УДК 681.3, 004.3

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

ПОРІВНЯННЯ ПОЛІНОМІАЛЬНОГО ТА НОРМАЛЬНОГО БАЗИСІВ ПРЕДСТАВЛЕННЯ ЕЛЕМЕНТІВ ПОЛІВ ГАЛУА

Порівняно апаратні та часові витрати під час виконання операцій над елементами полів Галуа GF(2^m), представленими у поліноміальному та нормальному базисах відповідно до алгоритму цифрового підпису, що ґрунтується на еліптичних кривих (Elliptic Curve Digital Signature Algorithm (ECDSA)).

The paper describes implementation of cryptographic coprocessor performing operations on elliptic curve points with coordinates in GF(2^m) according to Elliptic Curve Digital Signature Algorithm (ECDSA). Polynomial basis and normal basis arithmetic units for inversion are compared. When an optimal normal basis exists, the normal basis inversion performs more quick.

Вступ. З 1 січня 2004 року в Україні офіційно дозволено користуватися електронним цифровим підписом замість звичайного. Сьогодні в Україні діють два стандарти на цифровий підпис: міждержавний стандарт ГОСТ 34.310-95 та національний стандарт України ДСТУ 4145–2002. Останній стандартизує використання полів Галуа та еліптичних кривих в алгоритмах отримання та перевірки цифрового підпису (Elliptic Curve Digital Signature Algorithm (ECDSA)). Елементи поля Галуа можна подати у поліноміальному та нормальному базисах. У статті аналізується, який з базисів найкраще підходить для апаратної реалізації алгоритмів ДСТУ 4145–2002, а також обґрунтовується вибір допустимих полів з оптимальним нормальним базисом, в яких найпрацемісткіша операція ECDSA – обчислення оберненого елемента – апаратним способом виконується якнайшвидше.

Аналіз публікацій й постановка проблеми. З 1 січня 2004 року в Україні офіційно дозволено користуватися електронним цифровим підписом замість звичайного [1]; поступово впроваджуються механізми електронного документообігу [2]. В Україні діють два стандарти на цифровий підпис: міждержавний стандарт ГОСТ 34.310–95 [3] та національний стандарт України ДСТУ 4145-2002 [4]. В основу процедур отримання і перевірки цифрового підпису згідно з [4] покладено операції над елементами поля Галуа GF(2^m) (m – просте число, надалі такі поля, які відповідають вимогам [4], у статті називатимуться просто полями Галуа). Найпрацемісткішою операцією у таких полях є обчислення оберненого елемента, під час якого доводиться знаходити добутки елементів поля Галуа. У [5, 6] розглянуто питання застосування методу Мессі–Омури (Massey–Omura, [7]) під час множення двох елементів (x_N та y_N) поля Галуа у нормальному базисі (надалі – множення у нормальному базисі) згідно з стандартом [4]. Додатково у [6] робиться висновок про перевагу поліноміального базису у разі програмної реалізації. У роботі [8] порівняно апаратні способи множення і знаходження оберненого елемента поля Галуа GF(2^{162}), і показано, що під час апаратної реалізації переваги має нормальний базис.

У літературі не знайдено критеріїв обрання поля з оптимальним нормальним базисом для використання в кріптопроцесорі (крім тривіального побажання, щоб m було більшим). У цій роботі проаналізовано апаратні та часові витрати для пристроїв, які реалізують алгоритми цифрового підпису апаратним способом, формулюються рекомендації щодо вибору допустимого поля з оптимальним нормальним базисом з погляду швидкості виконання криптографічних перетворень.

Мета роботи. Метою роботи є аналіз апаратних і часових витрат на множення елементів поля Галуа GF(2^m) і обчислення оберненого елемента поля Галуа GF(2^m) при виконанні алгоритму цифрового

підпису ECDSA, зокрема й апаратним способом, а також вибір допустимого поля з оптимальним нормальним базисом, в якому обернений елемент апаратним способом знаходиться якнайшвидше.

