УДК 512.624.9

Оптимальные нормальные базисы 2-го и 3-го типов в конечных полях характеристики семь

С. Б. Гашков, А. Б. Фролов*, С. А. Лукин

Рассмотрены оптимальные нормальные базисы 2-го и 3-го типов и их модификации для имплементации арифметических операций в конечных полях характеристики семь. Описаны представления элементов данных полей в базисах подобных типов: переставленном, приведенном (редуцированном), редундантном, а также полиномиальном. Представлены алгоритмы преобразования между указанными представлениями и алгоритмы умножения с использованием полиномиального базиса, возведения в степень, равной степени характеристики поля, обращения и возведения в произвольную степень.

Ключевые слова: конечное поле, полиномиальный и оптимальный нормальный базисы, преобразование базисов, характеристика поля, конечное поле характеристики семь, возведение в степень, умножение, обращение, гиперэллиптическая кривая, спаривание Тейта.

Введение

Известно, что в полиномиальном базисе $\{1, x, ..., x^{n-1}\}$ поля $GF(q^n)$ характеристики q быстро выполняется умножение, а в нормальном базисе $\{x, x^q, ..., x^{q^{n-1}}\}$ — возведение в степень q^j [1, 2]. В [3] были открыты оптимальные нормальные базисы (о.н.б.) с умножением квадратичной сложности. В [4] описаны алгоритмы преобразования между о.н.б. 2-го или 3-го типов [3] и полиномиальным базисом (п.б.) сложности $O(n\ln n)$, а также предложено комбинировать использование п.б. и о.н.б., при этом конвертировать операнды в п.б. для последующего умножения и в о.н.б. для последующего возведения в степень q^j. В [5 — 7] изложен ряд модификаций умножения в о.н.б. 2-го или 3-го типа с использованием алгоритма умножения в кольце $GF(2)[X]$ с последующим конвертированием результата в о.н.б. 2-го типа. В [8] идея сочетания п.б. и о.н.б. развивается на основе использования приведенного о.н.б. 2-го или 3-го типов поля малой характеристики и описаны алгоритмы преобразований упомянутых выше базисов с оценками сложности, алгоритмы умножения и возведения в степень q^j и алгоритм обращения в приведенном о.н.б. в полях характеристики три. В настоящей работе рассмотрено преобразование базисов и реализация арифметических операций на их основе в полях характеристики семь. С использованием подобных операций возможна эффективная реализация операций в расширениях $GF(q^{2n})$ и $GF(q^{14n})$ поля $GF(q^n)$, в которых реализуются операции над дивизорами гиперэллиптических кривых, составляющие алгоритмическую основу операции спаривания, применяемой в криптографических протоколах согласования ключей, цифровой подписи и др. [9 — 11].

Преобразование базисов

Пусть $p = 2n + 1$ — простое число, p делит $q^{2n} - 1$. Возьмем $\alpha \in GF(q^{2n})$ такое, что $\alpha \neq 1$, $\alpha^p = 1$. Пусть q является примитивным корнем по модулю p из 1, т. е.

* abfrolov@mail.ru

множество всех степеней числа q по модулю p образует группу Z_p^* или же это множество является множеством всех квадратичных вычетов по модулю p. В первом случае q является квадратичным невычетом по модулю p, во втором случае $q^n \bmod p = 1$ и при $k < n$ и число q есть квадратичный вычет, а –1 является квадратичным невычетом [2].

Рассмотрим последовательность

$$\beta_i = \alpha^i + \alpha^{-i} = \alpha^i + \frac{1}{\alpha^i} \in GF(q^{2n})$$

для всех целых i (в случае $q^n \equiv 1(\bmod p)$, $\beta_i \in GF(q^n)$). Очевидно, что $\beta_i = \beta_{-i}$, $\beta_0 \in GF(q)$.

Рассмотрим базис $\{\beta_1, ..., \beta_n\} \subseteq GF(q^n)$. Он получается перестановкой π:

$$\pi(j) = \begin{cases} q^j \bmod p, \text{ если } q^j \bmod p \le n; \\ p - q^j \bmod p, \text{ если } q^j \bmod p > n. \end{cases}$$

из о.н.б. $\{\xi_1, ..., \xi_n\}$ где $\xi_i = \beta^{q^{i-1}}$, $i = 1, ..., n$ и называется переставленным о.н.б.: для $j = 0, ..., n-1$: $\beta_j = \xi_{\pi(j)}$. Обратное преобразование соответствует обратной перестановке π^{-1}: $\xi_j = \beta_{\pi^{-1}(j)}$, $j = 1, ..., n$. Если q — квадратичный невычет, то базис $\{\xi_1, ..., \xi_n\}$ называется о.н.б. 2-го типа, иначе он называется о.н.б. 3-го типа [2].

