Vincent Rijmen

List of Publications by Year
in descending order

133 papers	6,319 citations	109321 35 h-index	71685 76 g-index
145 all docs	145 docs citations	145 times ranked	1924 citing authors

#	Article	IF	Citations
1	The Design of Rijndael. Information Security and Cryptography, 2002, , .	0.3	1,681
2	The block cipher Square. Lecture Notes in Computer Science, 1997, , 149-165.	1.3	445
3	Secure Hardware Implementation of Nonlinear Functions in the Presence of Glitches. Journal of Cryptology, 2011, 24, 292-321.	2.8	213
4	A Side-Channel Analysis Resistant Description of the AES S-Box. Lecture Notes in Computer Science, 2005, , 413-423.	1.3	200
5	The Advanced Encryption Standard Process. Information Security and Cryptography, 2002, , 1-8.	0.3	183
6	The Block Cipher Rijndael. Lecture Notes in Computer Science, 2000, , 277-284.	1.3	153
7	The cipher SHARK. Lecture Notes in Computer Science, 1996, , 99-111.	1.3	124
8	RECTANGLE: a bit-slice lightweight block cipher suitable for multiple platforms. Science China Information Sciences, 2015, 58, 1-15.	4.3	115
9	The Wide Trail Design Strategy. Lecture Notes in Computer Science, 2001, , 222-238.	1.3	115
10	Higher-Order Threshold Implementations. Lecture Notes in Computer Science, 2014, , 326-343.	1.3	114
11	Linear hulls with correlation zero and linear cryptanalysis of block ciphers. Designs, Codes, and Cryptography, 2014, 70, 369-383.	1.6	106
12	Known-Key Distinguishers for Some Block Ciphers. , 2007, , 315-324.		96
13	Rebound Distinguishers: Results on the Full Whirlpool Compression Function. Lecture Notes in Computer Science, 2009, , 126-143.	1.3	95
14	Toward secure public-key blockwise fragile authentication watermarking. IET Computer Vision, 2002, 149, 57.	1.3	91
15	A More Efficient AES Threshold Implementation. Lecture Notes in Computer Science, 2014, , 267-284.	1.3	85
16	A Navigation Message Authentication Proposal for the Galileo Open Service. Navigation, Journal of the Institute of Navigation, 2016, 63, 85-102.	2.8	83
17	Analysis Methods for (Alleged) RC4. Lecture Notes in Computer Science, 1998, , 327-341.	1.3	76
18	The Design of Rijndael. Information Security and Cryptography, 2020, , .	0.3	73

#	Article	IF	Citations
19	Improved Impossible Differential Cryptanalysis of 7-Round AES-128. Lecture Notes in Computer Science, 2010, , 282-291.	1.3	69
20	Threshold Implementations of All 3 Ã—3 and 4 Ã—4 S-Boxes. Lecture Notes in Computer Science, 2012, , 76-91.	1.3	67
21	ALE: AES-Based Lightweight Authenticated Encryption. Lecture Notes in Computer Science, 2014, , 447-466.	1.3	59
22	Probability distributions of correlation and differentials in block ciphers. Journal of Mathematical Cryptology, 2007, 1, .	0.7	56
23	Links Among Impossible Differential, Integral and Zero Correlation Linear Cryptanalysis. Lecture Notes in Computer Science, 2015, , 95-115.	1.3	53
24	Secure Hardware Implementation of Non-linear Functions in the Presence of Glitches. Lecture Notes in Computer Science, 2009, , 218-234.	1.3	52
25	Trade-Offs for Threshold Implementations Illustrated on AES. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 2015, 34, 1188-1200.	2.7	48
26	Cryptanalysis of Reduced-Round SIMON32 and SIMON48. Lecture Notes in Computer Science, 2014, , 143-160.	1.3	48
27	Masking AES with $$d+1$$ Shares in Hardware. Lecture Notes in Computer Science, 2016, , 194-212.	1.3	41
28	Low-Data Complexity Attacks on AES. IEEE Transactions on Information Theory, 2012, 58, 7002-7017.	2.4	40
29	Does Coupling Affect the Security of Masked Implementations?. Lecture Notes in Computer Science, 2017, , 1-18.	1.3	40
30	Analysis of Step-Reduced SHA-256. Lecture Notes in Computer Science, 2006, , 126-143.	1.3	40
31	Exploiting Coding Theory for Collision Attacks on SHA-1. Lecture Notes in Computer Science, 2005, , 78-95.	1.3	37
32	Threshold implementations of small S-boxes. Cryptography and Communications, 2015, 7, 3-33.	1.4	36
33	A New MAC Construction ALRED and a Specific Instance ALPHA-MAC. Lecture Notes in Computer Science, 2005, , 1-17.	1.3	34
34	A family of trapdoor ciphers. Lecture Notes in Computer Science, 1997, , 139-148.	1.3	32
35	Masking AES With d+1 Shares in Hardware. , 2016, , .		32
36	Automatic Search of Linear Trails in ARX with Applications to SPECK and Chaskey. Lecture Notes in Computer Science, 2016, , 485-499.	1.3	30

