Shay Gueron

List of Publications by Year
in descending order

Source: https://exaly.com/author-pdf/6772039/publications.pdf

Version: 2024-02-01

117 papers	2,609 citations	304743 22 h-index	223800 46 g-index
124 all docs	124 docs citations	124 times ranked	1741 citing authors

#	Article	IF	Citations
1	The Dynamics of Herds: From Individuals to Aggregations. Journal of Theoretical Biology, 1996, 182, 85-98.	1.7	269
2	Cilia internal mechanism and metachronal coordination as the result of hydrodynamical coupling. Proceedings of the National Academy of Sciences of the United States of America, 1997, 94, 6001-6006.	7.1	191
3	Energetic considerations of ciliary beating and the advantage of metachronal coordination. Proceedings of the National Academy of Sciences of the United States of America, 1999, 96, 12240-12245.	7.1	189
4	Dopamine modulation of two subthreshold currents produces phase shifts in activity of an identified motoneuron. Journal of Neurophysiology, 1995, 74, 1404-1420.	1.8	165
5	The dynamics of group formation. Mathematical Biosciences, 1995, 128, 243-264.	1.9	127
6	Ciliary motion modeling, and dynamic multicilia interactions. Biophysical Journal, 1992, 63, 1045-1058.	0.5	109
7	53 Gbps Native ${m GF}(2 ^{4}) ^{2}$ Composite-Field AES-Encrypt/Decrypt Accelerator for Content-Protection in 45 nm High-Performance Microprocessors. IEEE Journal of Solid-State Circuits, 2011, 46, 767-776.	5.4	103
8	Computation of the Internal Forces in Cilia: Application to Ciliary Motion, the Effects of Viscosity, and Cilia Interactions. Biophysical Journal, 1998, 74, 1658-1676.	0.5	83
9	Self-organization of Front Patterns in Large Wildebeest Herds. Journal of Theoretical Biology, 1993, 165, 541-552.	1.7	73
10	Simulations of three-dimensional ciliary beats and cilia interactions. Biophysical Journal, 1993, 65, 499-507.	0.5	66
11	SHA-512/256. , 2011, , .		60
12	Intelâ€™s New AES Instructions for Enhanced Performance and Security. Lecture Notes in Computer Science, 2009, , 51-66.	1.3	59
13	The Equilibrium Behavior of Reversible Coagulation-Fragmentation Processes. Journal of Theoretical Probability, 1999, 12, 447-474.	0.8	56
14	Memory Encryption for General-Purpose Processors. IEEE Security and Privacy, 2016, 14, 54-62.	1.2	51
15	GCM-SIV. , 2015, , .		48
16	Fast prime field elliptic-curve cryptography with 256-bit primes. Journal of Cryptographic Engineering, 2015, 5, 141-151.	1.8	46
17	New Branch Prediction Vulnerabilities in OpenSSL and Necessary Software Countermeasures. , 2007, , 185-203.		46
18	Fast Garbling of Circuits Under Standard Assumptions. , 2015, , .		41