Можно проверить, что

$$\sum_{i=1}^{n} \beta_i = \sum_{i=1}^{n} (\alpha^i + \alpha^{-i}) = \sum_{i=1}^{2n} \alpha^i = -1 = \frac{q-1}{2}\beta_0,$$

поскольку

$$\alpha^{-i} = \alpha^{p-i} = \alpha^{2n+1-i}, \quad \sum_{i=0}^{2n} \alpha^i = \sum_{i=0}^{p-1} \alpha^i = \frac{\alpha^p - 1}{\alpha - 1} = 0.$$

Используем также приведенный (редуцированный) о.н.б. 2-го или 3-го типов $\{\beta_0, ..., \beta_{n-1}\}$, $\beta_0 = 2 \in GF(q)$, а также редундантный (избыточный) о.н.б. 2-го или 3-го типов $\{\beta_0, ..., \beta_{n-1}, \beta_n\}$. Преобразование из приведенного $\{\beta_0, ..., \beta_{n-1}\}$ в переставленный о.н.б. $\{\beta_1, ..., \beta_{n-1}, \beta_n\}$ осуществляется с учетом представления β_0 в виде $\beta_0 = -2\sum_{i=1}^{n} \beta_i$: для $\mathbf{x} \in GF(7^n)$, $\mathbf{x} = x_0\beta_0 + x_1\beta_1 + ... + x_{n-1}\beta_{n-1}$ в приведенном о.н.б. получим представление в переставленном о.н.б.:

$$\begin{aligned} \mathbf{x} &= x_0(-2)\sum_{i=1}^{n} \beta_i + x_1\beta_1 + \cdots + x_{n-1}\beta_{n-1} = \\ &= y_1\beta_1 + \ldots + y_{n-1}\beta_{n-1} + y_n\beta_n = \\ &= (x_1 - 2x_0)\beta_1 + \cdots + (x_{n-1} - 2x_0)\beta_{n-1} - 2x_0\beta_n. \end{aligned} \quad (1)$$

Обратное преобразование осуществляется с учетом представления

β_n в виде $\beta_n = \frac{q-1}{2}\beta_0 - \sum_{i=1}^{n-1}(\beta_i)$:

$$\begin{aligned} \mathbf{x} &= y_1\beta_1 + \ldots + y_{n-1}\beta_{n-1} + y_n\beta_n = \\ &= y_1\beta_1 + \cdots + y_{n-1}\beta_{n-1} + y_n\left(\frac{q-1}{2}\beta_0 - \sum_{i=1}^{n-1}\beta_i\right) = \\ &= \frac{q-1}{2}y_n\beta_0 + (y_1 - y_n)\beta_1 + \ldots + (y_{n-1} - y_n)\beta_{n-1} = \\ &= x_0\beta_0 + x_1\beta_1 + \cdots + x_{n-1}\beta_{n-1}. \end{aligned} \quad (2)$$

Преобразование из редундантного в приведенный о.н.б. проводится на основе представления β_n в виде:

$$\beta_n = \frac{q-1}{2}\beta_0 - \sum_{i=1}^{n-1}\beta_i : \text{для } \mathbf{x} \in GF(7^n) \text{ получим}$$

$$\begin{aligned} \mathbf{z} &= z_0\beta_0 + z_1\beta_1 + z_2\beta_2 + \ldots + z_{n-1}\beta_{n-1} + z_n\beta_n = \\ &= z_0\beta_0 + z_1\beta_1 + z_2\beta_2 + \ldots + z_{n-1}\beta_{n-1} + \left(\frac{q-1}{2}z_n\beta_0 - \sum_{i=1}^{n-1}\beta_i\right) = \\ &= \left(z_0 + \frac{q-1}{2}z_n\right)\beta_0 + (z_1 - z_n)\beta_1 + \\ &+ (z_2 - z_n)\beta_2 + \ldots + (z_{n-1} - z_n)\beta_{n-1} = \\ &= x_0\beta_0 + x_1\beta_1 + \cdots + x_{n-1}\beta_{n-1}. \end{aligned}$$

С другой стороны, преобразование из редундантного базиса в переставленный о.н.б. осуществляется так:

$$\begin{aligned} \mathbf{z} &= z_0\beta_0 + z_1\beta_1 + z_2\beta_2 + \ldots + z_{n-1}\beta_{n-1} + z_n\beta_n = \\ &= z_0(-2\sum_{i=1}^{n}\beta_i) + z_1\beta_1 + z_2\beta_2 + \ldots + z_{n-1}\beta_{n-1} + z_n\beta_n = \\ &= (z_1 - 2z_0)\beta_1 + (z_2 - 2z_0)\beta_2 + \ldots + (z_{n-1} - 2z_0)\beta_{n-1} + \\ &+ (z_n - 2z_0)\beta_n = y_1\beta_1 + \ldots + y_{n-1}\beta_{n-1} + y_n\beta_n. \end{aligned}$$

Преобразование представления элемента $\mathbf{x} \in GF(7^n)$ из приведенного о.н.б. $\{\beta_0, \beta_1, ..., \beta_{n-1}\}$ в полиномиальный базис $\{\beta^0, ..., \beta^{n-1}\}$, $\beta^0 = 1$, $\beta = \beta_1 = \alpha + \alpha^{-1} \in GF(q^n)$ обозначим $F(\mathbf{x})$ а обратное преобразование — $F^{-1}(\mathbf{x})$.

