Takaaki Mizuki

List of Publications by Citations

125 papers	1,272 citations	21 h-index	29 g-index
136 ext. papers	1,382 ext. citations	0.8 avg, IF	5.53 L-index

#	Paper	IF	Citations
125	Six-Card Secure AND and Four-Card Secure XOR. *Lecture Notes in Computer Science*, **2009**, 358-369	0.9	83
124	A formalization of card-based cryptographic protocols via abstract machine. *International Journal of Information Security*, **2014**, 13, 15-23	2.8	61
123	The Five-Card Trick Can Be Done with Four Cards. *Lecture Notes in Computer Science*, **2012**, 598-606	0.9	55
122	Analysis of Electromagnetic Information Leakage From Cryptographic Devices With Different Physical Structures. *IEEE Transactions on Electromagnetic Compatibility*, **2013**, 55, 571-580	2	39
121	Efficient Card-Based Protocols for Generating a Hidden Random Permutation Without Fixed Points. *Lecture Notes in Computer Science*, **2015**, 215-226	0.9	39
120	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	0.4	38
119	Voting with a Logarithmic Number of Cards. *Lecture Notes in Computer Science*, **2013**, 162-173	0.9	38
118	Card-Based Protocols for Any Boolean Function. *Lecture Notes in Computer Science*, **2015**, 110-121	0.9	33
117	Efficient card-based zero-knowledge proof for Sudoku. *Theoretical Computer Science*, **2020**, 839, 135-142	1.1	32
116	Physical Zero-Knowledge Proof for Makaro. *Lecture Notes in Computer Science*, **2018**, 111-125	0.9	29
115	The Minimum Number of Cards in Practical Card-Based Protocols. *Lecture Notes in Computer Science*, **2017**, 126-155	0.9	28
114	How to Implement a Random Bisection Cut. *Lecture Notes in Computer Science*, **2016**, 58-69	0.9	28
113	Securely Computing the Three-Input Majority Function with Eight Cards. *Lecture Notes in Computer Science*, **2013**, 193-204	0.9	27
112	Card-based protocols for securely computing the conjunction of multiple variables. *Theoretical Computer Science*, **2016**, 622, 34-44	1.1	26
111	Interactive Physical Zero-Knowledge Proof for Norinori. *Lecture Notes in Computer Science*, **2019**, 166-177	0.9	26
110	Practical card-based implementations of Yao's millionaire protocol. *Theoretical Computer Science*, **2020**, 803, 207-221	1.1	25
109	Efficient Evaluation of EM Radiation Associated With Information Leakage From Cryptographic Devices. *IEEE Transactions on Electromagnetic Compatibility*, **2013**, 55, 555-563	2	24

108	Card-Based Physical Zero-Knowledge Proof for Kakuro. *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, **2019**, E102.A, 1072-1078	0.4	24
107	Practical Card-Based Cryptography. *Lecture Notes in Computer Science*, **2014**, 313-324	0.9	24
106	Card-based protocols using unequal division shuffles. *Soft Computing*, **2018**, 22, 361-371	3.5	21
105	Secure implementations of a random bisection cut. *International Journal of Information Security*, **2020**, 19, 445-452	2.8	21
104	Securely Computing Three-Input Functions with Eight Cards. *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, **2015**, E98.A, 1145-1152	0.4	19
103	Five-Card AND Protocol in Committed Format Using Only Practical Shuffles **2018**,		19
102	Non-invasive EMI-based fault injection attack against cryptographic modules **2011**,		18
101	Efficient and Secure Multiparty Computations Using a Standard Deck of Playing Cards. *Lecture Notes in Computer Science*, **2016**, 484-499	0.9	18
100	Card-Based Protocols Using Regular Polygon Cards. *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, **2017**, E100.A, 1900-1909	0.4	17
99	Pile-Shifting Scramble for Card-Based Protocols. *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, **2018**, E101.A, 1494-1502	0.4	17
98	Multi-party Computation with Small Shuffle Complexity Using Regular Polygon Cards. *Lecture Notes in Computer Science*, **2015**, 127-146	0.9	17
97	Physical Zero-Knowledge Proof for Suguru Puzzle. *Lecture Notes in Computer Science*, **2020**, 235-247	0.9	15
96	How to construct physical zero-knowledge proofs for puzzles with a □single loop□condition. *Theoretical Computer Science*, **2021**, 888, 41-55	1.1	15
95	Card-based protocols for secure ranking computations. *Theoretical Computer Science*, **2020**, 845, 122-135	1.1	14
94	Five-Card Secure Computations Using Unequal Division Shuffle. *Lecture Notes in Computer Science*, **2015**, 109-120	0.9	14
93	A Physical ZKP for Slitherlink: How to Perform Physical Topology-Preserving Computation. *Lecture Notes in Computer Science*, **2019**, 135-151	0.9	14
92	Interactive Physical ZKP for Connectivity: Applications to Nurikabe and Hitori. *Lecture Notes in Computer Science*, **2021**, 373-384	0.9	14
91	Five-Card AND Computations in Committed Format Using Only Uniform Cyclic Shuffles. *New Generation Computing*, **2021**, 39, 97-114	0.9	13

