

# Oliver Kosut

## List of Publications by Year in descending order

Source: <https://exaly.com/author-pdf/9469241/publications.pdf>

Version: 2024-02-01

55  
papers

1,377  
citations

933447

10  
h-index

752698

20  
g-index

55  
all docs

55  
docs citations

55  
times ranked

1281  
citing authors

#	ARTICLE	IF	CITATIONS
1	Grid Topology Identification With Hidden Nodes via Structured Norm Minimization. , 2022, 6, 1244-1249.		5
2	A Second-Order Converse Bound for the Multiple-Access Channel via Wringing Dependence. IEEE Transactions on Information Theory, 2022, 68, 3552-3584.	2.4	3
3	Detection and Localization of Load Redistribution Attacks on Large-scale Systems. Journal of Modern Power Systems and Clean Energy, 2022, 10, 361-370.	5.4	10
4	Three Variants of Differential Privacy: Lossless Conversion and Applications. IEEE Journal on Selected Areas in Information Theory, 2021, 2, 208-222.	2.5	16
5	A Wringing-Based Proof of a Second-Order Converse for the Multiple-Access Channel under Maximal Error Probability. , 2021, , .		1
6	Evaluating Multiple Guesses by an Adversary via a Tunable Loss Function. , 2021, , .		2
7	Every Bit Counts: Second-Order Analysis of Cooperation in the Multiple-Access Channel. , 2021, , .		1
8	\$N-1\$ Reliability Makes It Difficult for False Data Injection Attacks to Cause Physical Consequences. IEEE Transactions on Power Systems, 2021, 36, 3897-3906.	6.5	8
9	Synthetic Time-Series Load Data via Conditional Generative Adversarial Networks. , 2021, , .		7
10	Authentication with Mildly Myopic Adversaries. , 2020, , .		4
11	Capacity Region of the Gaussian Arbitrarily-Varying Broadcast Channel. , 2020, , .		0
12	Maximal $\hat{\epsilon}$ -Leakage and its Properties. , 2020, , .		3
13	Authentication and Partial Message Correction over Adversarial Multiple-Access Channels. , 2020, , .		3
14	A Better Bound Gives a Hundred Rounds: Enhanced Privacy Guarantees via f-Divergences. , 2020, , .		10
15	Detecting load redistribution attacks via support vector models. IET Smart Grid, 2020, 3, 551-560.	2.2	5
16	Vulnerability Assessment of Large-scale Power Systems to False Data Injection Attacks. , 2020, , .		4
17	Tunable Measures for Information Leakage and Applications to Privacy-Utility Tradeoffs. IEEE Transactions on Information Theory, 2019, 65, 8043-8066.	2.4	46
18	List-Decoding Capacity of the Gaussian Arbitrarily-Varying Channel. Entropy, 2019, 21, 575.	2.2	7

#	ARTICLE	IF	CITATIONS
19	Fine Asymptotics for Universal One-to-One Compression of Parametric Sources. IEEE Transactions on Information Theory, 2019, 65, 2442-2458.	2.4	6
20	Corrections to "Fine Asymptotics for Universal One-to-One Compression of Parametric Sources" [Apr 19 2442-2458]. IEEE Transactions on Information Theory, 2019, 65, 4640-4640.	2.4	0
21	Data-Driven Generation of Synthetic Load Datasets Preserving Spatio-Temporal Features. , 2019, , .		10
22	Structured Coding for Authentication in the Presence of a Malicious Adversary. , 2019, , .		5
23	Robustness of Maximal $\hat{I}_{\pm}$ -Leakage to Side Information. , 2019, , .		7
24	Can Predictive Filters Detect Gradually Ramping False Data Injection Attacks Against PMUs?. , 2019, , .		5
25	Strong Converses are Just Edge Removal Properties. IEEE Transactions on Information Theory, 2019, 65, 3315-3339.	2.4	4
26	Can Attackers With Limited Information Exploit Historical Data to Mount Successful False Data Injection Attacks on Power Systems?. IEEE Transactions on Power Systems, 2018, 33, 4775-4786.	6.5	53
27	Unobservable False Data Injection Attacks against PMUs: Feasible Conditions and Multiplicative Attacks. , 2018, , .		9
28	Finite Blocklength and Dispersion Bounds for the Arbitrarily-Varying Channel. , 2018, , .		4
29	Capacity of the Gaussian Arbitrarily-Varying Channel with List Decoding. , 2018, , .		5
30	Variable Packet-Error Coding. IEEE Transactions on Information Theory, 2018, 64, 1530-1547.	2.4	4
31	Dispersion of the discrete arbitrarily-varying channel with limited shared randomness. , 2017, , .		2
32	On information-theoretic privacy with general distortion cost functions. , 2017, , .		16
33	Asymptotics and Non-Asymptotics for Universal Fixed-to-Variable Source Coding. IEEE Transactions on Information Theory, 2017, 63, 3757-3772.	2.4	24
34	Equivalence for Networks With Adversarial State. IEEE Transactions on Information Theory, 2017, 63, 4137-4154.	2.4	4
35	Vulnerability analysis and consequences of false data injection attack on power system state estimation. , 2017, , .		3
36	Fundamental limits of universal variable-to-fixed length coding of parametric sources. , 2017, , .		0

#	ARTICLE	IF	CITATIONS
37	On the fine asymptotics of information theoretic privacy. , 2016, , .		2
38	A new Type Size code for universal one-to-one compression of parametric sources. , 2016, , .		3
39	Decentralized MMSE attacks in electricity grids. , 2016, , .		1
40	Evaluating power system vulnerability to false data injection attacks via scalable optimization. , 2016, , .		11
41	Maximum Distortion Attacks in Electricity Grids. IEEE Transactions on Smart Grid, 2016, 7, 2007-2015.	9.0	22
42	On the relationship between edge removal and strong converses. , 2016, , .		3
43	False data injection attacks on power system state estimation with limited information. , 2016, , .		20
44	Network equivalence for a joint compound-arbitrarily-varying network model. , 2016, , .		4
45	Vulnerability Analysis and Consequences of False Data Injection Attack on Power System State Estimation. IEEE Transactions on Power Systems, 2016, 31, 3864-3872.	6.5	189
46	Sampling From Gaussian Markov Random Fields Using Stationary and Non-Stationary Subgraph Perturbations. IEEE Transactions on Signal Processing, 2015, 63, 576-589.	5.3	4
47	Cyber attacks on AC state estimation: Unobservability and physical consequences. , 2014, , .		38
48	New results on third-order coding rate for universal fixed-to-variable source coding. , 2014, , .		11
49	On the Dispersions of Three Network Information Theory Problems. IEEE Transactions on Information Theory, 2014, 60, 881-903.	2.4	75
50	Polytope Codes Against Adversaries in Networks. IEEE Transactions on Information Theory, 2014, 60, 3308-3344.	2.4	22
51	Universal fixed-to-variable source coding in the finite blocklength regime. , 2013, , .		15
52	Polytope codes for distributed storage in the presence of an active omniscient adversary. , 2013, , .		8
53	Sampling from Gaussian graphical models using subgraph perturbations. , 2013, , .		3
54	Malicious Data Attacks on the Smart Grid. IEEE Transactions on Smart Grid, 2011, 2, 645-658.	9.0	637

#	ARTICLE	IF	CITATIONS
55	Distributed Source Coding in the Presence of Byzantine Sensors. IEEE Transactions on Information Theory, 2008, 54, 2550-2565.	2.4	13