Science*, **2012**, 419-436	0.9	6
220	Enhancing Location Privacy for Electric Vehicles (at the Right time). *Lecture Notes in Computer Science*, **2012**, 397-414	0.9	21
219	Identity-Based Traitor Tracing with Short Private Key and Short Ciphertext. *Lecture Notes in Computer Science*, **2012**, 609-626	0.9	9
218	Efficient Escrow-Free Identity-Based Signature. *Lecture Notes in Computer Science*, **2012**, 161-174	0.9	5
217	Perfect Ambiguous Optimistic Fair Exchange. *Lecture Notes in Computer Science*, **2012**, 142-153	0.9	5
216	Enhancing the Perceived Visual Quality of a Size Invariant Visual Cryptography Scheme. *Lecture Notes in Computer Science*, **2012**, 10-21	0.9	10
215	(Strong) Multi-Designated Verifiers Signatures Secure against Rogue Key Attack. *Lecture Notes in Computer Science*, **2012**, 334-347	0.9	4
214	Attacking Animated CAPTCHAs via Character Extraction. *Lecture Notes in Computer Science*, **2012**, 98-113	0.9	3

213	On Capabilities of Hash Domain Extenders to Preserve Enhanced Security Properties. *Lecture Notes in Computer Science*, **2012**, 288-299	0.9	
212	The Construction of Ambiguous Optimistic Fair Exchange from Designated Confirmer Signature without Random Oracles. *Lecture Notes in Computer Science*, **2012**, 120-137	0.9	3
211	A Pre-computable Signature Scheme with Efficient Verification for RFID. *Lecture Notes in Computer Science*, **2012**, 1-16	0.9	
210	Efficient Self-certified Signatures with Batch Verification. *Lecture Notes in Computer Science*, **2012**, 179-194	0.9	
209	Multi-Level Controlled Signature. *Lecture Notes in Computer Science*, **2012**, 96-110	0.9	1
208	Towards Formalizing a Reputation System for Cheating Detection in Peer-to-Peer-Based Massively Multiplayer Online Games. *Lecture Notes in Computer Science*, **2012**, 291-304	0.9	
207	Privacy-Preserved Access Control for Cloud Computing **2011**,		13
206	Repeated Differential Properties of the AES-128 and AES-256 Key Schedules **2011**,		1
205	Distributed Privacy-Preserving Secure Aggregation in Vehicular Communication **2011**,		7
204	Identity-based trapdoor mercurial commitments and applications. *Theoretical Computer Science*, **2011**, 412, 5498-5512	1.1	5
203	Interactive conditional proxy re-encryption with fine grain policy. *Journal of Systems and Software*, **2011**, 84, 2293-2302	3.3	20
202	Optimistic Fair Exchange with Strong Resolution-Ambiguity. *IEEE Journal on Selected Areas in Communications*, **2011**, 29, 1491-1502	14.2	4
201	Preserving Transparency and Accountability in Optimistic Fair Exchange of Digital Signatures. *IEEE Transactions on Information Forensics and Security*, **2011**, 6, 498-512	8	20
200	Efficient Designated Confirmer Signature and DCS-Based Ambiguous Optimistic Fair Exchange. *IEEE Transactions on Information Forensics and Security*, **2011**, 6, 1233-1247	8	9
199	Efficient strong designated verifier signature schemes without random oracle or with non-delegatability. *International Journal of Information Security*, **2011**, 10, 373-385	2.8	30
198	Identity-based strong designated verifier signature revisited. *Journal of Systems and Software*, **2011** , 84, 120-129	3.3	24
197	Improving security of q-SDH based digital signatures. *Journal of Systems and Software*, **2011**, 84, 1783-1790	3.3	1
196	Group-oriented fair exchange of signatures. *Information Sciences*, **2011**, 181, 3267-3283	7.7	14

195	Provably secure server-aided verification signatures. *Computers and Mathematics With Applications*, **2011**, 61, 1705-1723	2.7	18
194	Extended cubes **2011**,		5
193	Self-certified ring signatures **2011**,		2
192	Short Signatures with a Tighter Security Reduction Without Random Oracles. *Computer Journal*, **2011**, 54, 513-524	1.3	2
191	Threshold ring signature without random oracles **2011**,		11
