# Yehuda Lindell

List of Publications by Year
in descending order

Source: https://exaly.com/author-pdf/6308326/publications.pdf

Version: 2024-02-01

| 117 | 7,202 | 94381 | 95218 |
|---|---|---|---|
| papers | citations | 37 h-index | 68 g-index |

| 125 | 125 | 125 | 2105 |
|---|---|---|---|
| all docs | docs citations | times ranked | citing authors |

| # | Article | IF | Citations |
|---|---|---|---|
| 1 | Introduction to Modern Cryptography. , 0, , . | | 497 |
| 2 | Privacy Preserving Data Mining. Journal of Cryptology, 2002, 15, 177-206. | 2.1 | 492 |
| 3 | A Proof of Security of Yaoâ€™s Protocol for Two-Party Computation. Journal of Cryptology, 2009, 22, 161-188. | 2.1 | 472 |
| 4 | Universally composable two-party and multi-party secure computation. , 2002, , . | | 334 |
| 5 | An Efficient Protocol for Secure Two-Party Computation in the Presence of Malicious Adversaries. Lecture Notes in Computer Science, 2007, , 52-78. | 1.0 | 260 |
| 6 | More efficient oblivious transfer and extensions for faster secure computation. , 2013, , . | | 231 |
| 7 | High-Throughput Semi-Honest Secure Three-Party Computation with an Honest Majority. , 2016, , . | | 217 |
| 8 | Efficient Secure Two-Party Protocols. Information Security and Cryptography, 2010, , . | 0.2 | 179 |
| 9 | Universally Composable Password-Based Key Exchange. Lecture Notes in Computer Science, 2005, , 404-421. | 1.0 | 169 |
| 10 | Efficient Protocols for Set Intersection and Pattern Matching with Security Against Malicious and Covert Adversaries. , 2008, , 155-175. | | 156 |
| 11 | Session-Key Generation Using Human Passwords Only. Lecture Notes in Computer Science, 2001, , 408-432. | 1.0 | 136 |
| 12 | How to Simulate It â€“ A Tutorial on the Simulation Proof Technique. Information Security and Cryptography, 2017, , 277-346. | 0.2 | 125 |
| 13 | Security Against Covert Adversaries: Efficient Protocols for Realistic Adversaries. , 2007, , 137-156. | | 121 |
| 14 | Security Against Covert Adversaries: Efficient Protocols for Realistic Adversaries. Journal of Cryptology, 2010, 23, 281-343. | 2.1 | 115 |
| 15 | Secure Two-Party Computation via Cut-and-Choose Oblivious Transfer. Lecture Notes in Computer Science, 2011, , 329-346. | 1.0 | 103 |
| 16 | Secure Computation on the Web: Computing without Simultaneous Interaction. Lecture Notes in Computer Science, 2011, , 132-150. | 1.0 | 95 |
| 17 | A Statistical Theory for Quantitative Association Rules. Journal of Intelligent Information Systems, 2003, 20, 255-283. | 2.8 | 91 |
| 18 | Fast Secure Multiparty ECDSA with Practical Distributed Key Generation and Applications to Cryptocurrency Custody. , 2018, , . | | 90 |

