УДК 519.7, 512.624

А.А. Бурцев[1], *С.Б. Гашков*[2]

[1]Московский физико-технический институт (государственный университет)
[2]Московский государственный университет имени М.В. Ломоносова

О схемной реализации арифметики в конечных полях характеристики 7 для вычисления спариваний*

Рассматриваются логические схемы из двухвходовых булевых элементов, реализующих двухместные булевы функции. Применительно к криптографическим протоколам на эллиптических кривых, основанным на спаривании, изучаются схемные методы умножения многочленов над полями характеристики 7. Рассматриваются схемные методы реализации арифметики полей $GF(7)$, $GF(7^2)$, $GF(7^n)$, $GF(7^{7n})$ и $GF(7^{14n})$, оценивается сложность и глубина соответствующих схем. Все вычисления, за исключением касающихся глубины схем, можно сформулировать и в терминах программной реализации.

Ключевые слова: схемы для арифметики в конечных полях, криптографические протоколы.

I. Введение

В работах [5–7] для реализации криптографических протоколов было предложено использовать эллиптические кривые над полями нечетной характеристики. Как следствие появился интерес к реализации арифметики в этих и других полях нечетной характеристики (см., например, [8–11]). Дуурсма И. и Ли Х.-С. [12, 13] модифицировали быстрый алгоритм для быстрого вычисления спаривания на эллиптических кривых $Y^2 = X^3 - X \pm 1$ над полями $GF(3^n)$ из [5] и применили его для реализации спаривания Тейта для гиперэллиптических кривых $C_b = Y^2 = X^p - X + b$, $b = \pm 1$, над полем $k = GF(p^n)$, $GCD(n, 2p) = 1$, $p \equiv 3 \pmod 4$, и над расширениями extensions $F = GF(p^{pn})$ и $K = GF(p^{2pn})$ поля k. Эти кривые могут рассматриваться как обобщение кривых $E_{3,b}$: $Y^2 = X^3 - X + b$. В первоначальной версии алгоритма Дуурсма–Ли помимо обычных арифметических операций используется операция извлечения кубического корня. Квон С. (см. [14]) предложил модификацию алгоритма Дуурсма–Ли без операции извлечения кубического корня. Этот модифицированный алгоритм мы называем ниже алгоритмом Дуурсма–Ли–Квона (ДЛК-алгоритмом). В [7] введено так называемое η-pairing и показано, что для его вычисления можно в два раза сократить длину цикла алгоритма Дуурсма–Ли. В статье [15] показано, как исключить извлечение кубических корней по модулю три при вычислении η-спаривания. В [16] предложен метод ускорения финального экспоненцирования при вычислении η-спаривания. Все эти алгоритмы реализованы в арифметике поля $GF(3^{6n})$. В [4] дано обобщение ДЛК-алгоритма на гиперэллиптические кривые C_b. Для реализации этого обобщенного алгоритма используются поля $GF(p^{2np})$ и подполя $GF(p^n)$ и $GF(p^{2n})$. Для случая $p = 3$ это обобщение ДЛК-алгоритма сделано в [6,8–10]. Можно показать (см. [4]), что увеличение p влечет уменьшение сложности схемной реализации умножения в поле $GF(p^{2pn})$ (при условии, что n изменятся так, что порядок поля существенно не меняется). В настоящей статье мы рассматриваем схемную реализацию арифметики в $GF(7)$, $GF(7^2)$, $GF(7^n)$, $GF(7^{7n})$, и $GF(7^{14n})$, оцениваем сложность и глубину соответствующих схем. Рассматриваются логические схемы из двухвходовых булевых элементов, реализующих двухместные булевы функции (см., например, [23]). Под сложностью схемы понимается количество составляющих схему функциональных элементов, что по существу совпадает с понятием битовой сложности. Глубина схемы есть максимальное число элементов в любой цепи, соединяющей входы схемы с её выходами. Результаты могут быть применены при реализации основанных на спаривании алгоритмов, упомянутых выше. В частности, можно показать, что с увеличением p уменьшается схемная сложность ДЛК-алгоритма (при сохранении того же уровня безопасности), что согласуется с идеей из [17] выбирать для реализации ДЛК-алгоритма поля характеристики $p = 7$. Все вычисления, за исключением касающихся глубины схем, можно сформулировать в терминах программной реализации, что может найти применение в компьютерной алгебре. В статье используются следующие обозначения: $M(q)$, $M(GF(q))$ — схемная сложность умножения, $A(q)$, $A(GF(q))$ — схемная сложность сложения в конечном поле $GF(q)$, имеющем порядок q. Обычно $q = 7$ либо $q = 7^m$. $D(M(q))$, $D(M(GF(q)))$ — глубина схемы умноже-

*Работа поддержана АВЦП «Развитие научного потенциала высшей школы», проект 2.1.1/12136

ния, $D(A(q))$, $D(A(GF(q)))$ — глубина схемы сложения в поле $GF(q)$.

