УДК 004.383

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

ОБЧИСЛЕННЯ ОБЕРНЕНОГО ЕЛЕМЕНТА В НОРМАЛЬНОМУ БАЗИСІ ПОЛІВ ГАЛУА *GF*(2^m) З ВИКОРИСТАННЯМ ПАРАЛЕЛЬНОГО ПОМНОЖУВАЧА

© Глухов В., Еліас Р., 2010

Описано апаратне вдосконалення методу Ito–Тічей–Цудзії знаходження оберненого елемента поля Галуа GF(2^m) в оптимальному нормальному базисі з використанням паралельного помножувача. Вдосконалення полягає у виконанні піднесення елемента до степеня 2^i шляхом циклічного зсуву елемента на *i* розрядів одночасно. Наслідком вдосконалення є зменшення часу виконання послідовності операцій піднесення до квадрата, що при використанні паралельних помножувачів скорочує час знаходження оберненого елемента приблизно в 10 разів.

Ключові слова: обернений елемент, поля Галуа GF(2^m), метод Ito–Тічей–Цудзії, паралельний помножувач.

The paper describes Itoh, Teechai, and Tsujii method of GF(2^m) inverse element calculation improvement in optimal normal base in case of parallel multiplier use. The improvement minimizes squaring time that reduces inverse element calculation time approximately to 10 times.

Keywords: inverse element, Galois field GF(2^m), Itoh, Teechai, and Tsujii method, parallel multiplier.

Вступ

Сучасні стандарти для роботи з цифровими підписами ґрунтуються на використанні полів Галуа та еліптичних кривих.

Елементи $\left\{\theta,\theta^2,\theta^{2^2},...,\theta^{2^{m-1}}\right\}$ основного поля Галуа GF(2^m) утворюють нормальний базис (θ – корені полінома *p*, що утворює поле). Усі інші елементи основного поля Галуа GF(2^m) можуть бути представлені 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*).

Для обчислення оберненого елемента в оптимальному нормальному базисі використовується алгоритм Ito–Тічей–Цудзії. Недоліком алгоритму є велика кількість операцій піднесення до квадрата. У нормальному базисі піднесення до квадрата виконується як циклічний зсув елемента на один двійковий розряд праворуч. При апаратній реалізації і використанні паралельного помножувача час виконання зсувів перевищує час множення і є основною складовою часу знаходження оберненого елемента. У роботі пропонується використовувати зсуви одночасно на декілька розрядів, що скоротить час знаходження оберненого елемента приблизно в 10 разів. Також наведено рекомендації з обрання поля Галуа GF(2^m) за умови використання зсуву на декілька розрядів і паралельних помножувачів.

1. Постановка проблеми

Для обчислення оберненого елемента в оптимальному нормальному базисі поля Галуа GF(2^m) використовується формула: $x^{-1} = x^{2^m-2} = x^{2(2^{m-1}-1)}$, $x \neq 0$. Для обчислення $x^{2^m-2} = x^{2(2^{m-1}-1)}$ існує ефективний алгоритм Ito–Тічей–Цудзії. Цей алгоритм застосовується для реалізації крип-

тографічних пристроїв, що виконують перетворення елементів поля Галуа і точок еліптичних кривих при виконанні операцій над цифровими підписами відповідно до стандартів, що діють в Україні.

Недоліком алгоритму є велика кількість операцій піднесення до квадрата $c \leftarrow c^2$. У нормальному базисі піднесення до квадрата виконується як циклічний зсув елемента на один двійковий розряд праворуч. Особливо відчутною велика кількість операцій піднесення до квадрата стає при використанні паралельних помножувачів, коли час виконання множення дорівнює часу зсуву на один біт. Тому актуальною є задача зменшення часу виконання зсувів.

2. Аналіз основних досліджень та публікацій

Сучасні стандарти [1, 2] для роботи з цифровими підписами ґрунтуються на використанні полів Галуа $GF(2^m)$ та еліптичних кривих. Для обчислення оберненого елемента в оптимальному нормальному базисі використовується алгоритм Ito–Тічей–Цудзії [3]. Даний алгоритм знаходить застосування при реалізації криптографічних пристроїв [4, 5], що виконують перетворення елементів поля Галуа [6] і точок еліптичних кривих [7] при виконанні операцій над цифровими підписами відповідно до стандартів [1, 2]. У роботі [7] розглядаються особливості використання паралельного і послідовного помножувачів для виконання операцій над елементами полів Галуа $GF(2^m)$ у нормальному базисі. У роботах [8, 9] розглядається вдосконалений метод Ito–Тічей–Цудзії, який ґрунтується на використанні багаторозрядних зсувів під час знаходження оберненого елемента, а також оцінений вплив вдосконалення для випадку використання послідовних помножувачів.

