УДК 681.3, 004.3

В.С. Глухов
Національний університет “Львівська політехніка”,
кафедра електронних обчислювальних машин

ОСОБЛИВОСТІ ВИКОНАННЯ ОПЕРАЦІЙ НАД МАТРИЦЯМИ У ПОЛЯХ ГАЛУА

Описано особливості виконання операцій над матрицями у полях Галуа.

The aspects of matrix operation execution in Galois fields are described.

Вступ

Наш світ стає все більше електронним в тому сенсі, що багато сфер людської діяльності вже великою мірою пов’язані з цифровим світом. Технології змінюють сталу термінологію – вже звичними стали словосполучення “електронний документообіг”, “електронна комерція”, “електронний уряд”. А з 1 січня 2004 року в Україні офіційно дозволено користуватися електронним цифровим підписом замість звичайного [1].

Сьогодні в Україні діють два стандарти на цифровий підпис: міждержавний стандарт ГОСТ 34.310-95 [2] та національний стандарт України ДСТУ 4145–2002 [3]. Поряд з великою кількістю літератури про основи і принципи захисту інформації [наприклад, 4–7, 13,] останнім часом у фахових виданнях розглядаються конкретні питання впровадження систем захисту інформації (зокрема і систем цифрового підпису) в нетрадиційних галузях [8], проектування структури цих засобів [9–11], питання стійкості закладених в них алгоритмів [12], організації взаємодії універсального та спеціалізованого процесорів, що входять до складу криптопроцесора [14].

Разом з ними актуальними є також і розглянуті у цій статті питання особливостей виконання операцій над матрицями у полях Галуа, оскільки стандарт ДСТУ 4145-2002 [3] не деталізує алгоритми виконання таких операцій для оптимального нормального базису, хоча і дає багато посилань на джерела, у яких можна знайти необхідні пояснення. Одним з цих джерел є стандарт IEEE 1363–2000 [15].

1. Окреслення проблеми

Основою процедур отримання і перевірки цифрового підпису згідно з стандартом ДСТУ 4145–2002 [3] є операції над елементами поля Галуа (Galois Field, GF). Елементи поля Галуа можуть утворювати поліноміальний і нормальний базиси. Якщо послідовність виконання операцій у поліноміальному базисі описана в стандарті доволі чітко, то про виконання операцій у нормальному базисі говориться доволі загально. Особливо це стосується виконання операції множення: “Для виконання множення спочатку треба обчислити мультипликативну матрицю M, що складається з рядків, які є розкладом в оптимальному нормальному базисі m добутків елементів базису вигляду $x \cdot x^{2^j}$, j = 0, …, m-1, тобто

$$M = \begin{Bmatrix} x \cdot x \\ \dots \\ x \cdot x^{2^j} \\ \\ x \cdot x^{2^{m-1}} \end{Bmatrix}$$

Перший розряд добутку z двох елементів поля x і y обчислюють за формулою

$$z_{m-1} = xMy^T,$$

де x – вектор-рядок, а y^T – вектор-стовпчик.

Наступні розряди добутку обчислюють за цією самою формулою, тільки замість самих векторів x і y^T використовують їхні послідовні циклічні зсуви на один розряд ліворуч. Однозначно утворити матрицю M за цим визначенням доволі важко.

2. Мета роботи

Метою роботи є аналіз операцій, які необхідні для виконання множення двох елементів поля Галуа у нормальному базисі і для утворення матриці M, а також визначення методів обчислення оберненої матриці у полі Галуа, особливостей застосування цих методів і встановлення структури спеціалізованого комп'ютера для виконання операцій над елементами поля Галуа.

3. Аналіз методів виконання операцій множення елементів поля Галуа у нормальному базисі

Елементи $\{t^{m-1}, \ldots, t^2, t, 1\}$ основного поля Галуа утворюють поліноміальний базис, елементи $\{\theta, \theta^2, \theta^{2^2}, \ldots, \theta^{2^{m-1}}\}$ основного поля Галуа утворюють нормальний базис (t і θ – корені полінома, що утворює поле). Усі інші елементи основного поля Галуа можуть бути записані як у поліноміальному базисі (у вигляді $\alpha_{m-1}t^{m-1} + \ldots + \alpha_2 t^2 + \alpha_1 t + \alpha_0$), так і у нормальному базисі (у вигляді $a_0\theta + a_1\theta^2 + a_2\theta^{2^2} + \ldots + a_{m-1}\theta^{2^{m-1}}$), де a_i – двійкові розряди (i = 0, 1, …, m-1).

