УДК 004.382

В.С. ГЛУХОВ

Національний університет «Львівська політехніка», Україна

ВБУДОВАНИЙ КОНТРОЛЬ МНОЖЕННЯ В ГАУСІВСЬКОМУ НОРМАЛЬНОМУ БАЗИСІ ПОЛІВ ГАЛУА $GF(2^M)$

У статті пропонується вдосконалений метод виявлення помилок при множенні елементів поля $GF(2^m)$ у гаусівському нормальному базисі типу 2 для пристроїв обробки цифрових підписів, що ґрунтуються на еліптичних кривих. Гаусівський нормальний базис типу 2 рекомендований Державним стандартом України ДСТУ 4145-2002. Для таких базисів парність арифметичного (у полі $GF(2^m)$) добутку двох елементів поля дорівнює парності їхнього логічного добутку, що покладене в основу методу. Реалізація не збільшує час множення і для помножувача Мессі-Омури вимагає додаткових апаратних витрат у вигляді двовходових елементів І та XOR і одного лічильного Т-тригера.

Ключові слова: *гарантоздатні системи, захист інформації, еліптичні криві, поле Галуа $GF(2^m)$, гаусівський нормальний базис типу 2, множення, контроль на парність, вбудований контроль.*

Вступ

Однією з складових гарантоздатних систем є їх конфіденційність. Гарантоздатна система повинна забезпечити захист від несанкціонованого використання інформації, від підміни інформації, від пошкодження інформації.

На сучасному етапі математичною основою для побудови пристроїв захисту інформації є поля Галуа та еліптичні криві. Скінченні поля Галуа $GF(2^m)$ широко використовуються в криптографічних методах, які використовують еліптичні криві. Операції над елементами полів $GF(2^m)$ використовуються для виконання основних операцій над точками еліптичних кривих – додавання та подвоєння. Серед операцій над елементами полів $GF(2^m)$ додавання є найпростішою операцією і вона виконується як логічна операція «виключне АБО» (додавання за модулем 2, XOR – eXclusive OR). В одному з способів ділення елементів поля $GF(2^m)$ A/B спочатку знаходиться обернений елемент B^{-1}, а потім – добуток AB^{-1}. При цьому для знаходження оберненого елемента виконується послідовність операцій множення. Відомі помножувачі елементів поля $GF(2^m)$ у різних базисах: у подвійному, нормальному та поліноміальному. Алгоритм множення у нормальному базисі вперше був запропонований Мессі та Омурою.

Для сучасних криптографічних пристроїв розрядність елементів поля може сягати від 160 до 2048 біт. Апаратна реалізація помножувача для таких полів є важкою задачею і вимагає більш ніж мільйона транзисторів; і, ймовірно, що помилка в роботі одного або більшої кількості транзисторів може приводити до некоректного результату при множенні елементів поля. У роботах останніх років звертається увага на вбудовані методи виявлення помилок (CED - concurrent error detection) за допомогою співставлення парності операндів та результатів. Такий підхід не дозволяє виявити усі можливі помилки, тому також використовуються методи повторного виконання операцій з переставленими місцями операндами.

Головною перевагою нормального базису є виконання операції піднесення до квадрату як циклічного зсуву на 1 біт. Гаусівські нормальні базиси типу 1 та 2 забезпечують менші апаратні витратами при реалізацію помножувачів. Державний стандарт України рекомендує використовувати для обробки цифрових підписів, що ґрунтуються на еліптичних кривих, гаусівський нормальний базис типу 2. У статті пропонується метод виявлення помилок при множенні елементів у гаусівському нормальному базисі типу 2 полів Галуа $GF(2^m)$, які використовуються в пристроях обробки цифрових підписів, що ґрунтуються на еліптичних кривих. Даний метод використовує ознаки парності операндів та результату і не вимагає використання багатовходових елементів XOR. Додаткове обладнання може бути під'єднане до відомих помножувачів, прикладом яких є помножувач Мессі-Омури.

1. Окреслення проблеми

Одним з методів контролю правильності виконання операцій над елементами поля Галуа $GF(2^m)$ є контроль на парність (перевіряється парність кількості двійкових одиниць у представленні елемента поля $GF(2^m)$. Найбільшу складність представляє ко-

нтроль операції множення. Контроль вимагає додаткових апаратних або часових витрат. Тому актуальною є задача вдосконалення існуючих методів виявлення помилок і на їх основі - створення економних вузлів виявлення помилок (детекторів помилок), які здатні працювати з існуючими помножувачами без суттєвої модифікації останніх.

