УДК 004.312.2:621.391.25:621.394.14(045)

**Кубицкий В.И.**

# СЛОЖНОСТЬ РЕАЛИЗАЦИИ ОПЕРАЦИЙ НАД ЭЛЕМЕНТАМИ КОНЕЧНОГО ПОЛЯ $GF(2^m)$

**ГосНИИ «Аэронавигация» (Россия, Москва)**

*Определяются аппаратурные и временные сложности реализации схем умножения элементов конечного поля GF($2^m$) для способа непосредственного умножения. Определены также сложности схем сложения. Сложности выполнения операций сложения и умножения приводятся как для двух любых элементов поля GF($2^m$), над которыми проводятся эти операции, так и для двух элементов, один из которых является фиксированным.*

Способ непосредственного умножения элементов конечного поля $GF(2^m)$ предложен в [1].

Здесь определим аппаратурные и временные сложности схем, с помощью которых можно будет реализовать этот способ. Сложности реализации будем определять как для схем, выполняющих операции над двумя любыми элементами поля, так и для схем, выполняющих операции над двумя элементами поля, один из которых является фиксированным.

Под *аппаратурной сложностью* реализации схемы будем понимать число функциональных элементов базисного набора (схем И с двумя входами, схем ИЛИ с двумя входами и схем НЕ) в схеме, реализующей заданную функцию.

Под *временной сложностью* реализации 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. Будем учитывать также, что сумматор по модулю 2 можно реализовать с помощью 4-х элементов базисного набора. Время сложения $t_C$ в сумматоре по модулю 2 составляет $3t$, так как принято, что время срабатывания схем И, ИЛИ и НЕ одинаковое и равно $t$.

Операции выполняются над элементами конечного поля, представленных многочленами:

$$\begin{aligned} a(x) &= a_{m-1}x^{m-1} + a_{m-2}x^{m-2} + \ldots + a_1 x + a_0, \\ b(x) &= b_{n-1}x^{n-1} + b_{n-2}x^{n-2} + \ldots + b_1 x + b_0, \end{aligned} \qquad (1)$$

где $a_i, b_j \in GF(2), n \le m$.

При умножении в качестве множимого используется элемент конечного поля, представленный многочленом $a(x)$, в качестве множителя - элемент конечного поля, представленный многочленом $b(x)$. Используем обозначения, принятые в [1].

## 1. Сложность реализации комбинационных схем сложения элементов конечного поля (КССЭ)

Сложение элементов конечного поля $GF(2^m)$ выполняется так же, как сложения двух многочленов над полем $GF(2)$. То есть производится одновременное поразрядное сложение по модулю 2 коэффициентов при неизвестных многочленов, представляющих элементы конечного поля, с помощью сумматоров по модулю 2.

Для построения комбинационной схемы сложения двух элементов конечного поля (КССЭ) необходимо иметь элементов базисного набора в количестве:

$$N_{КССЭ} = 4m .$$

При этом сложение выполняется за время равное:

$$T_{КССЭ} = 3t .$$

При выполнении сложения элементов поля, один из которых является фиксированным, сложность комбинационной схемы сложения (КССФЭ) будет следующей:

$$N_{КССФЭ} = 4v ,$$
$$T_{КССФЭ} = 3t ,$$

где $v$ – вес фиксированного элемента поля.

**2. Сложность реализации комбинационных схем непосредственного умножения элементов конечного поля (КСУЭ)**

Сначала определим сложность реализации схемы вычисления операционных коэффициентов $p_i^{(j)}$.

Схема одного $i$-го разряда устройства вычисления коэффициентов $p_i^{(j)}$ содержит $(m-1)(m-2)/2$ схем И и столько же сумматоров по модулю 2. Для одновременного вычисления всех $(m-1)$ $i$-ых коэффициентов необходимо иметь $m$ таких схем. Таким образом, получим следующую аппаратурную сложность реализации устройства (схемы) вычисления операционных коэффициентов (СВОК):

$N^{B}_{СВОК} \le 5m(m-1)(m-2)/2$ - верхняя граница.