#	Article	IF	Citations
19	A threeâ€“dimensional model for ciliary motion based on the internal 9 + 2 structure. Proceedings of the Royal Society B: Biological Sciences, 2001, 268, 599-607.	2.6	39
20	Efficient implementation of the Galois Counter Mode using a carry-less multiplier and a fast reduction algorithm. Information Processing Letters, 2010, 110, 549-553.	0.6	38
21	A model of herd grazing as a travelling wave, chemotaxis and stability. Journal of Mathematical Biology, 1989, 27, 595-608.	1.9	36
22	A fast Abel inversion algorithm. Journal of Applied Physics, 1994, 75, 4313-4318.	2.5	35
23	The steady-state distributions of coagulation-fragmentation processes. Journal of Mathematical Biology, 1998, 37, 1-27.	1.9	28
24	The Fermat-Steiner Problem. American Mathematical Monthly, 2002, 109, 443-451.	0.3	28
25	Encrypting the internet. , 2010, , .		27
26	SimpiraÂv2: A Family of Efficient Permutations Using the AES Round Function. Lecture Notes in Computer Science, 2016, , 95-125.	1.3	27
27	Controlling one-dimensional unimodal population maps by harvesting at a constant rate. Physical Review E, 1998, 57, 3645-3648.	2.1	23
28	The Fermat-Steiner Problem. American Mathematical Monthly, 2002, 109, 443.	0.3	23
29	Efficient software implementations of modular exponentiation. Journal of Cryptographic Engineering, 2012, 2, 31-43.	1.8	22
30	The Intel AES Instructions Set and the SHA-3 Candidates. Lecture Notes in Computer Science, 2009, , 162-178.	1.3	21
31	QC-MDPC Decoders with Several Shades of Gray. Lecture Notes in Computer Science, 2020, , 35-50.	1.3	20
32	Reduction of a channel-based model for a stomatogastric ganglion LP neuron. Biological Cybernetics, 1993, 69, 129-137.	1.3	19
33	A toolbox for software optimization of QC-MDPC code-based cryptosystems. Journal of Cryptographic Engineering, 2019, 9, 341-357.	1.8	18
34	On a Discrete Variational Problem Involving Interacting Particles. SIAM Journal on Applied Mathematics, 1999, 60, 1-17.	1.8	17
35	How Many Queries are Needed to Distinguish a Truncated Random Permutation from a Random Function?. Journal of Cryptology, 2018, 31, 162-171.	2.8	17
36	Software Implementation of Modular Exponentiation, Using Advanced Vector Instructions Architectures. Lecture Notes in Computer Science, 2012, , 119-135.	1.3	16

#	Article	IF	Citations
37	Fast Garbling of Circuits Under Standard Assumptions. Journal of Cryptology, 2018, 31, 798-844.	2.8	15
38	Better Bounds for Block Cipher Modes of Operation via Nonce-Based Key Derivation. , 2017, , .		14
39	Designing a Practical Code-Based Signature Scheme from Zero-Knowledge Proofs with Trusted Setup. Cryptography, 2022, 6, 5.	2.3	14
40	Fast software implementation of binary elliptic curve cryptography. Journal of Cryptographic Engineering, 2015, 5, 215-226.	1.8	13
41	CAKE: Code-Based Algorithm for Key Encapsulation. Lecture Notes in Computer Science, 2017, , 207-226.	1.3	13
42	Fast Polynomial Inversion for Post Quantum QC-MDPC Cryptography. Lecture Notes in Computer Science, 2020, , 110-127.	1.3	13
43	The three-dimensional motion of slender filaments. Mathematical Methods in the Applied Sciences, 2001, 24, 1577-1603.	2.3	11
44	The Fragility of AES-GCM Authentication Algorithm. , 2014, , .		11
45	Enhanced Montgomery Multiplication. Lecture Notes in Computer Science, 2003, , 46-56.	1.3	11
46	Parallelizing message schedules to accelerate the computations of hash functions. Journal of Cryptographic Engineering, 2012, 2, 241-253.	1.8	10
47	Speeding up CRC32C computations with Intel CRC32 instruction. Information Processing Letters, 2012, 112, 179-185.	0.6	10
48	Selfie: reflections on TLS 1.3 with PSK. Journal of Cryptology, 2021, 34, 1.	2.8	10
49	Simultaneous Hashing of Multiple Messages. Journal of Information Security, 2012, 03, 319-325.	0.8	10
50	Accelerating Big Integer Arithmetic Using Intel IFMA Extensions. , 2016, , .		9
51	Using Scan Side Channel to Detect IP Theft. IEEE Transactions on Very Large Scale Integration (VLSI) Systems, 2017, 25, 3268-3280.	3.1	9
52	Speeding Up SHA-1, SHA-256 and SHA-512 on the 2nd Generation Intel&amp;#x0AE; Core&amp;#153; Processors. , 2012, , .		8
53	Vectorization on ChaCha Stream Cipher. , 2014, , .		8
54	Fast multiplication of binary polynomials with the forthcoming vectorized VPCLMULQDQ instruction. , 2018, , .		8