3. Цілі статті

Метою роботи є вдосконалення методу Ito–Тічей–Цудзії знаходження оберненого елемента полів Галуа $GF(2^m)$ у нормальному базисі для випадку використання паралельних помножувачів, а також оцінка впливу вдосконалення на час знаходження оберненого елемента у цьому випадку.

4. Методу Ito–Тічей–Цудзії

Для обчислення оберненого елемента в оптимальному нормальному базисі використовують формулу: $x^{-1} = x^{2^m-2} = x^{2(2^{m-1}-1)}$, $x \neq 0$. Для обчислення $x^{2^m-2} = x^{2(2^{m-1}-1)}$ існує ефективний алгоритм Ito–Тічей–Цудзії:

нехай $m_r, \ldots, m_0$ – двійковий розклад цілого числа m-1. Тоді обчислення оберненого елемента виконують так:

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

(2) Для і від r-1 до 0 обчислюють:

(2.1) $c \leftarrow b$;

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

(2.3) $b \leftarrow bc$;

(2.4) $k \leftarrow 2k$;

(2.5) якщо m_i=1, то $b \leftarrow b^2 x$ та $k \leftarrow k$+1.

(3) $x^{-1} = b^2$.

Оригінальний алгоритм передбачає використання регістра з двовходовим мультиплексором на вході для виконання занесення початкового значення до регістру і подальшого його циклічного зсуву на один розряд за кожний такт (рис. 1).

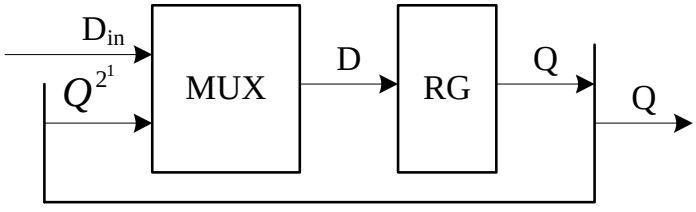

Рис. 1. Функціональна схема регістра зсуву на 1 розряд

5. Модифікація методу Іто–Тічей–Цудзії для варіанта послідовних помножувачів

В основу модернізації алгоритму покладено використання регістрів зсуву з багатовходовим мультиплексором на вході, що дає змогу виконувати зсув з програмованою величиною зсуву за один такт: з 4-входовим мультиплексором (рис. 2) або з 8-входовим мультиплексором (рис. 3).

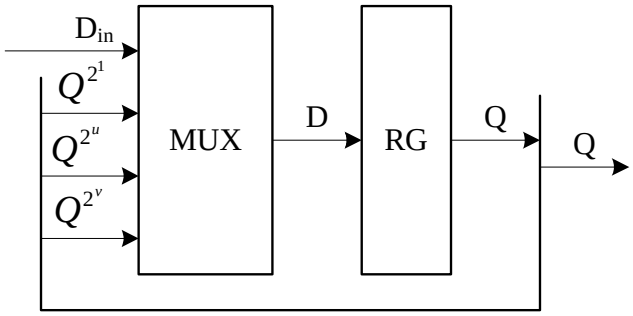

Рис. 2. Функціональна схема регістра зсуву на багато розрядів з 4-входовим мультиплексором

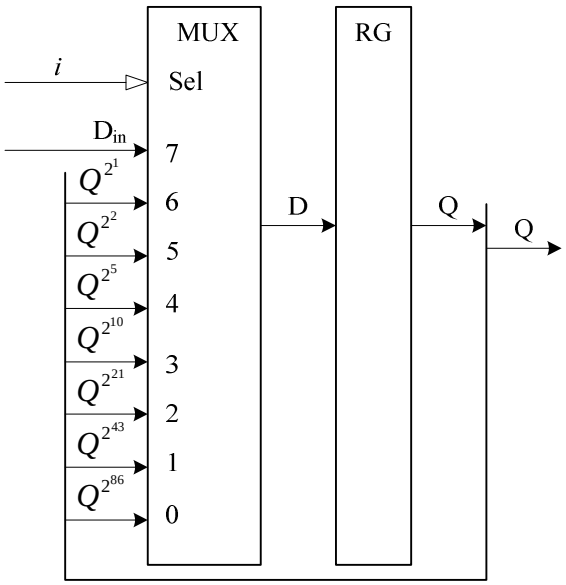

Рис. 3. Функціональна схема регістра зсуву на багато розрядів з 8-входовим мультиплексором

На рис. 2 та рис. 3 позначено:

D_{in} – дані для початкового завантаження регістра зсуву; Q^{2^j} – вихід Q регістра, циклічно зсунутий праворуч на j двійкові розряди.

