УДК 004.312.2:621.391.25:621.394.14(045)

[1]**Жуков И.А.**, д.т.н.,
[2]**Кубицкий В.И.**, к.т.н.

УМНОЖЕНИЕ ЭЛЕМЕНТОВ КОНЕЧНОГО ПОЛЯ GF(2^m) НА КОМБИНАЦИОННЫХ СХЕМАХ

[1]Национальный авиационный университет
[2]Всероссийский научно-исследовательский институт радиоаппаратуры
[1]zhuia@ukr.net,
[2]vkubitski@mail.ru

Разработаны метод и алгоритм непосредственного умножения элементов конечного поля GF(2^m) с использованием логических функций. Предлагается подход к построению комбинационных схем устройств, реализующих данный метод. Определены аппаратурные и временные сложности этих схем

Ключевые слова: конечные поля, комбинационные схемы, алгоритмы, сложность схем

Введение

Вычисления в конечных полях используются в теории кодирования, в криптографии, при цифровой обработке сигналов и в других областях науки и техники. Для выполнения операций над элементами конечных полей необходимо создавать специальные программные или аппаратные средства. При этом операции в конечных полях могут быть реализованы различными методами в зависимости от способа представления элементов конечного поля: на сдвиговых регистрах, в ПЗУ или ПЛМ, с использованием логических функций и др.

При разработке новых и усовершенствовании известных методов вычислений в конечных полях необходимо стремиться к улучшению таких параметров как время вычислений и аппаратурная сложность средств, реализующих эти методы. Анализ показывает, что перспективной с точки зрения времени вычислений является реализация операций в конечных полях методами, использующими логические функции.

В данной статье предложим метод умножения элементов конечного поля, основанный на использовании логических функций. Выведем математические выражения и разработаем алгоритм умножения элементов конечного поля $GF(2^m)$. Определим сложность схем устройств, реализующих разработанный метод.

Метод умножения элементов конечного поля

Представим элементы конечного поля $GF(2^m)$ в виде многочленов $a(x)$ и $b(x)$ над полем $GF(2)$, степень которых меньше m. Тогда умножение элементов поля $GF(2^m)$ выполняется по правилу умножения представляющих эти элементы многочленов по модулю заданного неприводимого многочлена $p(x) = x^m + p_{m-1}x^{m-1} + \ldots + p_0x^0 = x^m + h(x)$, т. е. $\left\langle a(x) \cdot b(x) \right|_{p(x)} = c(x)$.

Результатом умножения элементов конечного поля будет выражение

$$c = \sum_{i=0}^{m-1}(e_i + \sum_{j=0}^{m-2} p_i^{(j)} e_{m+j})\alpha^i, \qquad (1)$$

где $e_i = \sum_{u=0}^{i} a_{i-u} b_u$, $e_{m+j} = \sum_{u=1}^{m-1-j} a_{m-u} b_{j+u}$,

$p_i^{(j)} = \sum_{i=1}^{j} p_{m-1}\, p_i^{(j-1)} + p_{i-j}$

(при $j = 0$: $p_i^{(0)} = p_i$; при $i < j$: $p_{i-j} = 0$).

Назовём коэффициенты $p_i^{(j)}$ операционными коэффициентами конечного поля, а матрицу P этих коэффициентов – операционной матрицей конечного поля.

Метод умножения элементов конечного поля $GF(2^m)$ в соответствии с выражениями (1), основанный на умножении многочленов над полем $GF(2)$ с необходимостью вычисления операционных коэффициентов $p_i^{(j)}$, назовём методом

непосредственного умножения элементов конечного поля.

