УДК 681.3

М.М. КАСЯНЧУК, І.З. ЯКИМЕНКО, С.В. ІВАСЬЄВ, Н.М. МАНДЕБУРА, В.М. НЕМІШ
Тернопільський національний економічний університет

ДОСЛІДЖЕННЯ ЧАСОВИХ ХАРАКТЕРИСТИК АПАРАТНОЇ РЕАЛІЗАЦІЇ МЕТОДІВ ПОШУКУ ОБЕРНЕНОГО ЕЛЕМЕНТА ЗА МОДУЛЕМ

В роботі розроблені методи пошуку оберненого елемента за модулем, які ґрунтуються на покроковому додаванні залишку, що дозволяє уникати складних операцій та проводити обчислення над числами значно меншої розрядності в порівнянні з класичним підходом на основі алгоритму Евкліда та його наслідку. Реалізовано програмно-апаратні модулі зазначених методів на базі середовища розробки Aldec Active-HDL 9.1, та проведені дослідження часових характеристик, які вказують на переваги запропонованого методу.

Ключові слова: обернений елемент за модулем, алгоритм Евкліда, програмно-апаратні модулі, середовище Aldec Active-HDL 9.1.

M. KASIANCHUK, I. YAKYMENKO, S. IVASIEV, N.M. MANDEBURA, V.M. NEMISH
Ternopil National Economic University

RESEARCH OF TIME CHARACTERISTICS OF VEHICLE REALISATION OF THE SEARCHING METHODS OF THE INVERSE ELEMENT BY THE MODULE

The analysis of existing methods of the inverse element search by module was made and practical implementation was defined in the work, namely at multiplying the elliptic curve point by a number in affine coordinates over the field GF(p), in Diffie-Helman keys exchange protocols, asymmetric algorithms of RSA, El Gamal, Rabin information protection, the system of remainder classes, data encryption, to improve performance of wireless sensor networks, computing optimization in the methods of finding the largest common divisor, modular multiplication, exponentiation and factorization. It was established that existing approaches have certain functional limitations and are characterized with high temporal complexity, so the authors developed the search method of the reversed element by module, which is based on the step by step addition of the remainder and allows to avoid complex operations, that is to carry out calculations with the numbers with much smaller bit capacity in comparison with the classic approach based on Euclidean algorithm and its consequence. Block diagram of the proposed algorithm work was shown and hardware and software modules of these methods based on the Aldec Active-HDL 9.1 development environment were realized. The fragments of UML diagrams of designed devices of the reverse element search by module and time diagrams of their work were offered. Research of time characteristics, which point out the benefits of the search method of the inverse element by module, based on the step by step addition of the remainder, was conducted. Analytical expressions of time complexity characteristics were obtained and their graphic dependencies were built. It was established that efficiency of application of the developed method of the inverse element SEARCH by module defines the prospects for its application, in particular in asymmetric information security systems and development of the appropriate high-performance software and hardware.

Keywords: inverse element under modulo, Euclidean algorithm, software and hardware modules, Aldec Active-HDL 9.1 environment.

Вступ

Сучасні системи захисту інформаційних потоків у комп'ютерних мережах, які забезпечують необхідний рівень стійкості до різного виду атак, як правило, функціонують в реальному масштабі часу [1]. У зв'язку з цим програмні бібліотеки криптографічних перетворень [2] повинні задовольняти жорстким вимогам забезпечення необхідної швидкодії базових операцій [3, 4] в асиметричних системах захисту на етапах генерування ключів, шифрування та дешифрування. Однією з найбільш трудомістких та найбільш поширених операцій є пошук оберненого елемента у кільці лишків за модулем [5].

Ця операція багатократно використовується при виконанні множення точки еліптичної кривої на число у афінних координатах над полем GF(p) [6], у методі Діффі-Хелмана обміну ключами [4], криптоалгоритмах RSA, Ель-Гамаля [8], Рабіна [9], системі залишкових класів [10–12], кодуванні даних [13], для підвищення ефективності роботи безпровідних сенсорних мереж [14], оптимізації обчислень в методах знаходження найбільшого спільного дільника, модулярного множення [3], експоненціювання [4] та факторизації [15]. Тому є актуальною задача дослідження існуючих та розробки нових методів пошуку мультиплікативно оберненого елемента у кільці лишків за модулем.

