УДК 004.382

М.В. Ногаль
Національний університет "Львівська політехніка"
кафедра електронних обчислювальних машин

ДОДАВАННЯ І МНОЖЕННЯ В ПОЛЯХ ГАЛУА

Розглянуто алгоритми додавання і множення в полях Галуа, описано основні принципи побудови суматора і перемножувача згідно з наведеними алгоритмами. Наведено функціональні схеми пристроїв, показано доцільність їх описання мовою описання апаратних засобів для подальшої реалізації на ПЛІС.

The algorithms of addition and multiplication are considered in the fields of Galua, basic principles of construction of adder and multiplier are described in obedience to the resulted algorithms. The functional diagrams of devices are resulted.

Вступ. Еліптичні криві над скінченними полями – один з найперспективніших інструментів для побудови криптографічних алгоритмів. Сьогодні для цілей криптографії використовуються зазвичай еліптичні криві над простим полем і над полем характеристики 2. У скінченних полях (або полях Галуа, як їх ще називають) основними операціями є операції підсумовування і множення.

Постановка задачі. Розглянути принципи побудови суматорів і перемножувачів в полях Галуа, реалізувати їх у вигляді моделей мовою описання апаратних засобів.

Поля Галуа. Полем називають множину елементів, на якій визначено дві операції. Одна з них називається додаванням і позначається $a+b$, а інша – множенням і позначається $a \cdot b$, навіть якщо ці операції не є звичайними операціями додавання і множення чисел. Для того, щоб множина елементів, на якій задані операції додавання і множення, була полем, необхідно, щоб для кожної з цих операцій виконувалися всі групові аксіоми, а саме комутативність ($a+b = b+a$ і $ab = ba$), асоціативність ($a+(b+c) = (a+b)+c$ і $a(bc) = (ab)c$), а також виконувався дистрибутивний закон, тобто для трьох будь-яких елементів поля a, b, c була справедлива рівність $a(b+c) = ab+ac$ і $(b+c)a = ba+ca$.

Варто відмітити, що групові властивості для операції множення справедливі для всіх ненульових елементів поля.

Поля з скінченним числом елементів q називають полями Галуа на ім'я їх першого дослідника Евариста Галуа і позначають $GF(q)$[1].

Число елементів поля q називають порядком поля. Скінченні поля використовуються для побудови більшості відомих кодів і їх декодування.

Найменше число елементів, які утворюють поле, дорівнює 2. Таке поле повинне містити 2 одиничних елементи: **0** щодо операції додавання і **1** щодо операції множення. Це поле $GF(2)$, або двійкове.

Залежно від значення q розрізняють прості або розширені поля. Поле називають простим, якщо q – просте число. Для позначення простих чисел використовуватимемо символ p. Просте поле утворюють числа за модулем p: $0, 1, 2., p-1$, а операції додавання і множення виконуються за модулем p. Якщо ж поле утворене з q^m елементів, то таке поле називають розширенням поля степеня m над $GF(p)$ або розширеним полем. Воно містить p^m елементів і позначається $GF(p^m)$. Надалі будемо розглядати поля $GF(2^m)$. Будь-яке скінченне поле $GF(2^m)$ є m-вимірним вектором над полем $GF(2)$. Многочлен $f(t)$ степеня m над полем $GF(2)$ є многочлен вигляду

$$f(t) = t_m + f^{m-1} t_{m-1} + \ldots + f_0,$$

де коефіцієнти многочлена f_i належать $GF(2)$. Операції над такими многочленами виконуються як операції над звичайними многочленами, тільки операції над коефіцієнтами виконуються в полі $GF(2)$.