Для описания и обоснования этих преобразований в поле характеристики $q = 7$ потребуется

Лемма 1. *Справедливы тождества*

$$\beta_{7k} = \beta^{7^k}, \ \beta_i\beta_j = \beta_{i+j} + \beta_{i-j}. \quad (3)$$

Действительно,

$$\begin{aligned} \beta_i\beta_j &= (\alpha^i + \alpha^{-i})(\alpha^j + \alpha^{-j}) = \\ &= (\alpha^{i+j} + \alpha^{-(i+j)}) + (\alpha^{i-j} + \alpha^{-(i-j)}) = \\ &= \beta_{i+j} + \beta_{i-j}; \end{aligned}$$

$$\beta_{7^k} = (\alpha^{7^k} + \alpha^{-7^k}) = (\alpha + \alpha^{-1})^{7^k} = \beta_1^{7^k} = \beta^{7^k}, \text{ где } \beta = \beta_1$$

Следствие 1. *Справедливы тождества*

$$\begin{aligned} &\beta_{7^k} = \beta^{7^k}; \ \beta_{2\times 7^k} = \beta^{2\times 7^k} - 2; \ \beta_{3\times 7^k} = \beta^{3\times 7^k} - 3\beta^{7^k}; \\ &\beta_{4\times 7^k} = \beta^{4\times 7^k} - 4\beta^{2\times 7^k} + 2; \ \beta_{5\times 7^k} = \beta^{5\times 7^k} + 2\beta^{3\times 7^k} - 2\beta^{7^k}; \\ &\beta_{6\times 7^k} = \beta^{6\times 7^k} + \beta^{4\times 7^k} + 2\beta^{2\times 7^k} - 2, \end{aligned} \quad (4)$$

и для всех i, $0 < i < 7^k$ *справедливы тождества*

$$\begin{aligned}
&\beta_{7^k+i} = \beta^{7^k}\beta_i - \beta_{7^k-i};\ \beta_{2\times7^k+i} = \beta^{2\times7^k}\beta_i - \beta^{7^k}\beta_{7^k-i} - \beta_i;\\
&\beta_{3\times7^k+i} = \beta^{3\times7^k}\beta_i - \beta^{2\times7^k}\beta_{7^k-i} - 2\beta^{7^k}\beta_i + \beta_{7^k-i};\\
&\beta_{4\times7^k+i} = \beta^{4\times7^k}\beta_i - \beta^{3\times7^k}\beta_{7^k-i} + 4\beta^{2\times7^k}\beta_i + 2\beta^{7^k}\beta_{7^k-i} + \beta_i;\\
&\beta_{5\times7^k+i} = \beta^{5\times7^k}\beta_i - \beta^{4\times7^k}\beta_{7^k-i} - 4\beta^{3\times7^k}\beta_i -\\
&-4\beta^{2\times7^k}\beta_{7^k-i} - 4\beta^{7^k}\beta_i - \beta_{7^k-i};\\
&\beta_{6\times7^k+i} = \beta^{6\times7^k}\beta_i - \beta^{5\times7^k}\beta_{7^k-i} + \cdots\\
&\cdots + 2\beta^{4\times7^k}\beta_i + 4\beta^{3\times7^k}\beta_{7^k-i} - \beta^{2\times7^k}\beta_i + 4\beta^{7^k}\beta_{7^k-i} - \beta_i.
\end{aligned} \tag{5}$$

Эти тождества выводятся непосредственно применением тождеств (3).

Следствие 2. *Справедливы тождества, являющиеся обращениями тождеств (4):*

$$\begin{aligned}
&\beta^{7^k} = \beta_{7^k};\ \beta^{2\times7^k} = \beta_{2\times7^k} + \beta_0;\ \beta^{3\times7^k} = \beta_{3\times7^k} + 3\beta_{7^k};\\
&\beta^{4\times7^k} = \beta_{4\times7^k} + 4\beta_{2\times7^k} - 4\beta_0;\ \beta^{4\times7^k} = \beta_{4\times7^k} + 4\beta_{2\times7^k} - 1;\\
&\beta^{5\times7^k} = \beta_{5\times7^k} - 2\beta_{3\times7^k} - 4\beta_{7^k};\\
&\beta^{6\times7^k} = \beta_{6\times7^k} - \beta_{4\times7^k} + \beta_{2\times7^k} - 1.
\end{aligned} \tag{6}$$

и для всех i, $0 < i < 7^k$ *справедливы тождества, получающиеся обращением тождеств (5):*

$$\begin{aligned}
&\beta^{7^k}\beta_i = \beta_{7^k+i} + \beta_{7^k-i};\ \beta^{2\times7^k}\beta_i = \beta_{2\times7^k+i} + \beta_{2\times7^k-i} + 2\beta_i;\\
&\beta^{3\times7^k}\beta_i = \beta_{3\times7^k+i} + \beta_{3\times7^k-i} + 3\beta_{7^k+i} + 3\beta_{7^k-i};\\
&\beta^{4\times7^k}\beta_i = \beta_{4\times7^k+i} + \beta_{4\times7^k-i} + 4\beta_{2\times7^k+i} + 4\beta_{2\times7^k-i} - \beta_i;\\
&\beta^{5\times7^k}\beta_i = \beta_{5\times7^k+i} + \beta_{5\times7^k-i} - 2\beta_{3\times7^k+i} - 2\beta_{3\times7^k-i} +\\
&+3\beta_{7^k+i} + 3\beta_{7^k-i};\\
&\beta^{6\times7^k}\beta_i = \beta_{6\times7^k+i} + \beta_{6\times7^k-i} - \beta_{4\times7^k+i} - \beta_{4\times7^k-i} + \beta_{2\times7^k+i} +\\
&+\beta_{2\times7^k-i} - \beta_i.
\end{aligned} \tag{7}$$

Тождества (6), (7) выводятся непосредственно применением тождеств (3) и подтверждаются обращением тождеств (4) и (5).

