УДК 004.382

В.С. ГЛУХОВ, Р. ЕЛІАС

Національний університет «Львівська політехніка», Україна

ВИЯВЛЕННЯ ПОМИЛОК ПРИ ЗНАХОДЖЕННІ ОБЕРНЕНОГО ЕЛЕМЕНТА В ГАУСІВСЬКОМУ НОРМАЛЬНОМУ БАЗИСІ ТИПУ 2 ПОЛІВ ГАЛУА GF(2^m)

У статті пропонується метод виявлення помилок при знаходженні оберненого елемента в гаусівському нормальному базисі типу 2 полів Галуа GF(2^m), які використовуються в пристроях обробки цифрових підписів, що ґрунтуються на еліптичних кривих. Гаусівський нормальний базис типу 2 рекомендований Державним стандартом України ДСТУ 4145-2002. Пропонується останньою операцією при знаходженні оберненого елемента виконувати операцію множення проміжного результату на елемент поля Галуа, для якого шукається обернений елемент. Результат контролю останнього множення одночасно буде і результатом контролю усієї операції знаходження оберненого елемента.

Ключові слова: *гарантоздатні системи, захист інформації, еліптичні криві, поле Галуа GF(2^m), гаусівський нормальний базис типу 2, обернений елемент, 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 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, наприклад, у подвійному, нормальному та поліноміальному.

Для сучасних криптографічних пристроїв розрядність елементів поля може сягати від 160 до 2048 біт. Апаратна реалізація вузла знаходження оберненого елемента 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. У роботах останніх років звертається увага на вбудовані методи виявлення помилок (CED – concurrent error detection) за допомогою парності операндів та результатів. Такий підхід не дозволяє виявити усі можливі помилки, тому також використовуються методи повторного виконання операцій, що використовують переставлені місцями операнди.

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 знаходженні оберненого елемента в 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 операнда та результату і не вимагає виконання повторного знаходження оберненого елемента. 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). Відомі методи контролю правильності виконання операції знаходження оберненого еле-

мента поля Галуа $GF(2^m)$ розглядають її як послідовність простіших операцій над елементами поля $GF(2^m)$ - множення. Контроль при цьому зводиться до контролю послідовності операцій множення. Контроль вимагає додаткових апаратних або часових витрат, які є значними при переході до контролю більш простих операцій. Для зменшення витрат необхідно розробляти нові вузли помножувачів з властивістю вбудованого контролю, які різняться від помножувачів без можливості контролю. Тому актуальною є задача впровадження контролю власне операції знаходження оберненого елемента без прив'язки до методів його знаходження та без модифікації існуючих помножувачів.

2. Аналіз останніх досліджень та публікацій, мета статті

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 та 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}).

У роботі [7] для перевірки правильності знаходження оберненого елемента використовується тотожність $(A*B^{-1})*B= A*(B^{-1}*B) = A$. Перевірка ділення (знаходження оберненого елемента B^{-1}) здійснюється додатковим множенням результату ділення на B. У результаті такої перевірки повинно бути отримане значення аргументу A.

У роботі [8] запропонований метод вбудованої перевірки роботи систолічного вузла знаходження оберненого елемента поля $GF(2^m)$ у поліноміальному базисі, шляхом перевірки роботи його складових частин.

У роботах [9 – 15] наведені методи та схеми здійснення вбудованого контролю на парність роботи помножувачів елементів поля $GF(2^m)$ у нормальному базисі типу t (t може бути як парним, так і непарним).

У роботі [11] 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 A та B– елементів поля. Для непарних t, а також для поліноміального [16, 17] і дуального [18, 19] базисів парність результатів обчислюється складніше.

У роботі [20] розглянуті методи виявлення помилок у систолічних структурах, а в роботі [21] – методи виправлення помилок.

Державний стандарт України [22] серед іншого визначає гаусівські нормальні базиси типу 2, якими дозволяється користуватися під час обробки цифрових підписів, що ґрунтуються на еліптичних кривих.

Метою статті є визначення і обґрунтування методу контролю правильності знаходження оберненого елемента поля $GF(2^m)$ у гаусівському нормальному базисі типу 2 без контролю проміжних результатів.

3. 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, 22], що мають саме ієрархічну структуру (

рис. 1).

Стандарт [22] рекомендує для використання поля Галуа $GF(2^m)$ з представленням елементів у поліноміальному та у гаусівському нормальному базисах типу 2.