Аналіз останніх досліджень та публікацій. Однією з складових гарантоздатних систем [1] є їх конфіденційність. Гарантоздатна система повинна забезпечити захист від несанкціонованого використання інформації, від підміни інформації, від пошкодження інформації. У той же час, самі пристрої захисту інформації потребують контролю правильності функціонування. Одним з методів такого контролю є контроль на парність. У роботах [2 – 5] викладені основи здійснення контролю на парність (цифрового контролю за модулем 2) результатів арифметичної операції додавання. Показане, що $P_R=P_A+P_B+P_C$, де P_S – парність результату (суми), P_A та P_B – парності операндів, P_C – парність кількості переносів.

На сучасному етапі математичною основою для побудови пристроїв захисту інформації є поля Галуа і еліптичні криві [6]. Над елементами поля Галуа $GF(2^m)$ виконуються операції додавання A+B, множення AB, ділення A/B (шляхом множення на обернений елемент AB^{-1}). Відомі помножувачі елементів поля $GF(2^m)$ у різних базисах: у подвійному, нормальному та поліноміальному. Алгоритм множення у нормальному базисі вперше був запропонований Мессі та Омурою [7].

У роботах [8 – 15] наведені методи та схеми здійснення вбудованого контролю роботи помножувачів елементів поля $GF(2^m)$ у нормальному базисі типу t (t може бути як парним, так і непарним).

У роботі [10] наведені методи та схеми здійснення вбудованого контролю на парність операції множення елементів поля $GF(2^m)$ у гаусівському нормальному базисі типу t. Показане, що для парних t передбачувана парність добутку $P_S^{'} = \sum_{i=0}^{m-1} a_i b_i$, де a_i, b_i – біти операндів – елементів поля A та B. Для непарних t парність результатів обчислюється складніше.

Державний стандарт України [16] серед іншого визначає гаусівські нормальні базисі типу 2, якими дозволяється користуватися під час обробки цифрових підписів, що ґрунтуються на еліптичних кривих.

Метою статті є визначення і обґрунтування методів вбудованого контролю множення елементів поля $GF(2^m)$ у гаусівському нормальному базисі типу 2 для пристроїв обробки цифрових підписів, що ґрунтуються на еліптичних кривих.

2. Алгоритмічні та математичні основи

До складу гарантоздатних систем [1] входять пристрої, які забезпечують їхню конфіденційність. Одним з таких пристроїв є пристрій обробки цифрових підписів, який реалізує криптографічні алгоритми [6, 16].

Стандарт [16] рекомендує для використання поля Галуа $GF(2^m)$ з представленням елементів у поліноміальному базисі та у гаусівському нормальному базисах типу 2.

Нормальний базис для $GF(2^m)$ – це набір виду $BN = \left\{\theta^{2^0}, \theta^{2^1}, ..., \theta^{2^{m-1}}\right\}$ з властивістю, що ніяка підмножина елементів BN у сумі не дорівнює 0, тобто, елементи BN є лінійно незалежним. Для $GF(2^m)$ існують нормальні базиси для кожного додатного цілого m. Представлення поля $GF(2^m)$ у нормальному базисі полягає в сприйнятті двійкового рядка $(a_0 \; a_1 \; a_2 \; \dots \; a_{m-1})$ як елемента $a_0\theta + a_1\theta^2 + a_1\theta^{2^2} + ... + a_{m-1}\theta^{2^{m-1}}$.

Якщо $GF(2^m)$ має гаусівський нормальний базис типу 2 над GF(2), то наступний алгоритм [6] дозволяє ефективно знайти його польовий многочлен.

Вхід: Додатне ціле число m, для якого у полі $GF(2^m)$ існує гаусівський нормальний базис типу 2 над GF(2).

Вихід: Польовий многочлен p(t) для базису.

1. Set q(t) ← 1.
2. Set p(t) ← t + 1.
3. For i = 1 to m – 1 do
   - 3.1. r(t) ← q(t)
   - 3.2. q(t) ← p(t)
   - 3.3. p(t) := t q(t) + r(t).
4. Output p(t).