Многочлен *f(t)* ненульового степеня називається незвідним над полем $GF(2^m)$, якщо він ділиться без залишку над цим полем на самого себе і на многочлени нульового степеня [2]. Елемент *x* скінченного поля $GF(2^m)$ називається коренем многочлена *f(t)*, якщо *f(x)=0.* Якщо *x* – корінь незвідного многочлена *p(x)* степеня *m*, то елементи $(x^{m-1}, ..., 1)$ утворюють базис скінченного поля $GF(2^m)$ як векторного простору над полем *GF(2)*. Такий базис називається поліноміальним. Многочлен, коренем якого є примітивний елемент, називається примітивним многочленом. Якщо як *P(x)* вибрати примітивний многочлен степеня *m*, незвідний над полем *GF(2)*,то отримаємо поле $GF(2^m)$ зі всіх 2^m двійкових послідовностей довжини *m*. Поліноміальний базис задається примітивним многочленом.

Елементи скінченного поля в поліноміальному базисі зображаються многочленами степеня не більше *m-1* або, що еквівалентно, двійковими рядками довжини *m*, що складаються з коефіцієнтів таких многочленів. Операції додавання і множення у скінченному полі в такому разі – це операції над многочленами степеня не більше *m-1* зі зведенням результату за потреби за модулем примітивного многочлена.

Додавання двох елементів виконується як додавання відповідних многочленів або як додавання за модулем 2 відповідних до цих многочленів двійкових рядків. Множення двох елементів виконується як множення відповідних многочленів з подальшим зведенням результатів за модулем примітивного многочлена.

Нормальним базисом поля $GF(2^m)$ є множина

$$B = \left\{\theta, \theta^2, \theta^{2^2}, ..., \theta^{2^{m-1}}\right\} \tag{1}$$

Елементи множини можна подати у вигляді двійкових рядків ($a_0\ a_1\ a_2\ \dots\ a_{m-1}$)

$$a_0\theta + a_1\theta^2 + a_2\theta^{2^2} + ... + a_{m-1}\theta^{2^{m-1}} \tag{2}$$

Залежно від параметра T розрізняють типи нормального базису і нормальні поліноми:

При T=1: $p(x) = t^m + t^{m-1} + ... + t^2 + t + 1$;

при T=2: $p_0(t) = 1$, $p_1(t) = t + 1$, $p_{i+1}(t) = tp_i(t) + p_{i-1}(t)$, $i = 1, ..., m$.

Виконання операцій додавання і множення в простих скінченних полях *GF(q)*

Суматор за модулем обчислює суму $Z=(X+Y)_q$, де число Z дорівнює залишку від ділення суми X+Y на число q. Числа Z, X, Y, і q зображають в двійковій формі і мають розрядність n. Необхідно синтезувати суматор за модулем q для будь-якого значення n.

Розглянемо суму

$$S = (X + Y) + (2^n - q), \tag{3}$$

де S має n+1 двійкових розрядів. Очевидно, що сума S може приймати значення $S<2^n$ і $S>=2^n$ залежно від значень X і Y. Якщо сума $S<2^n$, то (n+1) розряд числа S дорівнює 0 і з співвідношення (1) отримуємо, що X+Y<q, а отже, Z=X+Y.

Якщо ж сума $S>=2^n$, то (n+1) розряд числа S дорівнює 1 і з співвідношеня (3) випливає, що X+Y>=q, а отже, Z=X+Y-q.Таким чином існує співвідношення

$$Z = (X + Y)_q = \begin{cases} X + Y, якщо\ \ X + Y < q \\ X + Y - q, якщо\ \ X + Y \geq q \end{cases} \tag{4}$$

На основі співвідношення (4) може бути побудована схема суматора за модулем, де q – будь-яке просте число. На рис.1 показана схема суматора для n-розрядного числа q. Суматор D1 виконує обчислення суми чисел X і Y, суматор D2 віднімає від суми X+Y значення q, оскільки 2^n-q – доповнення числа q до 2^n. Мультиплексор подає на вихід суму $Z=(X+Y)_q$ залежно від розряду s_{n+1} (а ним буде розряд переповнення одного з суматорів).

