УДК 681.31

І.З. Якименко, М.М. Касянчук, В.Л. Кімак
Інститут мікропроцесорних систем керування об'єктами
електроенергетики Карпатського державного центру АН України

ТЕОРЕТИЧНІ ОСНОВИ ЗМЕНШЕННЯ ЧАСОВОЇ ТА АПАРАТНОЇ СКЛАДНОСТІ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЙНИХ ПОТОКІВ НА ОСНОВІ ЕЛІПТИЧНИХ КРИВИХ З ВИКОРИСТАННЯМ ТЕОРЕТИКО-ЧИСЛОВОГО БАЗИСУ РАДЕМАХЕРА–КРЕСТЕНСОНА

Викладено теоретичні основи зменшення часової та апаратної складностей систем захисту інформаційних потоків на основі використання математичного апарату еліптичних кривих. Показано, що запропонований алгоритм модулярного експоненціювання з використанням теоретико-числового базису Радемахера–Крестенсона характеризується високою швидкодією та ефективністю.

Ключові слова: базис Радемахера–Крестенсона, еліптична крива, часова складність, ефективність.

The paper presents the theoretical foundations reduce systems time and hardware complexity of to protect information flow based on the using of mathematical elliptic curves tools. It is shown that the proposed algorithm modular exponentiation with using theoretical numerical Rademacher-Krestenson basis characterized by high speed and efficiency.

Key words: Rademacher-Krestenson basis, elliptic curve, the time complexity and efficiency.

Вступ

Алгоритм шифрування з використанням математичного апарату еліптичних кривих (ЕК) є малопоширеним алгоритмом захисту інформаційних потоків (ІП) у комп'ютерних системах. Його стійкість базується на вирішенні проблеми дискретного алгоритму, тобто знаходженні секретного ключа на основі відкритого.

У наведеній нижче табл. 1 порівняно наближені розміри параметрів еліптичних систем і криптосистеми RSA, що забезпечують однакову стійкість шифру. Ці дані отримано на основі сучасних методів розв'язання задачі дискретного логарифмування еліптичної кривої (Elliptic Curve Discrete Logarithm Problem – ECDLP) та факторизації великих цілих чисел [1].

Таблиця 1

Порівняння стійкості основних криптографічних алгоритмів

Система на основі еліптичної кривої (базова точка P)	*RSA (довжина модуля n)*
1024 біти	*3084 біти*
3250 бітів	*9750 бітів*
15500 бітів	*46500 бітів*

Як показує аналіз таблиці, використання еліптичних кривих дозволяє будувати стійкі системи з ключами значно менших розмірів порівняно з традиційними асиметричними криптоалгоритмами. Такі системи потребують меншого обсягу обчислювальних ресурсів, тому зручні для використання у старт-картках та портативних телефонах.

Незважаючи на вагомі переваги застосування ЕК, виникають певні проблеми та труднощі. Зокрема, виділяють такі класи задач:

1. Генерування параметрів еліптичної кривої.

2. Обчислення порядку еліптичної кривої.

3. Проблема дискретного логарифма.

Ці три класи задач взаємопов'язані та є ключовими в системах захисту інформаційних потоків з використанням ЕК: перших два – для шифрування і аналізу стійкості, третій – дешифрування.

Хоч розроблено підходи щодо вирішення згаданих проблем, існують певні труднощі стосовно продуктивності алгоритмів виконання основних операцій на ЕК за певний період часу. Тому актуальною залишається розробка нових методів, які дають змогу ефективно розв'язати цю задачу, зокрема з використанням теоретико-числових базисів (ТЧБ) Радемахера та Крестенсона [10].

Сучасні можливості становлення теорії та алгоритмів опрацювання ІП на основі різних ТЧБ та високопродуктивних спецпроцесорів також створюють базові засади підвищення ефективності формування, зменшення часової складності, швидкодії та захищеності ІП на основі використання високопродуктивних алгоритмів опрацювання великорозрядних чисел.