Сигнали керування на рис. 2 та 3 не позначено.

Циклічний зсув праворуч за один такт на j двійкові розряди елемента

$$\alpha = (a_0, a_1, ..., a_{m-j-1}, a_{m-j}, a_{m-j+1}, ..., a_{m-1}, a_0, a_1, ..., a_{m-j-1})$$

веде до піднесення його до степеня 2^j:

$$\alpha^{2^j} = (a_{m-j}, a_{m-j+1}, ..., a_{m-1}, a_0, a_1, ..., a_{m-j-1}).$$

Використання 4-входового мультиплексора дає змогу завантажити початкове значення у регістр зсуву, виконувати зсуви на 1, u та v двійкових розрядів (за один такт). Для різних поліномів значення u та v знаходять методом перебору.

Пункт 2.2. модифікованого алгоритму для 4-входового мультиплексора можна записати у такому вигляді:

(2.2)

(2.2.1) $S_u(i)$ разів обчислити $c \leftarrow c^{2^u}$ (тобто, за один *i*-й такт виконати циклічний зсув на *u* двійкові розряди, переславши інформацію через 3-й вхід мультиплексора *MUX*);

(2.2.2) $S_v(i)$ разів обчислити $c \leftarrow c^{2^v}$ (тобто, за один *i*-й такт виконати циклічний зсув на *v* двійкові розряди, переславши інформацію через 2-й вхід мультиплексора *MUX*);

(2.2.3) $S_1(i)$ разів обчислити $c \leftarrow c^{2^1}$ (тобто, за один *i*-й такт виконати циклічний зсув на 1 двійковий розряд, переславши інформацію через 1-й вхід мультиплексора *MUX*).

Значення $S_u(i)$, $S_v(i)$ та $S_1(i)$ попередньо обчислюються та зберігаються у разом з номерами *i* відповідних входів мультиплексора.

Пункт 2.2. модифікованого алгоритму для 8-входового мультиплексора можна записати у такому вигляді:

(2.2) обчислити $c \leftarrow c^{2^{k(i)}}$ (тобто, за один *i*-й такт виконати циклічний зсув на *k(i)* двійкових розрядів, переславши інформацію через *i*-й вхід мультиплексора *MUX*).

Значення *k(i)* попередньо обчислюють та забезпечують поданням відповідних сигналів на входи мультиплексора. Керування мультиплексором здійснює безпосередньо номер такту *i*.

При використанні послідовних помножувачів зменшення кількості тактів зсуву зменшує загальну кількість тактів виконання алгоритму не більше ніж на 10% [8, 9];

6. Модифікація методу Іто–Тічей–Цудзії для варіанта паралельних помножувачів

Організація піднесення до квадрата не залежить від типу помножувача (паралельного чи послідовного). При використанні паралельного помножувача збільшується вплив часу піднесення до квадрата на час виконання всього алгоритму.

Для допустимих основних полів з оптимальним нормальним базисом [1], для регістрів зсуву з 8-входовими мультиплексорами кількість операцій множення *n*, кількість тактів множення (паралельне множення) $N_m = n*1 = n$, кількість тактів однорозрядних зсувів $N_s = m-e-1$ та багаторозрядних зсувів *k* містить таблиця. Також наведений виграш у часі $(N_s+N_m)/(k+N_m)$ при використанні багаторозрядних зсувів.

Після аналізу (див. таблицю) можна зробити висновки:

– кількість тактів однорозрядних зсувів значно більша кількості тактів паралельного множення;

– зменшення кількості тактів зсуву зменшує загальну кількість тактів виконання алгоритму при використанні паралельного множення в 10–14 разів.