| # | Article | IF | Citations |
|---|---|---|---|
| 19 | Fast Secure Two-Party ECDSA Signing. Lecture Notes in Computer Science, 2017, , 613-644. | 1.0 | 89 |
| 20 | Fast Large-Scale Honest-Majority MPC for Malicious Adversaries. Lecture Notes in Computer Science, 2018, , 34-64. | 1.0 | 87 |
| 21 | Fast Cut-and-Choose Based Protocols for Malicious and Covert Adversaries. Lecture Notes in Computer Science, 2013, , 1-17. | 1.0 | 85 |
| 22 | High-Throughput Secure Three-Party Computation for Malicious Adversaries and an Honest Majority. Lecture Notes in Computer Science, 2017, , 225-255. | 1.0 | 84 |
| 23 | Secure Multi-Party Computation without Agreement. Journal of Cryptology, 2005, 18, 247-287. | 2.1 | 82 |
| 24 | Implementing Two-Party Computation Efficiently with Security Against Malicious Adversaries. Lecture Notes in Computer Science, 2008, , 2-20. | 1.0 | 82 |
| 25 | Optimized Honest-Majority MPC for Malicious Adversaries â€" Breaking the 1 Billion-Gate Per Second Barrier. , 2017, , . | | 77 |
| 26 | On the Limitations of Universally Composable Two-Party Computation without Set-up Assumptions. Lecture Notes in Computer Science, 2003, , 68-86. | 1.0 | 74 |
| 27 | Secure Two-Party Computation via Cut-and-Choose Oblivious Transfer. Journal of Cryptology, 2012, 25, 680-722. | 2.1 | 71 |
| 28 | A framework for password-based authenticated key exchange 1. ACM Transactions on Information and System Security, 2006, 9, 181-234. | 4.5 | 70 |
| 29 | Efficient Constant Round Multi-party Computation Combining BMR and SPDZ. Lecture Notes in Computer Science, 2015, , 319-338. | 1.0 | 69 |
| 30 | Secure multiparty computation. Communications of the ACM, 2021, 64, 86-96. | 3.3 | 69 |
| 31 | Secure Computation Without Authentication. Lecture Notes in Computer Science, 2005, , 361-377. | 1.0 | 65 |
| 32 | On the Limitations of Universally Composable Two-Party Computation Without Set-Up Assumptions. Journal of Cryptology, 2006, 19, 135-167. | 2.1 | 63 |
| 33 | Complete fairness in secure two-party computation. , 2008, , . | | 58 |
| 34 | Lower Bounds for Concurrent Self Composition. Lecture Notes in Computer Science, 2004, , 203-222. | 1.0 | 58 |
| 35 | A Framework for Constructing Fast MPC over Arithmetic Circuits with Malicious Adversaries and an Honest-Majority. , 2017, , . | | 57 |
| 36 | From Keys to Databasesâ€"Real-World Applications of Secure Multi-Party Computation. Computer Journal, 0, , . | 1.5 | 57 |

| # | Article | IF | Citations |
|---|---|---|---|
| 37 | More Efficient Oblivious Transfer Extensions with Security for Malicious Adversaries. Lecture Notes in Computer Science, 2015, , 673-701. | 1.0 | 56 |
| 38 | Highly-Efficient Universally-Composable Commitments Based on the DDH Assumption. Lecture Notes in Computer Science, 2011, , 446-466. | 1.0 | 55 |
| 39 | Bounded-concurrent secure two-party computation without setup assumptions. , 2003, , . | | 54 |
| 40 | Efficient Protocols for Set Intersection and Pattern Matching with Security Against Malicious and Covert Adversaries. Journal of Cryptology, 2010, 23, 422-456. | 2.1 | 54 |
| 41 | Optimizing Semi-Honest Secure Multiparty Computation for the Internet. , 2016, , . | | 52 |
| 42 | Secure Computation without Agreement. Lecture Notes in Computer Science, 2002, , 17-32. | 1.0 | 50 |
| 43 | GCM-SIV. , 2015, , . | | 48 |
| 44 | A Full Proof of the BGW Protocol for Perfectly Secure Multiparty Computation. Journal of Cryptology, 2017, 30, 58-151. | 2.1 | 48 |
| 45 | Complete Fairness in Secure Two-Party Computation. Journal of the ACM, 2011, 58, 1-37. | 1.8 | 46 |
| 46 | A Simpler Variant of Universally Composable Security for Standard Multiparty Computation. Lecture Notes in Computer Science, 2015, , 3-22. | 1.0 | 46 |
| 47 | Information-Theoretically Secure Protocols and Security under Composition. SIAM Journal on Computing, 2010, 39, 2090-2112. | 0.8 | 45 |
| 48 | Cut-and-Choose Yao-Based Secure Computation in the Online/Offline and Batch Settings. Lecture Notes in Computer Science, 2014, , 476-494. | 1.0 | 45 |
| 49 | Blazing Fast 2PC in the Offline/Online Setting with Security for Malicious Adversaries. , 2015, , . | | 44 |
| 50 | Information-theoretically secure protocols and security under composition. , 2006, , . | | 43 |
| 51 | Strict polynomial-time in simulation and extraction. , 2002, , . | | 41 |
| 52 | Fast Garbling of Circuits Under Standard Assumptions. , 2015, , . | | 41 |
| 53 | Fast Cut-and-Choose-Based Protocols for Malicious and Covert Adversaries. Journal of Cryptology, 2016, 29, 456-490. | 2.1 | 41 |
| 54 | A Simpler Construction of CCA2-Secure Public-Key Encryption under General Assumptions. Journal of Cryptology, 2006, 19, 359-377. | 2.1 | 40 |