II. Схемы для арифметики по модулю 7

Лемма 2.1. Умножение в $GF(7)$ может быть выполнено схемой сложности 25 и глубины 5. □

Заметим, что умножение числа $(x_2x_1x_0)_2$ по модулю 7 на числа $4 = (100)_2$, $2 = (010)_2$ равносильно циклическим сдвигам битов x_i, умножение на $1 = (001)_2$ — это тождественное преобразование, умножение на числа $3 = (011)_2 = -4$, $5 = (101)_2 = -2$, $6 = (110)_2 = -1$ делается точно также, но у результата меняется знак на противоположный, что равносильно прибавлению по модулю два ко всем битам результата знакового бита σ. Очевидно, этот бит можно вычислить по формуле $m(y_2, y_1, y_0) = (y_0 + y_1)(y_0 + y_2) + y_0$. Умножение на числа $(000)_2$ и $(111)_2$ даёт в результате $(000)_2$. Рассмотрим линейный оператор $u_1 = y_0 \oplus y_1 \oplus 1$, $u_0 = y_0 \oplus y_2 \oplus 1$. Очевидно, он принимает значение 11 на противоположных наборах 000, 111, значение 10 на противоположных наборах 011, 100, значение 01 на противоположных наборах 010, 101, значение 00 на противоположных наборах 001, 110. Рассмотрим оператор

$$d_2 = \neg u_1 \& \neg u_0,\ d_1 = u_1 \& \neg u_0,\ d_0 = \neg u_1 \& u_0.$$

На наборах 000, 111 он принимает значение 000, на наборах 100, 011 — значение 010, на наборах 010, 101 — значение 001, на наборах 001, 110 — значение 100. Рассмотрим оператор

$$\begin{aligned} a_2 &= d_2x_2 \vee d_1x_0 \vee d_0x_1, \\ a_1 &= d_2x_1 \vee d_1x_2 \vee d_0x_0, \\ a_0 &= d_2x_0 \vee d_1x_1 \vee d_0x_2. \end{aligned}$$

На наборах $000x_2x_1x_0$, $111x_2x_1x_0$ он принимает значение 000, на наборах $001x_2x_1x_0$, $110x_2x_1x_0$ — значение $x_2x_1x_0$, на наборах $010x_2x_1x_0$, $101x_2x_1x_0$ — значение $x_1x_0x_2$, $(x_1x_0x_2)_2 = 2(x_2x_1x_0)_2 \bmod 7$, на наборах $100x_2x_1x_0$, $011x_2x_1x_0$ — значение $x_0x_2x_1$, $(x_0x_2x_1)_2 = 4(x_2x_1x_0)_2 \bmod 7$. Тогда умножение чисел $(x_2x_1x_0)_2$, $(y_2y_1y_0)_2$ по модулю 7 реализуется оператором

$$z_2 = a_2 \oplus m,\ z_1 = a_1 \oplus m, z_0 = a_0 \oplus m.$$

Действительно, если $(y_2y_1y_0)_2 = 0$, то $m = 0$ и он принимает значение $(000)_2 = (000)_2 \cdot (x_2x_1x_0)_2 \bmod 7$; если $(y_2y_1y_0)_2 = 7$, то $m = 1$ и он принимает значение $(111)_2 = 7 = 0 \bmod 7 = (111)_2 \cdot (x_2x_1x_0)_2 \bmod 7$; если $(y_2y_1y_0)_2 = a = 1, 2, 4$, то $m = 0$ и он принимает значение $a(x_2x_1x_0)_2 \bmod 7$; если $(y_2y_1y_0)_2 = a = 3, 5, 6$, то $-a \bmod 7 = b = 4, 2, 1$, $m = 1$ и он принимает значение $-b(x_2x_1x_0)_2 \bmod 7 = a(x_2x_1x_0)_2 \bmod 7$. Сложность схемы для оператора m, d_2, d_1, d_0 равна 7, глубина выходов d_i равна 2, глубина выхода m равна 3. Сложность схемы для оператора a_2, a_1, a_0 равна $15 + 7 = 22$, глубина равна 5. Сложность схемы для оператора z_2, z_1, z_0 равна $22 + 3 = 25$, глубина равна 6. Если в схеме для a_2, a_1, a_0 заменить $\vee$ на $\oplus$, то оператор z_2, z_1, z_0 можно реализовать формулами