Аналіз літературних джерел

Криптосистеми на ЕК (КЕК) запропонували незалежно В. Міллер [2] і Н. Кобліц [3] в 1986 р. і вже близько 20 років їх інтенсивно аналізують криптографи світу. За винятком вже відомих криптографічно слабких кривих, стійкість КЕК сьогодні оцінюється як експонентна. Складність атаки на ключ у цьому випадку експоненціально пов'язана з його довжиною, тобто наростає дуже швидко і при деякій довжині ключа стає практично нереалізованою. Тому нині, по суті, немає альтернативи цим криптосистемам.

Сьогодні ЕК застосовують для реалізації різноманітних класів систем захисту інформації, зокрема, їх можна використовувати для побудови симетричних та асиметричних криптосистем, систем електронного цифрового підпису.

Однією з важливих задач на ЕК є пошук кількості раціональних точок, тобто порядку ЕК. Проведений аналіз показує, що для розв'язання цієї задачі можна застосувати такі алгоритми: «крок гіганта–крок малюка», Шуфа, Еткіна та Еліза [4–6].

Перший алгоритм ґрунтується на обчисленні високих степенів $x^p, y^p, x^{p^2}, y^{p^2}$ за модулем $f_l(x)$. Удосконалення алгоритму Шуфа показано в роботах Еткіна та Еліза [4, 5]. Їх основна операція – модулярне експоненціювання. Для зменшення часової складності алгоритмів Еткіна та Еліза доцільно скористатися ТЧБ Радемахера–Крестенсона.

Мета роботи

Мета цієї роботи полягає у розробленні теоретичних основ зменшення часової та апаратної складності систем захисту ІП на основі ЕК з використанням ТЧБ Радемахера–Крестенсона.

Опрацювання великорозрядних чисел у криптографії еліптичних кривих

Скористаємося алгоритмом піднесення до степеня з використання математичних основ теоретико-числових базисів Радемахера та Крестенсона, згідно з формулами [10]:

$$\begin{aligned} x^p \bmod f_l(x) &= \left(\prod_{i=0}^{n-1} x^{p_i 2^i}\right) \bmod f_l(x) = \prod_{k=0}^{n-1}\left(\sum_{j=0}^{n-1}\left(\sum_{i=0}^{n-1} x_i \cdot x_j \cdot 2^{i+j}\right)\right)^{p_k 2^k} \bmod f_l(x), \\ y^p \bmod f_l(x) &= \left(\prod_{i=0}^{n-1} y^{p_i 2^i}\right) \bmod f_l(x) = \prod_{k=0}^{n-1}\left(\sum_{j=0}^{n-1}\left(\sum_{i=0}^{n-1} y_i \cdot y_j \cdot 2^{i+j}\right)\right)^{p_k 2^k} \bmod f_l(x). \end{aligned} \quad (1)$$

Цей алгоритм є матричним, причому в стовпцях матриці записано величини $x^{2^i} \bmod f_l(x), y^{2^i} \bmod f_l(x)$ в базисі Радемахера, тобто y_{ij} та x_{ij}=0, 1 [10]. Тоді будь-який степінь x, y можна записати за степенями 2: $p = p_{n-1}2^{n-1}+\ldots+ +p_i2^i+\ldots+ p_12+p_0$, що дає змогу зменшити обчислювальну складність. Шуканий результат отримуємо, перемноживши відповідну кількість стовпців табл. 2 та табл. 3 з використанням формул:

$$\left(x^{2^i}\cdot x^{2^j}\right) mod\ f_l(x)=\left(\sum_{i=1}^{n-1}\sum_{j=1}^{n-1}x_{in-1}x_{jn-1}2^{i+j}\right) mod\ f_l(x),$$

$$\left(y^{2^i}\cdot y^{2^j}\right) mod\ f_l(x)=\left(\sum_{i=1}^{n-1}\sum_{j=1}^{n-1}y_{in-1}y_{jn-1}2^{i+j}\right) mod\ f_l(x).$$