190	On the security of the identity-based encryption based on DHIES from ASIACCS 2010 **2011**,		4
189	Server-aided signatures verification secure against collusion attack **2011**,		5
188	Practical RFID ownership transfer scheme. *Journal of Computer Security*, **2011**, 19, 319-341	0.8	13
187	Improving BDD Cryptosystems in General Lattices. *Lecture Notes in Computer Science*, **2011**, 152-167	0.9	5
186	Efficient Online/Offline Signatures with Computational Leakage Resilience in Online Phase. *Lecture Notes in Computer Science*, **2011**, 455-470	0.9	1
185	AniCAP: An Animated 3D CAPTCHA Scheme Based on Motion Parallax. *Lecture Notes in Computer Science*, **2011**, 255-271	0.9	8
184	Electronic Cash with Anonymous User Suspension. *Lecture Notes in Computer Science*, **2011**, 172-188	0.9	0
183	An Efficient Construction of Time-Selective Convertible Undeniable Signatures. *Lecture Notes in Computer Science*, **2011**, 355-371	0.9	1
182	Secure Exchange of Electronic Health Records **2011**, 1-22		1
181	Concurrent Signatures with Fully Negotiable Binding Control. *Lecture Notes in Computer Science*, **2011**, 170-187	0.9	1
180	CAPTCHA Challenges for Massively Multiplayer Online Games: Mini-game CAPTCHAs **2010**,		5
179	Efficient Trapdoor-Based Client Puzzle Against DoS Attacks **2010**, 229-249		3
178	Constructions of certificate-based signature secure against key replacement attacks*. *Journal of Computer Security*, **2010**, 18, 421-449	0.8	28

177	Functionalities of free and open electronic health record systems. *International Journal of Technology Assessment in Health Care*, **2010**, 26, 382-9	1.8	18
176	Attribute-based signature and its applications **2010**,		137
175	A framework for privacy policy management in service aggregation **2010**,		2
174	Trapdoor security in a searchable public-key encryption scheme with a designated tester. *Journal of Systems and Software*, **2010**, 83, 763-771	3.3	178
173	How to construct identity-based signatures without the key escrow problem. *International Journal of Information Security*, **2010**, 9, 297-311	2.8	20
172	Biometrics for electronic health records. *Journal of Medical Systems*, **2010**, 34, 975-83	5.1	33
171	Certificateless threshold signature scheme from bilinear maps. *Information Sciences*, **2010**, 180, 4714-4728	7.7	22
170	Improvement of Lattice-Based Cryptography Using CRT. *Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering*, **2010**, 275-282	0.2	3
169	On the Security of NOEKEON against Side Channel Cube Attacks. *Lecture Notes in Computer Science* , **2010**, 45-55	0.9	7
168	Further Observations on Optimistic Fair Exchange Protocols in the Multi-user Setting. *Lecture Notes in Computer Science*, **2010**, 124-141	0.9	5
167	Enhanced Security Notions for Dedicated-Key Hash Functions: Definitions and Relationships. *Lecture Notes in Computer Science*, **2010**, 192-211	0.9	6
166	Identity-Based Chameleon Hash Scheme without Key Exposure. *Lecture Notes in Computer Science*, **2010**, 200-215	0.9	10
165	Proof-of-Knowledge of Representation of Committed Value and Its Applications. *Lecture Notes in Computer Science*, **2010**, 352-369	0.9	6
164	Short Generic Transformation to Strongly Unforgeable Signature in the Standard Model. *Lecture Notes in Computer Science*, **2010**, 168-181	0.9	3
163	A Suite of Non-pairing ID-Based Threshold Ring Signature Schemes with Different Levels of Anonymity (Extended Abstract). *Lecture Notes in Computer Science*, **2010**, 166-183	0.9	17
162	A New Construction of Designated Confirmer Signature and Its Application to Optimistic Fair Exchange. *Lecture Notes in Computer Science*, **2010**, 41-61	0.9	7
161	Towards a Cryptographic Treatment of Publish/Subscribe Systems. *Lecture Notes in Computer Science*, **2010**, 201-220	0.9	2
160	STE3D-CAP: Stereoscopic 3D CAPTCHA. *Lecture Notes in Computer Science*, **2010**, 221-240	0.9	9