$$\begin{aligned} z_2 &= (d_2x_2 \oplus d_1x_0) \oplus (d_0x_1 \oplus m), \\ *z_1 &= (d_2x_1 \oplus d_1x_2) \oplus (d_0x_0 \oplus m), \\ *z_0 &= (d_2x_0 \oplus d_1x_1) \oplus (d_0x_2 \oplus m) \end{aligned} \qquad (2.1)$$

с той же сложностью 25 и глубиной 5. Отождествим набор $(111)_2$ с набором $(000)_2$, так как $7 = 0 \pmod 7$.

Лемма 2.2. Сложение в $GF(7)$ может быть выполнено схемой сложности 17 и глубины 8. □

Доказательство. Действительно, складываем два трехзначных двоичных числа при помощи схемы, построенной по формулам (2.1) со сложностью 12 и глубиной 7, получаем сумму $(\sigma, \varepsilon_2, \varepsilon_1, \varepsilon_0)_2$. Приведение по модулю

$$\begin{aligned} &(\sigma, \varepsilon_2, \varepsilon_1, \varepsilon_0)_2 = \\ &\quad = 2^3\sigma + (\varepsilon_2, \varepsilon_1, \varepsilon_0)_2 = (\varepsilon_2, \varepsilon_1, \varepsilon_0)_2 + \sigma = \\ &\qquad\qquad = (z_2z_1z_0)_2 \pmod 7 \end{aligned}$$

по формулам (2.1) имеет сложность 5 и глубину 3, так как при прибавлении однобитового числа формулы (2.1) приобретают вид

$$\begin{aligned} z_1 = x_1 + y_1, \quad z_2 = x_2 + (x_1y_1), \\ z_3 = x_3 + x_2(x_1y_1) \pmod 2. \end{aligned}$$

Таким образом, схема сложения в $GF(7)$ имеет сложность 17 и глубину 8. Если подсхему прибавления однобитового числа построить по формулам:

$$\begin{aligned} z_1 = x_1 + y_1, \quad z_2 = x_2 + (x_1y_1), \\ z_3 = x_3 + (x_2x_1)y_1 \pmod 2, \end{aligned}$$

немного изменив порядок действий, то сложность подсхемы будет 6, но глубина основной схемы увеличится лишь на 2, а не на 3, так как вычисление x_2x_1 можно произвести заранее. Эта схема сложения в $GF(7)$ имеет сложность 18 и глубину 7. Если схему сложения (2.1) переписать в виде

$$\begin{aligned} z_1 &= x_1 + y_1, \\ z_2 &= (x_2 + y_2) + (x_1y_1), \\ z_3 &= ((x_3 + y_3) + x_2y_2) + ((x_2 + y_2)(x_1y_1)), \\ z_4 &= ((x_3y_3) + (x_3 + y_3)(x_2y_2)) + \\ &\quad + (x_3 + y_3)((x_2 + y_2)(x_1y_1)), \end{aligned}$$

то полученная схема будет иметь сложность 14 и глубину 4. Таким образом, схема сложения в $GF(7)$ будет иметь сложность 20 и глубину 6.

Далее можно показать, что справедливы следующие утверждения.

Лемма 2.3. Существует схема для сложения сложности 18 и глубины 7 и схема для сложения сложности 20 и глубины 6. □

Лемма 2.4. Сложение в $GF(7)$ может быть выполнено схемой сложности 21 и глубины 4. □

Для умножения в поле $GF(7^2)$ можно использовать две схемы. Стандартная схема, основанная на формуле

$$(a+b\sigma)(c+d\sigma) = (ac-bd)+\sigma(ad+bc),$$

имеет сложность $4M(7)+2A(7) = 134$ и глубину $D(M(7))+D(A(7)) = 12$. Существует схема сложности 142 и глубины 9 и сложности 136 и глубины 11. Схема в нормальном базисе, основанная на формуле

$$((a+b)(c+d)-2bd)\gamma + ((a+b)(c+d)-2ac)\gamma^p,$$

имеет сложность $3M(7)+4A(7) = 146$ и глубину $D(M(7))+2D(A(7))$. Эта схема хуже. Но для больших p она имеет меньшую сложность, чем стандартная.