Следствие 3. *Пусть для чисел t, s, r, k и n выполняются неравенства* $s\times7^k < t \le (s+1)\times7^k$; $0 < k$; $0 < s \le 6$; $r\times7^k + t \le n$ *(не ограничивая общности, полагаем, что* $r\times7^k + t = n$, *считая «лишние» коэффициенты нулевыми).*

Тогда формула

$$\begin{aligned}
\mathbf{x} = \beta^{r\times7^k}\Bigg(&\sum_{i=0}^{7^k-1} x_{r\times7^k+i}\beta_i + \sum_{i=0}^{7^k-1} x_{r\times7^k+7^k+i}\beta_{7^k+i} +\\
&+\sum_{i=0}^{7^k-1} x_{r\times7^k+2\times7^k+i}\beta_{2\times7^k+i} + \ldots + \sum_{i=0}^{t} x_{r\times7^k+s\times7^k+i}\beta_{s\times7^k+i}\Bigg)
\end{aligned} \tag{8}$$

представляет тот же элемент поля $GF(7^n)$, *что и формула*

$$\begin{aligned}
x = \beta^{r\times7^k}\Bigg(&\sum_{j=0}^{s}\beta^{j7^k} y_{r\times7^k+j7^k}\beta_{j7^k} + \sum_{i=1}^{7^k-1} y_{r\times7^k+i}\beta_i +\\
&+\beta^{7^k}\sum_{i=1}^{7^k-1} y_{r\times7^k+7^k+i}\beta_{7^k+i} + \beta^{2\times7^k}\sum_{i=1}^{7^k-1} y_{r\times7^k+2\times7^k+i} +\\
&+\beta_{r\times72\times7^k+i} + \beta^{s\times7^k}\sum_{i=1}^{t} y_{r\times7^k+s\times7^k+i}\beta_{s\times7^k+i}\Bigg),
\end{aligned} \tag{9}$$

где (при сокращенных обозначениях $x_{r\times7^k+j\times7^k+i} = x_{j,i}$, $y_{r\times7^k+j\times7^k+i} = y_{j,i}$)

$$\begin{aligned}
&y_{0,0} = 2c(r)(x_{0,0} - x_{2,0} + x_{4,0} - x_{6,0});\ y_{1,0} = x_{1,0} - 2x_{3,0} - v_3;\\
&y_{2,0} = x_{2,0} + x_{4,0} + 2v_{4,0};\ y_{3,0} = v_3;\\
&y_{4,0} = v_4;\ y_{5,0} = x_{5,0};\ y_{6,0} = x_{6,0},
\end{aligned} \tag{10}$$

где $v_3 = (x_{3,0} + 2x_{5,0})$, $v_4 = (x_{4,0} + x_{6,0})$, $c(r) = 1$, *если* $r = 0$, *иначе* $c(r) = 4$, *и* (*при* $i = 1, \ldots, 7^k - 1$, *если* $k > 0$).

$$\begin{aligned}
&y_{0,i} = x_{0,i} - x_{1,7-i} - x_{2,i} + x_{3,7-i} + v_{4,i} - x_{6,i};\\
&y_{1,i} = x_{1,i} - x_{2,7-i} + 2(x_{4,7-i} - x_{3,i},) - 4v_{5,i};\\
&y_{2,i} = x_{2,i} - x_{3,7-i} + 4v_{4,i} - x_{6,i};\ y_{3,i} = x_{3,i} - x_{4,7-i} - 4v_{5,i};\\
&y_{4,i} = y_{4,i} + 2x_{6,i};\ y_{5,i} = v_{5,i};\ y_{6,i} = x_{6,i};
\end{aligned} \tag{11}$$

где $v_{4,i} = x_{4,i} - x_{5,7-i}$, $v_{5,i} = x_{5,i} - x_{6,7-i}$.

Эти тождества получаются применением тождеств (4), (5) к отдельным суммам формулы (8) и последующим почленным суммированием.

Обозначим $F_k(\mathbf{x})$ преобразование элемента $\mathbf{x}$ поля $GF(7^n)$, представленного формулой:

$$\sum_{r=0}^{s}\left(\beta^{r\times7^k}\sum_{i=0}^{n} x_{r\times7^k+i}\beta_i\right)$$

последовательным (или параллельным) применением преобразований по (10), (11) (или только (11) при $k = 0$) при различных значениях r.

Следствие 4. *Формула (9) эквивалентно преобразуется в (8) подстановками*

$$\begin{aligned}
&x_{0,0} = 4(d(r)y_{0,0} - y_{6,0}) + y_{2,0} - v_2);\ x_{1,0} = y_{1,0} + y_{3,0} + 2v_3;\\
&x_{2,0} = y_{2,0} + v_2 + y_{6,0}, x_{3,0} = v_3;\ x_{4,0} = y_{4,0} - y_{6,0};\\
&x_{5,0} = y_{5,0};\ x_{6,0} = y_{6,0},
\end{aligned} \tag{12}$$