Синтез помножувача елементів поля Галуа у нормальному і поліноміальному базисах. Елементи $\left\{t^{m-1},...,t^2,t,1\right\}$ основного поля Галуа утворюють поліноміальний базис, елементи $\left\{\theta,\theta^2,\theta^{2^2},...,\theta^{2^{m-1}}\right\}$ основного поля Галуа утворюють нормальний базис (t і θ – корені полінома p, що утворює поле). Усі інші елементи основного поля Галуа можна подати як у поліноміальному базисі (у вигляді $a_{m-1}t^{m-1}+...+a_2t^2+a_1t+a_0$), так і у нормальному базисі (у вигляді $a_0\theta+a_1\theta^2+a_2\theta^{2^2}+...+a_{m-1}\theta^{2^{m-1}}$), де a_i – двійкові розряди (i = 0, 1, …, m-1).

Додавання двох елементів у полі Галуа виконується як порозрядне додавання за модулем 2.

Під час множення двох елементів поля Галуа у поліноміальному базисі:

замість арифметичного додавання виконується операція додавання за модулем 2 (xor).

множення виконується за модулем p. За модулем p береться або весь результат множення, або кожний проміжний результат (так званий помножувач Мастровіто (Mastrovito, рис. 1) [9].

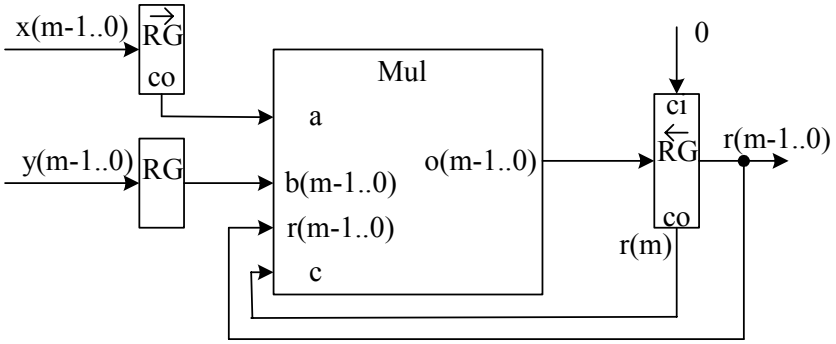


Рис. 1. Помножувач Мастровіто

Під час множення двох елементів (x_N та y_N) поля Галуа у нормальному базисі (надалі – множення у нормальному базисі) потрібно виконати такі операції:

скласти систему рівнянь

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

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

у полі Галуа знайти матрицю B, обернену до A: $B=A^{-1}$, $\det B \neq 0$;

утворити допоміжну матрицю C, де c_i – коефіцієнти полінома $p(t) = t^m + c_{m-1}t^{m-1} + ...c_1t + c_0$, що утворює відповідне поле Галуа;

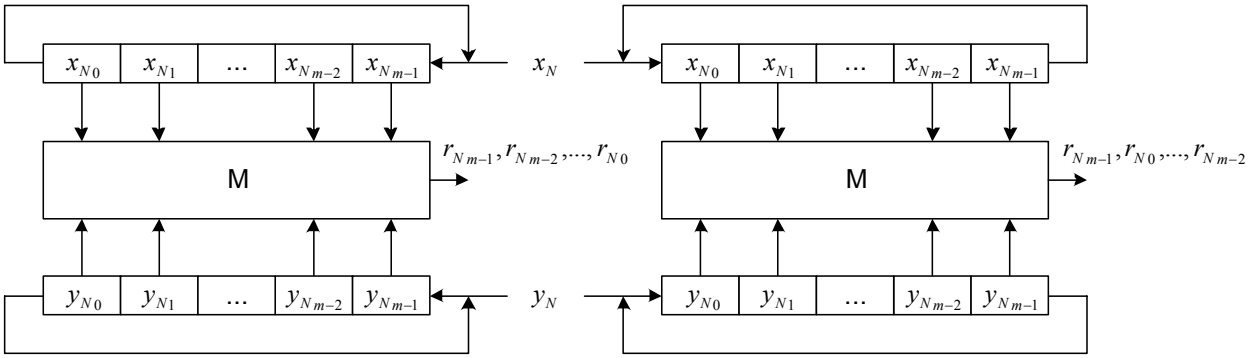
$$A = \begin{bmatrix} a_{0,0} & a_{0,1} & \cdots & a_{0,m-1} \\ a_{1,0} & a_{1,1} & \cdots & a_{1,m-1} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m-1,0} & a_{m-1,1} & \cdots & a_{m-1,m-1} \end{bmatrix},\ C = \begin{bmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots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

обчислити допоміжну матрицю D = ACB;

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

Тоді старший розряд результату $r_{N(m-1)} = x_N * M * y_N^t$.

