Takaaki Mizuki

List of Publications by Year
in descending order

130 papers	1,691 citations	257429 24 h-index	361001 35 g-index
136 all docs	136 docs citations	136 times ranked	183 citing authors

#	Article	IF	Citations
1	Six-Card Secure AND and Four-Card Secure XOR. Lecture Notes in Computer Science, 2009, , 358-369.	1.3	102
2	A formalization of card-based cryptographic protocols via abstract machine. International Journal of Information Security, 2014, 13, 15-23.	3.4	74
3	The Five-Card Trick Can Be Done with Four Cards. Lecture Notes in Computer Science, 2012, , 598-606.	1.3	63
4	Analysis of Electromagnetic Information Leakage From Cryptographic Devices With Different Physical Structures. IEEE Transactions on Electromagnetic Compatibility, 2013, 55, 571-580.	2.2	52
5	Efficient Card-Based Protocols for Generating a Hidden Random Permutation Without Fixed Points. Lecture Notes in Computer Science, 2015, , 215-226.	1.3	51
6	Efficient card-based zero-knowledge proof for Sudoku. Theoretical Computer Science, 2020, 839, 135-142.	0.9	45
7	Computational Model of Card-Based Cryptographic Protocols and Its Applications. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2017, E100.A, 3-11.	0.3	44
8	Card-Based Protocols for Any Boolean Function. Lecture Notes in Computer Science, 2015, , 110-121.	1.3	42
9	Voting with a Logarithmic Number of Cards. Lecture Notes in Computer Science, 2013, , 162-173.	1.3	42
10	Physical Zero-Knowledge Proof for Makaro. Lecture Notes in Computer Science, 2018, , 111-125.	1.3	39
11	Secure implementations of a random bisection cut. International Journal of Information Security, 2020, 19, 445-452.	3.4	34
12	Practical card-based implementations of Yao's millionaire protocol. Theoretical Computer Science, 2020, 803, 207-221.	0.9	34
13	Interactive Physical Zero-Knowledge Proof for Norinori. Lecture Notes in Computer Science, 2019, , 166-177.	1.3	34
14	Card-Based Physical Zero-Knowledge Proof for Kakuro. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2019, E102.A, 1072-1078.	0.3	34
15	The Minimum Number of Cards in Practical Card-Based Protocols. Lecture Notes in Computer Science, 2017, , 126-155.	1.3	33
16	Practical Card-Based Cryptography. Lecture Notes in Computer Science, 2014, , 313-324.	1.3	32
17	Card-based protocols for securely computing the conjunction of multiple variables. Theoretical Computer Science, 2016, 622, 34-44.	0.9	31
18	How to Implement a Random Bisection Cut. Lecture Notes in Computer Science, 2016, , 58-69.	1.3	31

#	Article	IF	Citations
19	Efficient Evaluation of EM Radiation Associated With Information Leakage From Cryptographic Devices. IEEE Transactions on Electromagnetic Compatibility, 2013, 55, 555-563.	2.2	30
20	Securely Computing the Three-Input Majority Function with Eight Cards. Lecture Notes in Computer Science, 2013, , 193-204.	1.3	30
21	Card-Based Protocols Using Regular Polygon Cards. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2017, E100.A, 1900-1909.	0.3	29
22	Card-based protocols using unequal division shuffles. Soft Computing, 2018, 22, 361-371.	3.6	26
23	How to construct physical zero-knowledge proofs for puzzles with a â€œsingle loopâ€• condition. Theoretical Computer Science, 2021, 888, 41-55.	0.9	26
24	Non-invasive EMI-based fault injection attack against cryptographic modules. , 2011, , .		25
25	Transient IEMI Threats for Cryptographic Devices. IEEE Transactions on Electromagnetic Compatibility, 2013, 55, 140-148.	2.2	25
26	Pile-Shifting Scramble for Card-Based Protocols. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2018, E101.A, 1494-1502.	0.3	23
27	Multi-party Computation with Small Shuffle Complexity Using Regular Polygon Cards. Lecture Notes in Computer Science, 2015, , 127-146.	1.3	21
28	Efficient and Secure Multiparty Computations Using a Standard Deck of Playing Cards. Lecture Notes in Computer Science, 2016, , 484-499.	1.3	21
29	Securely Computing Three-Input Functions with Eight Cards. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2015, E98.A, 1145-1152.	0.3	21
30	Five-Card AND Protocol in Committed Format Using Only Practical Shuffles. , 2018, , .		20
31	Physical zero-knowledge proof and NP-completeness proof of Suguru puzzle. Information and Computation, 2022, 285, 104858.	0.7	20
32	Card-based protocols for secure ranking computations. Theoretical Computer Science, 2020, 845, 122-135.	0.9	19
33	Card-Based ZKP for Connectivity: Applications to Nurikabe, Hitori, and Heyawake. New Generation Computing, 2022, 40, 149-171.	3.3	18
34	Five-Card AND Computations in Committed Format Using Only Uniform Cyclic Shuffles. New Generation Computing, 2021, 39, 97-114.	3.3	17
35	A Physical ZKP for Slitherlink: How to Perform Physical Topology-Preserving Computation. Lecture Notes in Computer Science, 2019, , 135-151.	1.3	17
36	Five-Card Secure Computations Using Unequal Division Shuffle. Lecture Notes in Computer Science, 2015, , 109-120.	1.3	16

