УДК 004.382

А.Р. Добуш, А.Т. Костик
Національний університет "Львівська політехніка",
кафедра електронних обчислювальних машин

МЕТОДИ ВБУДОВАНОГО КОНТРОЛЮ ВИКОНАННЯ ОПЕРАЦІЙ У ПОЛЯХ ГАЛУА ДЛЯ РЕАЛІЗАЦІЇ В НВІС

Наведено класифікацію методів для знаходження помилок під час виконання операцій у скінченних полях. Показана можливість використання систолічної архітектури і методу з надлишковими витратами часу для виявлення та виправлення помилок, що можуть виникати під час множення елементів полів Галуа, поданих в оптимальному нормальному базисі другого типу. Цей метод виявлення і виправлення помилок може бути застосований під час опрацювання цифрових підписів згідно з прийнятим в Україні стандартом.

Ключові слоава: поля Галуа, оптимальний нормальний базис, виправлення помилок.

The distribution of the categories of schemes for detecting errors when performing operations in finite fields was described. The possibility of using systolic architecture and method with time redundancy to correct errors that may occur during multiplication of the elements of the Galois field represented in an optimal normal basis of the second type was described. This method of error detection and correction can be used for processing the digital signature in accordance with the standard adopted in Ukraine.

Key words: Galois field, optimal normal basis, error correction.

Вступ

До операцій над елементами поля Галуа належать додавання, множення, піднесення до квадрата та знаходження оберненого елемента. Перевагами оптимального нормального базису є виконання операції піднесення до квадрата як циклічного зсуву на 1 біт та швидше знаходження оберненого елемента. Оскільки додавання та піднесення до квадрата елементів поля Галуа є порівняно простими операціями, основну увагу потрібно приділити операції множення.

У роботі розглянуто метод виявлення і виправлення помилок, що виникають під час множення елементів поля Галуа, які представлені в оптимальному нормальному базисі другого типу. Запропонований метод виправлення помилок передбачається використати під час опрацювання цифрового підпису згідно з державним стандартом.

Аналіз літературних джерел

Деякі випадкові помилки, під час опрацювання операцій над елементами скінченних полів можуть бути виявлені під час виконання операцій вищого рівня, наприклад, в еліптичній криптографії, якщо точка опиняється за межами еліптичної кривої – вона може бути легко виявлена за допомогою перевірки точки [1, 2]. Однак такі перевірки не завжди спрацьовують. У разі еліптичних кривих помилка може перемістити точку в іншу точку, не залишаючи криву, і це використовується в так званій "sign change fault attack" – атаці на еліптичну криву шляхом змін знака [3]. Тому необхідним є впровадження механізмів виявлення і, за можливості, виправлення помилок під час виконання операцій у скінченних полях.

Поля Галуа та еліптичні криві є математичною основою для побудови багатьох пристроїв захисту інформації. Під час проектування цифрових систем захисту інформації велика увага приділяється досягненню прийнятного рівня безпеки такої системи. Несправності можуть виник-

нути з природних причин або з навмисного впливу на пристрій зловмисника, як описано у [2–4]. Будь-яка несправність, ймовірно, призведе до помилкових результатів, які можуть зробити пристрій недієздатним, або може допомогти зловмисникові. Тому виправлення помилок під час виконання операцій над полями Галуа, згідно з прийнятим в Україні стандартом формування та перевірки цифрових підписів, є дуже важливим чинником стабільності і захищеності системи опрацювання цифрових підписів.

У [5] рекомендується збільшення степеня основного поля Галуа для цифрових підписів. Апаратна реалізація пристроїв для виконання операцій над елементами полів Галуа зі збільшеним степенем вимагатиме збільшення кількості використовуваних транзисторів. Помилка у роботі одного або кількох транзисторів, ймовірно, призведе до помилкових результатів. Також серед активних атак на криптосистеми поширеним типом атаки є атака на помилки.