Нормальний базис для $GF(2^m)$ – це набір виду $B_N = \left\{\theta^{2^0}, \theta^{2^1}, ..., \theta^{2^{m-1}}\right\}$ з властивістю, що ніяка підмножина елементів B_N у сумі не дорівнює 0, тобто, елементи B_N 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 $(a_0\, a_1\, a_2 \ldots a_{m-1})$ як елемента

$$a_0\theta + a_1\theta^2 + a_1\theta^{2^2} + ... + a_{m-1}\theta^{2^{m-1}}.$$

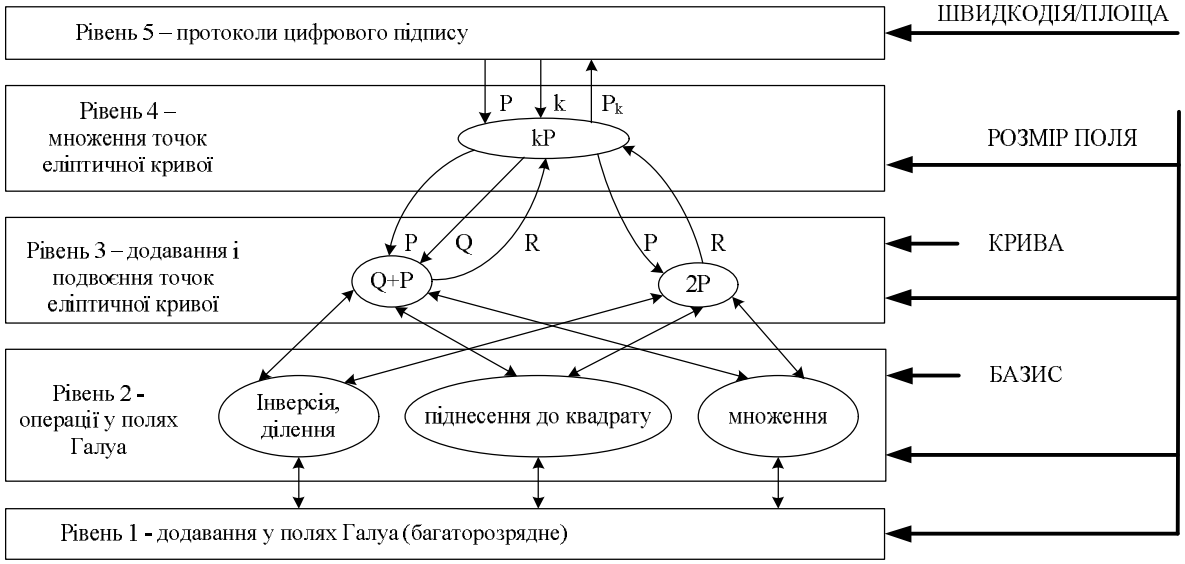

Рис. 1. Ієрархічні рівні алгоритмів

Помножувач для нормального базису був запропонований Мессі та Омурою [23].

Відомий алгоритм [6] знаходження оберненого елемента у нормальному базисі:

Вхід: Поле $GF(2^m)$ і відмінний від нуля елемент поля B.

Вихід: Обернений елемент B^{-1}.

1. Let $m - 1 = m_r m_{r-1} \ldots m_1 m_0$ be the binary representation of $m - 1$, where the most significant bit m_r of $m - 1$ is 1.
2. Set $\eta \leftarrow B$ and $k \leftarrow 1$.
3. For i from r – 1 downto 0 do
3.1. Set $\mu \leftarrow \eta$.
3.2. For j = 1 to k do
3.2.1. Set $\mu \leftarrow \mu^2$.
3.3. Set $\eta \leftarrow \mu\eta$ and $k \leftarrow 2k$.
3.4. If $m_i = 1$, then set $\eta \leftarrow \eta^2 B$ and $k \leftarrow k + 1$.
4. Output η^2.

За визначення $BB^{-1} = B/B = 1$. У нормальному базисі поля $GF(2^m)$ одиничний елемент представляється у вигляді 1…1, де кількість двійкових 1 дорівнює m. Стандарт [22] рекомендує використовувати гаусівський нормальний базис типу 2 для полів з непарним m. Тобто парність одиничного елемента $P_1=1$.

Загальна схема контролю роботи функціонального вузла на парність наведена на рис. 2, 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:

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

(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 $P'_{\oplus} = P_A \oplus P_B$.