Таблиця 2

Матриця знаходження x^{2^i} в базисі Радемахера–Крестенсона

$x_{n-1\ n-1}$	…	$x_{i\ n-1}$		$x_{1\ n-1}$	$x_{0\ n-1}$
…	…	…	…	…	…
$x_{n-1\ j}$	…	$x_{i\ j}$	…	$x_{1\ j}$	$x_{0\ j}$
…	…	…	…	…	…
$x_{n-1\ 1}$	…	$x_{i\ 1}$	…	$x_{1\ 1}$	$x_{0\ 1}$
$x_{n-1\ 0}$	…	$x_{i\ 0}$	…	$x_{1\ 0}$	$x_{0\ 0}$
$x^{2^{n-1}}$	...	x^{2^i}	...	x^{2^1}	x^{2^0}

Таблиця 3

Матриця знаходження y^{2^i} в базисі Радемахера–Крестенсона

$y_{n-1\ n-1}$	…	$y_{i\ n-1}$		$y_{1\ n-1}$	$y_{0\ n-1}$
…	…	…	…	…	…
$y_{n-1\ j}$	…	$y_{i\ j}$	…	$y_{1\ j}$	$y_{0\ j}$
…	…	…	…	…	…
$y_{n-1\ 1}$	…	$y_{i\ 1}$	…	$y_{1\ 1}$	$y_{0\ 1}$
$y_{n-1\ 0}$	…	$y_{i\ 0}$	…	$y_{1\ 0}$	$y_{0\ 0}$
$y^{2^{n-1}}$	...	y^{2^i}	...	y^{2^1}	y^{2^0}

Запропонований алгоритм піднесення до степеня двійкового числа будь-якої розрядності за модулем $f_l(x)$ дозволяє зменшити часову складність за рахунок заміни операції множення додаванням, підвищити швидкодію на 2 порядки (рис. 2) для чисел, розрядність яких менша за 64 біти, а в діапазоні від 64 бітів вдвічі. Числовий експеримент показав, що запропонований алгоритм піднесення до степеня двійкового числа будь-якої розрядності за модулем $f_l(x)$ у базисі Радемахера–Крестенсона дає змогу зменшити складність з $O2=n^3$ або $O1(n)=n^2\log n$ (метод Монтгомері) до $O(n)=\begin{cases} n\log_2 n, \textit{якщо}\ \ n<64 \\ \dfrac{n^2}{2}\log_2 n\cdot, n\geq 64. \end{cases}$ в $E(n)=\begin{cases} n, \textit{для}\ \ n<64 \\ 2\ , n\geq 64 \end{cases}$ разів. Ефективність запропонованого алгоритму показано на рис. 3.

Дослідження показали, що запропонований алгоритм характеризується високою швидкодією та ефективністю для виконання операції піднесення до степеня двійкового числа будь-якої розрядності за модулем $f_l(x)$. Зазначимо, шо у разі збільшення розрядності чисел зменшується ефективність (рис. 3), бо частина ресурсу комп'ютера буде задіяна на обробку службової інформації, що значно збільшує складність, кількість операцій та зменшує швидкодію. Оскільки операція модулярного експоненціювання є базовою в найпоширеніших системах захисту ІП з відкритими ключами (RSA, Ель–Гамаля тощо), то розроблений метод доцільно використовувати для розв'язання задач захисту ІП.