Представим выражение (1) в матричной форме

$$\begin{bmatrix} c_0 \\ c_1 \\ \vdots \\ c_{m-2} \\ c_{m-1} \end{bmatrix} = \begin{bmatrix} e_0 \\ e_1 \\ \vdots \\ e_{m-2} \\ e_{m-1} \end{bmatrix} \oplus \begin{bmatrix} p_0^{(0)} & p_0^{(1)} & \dots & p_0^{(m-2)} \\ p_1^{(0)} & p_1^{(1)} & \dots & p_1^{(m-2)} \\ \vdots & \vdots & \dots & \vdots \\ p_{m-2}^{(0)} & p_{m-2}^{(1)} & \dots & p_{m-2}^{(m-2)} \\ p_{m-1}^{(0)} & p_{m-1}^{(1)} & \dots & p_{m-1}^{(m-2)} \end{bmatrix} \otimes \begin{bmatrix} e_m \\ e_{m+1} \\ \vdots \\ e_{2m-3} \\ e_{2m-2} \end{bmatrix} = E_1 \oplus P \otimes E_2, \qquad (2)$$

где

$$\begin{bmatrix} e_0 \\ e_1 \\ \vdots \\ e_{m-2} \\ e_{m-1} \end{bmatrix} = \begin{bmatrix} a_0 & & & & \\ a_1 & a_0 & & & \\ \vdots & \vdots & \ddots & & \\ a_{m-2} & a_{m-3} & \dots & a_0 & \\ a_{m-1} & a_{m-2} & \dots & a_1 & a_0 \end{bmatrix} \otimes \begin{bmatrix} b_0 \\ b_1 \\ \vdots \\ b_{m-2} \\ b_{m-1} \end{bmatrix} = A_1 \otimes \begin{bmatrix} b_0 \\ b_1 \\ \vdots \\ b_{m-2} \\ b_{m-1} \end{bmatrix},$$

$$\begin{bmatrix} e_m \\ e_{m+1} \\ \vdots \\ e_{2m-3} \\ e_{2m-2} \end{bmatrix} = \begin{bmatrix} a_{m-1} & a_{m-2} & \dots & a_2 & a_1 \\ & a_{m-1} & \dots & a_3 & a_2 \\ & & \ddots & \vdots & \vdots \\ & & & a_{m-1} & a_{m-2} \\ & & & & a_{m-1} \end{bmatrix} \otimes \begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_{m-2} \\ b_{m-1} \end{bmatrix} = A_2 \otimes \begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_{m-2} \\ b_{m-1} \end{bmatrix}$$

Здесь $\otimes$, $\oplus$ – модульные операции умножения и сложения соответственно.

Запишем теперь выражение (2) в виде

$$\begin{bmatrix} c_0 \\ c_1 \\ \vdots \\ c_{m-2} \\ c_{m-1} \end{bmatrix} = \left\{ \begin{bmatrix} a_0 & & & & \\ a_1 & a_0 & & & \\ \vdots & \vdots & \ddots & & \\ a_{m-2} & a_{m-3} & \dots & a_0 & \\ a_{m-1} & a_{m-2} & \dots & a_1 & a_0 \end{bmatrix} \oplus \right.$$

$$\left. \oplus \begin{bmatrix} p_0^{(0)} & p_0^{(1)} & \dots & p_0^{(m-2)} \\ p_1^{(0)} & p_1^{(1)} & \dots & p_1^{(m-2)} \\ \vdots & \vdots & \dots & \vdots \\ p_{m-2}^{(0)} & p_{m-2}^{(1)} & \dots & p_{m-2}^{(m-2)} \\ p_{m-1}^{(0)} & p_{m-1}^{(1)} & \dots & p_{m-1}^{(m-2)} \end{bmatrix} \otimes \begin{bmatrix} 0 & a_{m-1} & a_{m-2} & \dots & a_2 & a_1 \\ & 0 & a_{m-1} & \dots & a_3 & a_2 \\ & & \ddots & & \vdots & \vdots \\ & & & & 0 & a_{m-1} & a_{m-2} \\ & & & & & 0 & a_{m-1} \end{bmatrix} \right\} \otimes \begin{bmatrix} b_0 \\ b_1 \\ \vdots \\ b_{m-2} \\ b_{m-1} \end{bmatrix} =$$

$$= (A_1 \oplus P \otimes A_2^*) \otimes B = A \otimes B. \qquad (3)$$

Выражения (2), (3) могут быть реализованы с помощью комбинационных схем. Покажем, как это можно сделать.