90	Transient IEMI Threats for Cryptographic Devices. *IEEE Transactions on Electromagnetic Compatibility*, **2013**, 55, 140-148	2	11
89	Six-Card Finite-Runtime XOR Protocol with Only Random Cut **2020**,		10
88	The Six-Card Trick: Secure Computation of Three-Input Equality. *Lecture Notes in Computer Science*, **2019**, 123-131	0.9	10
87	Necessary and Sufficient Numbers of Cards for Securely Computing Two-Bit Output Functions. *Lecture Notes in Computer Science*, **2017**, 193-211	0.9	10
86	Mechanism behind Information Leakage in Electromagnetic Analysis of Cryptographic Modules. *Lecture Notes in Computer Science*, **2009**, 66-78	0.9	10
85	An Implementation of Non-Uniform Shuffle for Secure Multi-Party Computation **2016**,		10
84	Analysis of Information Leakage Due to Operative Errors in Card-Based Protocols. *Lecture Notes in Computer Science*, **2018**, 250-262	0.9	9
83	A Secure Three-Input AND Protocol with a Standard Deck of Minimal Cards. *Lecture Notes in Computer Science*, **2021**, 242-256	0.9	9
82	Physical zero-knowledge proof and NP-completeness proof of Suguru puzzle. *Information and Computation*, **2021**, 104858	0.8	9
81	Secure Computation of Any Boolean Function Based on Any Deck of Cards. *Lecture Notes in Computer Science*, **2019**, 63-75	0.9	8
80	Card-Based ZKP for Connectivity: Applications to Nurikabe, Hitori, and Heyawake. *New Generation Computing*,1	0.9	8
79	Secure Multi-Party Computation Using Polarizing Cards. *Lecture Notes in Computer Science*, **2015**, 281-297	0.9	7
78	Characterization of optimal key set protocols. *Discrete Applied Mathematics*, **2003**, 131, 213-236	1	7
77	Zero-Knowledge Proof Protocol for Cryptarithmetic Using Dihedral Cards. *Lecture Notes in Computer Science*, **2021**, 51-67	0.9	7
76	Secure Multiparty Computations Using the 15 Puzzle. *Lecture Notes in Computer Science*, **2007**, 255-266	0.9	7
75	New Card-based Copy Protocols Using Only Random Cuts **2021**,		7
74	Secure Computation Protocols Using Polarizing Cards. *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, **2016**, E99.A, 1122-1131	0.4	7
73	A complete characterization of a family of key exchange protocols. *International Journal of Information Security*, **2002**, 1, 131-142	2.8	6