Наступні розряди результату ($r_{N(m-2)}$, …, $r_{N(0)}$) обчислюються за цією самою формулою, тільки замість самих векторів x_N та y_N використовуються їхні послідовні циклічні зсуви на один розряд вліво. Цю схему множення ілюструє рис. 2.



а б

Рис. 2. Помножувач згідно з стандартом [4] (а) та за методом Мессі–Омури [7] (б)

У полі Галуа елементами матриці M будуть тільки 0 та 1, у разі використання оптимального нормального базису кількість 1 у матриці буде мінімально можливою і дорівнюватиме 2*m-1.

На практиці операції з матрицями перетворюються на обчислення згідно з відомими формулами множення матриць, велика кількість 0 у матриці дає змогу значно спростити ці формули.

Можна отримати розряди добутку при використанні правого зсуву у тій самій послідовності, що і при використанні лівого, але при цьому необхідно трансформувати матрицю M.

На відміну від множення елементів поля Галуа у поліноміальному базисі, де усі дії виконуються над словами, при множенні у нормальному базисі дії виконуються над окремими розрядами операндів, причому над різними розрядами двох операндів. Тому програмна реалізація множення у нормальному базисі буде повільнішою за програмну реалізацію у поліноміальному базисі. У табл. 1 наведено результати порівняння часу виконання множення в полі Галуа $GF(2^{173})$ програмними способами.

Таблиця 1

Порівняння часу виконання множення програмним способом

Спосіб множення	Час виконання, %
Множення у поліноміальному базисі	100
Елементи представлені у нормальному базисі, множення здійснюється у поліноміальному базисі	240
Множення у нормальному базисі	4500

Апаратна реалізація не дає явних переваг жодному з базисів (табл. 2). Обидва методи послідовні, для отримання m-бітного результату потрібно m тактів роботи. Менше значення комплексного показника відповідає кращому варіанту (LUT, slices – функціональні елементи ПЛІС ф. Xilinx).

Перевага нормального базису проявляється під час виконання найпрацемісткішої операції над елементами поля Галуа – знаходження оберненого елемента (такого елемента b, що ab=1, якщо a≠0 – заданий елемент).

Таблиця 2

Порівняльні характеристики апаратних помножувачів для m = 173

Базис	Кількість тактів роботи	Апаратні витрати, slices	Апаратні витрати, LUT	Максимальна тактова частота, МГц	Комплексний показник, LUT/МГц
Поліноміальний, рис. 1	m = 173	275	526	146	3,6
Нормальний, рис. 2, а	m = 173	383	577	169	3,4

У поліноміальному базисі для знаходження оберненого елемента використовується узагальнений алгоритм Евкліда обчислення найбільшого спільного дільника (НСД) двох многочленів f(t) та c(t) [4]. Цей алгоритм виражає НСД d(t) як d(t)=a(t)f(t)+b(t)c(t), де a(t) і b(t) – деякі многочлени, що обчислюються при виконанні узагальненого алгоритму Евкліда. Цей алгоритм має такий вигляд:

Приймають a(t)=1, d(t)=f(t), u(t)=0, v(t)=c(t)/

Якщо v(t)=0, то приймають $b(t) = \dfrac{d(t) + f(t)a(t)}{c(t)}$ та закінчують виконання алгоритму.

За допомогою ділення з залишком обчислюють d(t)=q(t)v(t)+r(t), надалі обчислюють w(t)=a(t)+u(t)q(t), a(t)=u(t), d(t)=v(t), u(t)=w(t), v(t)=r(t) та переходять до кроку 2.