Загальна схема контролю роботи функціонального вузла на парність наведена на рис. 1, де позначено: A, B – операнди; R – результат; F – функціональний вузол, що підлягає контролю; F’ – вузол передбачення парності результату; P_A, P_B, P_R – біти парності операндів і результату:

$$P_A = \sum_{i=0}^{m-1} a_i \;,\; P_B = \sum_{i=0}^{m-1} b_i \;,\; P_R = \sum_{i=0}^{m-1} r_i \quad (1)$$

(сумування всюди відбувається за модулем 2); P'_R – передбачувана парність результату; $E_R = P_R^{'} \oplus P_R$ – ознака помилки результату.

Під час контролю на парність операцій над елементами поля Галуа $GF(2^m)$ враховують, що при додаванні передбачувана парність результату $P_{\oplus}^{'} = P_A \oplus P_B$.

Передбачувана парність результату множення у поліноміальному базисі (ВР) поля $GF(2^m)$, що утво-

рюється тричленними або п'ятичленними поліномами (парність яких дорівнює 1), задовольняє умові $P'_{BP} \oplus P_C = P_A \cdot P_B$, де P_C – парність «частки», яка утворюється при зведенні результату множення за модулем утворюючого полінома («частка» дорівнює кількості корекцій результату множення при його зведенні за модулем утворюючого полінома).

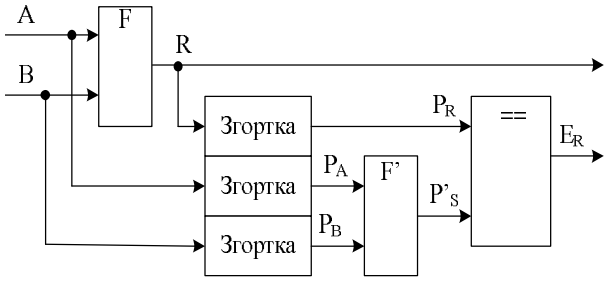

Рис. 1. Схема контролю на парність

Передбачувана парність результатів множення у гаусівському нормальному базисі парного типу (BNp), у тому числі і типу 2, поля $GF(2^m)$

$$P'_{BNp} = \sum_{i=0}^{m-1} a_i b_i \text{ [10].} \qquad (2)$$

Тобто, парність арифметичного (у полі $GF(2^m)$) добутку двох елементів поля дорівнює парності їхнього логічного добутку.

Під час множення двох елементів (А та В) поля Галуа *GF(2^m)* у нормальному базисі (далі множення у нормальному базисі) потрібно виконати такі операції [6]:

– скласти систему рівнянь

$$t = a_{0,0} + a_{0,1}t + a_{0,2}t^2 + ... + a_{0,m-1}t^{m-1} (\mathrm{mod}\, p(t));$$

$$t^2 = a_{1,0} + a_{1,1}t + a_{1,2}t^2 + ... + a_{1,m-1}t^{m-1} (\mathrm{mod}\, p(t));$$

$$t^4 = a_{2,0} + a_{2,1}t + a_{2,2}t^2 + ... + a_{2,m-1}t^{m-1} (\mathrm{mod}\, p(t));$$

……

$$t^{2^{m-1}} = a_{m-1,0} + a_{m-1,1}t + ... + a_{m-1,m-1}t^{m-1} (\mathrm{mod}\, p(t));$$

– з системи рівнянь утворити матрицю M_A з елементами $a_{i,j}$ (при правильно обраному поліномі, що утворює поле, детермінант матриці $\det M_A \neq 0$)

$$M_A = \begin{bmatrix} a_{0,0} & a_{0,1} & \cdots & a_{0,m-1} \\ a_{1,0} & a_{1,1} & \cdots & a_{1,m-1} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m-1,0} & a_{m-1,1} & \cdots & a_{m-1,m-1} \end{bmatrix};$$

– у полі Галуа $GF(2^m)$ знайти матрицю M_B, обернену до M_A: $M_B = M_A^{-1}$, $\det M_B \neq 0$.

– утворити допоміжну матрицю С, де c_i – коефіцієнти полінома $p(t) = t^m + c_{m-1}t^{m-1} + ...c_1 t + c_0$, що утворює відповідне поле Галуа $GF(2^m)$;

$$C = \begin{bmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \\ c_0 & c_1 & c_2 & \cdots & c_{m-1} \end{bmatrix};$$

– обчислити допоміжну матрицю $D = M_A * C * M_B$;

– з матриці D утворити помножувальну матрицю M, з елементами $\mu_{i,j} = d_{j-i,-i}$.