Реализация умножения элементов конечного поля

Умножение элементов поля $GF(2^m)$ в соответствии с выражением (3) можно выполнять в 3 этапа, применяя следующий алгоритм, который будем называть алгоритмом непосредственного умножения элементов конечного поля (алгоритм У3):

1. Производится умножение матриц $P \otimes A_2^*$:

$$\begin{bmatrix} 0 & p_0^{(0)} \otimes a_{m-1}, & p_0^{(0)} \otimes a_{m-2} \oplus p_0^{(1)} \otimes a_{m-1}, & \dots, & p_0^{(0)} \otimes a_1 \oplus \dots \oplus p_0^{(m-2)} \otimes a_{m-1} \\ 0 & p_1^{(0)} \otimes a_{m-1}, & p_1^{(0)} \otimes a_{m-2} \oplus p_1^{(1)} \otimes a_{m-1}, & \dots, & p_1^{(0)} \otimes a_1 \oplus \dots \oplus p_1^{(m-2)} \otimes a_{m-1} \\ \vdots & & & & \\ 0 & p_{m-2}^{(0)} \otimes a_{m-1}, & p_{m-2}^{(0)} \otimes a_{m-2} \oplus p_{m-2}^{(1)} \otimes a_{m-1}, \dots, & & p_{m-2}^{(0)} \otimes a_1 \oplus \dots \oplus p_{m-2}^{(m-2)} \otimes a_{m-1} \\ 0 & p_{m-1}^{(0)} \otimes a_{m-1}, & p_{m-1}^{(0)} \otimes a_{m-2} \oplus p_{m-1}^{(1)} \otimes a_{m-1}, & \dots, & p_{m-1}^{(0)} \otimes a_1 \oplus \dots \oplus p_{m-1}^{(m-2)} \otimes a_{m-1} \end{bmatrix} =$$

$$= \begin{bmatrix} 0 & d_{12}^{(1)} & d_{13}^{(1)} & \dots & d_{1m}^{(1)} \\ 0 & d_{22}^{(1)} & d_{23}^{(1)} & \dots & d_{2m}^{(1)} \\ \vdots & \vdots & \vdots & \dots & \vdots \\ 0 & d_{m-1,2}^{(1)} & d_{m-1,3}^{(1)} & \dots & d_{m-1,m}^{(1)} \\ 0 & d_{m2}^{(1)} & d_{m3}^{(1)} & \dots & d_{mm}^{(1)} \end{bmatrix} = D_1^{\cdot}$$

2. Выполняется сложение матриц $A_1 \oplus D_1$:

$$\begin{bmatrix} a_0, & d_{12}^{(1)}, & d_{13}^{(1)}, & \dots, & d_{1,m}^{(1)} \\ a_1, & a_0 \oplus d_{22}^{(1)}, & d_{23}^{(1)}, & \dots, & d_{2,m}^{(1)} \\ \vdots & \vdots & \vdots & \dots & \vdots \\ a_{m-2}, & a_{m-3} \oplus d_{m-1,2}^{(1)}, & a_{m-4} \oplus d_{m-1,3}^{(1)}, & \dots, & d_{m-1,m}^{(1)} \\ a_{m-1}, & a_{m-2} \oplus d_{m2}^{(1)}, & a_{m-3} \oplus d_{m3}^{(1)}, & \dots, & a_0 \oplus d_{m,m}^{(1)} \end{bmatrix} = \begin{bmatrix} d_{11}^{(2)} & d_{12}^{(2)} & \dots & d_{1,m}^{(2)} \\ d_{21}^{(2)} & d_{22}^{(2)} & \dots & d_{2,m}^{(2)} \\ \vdots & \vdots & \dots & \vdots \\ d_{m-1,1}^{(2)} & d_{m-1,2}^{(2)} & \dots & d_{m-1,m}^{(2)} \\ d_{m1}^{(2)} & d_{m2}^{(2)} & \dots & d_{m,m}^{(2)} \end{bmatrix} = D_2^{\cdot}$$