Сьогодні запропоновано багато схем для знаходження помилок під час виконання операцій у скінченних полях. Більшість цих методів можна розділити на категорії:

- використання парності суми бітів. Передбачається парність суми бітів результату операції і порівнюється з парністю суми бітів отриманого результату. Деякі приклади описані у [6–8];
- методи, які використовують масштабування вхідних множників за допомогою факторизації, і після множення правильність результату перевіряється одним або двома діленнями [9];
- нелінійні методи [10]. Цей підхід дорогий з погляду економії місця на кристалі та часу виконання, і може бути не дуже ефективним для виявлення випадкових помилок;
- методи з надлишковістю часу [11] або об'єму на кристалі, як показано на рис. 1, *а* і *б*. Метод з надлишковістю часу передбачає повторне обчислення і порівняння отриманих результатів. Використання такого методу вимагає збільшення затрат часу в n разів, залежно від реалізації. Своєю чергою, метод з надлишковістю об'єму на кристалі передбачає паралельне обчислення та порівняння вихідних результатів; такий метод передбачає дублювання обчислювальних елементів.

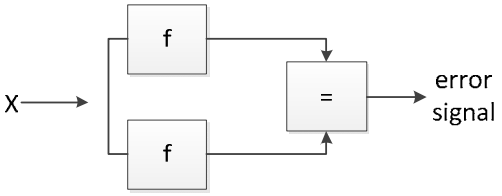

Рис. 1, а: паралельний обрахунок

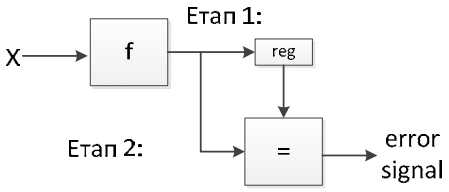

Рис. 1, б: послідовний обрахунок

Ефективність виконання операцій у скінченних полях дуже залежить від представлення елемента у скінченному полі. Елементи в полях GF(2^m) можуть бути представлені у трьох базисах: поліноміальному, подвійному і нормальному. В [12] використовуються поліноміальний і нормальний базиси. У [13] обґрунтовано, що під час проектування пристрою на кристалі, доцільніше використовувати саме оптимальний нормальний базис. Показано, що апаратно множення у поліноміальному і нормальному базисах вимагає приблизно однакових затрат часу. Однак найпрацемісткіша операція над елементами поля Галуа GF(2^m) – обчислення оберненого елемента у нормальному базисі виконується на порядок швидше.

Отже, для забезпечення стабільності і захищеності системи опрацювання цифрових підписів, потрібно не лише формувати сигнал про помилку під час виконання операцій над елементами поля Галуа, але і мати можливість виправляти такі помилки.

Мета роботи – представити метод для виправлення помилок, що можуть виникати під час виконання операції множення елементів полів Галуа, представлених в оптимальному, нормальному базисі другого типу, який може бути застосований під час опрацювання цифрових підписів згідно з прийнятим в Україні стандартом.

Алгоритмічні та математичні основи

Арифметичні операції у полях Галуа GF(2^m) широко використовуються в теорії кодування, цифрової обробки сигналів та криптосистем з відкритим ключем. Використання полів Галуа передбачає доволі швидке виконання арифметичних операцій над елементами полів: додавання, множення, знаходження оберненого елемента і піднесення до степеня. Додавання в GF(2^m) виконується звичайною операцією XOR. Операції знаходження оберненого елемента і піднесення до степеня потребує набагато більше часу, ніж інші базові операції додавання і множення. Виконання операції знаходження оберненого елемента виконується за допомогою ітеративного множення. Тому ефективна реалізація множення елементів поля Галуа є основним у криптографічних пристроях, які використовують поля Галуа.

Нормальний базис для GF(2^m) – це набір виду $BN = \{\theta^{2^0}, \theta^{2^1}, ..., \theta^{2^{m-1}}\}$ з властивістю, що жодна підмножина елементів BN в сумі не дорівнює 0, тобто елементи BN є лінійно незалежні. Представлення поля GF(2^m) у нормальному базисі полягає у сприйнятті двійкового рядка (a_0 a_1 a_2 a_{m-1}) як елемента $a_0\theta + a_1\theta^2 + a_2\theta^{2^2} + ... + a_{m-1}\theta^{2^{m-1}}$.

