CEUR-WS.org/Vol-2654/paper64.pdf

Experimental Research of the Developed Methods of Arithmetic Operations in Cryptographic Transformations according to the ECDSA Scheme

Andrew Okhrimenko [0000-0001-8270-2863] and Vladyslav Kovtun [0000-0002-4303-3510]

CIPHER PRO LLC, Kyiv, Ukraine
andrew.okhrimenko@gmail.com

Abstract. The national PKI regulates the use of a qualified electronic signature according to the algorithms of DSTU 4145-2002, ECDSA, DSA and RSA. Operations of creating and verifying electronic signature are based on various mathematical methods: transformation in a ring of integers, field of integers and polynomials, in a group of points of an elliptic curve. All these transformations are impossible without arithmetic operations on integers. In this work authors presented experimental results for implementation previously proposed methods of integers representation with delayed carry form and methods of arithmetic operations on numbers in this representation for ES cryptographic transformations according to the ECDSA scheme. To test the proposed methods of ECDSA cryptosystem operations over a prime GF (p) field, two software collections were prepared – using 32-bit machine words, and using 64-bit machine words. To compare the obtained results, operations without the use of the proposed methods were used as a reference. The comparison was made by comparing the average execution time of 1 million iterations of operations in the software implementation. Based on the analysis results it can be concluded that the proposed methods are more effective than classical.

Keywords: cybersecurity, cryptography, electronic signature, arithmetic operations, delayed carry form, ECDSA.

1 Introduction

Information technologies playing an increasingly important role in modern human and business relations. They can improve the efficiency of information exchange, the speed of decision-making, quality of goods and services, expand business areas, develop new markets and compete. As a result of information exchange, there is a need to ensure the security of this information. Traditionally to build information security systems consider a standard model of information security [1, 2], which consisting of the following categories: confidentiality, integrity and availability. In turn, this list, of course, expands the categories of authentication, integrity and non-repudiation [3]. These categories, which are part of the information security model, are implemented

Copyright © 2020 for this paper by its authors. Use permitted under Creative Commons License Attribution 4.0 International (CC BY 4.0). CybHyg-2019: International Workshop on Cyber Hygiene, Kyiv, Ukraine, November 30, 2019.

by the following services: encryption, electronic signature, development of a shared secret. Each of these services, separately, is not able to fully solve all the problems of information security, however, their use in the complex allows you to solve most of them.

To automate different activities, there is a need to build an electronic document management system, for which the categories of integrity, authenticity and irrefutability are represented greatest interest. These categories are successfully implemented using an electronic signature (ES). ES application areas are quite diverse – electronic document management systems for various purposes, reporting systems for regulatory authorities, Internet banking systems, public service portals, government registries, electronic bidding and public procurement systems, and others. This is dictated by the main property of ES – it can be used as an analogue of a handwritten signature or seal on a paper document.

With the ratification of the Association Agreement between Ukraine and the European Union on September 16, 2014, our country has committed itself to harmonize its own legislation with EU legislation. In particular, to bring the Law of Ukraine “About Electronic Digital Signature” in line with EU Regulation № 910/2014 “About electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC” (eIDAS) of 23 July 2014 year, which defines the basic requirements for providers of electronic signature and electronic identification services. Since the Law of Ukraine "On electronic digital signature" no longer meet the requirements of modern technology and the needs of consumers of electronic services, it was necessary to develop a new law, the purpose of which was to reform the legislation in the field of electronic digital signature taking into account the experience of the European Union, building a single area of trust based on a system of electronic trust services, recognition in Ukraine of electronic trust services provided by foreign providers of electronic trust services, which will ensure the active development of cross-border cooperation and integration of Ukraine into the global electronic information space. Such a law became the Law of Ukraine "On electronic trust services", which was adopted on October 5, 2017 and entered into force on November 7, 2018 [4, 5].

The Law of Ukraine "On Electronic Trust Services" has expanded the list of services, which, in turn, opens more opportunities for the state, business and citizens: website authentication, electronic identification, creating an electronic document, imposition of a qualified electronic signature and seal, timestamp, storage of electronic signatures and seals [4, 5].

