Lyudmila Kovalchuk

List of Publications by Year
in descending order

20	58	1683354 5	1719596 7
papers	citations	h-index	g-index

21	21	21	40
all docs	docs citations	times ranked	citing authors

#	Article	IF	Citations
1	Analysis of splitting attacks on Bitcoin and GHOST consensus protocols. , 2017, , .		9
2	Blockchain Technologies: Probability of Double-Spend Attack on a Proof-of-Stake Consensus. Sensors, 2021, 21, 6408.	2.1	9
3	Decreasing security threshold against double spend attack in networks with slow synchronization. Computer Communications, 2020, 154, 75-81.	3.1	8
4	Probability Models of Distributed Proof Generation for zk-SNARK-Based Blockchains. Mathematics, 2021, 9, 3016.	1.1	8
5	Cryptographic Properties of a New National Encryption Standard of Ukraine. Cybernetics and Systems Analysis, 2016, 52, 351-364.	0.4	5
6	Supersingular Twisted Edwards Curves Over Prime Fields. I. Supersingular Twisted Edwards Curves with j-Invariants Equal to Zero and 123. Cybernetics and Systems Analysis, 2019, 55, 347-353.	0.4	5
7	Upper-bound estimation of the average probabilities of integer-valued differentials in the composition of key adder, substitution block, and shift operator. Cybernetics and Systems Analysis, 2010, 46, 936-944.	0.4	4
8	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
9	Analysis of mixing properties of the operations of modular addition and bitwise addition defined on one carrier. Cybernetics and Systems Analysis, 2011, 47, 741-753.	0.4	2
10	Upper Bounds for the Average Probabilities of Difference Characteristics of Block Ciphers with Alternation of Markov Transformations and Generalized Markov Transformations. Cybernetics and Systems Analysis, 2014, 50, 386-393.	0.4	2
11	Exact Number of Elliptic Curves in the Canonical Form, Which are Isomorphic to Edwards Curves Over Prime Field. Cybernetics and Systems Analysis, 2015, 51, 165-172.	0.4	2
12	Achieving Security in Proof-of-Proof Protocol with Non-Zero Synchronization Time. Mathematics, 2022, 10, 2422.	1.1	1
13	A construction of the logarithm of a process on a matrix Lie group. Ukrainian Mathematical Journal, 1992, 44, 1371-1377.	0.1	0
14	Semimartingales with values on groups and lie algebras. Ukrainian Mathematical Journal, 1993, 45, 269-276.	0.1	0
15	Upper-bound estimates for the average probabilities of integer differentials of round functions of certain block ciphers. Cybernetics and Systems Analysis, 2012, 48, 701-710.	0.4	0
16	Mixing Properties of Operations Defined on the Set of N-Dimensional Vectors Over a Prime Finite Field. Cybernetics and Systems Analysis, 2014, 50, 603-612.	0.4	0
17	Algorithms for Base Point Generation on an Edwards Curve with the Use of Point Divisibility Criteria. Cybernetics and Systems Analysis, 2016, 52, 674-683.	0.4	0
18	Evaluation of the efficiency of differential addition of points of curves in the generalized Edwards form. Radiotekhnika, 2020, , 50-59.	0.1	0

#	Article	IF	Citations
19	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
20	Methods of Ensuring Privacy in a Decentralized Environment. Lecture Notes on Data Engineering and Communications Technologies, 2022, , 1-32.	0.5	0