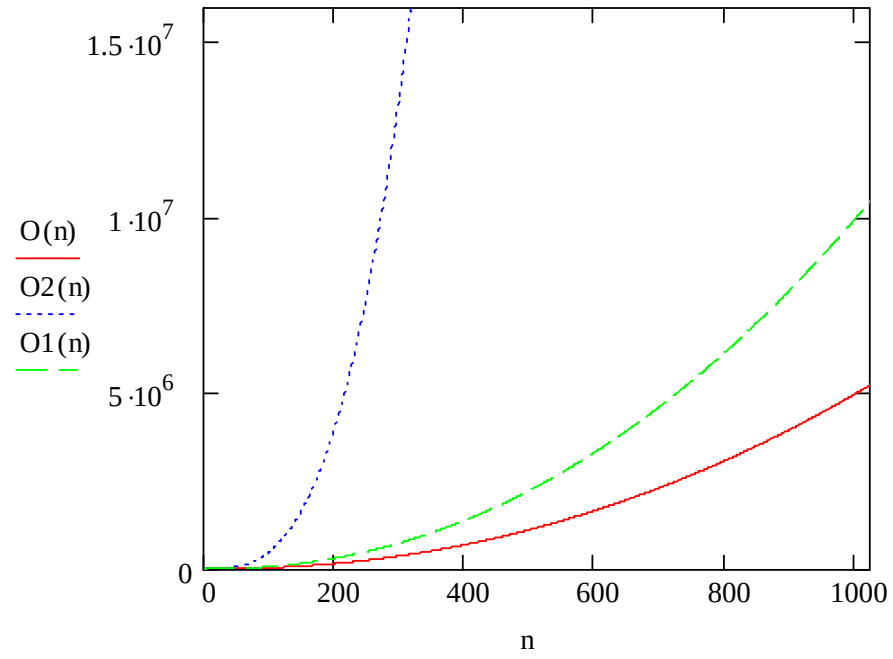

Рис. 2. Часова складність операції модулярного піднесення до степеня

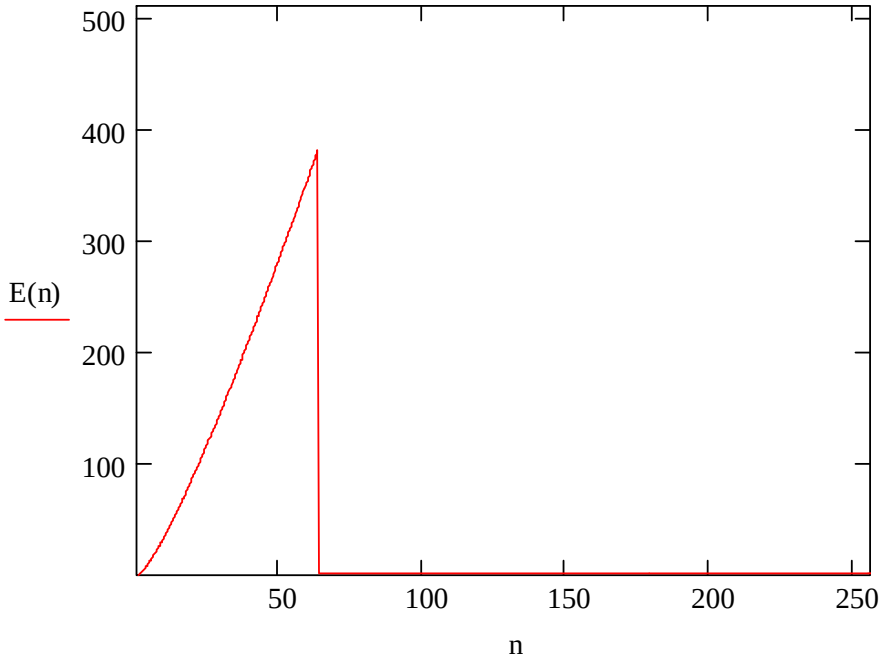

Рис. 3. Ефективність запропонованого алгоритму

Спецпроцесор виконання операції пошуку залишків великорозрядних чисел у криптографії еліптичних кривих

З метою вдосконалення виконання базових операцій у криптографії ЕК запропоновано метод пошуку залишків великорозрядних чисел з використанням ТЧБ Радемахера-Крестенсона. В основу запропонованого спецпроцесора покладено задачу зменшення апаратної складності та розширення функціональних можливостей пристрою обчислення залишку багаторозрядного двійкового числа за довільним цілочисловим багаторозрядним модулем *p*.

Поставлена задача розв'язується завдяки тому, що у пристрій, який містить n-розрядний регістр зсуву, вхід якого під'єднаний до шини запису кодового представлення числа, введено шину запису кодового представлення модуля P, яка підключена до першого входу k+1-розрядного регістра зсуву, другий адресний вхід якого підключений до першого виходу блока управління, другий і третій виходи якого відповідно приєднані до перших входів третього і четвертого k+1-розрядних регістрів зсуву, виходи яких відповідно підключені до першого і другого входів мультиплексора, третій вхід якого підключений до четвертого виходу блока управління, а вихід підключений до першого входу накопичувального суматора, другий вхід якого підключений до виходу другого k+1-розрядного регістра зсуву, а вихід з'єднаний з другим входом блока управління і вихідною шиною кодового представлення залишку.