Схемы каждого из разрядов имеют разное количество сумматоров по модулю 2. Так в схеме 1-го разряда на $(m-2)$ сумматоров меньше, чем в схеме $m$-го разряда; в схеме 2-го разряда – меньше на $(m-3)$; в схеме 3-го разряда - меньше на $(m-4)$;…; в схеме $(m-1)$-го разряда - меньше на 1. То есть по совокупности потребуется меньше сумматоров по модулю 2 на величину $(m-1)(m-1)/2$. Учитывая это, получим:

$N^{H}_{СВОК} \ge (m-1)[m(5m-14)+4]/2$ - нижняя граница.

Все значения коэффициентов $p_i^{(j)}$ будут получены через время:

$$T_{СВОК} = (m-2)(3m-1)t/2 .$$

Если потребуется запоминать все вычисленные значения $p_i^{(j)}$, то необходимо будет иметь $m(m-1)$ ячеек памяти.

Определим сложность КСУЭ.

В [1] показано, что умножение в поле $GF(2^m)$ можно производить в 3 этапа. В соответствии с этим выделено 3 уровня комбинационной схемы умножения (КСУЭ).

<u>На 1-ом уровне КСУЭ</u>, который представляет собой комбинационную схему умножения многочленов над полем $GF(2)$ (КСУМ), вычисляются величины $e_i$ $(i=\overline{0, 2m-2})$, представленные матрицами:

$$A_1 = \begin{bmatrix} e_0 \\ e_1 \\ e_2 \\ \vdots \\ e_{m-2} \\ e_{m-1} \end{bmatrix} = \begin{bmatrix} a_0 & & & & \\ a_1 & a_0 & & & \\ a_2 & a_1 & a_0 & & \\ \vdots & \vdots & & \ddots & \\ a_{m-2} & a_{m-3} & \dots & a_0 & \\ a_{m-1} & a_{m-2} & \dots & a_1 & a_0 \end{bmatrix} \otimes \begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ \vdots \\ b_{m-2} \\ b_{m-1} \end{bmatrix},$$

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

Этот уровень содержит $m^2$ схем И и $(m-1)^2$ сумматоров по модулю 2. С учетом того, что сумматор по модулю 2 реализуется из 4-х элементов базисного набора, аппаратурная сложность 1-го уровня КСУЭ составляет:

$$N_1 = N_{КСУМ} = m(5m-8)+4 .$$

Время умножения равно:

$$T_1 = T_{КСУМ} = t_И + (m-1)t_C = (3m-2)t .$$

<u>На 2-ом уровне КСУЭ</u> реализуется произведение матриц $P \otimes A_2$, т. е. вычисляются величины $e'_i$ $(i=\overline{0, m-1})$:

$$\begin{bmatrix} p^{(0)}_{m-1} & p^{(1)}_{m-1} & \dots & p^{(m-2)}_{m-1} \\ p^{(0)}_{m-2} & p^{(1)}_{m-2} & \dots & p^{(m-2)}_{m-2} \\ \vdots & \vdots & \dots & \vdots \\ p^{(0)}_{1} & p^{(1)}_{1} & \dots & p^{(m-2)}_{1} \\ p^{(0)}_{0} & p^{(1)}_{0} & \dots & p^{(m-2)}_{0} \end{bmatrix} \otimes$$

$$\otimes \begin{bmatrix} a_{m-1} & a_{m-2} & \dots & a_2 & a_1 \\ & a_{m-1} & \dots & a_3 & a_2 \\ & & \ddots \dots & \vdots & \vdots \\ & & & a_{m-1} & a_{m-2} \\ & & & & a_{m-1} \end{bmatrix} \otimes$$

$$\otimes \begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_{m-2} \\ b_{m-1} \end{bmatrix}.$$