#	Article	IF	Citations
55	Encrypting the internet. Computer Communication Review, 2010, 40, 135-146.	1.8	8
56	Blinded random corruption attacks. , 2016, , .		6
57	Combining Homomorphic Encryption with Trusted Execution Environment. , 2017, , .		6
58	Making AES Great Again: The Forthcoming Vectorized AES Instruction. Advances in Intelligent Systems and Computing, 2019, , 37-41.	0.6	6
59	Methods for Fast Computation of Integral Transforms. Journal of Computational Physics, 1994, 110, 164-170.	3.8	5
60	Two Applications of the Generalized Ptolemy Theorem. American Mathematical Monthly, 2002, 109, 362-370.	0.3	5
61	86.35 On the Inverse of the Hilbert Matrix. Mathematical Gazette, 2002, 86, 274.	0.0	5
62	A 2.1GHz 6.5mW 64-bit Unified PopCount/BitScan Datapath Unit for 65nm High-Performance Microprocessor Execution Cores. , 2008, , .		5
63	Speeding Up Big-Numbers Squaring. , 2012, , .		5
64	Vectorization of Poly1305 Message Authentication Code. , 2015, , .		5
65	Speed Records for Multi-prime RSA Using AVX2 Architectures. Advances in Intelligent Systems and Computing, 2016, , 237-245.	0.6	5
66	Surnaming Schemes, Fast Verification, and Applications to SGX Technology. Lecture Notes in Computer Science, 2017, , 149-164.	1.3	5
67	Fast constant time implementations of ZUC-256 on x86 CPUs. , 2019, , .		5
68	Fast Modular Squaring with AVX512IFMA. Advances in Intelligent Systems and Computing, 2019, , 3-8.	0.6	5
69	On Constant-Time QC-MDPC Decoders with Negligible Failure Rate. Lecture Notes in Computer Science, 2020, , 50-79.	1.3	5
70	Singleâ€projection radiography for noncircular symmetries: Generalization of the Abel transform method. Journal of Applied Physics, 1996, 79, 8879-8885.	2.5	4
71	A Weighted ErdÃƒÂ…Ã‚Â‘s-Mordell Inequality for Polygons. American Mathematical Monthly, 2005, 112, 257.	0.3	4
72	Where Does Security Stand? New Vulnerabilities vs. Trusted Computing. IEEE Micro, 2007, 27, 25-35.	1.8	4

#	Article	IF	Citations
73	Faster Secure Cloud Computations with a Trusted Proxy. IEEE Security and Privacy, 2017, 15, 61-67.	1.2	4
74	Balanced Permutations Evenâ€“Mansour Ciphers. Cryptography, 2017, 1, 2.	2.3	4
75	The Comeback of Reed Solomon Codes. , 2018, , .		4
76	On the applicability of the Fujisakiâ€“Okamoto transformation to the BIKE KEM. International Journal of Computer Mathematics: Computer Systems Theory, 2021, 6, 364-374.	1.1	4
77	The Risk of Cancer Might be Lower Than We Think. Alternatives to Lifetime Risk Estimates. Rambam Maimonides Medical Journal, 2018, 9, e0002.	1.0	4
78	Deterministic approximations for stochastic processes in population biology. Future Generation Computer Systems, 2001, 17, 893-899.	7.5	3
79	A Technique for Accelerating Characteristic 2 Elliptic Curve Cryptography. , 2008, , .		3
80	Speeding up Counter Mode in Software and Hardware. , 2014, , .		3
81	Hardware Implementation of AES Using Area-Optimal Polynomials for Composite-Field Representation GF(2^4)^2 of GF(2^8). , 2016, , .		3
82	On the Impossibility of Detecting Virtual Machine Monitors. IFIP Advances in Information and Communication Technology, 2009, , 143-151.	0.7	3
83	Software Optimizations for Cryptographic Primitives on General Purpose x86_64 Platforms. Lecture Notes in Computer Science, 2011, , 399-400.	1.3	3
84	Fast computation of limit cycles in an industrial application. Journal of Engineering Mathematics, 2001, 39, 79-86.	1.2	2
85	A Weighted Erdos-Mordell Inequality. American Mathematical Monthly, 2001, 108, 165.	0.3	2
86	White Box AES Using Intel's New AES Instructions. , 2013, , .		2
87	Attacks on Encrypted Memory and Constructions for Memory Protection. , 2016, , .		2
88	Using Scan Side Channel for Detecting IP Theft. , 2016, , .		2
89	Speeding-Up P-256 ECDSA Verification on x86-64 Servers. IEEE Letters of the Computer Society, 2019, 2, 12-15.	1.0	2
90	The advantage of truncated permutations. Discrete Applied Mathematics, 2021, 294, 214-223.	0.9	2