#	Article	IF	Citations
37	Differential Analysis of the LED Block Cipher. Lecture Notes in Computer Science, 2012, , 190-207.	1.3	30
38	Provable Security Evaluation of Structures Against Impossible Differential and Zero Correlation Linear Cryptanalysis. Lecture Notes in Computer Science, 2016, , 196-213.	1.3	30
39	Division cryptanalysis of block ciphers with a binary diffusion layer. IET Information Security, 2019, 13, 87-95.	1.7	29
40	Plateau characteristics. IET Information Security, 2007, 1, 11.	1.7	27
41	The Rebound Attack and Subspace Distinguishers: Application to Whirlpool. Journal of Cryptology, 2015, 28, 257-296.	2.8	27
42	Efficient and First-Order DPA Resistant Implementations of Keccak. Lecture Notes in Computer Science, 2014, , 187-199.	1.3	27
43	New Insights on AES-Like SPN Ciphers. Lecture Notes in Computer Science, 2016, , 605-624.	1.3	27
44	On the Collision Resistance of RIPEMD-160. Lecture Notes in Computer Science, 2006, , 101-116.	1.3	26
45	Rotation symmetry in algebraically generated cryptographic substitution tables. Information Processing Letters, 2008, 106, 246-250.	0.6	26
46	Whirlwind: a new cryptographic hash function. Designs, Codes, and Cryptography, 2010, 56, 141-162.	1.6	25
47	On Authentication with HMAC and Non-random Properties. Lecture Notes in Computer Science, 2007, , 119-133.	1.3	25
48	Cryptography on smart cards. Computer Networks, 2001, 36, 423-435.	5.1	24
49	Computational aspects of the expected differential probability of 4-round AES and AES-like ciphers. Computing (Vienna/New York), 2009, 85, 85-104.	4.8	24
50	Attack on Six Rounds of CRYPTON. Lecture Notes in Computer Science, 1999, , 46-59.	1.3	23
51	Generalisation of Hadamard matrix to generate involutory MDS matrices for lightweight cryptography. IET Information Security, 2018, 12, 348-355.	1.7	22
52	A New Classification of 4-bit Optimal S-boxes and Its Application to PRESENT, RECTANGLE and SPONGENT. Lecture Notes in Computer Science, 2015, , 494-515.	1.3	22
53	On Weaknesses of Nonâ€“surjective Round Functions. Designs, Codes, and Cryptography, 1997, 12, 253-266.	1.6	20
54	Two Attacks on Reduced IDEA. Lecture Notes in Computer Science, 1997, , 1-13.	1.3	20

#	Article	IF	Citations
55	On the Design and Security of RC2. Lecture Notes in Computer Science, 1998, , 206-221.	1.3	19
56	The First 10 Years of Advanced Encryption. IEEE Security and Privacy, 2010, 8, 72-74.	1.2	18
57	Key Difference Invariant Bias in Block Ciphers. Lecture Notes in Computer Science, 2013, , 357-376.	1.3	18
58	Whirlpool. , 2011, , 1384-1385.		17
59	Rebound Attack on Reduced-Round Versions of JH. Lecture Notes in Computer Science, 2010, , 286-303.	1.3	17
60	AES and the Wide Trail Design Strategy. Lecture Notes in Computer Science, 2002, , 108-109.	1.3	16
61	Using Normal Bases for Compact Hardware Implementations of the AES S-Box. Lecture Notes in Computer Science, 2008, , 236-245.	1.3	16
62	Cryptanalysis of the CFB mode of the DES with a reduced number of rounds. , 1993, , 212-223.		15
63	On the Decorrelated Fast Cipher (DFC) and Its Theory. Lecture Notes in Computer Science, 1999, , 81-94.	1.3	15
64	Weaknesses in the HAS-V Compression Function. , 2007, , 335-345.		15
65	Cryptanalysis of the Tiger Hash Function. , 2007, , 536-550.		15
66	The MESH Block Ciphers. Lecture Notes in Computer Science, 2004, , 458-473.	1.3	14
67	The Impact of Carries on the Complexity of Collision Attacks on SHA-1. Lecture Notes in Computer Science, 2006, , 278-292.	1.3	14
68	Efficient and First-Order DPA Resistant Implementations of Keccak. Lecture Notes in Computer Science, 2014, , 187-199.	1.3	14
69	Analysis and Recommendations for MAC and Key Lengths in Delayed Disclosure GNSS Authentication Protocols. IEEE Transactions on Aerospace and Electronic Systems, 2021, 57, 1827-1839.	4.7	13
70	Improved characteristics for differential cryptanalysis of hash functions based on block ciphers. Lecture Notes in Computer Science, 1995, , 242-248.	1.3	13
71	VerMI: Verification Tool for Masked Implementations. , 2018, , .		12
72	A new matrix form to generate all 3â€¯Ã—â€¯3 involutory MDS matrices over <mml:math xmlns:mml="http://www.w3.org/1998/Math/MathML" altimg="si1.gif" overflow="scroll"><mml:msub><mml:mrow><mml:mi mathvariant="double-struck">F</mml:mi></mml:mrow><mml:mrow><mml:msup><mml:mrow><mml:mn>2</mml:mn></mml:mrow><r Information Processing Letters, 2019, 147, 61-68.	0.6	12