3. Выполняется умножение матриц $D_2 \otimes B$:

$$\begin{bmatrix} d_{11}^{(2)} \otimes b_0 \oplus d_{12}^{(2)} \otimes b_1 \oplus & \dots & \oplus d_{1,m}^{(2)} \otimes b_{m-1} \\ d_{21}^{(2)} \otimes b_0 \oplus d_{22}^{(2)} \otimes b_1 \oplus & \dots & \oplus d_{2,m}^{(2)} \otimes b_{m-1} \\ \vdots & & \\ d_{m-1,1}^{(2)} \otimes b_0 \oplus d_{m-1,2}^{(2)} \otimes b_1 \oplus \dots \oplus & & d_{m-1,m}^{(2)} \otimes b_{m-1} \\ d_{m1}^{(2)} \otimes b_0 \oplus d_{m2}^{(2)} \otimes b_1 \oplus & \dots & \oplus d_{m,m}^{(2)} \otimes b_{m-1} \end{bmatrix} = C^{\cdot}$$

При таком алгоритме умножения не используются комбинационные схемы умножения многочленов над полем $GF(2)$ (КСУМ) [1]. Умножение элементов конечного поля с использованием КСУМ выполняется на устройствах, представленных в [2].

Рассмотрим подход к построению схем устройств, реализующих умножение элементов конечного поля с использованием логических функций на основе разработанного метода, и приведём их аппаратурные и временные сложности.

Построение схем будем производить с использованием функциональных элементов базисного набора: схем *И* с двумя входами, схем *ИЛИ* с двумя входами и схем *НЕ*.

Комбинационная схема умножения (КСУЭ-У3), реализующая алгоритм умножения в соответствии с выражением (3) (алгоритм У3), имеет 2 уровня.

1-ый уровень, на котором вычисляется матрица $D_2 = (A_1 \oplus P \otimes A_2^*)$, состоит из следующих групп функциональных ячеек (ФЯ):

$$G_1^{(1)} = \left\{ D_{11}^{(1)}, \quad D_{12}^{(1)}, \dots, \quad D_{1,m-1}^{(1)} \right\},$$
$$G_2^{(1)} = \left\{ D_{21}^{(1)}, \quad D_{22}^{(1)}, \dots, \quad D_{2,m-1}^{(1)} \right\},$$
$$\vdots$$
$$G_m^{(1)} = \left\{ D_{m1}^{(1)}, \quad D_{m2}^{(1)}, \dots, \quad D_{m,m-1}^{(1)} \right\},$$

где $D_{ij}^{(1)}$ – блоки ФЯ, состоящие из схем *И* и сумматоров по модулю 2.

Этот уровень содержит $m^2(m-1)/2$ схем *И* и $m(m-1)^2/2$ сумматоров по модулю 2. Наличие схем *И* даёт возможность менять многочлен $p(x)$. При фик-

сированном многочлене $p(x)$ эти схемы не нужны, т. к. значения $p_i^{(j)}$ заложены в структуру 1-го уровня.

2-ой уровень, на котором выполняется умножение матриц $D_2 \otimes B$ составляет группа ФЯ $G_1^{(2)} = \{C_0, \ C_1, \dots, \ C_{m-1}\}$, содержащая m^2 схем *И* и $m(m-1)$ сумматоров по модулю 2.