Для вирішення цього завдання можуть застосовуватися як алгоритмічні (математичні), так і програмно-апаратні методи оптимізації. Найкращих результатів можна добитися при спільному використанні обох цих підходів.

Огляд відомих рішень

Обернений елемент за модулем для ненульового елемента a простого поля $GF(p)$ є розв'язком рівняння $(a \cdot b) \bmod p = 1$, заданого в полі натуральних чисел $N\{+,\cdot\}$, причому розв'язок $a^{-1} \bmod p = b$ також є елементом поля GF(p) [16].

Найпростішим методом пошуку оберненого елемента $a^{-1} \bmod p = b$ є простий перебір всіх ненульових елементів простого поля $GF(p)$ з перевіркою кожного з них згідно умови $(a \cdot b) \bmod p = 1$. Однак він характеризується значною обчислювальною складністю.

Процедура пошуку оберненого елемента за модулем на основі алгоритму Евкліда полягає в наступному. З одного боку умова $(a \cdot b) \bmod p = 1$ еквівалентна виразу $a \cdot b - p \cdot t = 1$, де t - частка від ділення $a \cdot b$ на просте число p. З іншого боку, розширений алгоритм Евкліда дозволяє знайти найбільший спільний

дільник $НСД(a, p)$ для чисел a і p, а також g і h такі, що $a \cdot g + p \cdot h = НСД(a, p)$ Оскільки обернений елемент за модулем існує тільки у випадку, коли a і p – взаємно прості, то $a \cdot g + p \cdot h = 1$.

Для знаходження оберненого елемента за модулем можна також скористатися теоремою Ейлера ($a^{\varphi(p)} \equiv 1 \bmod p$), яка вірна для випадку взаємно простих a і p. Звідси $a^{\varphi(p)-1} \bmod p \equiv a^{-1} \bmod p$. Даний метод зводиться до задачі модулярного експоненціювання, що ускладнює процес пошуку для багаторозрядних чисел.

Мета роботи

Метою даної роботи є розробка ефективного методу пошуку оберненого елемента за модулем, реалізація відповідних програмно-апаратних застосувань на базі середовища розробки Aldec Active-HDL 9.1 та проведення дослідження часових характеристик запропонованого та класичного методів.

Ефективні методи знаходження оберненого елемента за модулем

Для знаходження оберненого елемента за модулем a^{-1}mod p, де $a<p$ і НСД(a, p)=1 пропонується такий метод. Спочатку обчислюється $a_0=p \bmod a \neq 0$. Далі послідовно виконується операція додавання:

$$\begin{gathered} a_1=(a_0+1) \bmod a; \\ a_2=(a_1+a_0) \bmod a=(2 \cdot a_0+1) \bmod a; \\ \ldots ; \\ a_i=(a_{i-1}+a_0) \bmod a=(i \cdot a_0+1) \bmod a; \end{gathered} \quad (1)$$

Описана процедура продовжується до тих пір, поки деяке число a_i не стане рівним нулю. Тоді обернений елемент визначається за формулою:

$$K = a^{-1} \bmod p = \frac{i \cdot p + 1}{a}. \quad (2)$$

На рис. 1 представлена блок-схема роботи даного алгоритму, а в таблиці 1 – приклад пошуку 101^{-1}mod167 запропонованим методом. В першому рядку записуються значення кількості кроків виконання алгоритму, а в другому значення a_i це продовжується до тих пір, поки деяке число $a_i=0$. В нашому випадку потрібно проробити 26 кроків для обчислення оберненого елемента за модулем.

Таблиця 1

Приклад пошуку 101^{-1}mod167 запропонованим методом

i	0	1	2	3	4	5	6	7	8
a_i	66	67	32	98	63	28	94	59	24
i	9	10	11	12	13	14	15	16	17
a_i	90	55	20	86	51	16	82	47	12
i	18	19	20	21	22	23	24	25	26
a_i	78	43	8	74	39	4	70	35	0

Згідно виразу (2), з таблиці 1 випливає: $K = 101^{-1} \bmod 167 = \frac{26 \cdot 167 + 1}{101} = 43.$

Основними операціями, які багаторазово повторюються при обчисленні оберненого елемента за модулем, є пошук залишків та додавання. Першу з них (p mod a) пропонується виконувати таким чином. Число p записується у двійковій формі: $p=p_{n-1} \cdot 2^{n-1}+\ldots+p_i \cdot 2^i+\ldots+p_1 \cdot 2^1+p_0 \cdot 2^0$, де $p_i=0,1$. Далі формується таблиця 2, у якій $p_{1i}=2^i \bmod a$.