The international electronic signature algorithm ECDSA is approved for use and is actively used in the national public key infrastructure of Ukraine. ECDSA is based on transformations in a group of points of an elliptic curve over a binary field $GF(2^m)$ or a prime field GF(p), as well as operations on prime field elements GF(p) [6].

Every year the number of services provided in electronic form increases, which in turn leads to growth of services that support ES and also ES user’s. In turn, this leads to an increase in the number of documents with one or more ES that should be checked, and processed in a short time. Therefore, the development of methods to ensure the efficiency of ES creation and verification by increasing the productivity of cryptographic transformations is an urgent scientific and practical task.

2 Proposed method

The productivity of cryptographic transformations can be increased by increasing the speed of operations with integers. In turn, the speed of operations with integers can be significantly increase by postponing the transfer operation from senior digits to junior, and for a loan on the contrary – from junior digits to seniors [7, 15]. In previous works the authors proposed integers representation with delayed carry form (DCF) and methods of arithmetic operations on numbers in this representation [8, 9].

An integer in a delayed carry form representation is a sequence of machine words of *w*-bit size, each of which contains a block of *r* bit length allocated for the accumulation of hyphenation, and a block of *v* bit length filled with bits of the number in binary form (where $w = r + v$).

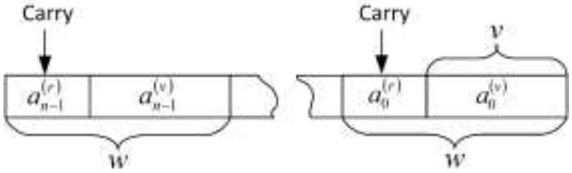

Fig. 1. Representation of integers in DCF

Specificity of the proposed DCF representation of integers is the absence of need to take into account transfers and loans, that allows to get rid of unnecessary operations of assignment and checks at implementation in high-level programming languages, and also from the register analysis of flags on possible transfer. In turn, this leads to increased efficiency of software implementation on processors with superscalar architecture and the capabilities of modern compilers in predicting transitions, parallel execution of commands, deployment of cycles, etc. The exception is the hyphen adjustment operation, which is performed sequentially from the lower machine words to the older ones. The following methods of arithmetic transformations with numbers in DCF-representation are offered by authors in previous works:

- method of addition (terms and sum in DCF-representation) and mixed addition;
- subtraction method (decrement, subtractor and difference in DCF representation) and mixed subtraction;
- method of shift to the left (number and result in DCF-representation) and mixed shift to the left (number in binary form, and result in DCF-representation);
- the method of shift to the right (number and result in DCF-representation) and mixed right-shift (number in binary form, and result in DCF-representation);
- multiplication method based on the Comba method;

- the method of elevation to the square;
- modulation method based on the Barrett method;
- division method based on Barrett's method;
- comparison method.

The proposed arithmetic operations were used in the implementation of cryptographic transformations of ES according to the ECDSA scheme.

3 Experimental research

Prime fields from NIST FIPS 186-3, namely P-192, P-224, P-256, P-384 and P-521 [10-14] are used for experimental researches of the offered methods of arithmetic operations in cryptographic transformations according to the ECDSA scheme [6].

To evaluate the effectiveness of the proposed methods, a software implementation was performed using Microsoft Visual Studio 2015 in C ++ programming language without the use of assembly inserts for the platform with Intel Core-i7 4770 3.40 GHz processor running Microsoft Windows 10 (x64).

To test the proposed methods of ECDSA cryptosystem operations over a prime GF (p) field, two software collections were prepared – using 32-bit machine words, and using 64-bit machine words. To compare the obtained results, operations without the use of the proposed methods were used as a reference. The comparison was made by comparing the average execution time of 1 million iterations of operations in the software implementation:

- using classical methods of arithmetic operations (original);
- using the proposed methods of arithmetic operations without parallelization (with improvements).

The use of parallelization in 2 or more streams is not considered, because the effect of their use is achieved at larger values of field size than those used in the cryptosystem ECDSA.