Суть розробки пояснюється тим, що в основу роботи пристрою покладено алгоритм обчислення залишку багаторозрядного двійкового числа Y за багаторозрядним цілочисловим модулем P згідно з рекурсивним виразом [12]:

$$b_i = [p]_{мд} + 2b_{i-1} + a_i, \ \ i = n, n-1, ..., 1, \qquad (2)$$

де n – розрядність числа Y, з якого визначається залишок b_i,a_i – біти двійкового числа Y, починаючи зі старшого розряду a_n, $[P]_{мд} - k + 1$ розрядна мантиса доповнюючого коду модуля P, b_i – поточне кодове значення залишку ($b_{i-1} = 0$).

На рис. 4 показано структурну схему спецпроцесора; де 1 – перший n-розрядний регістр зсуву; 2 – шина запису кодового представлення числа Y; 3 – шина запису кодового представлення модуля P; 4 – блок управління; 5 – другий k+1-розрядний регістр зсуву; 6 – третій k+1-розрядний регістр зсуву; 7 – четвертий k+1-розрядний регістр зсуву; 8 – однорозрядний накопичувальний суматор; 9 – мультиплексор; 10 – вихідна шина кодового представлення залишку b_i.

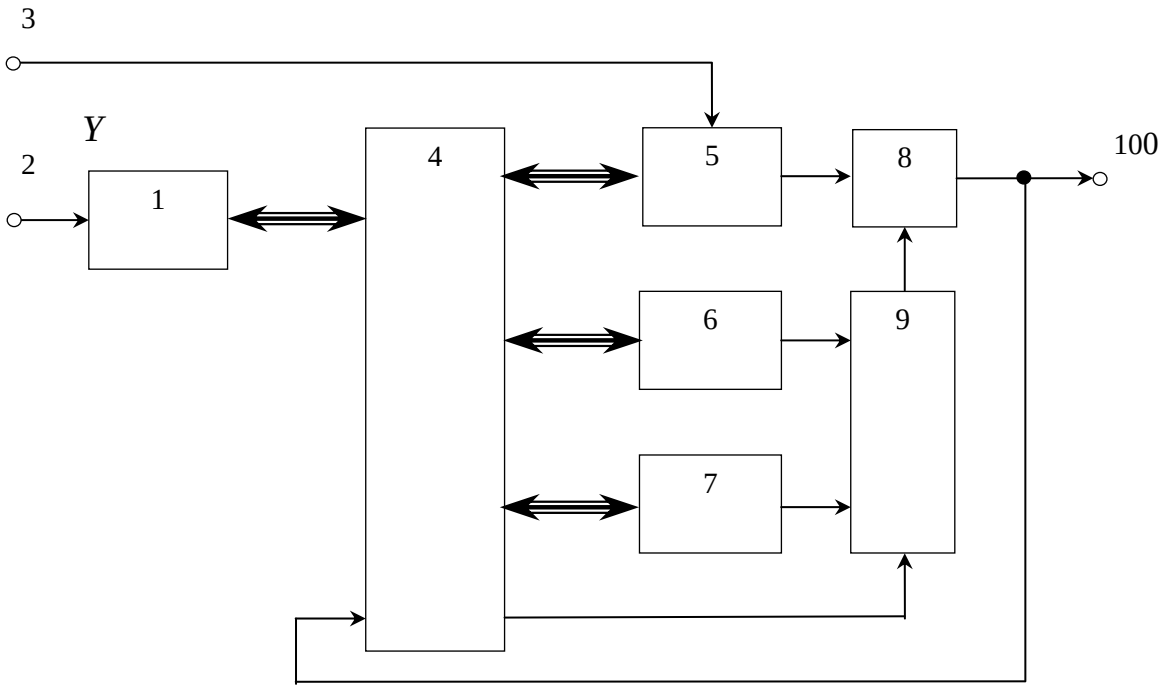

Рис. 4. Структурна схема пристрою пошуку залишків

Пристрій працює так. На початку циклів визначення залишку числа Y у перший n-розрядний регістр зсуву 1 і другий k+1-розрядний регістр зсуву 5, згідно з адресними сигналами блока управління 4 відповідно записуються двійковий код числа Y та мантиса доповнювального коду модуля P, а в третій 6 і четвертій 7 k+1-розрядні регістри зсуву записуються нулі. На початку кожного наступного циклу роботи пристрою на четвертому виході блока управління 4 формується сигнал «1», що дозволяє зсув на один розряд у бік старших розрядів на коді залишку b_{i-1} у регістрі