где $v_2 - 4v_{4,0}$; $v_3 = v_{3,0} - 2v_{5,0}$; $d(r) = 1$, *если* $r = 0$, иначе $d(r) = 2$, и *при* $k > 0$, $i = 1, \ldots, 7k - 1$

$$x_{j,0} = 4(y_{j,0} - y_{j,6}) + y_{j,2} - v_2;\ x_{j,1} = y_{j,1} + y_{j,3} + 2v_3;$$
$$x_{j,2} = y_{j,2} + v_2 + y_{j,6};\ x_{j,3} = v_3;\ x_{j,4} = y_{j,4} - y_{j,6}; \qquad (13)$$
$$x_{j,5} = y_{j,5};\ x_{j,6} = y_{j,6},$$

где $v_2 = 4y_{j,4}$; $v_3 = y_{j,3} - 2y_{j,5}$;

$$x_{0,i} = y_{0,i} + y_{1,7-i} + 2y_{2,i} - 4(y_{3,7-i} + y_{5,7-i}) - y_{4,i} - y_{6,i};$$
$$x_{1,i} = y_{1,i} + y_{2,7-i} - 4(y_{3,i} - y_{4,7-i} + y_{5,i}) + y_{6,7-i};$$
$$x_{2,i} = y_{2,i} + y_{3,7-i} + 4y_{4,i} - 2y_{5,7-i} + y_{6,i};$$
$$x_{3,i} = y_{3,i} + y_{4,7-i} - 2y_{5,i} - y_{6,7-i};$$
$$x_{4,i} = y_{4,i} + y_{5,7-i} - y_{6,i};\ x_{5,i} = y_{5,i} + y_{6,7-i};\ x_{6,i} = y_{6,i}$$

и эти преобразования обратны по отношению к преобразованиям по формулам (10), (11).

Данные тождества получаются применением тождеств (6), (7) к отдельным суммам формулы (9) и последующим почленным суммированием. Обратимость подтверждается непосредственно выполнением подстановок.

Обозначим $F_k^{-1}(\mathbf{y})$ преобразование элемента $\mathbf{y}$ поля $GF(7^n)$, представленного формулой

$$\sum_{r=0}^{s}\left(\beta_{r\times 7^k}\sum_{i=0}^{n} y^{r\times 7^k+i}\beta^i\right)$$

последовательным (или параллельным) применением преобразований по формулам (12), (13) (или только (12) при $k = 0$) при различных значениях r.

Теперь преобразование $F(\mathbf{x})$ можно представить рекурсивно:

базис рекурсии: принять $\mathbf{y}_0 = \mathbf{x}$;

шаг рекурсии: $\mathbf{y}_k = F_{d-k+1}(\mathbf{y}_{k-1})$. что означает применение преобразования F_{d-k+1} к элементу поля $\mathbf{y}_{k-1}$, полученному после k–1-го шага рекурсии или при $k = 1$ (после базисного преобразования).

Последовательная программа такого преобразования соответствует тождеству $\mathbf{y} = F(\mathbf{x}) = F_0(F_1(F_2(...(F_{d-1}(F_d(\mathbf{x})))))))$, где $d = \lceil \log_7 n \rceil - 1$.

Рекурсивное описание преобразования $F^{-1}(\mathbf{y})$ имеет вид:

базис рекурсии: $\mathbf{x}_0 = \mathbf{y}$;

шаг рекурсии: $\mathbf{x}_k = F^{-1}_{k-1}(\mathbf{x}_{k-1})$, что означает применение преобразования F^{-1}_{k-1} к элементу поля $\mathbf{x}_{k-1}$, полученному после k – 1- го шага рекурсии или при $k = 1$ (после базисного преобразования).

Последовательная программа этого преобразования соответствует тождеству $\mathbf{x} = F^{-1}(\mathbf{y}) = F_d^{-1}(F_{d-1}^{-1}(F_{d-2}^{-1}(...(F_{d-1}(F_1^{-1}(F_0(\mathbf{y})))))))$, где $d = \lceil \log_7 n \rceil - 1$.

Согласно рекурсивным описаниям с учетом описаний преобразований F_d, ..., F_0, F_0^{-1}, ..., F_d^{-1}, асимптотическая сложность преобразований $F(\mathbf{x})$ и $F^{-1}(\mathbf{y})$ оценивается как $O(n\ln n)$.

Последовательные программы таких преобразований позволяют подсчитать количество операций сложения и вычитания в них и уточнить асимптотическую оценку сложности.

На заключительном шаге F_d преобразования $F(\mathbf{x})$ (или начальном шаге F_0 преобразования $F^{-1}(\mathbf{y})$) выполняется $n_0 = \left\lceil \frac{n}{7} \right\rceil$ преобразований (11) (или (12)) при общей сложности $c_{rp}n_0$ (или $c_{pr}n_0$), $c_{rp} = c_{pr} = 9a + 4m_c$, m_c — сложность умножения на константы 2 или 4; a — сложность вычитания или сложения в $GF(7)$).