Experimental studies were performed for the main operations of the ECDSA cryptosystem over a prime GF (p) field:

- private key generation – is operations in a prime field of integers, modulo the order of the group – a prime number of common form;
- public key generation – is scalar multiplication by a fixed point ES (group generator);
- digest sign – is scalar multiplication by a fixed point ES (group generator);
- digest verify sign – is scalar multiplication by an arbitrary (public key) and a fixed point ES (group generator).

When generating a public key and creating a signature, scalar multiplication of a fixed (base) point is performed on the basis of the Lim-Lee algorithm using Chudnovsky projective coordinates [16-19].

It should be noted that the operations in the base field are performed modulo the prime number of a special kind – pseudomersen, and the operations in the field of the order of the base point, is modulo the prime number of the general form.

The values of these operations speed for the cryptosystem ECDSA on a prime field GF (p) are given in milliseconds.

Table 1 shows the results of operations speed measuring for ECDSA cryptosystem over a prime field GF (p) with and without the proposed methods using 32-bit machine words [20-24].

Table 1. The results of measuring the performance of ECDSA cryptosystem operations over a prime field GF(p) of different lengths using 32-bit machine words.

ECDSA (original)					
Operation/Base field	p192	p224	p256	p384	p521
Private key generation, ms	0,013	0,013	0,015	0,020	0,051
Public key generation, ms	0,410	0,681	1,360	3,030	4,775
Digest sign, ms	0,416	0,682	1,384	2,996	4,806
Digest verify sign, ms	0,420	0,694	1,400	3,100	4,937
ECDSA (with improvements)					
Operation/Base field	p192	p224	p256	p384	p521
Private key generation, ms	0,011	0,011	0,013	0,018	0,050
Public key generation, ms	0,403	0,642	1,330	2,863	4,604
Digest sign, ms	0,405	0,664	1,350	2,954	4,723
Digest verify sign, ms	0,408	0,680	1,370	3,072	4,856

To evaluate the effectiveness of the proposed methods using 32-bit machine words, the ratio of the measuring results for ECDSA cryptosystem operations is presented

To evaluate the effectiveness of the proposed methods using 32-bit machine words, the ratio of the results of measuring the operations of the ECDSA cryptosystem over a prime field GF (p) without using the proposed methods to the results using the proposed methods.

Table 2 shows the normalized results to demonstrate the effectiveness of the proposed methods. The effectiveness of the proposed methods for these operations:

- The private key generating operation is more efficient in 1.02-1.18 times for all fields under consideration.
- The public key generation operation is more efficient in 1.02-1.06 times efficient for all fields under consideration.
- The digest sign operation is more efficient in 1.01-1.03 times for all fields under consideration.
- The digest verify sign operation is more efficient in 1.01-1.03 times for all fields under consideration.

Table 2. Normalized results of measuring the speed of ECDSA cryptosystem operations over a prime field GF (p) of different lengths according to the results with and without proposed methods using 32-bit machine words.

Operation/Base field	p192	p224	p256	p384	p521
Private key generation	1,18	1,18	1,15	1,11	1,02
Public key generation	1,02	1,06	1,02	1,06	1,04
Digest sign	1,03	1,03	1,03	1,01	1,02
Digest verify sign	1,03	1,02	1,02	1,01	1,02

Table 3 shows the results of measuring the speed of operations of the cryptosystem ECDSA on a prime field GF (p) with and without the proposed methods for 64-bit machine words.

Table 3. The results of speed measuring for ECDSA cryptosystem operations over a prime field GF (p) of different lengths using 64-bit machine words.