159	Differential Fault Analysis of LEX. *Lecture Notes in Computer Science*, **2010**, 55-72	0.9	
158	How to Construct Identity-Based Signatures without the Key Escrow Problem. *Lecture Notes in Computer Science*, **2010**, 286-301	0.9	3
157	A Generic Construction of Dynamic Single Sign-on with Strong Security. *Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering*, **2010**, 181-198	0.2	5
156	Recursive Lattice Reduction. *Lecture Notes in Computer Science*, **2010**, 329-344	0.9	2
155	A Secure Channel Free Public Key Encryption with Keyword Search Scheme without Random Oracle. *Lecture Notes in Computer Science*, **2009**, 248-258	0.9	39
154	Short fail-stop signature scheme based on factorization and discrete logarithm assumptions. *Theoretical Computer Science*, **2009**, 410, 736-744	1.1	8
153	Improved searchable public key encryption with designated tester **2009**,		67
152	**2009**,		3
151	Is the Notion of Divisible On-Line/Off-Line Signatures Stronger than On-Line/Off-Line Signatures?. *Lecture Notes in Computer Science*, **2009**, 129-139	0.9	1
150	Secure searchable public key encryption scheme against keyword guessing attacks. *IEICE Electronics Express*, **2009**, 6, 237-243	0.5	77
149	Certificate-Based Signatures: New Definitions and a Generic Construction from Certificateless Signatures. *Lecture Notes in Computer Science*, **2009**, 99-114	0.9	5
148	How to Balance Privacy with Authenticity. *Lecture Notes in Computer Science*, **2009**, 184-201	0.9	1
147	Ranking Attack Graphs with Graph Neural Networks. *Lecture Notes in Computer Science*, **2009**, 345-359	0.9	7
146	Dynamic Universal Accumulators for DDH Groups and Their Application to Attribute-Based Anonymous Credential Systems. *Lecture Notes in Computer Science*, **2009**, 295-308	0.9	49
145	Asymmetric Group Key Agreement. *Lecture Notes in Computer Science*, **2009**, 153-170	0.9	69
144	Broadcast Attacks against Lattice-Based Cryptosystems. *Lecture Notes in Computer Science*, **2009**, 456-472	0.9	8
143	A New Variant of the Cramer-Shoup KEM Secure against Chosen Ciphertext Attack. *Lecture Notes in Computer Science*, **2009**, 143-155	0.9	6
142	New Privacy Results on Synchronized RFID Authentication Protocols against Tag Tracing. *Lecture Notes in Computer Science*, **2009**, 321-336	0.9	14

141	Anonymous Conditional Proxy Re-encryption without Random Oracle. *Lecture Notes in Computer Science*, **2009**, 47-60	0.9	15
140	How to Prove Security of a Signature with a Tighter Security Reduction. *Lecture Notes in Computer Science*, **2009**, 90-103	0.9	3
139	Universal Designated Verifier Signatures with Threshold-Signers. *Lecture Notes in Computer Science*, **2009**, 89-109	0.9	3
138	Identity-Based Identification Scheme Secure against Concurrent-Reset Attacks without Random Oracles. *Lecture Notes in Computer Science*, **2009**, 94-108	0.9	6
137	Online/Offline Ring Signature Scheme. *Lecture Notes in Computer Science*, **2009**, 80-90	0.9	6
136	Security Vulnerability of ID-Based Key Sharing Schemes. *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, **2009**, E92-A, 2641-2643	0.4	
135	Policy-Controlled Signatures. *Lecture Notes in Computer Science*, **2009**, 91-106	0.9	3
134	Analysis of Property-Preservation Capabilities of the ROX and ESh Hash Domain Extenders. *Lecture Notes in Computer Science*, **2009**, 153-170	0.9	3
133	Efficient Non-interactive Range Proof. *Lecture Notes in Computer Science*, **2009**, 138-147	0.9	6
132	Escrowed Deniable Identification Schemes. *Communications in Computer and Information Science*, **2009**, 234-241	0.3	1
131	Publicly Verifiable Privacy-Preserving Group Decryption. *Lecture Notes in Computer Science*, **2009**, 72-83	0.9	6
130	Enhanced Target Collision Resistant Hash Functions Revisited. *Lecture Notes in Computer Science*, **2009**, 327-344	0.9	5