Тоді старший розряд результату $r_{m-1} = A*M*B^t$.

Наступні розряди результату (r_{m-2}, …, r_0) обчислюються за цією самою формулою, тільки замість самих векторів А та В використовуються їхні послідовні циклічні зсуви на один розряд вліво. Дану схему множення ілюструє рис. 2 (а).

Помножувач згідно з рис. 2 далі умовно називається помножувачем з лівим зсувом, а відомий помножувач Мессі-Омури для такої ж матриці М – помножувачем з правим зсувом.

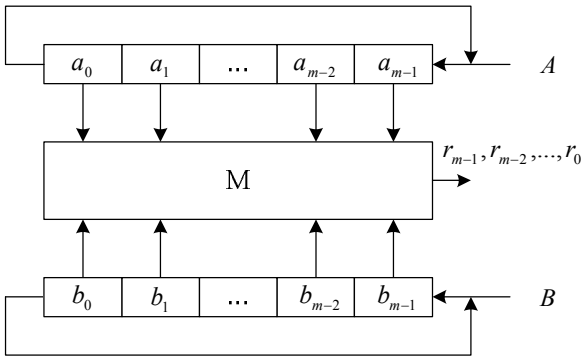

Рис. 2. Помножувач згідно з [6]

У полі Галуа $GF(2^m)$ елементами матриці *M* будуть тільки 0 та 1, при використання гаусівського нормального базису типу 2 кількість 1 у матриці буде мінімально можливою і рівною $2m$-1.

На практиці операції з матрицям перетворюються на обчислення згідно з відомими формулами множення матриць, велика кількість 0 у матриці дозволяє суттєво спростити ці формули.

Математична матриця *M* реалізується у вигляді логічної матриці (рис. 3)), яка складається з:

матриці з m-1 двовходових суматорів за модулем 2 (xor2);

матриці з m двовходових елементів 2I;

1-го m-входового суматора за модулем 2 (xor_m).

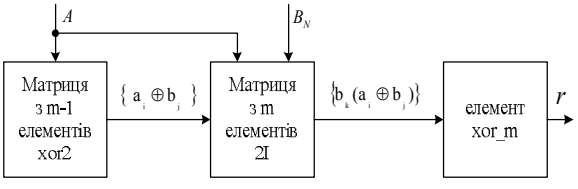

Рис. 3. Логічна матриця *M*

3. Вбудований контроль множення у гаусівському нормальному базисі типу 2

Для гаусівського нормального базису типу 2 з формул (1) та (2) випливає, що

$$E_R = P_R' \oplus P_R = \sum_{i=0}^{m-1} a_i b_i \oplus \sum_{j=0}^{m-1} s_j = \sum_{i=0}^{m-1} (a_i b_i \oplus s_i) \quad (3)$$

При відсутності помилок $E_R = 0$.

Відомий [15] послідовний помножувач для нормального базису поля $GF(2^m)$ з детектором помилок на основі тригера XOR#1, на якому підраховується передбачувана парність результату і (m+1)–входового елемента XOR#2, за допомогою якого формується ознака помилки $\hat{e}_C$ (рис. 4).

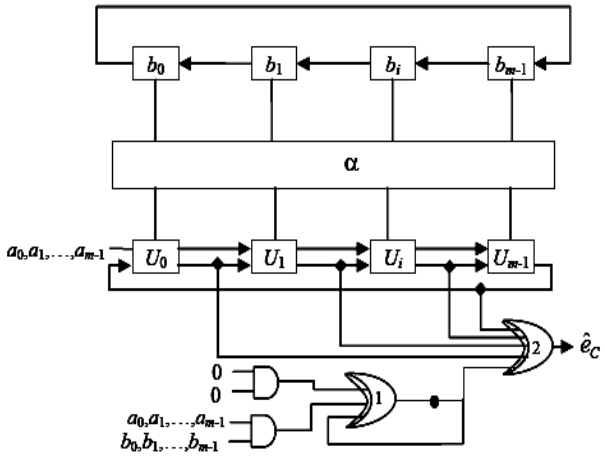

Рис. 4. Відомий послідовний помножувач

З метою зменшення апаратних витрат пропонується інша схема детектора помилок (рис. 5), яка відповідає формулі (3). До складу пропонованого детектора входять двовходовий елемент XOR та Т-тригер, на якому фіксується ознака помилки. Схема наведена на рис. 5. Після закінчення множення стан тригера дорівнює 0 при відсутності помилок і 1 при наявності непарної кількості помилок.