ECDSA (original)					
Operation/Base field	p192	p224	p256	p384	p521
Private key generation, ms	0,0048	0,0068	0,0078	0,0137	0,0265
Public key generation, ms	0,1307	0,3079	0,4841	0,9165	1,0273
Digest sign, ms	0,1372	0,3345	0,4950	0,9830	1,0524
Digest verify sign, ms	0,1338	0,3558	0,5162	0,9905	1,0941
ECDSA (with improvements)					
Operation/Base field	p192	p224	p256	p384	p521
Private key generation, ms	0,0047	0,0064	0,0072	0,0132	0,0257
Public key generation, ms	0,1252	0,2991	0,4785	0,9096	1,0174
Digest sign, ms	0,1320	0,3262	0,4840	0,9333	1,0326
Digest verify sign, ms	0,1322	0,3442	0,5119	0,9561	1,0589

To evaluate the effectiveness of the proposed methods using 64-bit machine words, the ratio of the results of measuring the operations of the cryptosystem ECDSA over a prime field GF (p) without using the proposed methods to the results using the proposed methods.

Table 4 shows the normalized results to demonstrate the effectiveness of the proposed methods. The effectiveness of the proposed methods for these operations:

- The private key generating operation is more efficient in 1,02-1,08 times for all fields under consideration.
- The public key generation operation is more efficient in 1,01-1,04 times for all fields under consideration.
- The digest sign operation is more efficient in 1,02-1,05 times for all fields under consideration.
- The digest verify sign operation is more efficient in 1,01-1,04 times for all fields under consideration.

Table 4. Normalized results of speed measuring for ECDSA cryptosystem operations over a prime field GF (p) of different lengths on the results with and without the proposed methods for 64-bit machine words

Operation/Base field	p192	p224	p256	p384	p521
Private key generation	1,02	1,06	1,08	1,04	1,03
Public key generation	1,04	1,03	1,01	1,01	1,01
Digest sign	1,04	1,03	1,02	1,05	1,02
Digest verify sign	1,01	1,03	1,01	1,04	1,03

Based on the analysis results it can be concluded that the proposed methods are more effective than classical.

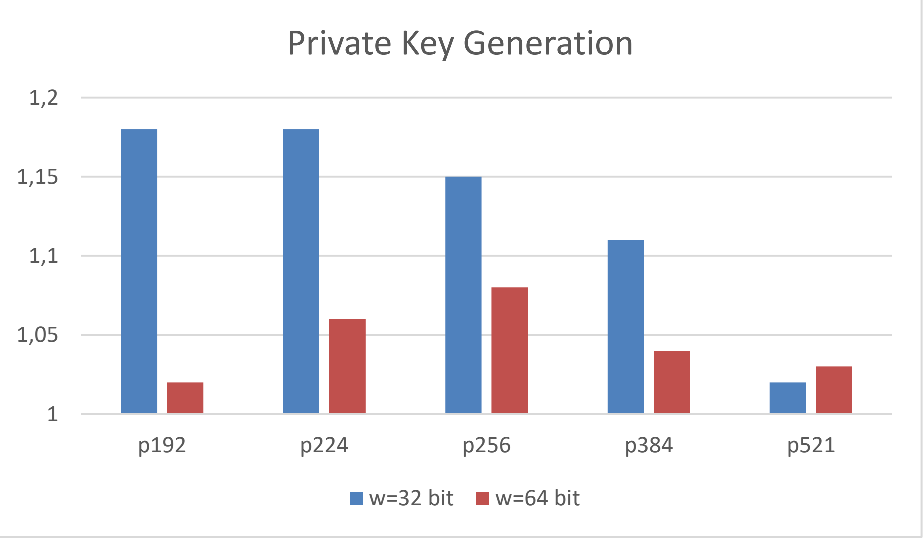

Fig. 2. Efficiency diagram of proposed methods for private key generating operation