6 та запис старшого біта числа Y a_i у молодший розряд третього регістра 6, що відповідає запису в цей регістр $2b_{i-1} + a_i$

У кожному поточному циклі роботи пристрою одночасно через мультиплексор 9 на входи однорозрядного накопичувального суматора 8 порозрядно зчитується код мантиси модуля $P([P]_{мд})$ розрядністю $k+1$ та код відповідного регістра 6 або 7. При цьому одночасно відбувається запис нового залишку b_i у відповідний регістр 7 або 6 згідно з адресними входами блока управління 4.

У результаті впродовж $k+1$ такту в однорозрядному накопичувальному суматорі 8 порозрядно формується сума кодів згідно з виразом (1), яка завершується формуванням на виході суматора 8 останнього біта «0» або «1», значення якого надходить на другий вхід блока управління 4. При цьому, якщо вказаний біт є «1», то це означає, що поточний залишок b_i у регістрі 6 менший від значення модуля p ($b_i < P$) і відбувається зсув інформації в регістрі 6 на один розряд у бік старших розрядів, а в молодший розряд записується наступний молодший біт числа Y. У разі формування на виході суматора сигналу «0» це означає, що $b_i \geq P$ і на вхід мультиплексора 9 подається сигнал «0», який формується на четвертому виході блока управління 4 і починається новий цикл підсумування у суматорі 8 кодів $[P]_{мд}$ другого регістра 5 та четвертого регістра 7, запис інформації у регістр 6 до появи біта «0» в кінці k+1 такту на виході суматора 8. У результаті виконується попередній цикл.

Після зчитування останнього молодшого біта числа Y a_1 в одному з регістрів 6 або 7 формується код залишку b_1, який зчитується через мультиплексор 9 і суматор 8 на вихідну шину 10 пристрою, при цьому на виході другого регістра 5 формується сигнал «0».

Основними параметрами під час дослідження процесорів є апаратна складність та швидкодія. Порівняємо швидкодію запропонованого спецпроцесора з відомими аналогами та пристроями для обчислення залишку числа за модулем.

Пристрій пошуку залишків у двійковому коді складається з лічильника, послідовний вхід якого є входом в пристрій, виходи підключені до перших входів суматора, на другі входи якого подається доповнювальний код модуля р, виходи якого підключені до паралельних входів регістра. Функції пристрою реалізуються згідно з мікрокомандами блока управління. Недоліком пристрою є зростання розрядності суматора та регістрів у разі зростання вхідного двійкового числа, а також низька швидкодія, зумовлена наскрізними переносами великорозрядного суматора. Швидкодію такого пристрою позначимо через $V1(n)$.

Відомий пристрій визначення залишку згорткою за непарним модулем $P = 2^n - 1$, який містить n-розрядний регістр і логічні схеми [13]. Його недоліком є велика апаратна складність та функціональна обмеженість, що ускладнює його застосування при визначенні залишку багаторозрядних двійкових чисел з числом розрядів $n=2^{10}..2^{30}$, а також не забезпечує визначення залишку за довільним цілочисловим багаторозрядним модулем P.

Пристрій обчислення залишку шляхом згортки унітарного коду числа містить лічильник і логічні схеми [14]. Його недоліком є низька швидкодія, що обмежує його функціональні можливості при визначенні залишку чисел великої розрядності.

Найближчим за технічною суттю до запропонованого методу є пристрій визначення залишку згорткою за непарним модулем, який містить лічильник, n-розрядний регістр зсуву і k-розрядний суматор, охоплений зворотним зв'язком, шину запису кодового представлення числа [13].