III. Умножение в поле $GF(7^{2n})$ над полем $GF(7^2)$

Умножение многочленов 23-й и 24-й степени. Для вычисления ДПФ 48 порядка используем стандартную конструкцию, описанную например, в [20].

Пусть $\varepsilon = \omega_3 \neq 1$, $\varepsilon^3 = 1$. В поле $GF(7)$ $\varepsilon = 2$, $\varepsilon^2 = 4$.

Тогда F_3 определяется равенствами

$$y_0 = x_0 + x_1 + x_2,$$
$$y_1 = x_0 + \varepsilon x_1 + \varepsilon^2 x_2,$$
$$y_2 = x_0 + \varepsilon^2 x_1 + \varepsilon^4 x_2,$$

и вычисляется формулами

$$z_1 = x_1 + x_2, \quad z_2 = x_1 - x_2, \quad z_3 = \varepsilon z_2,$$
$$z_4 = z_3 - x_2, \quad z_5 = z_1 + z_4,$$
$$y_0 = x_0 + z_1, \quad y_1 = x_0 + z_4, \quad y_2 = x_0 - z_5.$$

Далее будет удобно применять схему F_3, приспособленную не к числам x_i, а к произвольным векторам. Эта схема такова:

$$z_1 = x_1+x_2, \quad z_2 = x_1-x_2, \quad z_3 = \left(\frac{\varepsilon+\varepsilon^2}{2}-1\right)z_1,$$
$$z_4 = \frac{\varepsilon-\varepsilon^2}{2}z_2, \quad y_0 = x_0+z_1,$$
$$z_5 = y_0+z_3, \quad y_1 = z_5+z_4, \quad y_2 = z_5-z_4.$$

В поле $GF(7)$ имеем: $\frac{\varepsilon-\varepsilon^2}{2} = -1$, $\frac{\varepsilon+\varepsilon^2}{2}-1 = 2$. Поэтому в этой схеме $z_3 = 2z_1$, $z_4 = -z_2$. Она удобна для векторизации, то есть для применения к векторам x_i, которые сами являются результатами применения одного линейного преобразования $x_i = F(X_i)$. Тогда для вычисления F_3 в указанной схеме можно использовать новые операции:

$$Z_1 = X_1 + X_2,$$
$$Z_2 = X_1 - X_2,$$
$$y_0 = x_0 + z_1 = F(X_0 + Z_1),$$
$$z_3 = 2z_1 = 2F(Z_1),$$
$$z_4 = -z_2 = -F(Z_2),$$

оставив остальные без изменения. Если первоначальный вариант схемы при применении к векторам $x_i = F(X_i)$ требует трехкратного вычисления преобразования F, 6 векторных сложений и 2 скалярных умножения, то указанный вариант требует те же 6 векторных сложений, но не требует скалярных умножений; вместо трехкратного вычисления F оно вычисляется один раз в чистом виде и два раза — умноженным на скаляры 2, -1. Это понадобится далее.

Для вычисления ДПФ порядка 16 достаточно 17 скалярных умножений и 64 сложений. В поле $GF(7^2)$ умножение на w^4 «бесплатно» (то есть имеет нулевую сложность), поэтому пропадает $1+2+4$ скалярных умножений и остается только 10.

Для вычисления ДПФ порядка 48 в поле $GF(7^2)$ применяем теорему Гуда–Томаса (см. [20]) и представляем $F_{48}(X)$ в виде

$$F_{48} = F_3(F_{16}(X_1), F_{16}(X_2), F_{16}(X_3)),$$

где X_i — вектора, составленные из компонент вектора X по следующему правилу:

$$X_1 = (x_0,\ x_3,\ \ldots,\ x_{45}),$$
$$X_2 = (x_{16},\ x_{19},\ \ldots,\ x_{46},\ x_1,\ x_4,\ \ldots,\ x_{12}),$$
$$X_3 = (x_{32},\ x_{35},\ \ldots,\ x_{47},\ x_2,\ x_5,\ \ldots,\ x_{29}),$$

а F_3 — это векторизация ДПФ 3-го порядка, рассмотренная выше. Так как для его вычисления используется 6 векторных сложений (то есть 96 обычных) и вычисляются преобразования F_{16}, $2F_{16}$, $-F_{16}$, то дополнительно нужно 192 сложения и 30 скалярных умножений. Окончательно необходимо провести 288 сложений и 30 скалярных умножений. Для умножения многочленов степени 23 достаточно сделать 48 умножений и три преобразования Фурье F_{48}. Значит, кроме умножений, достаточно не более 864 сложений и 90 скалярных умножений. Отметим, что в первых двух ДПФ экономится по 48 сложений в каждом. Действительно, в векторе коэффициентов многочлена только первые 24 коэффициента могут быть