#	Article	IF	Citations
37	The Six-Card Trick: Secure Computation of Three-Input Equality. Lecture Notes in Computer Science, 2019, , 123-131.	1.3	16
38	Mechanism behind Information Leakage in Electromagnetic Analysis of Cryptographic Modules. Lecture Notes in Computer Science, 2009, , 66-78.	1.3	15
39	An Implementation of Non-Uniform Shuffle for Secure Multi-Party Computation. , 2016, , .		12
40	A Secure Three-Input AND Protocol withÂaÂStandard Deck of Minimal Cards. Lecture Notes in Computer Science, 2021, , 242-256.	1.3	12
41	Six-Card Finite-Runtime XOR Protocol with Only Random Cut. , 2020, , .		12
42	New Card-based Copy Protocols Using Only Random Cuts. , 2021, , .		11
43	Necessary and Sufficient Numbers of Cards for Securely Computing Two-Bit Output Functions. Lecture Notes in Computer Science, 2017, , 193-211.	1.3	11
44	Zero-Knowledge Proof Protocol forÂCryptarithmetic Using Dihedral Cards. Lecture Notes in Computer Science, 2021, , 51-67.	1.3	11
45	A complete characterization of a family of key exchange protocols. International Journal of Information Security, 2002, 1, 131-142.	3.4	10
46	Secure Multi-Party Computation Using Polarizing Cards. Lecture Notes in Computer Science, 2015, , 281-297.	1.3	10
47	Card-Based Covert Lottery. Lecture Notes in Computer Science, 2021, , 257-270.	1.3	10
48	Secure Computation of Any Boolean Function Based on Any Deck of Cards. Lecture Notes in Computer Science, 2019, , 63-75.	1.3	10
49	Analysis of Electromagnetic Radiation from Transmission Line with Loose Contact of Connector. IEICE Transactions on Electronics, 2011, E94-C, 1427-1430.	0.6	9
50	Physical authentication using side-channel information. , 2016, , .		9
51	A study on an Effective Evaluation Method for EM Information Leakage without Reconstructing Screen. , 2019, , .		9
52	Analysis of Information Leakage Due to Operative Errors in Card-Based Protocols. Lecture Notes in Computer Science, 2018, , 250-262.	1.3	9
53	A Card-Minimal Three-Input ANDÂProtocol Using Two Shuffles. Lecture Notes in Computer Science, 2021, , 668-679.	1.3	9
54	Evaluation of Information Leakage from Cryptographic Hardware via Common-Mode Current. IEICE Transactions on Electronics, 2012, E95.C, 1089-1097.	0.6	9

#	Article	IF	Citations
55	Card-based Single-shuffle Protocols for Secure Multiple-input AND and XOR Computations. , 2022, , .		9
56	Suppression of information leakage from electronic devices based on SNR. , 2011, , .		8
57	Another Use ofÂtheÂFive-Card Trick: Card-Minimal Secure Three-Input Majority Function Evaluation. Lecture Notes in Computer Science, 2021, , 536-555.	1.3	8
58	Characterization of optimal key set protocols. Discrete Applied Mathematics, 2003, 131, 213-236.	0.9	7
59	Secure Computation Protocols Using Polarizing Cards. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2016, E99.A, 1122-1131.	0.3	7
60	Efficient Generation of a Card-Based Uniformly Distributed Random Derangement. Lecture Notes in Computer Science, 2021, , 78-89.	1.3	7
61	Preface: Special Issue on Card-Based Cryptography. New Generation Computing, 2021, 39, 1-2.	3.3	7
62	Card-Based Protocol Against Actively Revealing Card Attack. Lecture Notes in Computer Science, 2019, , 95-106.	1.3	7
63	Secure Multiparty Computations Using the 15 Puzzle. Lecture Notes in Computer Science, 2007, , 255-266.	1.3	7
64	How to Implement a Non-uniform or Non-closed Shuffle. Lecture Notes in Computer Science, 2020, , 107-118.	1.3	7
65	AN APPLICATION OF ESOP EXPRESSIONS TO SECURE COMPUTATIONS. Journal of Circuits, Systems and Computers, 2007, 16, 191-198.	1.5	6
66	Evaluating card-based protocols in terms of execution time. International Journal of Information Security, 2021, 20, 729-740.	3.4	6
67	Actively revealing card attack on card-based protocols. Natural Computing, 0, , 1.	3.0	6
68	Analyzing Execution Time of Card-Based Protocols. Lecture Notes in Computer Science, 2018, , 145-158.	1.3	6
69	Mechanism of Increase in Inductance at Loosened Connector Contact Boundary. IEICE Transactions on Electronics, 2012, E95.C, 1502-1507.	0.6	6
70	Information leakage due to operative errors in card-based protocols. Information and Computation, 2022, 285, 104910.	0.7	6
71	On contact conditions in connectors to cause Common Mode radiation. , 2008, , .		5
72	Precisely timed IEMI fault injection synchronized with EM information leakage. , 2014, , .		5