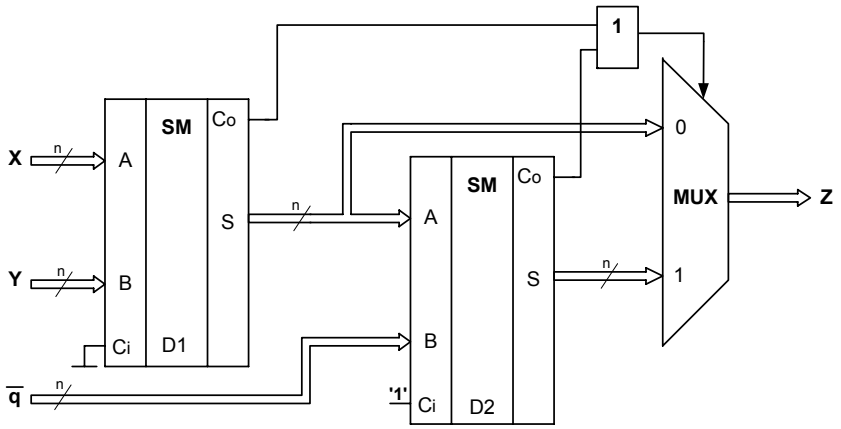
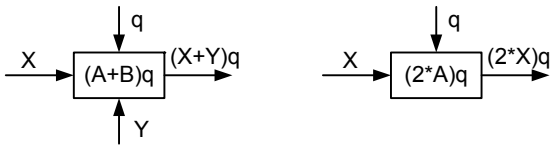


Рис. 1. n-розрядний суматор за модулем

Такий суматор можна описати однією з мов описання апаратних засобів для подальшого синтезу на ПЛІС. Було описано 1024-х розрядний суматор на VHDL.

У структурних схемах для суматорів за модулем q будемо використовувати умовне позначення, яке зображено на рис. 2а.



а *б*

Рис. 2. Умовне графічне позначення суматора за модулем q і перемножувача за модулем

Для добутку чисел X*Y існує співвідношення

$$X * Y = \sum_{p=1}^{n} y_p * X * 2^{p-1}, \tag{5}$$

де y_p=0 або 1. З цього випливає, що для побудови пермножувача за модулем q необхідно синтезувати типову схему, яка виконує операцію $(2*X)_q$ – перемноження на 2 за модулем q. Дійсно, оскільки $(X*2^{j+1})_q=(2*(X*2^j)_q)_q$, значення $(X*2^{p-1})_q$ можуть бути отримані послідовним використанням перемножувачів на 2 за модулем Правило побудови схеми такого перемножувача отримуємо з співвідношень (3) і (4), якщо візьмемо X=Y і S=2*X+(2^n-q). На рис. 2б показано умовне позначення перемножувача на 2 за модулем. На рис. 3 показано схема перемножувача на 2 за модулем для n-розрядного q. Перемноження числа X на 2 досягається зсувом розрядів числа X на один розряд відносно входів суматора, а тому потрібний лише один суматор. На виході мультиплексора отримуємо величину $Z=(2*X)_q$.

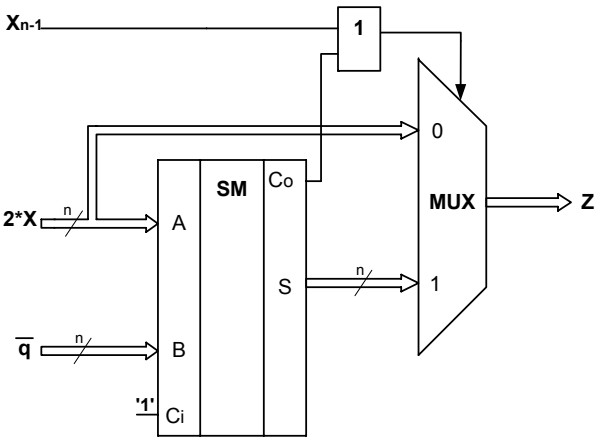


Рис. 3. n-розрядний перемножувач на 2 за модулем

На рис. 4 показана структурна схема перемножувача за модулем, яка обчислює величину

$$Z = (X * Y)_q = (\sum_{p=1}^{n} y_p * X * 2^{p-1})q, \qquad (6)$$

тут q і Z –n-розрядні двійкові числа. Тут числа q і X являють собою n-розрядні дані, а вузол & – сукупність логічних елементів І для порозрядного логічного перемноження числа X на розряди y_p, де p=1, 2, …, n.