Якщо як f(t) взяти примітивний многочлен поля, а замість c(t) – многочлен, що зображає елемент поля, то d(t) є одиничним многочленом і наведене вище співвідношення за модулем примітивного многочлена перетворюється на співвідношення b(t)c(t)=1 mod f(t), тобто многочлен b(t) зображує елемент, обернений до c(t). Згідно з [10] кількість операцій над елементами поля Галуа під час виконання цього алгоритму дорівнює $O(m^2)$.

Час обчислення оберненого елемента можна визначити, підраховуючи тільки кількість довгих операцій. Кількість довгих операцій (множення – Nm, подвійне множення – Ndm, ділення – Nd, подвійне ділення – Ndd) під час обчислення оберненого елемента у поліноміальному базисі $GF(2^{163})$ залежить від елемента і для деяких елементів, згаданих у додатку Б.1 [4], наведена у табл. 3.

Таблиця 3

Кількість довгих операцій під час обчислення оберненого елемента у поліноміальному базисі для $GF(2^{163})$

Елементи поля $GF(2^{163})$	x_p	y_p	h	n	b	D	e
Nm	76	89	84	44	83	90	95
Ndm	1	1	1	1	1	1	1
Nd	76	89	84	44	83	90	95
Ndd	1	1	1	1	1	1	1
Разом	154	180	170	90	168	182	192

Для обчислення оберненого елемента в оптимальному нормальному базисі використовується формула: $x^{-1} = x^{2m-2}$, $x \neq 0$. Для обчислення правої частини існує ефективний алгоритм Ito-Цідзії (Itoh, Tsijii) [4]: нехай m_r, …, m_0 – двійковий розклад цілого числа m-1. Тоді обернений елемент обчислюють так:

$b \leftarrow x$; $k \leftarrow 1$.

Для i від r-1 до 0 обчислюють:

$c \leftarrow b$;

для j від 1 до k обчислюють $c \leftarrow c^2$;

$b \leftarrow bc$;

$k \leftarrow 2k$;

якщо $m_j=1$, то $b \leftarrow b^2x$ та $k \leftarrow k+1$.

$x^{-1}=b^2$.

Кількість n довгих операцій (множення) у разі використання цього алгоритму не залежить від значення елемента і дорівнює зменшеній на 1 сумі кількості біт у записі числа m-1 (k=[log(m-1)]) плюс кількість ненулевих біт (функція w) у цьому записі (e=w(m-1)). Для допустимих основних полів з оптимальним нормальним базисом ([4], (табл. 2) кількість операцій множення n наведено у табл. 4.

Таблиця 4

Кількість множень під час обчислення оберненого елемента у нормальному базисі

№ з/п	m	$(m-1)_{10}$	$(m-1)_2$	k=[log(m-1)]	e= w(m-1)-1	n=k+e-1	Кількість тактів, n*m
1	173	172	10101100	7	4	10	1730
2	179	178	10110010	7	4	10	1790
3	191	190	10111110	7	6	12	2292
4	233	232	11101000	7	4	10	2330
5	239	238	11101110	7	6	12	2868
6	251	250	11111010	7	6	12	3012
7	281	280	100011000	8	3	10	2810
8	293	292	100100100	8	3	10	2930
9	359	358	101100110	8	5	12	4308
10	419	418	110100010	8	4	11	4609
11	431	430	110101110	8	6	13	5603
12	443	442	110111010	8	6	13	5759
13	491	490	111101010	8	6	13	6383
14	509	508	111111100	8	7	14	7126