Недоліком пристрою є велика апаратна складність, зумовлена наявністю багаторозрядного двійкового суматора з кількістю розрядів, що дорівнює довжині коду k, багаторозрядного модуля P, та обмежені функціональні можливості визначення залишку тільки за непарним модулем.

При реалізації пристрою доцільно як регістри використати багаторозрядну флеш-пам'ять. В основу запропонованого спецпроцесора входять два регістри на основі флеш-памяті, два цифрових компаратори, суматор, регістр зсуву та блок управління (табл. 4). Його основні параметри – апаратна складність та швидкодія $V2(n)$.

Таблиця 4

Характеристика спецпроцесора пошуку залишків

№	Компоненти	Кількість, шт.	Коефіцієнт апаратної складності C_A,	Кбіт
1	Флеш-память	2	10	1
2	Цифровий компаратор	2	1	0,01
3	Суматор	1	2	0,01
4	Блок управління	1	5	0,1
5	Регістр зсуву	1	3	0,03

Враховуючи вищенаведені характеристики пристроїв пошуку залишків за модулем, наведемо аналітичні вирази швидкодії розглянутих пристроїв:

$$V(n) = \frac{1}{2 \cdot n}, \tag{3}$$

де $V(n)$ – кількість залишків з розрядністю n процесор шукає в унітарному коді за 1 с;

$$V1(n) = 2^{\log_2 p - n}, \tag{4}$$

де V1(n) – кількість залишків з розрядністю n процесор шукає в двійковому коді за 1 с; p – модуль;

$$V2(n) = 2^{40-2n}, \tag{5}$$

де $V2(n)$ – кількість залишків з розрядністю n процесор шукає у базисі Крестенсона за 1 с; $i = 5…9$.

На рис. 5 показано графічні залежності швидкодії розглянутих пристроїв пошуку залишків за модулем від розрядності чисел.

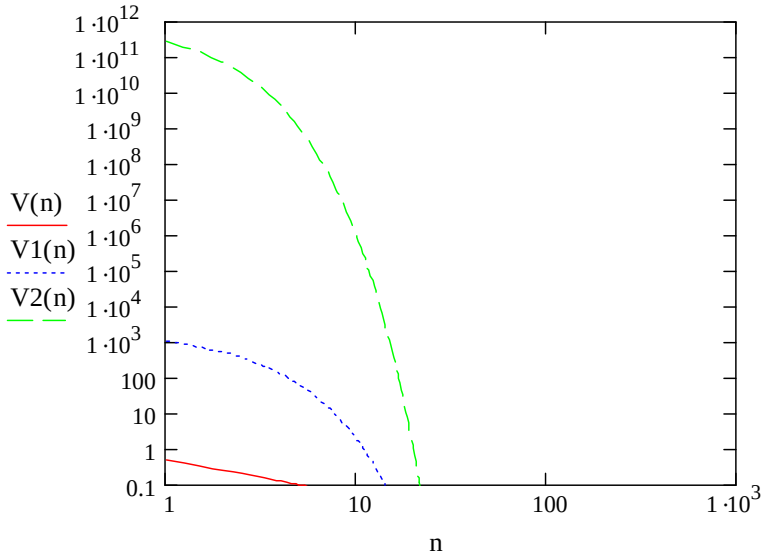

Рис. 5. Швидкодія розглянутих пристроїв пошуку залишків за модулем

З результатів дослідження видно, що запропонований спецпроцесор дає змогу знаходити найбільшу кількість залишків за 1 с порівняно з відомими аналогами.

Висновки

У роботі викладено теоретичні основи опрацювання великорозрядних чисел у криптографії на ЕК. Основними перевагами запропонованих теоретичних положень є зменшення часової та апаратної складностей виконання операцій множення та експоненціювання точок на ЕК на 1-2 порядки, що відкриває нові перспективи високопродуктивного застосування у задачах захисту даних в комп'ютерних системах.

1. Карпінський М., Васильцов І., Якименко І., Кінах Я. Метод генерування параметрів еліптичних кривих // Правове, нормативне, та метрологічне забезпечення системи захисту інформації в Україні. – Київ. – 2003. – С. 67–73. 2. Miller V. S. Use of Elliptic Curves in Cryptography.