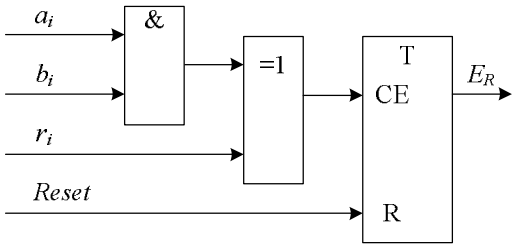

Рис. 5. Пропонований вузол CED детектора помилок

Схема вузла помножувача, з вузлом виявлення помилок наведена на рис. 6.

Т-тригер працює синхронно з регістрами зсуву помножувача. Перед початком множення тригер повинний бути скинутий в стан 0.

Результати порівняння помножувачів містить таблиця 1.

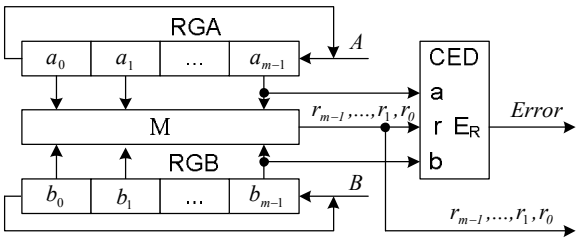

Рис. 6. Пропонований помножувач з вузлом виявленням помилок

Таблиця 1

Порівняння помножувачів

Помножувач	Тригерів	Елементів I	Елем. XOR	Входів елементів XOR
Відомий	1	1	2	m+4
Пропонований	1	1	1	2

Висновки

У статті визначений і обґрунтований метод вбудованого контролю операції множення елементів поля $GF(2^m)$ у гаусівському нормальному базисі типу 2 для пристроїв обробки цифрових підписів, що ґрунтуються на еліптичних кривих.. Для таких базисів парність арифметичного (у полі $GF(2^m)$) добутку двох елементів поля дорівнює парності їхнього логічного добутку, що покладене в основу методу. Реалізація не збільшує час множення і вимагає додаткових апаратних витрат у вигляді двовходових елементів I та XOR і одного лічильного Т-тригера.

Література

1. Basic Concepts and Taxonomy of Dependable and Secure Computing / A. Avizienis, J.C. Laprie, B. Randell, C. Landwehr // IEEE Transactions on Dependable and Secure Computing. – 2004. – vol. 1. – P. 11 - 33.

2. Журавлев Ю.П. Надежность и контроль ЭВМ / Ю.П. Журавлев, Л.А.Котелюк, И. Циклинский. – М.: Сов. радио, 1978. – 416 с.

3. Хетагуров А.Я. Основы проектирования управляющих вычислительных систем / А. Я. Хетагуров. – М.: Радио и связь, 1991. – 288 с.

4. Справочник по цифровой вычислительной технике. Под ред. Б.Н.Малиновского. – К.: Техніка, 1974. – 222 с.

5. Справочник по цифровой вычислительной технике (электронные вычислительные машины и системы). Под ред. Б.Н. Малиновского. – К.: Техніка, 1980. – 436 с.

6. IEEE Std 1363-2000 IEEE Standard Specifications for Public-Key Cryptography Sponsor Microprocessor and Microcomputer Standards Committee of the IEEE Computer Society. Approved 30 January 2000.

7. U. S. Patent Number 4,587,627 U.S.A. Computational method and apparatus for finite field arithmetic / J. Omura and J. Massey. – May 1986.

8. Lee C.Y. Concurrent error detection in bit-serial normal basis of GF(2^m) / C.Y. Lee, C.C. Chen, E.H. Lu. // VLSI Test Technology Workshop. – July 16-18, 2008. Tainan, Taiwan.

9. Lee C.Y. Concurrent error detection in bit-serial normal basis multipliers over GF(2^m) / C.Y. Lee, C.C. Chen, E.H. Lu //. IEEE Trans. VLSI. 2010.