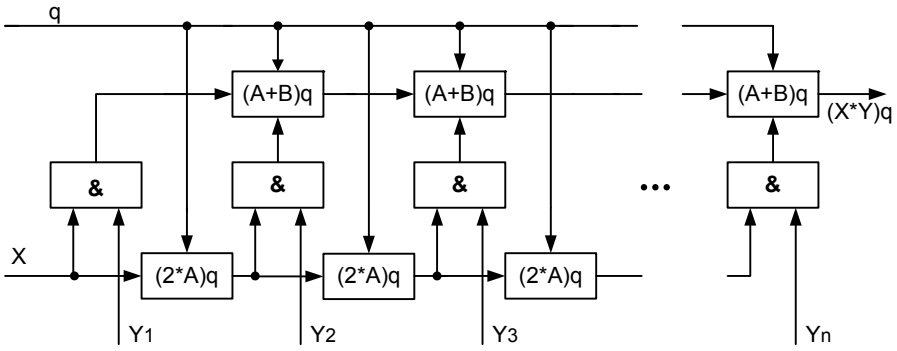


Рис. 4. n-розрядний перемножувач за модулем

Виконання операцій додавання і множення в поліноміальному базисі скінченного поля *GF(2^n)*

Додавання двох елементів виконується як додавання відповідних многочленів або як додавання за модулем 2 відповідних до цих многочленів двійкових рядків.

Тобто, додавання реалізується як порозрядне додавання за модулем 2 двох n-розрядних двійкових рядків.

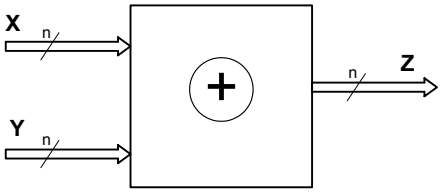


Рис. 5. n-розрядний додавач в поліноміальному базисі скінченного поля

Множення двох елементів виконується як множення відповідних многочленів з подальшим зведенням результатів за модулем примітивного многочлена.

Розглянемо такий приклад: маємо поле $GF(2^2)$, що задано примітивним многочленом a^4+a+1, обчислимо $(1011)\cdot(1001) = (a^3+a+1)\cdot(a^3+1)$. Спочатку отримаємо добуток многочленів, а потім зведемо результат за модулем примітивного многочлена.

Добуток дорівнюватиме $(a^3+a+1)\cdot(a^3+1) = a^6+a^3+a^4+a+a^3+1 = a^6+a^4+a^3+a^3+a+1 = a^6+a^4+a+1$. Можна виконувати множення двійкових рядків, воно буде виконуватись як звичайне множення, тільки

			1	0	1	1	(a^3+a+1)
		*					
			1	0	0	1	(a^3+1)
			1	0	1	1	
		⊕					
		0	0	0	0		
	⊕						
	0	0	0	0			
⊕							
1	0	1	1				
1	0	1	0	0	1	1	(a^6+a^4+a+1)

Для загального випадку, коли потрібно обчислити C=X*Y, де X і Y *n*-розрядні двійкові рядки, а C – *(2n-1)*-розрядний результат можна скористатись таким алгоритмом:

T:={0,0,…,0, x_{n-1},…,x_1,x_0}; C:={0,0,…,0};
для і від 0 до (n-1) виконати
початок
якщо y_i=1 тоді C:=C⊕T;
T=T логічний зсув вліво на 1 позицію;
i:=i+1;
кінець.