Таблиця 2

Знаходження залишків степенів двійки

2^{n-1}	2^{n-2}	…	2^i	…	2	1
p_{n-1}	p_{n-2}	…	p_i	…	p_1	p_0
$p_{1\,n-1}$	$p_{1\,n-2}$	…	$p_{1\,i}$	…	$p_{1\,1}$	$p_{1\,0}$

Пошук p_{1i} здійснюється домноженням на 2 попереднього елемента p_{1i-1} (дописуванням нуля в молодший розряд числа p_{1i-1} у двійковій формі) та порівнянням з модулем p:

$$p_{1i} = \begin{cases} 2 \cdot p_{1\,i-1}, & 2 \cdot p_{1\,i-1} < p \\ 2 \cdot p_{1\,i-1} - p, & 2 \cdot p_{1\,i-1} \geq p. \end{cases} \quad (3)$$

Шуканий залишок буде дорівнювати сумі тих p_{1i}, для яких відповідні p_i рівні 1. В таблиці 3 наведено приклад пошуку залишку 167 mod 101 вказаним методом без використання громіздкої операції ділення.

Таблиця 3

Приклад пошуку залишку 167 mod 101

p_{1i}	27	64	32	16	8	4	2	1
p_i	1	0	1	0	0	1	1	1

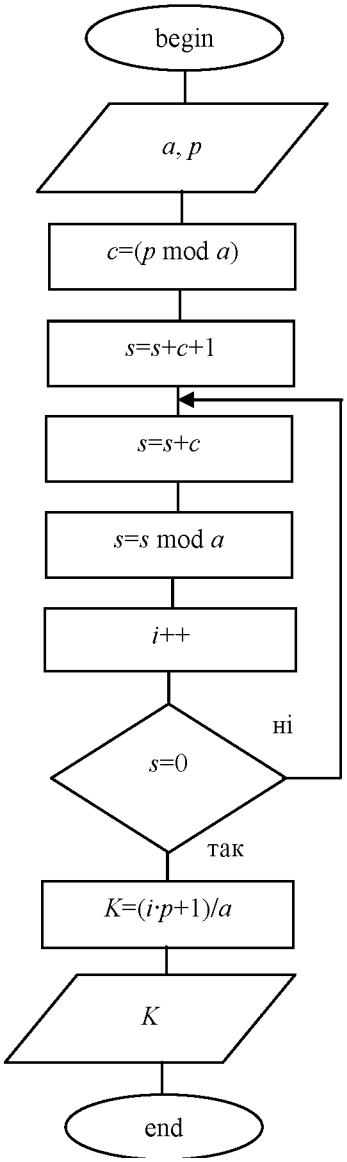

Рис.1. Блок-схема роботи запропонованого алгоритму

З врахуванням вищесказаного 167 mod 101=(27+32+4+2+1) mod 101=66.
В таблиці 4 представлена часова складність основних операцій запропонованого алгоритму

Таблиця 4

Часова складність базових операцій запропонованого алгоритму

№	Основні операції	Часова складність запропонованих алгоритмів
1.	$i \cdot a_{10}+1$	$O(i \cdot n)$
2.	$(i \cdot a_{10}+1) \bmod a_3$	$O\left(i \cdot \left(\frac{n}{2}+\log_2 n/2\right)\right)$

Загальна часова складність пошуку оберненого елемента запропонованим методом, вважаючи $\max i=log_2 n$, становить $O1\left(\frac{n \cdot \log_2 n}{2}+\log_2 n \cdot \log_2 n/2\right)$. Класичний метод з використанням розширеного алгоритму Евкліда приводить до такого результату: $O(n^3)$ [17]. На рис. 2 представлено залежності часових складностей класичного (графік різко зростає) і запропонованого (графік зростає набагато повільніше в порівнянні з попереднім) методів в логарифмічній шкалі з основою 10.