129	Privacy for Private Key in Signatures. *Lecture Notes in Computer Science*, **2009**, 84-95	0.9	1
128	Mobile ad-hoc network key management with certificateless cryptography **2008**,		10
127	Identity-Based On-Line/Off-Line Signcryption **2008**,		14
126	A Generic Construction of Identity-Based Online/Offline Signcryption **2008**,		9
125	Securing wireless mesh networks with ticket-based authentication **2008**,		10
124	Efficient lattice-based signature scheme. *International Journal of Applied Cryptography*, **2008**, 1, 120	0.8	

123	A Provable Secure ID-Based Explicit Authenticated Key Agreement Protocol Without Random Oracles. *Journal of Computer Science and Technology*, **2008**, 23, 832-842	1.7	7
122	Secure universal designated verifier signature without random oracles. *International Journal of Information Security*, **2008**, 7, 171-183	2.8	24
121	Efficient generic on-line/off-line (threshold) signatures without key exposure. *Information Sciences*, **2008**, 178, 4192-4203	7.7	31
120	A Five-Round Algebraic Property of the Advanced Encryption Standard. *Lecture Notes in Computer Science*, **2008**, 316-330	0.9	1
119	Transport Layer Identification of Skype Traffic. *Lecture Notes in Computer Science*, **2008**, 465-481	0.9	0
118	Traceable and Retrievable Identity-Based Encryption. *Lecture Notes in Computer Science*, **2008**, 94-110	0.9	20
117	Public Key Encryption with Keyword Search Revisited. *Lecture Notes in Computer Science*, **2008**, 1249-1259	0.9	185
116	A Digital Signature Scheme Based on CVP □**2008**, 288-307		9
115	Efficient Optimistic Fair Exchange Secure in the Multi-user Setting and Chosen-Key Model without Random Oracles. *Lecture Notes in Computer Science*, **2008**, 106-120	0.9	23
114	Practical Anonymous Divisible E-Cash from Bounded Accumulators. *Lecture Notes in Computer Science*, **2008**, 287-301	0.9	24
113	Constructing Strong KEM from Weak KEM (or How to Revive the KEM/DEM Framework). *Lecture Notes in Computer Science*, **2008**, 358-374	0.9	8
112	Certificate-Based Signature Schemes without Pairings or Random Oracles. *Lecture Notes in Computer Science*, **2008**, 285-297	0.9	27
111	RFID Privacy Models Revisited. *Lecture Notes in Computer Science*, **2008**, 251-266	0.9	31
110	Server-Aided Verification Signatures: Definitions and New Constructions. *Lecture Notes in Computer Science*, **2008**, 141-155	0.9	20
109	Ambiguous Optimistic Fair Exchange. *Lecture Notes in Computer Science*, **2008**, 74-89	0.9	26
108	Sanitizable Signatures Revisited. *Lecture Notes in Computer Science*, **2008**, 80-97	0.9	12
107	Designated Verifier Signature: Definition, Framework and New Constructions. *Lecture Notes in Computer Science*, **2007**, 1191-1200	0.9	18
106	Comparing and debugging firewall rule tables. *IET Information Security*, **2007**, 1, 143	1.4	5

105	Security and access of health research data. *Journal of Medical Systems*, **2007**, 31, 103-7	5.1	15
104	Breaking and Repairing Trapdoor-Free Group Signature Schemes from Asiacrypt□2004. *Journal of Computer Science and Technology*, **2007**, 22, 71-74	1.7	
103	Revocable Ring Signature. *Journal of Computer Science and Technology*, **2007**, 22, 785-794	1.7	37
102	Short Group Signatures Without Random Oracles. *Journal of Computer Science and Technology*, **2007**, 22, 805-821	1.7	
101	Compact sequential aggregate signatures **2007**,		6
100	Securing personal health information access in mobile healthcare environment through short signature schemes. *International Journal of Mobile Communications*, **2007**, 5, 215	1.2	2
99	Efficient Partially Blind Signatures with Provable Security. *Lecture Notes in Computer Science*, **2007**, 1096-1105	0.9	2
98	Certificateless Signature Revisited **2007**, 308-322		115
97	Certificate-Based Signature: Security Model and Efficient Construction. *Lecture Notes in Computer Science*, **2007**, 110-125	0.9	32