Далі для отримання результату знаходимо залишок від ділення отриманного добутку на примітивний многочлен.

$$
\begin{array}{l|l}
a^6+\ a^4\ \ +a+1 & a^4+a+1 \\
\oplus\ a^6\ \ +a^3+a^2 & \hline \\
\hline
a^4+a^3+a^2+a+1 & a^2+1 \\
\oplus\ a^4\ \ +a+1 & \\
\hline
a^3+a^2 &
\end{array}
$$

Якщо ділити двійкові рядки, то побачимо

					(a^6+a^4+a+1)				(a^4+a+1)			
	1	0	1	0	0	1	1	1	0	0	1	1
⊕	1	0	0	1	1	0	0	1	0	1		
	0	0	1	1	1	1	1	(a^2+1)				
⊕	0	0	1	0	0	1	1					
	0	0	0	1	1	0	0					
				(a^3+a^2)								

Для загального випадку, коли потрібно обчислити Z=C mod q, де C – *(2n-1)*-розрядний, q – (*n+1)*-розрядний двійковий рядок, а Z – *n*-розрядний результат можна скористатись таким алгоритмом:

T:=C; YY:={q_n,q_{n-1},…,q_0,0,…,0};
для і від (2n-2) до n виконати
початок
якщо x_i=1 тоді T:=T⊕YY;
YY=YY логічний зсув вправо на 1 позицію;
i:=i-1;
кінець.
Z:={t_{n-1},…,t_1,t_0}

Виконання операцій додавання і множення
в нормальному базисі скінченного поля $GF(2^m)$

Додавання двох елементів виконується як додавання відповідних многочленів або як додавання за модулем 2 відповідних до цих многочленів двійкових рядків. Тобто додавання реалізується аналогічно як і додавання в поліноміальному базисі.

Множення елементів в нормальному базисі виконується так:

Вхідні дані: двійкові рядки $a = (a_0\ a_1\ \dots\ a_{m-1})$ і $b = (b_0\ b_1\ \dots\ b_{m-1})$ і мультиплікативна матриця M. Результат $c = (c_0\ c_1\ \dots\ c_{m-1})$. Алгоритм множення:

1. Set x ← a.

2. Set y ← b.

3. For k from 0 to m – 1 do

3.1 Compute via matrix multiplication

$$c_k := x\ M\ y^{tr}$$

where y^{tr} denotes the matrix transpose of the vector y.

3.2 Set x ← LeftShift(x) and y ← LeftShift(y), where LeftShift denotes the circular left shift operation.

4. Output c = (c0 c1 … cm–1).

Для обчислення мультиплікативної матриці M виконуються такі обчислення:

$t=a_{0,0}+a_{0,1}t+a_{0,2}t^2+\dots+a_{0,m-1}t^{m-1}(mod(p(t)))$

$t^2=a_{1,0}+a_{1,1}t+a_{1,2}t^2+\dots+a_{1,m-1}t^{m-1}(mod(p(t)))$

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

...

$t^{2^{m-1}}=a_{m-1,0}+a_{m-1,1}t+a_{m-1,2}t^2+\dots+a_{m-1,m-1}t^{m-1}(mod(p(t)))$

Отримаємо матрицю A:

$$A := \begin{bmatrix} a_{0,0} & a_{0,1} & \dots & a_{0,m-1} \\ a_{1,0} & a_{1,1} & \dots & a_{1,m-1} \\ \dots & \dots & \dots & \dots \\ a_{m-1,0} & a_{m-1,1} & \dots & a_{m-1,m-1} \end{bmatrix}$$

Обчислимо матрицю B: $B=A^{-1}$. Маючи нормальний поліном

$p(t) = t^m + c_{m-1}t^{m-1} + \dots + c_1 t + c_0$ і матриці A і B, спочатку визначимо матрицю C

$$C := \begin{bmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & 1 \\ c_0 & c_1 & c_2 & \dots & c_{m-1} \end{bmatrix}$$