| # | Article | IF | Citations |
|---|---|---|---|
| 55 | Session-Key Generation Using Human Passwords Only. Journal of Cryptology, 2006, 19, 241-340. | 2.1 | 40 |
| 56 | Constructions of truly practical secure protocols using standardsmartcards. , 2008, , . | | 39 |
| 57 | An Efficient Transform from Sigma Protocols to NIZK with a CRS and Non-programmable Random Oracle. Lecture Notes in Computer Science, 2015, , 93-109. | 1.0 | 39 |
| 58 | Lower bounds for non-black-box zero knowledge. Journal of Computer and System Sciences, 2006, 72, 321-391. | 0.9 | 36 |
| 59 | Utility Dependence in Correct and Fair Rational SecretÂSharing. Journal of Cryptology, 2011, 24, 157-202. | 2.1 | 35 |
| 60 | Concurrently-Secure Blind Signatures Without Random Oracles or Setup Assumptions. , 2007, , 323-341. | | 35 |
| 61 | 1/p-Secure Multiparty Computation without Honest Majority and the Best of Both Worlds. Lecture Notes in Computer Science, 2011, , 277-296. | 1.0 | 35 |
| 62 | Black-Box Constructions of Protocols for Secure Computation. SIAM Journal on Computing, 2011, 40, 225-266. | 0.8 | 34 |
| 63 | More Efficient Constant-Round Multi-party Computation from BMR and SHE. Lecture Notes in Computer Science, 2016, , 554-581. | 1.0 | 34 |
| 64 | More Efficient Oblivious Transfer Extensions. Journal of Cryptology, 2017, 30, 805-858. | 2.1 | 31 |
| 65 | On the Black-Box Complexity of Optimally-Fair Coin Tossing. Lecture Notes in Computer Science, 2011, , 450-467. | 1.0 | 31 |
| 66 | The IPS Compiler: Optimizations, Variants and Concrete Efficiency. Lecture Notes in Computer Science, 2011, , 259-276. | 1.0 | 31 |
| 67 | On Combining Privacy with Guaranteed Output Delivery in Secure Multiparty Computation. Lecture Notes in Computer Science, 2006, , 483-500. | 1.0 | 30 |
| 68 | Privacy-Preserving Search of Similar Patients in Genomic Data. Proceedings on Privacy Enhancing Technologies, 2018, 2018, 104-124. | 2.3 | 29 |
| 69 | Strict Polynomial-Time in Simulation and Extraction. SIAM Journal on Computing, 2004, 33, 783-818. | 0.8 | 28 |
| 70 | Utility Dependence in Correct and Fair Rational Secret Sharing. Lecture Notes in Computer Science, 2009, , 559-576. | 1.0 | 27 |
| 71 | Fairness versus Guaranteed Output Delivery in Secure Multiparty Computation. Lecture Notes in Computer Science, 2014, , 466-485. | 1.0 | 27 |
| 72 | Concurrent general composition of secure protocols in the timing model. , 2005, , . | | 25 |