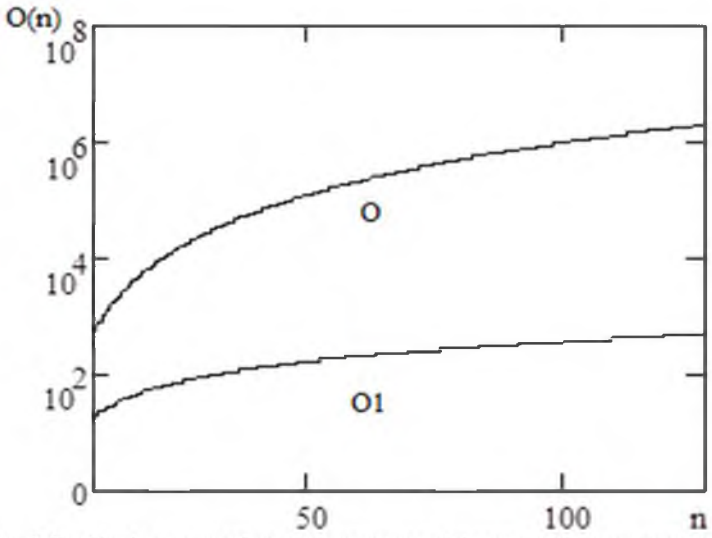

Рис. 2. Графічні залежності часових складностей і запропонованого методів

Отже, розроблений метод дозволяє уникати складних операцій, зокрема, ділення з остачею, та проводити обчислення над числами значно меншої розрядності в порівнянні з класичним методом пошуку оберненого елемента за модулем з використанням алгоритму Евкліда та його наслідку.

Дослідження часових характеристик апаратної реалізації методів пошуку оберненого елемента за модулем

Для експериментального дослідження часових затрат пошуку оберненого елемента за модулем з використанням розширеного алгоритму Евкліда та запропонованого методу для кожного з них було здійснено програмно-апаратну реалізацію на базі середовища розробки Aldec Active-HDL 9.1. Фрагменти UML-діаграм спроектованих пристроїв, на яких вказані усі стандартні бібліотеки та компоненти для їх коректної роботи, представлено на рисунку 3.

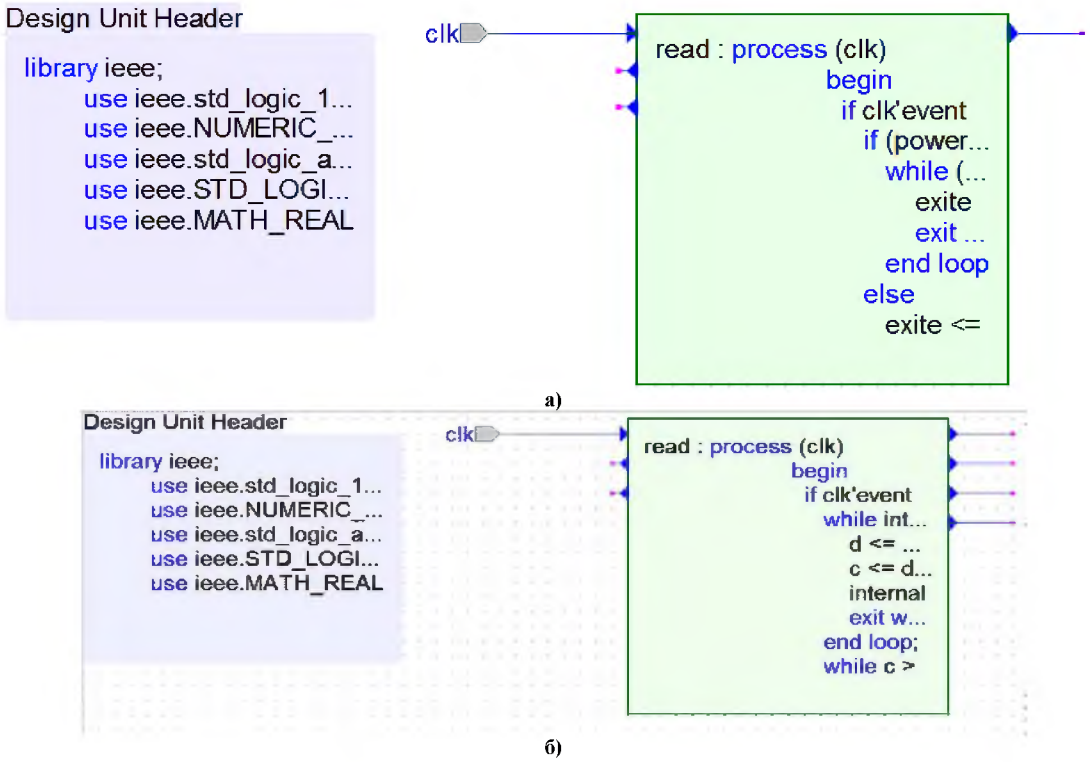

Рис. 3. Фрагменти UML-діаграм спроектованих пристроїв пошуку оберненого елемента за модулем: а) на основі алгоритму Евкліда; б) на основі запропонованого методу

На рисунку 4 представлено часові діаграми роботи спроектованих пристроїв пошуку оберненого елемента за модулем (для прикладу було вибрано $60000^{-1}\text{mod}65537$) на основі розширеного алгоритму Евкліда та запропонованого методу.