Під час множення двох елементів (x_N та y_N) поля Галуа у нормальному базисі (далі множення у нормальному базисі) виконують такі операції:

Перехід Н-П від представлення операнів (x_N та y_N) у нормальному базисі $\{\theta, \theta^2, \theta^{2^2}, \ldots, \theta^{2^{m-1}}\}$ до представлення у поліноміальному базисі $\{t^{m-1}, \ldots, t^2, t, 1\}$ (x_P та y_P);

Множення операндів у поліноміальному базисі $r_P = x_P * y_P$; ;

Перехід П-Н від представлення результату r_P у поліноміальному базисі $\{t^{m-1}, \ldots, t^2, t, 1\}$ до представлення у нормальному базисі $\{\theta, \theta^2, \theta^{2^2}, \ldots, \theta^{2^{m-1}}\}$ (r_N);.

Для переходу від Н-П необхідно скласти систему рівняннь

$$t = a_{0,0} + a_{0,1}t + a_{0,2}t^2 + \ldots + a_{0,m-1}t^{m-1} \pmod{p(t)}$$
$$t^2 = a_{1,0} + a_{1,1}t + a_{1,2}t^2 + \ldots + a_{1,m-1}t^{m-1} \pmod{p(t)}$$
$$t^4 = a_{2,0} + a_{2,1}t + a_{2,2}t^2 + \ldots + a_{2,m-1}t^{m-1} \pmod{p(t)}$$
$$\ldots$$
$$t^{2^{m-1}} = a_{m-1,0} + a_{m-1,1}t + a_{m-1,2}t^2 + \ldots + a_{m-1,m-1}t^{m-1} \pmod{p(t)}$$

послідовно підносячи до квадрата кожне попереднє рівняння (всі дії виконують у відповідному полі Галуа). З системи рівняннь утворюється матриця A з елементами $a_{i,j}$ (i (j) – номер рядка (стовпчика) матриці A).

$$A := \begin{bmatrix} a_{0,0} & a_{0,1} & \cdots & a_{0,m-1} \\ a_{1,0} & a_{1,1} & \cdots & a_{1,m-1} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m-1,0} & a_{m-1,1} & \cdots & a_{m-1,m-1} \end{bmatrix}.$$

Якщо правильно вибрано поліном, що утворює поле, A≠0):

У полі Галуа знаходять матрицю B, обернену до A: $B=A^{-1}$, B≠0.

Для переходу Н-П необхідно здійснити множення $x_N*A = x_P$, $y_N*A = y_P$,

Для переходу П-Н необхідно здійснити множення $r_P*B = r_N$.

4. Особливості обчислення оберненої матриці у полі Галуа

Квадратна матриця B з елементами $b_{i,j}$, обернена до квадратної матриці A з елементами $a_{i,j}$ обчислюється загальновідомим методом $B= |d_{i,j}|/d$, де

$|d_{i,j}|$ – матриця з елементами $d_{i,j}$;

$d_{i,j}$ – детермінанти мінорів відповідних елементів $a_{i,j}$ матриці A;

$d \neq 0$ детермінант матриці A,

i (j) – номер рядка (стовпчика) матриці A.

У полі Галуа d=1, $d_{i,j} = \{0;1\}$ (у полі Галуа детермінант може дорівнювати або 0, або 1).

Мінори матриці загалом утворюються викреслюванням стовпчика j та рядка матриці i, у яких розташований відповідний елемент $a_{i,j}$.

Реально під час обчислення зручніше не викреслювати рядки і стовпчики, а замінити стовпчик j та рядок i з елементом $a_{i,j}$ на стовпчик та рядок з усіма нульовими елементами крім $a_{i,j}$, після чого обчислити детермінант для такої новоутвореної матриці.

Обчислювати детермінанти можна одним із загальновідомих методів, наприклад, методом Гаусса [16]. Особливістю застосування методу Гаусса до матриць у полях Галуа є те, що на кінцевому етапі застосування методу Гаусса утворюється трикутна матриця, у головній діагоналі якої є тільки 1 (якщо детермінант цієї матриці дорівнює 1) або один або більше від 0 (якщо детермінант цієї матриці дорівнює 0).

Тобто обчислювати значення детермінанта методом Гаусса у полях Галуа можна тільки до знаходження першого 0 у діагоналі, що скорочує час обчислення.