96	New constructions of fuzzy identity-based encryption **2007**,		30
95	Cryptanalysis of BGW Broadcast Encryption Schemes for DVD Content Protection. *Lecture Notes in Computer Science*, **2007**, 32-41	0.9	
94	A Generic Construction for Universally-Convertible Undeniable Signatures **2007**, 15-33		1
93	Convertible Undeniable Proxy Signatures: Security Models and Efficient Construction. *Lecture Notes in Computer Science*, **2007**, 16-29	0.9	1
92	(Convertible) Undeniable Signatures Without Random Oracles. *Lecture Notes in Computer Science*, **2007**, 83-97	0.9	9
91	Efficient Authentication Schemes for AODV and DSR **2007**, 367-389		
90	Multi-party Stand-Alone and Setup-Free Verifiably Committed Signatures **2007**, 134-149		11
89	Certificate Based (Linkable) Ring Signature **2007**, 79-92		28
88	Efficient Generic On-Line/Off-Line Signatures Without Key Exposure. *Lecture Notes in Computer Science*, **2007**, 18-30	0.9	43

87	An Adversary Aware and Intrusion Detection Aware Attack Model Ranking Scheme. *Lecture Notes in Computer Science*, **2007**, 65-86	0.9	2
86	Practical Compact E-Cash **2007**, 431-445		19
85	Provably Secure Pairing-Based Convertible Undeniable Signature with Short Signature Length. *Lecture Notes in Computer Science*, **2007**, 367-391	0.9	16
84	Identity-Based Proxy Signature from Pairings. *Lecture Notes in Computer Science*, **2007**, 22-31	0.9	23
83	Achieving Mobility and Anonymity in IP-Based Networks **2007**, 60-79		3
82	New Construction of Group Secret Handshakes Based on Pairings. *Lecture Notes in Computer Science*, **2007**, 16-30	0.9	1
81	Formal Definition and Construction of Nominative Signature. *Lecture Notes in Computer Science*, **2007**, 57-68	0.9	8
80	Provably Secure Identity-Based Undeniable Signatures with Selective and Universal Convertibility. *Lecture Notes in Computer Science*, **2007**, 25-39	0.9	5
79	Securing electronic health records with broadcast encryption schemes. *International Journal of Electronic Healthcare*, **2006**, 2, 175-84	0	6
78	Identity-based anonymous designated ring signatures **2006**,		3
77	Self-organised group key management for ad hoc networks **2006**,		4
76	Designated group credentials **2006**,		4
75	Event-Oriented k-Times Revocable-iff-Linked Group Signatures. *Lecture Notes in Computer Science*, **2006**, 223-234	0.9	12
74	Constant-Size ID-Based Linkable and Revocable-iff-Linked Ring Signature. *Lecture Notes in Computer Science*, **2006**, 364-378	0.9	23
73	Online/Offline Signatures and Multisignatures for AODV and DSR Routing Security. *Lecture Notes in Computer Science*, **2006**, 99-110	0.9	25
72	Efficient ID-Based Authenticated Group Key Agreement from Bilinear Pairings. *Lecture Notes in Computer Science*, **2006**, 521-532	0.9	5
71	Proxy Signature Without Random Oracles. *Lecture Notes in Computer Science*, **2006**, 473-484	0.9	22
70	Ad Hoc Group Signatures. *Lecture Notes in Computer Science*, **2006**, 120-135	0.9	7

69	Short Linkable Ring Signatures Revisited. *Lecture Notes in Computer Science*, **2006**, 101-115	0.9	41
68	Convertible identity-based anonymous designated ring signatures. *International Journal of Security and Networks*, **2006**, 1, 218	0.5	15
67	Information security and privacy of health data. *International Journal of Healthcare Technology and Management*, **2006**, 7, 492	0.3	3
66	Personal health record systems and their security protection. *Journal of Medical Systems*, **2006**, 30, 309-155	5.1	56
65	Authenticated AODV Routing Protocol Using One-Time Signature and Transitive Signature Schemes. *Journal of Networks*, **2006**, 1,		6
64	Zero-Knowledge Proof of Generalized Compact Knapsacks (or A Novel Identification/Signature Scheme). *Lecture Notes in Computer Science*, **2006**, 531-540	0.9	