72	Card-Based Protocol Against Actively Revealing Card Attack. *Lecture Notes in Computer Science*, **2019**, 95-106	0.9	6
71	Efficient Generation of a Card-Based Uniformly Distributed Random Derangement. *Lecture Notes in Computer Science*, **2021**, 78-89	0.9	6
70	Card-Based Covert Lottery. *Lecture Notes in Computer Science*, **2021**, 257-270	0.9	6
69	Analysis of Electromagnetic Radiation from Transmission Line with Loose Contact of Connector. *IEICE Transactions on Electronics*, **2011**, E94-C, 1427-1430	0.4	5
68	On contact conditions in connectors to cause Common Mode radiation **2008**,		5
67	AN APPLICATION OF ESOP EXPRESSIONS TO SECURE COMPUTATIONS. *Journal of Circuits, Systems and Computers*, **2007**, 16, 191-198	0.9	5
66	Mechanism of Increase in Inductance at Loosened Connector Contact Boundary. *IEICE Transactions on Electronics*, **2012**, E95.C, 1502-1507	0.4	5
65	A Card-Minimal Three-Input AND Protocol Using Two Shuffles. *Lecture Notes in Computer Science*, **2021**, 668-679	0.9	5
64	Card-Based Secure Ranking Computations. *Lecture Notes in Computer Science*, **2019**, 461-472	0.9	5
63	Secure Multiparty Computations Using a Dial Lock **2007**, 499-510		5
62	Evaluation of Information Leakage from Cryptographic Hardware via Common-Mode Current. *IEICE Transactions on Electronics*, **2012**, E95.C, 1089-1097	0.4	5
61	Cooking Cryptographers: Secure Multiparty Computation Based on Balls and Bags **2021**,		5
60	Actively revealing card attack on card-based protocols. *Natural Computing*,1	1.3	5
59	Dealing Necessary and Sufficient Numbers of Cards for Sharing a One-Bit Secret Key (Extended Abstract). *Lecture Notes in Computer Science*, **1999**, 389-401	0.9	5
58	Suppression of information leakage from electronic devices based on SNR **2011**,		4
57	Another Use of the Five-Card Trick: Card-Minimal Secure Three-Input Majority Function Evaluation. *Lecture Notes in Computer Science*, **2021**, 536-555	0.9	4
56	Practical and Easy-to-Understand Card-Based Implementation of Yao□ Millionaire Protocol. *Lecture Notes in Computer Science*, **2018**, 246-261	0.9	4
55	Analyzing Execution Time of Card-Based Protocols. *Lecture Notes in Computer Science*, **2018**, 145-158	0.9	4

54	Preface: Special Issue on Card-Based Cryptography. *New Generation Computing*, **2021**, 39, 1-2	0.9	4
53	Physical authentication using side-channel information **2016**,		4
52	Precisely timed IEMI fault injection synchronized with EM information leakage **2014**,		3
51	Evaluation of Resistance and Inductance of Loose Connector Contact. *IEICE Transactions on Electronics*, **2013**, E96.C, 1148-1150	0.4	3
50	Modeling connector contact condition using a contact failure model with equivalent inductance **2010**,		3
49	AN APPLICATION OF ST-NUMBERING TO SECRET KEY AGREEMENT. *International Journal of Foundations of Computer Science*, **2011**, 22, 1211-1227	0.6	3
48	How to Implement a Non-uniform or Non-closed Shuffle. *Lecture Notes in Computer Science*, **2020**, 107-118	0.9	3
47	Card-Based Zero-Knowledge Proof Protocols for Graph Problems and Their Computational Model. *Lecture Notes in Computer Science*, **2021**, 136-152	0.9	3
46	Public-PEZ Cryptography. *Lecture Notes in Computer Science*, **2020**, 59-74	0.9	3
45	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
44	A study on an Effective Evaluation Method for EM Information Leakage without Reconstructing Screen **2019**,		3
43	Evaluating card-based protocols in terms of execution time. *International Journal of Information Security*, **2021**, 20, 729-740	2.8	3
42	Eulerian Secret Key Exchange. *Lecture Notes in Computer Science*, **1998**, 349-360	0.9	3
41	Method for estimating fault injection time on cryptographic devices from EM leakage **2015**,		2
40	Map-based analysis of IEMI fault injection into cryptographic devices **2013**,		2
39	Contact Conditions in Connectors that Cause Common Mode Radiation. *IEICE Transactions on Electronics*, **2011**, E94-C, 1369-1374	0.4	2
38	Information leakage from cryptographic hardware via common-mode current **2010**,		2
37	A one-round secure message broadcasting protocol through a key sharing tree. *Information Processing Letters*, **2009**, 109, 842-845	0.8	2