Обчислимо $D := ACB$ в полі GF (2); $d_{i,j}$ є (i, j) елементом матриці D, для $0 \le i,j < m$, визначимо мультиплікативну матрицю M так, де $\mu_{i,j} := d_{j-i,-i}$:

$$M := \begin{bmatrix} \mu_{0,0} & \mu_{0,1} & \dots & \mu_{0,m-1} \\ \mu_{1,0} & \mu_{1,1} & \dots & \mu_{1,m-1} \\ \dots & \dots & \dots & \dots \\ \mu_{m-1,0} & \mu_{m-1,1} & \dots & \mu_{m-1,m-1} \end{bmatrix}$$

У матриці M є *2*m-1* ненульових елементів. Практично замість мультиплікативної матриці обчислюються явні формули, які виражають один розряд добутку через розряди співмножників. Елемент перемножувача, що обчислює один розряд добутку, показаний на рис. 6.

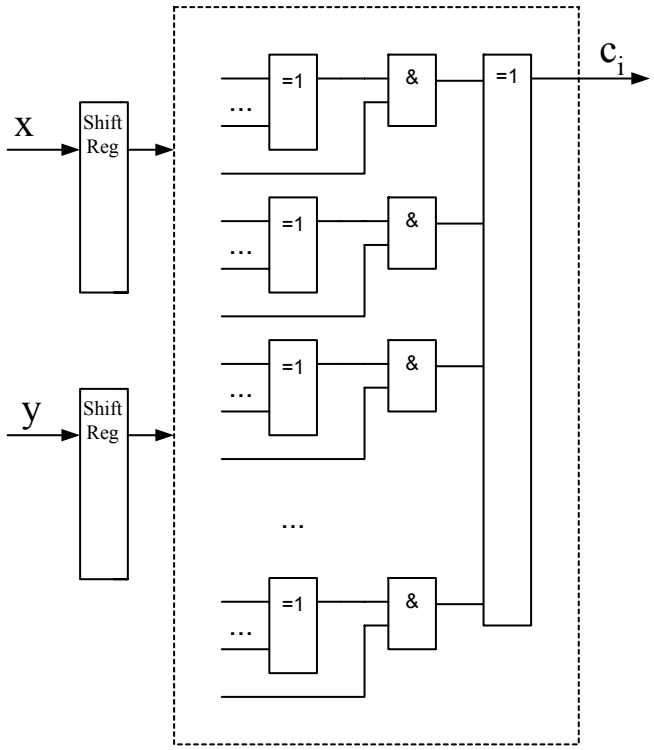


Рис. 6. Елемент перемножувача
в нормальному базисі скінченного поля

Висновки. Розглянуто алгоритми додовання і множення в полях Галуа, реалізовано суматор і перемножувач в полях Галуа мовою описання апаратних засобів VHDL, синтезовані ядра перевірені на функціональному рівні.

1. Конечные поля. В 2-х томах. 1988 Лидл Р. Нидеррайтер Г. Перевод на русский язик с дополнениями. – М.: Мир, 1988. 2. IEEE 1363-2000: Standard Specifications For Public Key Cryptography. 2000. The Institute of Electrical and Electronics Engineers, Inc. 3. Алгоритмические основы эллиптической криптографии. 2000. / А.А. Болотов, С.Б. Гашков, А.Б. Фролов, А.А. Часовских. – М.: Энергетический ин-т. 4. Пухальский Г.И., Новосельцева Т.Ф. Цифровые устройства: Учеб. пособие для втузов. – СПб: Политехника, 1996. – 885 с. 5. Пухальский Г.И., Новосельцева Т.Ф. Проектирование дискретных устройств на интегральных микросхемах: Справочник. – М.: Радио и связь, 1990. – 304с.