Для варианта построения схемы с возможностью изменения неприводимого полинома $p(x)$ этот уровень составляет группа функциональных ячеек (ФЯ), которая содержит $m(m-1)$ схем И и $m(m-2)$

сумматоров по модулю 2. Здесь схемы И необходимы для того, чтобы иметь возможность изменять полином *p(x)*. Аппаратурные затраты составляют:

$$N_2 = m(5m-9).$$

Временная сложность 2-го уровня КСУЭ равна:

$$T_2 = t_И + (m-2)t_C = (3m-5)t.$$

При фиксированном полиноме *p(x)* схемы И не нужны, так как коэффициенты $p_i^{(j)}$ заложены в структуру схемы умножения матриц $P \otimes A_2$. При этом, как показано в [1], операционная матрица *P* будет иметь не менее (*m-k*)(*m-w*) нулевых коэффициентов $p_i^{(j)}$. Тогда количество сумматоров по модулю 2 в схеме умножения матриц $P \otimes A_2$ не больше (*k+w*-2)*m-kw*. Значит, аппаратурная сложность будет не больше:

$$N_2^Ф = 4[m(k+w-2)-kw].$$

Здесь $w$ - вес полинома $h(x) = $
$= p_{m-1} \cdot x^{m-1} + \ldots + p_0 \cdot x^0$, являющегося частью неприводимого примитивного полинома $p(x) = x^m + p_{m-1} \cdot x^{m-1} + \ldots +$
$+ p_0 \cdot x^0 = x^m + h(x)$ степени $m$;
$k = m-r-1$ - степень полинома *h(x)*, $(r = \overline{0, m-2})$.

Временная сложность 2-го уровня КСУЭ равна:

$$T_2^Ф = (w_1-1)t_C = 3(w_1-1)t,$$

где $w_1$ - максимальный вес из множества весов $\{w_0^{(i)}, \ldots, w_{m-1}^{(i)}\}$ векторов

$$[p_0^{(0)}, p_0^{(1)}, \ldots, p_0^{(m-2)}]$$
$$,\ldots\ldots\ldots\ldots\ldots,$$
$$[p_{m-1}^0, p_{m-1}^1, \cdots, p_{m-1}^{m-2}].$$

<u>На 3-м уровне КСУЭ</u> реализуется сумма векторов $e_i$ и $e'_i$ $(i = \overline{0, m-1})$. Этот уровень составляет группа ФЯ, которая содержит $m$ сумматоров по модулю 2. Аппаратурная сложность 3-го уровня КСУЭ равна:

$$N_3 = 4m.$$

Временная сложность 3-го уровня КСУЭ составляет:

$$T_3 = t_C = 3t.$$

Определим аппаратурную и временную сложности схем умножения для нескольких вариантов задания неприводимого полинома *p(x)*.

*1) Для случая умножения с возможностью изменения неприводимого полинома p(x) заданной степени с предварительным вычислением операционных коэффициентов* $p_i^{(j)}$ *и их хранением.*

Расчет показывает, что КСУЭ имеет следующую аппаратурную сложность (без учета сложности вычисления величин $p_i^{(j)}$ и их хранения):

$$N_{КСУЭ}^{II} = N_1 + N_2 + N_3 = m(10m-13)+4.$$

Время умножения составляет:

$$T_{КСУЭ}^{II} = 2t_И + mt_C = (3m+2)t.$$

*2) Для фиксированного полинома p(x).*

В этом случае величины $p_i^{(j)}$ вычисляются заранее (до синтеза схемы) и их значения (0 или 1) учитываются в структуре схемы умножения, во 2-ом уровне которой будут отсутствовать некоторые элементы, характерные для схем, реализующих приведенный выше случай (1) (схемы И для умножения величин $e_k \otimes p_i^{(j)}$ $k = \overline{m, 2m-2}$ и некоторые сумматоры по модулю 2). Отсутствуют те сумматоры по модулю 2, для которых одним из слагаемых является произведение величин $e_k \otimes p_i^{(j)}$, в котором $p_i^{(j)}=0$.

