Rafael Dowsley

List of Publications by Year
in descending order

37 papers	661 citations	687363 13 h-index	677142 22 g-index
37 all docs	37 docs citations	37 times ranked	440 citing authors

#	Article	IF	Citations
1	Fast Privacy-Preserving Text Classification Based on Secure Multiparty Computation. IEEE Transactions on Information Forensics and Security, 2022, 17, 428-442.	6.9	9
2	Privacy-preserving training of tree ensembles over continuous data. Proceedings on Privacy Enhancing Technologies, 2022, 2022, 205-226.	2.8	7
3	High performance logistic regression for privacy-preserving genome analysis. BMC Medical Genomics, 2021, 14, 23.	1.5	24
4	Security, Privacy, and Reliability in Digital Healthcare Systems Using Blockchain. Electronics (Switzerland), 2021, 10, 2034.	3.1	47
5	Information-Theoretically Secure String Commitments Based on Packet Reordering Channels. IEEE Access, 2021, 9, 139928-139945.	4.2	0
6	On the Commitment Capacity of Unfair Noisy Channels. IEEE Transactions on Information Theory, 2020, 66, 3745-3752.	2.4	11
7	On the Composability of Statistically Secure Random Oblivious Transfer. Entropy, 2020, 22, 107.	2.2	2
8	Efficient Composable Oblivious Transfer from CDH in the Global Random Oracle Model. Lecture Notes in Computer Science, 2020, , 462-481.	1.3	4
9	Protecting Privacy of Users in Brain-Computer Interface Applications. IEEE Transactions on Neural Systems and Rehabilitation Engineering, 2019, 27, 1546-1555.	4.9	31
10	Efficient and Private Scoring of Decision Trees, Support Vector Machines and Logistic Regression Models Based on Pre-Computation. IEEE Transactions on Dependable and Secure Computing, 2019, 16, 217-230.	5.4	82
11	Privacy-preserving linear regression for brain-computer interface applications. , 2018, , .		5
12	Privacy-Preserving User Profiling with Facebook Likes. , 2018, , .		5
13	Privacy-Preserving Scoring of Tree Ensembles: A Novel Framework for AI in Healthcare. , 2018, , .		18
14	Commitment and Oblivious Transfer in the Bounded Storage Model With Errors. IEEE Transactions on Information Theory, 2018, 64, 5970-5984.	2.4	2
15	On the Oblivious Transfer Capacity of Generalized Erasure Channels Against Malicious Adversaries: The Case of Low Erasure Probability. IEEE Transactions on Information Theory, 2017, 63, 6819-6826.	2.4	7
16	A survey on design and implementation of protected searchable data in the cloud. Computer Science Review, 2017, 26, 17-30.	15.3	16
17	Unconditionally Secure, Universally Composable Privacy Preserving Linear Algebra. IEEE Transactions on Information Forensics and Security, 2016, 11, 59-73.	6.9	13
18	Efficient Unconditionally Secure Comparison and Privacy Preserving Machine Learning Classification Protocols. Lecture Notes in Computer Science, 2015, , 354-367.	1.3	15

#	Article	IF	Citations
19	Public-Key Encryption Schemes with Bounded CCA Security and Optimal Ciphertext Length Based on the CDH and HDH Assumptions. Computer Journal, 2015, 58, 2738-2746.	2.4	0
20	Fast, Privacy Preserving Linear Regression over Distributed Datasets based on Pre-Distributed Data. , 2015, , .		42
21	Information-theoretically secure oblivious polynomial evaluation in the commodity-based model. International Journal of Information Security, 2015, 14, 73-84.	3.4	26
22	Weakening the Isolation Assumption of Tamper-Proof Hardware Tokens. Lecture Notes in Computer Science, 2015, , 197-213.	1.3	6
23	How Secure is Deterministic Encryption?. Lecture Notes in Computer Science, 2015, , 52-73.	1.3	9
24	Digital Signatures from Strong RSA without Prime Generation. Lecture Notes in Computer Science, 2015, , 217-235.	1.3	5
25	Towards Trusted eHealth Services in the Cloud. , 2015, , .		12
26	Oblivious transfer in the bounded storage model with errors. , 2014, , .		6
27	Universally Composable Oblivious Transfer Based on a Variant of LPN. Lecture Notes in Computer Science, 2014, , 143-158.	1.3	22
28	On the Impossibility of Structure-Preserving Deterministic Primitives. Lecture Notes in Computer Science, 2014, , 713-738.	1.3	5
29	A CCA2 Secure Variant of the McEliece Cryptosystem. IEEE Transactions on Information Theory, 2012, 58, 6672-6680.	2.4	22
30	Oblivious Transfer Based on the McEliece Assumptions. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2012, E95-A, 567-575.	0.3	5
31	Standard Security Does Not Imply Security against Selective-Opening. Lecture Notes in Computer Science, 2012, , 645-662.	1.3	56
32	Achieving Oblivious Transfer Capacity of Generalized Erasure Channels in the Malicious Model. IEEE Transactions on Information Theory, 2011, 57, 5566-5571.	2.4	19
33	Do you know where your cloud files are?. , 2011, , .		52
34	A Two-Party Protocol with Trusted Initializer for Computing the Inner Product. Lecture Notes in Computer Science, 2011, , 337-350.	1.3	15
35	Universally Composable and Statistically Secure Verifiable Secret Sharing Scheme Based on Pre-Distributed Data. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2011, E94-A, 725-734.	0.3	13
36	A CCA2 Secure Public Key Encryption Scheme Based on the McEliece Assumptions in the Standard Model. Lecture Notes in Computer Science, 2009, , 240-251.	1.3	24

#	Article	IF	Citations
37	Oblivious Transfer Based on the McEliece Assumptions. Lecture Notes in Computer Science, 2008, , 107-117.	1.3	24