На j-м шаге преобразования $F(\mathbf{x})$ выполняется $n_j = \left\lceil \frac{n}{7^{j+1}} \right\rceil$ преобразований (10), каждое сложности, $a_{rp} \times (7^j)$, $a_{rp} = 5m_c + 17a$ и такое же количество преобразований (11) каждое сложности c_{rp} при суммарной сложности шага рекурсии (этапа последовательной программы) $n_j\times(a_{rp}\times(7^s) + c_{rp})$ аддитивных операций. Получается, что сложность преобразования из приведенного в полиномиальный базис по предложенным тождествам равна

$$L_{rp}(n) = \sum_{j=1}^{k-1} n_j \times (a_{rp} \times (7^j) + b_{rp}) + c_{rp}n_0.$$

Аналогично рассчитывается сложность обратного преобразования $F^{-1}(\mathbf{y})$:

$$L_{pr}(n) = \sum_{j=1}^{k-1} n_j \times (a_{pr} \times (7^j) + b_{pr}) + c_{pr}n_0,$$

где $a_{pr} = 6m_c + 21a$; $b_{pr} = c_{pr}$.

Чтобы получить замкнутую формулу верхней оценки сложности, будем считать, что $n = 7^k$ (если $7^{k-1} < n < 7^k$, то полагаем, что недостающие старшие элементы нулевые). Тогда $n_0 = 7^{k-1}$, $n_j = 7^{k-j-1}$ и верхние оценки сложности получаются следующими:

$$L_{rp}(n) = \sum_{j=1}^{k-1} 7^{k-j-1} \times (a_{rp} \times (7^j) + b_{rp}) + c_{rp}n_0 =$$
$$= \frac{a_{rp}}{7} n\log_7 n - \frac{(a_{rp} - c_{rp})}{7} n + \left(\frac{n-7}{42}\right) b_{pr};$$

$$L_{pr}(n) = \sum_{j=1}^{k-1} 7^{k-j-1} \times (a_{pr} \times (7^j) + b_{pr}) + c_{pr}n_0 =$$
$$= \frac{a_{pr}}{7} n\log_7 n - \frac{(a_{pr} - c_{pr})}{7} n + \left(\frac{n-7}{42}\right) b_{pr}.$$

Таким образом, при n, $n \le m$, $m = 7^{\lceil \log 7n \rceil}$ справедливы неравенства

$$L_{rp}(n) \le L_{rp}(m);\ L_{pr}(n) \le L_{pr}(m).$$

Для конкретных последовательных программ оценки можно уточнить:

$L_{rp}(29) = 93a + 21m$ при $L_{rp}(7^2) = 191a + 67m_c$;
$L_{pr}(57) = 236a + 79m_c$ при $L_{pr}(7^3) = 2571a + 816m_c$.

В арифметике конечных полей, имеющих о.н.б. 2-го или 3-го типов, используются также удвоенный полиномиальный $\{1, \beta, \beta^2, ..., \beta^{n-1}, \beta^n, \beta^{n+1}, ..., \beta^{2n-1}\}$ и удвоенный приведенный нормальный $\{\beta_0, \beta_1, \beta_2, ..., \beta_{n-1}, \beta_n, \beta_{n+1}, ..., \beta_{2n-1}\}$ базисы.

Следствие 3. Для представлений элементов $\mathbf{x}$ и $\mathbf{y}$ поля $CF(7^n)$ в удвоенном полиномиальном и удвоенном приведенном о.н.б. 2-го или 3-го типов выполняются тождества $\mathbf{y} = F(\mathbf{x})$, $\mathbf{x} = F^{-1}(\mathbf{y})$.

Лемма 2. Представление $\mathbf{x} = x_0\beta_0 + x_1\beta_1 + ... + x_{n-1}\beta_{n-1} + x_n\beta_n$ элемента $(x_0, x_1, ..., x_{n-1}, x_n)$ поля $GF(7^n)$ в редундантном о.н.б. 2-го или 3-го типов получается из его представления $\mathbf{x} = z_0\beta_0 + z_1\beta_1 + ... + z_{n-1}\beta_{n-1} + z_n\beta_n + z_{n+1}\beta_{n+1} + ... + z_{2n-1}\beta_{2n-1}$ в удвоенном приведенном базисе при $x_0 = z_0$, $x_1 = z_1$, $x_2 = z_2$, $x_i = z_i + z_{2n+1-i}$, $i = 3, ..., n-1$.

Действительно, справедливы тождества $\beta_i = \beta_{2n+1-i}$, $i = 3, ..., n-1$, т.к.

$$\beta_{2n+1-i} = \alpha^{2n+1-i} + \frac{1}{\alpha^{2n+1-i}} = \alpha^{2n+1}\alpha^{-i} + \frac{1}{\alpha^{2n+1}\alpha^{-i}} = \alpha^{-i} + \frac{1}{\alpha^{-i}} = \beta_{-1} = \beta_i.$$

Арифметика конечных полей с использованием о.н.б. 2-го и 3-го типов

Умножение элементов $\mathbf{x} = (x_0, x_1, ..., x_{n-1})$, $\mathbf{y} = (y_0, y_1, ..., y_{n-1})$ поля $GF(q^n)$ характеристики q, заданных в приведенном о.н.б. 2-го или 3-го типов, можно выполнить по следующему алгоритму.