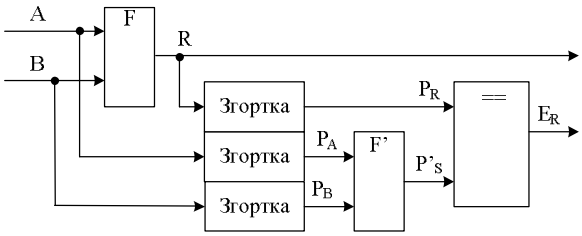

Рис. 2. Схема контролю на парність

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

$$P'_{B_{Np}} = \sum_{i=0}^{m-1} a_i b_i \text{ [11].} \qquad (2)$$

4. Визначення помилок при знаходженні оберненого елемента у гаусівському нормальному базисі типу 2

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

$$P'_{B_{Np}} = \sum_{i=0}^{m-1} b_i b_i^{-1} = P_1 = 1. \qquad (3)$$

Дану властивість пропонується покласти в основу методу виявлення помилок при знаходженні оберненого елемента. Перевірку правильності знаходження оберненого елемента можна виконати додатковим множенням. Ознакою правильного знаходження оберненого елемента є правильний результат такого множення – одиничний елемент з парністю P_1=1.

Недоліком такого методу є складність порівняння результату контрольного множення з 1, а також необхідність виконання додаткових операцій множення і порівняння після знаходження оберненого елемента. Цей недолік можна усунути модифікацією алгоритму [6] знаходження оберненого елемента, так щоб останньою операцією було множення на елемент поля B, для якого шукають обернене значення:

$$B^{-1} = B \cdot B^{-2} = B \cdot (B^2)^{-1} = B \cdot X. \qquad (4)$$

Тобто, пропонується обернений елемент шукати для елемента B^2 ($B^{-2} = X$), після чого виконується множення знайденого значення на число B. Як і в попередньому випадку для контролю потрібно виконати додаткове множення.

Пропонується схема детектора помилок при обчисленні оберненого елемента (рис. 3), яка відповідає формулі (4). Детектор може бути під'єднаний до існуючого помножувача Мессі-Омури [23] (помножувач із правим зсувом) або до аналогічного помножувача, визначеного стандартом [6] (помножувач із лівим зсувом) і містить двовходовий елемент *XOR* та *T*-тригер, на якому фіксується парність добутку прямого та оберненого елементів поля. Схема детектора наведена на рис. 3. Після закінчення множення стан тригера дорівнює 1 при відсутності помилок і 0 при наявності помилки. Дана ознака має сенс тільки при виконанні останнього множення у послідовності обчислення оберненого елемента.

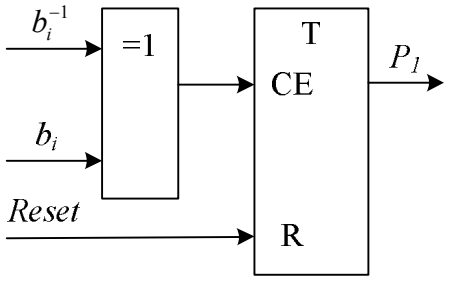

Рис. 3. Пропонований вузол CED детектора помилок при обчисленні оберненого елемента

Схема вузла помножувача, де позначені операнди, що приймають участь в операції множення на останньому кроці модифікованого алгоритму знаходження оберненого елемента, з вузлом визначення помилок при обчисленні оберненого елемента наведена на рис. 4.

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

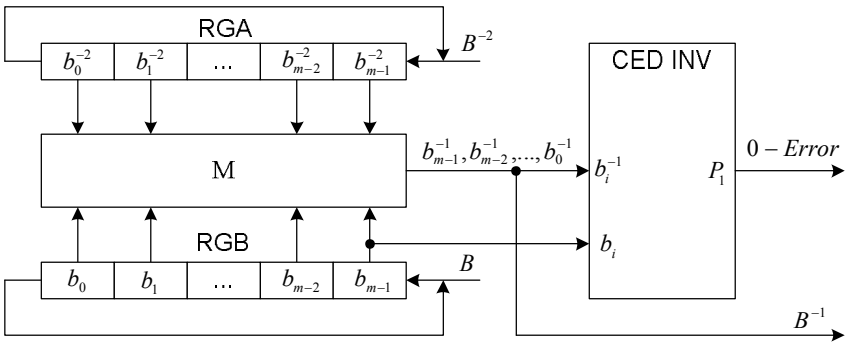

Рис. 4. Пропонований помножувач з лівим зсувом з вузлом визначення помилок при знаходженні оберненого елемента

Висновки

У статті визначений і обґрунтований метод контролю правильності знаходження оберненого елемента поля GF(2^m) у гаусівському нормальному базисі типу 2 без контролю проміжних результатів. Для таких базисів парність добутку прямого та оберненого елементів

$$P'_{NBp} = \sum_{i=0}^{m-1} b_i b_i^{-1} = P_1 = 1,$$

що покладене в основу методу. Реалізація методу збільшує час знаходження оберненого елемента на час виконання одного множення і вимагає додаткових апаратних витрат у вигляді одного елемента *XOR* та одного лічильного Т-тригера.