При построении КСУЭ для любого неприводимого многочлена *p(x)* заданной степени можно добиться однородности и универсальности структуры схемы. Для этого в качестве базовой ячейки (БЯ) выбирается функциональная ячейка (ФЯ), состоящая из одного двухвходового элемента *И* и сумматора по модулю 2.

Построенная таким образом схема будет называться универсальной КСУЭ (УКСУЭ).

Универсальная КСУЭ (УКСУЭ-У3), реализующая выражение (3) и построенная на основе БЯ, как и КСУЭ-У3, имеет 2 уровня.

1-ый уровень УКСУЭ-У3 составляют блоки ФЯ $D_{ij}^{(1)}$ $(i = \overline{1, m}, \quad j = \overline{1, m-1})$, каждый из которых состоит из одной $(D_{11}^{(1)}, \ D_{21}^{(1)}, \dots, \ D_{m1}^{(1)})$ или нескольких (все остальные) БЯ.

2-ой уровень УКСУЭ-У3 состоит из блоков ФЯ C_i $(i = \overline{0, m-1})$, каждый из которых содержит m БЯ.

Структуру УКСУЭ-У3 можно наращивать при увеличении степени многочлена $p(x)$. Для этого необходимо сделать следующее:

1) каждый из регистров Рг1 и Рг2, в которых хранятся двоичные последовательности a и b соответственно, дополнить одной ячейкой со стороны старших разрядов и записать в них новые двоичные последовательности a и b;

2) каждую группу ФЯ $G_i^{(1)} = \{D_{i1}^{(1)}, \ D_{i2}^{(1)}, \dots, \ D_{i,m-1}^{(1)}\}$ $(i = \overline{1, m})$ дополнить блоком $D_{im}^{(1)}$, состоящим из m БЯ;

3) каждый блок C_i $(i = \overline{0, m-1})$ группы ФЯ $G_1^{(2)}$ дополнить одной БЯ, вход сумматора которой соединить с соответствующим выходом c_i, а входы схем *И* – с выходом b_m нового старшего разряда регистра Рг2 и выходом нового блока $D_{im}^{(1)}$;

4) создать новую группу ФЯ $G_{m+1}^{(1)} = \{D_{m+1,1}^{(1)}, \ D_{m+1,2}^{(1)}, \dots, \ D_{m+1,m}^{(1)}\}$ и дополнить ею 1-ый уровень УКСУЭ-У3. Входы этой группы соединить с соответствующими выходами регистра Рг1;

5) группу ФЯ $G_1^{(2)} = \{C_0, \ C_1, \dots, \ C_{m-1}\}$ дополнить блоком C_m из $(m+1)$ БЯ, входы которого соединить с соответствующим выходами группы $G_{m+1}^{(1)}$ и регистров Рг1 и Рг2;

6) на входы группы ФЯ 1-го уровня УКСУЭ-У3 подать новые значения $p_i^{(j)}$.

Определим аппаратурную и временную сложности схем.

Под аппаратурной сложностью (*N*) схемы будем понимать количество функциональных элементов базисного набора в схеме, реализующей заданную функцию.

Под временной сложностью (*T*) схемы будем понимать время, необходимое для реализации схемой заданной функции; при этом за единицу времени принимается время срабатывания элемента базисного набора (*t*).

Примем, что сложность (аппаратурная и временная) всех функциональных элементов базисного набора одинакова.

Время срабатывания элементов *И*, *ИЛИ*, *НЕ* и сумматора по модулю 2 обозначим как $t_И$, $t_{ИЛИ}$, $t_{НЕ}$, t_C соответственно. При этом $t_И = t_{ИЛИ} = t_{НЕ} = t$. Время сложения t_C в сумматоре по модулю 2, который можно реализовать с помощью 4-х элементов базисного набора, составляет 3*t*.

Определим сложность КСУЭ-У3 для нескольких вариантов построений.