1. Преобразовать сомножители в полиномиальный базис:

$$\mathbf{x} \to \mathbf{x}' = (x_0', x_1', \ldots, x_{n-1}'), \mathbf{y} \to \mathbf{y}' = (y_0', y_1', \ldots, y_{n-1}').$$

2. Вычислить произведение в кольце $GF(q)$ рассматривая его (с добавленным нулевым $(2n-1)$-м мономом) как представление в удвоенном полиномиальном базисе:

$$\{1, \beta, \beta^2, \ldots, \beta^{2n-2}, \beta^{2n-1}\}:$$
$$\mathbf{x} \times \mathbf{y} = \mathbf{z} = (z_0, z_1, z_2, z_3 \ldots, z_{2n-2}, 0).$$

3. Преобразовать результат из удвоенного полиномиального базиса в удвоенный приведенный о.н.б. $\{\beta_0, \beta_1, \beta_2, ..., \beta_{2n-1}\}$, применив рекурсивный алгоритм преобразования $F^{-1}: \mathbf{z} \to \mathbf{z}' = (z_0', z_1', z_2', z_3' \ldots, z_{2n-2}', z_{2n-1}')$.

4. Преобразовать полученный элемент $\mathbf{z}'$ в редундантный о.н.б. $\{\beta_0, \beta_1, ..., \beta_n\}$, применив тождества $\beta_{2n+1-i} = \beta_i$, $i = 3, ..., n$, т.е. сложив элементы z_i и z_{2n+1-i}, $i = 3, ..., n$ и сохранив значения z_0 и z_1:

$$\mathbf{z}'' = (z_0, z_1, z_2, z_3 + z_{2n-2}, \ldots, z_n + z_{n+1}) = (z_0'', z_1'', z_2'', \ldots, z_n'').$$

5. Преобразовать полученный элемент $\mathbf{z}''$ в приведенный о.н.б.:

$$\mathbf{z}'' \to \mathbf{z}''' = (z_0'' + \frac{1}{2}(q-1)x_n) + (z_1'' - z_n'') + (z_2'' - z_n'') + \ldots + (z_{n-1}'' - z_n'')).$$

Асимптотическая сложность этого алгоритма $O(n\ln n + M(n))$, где $M(n)$ — сложность операции умножения в кольце

Модифицированная операция умножения отличается тем, что один из сомножителей представлен в п.б. и результат четвертого пункта конвертируется в переставленный о.н.б.

Пример. Пусть после преобразования множителей в полиномиальный базис получены элементы x_1 и x_2 в результате их перемножения в кольце $GF(7)[X]$ получено произведение x_1x_2, представленное в удвоенном полиномиальном базисе. Получим его представление в приведенном о.н.б. и покажем, что этот результат соответствует приведению по модулю неприводимого многочлена, корнем которого порождается поле $GF(7^{29})$. Это проиллюстрировано следующим листингом.

Умножение в полиномиальном базисе для получения эталона
Неприводимый полином (вектор коэффициентов в порядке возрастания степеней переменной):
(11000005161550440000134311011),
множители x_1, x_2:
x_1 = (00000000000000000000000000001),
x_2= (001),
произведение x_1x_2 в удвоенном полиномиальном базисе (п.б.), здесь и ниже старшие нулевые коэффициенты не указываются:
x_1x_2 = (00000000000000000000000000001),
произведение x_1x_2 в поле $GF(2^{\wedge}n)$, эталон:
$x_1x_2$field = (10600005352402403000012165061).
Переведем x_1x_2 из удвоенного п.б. в удвоенный приведенный, затем в редундантный, далее в приведенный базисы поля $GF(2^{\wedge}n)$ и вернем в полиномиальный, ожидая совпадение с эталоном, тем самым осуществим приведение x_1x_2 по модулю неприводимого многочлена:
x_1x_2 в удвоенном приведенном базисе:
(50600000000040104000000000010201);
x1x2 в редундантном вазисе:
(50600000000040104000000000001021);
x_1x_2 в приведенном базисе:
(16566666666636063666666666061);
x_1x_2 в полиномиальном базисе (восстановлено из приведенного):
(10600005352402403000012165061),
как и должно быть по эталону.

Операция возведения в степень $q^j, j \in \mathbf{N}$ в приведенном о.н.б. выполняется по следующему алгоритму.

1. Преобразовать представление $\mathbf{x}$ в приведенном о.н.б. в представление $\mathbf{x}'$ в переставленном о.н.б. по формуле (1).

2. Возвести в степень q^j, $j \in \mathbf{N}$ с учетом перестановки π

$$\mathbf{y}' = \mathbf{x}'^{7^j} = (x'_{\pi(\pi^{-1}(1)-j)}, \ldots, x'_{\pi(\pi^{-1}(i)-j)}, \ldots, x'_{\pi(\pi^{-1}(n)-j)})$$

3. Преобразовать результат в приведенный о.н.б. по формуле (2).Число сложений по этому алгоритму равно $2n - 2$ асимптотическая сложность $O(n)$.

В модифицированной операции возведения в степень q^j не исполняется первый пункт описанного алгоритма, т.к. вход задается в переставленном о.н.б. Число сложений в модифицированном алгоритме равно $n - 1$.

Для возведения в степень используется обычный алгоритм с разложением показателя степени по степеням семерки и использованием алгоритма возведения в степени q^j и модифицированной операции умножения на каждом шаге.

Операция обращения в $GF(q^n)$ в приведенном о.н.б. 2-го или 3-го типов может быть реализована с применением обобщенного в [12] бинарного алгоритма Евклида [13] со сложностью $O(n^t)$, $2 < t < 3$. Пусть $F(X)$ есть неприводимый многочлен, корень которого порождает базис поля $GF(7^n)$.