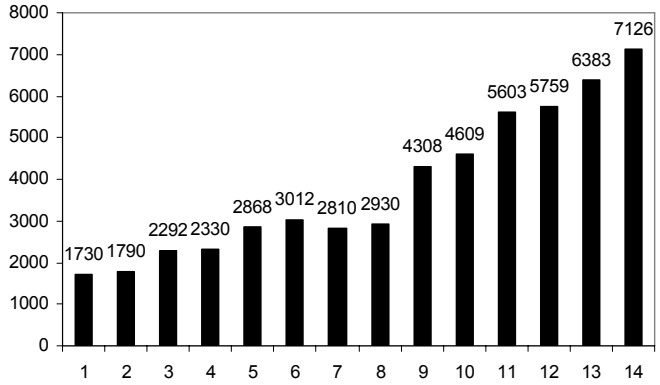


Рис. 3. Кількість тактів множення під час обчислення оберненого елемента у нормальному базисі (по осі X – номери полів з табл. 4)

Порівнюючи дані табл. 3 та 4, можна зробити висновки:

1. Кількість довгих операцій при знаходженні оберненого елемента у нормальному базисі на порядок менша ніж у поліноміальному базисі.

2. Серед основних полів з оптимальним нормальним базисом виділяються декілька з найменшою кількістю множень (10) – це поля зі степенями поліномів m = 173, 179, 281, 293.

3. Якщо кращим вважати поле, в якому для обчислення обернених елементів треба витрачати меншу кількість тактів ніж хоча б в одному полі з меншим порядковим номером (з меншим m), то найкращими є поля зі степенями поліномів m=281 та m=293 (7-ме та 8-ме поля, табл. 4 та рис. 3).

Висновки. У статті проаналізовано апаратні і часові витрати на множення елементів поля Галуа $GF(2^m)$ та обчислено обернений елемент поля Галуа $GF(2^m)$ під час виконання алгоритму цифрового підпису ECDSA програмним і апаратним способами. Показано, що апаратно множення в

поліноміальному і нормальному базисах вимагає приблизно однакових апаратних витрат часу. Однаке найпрацемісткіша операція над елементами поля Галуа GF(2^m) – обчислення оберненого елемента в нормальному базисі виконується на порядок швидше. Також обґрунтовано вибір допустимих полів з оптимальним нормальним базисом, в якому знаходять обернений елемент апаратним способом якнайшвидше. Це поля, для яких m = 173, 179, 281, 293.

1. Соболев О. Электронная цифровая подпись в Украине: началось внедрение ЭЦП // Чип – Украина. – 2003. – № 11. – С. 14–16. 2. Постанова Верховної ради України № 789-V від 21.03.2007 р. "Про прийняття за основу проекту Закону України "Про Загальнодержавну програму введення електронного документообороту з використанням електронного цифрового підпису". 3. 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. 4. Національний стандарт України ДСТУ 4145-2002. Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевіряння. – К.: Держ. комітет України з питань технічного регулювання та споживчої політики, 2003. 5. Глухов В.С. Операційний пристрій для роботи з елементами поля Галуа, представленими у нормальній формі // Зб. матеріалів міжвуз. наук.-техн. конф. наук.-пед. працівників "Проблеми та перспективи розвитку економіки і підприємництва та комп'ютерних технологій в Україні". – Львів: Ліга-Прес, 2007. 6. Глухов В.С. Обчислювальний пристрій для операцій над еліптичними кривими // Вісн. Нац. ун-ту "Львівська політехніка". – 2006. – № 573. – С. 54–61. 7. Omura J. and Massey J. Computational method and apparatus for finite field arithmetic. U.S. Patent Number 4, 587, 627, May 1986. 8. Schmidt J., Novotný M., Jäger M., Bečvář M., Jáchim M.. M.: Comparison of the Polynomial and Optimal Normal Basis ECDSA for GF(2^162) In: Proceedings of IEEE Design and Diagnostics of Electronic Circuits and Systems Workshop 2002.(DDECS02): Brno: University of Technology, 2002. – P. 150–157. 9. Mastrovito E.D. VLSI architectures for multiplication over finite field GF(2m). In T. Mora, editor, Applied Algebra, Algebraic Algorithms, and Error-Correcting Codes, 6th International Conference, AAECC-6, Lecture Notes in Computer Science, No. 357. – P. 297–309, Rome, Italy, July 1988. New York, NY: Springer-Verlag. 10. Handbook of Applied Cryptography, by A. Menezes, P van Oorschot, and S. Vanstone, CRC Press, 1996.