10. Lee C.Y. Concurrent Error Detection in Multiplexer-Based Multiplier for Normal Basis of GF(2^m) Using Double Parity Prediction Scheme / C.Y. Lee, C.W. Chiou, J.M. Lin // The Journal of Signal Processing Systems. Springer Science + Business Media, LLC. – April 2009. Published online 21.

11. Concurrent Error Detection and Correction in Gaussian Normal Basis Multiplier over GF(2^m) / C.W. Chiou, C.C. Chang, C.Y. Lee, T.W. Hou, J.M. Lin // IEEE Transactions on Computers. – June 2009 – Vol. 58, no. 6.

12. Lee C.Y. Concurrent Error Detection in Digit-Serial Normal Basis Multiplication over GF(2^m) / C.Y. Lee. // 22nd International Conference on Advanced Information Networking and Applications – Workshops (AINA2008) March 25 - 28, 2008, Okinawa, Japan.(EI). –P. 1499-1504.

13. Lee C.Y. Concurrent Error Detection Architectures for Gaussian Normal Basis Multiplication over GF(2^m). / C.Y. Lee. // Integration – The VLSI Journal. 2010/01.

14. Lee C.Y. Concurrent Error Detection in Bit-Serial Normal Basis Multiplication Over GF(2^m) Using Multiple Parity Prediction Schemes. Very Large Scale Integration (VLSI) Systems. / C.Y. Lee, P.K. Meher, J.C. Patra, // IEEE Transactions on. Accepted for future publication. First Published: 2009-08-25.

15. Concurrent error detection/correction in finite field arithmetic architectures over GF(2^m) / C.Y. Lee, P.K. Meher, C.W. Chiou, J.M. Lin. // Cryptography Research Perspectives. – 2008 Nova Science Publishers, Inc. P. 49-96.

16. ДСТУ 4145-2002. Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевіряння. Київ. Державний комітет України з питань технічного регулювання та споживчої політики. 2003.

Поступила в редакцию 21.01.2010

Рецензент: д-р техн. наук, проф., проф. кафедри СКС Р.Б. Дунець, Національний університет «Львівська політехніка», Львів.

ВСТРОЕННЫЙ КОНТРОЛЬ УМНОЖЕНИЯ В ГАУССОВСКОМ НОРМАЛЬНОМ БАЗИСЕ ПОЛЕЙ ГАЛУА GF(2^M)

В.С. Глухов

В статье предлагается усовершенствованный метод выявления ошибок при умножении элементов поля GF(2m) в гауссовском нормальном базисе типа 2 для устройств обработки цифровых подписей, которые основываются на эллиптических кривых. Гауссовский нормальный базис типа 2 рекомендован Государственным стандартом Украины ДСТУ 4145-2002. Для таких базисов четность арифметического (в поле *GF*(2^m)) произведения двух элементов поля равняется четности их логического произведения, что положено в основу метода. Реализация не увеличивает время умножения и для умножителя Месси-Омуры требует дополнительных аппаратных расходов в виде двухвходовых элементов И и XOR, а также одного счетного Т-триггера.

Ключевые слова: гарантоспособные системы, защита информации, цифровая подпись, эллиптические кривые, поле Галуа GF(2^m), гауссовский нормальный базис типа 2, умножение, контроль на четность, обнаружение ошибок.

CONCURRENT ERROR DETECTION FOR GAUSSIAN NORMAL BASIS TYPE 2 MULTIPLICATION OVER GF(2M)

V.S. Hlukhov

In this paper concurrent error detection schemes have been presented for a Gaussian normal basis type 2 over GF(2^m) multiplier. Gaussian normal basis of type 2 is recommended to use by Ukraine standard DSTU 4145-2002. For this basis the parity of arithmetic product of two field elements is equal to parity of their logical product. This feature is used in proposed method. For Massey-Omura multiplier additional hardware resources are two-input AND and XOR gates and one T-type flip-flop.

Key words: dependable system, information security, elliptic curve, Galois Field GF(2^m), Gaussian normal basis of type 2, multiplication, parity check, concurrent error detection.

Глухов Валерій Сергійович – канд. техн. наук, доцент, доцент кафедри електронних обчислювальних машин Національного університету «Львівська політехніка», Львів, Україна, e-mail: valeriygl@ukr.net.