Алгоритм операции обращения имеет вид:

1. Преобразовать элемент $\mathbf{x} \in GF(q^n)$ из приведенного о.н.б. в полиномиальный базис.

2. $\mathbf{b} \leftarrow 1$; $\mathbf{c} \leftarrow 1$; $\mathbf{u} \leftarrow \mathbf{c}$; $\mathbf{v} \leftarrow \mathbf{f}(X)$;

3. Пока deg $\mathbf{u} > 0$:

пока $u_0 = 0$:

$\mathbf{u} \leftarrow \mathbf{u}/X$;

если $b_0 = 0$:$\mathbf{b} \leftarrow \mathbf{b}/X$;

иначе: $\mathbf{b} \leftarrow (\mathbf{b} - f_0^{-1} b_0 \mathbf{f}(X))/X$;

если deg $\mathbf{u} > 0$:

если deg $\mathbf{u} <$ deg $\mathbf{v}$:$\mathbf{u} \leftrightarrow \mathbf{v}$, $\mathbf{b} \leftrightarrow \mathbf{c}$;

$\mathbf{b} \leftarrow (-v_0)\mathbf{b} + \mathbf{c}u_0$, $\mathbf{u} \leftarrow (-v_0)\mathbf{u} + \mathbf{v}u_0$.

4. Преобразовать $\mathbf{b}u_0^{-1}$ в приведенный о.н.б. и вернуть.

Алгоритм возведения в степень $d \in \mathbf{N}$ в $GF(7^n)$:

Вход: $\mathbf{a} \in GF(7^n)$, $d \in (0, -1, -3, 1, 2, 3)^n$.

Выход: $\mathbf{a}^d \in GF(7^n)$.

1. $\mathbf{a}[1] = \mathbf{a}$; $\mathbf{a}[2] = \mathbf{a}^2$; $\mathbf{a}[3] = \mathbf{a}[2] \times \mathbf{a}$;

$a[3] = a[2] \times a$; $\mathbf{a}[4] = \mathbf{a}[3] \times \mathbf{a}$; $\mathbf{a}[5] = \mathbf{a}[4] \times \mathbf{a}$; $\mathbf{a}[6] = \mathbf{a}[5] \times \mathbf{a}$;

преобразовать элементы $\mathbf{a}[1] - \mathbf{a}[6]$ в п.б.

2. Для $i = \overline{(0, |d|)}$:

если $d[|d|-i-1] = 0$: $j = j+1$,

иначе: $\mathbf{b} = b^{7^j}$; $\mathbf{b} = \mathbf{b} \times \mathbf{a}\,[d[|d|-i-1]]$; $j = 1$;

3. Вернуть $\mathbf{b} = \mathbf{b}^{7^j}$.

Авторы выражают благодарность к.ф.-м.н И. С. Сергееву за полезные замечания. Работа выполнена при поддержке РФФИ (проект № 14-01-00671а).

Литература

1. **Лидл. Р., Нидеррайтер Г.** Конечные поля. Т. 1, 2. М.: Мир, 1988.

2. **Болотов А.А., Гашков С.Б., Фролов А.Б., Часовских А.А.** Элементарное введение в эллиптическую криптографию. Алгебраические и алгоритмические основы. М.: КомКнига, 2012.

3. **Mullin R.C., Onyszchuk I.M.,Vanstone S.A., Wilson R.M.** Optimal Normal Bases in GF(pn) // Discrete Appl. Math. 1988 89). 22, 149-161.

4. **Болотов А.А., Гашков С.Б.** О быстром умножении в нормальных базисах конечных полей // Дискретная математика. 2001. Т. 13. Вып. 3. С. 3 — 31.

5. **Shokrollahi J.** Efficient implementation of elliptic curve cryptography on FPGA: PhD thesis. Universitet Bonn, 2007.

6. **Gathen von zur J., Shokrollahi A., Shokrollahi J.** Efficient multiplication using type 2 optimal normal bases. // Proc. WAIFI 07, LNCS. 2007. P. 55 — 68.

7. **Bernstein D.J., Lange T.** Type-II Optimal Polynomial Bases, Arithmetic of Finite Fields // Proc. LNCS, 6087. 2010. P. 41 — 61.

8. **Gashkov S., Frolov A., Lukin S., Sukhanova O.** Arithmetic in the finite fields using optimal normal and polynomial bases in combination // Advances in Intelligent Systems and Computing. 2015. P. 153 — 162.

9. **Koblitz N.** Algebraic aspects of Cryptography. Berlin Heidelberg: Springer Verlag, 1998.

10. **Koblitz N., Menezes A.** Pairing-based cryptography at high security levels // Proc.Tenth IMA Intern. conf. cryptography and coding. 2005. P. 3 — 36.

11. **Гашков С.Б. и др.** О схемной и программной реализации арифметики в конечных полях характеристики 7 для вычисления спариваний // Фундаментальная и прикладная математика. 2009. № 3. С. 75 — 111.

12. **Гашков С.Б., Фролов А.Б., Шилкин С.О.** О некоторых алгоритмах обращения и деления в конечных кольцах и полях // Вестник МЭИ. 2006. № 6. С. 20 — 31.

13. **Hankerson D., López J.H., Menezes A.** Software implementation of elliptic curve cryptography over binary fields. CHES 2000 // LNCS. 2000. N 1965. P. 1 — 23.

Статья поступила в редакцию 22.10.2015