У [12] описані дії, які потрібно виконати для множення двох елементів (A та B) поля Галуа у нормальному базисі:

– скласти систему рівнянь:

$$t = a_{0,0} + a_{0,1}t + a_{0.2}t^2 + ... + a_{0.m-1}t^{m-1} \pmod{p(t)};$$
$$t^2 = a_{1,0} + a_{1,1}t + a_{1.2}t^2 + ... + a_{1.m-1}t^{m-1} \pmod{p(t)};$$
$$t^4 = a_{2,0} + a_{2,1}t + a_{2.2}t^2 + ... + a_{2.m-1}t^{m-1} \pmod{p(t)};$$
$$\text{..... ....}$$
$$t^{2^{m-1}} = a_{m-1,0} + a_{m-1,1}t + a_{m-1.2}t^2 + ... + a_{m-1.m-1}t^{m-1} \pmod{p(t)};$$

– з системи рівнянь утворити матрицю M_A з елементами $a_{i,j}$:

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

– 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 C, де c_i – коефіцієнти полінома $p(t) = t^m + c_{m-1}t^{m-1} + \ldots + c_1 t + c_0$, що утворює відповідне поле Галуа GF(2^m):

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

– обчислити допоміжну матрицю $D = M_A \cdot C \cdot M_B$;

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

У такому випадку старший розряд результату $r_{m-1} = A \cdot M \cdot B^t$. Наступні розряди результату (r_{m-2}, …,r_0) обчислюються за цією формулою, тільки замість самих векторів A та B використовуються результати послідовних циклічних зсувів цих векторів на один розряд вліво.

Виправлення помилок під час множення

Набір елементів $M = \{\beta, \beta^2, \beta^2, ..., \beta^{2^{m-1}}\}$, де $\beta \in GF(2^m)$ називається нормальним базисом. Оптимальний нормальний базис поля Галуа $GF(2^m)$ другого типу, далі ОНБ може формуватись за допомогою використання нормального елемента $\beta = \gamma + \gamma^{-1}$, де γ – корінь степеня ($2m$+1), оскільки $\gamma^{2m+1} = 1$ і $\gamma^i \neq 1$ для будь-якого $1 \leq i \leq 2m+1$. Отже, ОНБ другого типу може існувати тільки, коли число $p = 2m+1$ є простим, і також, коли виконуються такі умови: число 2 є примітивним коренем по модулю p, m є мультиплікативним порядком числа 2 по модулю p.

Базовими операціями над елементами полів Галуа GF(2^m) є множення і додавання. Оскільки додавання є простою операцією, особливу увагу потрібно звернути на виконання множення. Нехай C буде результатом множення *A* і *B*, де *A*, *B*, *C* ∈ *GF*(2^m). Представлення елементів *A* і *B* відбувається так:

$$A = \sum_{j=0}^{mt/2} a_j(\gamma^j + \gamma^{-j}), B = \sum_{j=0}^{mt} b_j'' \gamma^j ; \quad (1)$$

$$C = A \times B = (a_1(\gamma^1 + \gamma^{-1}) + ... + a_{mt/2}(\gamma^{mt/2} + \gamma^{-mt/2}))B = (a_1\gamma^1 + ... + a_{mt/2}\gamma^{mt/2})B + (a_1\gamma^{-1} + a_2\gamma^{-2} + ... + a_{mt/2}\gamma^{-mt/2})B = C1 + C2. \quad (2)$$

Якщо $B^{(i)} = \gamma^i B$ для $1 \le i \le mt/2$, тоді частину формули 5 для *C*1 можна записати так:

$$C1 = a_1^* B^{(1)} + a_2^* B^{(2)} + ... + a_{mt/2}^* B^{(mt/2)} = c1_0'' \gamma^0 + c1_1'' \gamma^1 + c1_2'' \gamma^2 + ... + c1_{mt}'' \gamma^{mt} . \quad (3)$$

$B^{(i)}$ та $B^{(i+1)}$ описані в 4 і 5 відповідно:

$$B^{(i)} = b_0^{(i)}\gamma^0 + b_1^{(i)}\gamma^1 + ... + b_{mt-1}^{(i)}\gamma^{mt-1} + b_{mt}^{(i)}\gamma^{mt} ; \quad (4)$$

$$B^{(i+1)} = B^i\gamma = b_{mt}^i\gamma^0 + b_0^i\gamma^1 + b_1^i\gamma^2 + .. + b_{mt-1}^i\gamma^{mt} . \quad (5)$$

Аналогічно, *C*2 можна розписати, як показано у формулах 6 і 7:

$$C2 = a_1^* B^{(-1)} + a_2^* B^{(-2)} + ... + a_{mt/2}^* B^{(-mt/2)} ; \quad (6)$$

$$B^{(-i)} = b_0^{(-i)}\gamma^0 + b_1^{(-i)}\gamma^1 + ... + b_{mt-1}^{(-i)}\gamma^{mt-1} + b_{mt}^{(-i)}\gamma^{mt} . \quad (7)$$

Отже, за допомогою елемента *U*, зображеного на рис. 2, утворюється систолічна структура. Результатом роботи цієї структури є множення двох елементів полів Галуа. У формулі (2) результат множення *C=C1+C2*. На рис. 3 зображений систолічний помножувач з виправленням помилок.