63	Privately Retrieve Data from Large Databases. *Lecture Notes in Computer Science*, **2006**, 367-378	0.9	
62	Separable Identity-Based Deniable Authentication: Cryptographic Primitive for Fighting Phishing. *Lecture Notes in Computer Science*, **2006**, 68-80	0.9	1
61	X2BT Trusted Reputation System: A Robust Mechanism for P2P Networks. *Lecture Notes in Computer Science*, **2006**, 364-380	0.9	4
60	Short (Identity-Based) Strong Designated Verifier Signature Schemes. *Lecture Notes in Computer Science*, **2006**, 214-225	0.9	15
59	Three-Round Secret Handshakes Based on ElGamal and DSA. *Lecture Notes in Computer Science*, **2006**, 332-342	0.9	13
58	An Efficient Static Blind Ring Signature Scheme. *Lecture Notes in Computer Science*, **2006**, 410-423	0.9	9
57	Efficient Partially Blind Signatures with Provable Security. *Lecture Notes in Computer Science*, **2006**, 345-354	0.9	12
56	Constant-Size Dynamic k-TAA. *Lecture Notes in Computer Science*, **2006**, 111-125	0.9	110
55	Restricted Universal Designated Verifier Signature. *Lecture Notes in Computer Science*, **2006**, 874-882	0.9	10
54	Multi-party Concurrent Signatures. *Lecture Notes in Computer Science*, **2006**, 131-145	0.9	7
53	On the Integration of Public Key Data Encryption and Public Key Encryption with Keyword Search. *Lecture Notes in Computer Science*, **2006**, 217-232	0.9	49
52	Efficient Signcryption Without Random Oracles. *Lecture Notes in Computer Science*, **2006**, 449-458	0.9	3

51	Efficient Provably Secure Restrictive Partially Blind Signatures from Bilinear Pairings. *Lecture Notes in Computer Science*, **2006**, 251-265	0.9	11
50	Ring Signature with Designated Linkability. *Lecture Notes in Computer Science*, **2006**, 104-119	0.9	12
49	Universal Designated Verifier Signature Without Delegatability. *Lecture Notes in Computer Science*, **2006**, 479-498	0.9	17
48	Escrowed Linkability of Ring Signatures and Its Applications. *Lecture Notes in Computer Science*, **2006**, 175-192	0.9	27
47	On the Internal Structure of Alpha-MAC. *Lecture Notes in Computer Science*, **2006**, 271-285	0.9	4
46	A New Signature Scheme Without Random Oracles from Bilinear Pairings. *Lecture Notes in Computer Science*, **2006**, 67-80	0.9	14
45	Compact E-Cash from Bounded Accumulator. *Lecture Notes in Computer Science*, **2006**, 178-195	0.9	19
44	Identity-Based Partial Message Recovery Signatures (or How to Shorten ID-Based Signatures). *Lecture Notes in Computer Science*, **2005**, 45-56	0.9	24
43	Provably secure fail-stop signature schemes based on RSA. *International Journal of Wireless and Mobile Computing*, **2005**, 1, 53	0.4	3
42	Attack on Han et al.□ ID-based confirmer (undeniable) signature at ACM-EC□3. *Applied Mathematics and Computation*, **2005**, 170, 1166-1169	2.7	
41	Efficient Multi-receiver Identity-Based Encryption and Its Application to Broadcast Encryption. *Lecture Notes in Computer Science*, **2005**, 380-397	0.9	77
40	Tripartite Concurrent Signatures. *IFIP Advances in Information and Communication Technology*, **2005**, 425-441	0.9	3
39	Certificateless Public Key Encryption Without Pairing. *Lecture Notes in Computer Science*, **2005**, 134-148	0.9	95
38	On Securing RTP-Based Streaming Content with Firewalls. *Lecture Notes in Computer Science*, **2005**, 304-319	0.9	1
37	Secure AODV Routing Protocol Using One-Time Signature. *Lecture Notes in Computer Science*, **2005**, 288-297	0.9	
36	Token-Controlled Public Key Encryption. *Lecture Notes in Computer Science*, **2005**, 386-397	0.9	9
35	On the Security of Nominative Signatures. *Lecture Notes in Computer Science*, **2005**, 329-335	0.9	14
34	Universal Designated Verifier Signature Proof (or How to Efficiently Prove Knowledge of a Signature). *Lecture Notes in Computer Science*, **2005**, 644-661	0.9	23