36	Efficient mapping of EM radiation associated with information leakage for cryptographic devices **2012**,		2
35	Necessary and Sufficient Numbers of Cards for the Transformation Protocol. *Lecture Notes in Computer Science*, **2004**, 92-101	0.9	2
34	Multi-party Computation Based on Physical Coins. *Lecture Notes in Computer Science*, **2018**, 87-98	0.9	2
33	Light Cryptography. *IFIP Advances in Information and Communication Technology*, **2019**, 89-101	0.5	2
32	Committed-format AND protocol using only random cuts. *Natural Computing*,1	1.3	2
31	Coin-based Secure Computations. *International Journal of Information Security*,1	2.8	2
30	Information Leakage Due to Operative Errors in Card-based Protocols. *Information and Computation*, **2022**, 104910	0.8	2
29	Information Leakage Threats for Cryptographic Devices Using IEMI and EM Emission. *IEEE Transactions on Electromagnetic Compatibility*, **2018**, 60, 1340-1347	2	1
28	Secure Multi-Party Computations Using a Deck of Cards. *Ieice Ess Fundamentals Review*, **2016**, 9, 179-187	0.1	1
27	Fundamental study on randomized processing in cryptographic IC using variable clock against Correlation Power Analysis **2015**,		1
26	Basic Study on the Method for Real-Time Video Streaming with Low Latency and High Bandwidth Efficiency **2015**,		1
25	Minimizing ESCT forms for two-variable multiple-valued input binary output functions. *Discrete Applied Mathematics*, **2014**, 169, 186-194	1	1
24	Investigation on the effect of parasitic inductance at connector contact boundary on electromagnetic radiation **2012**,		1
23	ABSOLUTELY SECURE MESSAGE TRANSMISSION USING A KEY SHARING GRAPH. *Discrete Mathematics, Algorithms and Applications*, **2012**, 04, 1250053	0.5	1
22	A Revised Transformation Protocol for Unconditionally Secure Secret Key Exchange. *Theory of Computing Systems*, **2008**, 42, 187-221	0.6	1
21	Best Security Index for Digital Fingerprinting. *Lecture Notes in Computer Science*, **2005**, 398-412	0.9	1
20	Secure Computations in a Minimal Model Using Multiple-Valued ESOP Expressions. *Lecture Notes in Computer Science*, **2006**, 547-554	0.9	1
19	Quantitative Evaluation of Inductance at the Coaxial Connector Contact Failure Portion. *IEEJ Transactions on Fundamentals and Materials*, **2016**, 136, 347-352	0.2	1

18	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	0.5	1
17	Investigation of Noise Interference due to Connector Contact Failure in a Coaxial Cable. *IEICE Transactions on Electronics*, **2014**, E97.C, 900-903	0.4	1
16	Efficient Electromagnetic Analysis for Cryptographic Module on the Frequency Domain. *Electronics and Communications in Japan*, **2016**, 99, 24-32	0.4	1
15	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	
14	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		
13	Characterization of Optimal Key Set Protocols. *Lecture Notes in Computer Science*, **2000**, 273-285	0.9	
12	Necessary and Sufficient Numbers of Cards for Sharing Secret Keys on Hierarchical Groups. *Lecture Notes in Computer Science*, **2001**, 196-207	0.9	
11	Worst-Case Optimal Fingerprinting Codes for Non-threshold Collusion. *Lecture Notes in Computer Science*, **2006**, 203-216	0.9	
10	Secret Key Amplification from Uniformly Leaked Key Exchange Complete Graph. *Lecture Notes in Computer Science*, **2018**, 20-31	0.9	
9	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	
8	Efficient Electromagnetic Analysis for Cryptographic Module on the Frequency Domain. *IEEJ Transactions on Fundamentals and Materials*, **2015**, 135, 515-521	0.2	
7	Minimizing AND-EXOR Expressions for Multiple-Valued Two-Input Logic Functions. *Lecture Notes in Computer Science*, **2009**, 301-310	0.9	
6	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	
5	Analysis of Magnetic Field Distribution around Connector with Contact Failure. *IEEJ Transactions on Fundamentals and Materials*, **2012**, 132, 417-420	0.2	
4	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	
3	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	
2	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	
1	Fundamental Study on a Mechanism of Faulty Outputs from Cryptographic Modules Due to IEMI. *Electronics and Communications in Japan*, **2016**, 99, 72-78	0.4	