С учетом этого аппаратурная сложность КСУЭ составляет:

$$N_{КСУЭ}^{ВФ} = N_1 + N_2^Ф + N_3 \le$$
$$\le m[5m+4(k+w)-12]-4(kw-1)$$ - верхняя граница.

Как известно, для многих значений $m$ существуют неприводимые над полем $GF(2^m)$ примитивные полиномы, вес которых равен 3 (а значит $w$=2) и $k$=1. Получается нижняя граница аппаратурной сложности:

$N^{НФ}_{КСУЭ} \geq 5m^2 - 4$ - нижняя граница.

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

$$T^{Ф}_{КСУЭ} = T_1 + T_3 = t_И + mt_С = (3m+1)t.$$

*3) Для случая умножения с возможностью изменения неприводимого полинома p(x) заданной степени и вычислением величин* $p_i^{(j)}$.

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

$N^{ВП}_{КСУЭ} \leq N^{В}_{СВОК} + N^{П}_{КСУЭ} = \{m[5m(m-1)-16]+8\}/2$ - верхняя граница,

$N^{НП}_{КСУЭ} \geq N^{Н}_{СВОК} + N^{П}_{КСУЭ} = \{m[m(5m+1)-8]+4\}/2$ - нижняя граница.

Здесь при определении верхней границы сложности КСУЭ учитывалось, что сложности всех схем поразрядного вычисления коэффициентов $p_i^{(j)}$ одинаковы. При определении нижней границы эти сложности разные из-за неодинакового количества сумматоров по модулю 2.

Временная сложность КСУЭ:

$T^{(4)}_{КСУЭ} = T_{СВОК} + T_2 + T_3 = [m(3m-1)-2]t/2$

- для $m \geq 4$,

$T^{(3)}_{КСУЭ} = T_1 + T_2 + T_3 = 2(3m-2)t$ - для $m \leq 3$.

### 3. Сложность реализации универсальных комбинационных схем непосредственного умножения элементов конечного поля (УКСУЭ)

При построении КСУЭ для любого неприводимого полинома $p(x)$ заданной степени можно добиться однородности и универсальности структуры схемы, в отличие от структур линейных последовательностных машин [2], определяемых конкретным видом элементов конечного поля, над которыми производятся операции. 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), которая, как и КСУЭ, имеет три уровня.

1-й уровень УКСУЭ представляет собой универсальную КСУМ (УКСУМ) и имеет следующую аппаратурную сложность:

$$N_1 = N_{УКСУМ} = 5m^2.$$

Время умножения равно:

$$T_1 = T_{УКСУМ} = t_И + mt_С = (3m+1)t;$$

2-й уровень УКСУЭ содержит $m(m$-1) схем И и $m(m$-1) сумматоров по модулю 2.

Аппаратурные затраты составляют:

$$N_2 = 5m(m-1).$$

Временная сложность 2-го уровня УКСУЭ равна:

$$T_2 = t_И + (m-1)t_С = (3m-2)t.$$

3-й уровень.

Аппаратурная сложность 3-го уровня УКСУЭ равна:

$$N_3 = 5m.$$

Временная сложность 3-го уровня УКСУЭ составляет:

$$T_3 = t_И + t_С = 4t.$$

Таким образом, сложность УКСУЭ равна:

$$N_{УКСУЭ} = N_1 + N_2 + N_3 = 10m^2,$$

$$T_{УКСУЭ} = T_1 + T_3 = (3m+5)t.$$

Отметим, что при определении сложности реализации УКСУЭ не учитывалась сложность реализации схемы вычисления операционных коэффициентов $p_i^{(j)}$.