отличны от нуля, поэтому в векторе X_1 последние 8 коэффициентов нулевые, в векторе X_2 имеется 8 подряд идущих (в циклическом смысле) нулевых коэффициентов и в векторе X_3 тоже. Деление многочленов 15 степени с такими наборами коэффициентов на двучлены $x^8 \pm 1$ с остатком выполняется бесплатно: для нахождения остатка нужен только сдвиг коэффициентов, возможно, со сменой знака у некоторых из них. Глубина F_{48} равна $8D(A(7))$. Поэтому сложность циклической свёртки (см. [20]) многочленов 23-й степени равна

$$858A(GF(7^2)) + 48M(GF(7^2)) = 35\,604.$$

Глубина равна $16D(A(7)) + D(M(GF(7^2)))$.

Можно проверить, что сложность и глубина циклической свертки многочленов 24-й степени оценивается так же. Но для умножения многочленов 24-й степени, кроме вычисления этой свертки, нужно еще одно умножение и одно вычитание в $GF(7^2)$.

Умножение многочленов 27-й, 31-й и 49-й степени. Можно показать, что сложность умножения многочленов степени 27 равна

$$874A(GF(7^2)) + 62M(GF(7^2)) = 38\,024,$$

а глубина равна $17D(A(7)) + D(M(GF(7^2)))$.

Сложность умножения многочленов степени 31 равна

$$\begin{aligned}890A(GF(7^2)) + 48M(GF(7^2)) + 15A(GF(7^2)) + \\ + 44M(GF(7^2)) + 99A(GF(7^2)) = \\ = 1004A(GF(7^2)) + 92M(GF(7^2)) = 46\,464,\end{aligned}$$

а глубина равна $18D(A(7)) + D(M(7)) = 131$.

Сложность умножения многочленов степени 49 равна 90 112, а глубина равна $20D(A(7)) + D(M(7))$.

Замечание. Можно показать, что даже для малых степеней $n \leqslant 31$ использование ДПФ имеет преимущество перед школьным методом, методом Карацубы [18, 22] и методом Тоома [19, 22].

IV. Схемы для умножения в поле $GF(7^{14n})$ над полем $GF(7^{2n})$

Умножение двух многочленов шестой степени. Построим схему для умножения двух многочленов шестой степени $f_0 + f_1X + \cdots + f_6X^6$, $g_0 + g_1X + \cdots + g_6X^6$ с коэффициентами из $GF(7^{2n})$ методом Тоома [19, 22]. Выберем узлы интерполяции: $0, \pm1, \pm2, \pm3, \pm\sigma, \pm2\sigma, \pm3\sigma$. Здесь σ есть «мнимая единица» в $GF(7^2)$, представленном в виде квадратичного расширения $GF(7)$, так что $\sigma^2 = -1 \bmod 7$. Значения в узлах многочлена f представим следующим образом:

$$\begin{aligned}
f(0) &= f_0,\\
f(1) &= ((f_0 + {}_1f_4) + {}_3(f_2 + {}_2f_6)) + \\
&\quad + {}_6((f_1 + {}_4f_5) + {}_5f_3),\\
f(-1) &= ((f_0 + f_4) + (f_2 + f_6)) - \\
&\quad - {}_7((f_1 + f_5) + f_3),\\
f(\sigma) &= ((f_0 + f_4) - {}_8(f_2 + f_6)) + \\
&\quad + {}_{10}((f_1 + f_5) - {}_9f_3)\sigma,\\
f(-\sigma) &= ((f_0 + f_4) - (f_2 + f_6)) - \\
&\quad - {}_{11}((f_1 + f_5) - f_3)\sigma,\\
f(2) &= ((f_0 + {}_{12}2f_4) + {}_{14}(4f_2 + {}_{13}f_6)) + \\
&\quad + {}_{17}((2f_1 + {}_{15}4f_5) + {}_{16}f_3),\\
f(-2) &= ((f_0 + 2f_4) + (4f_2 + f_6)) - \\
&\quad - {}_{18}((2f_1 + 4f_5) + f_3),\\
f(2\sigma) &= ((f_0 + 2f_4) - {}_{19}(4f_2 + f_6)) + \\
&\quad + {}_{21}((2f_1 + 4f_5) - {}_{20}f_3)\sigma,\\
f(-2\sigma) &= ((f_0 + 2f_4) - (4f_2 + f_6)) - \\
&\quad - {}_{22}((2f_1 + 4f_5) - f_3)\sigma,\\
f(3) = f(-4) &= ((f_0 + {}_{23}4f_4) + {}_{25}(2f_2 + {}_{24}f_6)) + \\
&\quad + {}_{28}((4f_1 + {}_{26}2f_5) - {}_{27}f_3),\\
f(-3) = f(4) &= ((f_0 + 4f_4) + (2f_2 + f_6)) - \\
&\quad - {}_{29}((4f_1 + 2f_5) - f_3),\\
f(3\sigma) = f(-4\sigma) &= ((f_0 + 4f_4) - {}_{30}(2f_2 + f_6)) + \\
&\quad + {}_{32}((4f_1 + 2f_5) + {}_{31}f_3)\sigma,\\
f(-3\sigma) = f(4\sigma) &= ((f_0 + 4f_4) - (2f_2 + f_6)) - \\
&\quad - {}_{33}((4f_1 + 2f_5) + f_3)\sigma.
\end{aligned}$$