Кількість тактів обчислення оберненого елемента при використанні паралельного множеня

№ з\п	m	$(m-1)_{10}$	$(m-1)_2$	k	e	n	N_m	N_s	N_s+N_m	$k+N_m$	$(N_s+N_m)/(k+N_m)$ – виграш (разів)
1	173	172	10101100	7	4	10	10	168	178	17	10,5
2	179	178	10110010	7	4	10	10	174	184	17	10,8
3	191	190	10111110	7	6	12	12	184	196	19	10,3
4	233	232	11101000	7	4	10	10	228	238	17	14
5	239	238	11101110	7	6	12	12	232	244	19	12,8
6	251	250	11111010	7	6	12	12	244	256	19	13,5
7	281	280	100011000	8	3	10	10	277	287		
8	293	292	100100100	8	3	10	10	289	299		
9	359	358	101100110	8	5	12	12	353	365		
10	419	418	110100010	8	4	11	11	414	425		
11	431	430	110101110	8	6	13	13	424	437		
12	443	442	110111010	8	6	13	13	436	449		
13	491	490	111101010	8	6	13	13	484	497		
14	509	508	111111100	8	7	14	14	501	515		

Таблиця містить позначки: $k=[log(m-1)]$; $e= w(m-1)$; $w(x)$ – функція підрахунку кількості ненулевих біт у числі x; $n=k+e-1$; $N_m= n*m$; $N_s=m-e-1$.

7. Вибір основного поля з оптимальним нормальним базисом для варіанта паралельного множення

Серед основних полів з оптимальним нормальним базисом виділяються декілька з найменшою кількістю тактів множення і багаторозрядного зсуву (=17) – це поля з степенями поліномів m = 173, 179, 233 (див. таблицю).

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 найкращим є поле із степенем поліному m=233 (4-те поле, див. таблицю).

Висновки

У роботі описано вдосконалення алгоритму Іто–Тічей–Цудзії знаходження оберненого елемента поля Галуа GF(2^m) в оптимальному нормальному базисі для випадку використання паралельних помножувачів. Вдосконалення полягає у зменшенні часу виконання послідовності операцій піднесення до квадрата (послідовності операцій циклічного зсуву праворуч на один двійковий розряд). Використання вузлів циклічного зсуву одночасно на декілька розрядів дає змогу скоротити час виконання послідовності зсувів приблизно на порядок, а час виконання алгоритму загалом приблизно у 10–14 разів.

З метою зменшення тривалості обчислень рекомендується при використанні паралельних помножувачів під час опрацьовання цифрових підписів відповідно до стандарту України ДСТУ 4145-2002 у нормальному базисі полів Галуа GF(2^m) використовувати поля зі степенем полінома m=233.

1. Національний стандарт України 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. 2. 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. 3. Itoh, T., Teechai, O., and Tsujii, S. "A Fast Algorithm for Computing Multiplicative Inverses in GF(2t) Using Normal Bases," J. Society for Electronic Communications (Japan) 44 (1986), pp. 31-36. 4. Глухов В., Заіченко Н., Оліярник Б. Шифропроцесор для бортових інформаційно-керуючих систем // Наукові нотатки: Міжвузівський збірник (за напрямком «Інженерна механіка»). – Луцьк: Луцький державний технічний університет, 2007. – Вип. 19. – С.33–43. 5. Глухов В.С., Євтушенко К.С., Заіченко Н.В., Оліярник Б.О. Криптографічні засоби спеціалізованої бортової ЕОМ для бронетехніки // Вісник Хмельницького національного університету. – Хмельницький, 2007. – № 2. – Т. 2. – С. .29–33. 6. Глухов В.С. Операційний пристрій для роботи з елементами поля Галуа, представленими у нормальній формі // Матеріали науково-технічної конференції ІППТ при Нац. ун-ті «Львівська політехніка». – Львів, 2007. 7. Глухов В.С. Обчислювальний пристрій для операцій над еліптичними кривими // Вісник Нац. ун-ту "Львівська політехніка" "Комп'ютерні системи та мережі". – Львів, 2006. – № 573. –С. 54–61. 8. Hlukhov V. Improvement of Algorithm for Computing Multiplicative Inverses in GF(2^m) Using Normal Bases. Матеріали конференції ACSN'2007. – Львів, 2007. 9. Глухов В.С.. Вдосконалення алгоритму обчислення оберненого елемента GF(2^t) в нормальному базисі // Вісник Нац. ун-ту "Львівська політехніка" "Комп`ютерні системи та мережі". –. Львів, 2007. – № 603. – С. 20–26.