#	Article	IF	Citations
73	Security analysis of the message authenticator algorithm (MAA). European Transactions on Telecommunications, 1997, 8, 455-470.	1.2	11
74	Linear Frameworks for Block Ciphers. Designs, Codes, and Cryptography, 2001, 22, 65-87.	1.6	11
75	Recent Developments in the Design of Conventional Cryptographic Algorithms. Lecture Notes in Computer Science, 1998, , 105-130.	1.3	11
76	Correlated Keystreams in Moustique. , 2008, , 246-257.		11
77	Analysis of the Hash Function Design Strategy Called SMASH. IEEE Transactions on Information Theory, 2008, 54, 3647-3655.	2.4	10
78	Nonlinear diffusion layers. Designs, Codes, and Cryptography, 2018, 86, 2469-2484.	1.6	10
79	Improved Square Attacks against Reduced-Round Hierocrypt. Lecture Notes in Computer Science, 2002, , 165-173.	1.3	10
80	Collision Attack on 5 Rounds of GrÃ¸stl. Lecture Notes in Computer Science, 2015, , 509-521.	1.3	9
81	Threshold Implementations in the Robust Probing Model. , 2019, , .		9
82	Rhythmic Keccak: SCA Security and Low Latency in HW. Iacr Transactions on Cryptographic Hardware and Embedded Systems, 0, , 269-290.	0.0	9
83	Colliding Message Pair for 53-Step HAS-160. , 2007, , 324-334.		9
84	A new counting method to bound the number of active S-boxes in Rijndael and 3D. Designs, Codes, and Cryptography, 2017, 83, 327-343.	1.6	8
85	Decomposition of permutations in a finite field. Cryptography and Communications, 2019, 11, 379-384.	1.4	8
86	Second Preimages for SMASH. Lecture Notes in Computer Science, 2006, , 101-111.	1.3	8
87	Producing Collisions for PANAMA. Lecture Notes in Computer Science, 2002, , 37-51.	1.3	8
88	Breaking a New Hash Function Design Strategy Called SMASH. Lecture Notes in Computer Science, 2006, , 233-244.	1.3	8
89	New criteria for linear maps in AES-like ciphers. Cryptography and Communications, 2009, 1, 47-69.	1.4	6
90	Refinements of the ALRED construction and MAC security claims. IET Information Security, 2010, 4, 149.	1.7	6