Здійснення переходів Н-П та П-Н та власне множення можно сумістити у часі. Наприклад, стандарт IEEE 1363-2000 радить для цього:

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;

обчислити допоміжну матрицю D = ACB;

утворити помножувальну матрицю M, де $\mu_{i,j} := d_{j-i,-i}$.

$$C := \begin{bmatrix} 0 & 1 & 0 & \ldots & 0 \\ 0 & 0 & 1 & \ldots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \ldots & 1 \\ c_0 & c_1 & c_2 & \ldots & c_{m-1} \end{bmatrix} \quad M := \begin{bmatrix} \mu_{0,0} & \mu_{0,1} & \cdots & \mu_{0,m-1} \\ \mu_{1,0} & \mu_{1,1} & \cdots & \mu_{1,m-1} \\ \vdots & \vdots & \ddots & \vdots \\ \mu_{m-1,0} & \mu_{m-1,1} & \cdots & \mu_{m-1,m-1} \end{bmatrix}$$

Тоді $r_N = x_N * M * y_N^t$, як це і вказано у стандарті ДСТУ 4145-2002, де

y_N^t – матриця-стовпчик, яка є результатом транспонування матриці-рядка y_N (тобто, операнда y_N, двійкові розряди якого розглядають як елементи матриці-рядка).

Незважаючи на спрощення множення у разі використання помножувальної матриці M, для її визначення все одно необхідно знаходити матрицю B, обернену до матриці A.

5. Підхід до проектування структури спеціалізованого комп'ютера, що виконує операції над полями Галуа

З аналізу алгоритмів роботи з цифровим підписом видно, що операції переходу Н-П та П-Н можуть зустрічатися доволі часто, але матриці, які беруть в них участь (A, B, C, D та M), можуть бути розраховані один раз і надалі зберігатися у постійній пам'яті. Нові матриці необхідно розраховувати тільки під час зміни полінома, що утворює поле Галуа. Спеціалізований комп'ютер (спецобчислювач) [14], який виконує операції над полями Галуа, у такому разі може бути розділений на дві частини:

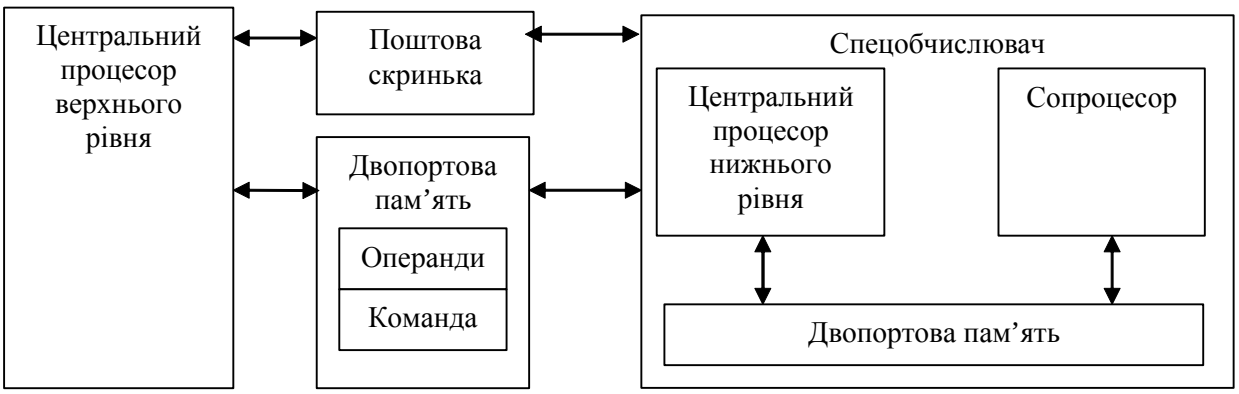
універсальний центральний процесор, менш повільний, на який покладаються задачі:

1) взаємодії з процесором вищого рівня;

2) обчислення і збереження матриць (A, B, C, D та M) перетворень;

3) організації роботи спеціалізованого співпроцесора;

спеціалізований співпроцесор, який використовує матриці для швидких обчислень, необхідних для утворення та перевірки цифрового підпису (рис. 1).



Криптографічна система

Взаємодія між двома складовими частинами спецобчислювача здійснюється через двопортову пам'ять, як і взаємодія універсального процесора з процесором вищого рівня.

