Svetla PEtkova-Nikova

List of Publications by Year
in descending order

43	1,451	471061 17	433756 31
papers	citations	h-index	g-index

47	47	47	460
all docs	docs citations	times ranked	citing authors

#	Article	IF	Citations
1	Resilient uniformity: applying resiliency in masking. Cryptography and Communications, 2022, 14, 41-58.	0.9	1
2	Letâ€™s Tessellate: Tiling for Security Against Advanced Probe and Fault Adversaries. Lecture Notes in Computer Science, 2021, , 181-195.	1.0	1
3	Exploring the storj network. , 2021, , .		9
4	LLTI: Low-Latency Threshold Implementations. IEEE Transactions on Information Forensics and Security, 2021, , 1-1.	4.5	1
5	My Gadget Just Cares for Me - How NINA Can Prove Security Against Combined Attacks. Lecture Notes in Computer Science, 2020, , 35-55.	1.0	9
6	Authenticated and auditable data sharing via smart contract. , 2020, , .		5
7	Decomposition of permutations in a finite field. Cryptography and Communications, 2019, 11, 379-384.	0.9	8
8	Guards in action: First-order SCA secure implementations of KETJE without additional randomness. Microprocessors and Microsystems, 2019, 71, 102859.	1.8	0
9	Constructions of S-boxes with uniform sharing. Cryptography and Communications, 2019, 11, 385-398.	0.9	3
10	TIS'19. , 2019, , .		0
11	A Privacy-Preserving Device Tracking System Using a Low-Power Wide-Area Network. Lecture Notes in Computer Science, 2018, , 347-369.	1.0	2
12	Guards in Action: First-Order SCA Secure Implementations of Ketje Without Additional Randomness. , 2018, , .		2
13	VerMI: Verification Tool for Masked Implementations. , 2018, , .		12
14	CAPA: The Spirit of Beaver Against Physical Attacks. Lecture Notes in Computer Science, 2018, , 121-151.	1.0	21
15	Practically Efficient Secure Distributed Exponentiation Without Bit-Decomposition. Lecture Notes in Computer Science, 2018, , 291-309.	1.0	4
16	Does Coupling Affect the Security of Masked Implementations?. Lecture Notes in Computer Science, 2017, , 1-18.	1.0	40
17	Securing the PRESENT Block Cipher Against Combined Side-Channel Analysis and Fault Attacks. IEEE Transactions on Very Large Scale Integration (VLSI) Systems, 2017, 25, 3291-3301.	2.1	25
18	Masking AES With d+1 Shares in Hardware. , 2016, , .		32

#	Article	IF	Citations
19	Theory of Implementation Security Workshop (TIs 2016). , 2016, , .		0
20	More Efficient Private Circuits II through Threshold Implementations. , 2016, , .		12
21	Masking AES with $$d+1$$ Shares in Hardware. Lecture Notes in Computer Science, 2016, , 194-212.	1.0	41
22	Reversed genetic algorithms for generation of bijective s-boxes with good cryptographic properties. Cryptography and Communications, 2016, 8, 247-276.	0.9	57
23	Higher-Order Threshold Implementation of the AES S-Box. Lecture Notes in Computer Science, 2016, , 259-272.	1.0	23
24	Trade-Offs for Threshold Implementations Illustrated on AES. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 2015, 34, 1188-1200.	1.9	48
25	Threshold implementations of small S-boxes. Cryptography and Communications, 2015, 7, 3-33.	0.9	36
26	Consolidating Masking Schemes. Lecture Notes in Computer Science, 2015, , 764-783.	1.0	128
27	TuLP: A Family of Lightweight Message Authentication Codes for Body Sensor Networks. Journal of Computer Science and Technology, 2014, 29, 53-68.	0.9	17
28	A More Efficient AES Threshold Implementation. Lecture Notes in Computer Science, 2014, , 267-284.	1.0	85
29	Efficient and First-Order DPA Resistant Implementations of Keccak. Lecture Notes in Computer Science, 2014, , 187-199.	1.0	27
30	Higher-Order Threshold Implementations. Lecture Notes in Computer Science, 2014, , 326-343.	1.0	114
31	Threshold Implementations of All 3 Ã—3 and 4 Ã—4 S-Boxes. Lecture Notes in Computer Science, 2012, , 76-91.	1.0	67
32	Secure Hardware Implementation of Nonlinear Functions in the Presence of Glitches. Journal of Cryptology, 2011, 24, 292-321.	2.1	213
33	Whirlwind: a new cryptographic hash function. Designs, Codes, and Cryptography, 2010, 56, 141-162.	1.0	25
34	Galois geometries and applications. Designs, Codes, and Cryptography, 2010, 56, 85-86.	1.0	0
35	Secure Hardware Implementation of Non-linear Functions in the Presence of Glitches. Lecture Notes in Computer Science, 2009, , 218-234.	1.0	52
36	Using Normal Bases for Compact Hardware Implementations of the AES S-Box. Lecture Notes in Computer Science, 2008, , 236-245.	1.0	16

#	Article	IF	Citations
37	A Modification of Jarecki and Saxena Proactive RSA Signature Scheme. , 2007, , .		0
38	A Weakness in Some Oblivious Transfer and Zero-Knowledge Protocols. Lecture Notes in Computer Science, 2006, , 348-363.	1.0	0
39	Improvement of the Delsarte Bound for Ï„-Designs When It Is Not the Best Bound Possible. Designs, Codes, and Cryptography, 2003, 28, 201-222.	1.0	6
40	On the non-minimal codewords in binary Reedâ€“Muller codes. Discrete Applied Mathematics, 2003, 128, 65-74.	0.5	10
41	On lower bounds on the size of designs in compact symmetric spaces of rank 1. Archiv Der Mathematik, 1997, 68, 81-88.	0.3	6
42	Rhythmic Keccak: SCA Security and Low Latency in HW. Iacr Transactions on Cryptographic Hardware and Embedded Systems, 0, , 269-290.	0.0	9
43	M&M: Masks and Macs against Physical Attacks. Iacr Transactions on Cryptographic Hardware and Embedded Systems, 0, , 25-50.	0.0	12