#	Article	IF	Citations
91	Memoryless near-collisions via coding theory. Designs, Codes, and Cryptography, 2012, 62, 1-18.	1.6	6
92	Impact analysis of SBAS authentication. Navigation, Journal of the Institute of Navigation, 2018, 65, 517-532.	2.8	6
93	On the automorphisms and isomorphisms of MDS matrices and their efficient implementations. Turkish Journal of Electrical Engineering and Computer Sciences, 2020, 28, 275-287.	1.4	6
94	Differential Cryptanalysis of Q. Lecture Notes in Computer Science, 2002, , 174-186.	1.3	6
95	Cryptanalysis of McGuffin. Lecture Notes in Computer Science, 1995, , 353-358.	1.3	6
96	A Simple Key-Recovery Attack on McOE-X. Lecture Notes in Computer Science, 2012, , 23-31.	1.3	6
97	Impact of Rotations in SHA-1 and Related Hash Functions. Lecture Notes in Computer Science, 2006, , 261-275.	1.3	6
98	Equivalent Keys of HPC. Lecture Notes in Computer Science, 1999, , 29-42.	1.3	5
99	Numerical solvers and cryptanalysis. Journal of Mathematical Cryptology, 2009, 3, .	0.7	5
100	Green Cryptography: Cleaner Engineering through Recycling. IEEE Security and Privacy, 2009, 7, 71-73.	1.2	5
101	Improved Fault Analysis on SIMON Block Cipher Family. , 2016, , .		5
102	Impossible meet-in-the-middle fault analysis on the LED lightweight cipher in VANETs. Science China Information Sciences, 2018, 61, 1.	4.3	5
103	Improved Impossible Differential Attacks on Large-Block Rijndael. Lecture Notes in Computer Science, 2013, , 126-140.	1.3	5
104	Representations and Rijndael Descriptions. Lecture Notes in Computer Science, 2005, , 148-158.	1.3	4
105	The phantom of differential characteristics. Designs, Codes, and Cryptography, 2020, 88, 2289-2311.	1.6	4
106	Security of a Wide Trail Design. Lecture Notes in Computer Science, 2002, , 1-11.	1.3	4
107	Rotational Cryptanalysis on MAC Algorithm Chaskey. Lecture Notes in Computer Science, 2020, , 153-168.	1.3	4
108	A Bit-Vector Differential Model for the Modular Addition by a Constant. Lecture Notes in Computer Science, 2020, , 385-414.	1.3	4

#	Article	IF	Citations
109	CIPHERTEXT-ONLY ATTACK ON AKELARRE. Cryptologia, 2000, 24, 135-147.	0.5	3
110	Algebraic cryptanalysis of a small-scale version of stream cipher Lex. IET Information Security, 2010, 4, 49.	1.7	3
111	Constructions of S-boxes with uniform sharing. Cryptography and Communications, 2019, 11, 385-398.	1.4	3
112	Proposing an MILP-based method for the experimental verification of difference-based trails: application to SPECK, SIMECK. Designs, Codes, and Cryptography, 2021, 89, 2113-2155.	1.6	3
113	WARX: efficient white-box block cipher based on ARX primitives and random MDS matrix. Science China Information Sciences, 2022, 65, 1.	4.3	3
114	Efficient methods to generate cryptographically significant binary diffusion layers. IET Information Security, 2017, 11, 177-187.	1.7	2
115	Guards in Action: First-Order SCA Secure Implementations of Ketje Without Additional Randomness. , 2018, , .		2
116	New observations on invariant subspace attack. Information Processing Letters, 2018, 138, 27-30.	0.6	2
117	Revisiting the Wrong-Key-Randomization Hypothesis. Journal of Cryptology, 2020, 33, 567-594.	2.8	2
118	Optimal Covering Codes for Finding Near-Collisions. Lecture Notes in Computer Science, 2011, , 187-197.	1.3	2
119	A bit-vector differential model for the modular addition by a constant and its applications to differential and impossible-differential cryptanalysis. Designs, Codes, and Cryptography, 2022, 90, 1797-1855.	1.6	2
120	Periodic Properties of Counter Assisted Stream Ciphers. Lecture Notes in Computer Science, 2004, , 39-53.	1.3	1
121	Equivalent descriptions for the DES. Electronics Letters, 2004, 40, 237.	1.0	1
122	Green Cryptography: Cleaner Engineering through Recycling, Part 2. IEEE Security and Privacy, 2009, 7, 64-65.	1.2	1
123	Extracts from the SHA-3 Competition. Lecture Notes in Computer Science, 2013, , 81-85.	1.3	1
124	Design Trade-offs in Threshold Implementations. , 2019, , .		1
125	Collisions for the WIDEA-8 Compression Function. Lecture Notes in Computer Science, 2013, , 162-173.	1.3	1
126	Correlation Distribution Analysis of a Two-Round Key-Alternating Block Cipher. Tatra Mountains Mathematical Publications, 2019, 73, 109-130.	0.2	1

#	Article	IF	Citations
127	Theory of Implementation Security Workshop (TIs 2016). , 2016, , .		0
128	Guards in action: First-order SCA secure implementations of KETJE without additional randomness. Microprocessors and Microsystems, 2019, 71, 102859.	2.8	0
129	Proving Key Usage. Lecture Notes in Computer Science, 2005, , 65-72.	1.3	0
130	Conventional Cryptographic Primitives. , 2010, , 207-227.		0
131	Collision Attack on the Hamsi-256 Compression Function. Lecture Notes in Computer Science, 2012, , 156-171.	1.3	0
132	TIS'19. , 2019, , .		0
133	Second Preimages for Iterated Hash Functions and Their Implications on MACs. , 2007, , 68-81.		0