#	Article	IF	Citations
73	Cooking Cryptographers: Secure Multiparty Computation Based on Balls and Bags. , 2021, , .		5
74	Secure Multiparty Computations Using a Dial Lock. , 2007, , 499-510.		5
75	Modeling connector contact condition using a contact failure model with equivalent inductance. , 2010, , .		4
76	Information leakage from cryptographic hardware via common-mode current. , 2010, , .		4
77	Evaluation of Resistance and Inductance of Loose Connector Contact. IEICE Transactions on Electronics, 2013, E96.C, 1148-1150.	0.6	4
78	Basic Study on the Method for Real-Time Video Streaming with Low Latency and High Bandwidth Efficiency. , 2015, , .		4
79	Information Leakage Threats for Cryptographic Devices Using IEMI and EM Emission. IEEE Transactions on Electromagnetic Compatibility, 2018, 60, 1340-1347.	2.2	4
80	Committed-format AND protocol using only random cuts. Natural Computing, 2021, 20, 639-645.	3.0	4
81	Public-PEZ Cryptography. Lecture Notes in Computer Science, 2020, , 59-74.	1.3	4
82	Practical and Easy-to-Understand Card-Based Implementation of Yaoâ€™s Millionaire Protocol. Lecture Notes in Computer Science, 2018, , 246-261.	1.3	4
83	Contact Conditions in Connectors that Cause Common Mode Radiation. IEICE Transactions on Electronics, 2011, E94-C, 1369-1374.	0.6	3
84	AN APPLICATION OF ST-NUMBERING TO SECRET KEY AGREEMENT. International Journal of Foundations of Computer Science, 2011, 22, 1211-1227.	1.1	3
85	Study on the effect of clock rise time on fault occurrence under IEMI. , 2018, , .		3
86	Necessary and Sufficient Numbers of Cards for the Transformation Protocol. Lecture Notes in Computer Science, 2004, , 92-101.	1.3	3
87	Fundamental Study on Mechanism of Electromagnetic Field Radiation from Electric Devices with Loose Contact of Connector. IEEJ Transactions on Fundamentals and Materials, 2012, 132, 373-378.	0.2	3
88	The Source Estimation of Electromagnetic Information Leakage from Information Devices. , 2020, , .		3
89	A Revised Transformation Protocol for Unconditionally Secure Secret Key Exchange. Theory of Computing Systems, 2008, 42, 187-221.	1.1	2
90	A one-round secure message broadcasting protocol through a key sharing tree. Information Processing Letters, 2009, 109, 842-845.	0.6	2

#	Article	IF	Citations
91	Relationship between connector contact points and common-mode current on a coaxial transmission line. , 2009, , .		2
92	Efficient mapping of EM radiation associated with information leakage for cryptographic devices. , 2012, , .		2
93	Map-based analysis of IEMI fault injection into cryptographic devices. , 2013, , .		2
94	Analysis of EM emission from cryptographic devices. , 2014, , .		2
95	Fundamental study on randomized processing in cryptographic IC using variable clock against Correlation Power Analysis. , 2015, , .		2
96	Method for estimating fault injection time on cryptographic devices from EM leakage. , 2015, , .		2
97	A Practical Evaluation Method for EM Information Leakage by Using Audible Signal. , 2019, , .		2
98	Secure Computations in a Minimal Model Using Multiple-Valued ESOP Expressions. Lecture Notes in Computer Science, 2006, , 547-554.	1.3	2
99	Study on Information Leakage of Input Key due to Frequency Fluctuation of RC Oscillator in Keyboard. IEICE Transactions on Communications, 2013, E96.B, 2633-2638.	0.7	2
100	Multi-party Computation Based on Physical Coins. Lecture Notes in Computer Science, 2018, , 87-98.	1.3	2
101	Light Cryptography. IFIP Advances in Information and Communication Technology, 2019, , 89-101.	0.7	2
102	Measurement on Effect of Controlled Wave Phase in EM Fault Injection Attack. , 2020, , .		2
103	Coin-based Secure Computations. International Journal of Information Security, 0, , 1.	3.4	2
104	ABSOLUTELY SECURE MESSAGE TRANSMISSION USING A KEY SHARING GRAPH. Discrete Mathematics, Algorithms and Applications, 2012, 04, 1250053.	0.6	1
105	Investigation on the effect of parasitic inductance at connector contact boundary on electromagnetic radiation. , 2012, , .		1
106	Minimizing ESCT forms for two-variable multiple-valued input binary output functions. Discrete Applied Mathematics, 2014, 169, 186-194.	0.9	1
107	Fundamental study on fault occurrence mechanisms by intentional electromagnetic interference using impulses. , 2015, , .		1
108	Efficient Electromagnetic Analysis for Cryptographic Module on the Frequency Domain. Electronics and Communications in Japan, 2016, 99, 24-32.	0.5	1