| # | Article | IF | Citations |
|---|---|---|---|
| 73 | Fast Distributed RSA Key Generation forÂSemi-honest and Malicious Adversaries. Lecture Notes in Computer Science, 2018, , 331-361. | 1.0 | 25 |
| 74 | Fairness Versus Guaranteed Output Delivery in Secure Multiparty Computation. Journal of Cryptology, 2017, 30, 1157-1186. | 2.1 | 24 |
| 75 | Generalizing the SPDZ Compiler For Other Protocols. , 2018, , . | | 24 |
| 76 | Private Web Search with Malicious Adversaries. Lecture Notes in Computer Science, 2010, , 220-235. | 1.0 | 24 |
| 77 | Lower Bounds and Impossibility Results forÂConcurrent Self Composition. Journal of Cryptology, 2008, 21, 200-249. | 2.1 | 23 |
| 78 | On Achieving the â€œBest of Both Worldsâ€•in Secure Multiparty Computation. SIAM Journal on Computing, 2011, 40, 122-141. | 0.8 | 23 |
| 79 | Collusion-Free Multiparty Computation in the Mediated Model. Lecture Notes in Computer Science, 2009, , 524-540. | 1.0 | 23 |
| 80 | An Efficient Protocol for Secure Two-Party Computation in the Presence of Malicious Adversaries. Journal of Cryptology, 2015, 28, 312-350. | 2.1 | 21 |
| 81 | Fair and Efficient Secure Multiparty Computation with Reputation Systems. Lecture Notes in Computer Science, 2013, , 201-220. | 1.0 | 21 |
| 82 | General Composition and Universal Composability inÂSecure Multiparty Computation. Journal of Cryptology, 2009, 22, 395-428. | 2.1 | 20 |
| 83 | An End-to-End System for Large Scale P2P MPC-as-a-Service and Low-Bandwidth MPC for Weak Participants. , 2018, , . | | 20 |
| 84 | Two-Thirds Honest-Majority MPC for Malicious Adversaries at Almost the Cost of Semi-Honest. , 2019, , . | | 20 |
| 85 | A Full Characterization of Functions that Imply Fair Coin Tossing and Ramifications to Fairness. Lecture Notes in Computer Science, 2013, , 243-262. | 1.0 | 18 |
| 86 | Efficient Scalable Constant-Round MPC via Garbled Circuits. Lecture Notes in Computer Science, 2017, , 471-498. | 1.0 | 17 |
| 87 | Concurrent Composition of Secure Protocols in the Timing Model. Journal of Cryptology, 2007, 20, 431-492. | 2.1 | 16 |
| 88 | On the composition of authenticated Byzantine Agreement. Journal of the ACM, 2006, 53, 881-917. | 1.8 | 15 |
| 89 | Fast Garbling of Circuits Under Standard Assumptions. Journal of Cryptology, 2018, 31, 798-844. | 2.1 | 15 |
| 90 | Adaptive Zero-Knowledge Proofs and Adaptively Secure Oblivious Transfer. Journal of Cryptology, 2011, 24, 761-799. | 2.1 | 14 |