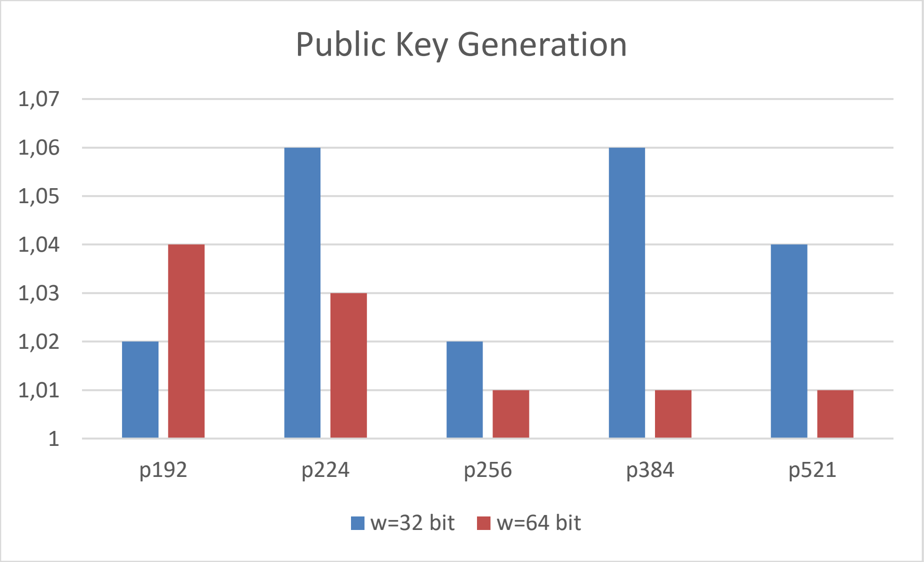

Fig. 3. Efficiency diagram of proposed methods for public key generating operation