### 4. Сложность реализации комбинационных схем непосредственного

**умножения на фиксированный элемент конечного поля**

Умножение произвольного элемента $a=(a_0,\dots,a_{m-1})$ поля $GF(2^m)$ на фиксированный элемент $b=(b_0,\dots,b_{n-1})$ этого поля можно производить на рассмотренных КСУЭ (здесь $n \le m$). Но для данного умножения эти схемы можно упростить. Здесь значения величин $b_i$ (0 или 1) фиксированного элемента $b$ известны заранее (до синтеза схемы) и учитываются в структуре схемы умножения, в которой будут отсутствовать некоторые элементы, характерные для КСУЭ.

Комбинационные схемы умножения на фиксированный элемент поля (КСУФЭ) также, как и КСУЭ, имеют 3 уровня.

Пусть $v$ – вес фиксированного элемента; $K$ – множество степеней неизвестной многочлена, представляющего фиксированный элемент, коэффициенты $b_i$ при которой не равны 0; $|K| = v$.

Определим сложности реализации схем умножения на фиксированный элемент конечного поля для нескольких вариантов задания неприводимого полинома $p(x)$.

1) *Для случая умножения с возможностью изменения неприводимого полинома $p(x)$ заданной степени с предварительным вычислением операционных коэффициентов $p_i^{(j)}$ и их хранением.*

1-й уровень КСУФЭ представляет собой комбинационную схему умножения любого многочлена на фиксированный многочлен (КСУФМ) над полем $GF(2)$ и имеет следующую аппаратурную сложность:

$$N_1 = N_{КСУФМ} = \\ = 4[(v-1)(m-1) - \sum_{i=1}^{v-1}(k_{i+1} - k_i - 1)] = \\ = 4[m(v-1) - \sum_{i=1}^{v-1}(k_{i-1} - k_i)].$$

Время умножения на 1-ом уровне КСУФЭ равно:

$$T_1 = T_{КСУФМ} = (v-1)t_C = 3(v-1)t .$$

При $v=n$ получаем верхние границы сложности реализации 1-го уровня КСУФЭ:

$$N_1^B = N_{КСУФМ}^B \le 4(n-1)(m-1) \text{ при } n<m,$$

$$N_1^B = N_{КСУФМ}^B \le 4(m-1)^2 \text{ при } n=m;$$

$$T_1^B = T_{КСУФМ}^B \le (n-1)t_C = 3(n-1)t \text{ при } n<m,$$

$$T_1^B = T_{КСУФМ}^B \le (m-1)t_C = 3(m-1)t \text{ при } n=m.$$

2-й уровень КСУФЭ содержит $m(n$-1) схем И и $m(n$-2) сумматоров по модулю 2. Здесь схемы И необходимы для того, чтобы иметь возможность изменять полином $p(x)$.

Сложность 2-го уровня КСУФЭ не зависит от веса фиксированного элемента и равна сложности 2-го уровня КСУЭ.

Аппаратурные затраты составляют:

$$N_2 = m(5n-9).$$

Временная сложность 2-го уровня КСУФЭ равна:

$$T_2 = t_H + (n-2)t_C = (3n-5)t .$$

Пусть $s_2$ - количество расположенных подряд нулей в фиксированном элементе, начиная с младшего разряда. Тогда аппаратурная сложность 3-го уровня КСУФЭ равна:

$$N_3 = 4(m - s_2).$$

Если $s_2 \ne n$ (обратное означало бы, что фиксированный элемент конечного поля равен 0), то временная сложность 3-го уровня КСУФЭ составляет:

$$T_3 = t_C = 3t .$$

При $v=n$ величины $s_2=0$ и получим верхнюю границу аппаратурной сложности 3-го уровня КСУФЭ:

$$N_3^B \le 4m .$$

Таким образом, для общего случая умножения с возможностью изменения неприводимого полинома $p(x)$ заданной степени имеем:

а) аппаратурную сложность КСУФЭ:

$$N^{II}_{КСУФЭ} = N_1 + N_2 + N_3 =$$
$$= m[4(v-1)+5(n-1)] - 4[(v-1) +$$
$$+ \sum_{i=1}^{v-1}(k_{i+1} - k_i - 1) + s_2];$$

б) время умножения на КСУФЭ (с учетом того, что $T_2 > T_1$ при $v < n$):

$$T^{II}_{КСУФЭ} = T_2 + T_3 = (3n-2)t.$$

Верхние границы сложности КСУФЭ для изменяемого полинома *p(x)* заданной степени получим при $v = n$:

а) аппаратурная сложность:

$$N^{BII}_{КСУФЭ} = N^B_1 + N_2 + N^B_3 \le (n-1)(9m-4)$$

- верхняя граница;

б) временная сложность (с учетом того, что $T^B_1 > T_2$):

$T^{BII}_{КСУФЭ} = T^B_2 + T_3 \le 3nt$ - верхняя граница.

2) *Для фиксированного полинома p(x).*

Здесь неприводимый полином *p(x)* фиксирован, а операционные коэффициенты $p_i^{(j)}$ вычислены заранее и их значения учтены в структуре схемы.

<u>1-й уровень</u> КСУФЭ для фиксированного полинома *p(x)* представляет собой комбинационную схему умножения любого многочлена на фиксированный многочлен (КСУФМ) над полем $GF(2)$ и имеет такие же аппаратурную и временную сложности, как 1-ый уровень КСУФЭ для рассмотренного выше случая изменяемого полинома *p(x)*.

Если для <u>2-го уровня</u> КСУФЭ учесть, что множитель $b = (b_0, \dots, b_{n-1})$ является фиксированным элементом, сложность может быть уменьшена по сравнению со сложностью 2-го уровня КСУЭ для случая фиксированного полинома *p(x)*.

Как было показано, аппаратурная сложность 2-го уровня КСУЭ равна:

$$N^{\Phi}_{2\,КСУЭ} = 4[m(k+w-2) - kw].$$

Так как *deg b(x)≤m*-1, то необходимо из общего количества $[m(k+w-2)-kw]$ сумматоров по модулю 2 вычесть величину:

$$[(m-1)-(n-1)]m$$

при $[(m-1)-(n-1)] < k$;

$$m(k-1) + (w-1)[(m-1)-(n-1)-k+1]$$

при $[(m-1)-(n-1)] \ge k$.

Получим аппаратурную сложность 2-го уровня КСУФЭ для фиксированного полинома *p(x)*:

$$N_2^{\Phi(1)} = 4\{m[(k+w-2)-(m-n)] - kw\}$$

при $[(m-1)-(n-1)] < k$;

$$N_2^{\Phi(2)} = 4[(n-1)(w-1) - k]$$

при $[(m-1)-(n-1)] \ge k$.

Видно, что аппаратурная сложность 2-го уровня КСУФЭ не зависит от веса фиксированного элемента.

Временная сложность 2-го уровня КСУФЭ также не зависит от веса фиксированного элемента и равна:

$$T_2^{\Phi} = (w_2 - 1)t_C = 3(w_2-1)t,$$

где $w_2$ - максимальный вес из множества весов $\{w_0^{(i)}, \dots, w_{m-1}^{(i)}\}$ векторов

$$[p_{m-1}^{(0)}, p_{m-1}^{(1)}, \dots, p_{m-1}^{(n-2)}]$$
$$,\dots\dots\dots\dots\dots\dots ;$$
$$[p_0^{(0)}, p_0^{(1)}, \dots, p_0^{(n-2)}]$$

($n$-1) - степень полинома *b(x)*, представляющего фиксированный элемент конечного поля.

Как уже отмечалось, для многих значений $m$ существуют неприводимые над полем $GF(2^m)$ примитивные полиномы с величинами $w$=2 и $k$=1. Тогда получим нижнюю границу аппаратурной сложности 2-го уровня КСУФЭ:

$$N_2^{H\Phi(1)} \ge 4(m-2)$$

при $[(m-1)-(n-1)] < k$;

$$N_2^{H\Phi(2)} \ge 4(n-2)$$

при $[(m-1)-(n-1)] \ge k$.