Сложность этих вычислений, учитывая указанные скобками разбиения (порядок действий при конструировании схемы занумерован индексами при арифметических операциях), равна $33A(GF(7^{2n})) = 66nA(7)$. В этом равенстве учтено, что $A(GF(7^{2n})) = 2nA(7)$. Глубина этой схемы равна $3D(A(7))$. Те же вычисления необходимо проделать и для многочлена g. Суммарная сложность их равна $132nA(7)$. Найдём значения многочлена $h(X) = f(X) \cdot g(X)$, $h(X) = h_0 + h_1X + \cdots + h_{12}X^{12}$ в выбранных узлах a_j, $j = 0, \ldots, 12$. Сложность вычисления $h_j = h(a_j) = f(a_j)g(a_j)$, $j = 0, \ldots 12$, при $p = 7$ составляет $13(3M(GF(7^n)) + 4A(GF(7^n))) = 39M(GF(7^n)) + 52nA(7)$. Здесь использован нормальный базис с оценками сложности арифметики в нём из леммы 2.4, элемент из $GF(7^{2n})$ представлен в виде многочлена степени $n-1$ над $GF(7^2)$. Оценим сложность схемы для интерполяции. Многочлен $h(X)$, согласно методу Лагранжа, представляется в виде

суммы фундаментальных многочленов. Фундаментальные многочлены (по (mod 7)) после некоторой перестановки есть:

$$
\begin{aligned}
&-(X^4-4)(X^4-2)(X^4-1)h(0) = \\
&\qquad = -(X^8+X^4+1)(X^4-1)h(0),\\
&-4X(X^4-4)(X^4-2)(X^2-1)(X+\sigma)h(\sigma),\\
&-4X(X^4-4)(X^4-2)(X^2-1)(X-\sigma)h(-\sigma),\\
&-4X(X^8+X^4+1)(X^2+1)(X+1)h(1),\\
&-4X(X^8+X^4+1)(X^2+1)(X-1)h(-1),\\
&-4X(X^4-1)(X^4-4)(X^2+4)(X+2)h(2),\\
&-4X(X^4-1)(X^4-4)(X^2+4)(X-2)h(-2),\\
&-4X(X^4-1)(X^4-4)(X^2-4)(X+2\sigma)h(2\sigma),\\
&-4X(X^4-1)(X^4-4)(X^2-4)(X-2\sigma)h(-2\sigma),\\
&-4X(X^4-1)(X^4-2)(X^2-2)(X+4\sigma)h(3\sigma),\\
&-4X(X^4-1)(X^4-2)(X^2-2)(X-4\sigma)h(-3\sigma),\\
&-4X(X^4-1)(X^4-2)(X^2+2)(X+4)h(-3),\\
&-4X(X^4-1)(X^4-2)(X^2+2)(X-4)h(3),
\end{aligned}
$$

так как для получения k-го фундаментального многочлена нужно из произведения

$$
\begin{aligned}
&X\times(X-1)\times(X+1)\times(X-2)\times(X+2)\times\\
&\quad\times(X-3)\times(X+3)\times(X-\sigma)\times(X+\sigma)\times\\
&\quad\times(X-2\sigma)\times(X+2\sigma)\times(X-3\sigma)\times(X+3\sigma)
\end{aligned}
$$