Advances in Cryptology // Proceedings of CRYPTO"85, Springer Verlag Lecture in Computer Science 218. - 1986. – P. 417–726. 3. Koblitz N. Elliptic Curve Cryptosystems // Mathematics of Computation, 48. – 1987. – P. 203–209. 4. Акушский И.Я. Машинная арифметика в остаточных классах // Акушский И.Я., Юдицкий Д.И. – М: Сов. радио, 1968. – 440 с. 5. ATKIN A. O. L. 1986a. Schoof's algorithm. Manuscript. 6. ELKIES N. D. Elliptic and modular curves over finite fields and related computational issues. In Computational Perspectives on Number Theory: Proceedings of a Conference in Honor of A. O.L. Atkins, D.A. Buell and J.T. Teitelbaum, eds. AMS/IP Studies in Advanced Mathematics, vol. 7. American Mathematics Society, Providence, R. I.– 1998.– pp. 21–76. 7. Schoof R. Elliptic curves over finite fields and the computation of square roots modulo p./ R. Schoof. – Bordeaux: Math. Comput. – 1985. – № 44. – 483–494 p. 8. Бессалов А.В. Криптосистемы на эллиптических кривых: учеб. пособие / А.В. Бессалов, А.Б. Телиженко. – К.: ІВЦ «Видавництво «Політехніка». 2004. – 224 С. 9. Задірака В.К. Комп'ютерна арифметика багаторозрядних чисел // В.К. Задірака, О.С. Олексюк – К.: 2003. – 264 с. 10. Николайчук Я.М. Теорія джерел інформації. – Тернопіль: ТзОВ "Терно–граф", 2010. – 536 с. 11. Kasyanchuk M. Matrix Algorithms of Processing of the Information Flow in Computer Systems Based on Theoretical and Numerical Krestenson's Basis // M.Kasyanchuk, I.Yakymenko, Ya. Nykolaychuk. / Proceedings of the X–th International Conference "Modern Problems of Radio Engineering, Telecommunications and Computer Science" (TCSET–2010).–L'viv–Slavske.– 2010. – P.241. 12. Николайчук Я.М., Якименко І.З., Воронич А.Р., Волинський О.І. Пристрій визначення залишку багаторозрядного числа: патент на корисну модель № 68872. МПК G 06 F7/00. Опубл. 10.04.2012. Бюл. № 7. 13. Хетагуров Я.А. Повышение надежности цифровых устройств методами избыточного кодирования / Хетагуров Я.А., Руднев Ю.П. – М.: Энергия, 1974. – 272 с. 14. Новиков Л.Г., Шурыгин И.Т. Счётчики импульсов с коэффициентами счёта, управляемыми с помощью двоичного кода / Новиков Л.Г., Шурыгин И.Т. // Приборы и системы управления. – 1972. – № 6, – С. 30–31.

УДК 681.5, 62.5

Ю.В. Яцук, А.Г. Павельчак, М.В. Бобош
Національний університет "Львівська політехніка",
кафедра комп'ютеризованих систем автоматики

СИСТЕМА АВТОМАТИЧНОГО КЕРУВАННЯ СКЛАДСЬКИМ ПРИМІЩЕННЯМ

Розроблено систему автоматичного керування складським приміщенням з використанням програмованих логічних контролерів, реалізовано та протестовано на виготовленому макеті чотири режими роботи програми. Створено автоматизоване робоче місце оператора за допомогою системи диспетчерського контролю та управління.

Ключові слова: програмований логічний контролер, макет, програма керування, система диспетчерського контролю та управління.

Developed model of automatic warehouse using programmable logic controllers, implemented and tested on a breadboard four modes of the program. Created a workstation for operator using specific system supervisory control and data acquisition.

Key words: programmable logic controller, layout, program management, supervisory control and data acquisition.

Вступ

Для автоматизації технологічних процесів використовують різноманітні пристрої: виконавчі механізми, сенсори, пристрої керування тощо. За останні роки вони розвинулись із "простих" до надзвичайно складних систем, які вміщують в одному корпусі не тільки аналогові та цифрові входи-виходи для під'єднання сенсорів та виконавчих механізмів, але і мікроконтролери, в яких розташову-