33	Security Analysis of Michael: The IEEE 802.11i Message Integrity Code. *Lecture Notes in Computer Science*, **2005**, 423-432	0.9	5
32	A Short Proxy Signature Scheme: Efficient Authentication in the Ubiquitous World. *Lecture Notes in Computer Science*, **2005**, 480-489	0.9	18
31	Identity-Based Universal Designated Verifier Signatures. *Lecture Notes in Computer Science*, **2005**, 825-834	0.9	14
30	Short Designated Verifier Proxy Signature from Pairings. *Lecture Notes in Computer Science*, **2005**, 835-844	0.9	11
29	Efficient Authentication Scheme for Routing in Mobile Ad Hoc Networks. *Lecture Notes in Computer Science*, **2005**, 854-863	0.9	6
28	Short E-Cash. *Lecture Notes in Computer Science*, **2005**, 332-346	0.9	13
27	On the Security of Certificateless Signature Schemes from Asiacrypt 2003. *Lecture Notes in Computer Science*, **2005**, 13-25	0.9	113
26	Generic Construction of (Identity-Based) Perfect Concurrent Signatures. *Lecture Notes in Computer Science*, **2005**, 194-206	0.9	12
25	Identity-Based Authenticated Broadcast Encryption and Distributed Authenticated Encryption. *Lecture Notes in Computer Science*, **2004**, 169-181	0.9	10
24	An Efficient Signature Scheme from Bilinear Pairings and Its Applications. *Lecture Notes in Computer Science*, **2004**, 277-290	0.9	200
23	Identity-Based Strong Designated Verifier Signature Schemes. *Lecture Notes in Computer Science*, **2004**, 313-324	0.9	45
22	Deniable Partial Proxy Signatures. *Lecture Notes in Computer Science*, **2004**, 182-194	0.9	1
21	Non-interactive Deniable Ring Authentication. *Lecture Notes in Computer Science*, **2004**, 386-401	0.9	22
20	Deniable Ring Authentication Revisited. *Lecture Notes in Computer Science*, **2004**, 149-163	0.9	11
19	X2Rep: Enhanced Trust Semantics for the XRep Protocol. *Lecture Notes in Computer Science*, **2004**, 205-219	0.9	11
18	Perfect Concurrent Signature Schemes. *Lecture Notes in Computer Science*, **2004**, 14-26	0.9	22
17	Identity-Based Broadcasting. *Lecture Notes in Computer Science*, **2003**, 177-190	0.9	6
16	An Efficient Fail-Stop Signature Scheme Based on Factorization. *Lecture Notes in Computer Science*, **2003**, 62-74	0.9	3

15	Efficient Verifiably Encrypted Signature and Partially Blind Signature from Bilinear Pairings. *Lecture Notes in Computer Science*, **2003**, 191-204	0.9	62
14	On Classifying Conference Key Distribution Protocols. *Lecture Notes in Computer Science*, **2001**, 51-59	0.9	
13	A General Construction for Fail-Stop Signature using Authentication Codes **2001**, 343-356		2
12	How to Construct Fail-Stop Confirmer Signature Schemes. *Lecture Notes in Computer Science*, **2001**, 435-444	0.9	
11	A New and Efficient Fail-stop Signature Scheme. *Computer Journal*, **2000**, 43, 430-437	1.3	12
10	Key Management for Secure Multicast with Dynamic Controller. *Lecture Notes in Computer Science*, **2000**, 178-190	0.9	2
9	Fail-Stop Signature for Long Messages (Extended Abstract). *Lecture Notes in Computer Science*, **2000**, 165-177	0.9	3
8	Threshold Fail-Stop Signature Schemes Based on Discrete Logarithm and Factorization. *Lecture Notes in Computer Science*, **2000**, 292-307	0.9	2
7	Remark on self-certified group-oriented cryptosystem without combiner. *Electronics Letters*, **1999**, 35, 1539	1.1	3
6	Fail-Stop Threshold Signature Schemes Based on Elliptic Curves. *Lecture Notes in Computer Science*, **1999**, 103-116	0.9	2
5	Secure Exchange of Electronic Health Records1403-1424		
4	Ideals of Largest Weight in Constructions Based on Directed Graphs. *Bulletin of Mathematical Sciences and Applications*,15, 8-16		
3	On delegatability of MDVS schemes. *Journal of Computer Virology and Hacking Techniques*,1	3	
2	Verifiable data streaming with efficient update for intelligent automation systems. *International Journal of Intelligent Systems*,	8.4	2
1	Securing Mobile Data Computing in Healthcare1930-1939		