1) Для любого неприводимого многочлена $p(x)$ заданной степени с предварительным вычислением величин $p_i^{(j)}$ *и их хранением.*

Расчёт показывает, что КСУЭ-УЗ имеет следующую аппаратурную и временную сложность (без учёта сложности вычисления величин $p_i^{(j)}$ и их хранения):

$$\widetilde{N}_{КСУЭ}^{ВФ} \le (2w+5)m^2 + 2\{m[k(k+1)-3w-2]-[k(k-1)-4]w-[k(k+3)+2]\}.$$

Здесь w, k – вес и степень многочлена $h(x)$ соответственно.

При $w=2$ и $k=1$ получим нижнюю границу аппаратурной сложности:

$$\widetilde{N}_{КСУЭ}^{НФ} \ge 9m^2 - 12m + 4.$$

Время умножения двух элементов поля $GF(2^m)$ на КСУЭ-УЗ для фиксированного многочлена $p(x)$ равно:

$$\widetilde{N}_{КСУЭ}^{В\ ИВ} \le m[m(5m-7)+3] \quad \text{– верхняя граница,}$$

$$\widetilde{N}_{КСУЭ}^{Н\ ИВ} \ge m[m(5m-9)+7]-2 \quad \text{– нижняя граница.}$$

$$\widetilde{T}_{КСУЭ}^{ИВ} = [(m-2)(3m-1)+16]t/2.$$

Сложность УКСУЭ-УЗ составляет (без учёта сложности схемы вычисления операционных коэффициентов $p_i^{(j)}$):

$\widetilde{N}_{УКСУЭ} = 5m^2(m+1)/2$, $\widetilde{T}_{УКСУЭ} = (3m+2)t$.

Вычисление операционных коэффициентов $p_i^{(j)}$ выполняется на устройствах, представленных в [3].

Выводы

Разработанный метод непосредственного умножения элементов конечного поля $GF(2^m)$ позволяет создавать устройства, реализующие этот метод, на комбинационных схемах. Структура таких схем однородна, универсальна и легко наращиваема. Полученные аналитические выражения сложности схем дают возможность делать выбор схем для различных вариантов их построения. Комбинационные схемы, реализующие новый метод вычислений в конечных полях, сокращают время вычислений по сравнению с реализацией на регистрах сдвига.

$$\widetilde{N}_{КСУЭ}^{И} = m(m+1)(5m-4)/2,$$

$$\widetilde{T}_{КСУЭ}^{И} = (3m+2)t.$$

2) Для фиксированного неприводимого многочлена $p(x)$ заданной степени.

С учётом нулевых элементов операционной матрицы P верхняя граница аппаратурной сложности КСУЭ-УЗ составляет:

$$\widetilde{T}_{КСУЭ}^{Ф} = (3m+1)t.$$

3) Для любого неприводимого многочлена $p(x)$ заданной степени и вычислением величин $p_i^{(j)}$.

Сложность КСУЭ-УЗ при одновременном вычислении всех $(m-1)$ *i*-ых коэффициентов $p_i^{(j)}$ равна:

Список литературы

1. Кубицкий В. И. Операции над многочленами в поле GF(2) / В. И. Кубицкий // Науч. вестн. ГосНИИ "Аэронавигация". – 2007. – №7. – С. 185-194.

2. Пат. №25491 Украина, МПК G06F 7/49 (2007/01). Пристрій для множення елементів скінченних полів GF(2^n) / Жуков И.А., Кубицкий В.И., Синельников А.А.; патентообладатель Нац. авиац. ун-т. - № u 2007 03644; заявл. 02.04.2007; опубл. 10.08.2007, Бюл. № 12.

3. Пат. №43629 Украина, МПК (2009) H03M 7/00. Пристрій для множення елементів скінченних полів GF(2^n) / Жуков И.А., Кубицкий В.И., Синельников А.А.; патентообладатель Нац. авиац. ун-т. – № u 2009 02754; заявл. 25.03.2009; опубл. 25.08.2009, Бюл. № 16.

Статью представлено в редакцию 15.09.2014