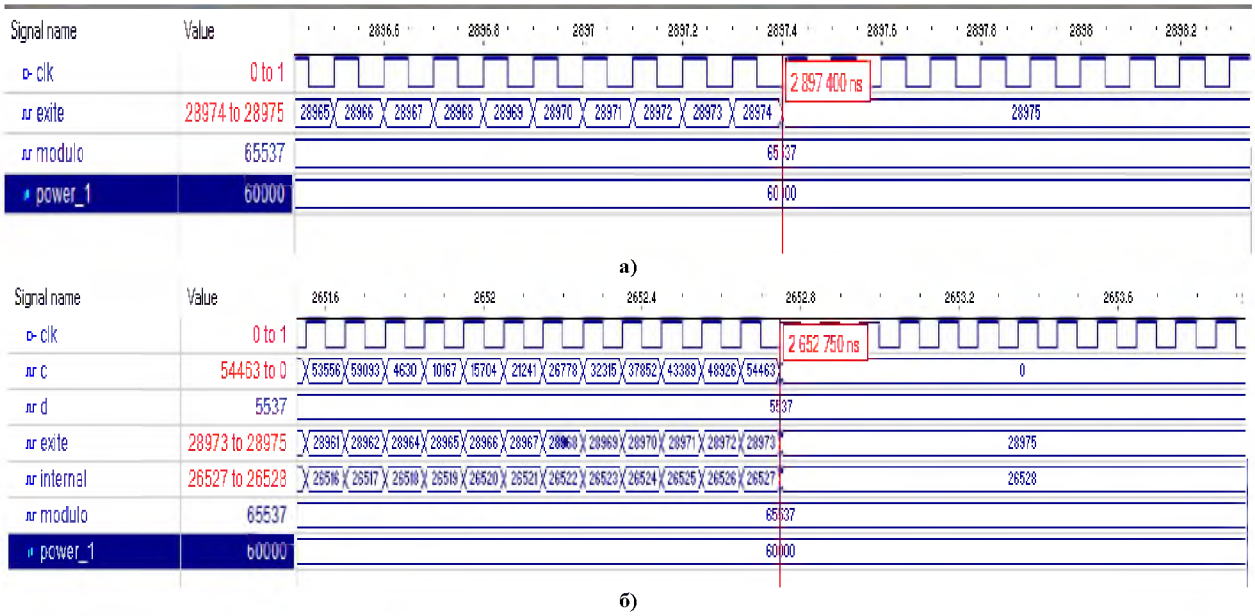

Рис. 4. Часова діаграма пошуку оберненого елемента за модулем:
а) на основі алгоритму Евкліда; б) на основі запропонованого методу

Наведений приклад ілюструє, що час роботи системи зменшився із 2,8974 мс (на основі алгоритму Евкліда) до 2,65275 мс (на основі запропонованого методу додавання залишків), тобто приблизно в 1,09 разів.

При дослідженні часових параметрів програмно-апаратної реалізації вищеназваними методами число p=65537 вибиралося простим і фіксованим, щоб для будь-якого $a<p$ існував обернений елемент. Число a змінювалося від 5000 до 65000 з кроком 5000. Результати чисельного експерименту наведено в таблиці 5.