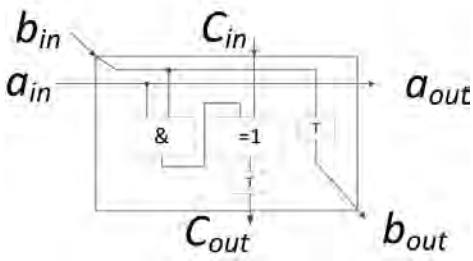

Рис. 2. Елемент U

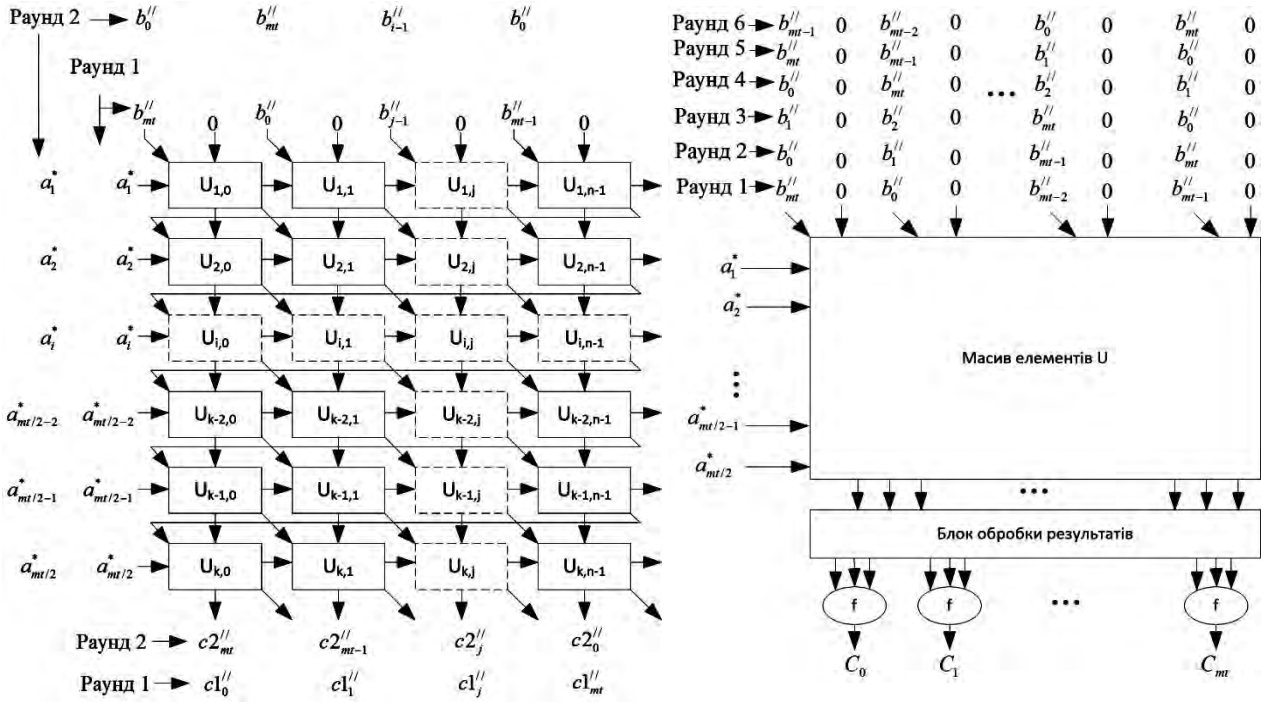

Рис. 3. Масив елементів та систолічний помножувач з виправленням помилок на його основі

Для виявлення помилки пропонується збільшити кількість раундів до 4, отже, час обчислення збільшується у 2 рази.

У [4] пропонується перевіряти наявність помилки переобчисленням результату із зсунутими операндами, відтак результат може бути обчислений за допомогою множення $C=A\times B$ і $C = RoR(A\times RoL(B))$, RoL і RoR – циклічний зсув на один розряд вліво і вправо відповідно. Ознака помилки формується за умови неідентичності результатів.

