Yosuke Todo

List of Publications by Year in descending order

Source: https://exaly.com/author-pdf/5668994/publications.pdf

Version: 2024-02-01

53 papers	1,247 citations	471061 17 h-index	377514 34 g-index
55 all docs	55 docs citations	55 times ranked	343 citing authors

#	Article	IF	Citations
1	Sycon: a new milestone in designing ASCON-like permutations. Journal of Cryptographic Engineering, 2022, 12, 305-327.	1.5	3
2	New Attacks from Old Distinguishers Improved Attacks on Serpent. Lecture Notes in Computer Science, 2022, , 484-510.	1.0	1
3	Designing S-Boxes Providing Stronger Security Against Differential Cryptanalysis for Ciphers Using Byte-Wise XOR. Lecture Notes in Computer Science, 2022, , 179-199.	1.0	1
4	Modeling for Three-Subset Division Property without Unknown Subset. Journal of Cryptology, 2021, 34, 1.	2.1	7
5	PRINCEv2. Lecture Notes in Computer Science, 2021, , 483-511.	1.0	8
6	Massive Superpoly Recovery withÂNested Monomial Predictions. Lecture Notes in Computer Science, 2021, , 392-421.	1.0	15
7	On the Data Limitation of Small-State Stream Ciphers: Correlation Attacks on Fruit-80 and Plantlet. Lecture Notes in Computer Science, 2020, , 365-392.	1.0	6
8	Modeling for Three-Subset Division Property Without Unknown Subset. Lecture Notes in Computer Science, 2020, , 466-495.	1.0	32
9	Out of Oddity â€“ New Cryptanalytic Techniques Against Symmetric Primitives Optimized for Integrity Proof Systems. Lecture Notes in Computer Science, 2020, , 299-328.	1.0	22
10	Improved Differential-Linear Attacks with Applications to ARX Ciphers. Lecture Notes in Computer Science, 2020, , 329-358.	1.0	24
11	Lower Bounds on the Degree of Block Ciphers. Lecture Notes in Computer Science, 2020, , 537-566.	1.0	17
12	Improved Integral Attack on HIGHT. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2019, E102.A, 1259-1271.	0.2	0
13	Improved Division Property Based Cube Attacks Exploiting Algebraic Properties of Superpoly. IEEE Transactions on Computers, 2019, 68, 1470-1486.	2.4	4
14	Nonlinear Invariant Attack: Practical Attack on Full SCREAM, iSCREAM, and Midori64. Journal of Cryptology, 2019, 32, 1383-1422.	2.1	17
15	Tight Bounds of Differentially and Linearly Active S-Boxes and Division Property of Lilliput. IEEE Transactions on Computers, 2018, 67, 717-732.	2.4	5
16	Programming the Demirci-SelÃ§uk Meet-in-the-Middle Attack with Constraints. Lecture Notes in Computer Science, 2018, , 3-34.	1.0	17
17	Several MILP-Aided Attacks Against SNOW 2.0. Lecture Notes in Computer Science, 2018, , 394-413.	1.0	8
18	Cube Attacks on Non-Blackbox Polynomials Based on Division Property. IEEE Transactions on Computers, 2018, 67, 1720-1736.	2.4	19