| # | Article | IF | Citations |
|---|---|---|---|
| 91 | Better Bounds for Block Cipher Modes of Operation via Nonce-Based Key Derivation. , 2017, , . | | 14 |
| 92 | On the Feasibility of Extending Oblivious Transfer. Lecture Notes in Computer Science, 2013, , 519-538. | 1.0 | 14 |
| 93 | Hiding the Input-Size in Secure Two-Party Computation. Lecture Notes in Computer Science, 2013, , 421-440. | 1.0 | 14 |
| 94 | Impossibility Results for Universal Composability inÂPublic-Key Models and with Fixed Inputs. Journal of Cryptology, 2011, 24, 517-544. | 2.1 | 13 |
| 95 | Secure Computation Without Authentication. Journal of Cryptology, 2011, 24, 720-760. | 2.1 | 12 |
| 96 | Attribute-based Key Exchange with General Policies. , 2016, , . | | 12 |
| 97 | Efficient Constant-Round Multi-party Computation Combining BMR and SPDZ. Journal of Cryptology, 2019, 32, 1026-1069. | 2.1 | 12 |
| 98 | Handling Expected Polynomial-Time Strategies in Simulation-Based Security Proofs. Lecture Notes in Computer Science, 2005, , 128-149. | 1.0 | 12 |
| 99 | Perfectly-Secure Multiplication for Any tâ€‰<â€‰n/3. Lecture Notes in Computer Science, 2011, , 240-258. | 1.0 | 11 |
| 100 | A Note on Constant-Round Zero-Knowledge Proofs of Knowledge. Journal of Cryptology, 2013, 26, 638-654. | 2.1 | 11 |
| 101 | Adaptive Zero-Knowledge Proofs and Adaptively Secure Oblivious Transfer. Lecture Notes in Computer Science, 2009, , 183-201. | 1.0 | 11 |
| 102 | Adding Distributed Decryption and Key Generation to a Ring-LWE Based CCA Encryption Scheme. Lecture Notes in Computer Science, 2019, , 192-210. | 1.0 | 9 |
| 103 | Adaptively Secure Computation with Partial Erasures. , 2015, , . | | 8 |
| 104 | Handling Expected Polynomial-Time Strategies inÂSimulation-Based Security Proofs. Journal of Cryptology, 2008, 21, 303-349. | 2.1 | 7 |
| 105 | Malicious Adversaries. Information Security and Cryptography, 2010, , 81-108. | 0.2 | 6 |
| 106 | Fast Secure Two-Party ECDSA Signing. Journal of Cryptology, 2021, 34, 1. | 2.1 | 5 |
| 107 | Completeness for Symmetric Two-Party Functionalities - Revisited. Lecture Notes in Computer Science, 2012, , 116-133. | 1.0 | 5 |
| 108 | Secure Two-Party Computation with Fairness - A Necessary Design Principle. Lecture Notes in Computer Science, 2017, , 565-580. | 1.0 | 4 |

| # | Article | IF | Citations |
|---|---|---|---|
| 109 | Sigma Protocols and Efficient Zero-Knowledge1. Information Security and Cryptography, 2010, , 147-175. | 0.2 | 4 |
| 110 | $${varvec{1/p}}$$-Secure Multiparty Computation without an Honest Majority and the Best of Both Worlds. Journal of Cryptology, 2020, 33, 1659-1731. | 2.1 | 3 |
| 111 | Semi-honest Adversaries. Information Security and Cryptography, 2010, , 53-80. | 0.2 | 2 |
| 112 | Fast Garbling of Circuits over 3-ValuedÂLogic. Lecture Notes in Computer Science, 2018, , 620-643. | 1.0 | 2 |
| 113 | On the Feasibility of Extending Oblivious Transfer. Journal of Cryptology, 2018, 31, 737-773. | 2.1 | 1 |
| 114 | Completeness for Symmetric Two-Party Functionalities: Revisited. Journal of Cryptology, 2018, 31, 671-697. | 2.1 | 1 |
| 115 | Handling Expected Polynomial-Time Strategies in Simulation-Based Security Proofs*. SSRN Electronic Journal, 0, , . | 0.4 | 0 |
| 116 | Oblivious Transfer and Applications. Information Security and Cryptography, 2010, , 177-212. | 0.2 | 0 |
| 117 | The kth-Ranked Element. Information Security and Cryptography, 2010, , 213-226. | 0.2 | 0 |