Таблиця 5

Порівняльні характеристики часових затрат обчислення оберненого елемента за модулем в середовищі розробки Aldec Active-HDL 9.1

N п/п	a	$a^{-1} \bmod p$	Час роботи, *ns*	
			Алгоритм Евкліда та його наслідок	Метод додавання залишку
1	5000	20015	201300	113540
2	10000	42776	4277500	652750
3	15000	50363	5036200	1152750
4	20000	21388	2138700	652750
5	25000	4003	400200	152750
6	30000	57950	5794900	2652750
7	35000	40309	4030800	2152750
8	40000	10694	1069300	3552750
9	45000	60479	5542000	6553550
10	50000	34770	3476900	2652750
11	55000	37567	3756600	3152750
12	60000	28975	2897400	2652750
13	65000	56994	4845000	3553450
Середній час	-	-	3343600	2280619

На рис. 5 представлені графічні залежності часових затрат пошуку оберненого елемента класичним (графік 1) та запропонованим (крива 2) методами згідно таблиці 5, а також усереднені значення отриманих результатів (прямі 3 та 4 відповідно).

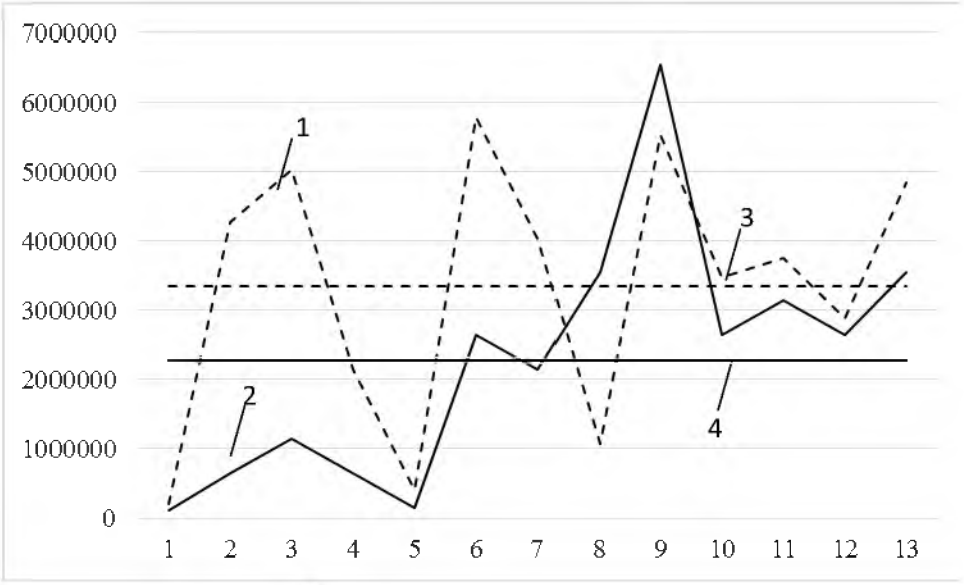

Рис. 5. Часові характеристики VHDL-реалізації класичного (штрихові лінії) та запропонованого (суцільні лінії) методів пошуку оберненого алгоритму за модулем

Результати проведених досліджень показують, що тільки у двох із тринадцяти випадків при a=40000 та a=45000 запропонований метод поступається класичному, що пояснюється необхідністю виконання великої кількості операцій додавання. Середній час пошуку оберненого елемента за модулем за допомогою алгоритму Евкліда (3343600 ns) в 1,47 разів більший від аналогічного параметра з використанням додавання залишків (2280619 ns).

Висновки

В роботі здійснено експериментальне порівняння часових затрат пошуку оберненого елемента за модулем на основі розширеного алгоритму Евкліда та запропонованого методу додавання залишку, який дозволяє уникати виконання складних арифметичних операцій та проводити обчислення над числами значно меншої розрядності. Реалізація програмно-апаратних модулів зазначених алгоритмів на базі середовища розробки Aldec Active-HDL 9.1 показала, що середній час пошуку оберненого елемента за модулем класичним методом в 1,47 рази більший від аналогічного параметра з використанням запропонованого методу. Отримано аналітичні вирази характеристик часової складності та побудовано їх графічні залежності. Ефективність застосування розробленого методу пошуку оберненого елемента за модулем визначає перспективи щодо його застосування, зокрема в асиметричних системах захисту інформації, та розробки відповідних високопродуктивних програмно-апаратних засобів.

Література

1. Ma Q. An integrated framework for information security management / Q. Ma, B. M. Schmidt, J. M. Pearson // Review of Business. Retrieved – 26 October 2013. – P. 58–69.

2. Stallings W. Cryptography and Network Security: Principles and Practice. 5th Prentice Hall Press Upper Saddle River, NJ, USA. 2010. – 719 p.