#	Article	IF	Citations
19	On the Complexity of Impossible Differential Cryptanalysis. Security and Communication Networks, 2018, 2018, 1-11.	1.0	1
20	Fast Correlation Attack Revisited. Lecture Notes in Computer Science, 2018, , 129-159.	1.0	21
21	Improved Division Property Based Cube Attacks Exploiting Algebraic Properties of Superpoly. Lecture Notes in Computer Science, 2018, , 275-305.	1.0	35
22	On the Design Rationale of SIMON Block Cipher: Integral Attacks and Impossible Differential Attacks against SIMON Variants. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2018, E101.A, 88-98.	0.2	7
23	New Differential Bounds and Division Property of Lilliput: Block Cipher with Extended Generalized Feistel Network. Lecture Notes in Computer Science, 2017, , 264-283.	1.0	8
24	New Algorithm for Modeling S-box in MILP Based Differential and Division Trail Search. Lecture Notes in Computer Science, 2017, , 150-165.	1.0	27
25	Cube Attacks on Non-Blackbox Polynomials Based on Division Property. Lecture Notes in Computer Science, 2017, , 250-279.	1.0	60
26	Integral Cryptanalysis on Full MISTY1. Journal of Cryptology, 2017, 30, 920-959.	2.1	27
27	New Impossible Differential Search Tool from Design and Cryptanalysis Aspects. Lecture Notes in Computer Science, 2017, , 185-215.	1.0	73
28	Improved Integral Attack on HIGHT. Lecture Notes in Computer Science, 2017, , 363-383.	1.0	4
29	Division Property: Efficient Method to Estimate Upper Bound of Algebraic Degree. Lecture Notes in Computer Science, 2017, , 553-571.	1.0	2
30	Analyzing Key Schedule of Simon: Iterative Key Differences and Application to Related-Key Impossible Differentials. Lecture Notes in Computer Science, 2017, , 141-158.	1.0	4
31	Gimli : A Cross-Platform Permutation. Lecture Notes in Computer Science, 2017, , 299-320.	1.0	51
32	GIFT: A Small Present. Lecture Notes in Computer Science, 2017, , 321-345.	1.0	221
33	Impossible Differential Attack against 14-Round <i>Piccolo</i>-80 without Relying on Full Code Book. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2016, E99.A, 154-157.	0.2	4
34	New Conditional Differential Cryptanalysis for NLFSR-based Stream Ciphers and Application to Grain v1. , 2016, , .		10
35	Efficient Implementations for Practical Linear Cryptanalysis and Its Application to FEAL-8X. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2016, E99.A, 31-38.	0.2	0
36	Bit-Based Division Property and Application to Simon Family. Lecture Notes in Computer Science, 2016, , 357-377.	1.0	113

#	Article	IF	Citations
37	Wide Trail Design Strategy for Binary MixColumns. Lecture Notes in Computer Science, 2016, , 467-484.	1.0	0
38	Compact Representation for Division Property. Lecture Notes in Computer Science, 2016, , 19-35.	1.0	6
39	Nonlinear Invariant Attack. Lecture Notes in Computer Science, 2016, , 3-33.	1.0	27
40	Structural Evaluation by Generalized Integral Property. Lecture Notes in Computer Science, 2015, , 287-314.	1.0	172
41	Integral Cryptanalysis on Full MISTY1. Lecture Notes in Computer Science, 2015, , 413-432.	1.0	61
42	Upper Bounds for the Security of Several Feistel Networks. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2015, E98.A, 39-48.	0.2	0
43	Fast Fourier Transform Key Recovery for Integral Attacks. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2015, E98.A, 1944-1952.	0.2	3
44	How Much Can Complexity of Linear Cryptanalysis Be Reduced?. Lecture Notes in Computer Science, 2015, , 117-131.	1.0	1
45	FFT Key Recovery for Integral Attack. Lecture Notes in Computer Science, 2014, , 64-81.	1.0	8
46	Cryptanalysis of Reduced-Round SIMON32 and SIMON48. Lecture Notes in Computer Science, 2014, , 143-160.	1.0	48
47	Practical Cryptanalysis of a Public-Key Encryption Scheme Based on New Multivariate Quadratic Assumptions. Lecture Notes in Computer Science, 2014, , 446-464.	1.0	4
48	Upper Bounds for the Security of Several Feistel Networks. Lecture Notes in Computer Science, 2013, , 302-317.	1.0	6
49	New Property of Diffusion Switching Mechanism on CLEFIA and Its Application to DFA. Lecture Notes in Computer Science, 2013, , 99-114.	1.0	1
50	Falsification Attacks against WPA-TKIP in a Realistic Environment. IEICE Transactions on Information and Systems, 2012, E95-D, 588-595.	0.4	14
51	Proposal of a Secure WEP Operation against Existing Key Recovery Attacks and its Evaluation. , 2012, , .		6
52	Cryptanalysis for RC4 and Breaking WEP/WPA-TKIP. IEICE Transactions on Information and Systems, 2011, E94-D, 2087-2094.	0.4	8
53	Links between Division Property and Other Cube Attack Variants. IACR Transactions on Symmetric Cryptology, 0, , 363-395.	0.0	3