#	Article	IF	Citations
109	Secure Multi-Party Computations Using a Deck of Cards. Ieice Ess Fundamentals Review, 2016, 9, 179-187.	0.1	1
110	Best Security Index for Digital Fingerprinting. Lecture Notes in Computer Science, 2005, , 398-412.	1.3	1
111	Influence of PCB and Attached Line of Hardware on Electromagnetic (EM) Information Leakage. IEEJ Transactions on Fundamentals and Materials, 2012, 132, 173-179.	0.2	1
112	Investigation of Noise Interference due to Connector Contact Failure in a Coaxial Cable. IEICE Transactions on Electronics, 2014, E97.C, 900-903.	0.6	1
113	Quantitative Evaluation of Inductance at the Coaxial Connector Contact Failure Portion. IEEJ Transactions on Fundamentals and Materials, 2016, 136, 347-352.	0.2	1
114	Sharing secret keys along a Eulerian circuit. Electronics and Communications in Japan, Part III: Fundamental Electronic Science (English Translation of Denshi Tsushin Gakkai Ronbunshi), 2000, 83, 33-42.	0.1	0
115	An efficient method for estimating the area of information propagation through electromagnetic radiation. , 2012, , .		0
116	Influence of PCB and attached line of hardware on electromagnetic (EM) information leakage. Electrical Engineering in Japan (English Translation of Denki Gakkai Ronbunshi), 2013, 182, 1-9.	0.4	0
117	Fundamental Study on a Mechanism of Faulty Outputs from Cryptographic Modules Due to IEMI. Electronics and Communications in Japan, 2016, 99, 72-78.	0.5	0
118	A study on an evaluation method for EM information leakage utilizing controlled image displaying. , 2018, , .		0
119	Experimental Study on Measurement Resolution of Side Channel Waveform in Correlation Power Analysis. , 2020, , .		0
120	Characterization of Optimal Key Set Protocols. Lecture Notes in Computer Science, 2000, , 273-285.	1.3	0
121	Necessary and Sufficient Numbers of Cards for Sharing Secret Keys on Hierarchical Groups. Lecture Notes in Computer Science, 2001, , 196-207.	1.3	0
122	Worst-Case Optimal Fingerprinting Codes for Non-threshold Collusion. Lecture Notes in Computer Science, 2006, , 203-216.	1.3	0
123	Minimizing AND-EXOR Expressions for Multiple-Valued Two-Input Logic Functions. Lecture Notes in Computer Science, 2009, , 301-310.	1.3	0
124	Analysis of Magnetic Field Distribution around Connector with Contact Failure. IEEJ Transactions on Fundamentals and Materials, 2012, 132, 417-420.	0.2	0
125	Recent Research Trends in Side Channel Attack on Cryptographic Modules and its Countermeasure. IEEJ Transactions on Fundamentals and Materials, 2012, 132, 9-12.	0.2	0
126	Effect of Contact Failure of Connector in Electronic Control Units on Radiated Emissions. IEEJ Transactions on Fundamentals and Materials, 2012, 132, 456-457.	0.2	0

#	Article	IF	Citations
127	Effect of Connector Contact Points on Common-Mode Current on a Coaxial Transmission Line. IEEJ Transactions on Fundamentals and Materials, 2013, 133, 273-277.	0.2	0
128	Fundamental Study on a Mechanism of Faulty Outputs from Cryptographic Modules due to IEMI. IEEJ Transactions on Fundamentals and Materials, 2015, 135, 276-281.	0.2	0
129	Efficient Electromagnetic Analysis for Cryptographic Module on the Frequency Domain. IEEJ Transactions on Fundamentals and Materials, 2015, 135, 515-521.	0.2	0
130	Secret Key Amplification from Uniformly Leaked Key Exchange Complete Graph. Lecture Notes in Computer Science, 2018, , 20-31.	1.3	0