удалить $(X-k)$, $k=\pm1,\pm2,\pm3,\pm\sigma,\pm2\sigma,\pm3\sigma$, перемножить оставшиеся скобки и результат домножить на $h(k)$ и разделить на значение от k полученного многочлена, которое равно -2, за исключением случая $k=0$, где оно равно -1. Пусть $d_0=-h(0)$, $d_1=-4h(1)$, $d_2=-4h(-1)$, …, $d_{11}=-4h(3\sigma)$, $d_{12}=-4h(-3\sigma)$. Вычисление коэффициентов многочлена $h(X)$ по его значениям в 13 узлах можно представить в следующем виде:

$$
\begin{aligned}
h(X) = (X^8+{}^1X^4+{}^11)&[d_0(X^4-1)+\\
&+{}^1X(X^2-1)(d_7(X+\sigma)+{}^2d_8(X-\sigma))+\\
&+{}^4X(X^2+1)(d_1(X+1)+{}^2d_2(X-1))]+\\
+{}^{12}X(X^4-{}^41)&[(X^4-2)((X^2-2)(d_{11}(X+4\sigma)+\\
+{}^2d_{12}(X-4\sigma))&+{}^4(X^2+2)(d_5(X+4)+{}^2d_6(X-4)))+\\
+{}^8(X^4-4)&((X^2+4)(d_4(X-2)+{}^2d_3(X+2))+\\
&+{}^4(X^2-4)(d_9(X-2\sigma)+{}^2d_{10}(X+2\sigma)))].
\end{aligned}
$$

Индексы k сверху над каждой операцией указывают ее сложность в виде $kA(GF(7^{2n}))$. Отсутствие индекса означает, что сложность равна нулю. Поэтому сложность этих вычислений равна $A(GF(7^{2n}))[(2+2+4+1)+1+1)+12+4+{}+((2+2+4)\cdot2+8)]=2nA(7)\cdot51=102nA(7)$. Глубина этой схемы равна $6D(A(7))$. Суммируя полученные оценки, находим, что сложность умножения многочленов степени $\leqslant 6$ над $GF(7^{2n})$ есть $L=132nA(7)+13M(GF(7^{2n}))+102nA(7)=13M(GF(7^{2n}))+234nA(7)$. Глубина схемы равна $9D(A(7))+D(M(GF(7^{2n})))$. Приведение по модулю X^7-X+2 многочлена двенадцатой степени $d_0+d_1X+\cdots+d_{12}X^{12}=c_0+c_1X+\cdots+c_6X^6 \pmod{X^7-X+2}$ выполняется по формулам: $c_6=d_6+d_{12}$, $c_5=d_5-2d_{12}+d_{11}$, $c_4=d_4-2d_{11}+d_{10}$, …, $c_1=d_1-2d_8+d_7$, $c_0=d_0-2d_7$, которые содержат 12 сложений-вычитаний в $GF(7^{2n})$) и 6 удвоений (удвоения бесплатны при схемной реализации). Таким образом, приведение по модулю X^7-X+2 имеет сложность $12A(GF(7^{2n}))=24nA(7)$ и глубину $2D(A(7))$, и тогда, учитывая полученную оценку сложности умножения многочленов шестой степени с коэффициентами из $GF(7^{2n})$, имеем

$$M(GF(7^{14n})\leqslant 13M(GF(7^{2n}))+258nA(7).$$

Для глубины справедливо неравенство

$$D(M(GF(7^{14n})))\leqslant 11D(A(7))+D(M(GF(7^{2n}))).$$

Умножение многочленов степени 6 на многочлены степени 3. В алгоритме ДЛК на самом деле используется не умножение произвольных многочленов степени $p-1$ над полем $GF(p^{2n})$, а многочлена степени $p-1$ на многочлен степени $(p+1)/2$, у которого старший коэффициент равен 1. Представляя последний в виде суммы $X^{(p+1)/2}$ и многочлена степени не выше $(p-1)/2$, получаем, что такое умножение сводится к умножению многочлена степени $p-1$ на многочлен вдвое меньшей степени и $p-1$ сложениям в поле $GF(p^{2n})$. При $p=7$ умножается многочлен степени 6 на многочлен степени 3. Можно показать, что сложность такого умножения не превосходит

$$10M(GF(7^{2n}))+140nA(7),$$

а глубина соответствующей схемы не превосходит

$$10D(A(7))+D(M(GF(7^{2n}))).$$

Литература

1. *Blake I., Seroussi G., Smart N.* Elliptic curves in cryptography. – Cambridge: Cambridge University Press, 1999.