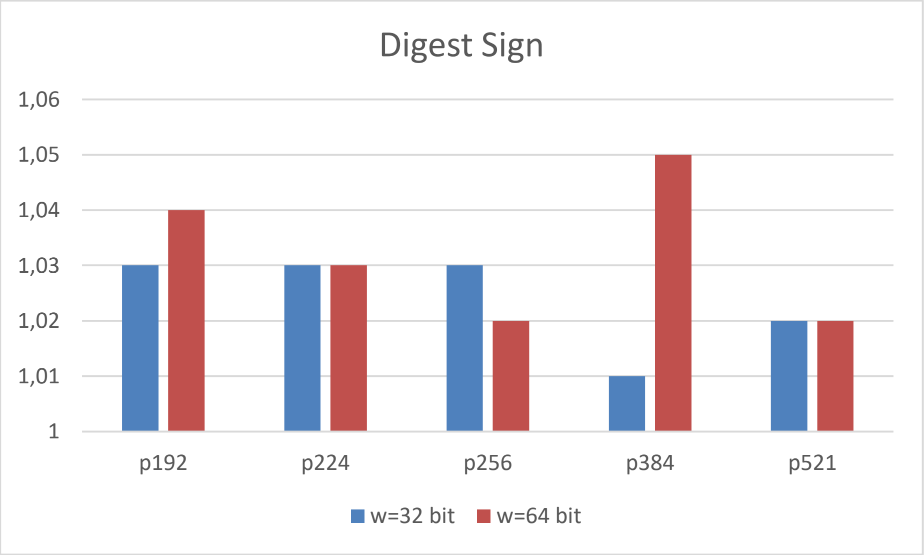

Fig. 4. Efficiency diagram of proposed methods for digest sign operation

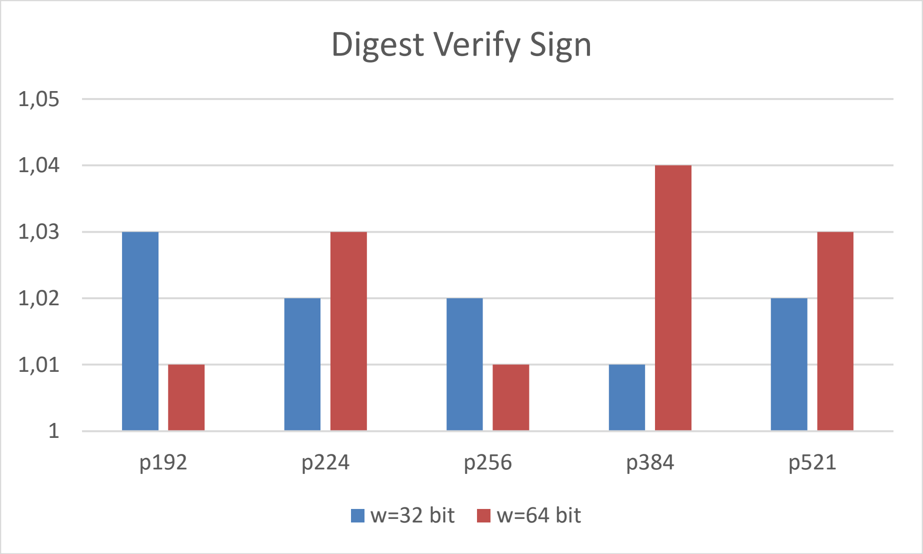

Fig. 5. Efficiency diagram of proposed methods for digest verify sign operation

Table 5 shows a summary of the normalized results of measuring the speed of operations using the proposed methods of arithmetic operations.

Table 5. Summary table of normalized results of measuring the speed of cryptographic operations of the cryptosystem ECDSA

Operation	***w*=32 bit**	***w*=64 bit**
Private key generation	1,02-1,18	1,02-1,08
Public key generation	1,02-1,06	1,01-1,04
Digest sign	1,01-1,03	1,02-1,05
Digest verify sign	1,01-1,03	1,01-1,04

4 Conclusions

In general, according to Table 5, cryptographic operations of the ECDSA cryptosystem using the proposed methods of arithmetic operations in the group of ES points over a prime field are more efficient:

- private key generation – in 1,02-1,18 times for *w*=32 bit, and 1,02-1,08 times for *w*=64 bit;
- public key generation – in 1,02-1,06 times for *w*=32 bit, and 1,01-1,04 times for *w*=64 bit;
- digest sign – in 1,01-1,03 times for *w*=32 bit, and 1,02-1,05 times for *w*=64 bit;
- digest verify sign – in 1,01-1,03 times for *w*=32 bit, and 1,01-1,04 times for *w*=64 bit.

Due to the slight difference in the binary lengths of integers - elements of a prime field, their binary length has virtually no effect on the effectiveness of the proposed methods.

In addition, it should be noted that modern processors are built on a 64-bit architecture, which shows a much higher efficiency of 64-bit implementations of both classical and proposed methods.

References

1. William Stallings. 2016. Network Security Essentials: Applications and Standards (6th ed.). Pearson, 464 pages
2. NIST SP 800-27 Rev A, Engineering Principles for Information Technology Security (A Baseline for Achieving Security), Revision A
3. Rolf Oppliger. Contemporary Cryptography, Second Edition (Artech House Computer Security Series) 2nd Edition, 2012, 571 pages
4. Law of Ukraine “About Electronic Documents and Electronic Document Circulation” from May 22, 2003 № 851-IV. (in Ukrainian)
5. Law of Ukraine from 05.10.2017 № 2155-VIII "About electronic trust services" (in Ukrainian)
6. RFC 6979. Deterministic Usage of the Digital Signature Algorithm (DSA) and Elliptic Curve Digital Signature Algorithm (ECDSA)
7. A. Okhrimenko, V. Kovtun, “Integer multiplication using delayed carry for public key cryptosystem”, Informatsionnyye tekhnologi i sistemy v upravlenii, obrazovanii, nauke: Monografiya, pod red. prof. V.S. Ponomarenko, Khar'kov: Tsifrova drukarnya №1, 2013, S. 69-82. (in Russian)
8. A. Okhrimenko, V.Yu. Kovtun, O.L. Stokipniy, “Integer representation with delayed carry”, AVIATION IN THE XXI-st CENTURY – Safety in Aviation and Space Technologies: VI World Congress, September 23-25, 2014., К., 2014, P. 1.11.10-1.11.14.
9. A.A. Okhrimenko, “Arithmetic with delayed carry”, Zakhist ínformatsíí̈, T. 16, No. 2, pp. 130-138, 2014. (in Russian)
10. Bhattacharyya SS, Deprettere EF, Leupers R, Takala J, editors. Handbook of Signal Processing Systems. 2nd ed. Springer, 2013. 1399 pp.
11. Brent R.P., Zimmermann P. Modern Computer Arithmetic. New York: Cambridge University Press, 2011. 236 pp.
12. Hankerson, D.; Vanstone, S.; Menezes, A. Guide to Elliptic Curve Cryptography. Springer Professional Computing. New York: Springer. - 2004. – 311 p. doi:10.1007/b97644
13. J.H. Saltzer, M.D. Schroeder, "The Protection of In formation in Computer Systems", Proc. IEEE, vol. 63, no. 9, pp. 1278-1308, 1975.
14. Menezes A.J., Vanstone S.A., and Oorschot P.C.V. Handbook of Applied Cryptography. 1st ed. Boca Raton: CRC Press, 1996. 780 pp.
15. R. Brumnik, V. Kovtun, A. Okhrimenko, S. Kavun, “Techniques for Performance Improvement of Integer Multiplication in Cryptographic Applications”, Mathematical Problems in Engineering, 2014, P. 1-7.
16. S. Gnatyuk, T. Zhmurko, P. Falat, Efficiency Increasing Method for Quantum Secure Direct Communication Protocols, Proceedings of the 2015 IEEE 8th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS’2015), Warsaw, Poland, September 24-26, Vol. 1, 2015, pp. 468-472.