Для виправлення помилки пропонується проводити шість раундів обчислення Перші три раунди для обчислення $C1=A\times B$, $C1=RoR(A\times RoL(B)$ та $C1=RoR(RoR(A\times RoL(Rol(B))))$, наступні три раунди – для обчислення $C2$ та $C2$ із зсунутими операндами. У такому випадку час обчислення зростає у 3 рази. У кожному з розрядів результату помилка виправляється за допомогою мажоритарного елемента.

Якщо потрібно лише перевірити правильність виконання, існують ефективніші методи отримання ознаки помилки. В основу таких методів покладено той факт, що парність арифметичного добутку двох елементів поля дорівнює парності їхнього логічного добутку. Один з таких методів описаний в [12]. Однак такі методи не передбачають виправлення помилки.

Метод виявлення і виправлення помилок, наведений у роботі, пропонується використовувати лише тоді, коли необхідно виправити помилки, які виникають під час множення елементів поля Галуа.

Висновок

Показана можливість використання систолічної архітектури і методу з надлишковою витратою часу для виправлення помилок, що можуть виникати під час множення елементів полів Галуа, представлених в оптимальному нормальному базисі другого типу. Цей метод виявлення і виправлення помилок може бути застосований під час опрацювання цифрових підписів згідно з прийнятим в Україні стандартом.

1. Спеціалізований однорозрядний процесор для захисту інформації в гарантоздатних системах / В.С. Глухов, М.В. Ногаль // Радіоелектронні і комп'ютерні системи. – 2008. – №5. – С.104–108. 2. Biehl I., Meyer B. and Muller V. Differential fault attacks on elliptic curve cryptosystems. In Proc. 20th Int'l Conf. CRYPTO, pages 131–146. Springer-Verlag, 2000. 3. Blomer J., Otto M. and Seifert J.-P. Sign change fault attacks on elliptic curve cryptosystems. Cryptology eprint archive, Report 2004/227, 2004. http://eprint.iacr.org/2004/227. 4. Boneh D., Demillo R. and Lipton R. On the improtance of checking cryptographic protocols for faults. In Proceedings of the International Conference on the Theory and Applications of Cryptographic Techniques (Eurocrypt), pages 37–51. Springer-Verlag, 1997. 5. Переваги реалізації у НВІС пристроїв для обробки цифрового підпису, що ґрунтується на властивостях груп точок еліптичної кривої / А.Р. Добуш // Вісник Національного університету "Львівська політехніка" "Комп'ютерні системи та мережі". – 2012. – №745. – С.78–85. 6. Bayat-Sarmadi S. and Hasan M.A. Detecting errors in a polynomial basis multiplier using multiple parity bits for both inputs. In proceeding of the 25th IEEE International Conference on Computer Design (ICCD), pages 368–375, Lake Tahoe, CA, 2007. 7. Fenn S., Gossel M., Benaissa M. and Taylor D. Online error detection for bit-serial multipliers in GF(2m). J. Electronics Testing: Theory and Applications, 13:29–40, 1998. 8. Глухов В.С. Вбудований контроль множення в гауссівському нормальному базисі типу 2 полів Галуа GF(2m) // Науково-технічний журнал "Радіоелектронні і комп'ютерні системи. – Харків: ХАІ, 2010. – № 6(47). – С. 255–259. 9. Bayat-Sarmadi S. and Hasan M.A. Run-time error detection of polynomial basis multiplication using linear codes. In Proceedings of the 18th IEEE International Conference on Application-specific Systems, Architectures and Processors (ASAP), pages 102–110, Monterey, CA, 2005. 10. Gaubatz G., Sunar B., and Karpovsky M.G. Non-linear residue codes for robust public-key arithmetic. In Proc. 3rd Workshop on Fault Tolerance and Diagnosis in Cryptography (FTDC), pages 173–184, 2006. 11. Patel J.H. Concurrent Error Detection in ALU's by Recomputing with Shifted Operands / J.H. Patel, L.Y. Fung: IEEE Trans. Computers. – Vol. 31, No. 7, Липень 1982. – С.589–595. 12. 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. 13. Глухов В.С. Порівняфння поліноміального та нормального базисів представлення елементів полів Галуа // Вісник Національного університету "Львівська політехніка". – 2007. – С.22–27.