Запропоновані методи були реалізовані у вигляді програми мовою Pascal. Були розроблені такі підпрограми:

підпрограми роботи з "великими" числами одинарного і подвійного формату (4 цілочислові арифметичні операції, зокрема ділення з залишком, інкремент, декремент, логічні операції, зсуви, перетворення форматів). "Значення" чисел (їхня розрядність) задається програмно, обмежується тільки ресурсами комп'ютера, на якому виконується програма, і задовольняє вимоги стандарту [3];

підпрограми роботи з "великими" полями Галуа (додавання, множення) у поліноміальному базисі;

підпрограми роботи з "великими" полями Галуа (додавання, множення) у нормальному базисі;

підпрограми роботи з матрицями у "великих" полях Галуа (утворення, транспонування, визначення детермінантів, знаходження оберненої матриці, множення вектора на матрицю, множення матриць);

підпрограми переходу від поліноміального базису до нормального і навпаки;

підпрограми роботи з еліптичними кривими (додавання точок, подвоєння точки, множення на константу, знаходження оберненої точки та інші).

Під час перевірки і налагодження програм використовувалися засоби математичного пакету Maple 7.

Правильність вибраного підходу була перевірена виконанням тестових прикладів, які наведені у стандарті ДСТУ 4145-2002 для операцій над елементами поля Галуа як у поліноміальному, так і у нормальному базисах.

Висновки

Виконано аналіз стандартів утворення і перевірки цифрового підпису, особлива увага приділена виконанню операцій множення над елементами поля Галуа, що утворюють нормальний базис. Показано, які операції потрібно виконувати для такого множення, найскладнішою з них є операція утворення оберненої матриці. Запропоновано використовувати метод Гаусса для визначення детермінантів матриць і метод знаходження детермінантів мінорів матриць, за якими замість утворення мінорів здійснюється перетворення основної матриці.

Також запропонована структура спеціалізованого комп'ютера, призначеного для виконання операцій у полях Галуа, зокрема і над матрицями. Здійснено розподіл операцій між його складовими частинами.

1. Соболев О. Электронная цифровая подпись в Украине: началось внедрение ЭЦП // Чип – Украина № 11. 2003. – С. 14–16. 2. Межгосударственный стандарт ГОСТ 34.310-95. Информационная технология. Криптографическая защита информации. Процедура выработки и проверки электронной цифровой подписи на базе асимметричного криптографического алгоритма. Межгосударственный совет по стандартизации, метрологии и сертификации. Минск. Госстандарт Украины, с дополнениями, 1997. 3. Національний стандарт України ДСТУ 4145-2002. Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що грунтується на еліптичних кривих. Формування та перевіряння. – К. – Державний комітет України з питань технічного регулювання та споживчої політики. 2003. 4. Ємець В., Мельник А., Попович Р. Сучасна криптографія. Основні поняття. – Львів, 2003. 5. Коркішко Т., Мельник А., Мельник В. Алгоритми та процеси симетричного блокового шифрування. – Львів, 2003. 6. Баричев С., Серов Р. Основы современной криптографии. – М., 2001. 7. Черемушкин А.В. Лекции по арифметическим алгоритмам в криптографии. – М., 2002. 8. Глухов В.С., Мельник А.О., Пуйда В.Я. Дослідження шляхів створення кодера та декодера відеосигналу // Вісник Національного університету "Львівська політехніка". – 2003. – № 492. – С. 35 – 47. 9. Мельник А.О., Коркішко Т.А. Система підтримки виконання алгоритмів криптографічного захисту інформації на основі програмованого процесора та криптографічних акселераторів // Вісник Державного університету "Львівська політехніка". – 2000. – № 385. – С. 77–80. 10. Коркішко Т.А., Мельник А.О. Вимоги до продуктивності процесів шифрування симетричними блоковими алгоритмами // Вісник Національного університету "Львівська політехніка". – 2001. – № 437. –С. 83–90. 11. Морозов Ю.В. Інтелектуальна карта для системи цифрового підпису // Вісник Національного університету "Львівська політехніка". – 2003. – № 492 С.107 – 111. 12. Попович Р.Б. Криптоаналіз системи RSA на основі пошуку функції Ейлера // Вісник Національного університету "Львівська політехніка". – 2003. – № 492. – С. 128 – 133. 13. Введение в криптографию. Под ред. В.В. Ященко. – М., 2000. 14. Глухов В.С. Система команд криптографічного процесора // Вісник Національного університету "Львівська політехніка". – 2004. – № 523. – С. 42–50. 15. 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. 16. Демидович Б.П, Марон И.А..Основы вычислительной математики. – М., 1970.