3. Николайчук Я.М. Векторно-модульний метод множення багаторозрядних чисел в базисі Радемахера-Крестенсона / Я.М. Николайчук, М.М. Касянчук, І.З. Якименко, С.В. Івасьєв // Вісник Національного університету «Львівська політехніка». Комп'ютерні системи та мережі. – 2014. – № 694. – С. 118–125.

4. Kozaczko D. Vector Module Exponential in the Remaining Classes System / D. Kozaczko, M. Kasianchuk, I. Yakymenko, S. Ivasiev / Proceedings of the 2015 IEEE 8th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS–2015), Warsaw, Poland, V.1, September – 2015, p. 161–163.

5. Kasyanchuk M.M. Foundations for the Analytical Computation of Coefficients of Basic Numbers of Krestenson's Transformation / M.M. Kasyanchuk, Ya. M. Nykolaychuk, I. Z. Yakymenko_/ Cybernetics and Systems Analysis. – September, 2014. – Volume 50, Issue 5. – pp. 649–654.

6. Hankerson D. Guide to Elliptic Curve Cryptography / D. Hankerson, A. Menezes, V. Scott / Springer-Verlag New York, USA, 2004, 311 p.

7. Koblitz N. Another look at non-standard discrete log and Diffie-Hellman problems / N. Koblitz, A. Menezes // Cryptology ePrint Archive. Report 2007/442, 2007. URL: http://eprint.iacr.org/.

8. Якименко І.З. Теорія алгоритмів RSA та Ель–Гамаля в розмежованій системі числення Радемахера–Крестенсона / І.З. Якименко, М.М. Касянчук, О.І. Волинський, І.Р. Пітух // Вісник Хмельницького національного університету. Технічні науки. – 2011. – № 3. – С. 265–273.

9. Касянчук М.М. Модифікований метод шифрування Рабіна з використанням різних форм системи

залишкових класів / М.М. Касянчук, І.З. Якименко, Л.О. Дубчак, Н.А. Рендзеняк, Н.М. Мандебура // Вісник Хмельницького національного університету. Технічні науки. – 2017. – № 1(245). – С. 127–131.

10. Kasianchuk M. N. Theoretical Foundations of the Modified Perfect form of Residue Number System / M. N. Kasianchuk, Ya. N. Nykolaychuk, I.Z. Yakymenko / Cybernetics and Systems Analysis, 2014, p. 219-223.

11. Kasianchuk M. N. Theory and Methods of Constructing of Modules System of the Perfect Modified Form of the System of Residual Classes / M. N Kasianchuk, Ya. N Nykolaychuk, I.Z. Yakymenko // Journal of Automation and Information Sciences. 2016, Vol. 48, № 8, p. 56–63.

12. Omondi A. Residue Number System: Theory and Implementation. Imperial College Press / A. Omondi, B. Premkumar. vol. 2, 2007. – 296 p.

13. Sachenko A. Data Encoding in Residue Number System / A. Sachenko, V. Yatskiv, R. Krepych, A. Karachka // Proceeding of the International Workshop on Intelligent Data Acquisition and Advanced Computing Systems: IDAACS'2009, 2009, p. 679–681.

14. Zhengbing Hu. Increasing the Data Transmission Robustness in WSN Using the Modified Error Correction Codes on Residue Number System / Hu Zhengbing. V. Yatskiv, A. Sachenko // Elektronika ir Elektrotechnika. Vol 21, No 1, 2015, p. 76–81.

15. Karpiński M. Advanced method of factorization of multi-bit numbers based on Fermat's theorem in the system of residual classes / M. Karpiński, S. Ivasiev, I. Yakymenko, M. Kasianchuk, T. Gancarczyk // Proc. of 16th International Conference on Control, Automation and Systems (ICCAS–2016), Gyeongju, Korea, V. 1, October, 2016, p. 1484–1486.

16. Вербіцький О.В. Вступ до криптології / О.В. Вербінський – Львів : ВНТЛ, 1998. – 248 с.

17. Dasgupta S. Algorithms / S. Dasgupta, C. Papadimitriou, U. Vazirani // McGraw-Hill Science, Engineering, Math; 1 edition, 13 September, 2006, 336 p.

References

1. Ma Q. An integrated framework for information security management / Q. Ma, B. M. Schmidt, J. M. Pearson // Review of Business. Retrieved – 26 October 2013. – P. 58–69.

2. Stallings W. Cryptography and Network Security: Principles and Practice. 5th Prentice Hall Press Upper Saddle River, NJ, USA. 2010. – 719 p.