#	Article	IF	Citations
91	Software Optimizations of NTRUEncrypt for Modern Processor Architectures. Advances in Intelligent Systems and Computing, 2016, , 189-199.	0.6	2
92	Two Are Better than One: Software Optimizations for AES-GCM over Short Messages. Advances in Intelligent Systems and Computing, 2018, , 187-191.	0.6	2
93	Fallacies, Flaws, and Flimflam. College Mathematics Journal, 2000, 31, 120-123.	0.1	1
94	Two Applications of the Generalized Ptolemy Theorem. American Mathematical Monthly, 2002, 109, 362.	0.3	1
95	Quick Verification of RSA Signatures. , 2011, , .		1
96	Fast Quicksort Implementation Using AVX Instructions. Computer Journal, 2015, , bxv063.	2.4	1
97	Paillier-encrypted databases with fast aggregated queries. , 2017, , .		1
98	Randomness Tests in Hostile Environments. IEEE Transactions on Dependable and Secure Computing, 2018, 15, 289-294.	5.4	1
99	The three-dimensional motion of slender filaments. Mathematical Methods in the Applied Sciences, 2001, 24, 1577.	2.3	1
100	Spatial Interpolation Methods for Integrating Newton's Equation. Journal of Computational Physics, 1996, 129, 87-100.	3.8	0
101	Flying in a floating (point) world. International Journal of Computers for Mathematical Learning, 1999, 4, 225-234.	0.6	0
102	Fallacies, Flaws, and Flimflam. College Mathematics Journal, 2000, 31, 205-207.	0.1	0
103	Speeding Up a Numerical Algorithm. College Mathematics Journal, 2001, 32, 33-38.	0.1	0
104	Characterization of regular Diophantine quadruples. Elemente Der Mathematik, 2001, 56, 71-81.	0.1	0
105	On Smoluchowski Equations for Coagulation Processes with Multiple Absorbing States. Monte Carlo Methods and Applications, 2001, 7, .	0.8	0
106	A Game-Like Activity for Learning Cantor's Theorem. College Mathematics Journal, 2001, 32, 122.	0.1	0
107	86.18 Infinitely Many Primes in Arithmetic Progressions: The Cyclotomic Polynomial Method. Mathematical Gazette, 2002, 86, 110.	0.0	0
108	Mitigating collision and preimage attacks against the generalized MDC-2 mode of operation. , 2010, , .		0

#	Article	IF	Citations
109	Software Optimizations for DES. Advances in Intelligent Systems and Computing, 2018, , 133-138.	0.6	0
110	Cryptosystems with a multi prime composite modulus. , 2018, , .		0
111	Key Management Systems at the Cloud Scale. Cryptography, 2019, 3, 23.	2.3	0
112	A probabilistic variant of Sperner â€™s theorem and of maximal <mml:math xmlns:mml="http://www.w3.org/1998/Math/MathML" display="inline" id="d1e25" altimg="si14.svg"><mml:mi>r</mml:mi></mml:math>-cover free families. Discrete Mathematics, 2020, 343, 112027.	0.7	0
113	Binding BIKE Errors to a Key Pair. Lecture Notes in Computer Science, 2021, , 275-281.	1.3	0
114	Energetic Considerations of Ciliary Beating. The IMA Volumes in Mathematics and Its Applications, 2001, , 81-96.	0.5	0
115	The Sky Has Its Limits in COVID-19 Testing. Rambam Maimonides Medical Journal, 2020, 11, e0020.	1.0	0
116	Speeding Up a Numerical Algorithm. College Mathematics Journal, 2001, 32, 33.	0.1	0
117	Software Optimization of Rijndael for Modern x86-64 Platforms. Advances in Intelligent Systems and Computing, 2022, , 147-153.	0.6	0