Література

1. Avizienis A. 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. Цикинский. – 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.

5. Справочник по цифровой вычислительной технике (электронные вычислительные машины и системы) / под ред. Б.Н. Малиновского. К.: Техніка, 1980.

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. Stern R. Register Transfer Level Concurrent Error Detection in Elliptic Curve Crypto Implementations. / R. Stern, N. Joshi, K. Wu, R. Karri // Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC 2007). – Vienna, Austria. – September 10, 2007.

8. Chuang Y-C. On-line error detection schemes for a systolic finite-field inverter / Y.-C. Chuang, C.-W. Wu // Test Symposium, 1998. Proceedings. – Seventh Asian Volume. – Issue 2-4. –Dec 1998. – P. 301-305.

9. 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.

10. 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. – 2010/02.

11. 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, 2009.

12. Chiou C.W. 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. – Vol. 58. – № 6. – June 2009.

13. 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). – 2008. –March 25-28. – Okinawa, Japan. – P.1499-150.

14. 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.

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

16. Lee C.-Y. Concurrent error detection in polynomial basis multiplier over GF(2^m) / C.-Y. Lee, C.W. Chiou, J.-M. Lin // Journal of Electronic Testing: Theory and Applications. – 2006/05.

17. Chiou C.W. Concurrent error detection in Montgomery multiplication over GF(2^m) / C.W. Chiou, C.-Y. Lee, A.-W. Deng, J.-M. Lin // IEICE Transactions on Fundamentals. 2006. – Vol. E89-A. – №2. – P. 566-574.

18. Chiou C.W. Concurrent Error Detection and Correction in Dual Basis Multiplier over GF(2^m) / C.W. Chiou, C.-Y. Lee, J.-M. Lin, T.-W. Hou, C.-C. Chang // IET Circuits, Devices & Systems. – 2009. – Vol. 3. – Iss. 1. – P. 22–40

19. Lee C.-Y. Concurrent error detection in a bit-parallel systolic multiplier for dual basis of GF(2^m) / C.-Y. Lee, C.W. Chiou, J.-M. Lin // Journal of Electronic Testing: Theory and Applications. –2005. – Vol. 21. – P. 539-549.

20. Bayat-Sarmadi S. Concurrent Error Detection in Finite Field Arithmetic Operations using Pipelined and Systolic Architectures / S. Bayat-Sarmadi, M.A. Hasan // IEEE Transactions on Computers. – 2009. – Vol. 58. – №11. – P. 1553-1567.

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

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

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

Надійшла до редакції 13.01.2010

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

ОБНАРУЖЕНИЕ ОШИБОК ПРИ НАХОЖДЕНИИ ОБРАТНОГО ЭЛЕМЕНТА В ГАУССОВСКОМ НОРМАЛЬНОМ БАЗИСЕ ТИПА 2 ПОЛЕЙ ГАЛУА GF(2^m)

В.С. Глухов, Р. Элиас

В статье предлагается метод обнаружения ошибок при нахождении обратного элемента в Гауссовском нормальном базисе типа 2 полей Галуа GF(2^m), которые используются в устройствах обработки цифровых подписей на основе эллиптических кривых. Гауссовский нормальный базис типа 2 рекомендуется Государственным стандартом Украины ДСТУ 4145-2002. Предлагается последней операцией при нахождении обратного элемента выполнять умножение промежуточного результата на элемент поля Галуа, для которого ищется обратный элемент. Результат контроля последнего умножения одновременно будет и результатом контроля операции нахождения обратного элемента.

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

CONCURRENT ERROR DETECTION FOR A GAUSSIAN NORMAL BASIS TYPE 2 GF(2^m) INVERTER

V.S. Hlukhov, R. Elias

In this paper concurrent error detection (CED) schemes have been presented for a Gaussian normal basis type 2 over GF(2^m) inverter. Gaussian normal basis of type 2 is recommended to use by Ukraine standard DSTU 4145-2002. It is proposed to perform as a final inversion operation a multiplication of intermediate result by the element of the GF(2^m) which a reverse element is searched for. A result of such multiplication check simultaneously will be the result of full inversion process check.

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

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

Родріг Еліас – аспірант 2 року навчання, кафедра електронних обчислювальних машин, Національний університет «Львівська політехніка», Львів, Україна, e-mail: rodrigue.elias@liu.edu.lb.