2. *Blake I.,Seroussi G., Smart N.* Advances in elliptic curve cryptograhy. – Cambridge: Cambridge University Press, 2005.

3. *Болотов А.А., Гашков С.Б., Фролов А.Б., Часовских А.А.* Элементарное введение в эллиптическую криптографию. Алгебраические и алгоритмические основы. – М.: КомКнига, 2006.

4. *Болотов А.А., Гашков С.Б., Фролов А.Б., Часовских А.А.* Элементарное введение в эллиптическую криптографию. Протоколы криптографии на эллиптических кривых. – М.: КомКнига, 2006.

5. *Barreto P.S.L.M., Kim H.Y., Lynn B., Scott M.* Efficient algorithms for pairing-based cryptosystems // Crypto-2002, LNCS 2442, 2002. – P. 354–368.

6. *Scott M. and Barreto P.S.M.L.* Compressed pairing // CRYPTO-2004, LNCS 3152(2004), P. 140–156.

7. *Barreto P.S.M.L., Galbraith S., O hEigeartaigh C. and Scott M.* Efficient pairing computation on supersingular abelian varieties // Cryptology ePrint Archive, Report 2004/375. http://eprint.iacr.org/2004/375

8. *Kerins T., Marname W.P., Popovici E.M., and Barreto P.S.L.M.* Efficient hardware for Tate pairing calculation in characteristic three // CHES-2005.

9. *Page D., Smart N.P.* Hardware implementation of finite fields of characteristic three // CHES-2002, LNCS, 2002.

10. *Granger R., Page D., Stam M.* Hardware and software normal basis arithmetic for pairing based cryptography in characteristic three // IEEE Trans. on Comp. – 2005. – V. 54, N 7. – P. 852–860.

11. *Bailey D.V., Paar C.* Efficient arithmetic in finite field extensions with application in elliptic curve cryptography // J. of Cryptology. – 2001. – 14:3. – P. 156–173.

12. *Duursma I. and Lee H.-S.* Tate pairing implementation for hyperelliptic curves $y^2 = x^p - x + d$ // Asiacrypt-2003, LNCS 2894, 2003. – P. 111–123.

13. *Duursma I. and Lee H.-S.* Tate pairing implementation for tripartite key agreement // Cryptology ePrint Archive, Report 2003/053. http://eprint.iacr.org/2003/053

14. *Kwon S.* Efficient Tate pairing computation for supersingular elliptic curves over binary fields // Cryptology ePrint Archive, Report 2004/303. http://eprint.iacr.org/2004/303

15. *Beuchat J-L., Shiraze M., Takagi T. and Okamoto E.* An algorithm for the η_T-pairing calculation in characteristic three and its hardwareimplementation // Cryptology ePrint Archive, Report 2006/327. http://eprint.iacr.org/2006/327

16. *Shiraze M., Takagi T. and Okamoto E.* Some efficient algorithms for the final exponentiation ofn η_T- pairing // Cryptology ePrint Archive, Report 2006/. http://eprint.iacr.org/2006/

17. *Eunjeong Lee, Huang-Sook Lee and Yoonjin Lee.* Fast computation of Tate pairing on general divisors for hyperelliptic curves of genus 3 // Cryptology ePrint Archive, Report 2006/125. http://eprint.iacr.org/2006/125

18. *Карацуба А.А., Офман Ю.П.* Умножение многозначных чисел на автоматах // Доклады АН СССР, 1962, – Т. 145(2). – С. 293–294.

19. *Тоом А.Л.* О сложности схемы из функциональных элементов, реализующей умножение целых чисел // Доклады АН СССР, 1963. – Т. 150. – С. 496–498.

20. *Ноден П., Китте К.* Алгебраическая алгоритмика. – М.: Мир, 1999.

21. *Болотов А.А., Гашков С.Б., Фролов А.Б., Часовских А.А.* Программные и схемные методы умножения многочленов для эллиптической криптографии // Известия РАН. Теория и системы управления. – 2000, № 5. – С. 66–75.

22. *Дональд Э. Кнут.* Искусство программирования. Том 2. Получисленные алгоритмы. Третье издание. – Изд. Вильямс. 2000.

23. *Лупанов О.Б.* Асимптотические оценки сложности управляющих систем. – М.: Изд-во Московского университета. 1984.

Поступила в редакцию 18.01.2011