17. S. Gnatyuk, A. Okhrimenko, M. Kovtun, T. Gancarczyk, V. Karpinskyi, Method of Algorithm Building for Modular Reducing by Irreducible Polynomial, Proceedings of the 16th International Conference on Control, Automation and Systems, Oct. 16-19, Gyeongju, Korea, 2016, pp. 1476-1479.
18. Hu Z., Gnatyuk S., Kovtun M., Seilova N. Method of searching birationally equivalent Edwards curves over binary fields, Advances in Intelligent Systems and Computing, Vol. 754, pp. 309-319, 2019.
19. S. Gnatyuk, V. Kinzeryavyy, M. Iavich, D. Prysiazhnyi, Kh. Yubuzova, High-Performance Reliable Block Encryption Algorithms Secured against Linear and Differential Cryptanalytic Attacks, CEUR Workshop Proceedings, Vol. 2104, pp. 657-668, 2018.
20. Tynymbayev S., Gnatyuk S.A., Aitkhozhayeva Y.Z., Berdibayev R.S., Namazbayev T.A. Modular reduction based on the divider by blocking negative remainders, News of the National Academy of Sciences of the Republic of Kazakhstan, Series of Geology and Technical Sciences, №2 (434), pp. 238-248, 2019.
21. Hryshchuk R., Molodetska K., Syerov Y. Method of Improving the Information Security of Virtual Communities in Social Networking Services. CEUR Workshop Proceedings. 2019. Vol 2392: Proceedings of the 1st International Workshop on Control, Optimisation and Analytical Processing of Social Networks, COAPSN-2019. p. 23–41.
22. Kalimoldayev M., Tynymbayev S., Gnatyuk S., Ibraimov M., Magzom M. The device for multiplying polynomials modulo an irreducible polynomial, News of the National Academy of Sciences of the Republic of Kazakhstan, Series of Geology and Technical Sciences, №2 (434), pp. 199-205, 2019.
23. Holub S., Khymytsia N., Holub M., Fedushko S. The Intelligent Monitoring of Messages on Social Networks. CEUR Workshop Proceedings. Vol 2616: Proceedings of the 2nd International Workshop on Control, Optimisation and Analytical Processing of Social Networks (COAPSN-2020), Lviv, Ukraine, May 21, 2020. p. 308-317. http://ceur-ws.org/Vol-2616/paper26.pdf
24. Iavich M., Gagnidze A., Iashvili G., Gnatyuk S., Vialkova V. Lattice based Merkle, CEUR Workshop Proceedings, Vol. 2470, pp. 13-16, 2019.
25. Gnatyuk S., Kinzeryavyy V., Kyrychenko K., Yubuzova Kh., Aleksander M., Odarchenko R. Secure Hash Function Constructing for Future Communication Systems and Networks, Advances in Intelligent Systems and Computing, Vol. 902, pp. 561-569, 2020.