3. Nykolaychuk Ya.M. Vector-modular method of multiplying multi-digit numbers in the basis of Rademacher-Krestenson / Ya.M. Nykolaychuk, M.M. Kasyanchuk, I.Z. Yakymenko, S.V. Ivas'ev // Bulletin of the National University "Lviv Polytechnic" "Computer Systems and Networks". – No. 694. – 2014. – P. 118–125.

4. Kozaczko D. Vector Module Exponential in the Remaining Classes System / D. Kozaczko, M. Kasianchuk, I. Yakymenko, S. Ivasiev / Proceedings of the 2015 IEEE 8th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS–2015), Warsaw, Poland, V.1, September – 2015, p. 161–163.

5. Kasyanchuk M.M. Foundations for the Analytical Computation of Coefficients of Basic Numbers of Krestenson's Transformation / M.M. Kasyanchuk, Ya. M. Nykolaychuk, I. Z. Yakymenko_/ Cybernetics and Systems Analysis. – September, 2014. – Volume 50, Issue 5. – pp. 649–654.

6. Hankerson D. Guide to Elliptic Curve Cryptography / D. Hankerson, A. Menezes, V. Scott / Springer-Verlag New York, USA, 2004, 311 p.

7. Koblitz N. Another look at non-standard discrete log and Diffie-Hellman problems / N. Koblitz, A. Menezes // Cryptology ePrint Archive. Report 2007/442, 2007. URL: http://eprint.iacr.org/.

8. Yakymenko I.Z. Theory of algorithms of RSA and El Gamal in a delimited Rademacher-Krestenson system / I.Z. Yakymenko, M.M. Kasyanchuk, O.I. Volynsky, I.P. Pitukh // Herald of Khmelnytsky National University. Technical sciences. - №3. - 2011. – pp. 265-273.

9. Kasyanchuk M.M. Modified method of encryption of Rabin using various forms of the system of residual classes / M.M. Kasyanchuk, I.Z. Yakymenko, L.O. Dubchak, N.A. Rendzianyak, N.M. Mandebur / Herald of Khmelnytsky National University. Technical sciences. - No. 1 (245). - 2017. – p. 127-131.

10. Kasianchuk M. N. Theoretical Foundations of the Modified Perfect form of Residue Number System / M. N. Kasianchuk, Ya. N. Nykolaychuk, I.Z. Yakymenko / Cybernetics and Systems Analysis, 2014, p. 219-223.

11. Kasianchuk M. N. Theory and Methods of Constructing of Modules System of the Perfect Modified Form of the System of Residual Classes / M. N Kasianchuk, Ya. N Nykolaychuk, I.Z. Yakymenko // Journal of Automation and Information Sciences. 2016, Vol. 48, № 8, p. 56–63.

12. Omondi A. Residue Number System: Theory and Implementation. Imperial College Press / A. Omondi, B. Premkumar. vol. 2, 2007. – 296 p.

13. Sachenko A. Data Encoding in Residue Number System / A. Sachenko, V. Yatskiv, R. Krepych, A. Karachka // Proceeding of the International Workshop on Intelligent Data Acquisition and Advanced Computing Systems: IDAACS'2009, 2009, p. 679–681.

14. Zhengbing Hu. Increasing the Data Transmission Robustness in WSN Using the Modified Error Correction Codes on Residue Number System / Hu Zhengbing. V. Yatskiv, A. Sachenko // Elektronika ir Elektrotechnika. Vol 21, No 1, 2015, p. 76–81.

15. Karpiński M. Advanced method of factorization of multi-bit numbers based on Fermat's theorem in the system of residual classes / M. Karpiński, S. Ivasiev, I. Yakymenko, M. Kasianchuk, T. Gancarczyk // Proc. of 16th International Conference on Control, Automation and Systems (ICCAS–2016), Gyeongju, Korea, V. 1, October, 2016, p. 1484–1486.

16. Verbitskyi O. V. Introduction to cryptology. – Lviv, 1998. – 248 s.

17. Dasgupta S. Algorithms / S. Dasgupta, C. Papadimitriou, U. Vazirani // McGraw-Hill Science, Engineering, Math; 1 edition, 13 September, 2006, 336 p.

Рецензія/Peer review : 06.11.2017 р. Надрукована/Printed :19.11.2017 р.
Рецензент: д.т.н., проф. Березький О.М.