Величина $[(m-1)-(n-1)] = s_1$ характеризует количество расположенных подряд нулей в фиксированном элементе, начиная со старшего разряда.

Таким образом, аппаратурная сложность КСУФЭ для фиксированного полинома $p(x)$ равна:

а) при $s_1 < k$:

$$N^{\Phi(1)}_{КСУФЭ} = N_1 + N_2^{\Phi(1)} + N_3 =$$
$$= 4\{m[(k+w-2)+v-(m-n)]-kw-$$
$$-[(v-1)++\sum_{i=1}^{v-1}(k_{i-1}-k_i-1)+s_2]\};$$

б) при $k \le s_1$:

$$N^{\Phi(2)}_{КСУФЭ} = N_1 + N_2^{\Phi(2)} + N_3 =$$
$$= 4\{mv+(n-1)(w-1)-k-$$
$$-[(v-1)++\sum_{i=1}^{v-1}(k_{i+1}-k_i-1)+s_2]\}.$$

Верхнюю границу аппаратурной сложности КСУФЭ для фиксированного полинома $p(x)$ получим при $v=n$. Она равна:

а) при $s_1 < k$:

$$N^{В\Phi(1)}_{КСУФЭ} = N_1^B + N_2^{\Phi(1)} + N_3^B \le$$
$$\le 4\{(n-1)(m-1)+$$
$$+m[(k+w-2)-(m-n)+1]-kw\}.$$

б) при $k \le s_1$:

$$N^{В\Phi(2)}_{КСУФЭ} = N_1^B + N_2^{\Phi(2)} + N_3^B \le$$
$$\le 4[mn+(n-1)(w-2)-k].$$

Нижняя граница аппаратурной сложности КСУФЭ для фиксированного полинома $p(x)$ получается при $w$=2 и $k$=1. Она составляет:

а) при $s_1 < k$:

$$N^{Н\Phi}_{КСУФЭ} = N_1 + N_2^{Н\Phi(1)} + N_3 \ge$$
$$\ge 4\{(v+1)(m-1)-[\sum_{i=1}^{v-1}(k_{i-1}-k_i-1)+s_2]\};$$

б) при $k \le s_1$:

$$N^{Н\Phi}_{КСУФЭ} = N_1 + N_2^{Н\Phi(2)} + N_3 \ge$$
$$\ge 4\{v(m-1)+(n-1)-[\sum_{i=1}^{v-1}(k_{i+1}-k_i-1)+s_2]\}.$$

Время умножения на КСУФЭ для фиксированного полинома $p(x)$ равно:

$$T^{\Phi}_{КСУФЭ} = \begin{cases} T_1 + T_3 = vt_C = 3vt, \\ \quad при \quad v \ge w_2; \\ T_2^{\Phi} + T_3 = w_2 t_C = 3w_2 t, \\ \quad при \quad w_2 \ge v. \end{cases}$$

### Выводы

Полученные математические выражения для определения сложности схем, реализующих непосредственное умножение элементов конечного поля $GF(2^m)$, позволяют определять и давать оценку этой сложности, а также делают возможным производить выбор наилучших схем по параметрам сложности (аппаратурной, временной) с учетом других известных для выполнения указанной операции схем, если известны сложности этих схем.

### Список литературы

1. *Жуков И. А., Кубицкий В.И., Дрововозов В.И.* Алгоритмы выполнения операций над элементами конечного поля $GF(2^m)$ в вычислительных устройствах. – Матеріали VIII Міжнародної науково-технічної конференції "АВІА-2007". – Т.1. – К.: НАУ, 2007.– С. 13.5-13.8.

2. *Гилл А.* Линейные последовательностные машины. – М.: Наука, 1974. – 287 с.