Roman Oliynykov

List of Publications by Year
in descending order

Source: https://exaly.com/author-pdf/4068460/publications.pdf

Version: 2024-02-01

29 papers	904 citations	1306789 7 h-index	1372195 10 g-index
30 all docs	30 docs citations	30 times ranked	672 citing authors

#	Article	IF	Citations
1	Ouroboros: A Provably Secure Proof-of-Stake Blockchain Protocol. Lecture Notes in Computer Science, 2017, , 357-388.	1.0	665
2	Zendoo: a zk-SNARK Verifiable Cross-Chain Transfer Protocol Enabling Decoupled and Decentralized Sidechains. , 2020, , .		44
3	Influence of addition modulo 2 n on algebraic attacks. Cryptography and Communications, 2016, 8, 277-289.	0.9	26
4	A Prospective Lightweight Block Cipher for Green IT Engineering. Studies in Systems, Decision and Control, 2019, , 95-112.	0.8	26
5	A Method for Security Estimation of the Spn-Based Block Cipher Against Related-Key Attacks. Tatra Mountains Mathematical Publications, 2014, 60, 25-45.	0.1	19
6	Properties of Linear Transformations for Symmetric Block Ciphers on the Basis of MDS-Codes. , 2011, , .		16
7	Improvement of the high nonlinear S-boxes generation method. , 2016, , .		15
8	Optimization of the High Nonlinear S-Boxes Generation Method. Tatra Mountains Mathematical Publications, 2017, 70, 93-105.	0.1	12
9	Improvement for distinguisher efficiency of the 3-round Feistel network and a random permutation. , 2011, , .		11
10	Analysis of splitting attacks on Bitcoin and GHOST consensus protocols. , 2017, , .		9
11	Blockchain Technologies: Probability of Double-Spend Attack on a Proof-of-Stake Consensus. Sensors, 2021, 21, 6408.	2.1	9
12	Comparison of Modern Network Attacks on TLS Protocol. , 2018, , .		8
13	Decreasing security threshold against double spend attack in networks with slow synchronization. Computer Communications, 2020, 154, 75-81.	3.1	8
14	Probability Models of Distributed Proof Generation for zk-SNARK-Based Blockchains. Mathematics, 2021, 9, 3016.	1.1	8
15	Results of Ukrainian national public cryptographic competition. Tatra Mountains Mathematical Publications, 2010, 47, 99-113.	0.1	7
16	Open problems of proving security of ARX-based ciphers to differential cryptanalysis. , 2017, , .		6
17	Search for one-round differential characteristics of lighweight block cipher Cypress-256. , 2018, , .		4
18	Decreasing Security Threshold Against Double Spend Attack in Networks with Slow Synchronization. , 2019, , .		4

#	Article	IF	Citations
19	Comparative Analysis of Consensus Algorithms Using a Directed Acyclic Graph Instead of a Blockchain, and the Construction of Security Estimates of Spectre Protocol Against Double Spend Attack. Lecture Notes on Data Engineering and Communications Technologies, 2022, , 203-224.	0.5	3
20	Number of confirmation blocks for Bitcoin and GHOST consensus protocols on networks with delayed message delivery. , 2018, , .		2
21	An Approach to Search for Multi-Round Differential Characteristics of Cypress-256. , 2018, , .		1
22	Comparing Performances of Cypress Block Cipher and Modern Lighweight Block Ciphers on Different Platforms. , 2019, , .		1
23	The Method of Searching for Differential Trails of ARX-based Block Cipher Cypress. , 2020, , .		0
24	Method and technique of formal design of complex information security system in information and telecommunication systems. Radiotekhnika, 2020, , 91-96.	0.1	0
25	Upper bound probability of double spend attack on SPECTRE. , 2020, , .		0
26	On Generation of Cycles, Chains and Graphs of Pairing-Friendly Elliptic Curves. , 2020, , .		0
27	Analysis and Research of Threat, Attacker and Security Models of Data Depersonalization in Decentralized Networks. Lecture Notes on Data Engineering and Communications Technologies, 2022, , 71-88.	0.5	0
28	Methods of Ensuring Privacy in a Decentralized Environment. Lecture Notes on Data Engineering and Communications Technologies, 2022, , 1-32.	0.5	0
29	Methods and means of deanonymization of transactions in blockchain. Radiotekhnika, 2021, , 52-58.	0.1	0