Кодирование алфавитов точками эллиптических кривых

В. Ю. Лёвин

В настоящее время информационые технологии бурно развиваются, вычислительная техника становится все мощнее и мощнее. Многие криптосистемы с открытым ключем становятся ненадежными. Последнее стало основной предпосылкой создания надежных криптосистем на основе эллиптических кривых. Большинство эллиптических криптосистем используют представление объекта шифрования в виде набора точек на эллиптической кривой, однако, такой переход нужно еще совершить. Для осуществления такого перехода Нил Коблиц (N. Koblitz) в 1985 году предложил использовать вероятностный алгоритм представления открытых текстов [1]. На сегодняшний день этот алгоритм претерпел мало изменений и является малоизученным. В данной работе удалось построить новый, детерминированный, способный работать в системах реального времени алгоритм кодирования открытых текстов.

Обозначим через K конечное поле, то есть поле вида $\mathbb{F}_q$, где $q = p^n$, p — простое, $n \in \mathbb{N}$.

Определение 1. (эллиптической кривой в форме Вейерштрасса) Пусть $\operatorname{char} K \neq 2, 3$ и x^3+ax+b — кубический многочлен без кратных корней ($a, b \in K$). Эллиптической кривой над K ($E(K)$) называется множество точек (x, y) $x, y \in K$, удовлетворяющих уравнению

$$y^2 = x^3 + ax + b \tag{1}$$

вместе с единственным элементом O — бесконечно удаленной точкой.

Схематично последнее можно записать в виде:

$$E(K) = \left\{(x, y) \in K \times K \,:\, y^2 = x^3 + ax + b,\ \ a, b \in K\right\} \cup \{O\}\,.$$

Рассмотрим произвольный конечный алфавит $A = \{a_0, a_2, \ldots, a_{M-1}\}$. Поставим в соответствие каждому символу a_m алфавита A его номер m. Закодируем символы алфавита A, проинтерпретированные как числа $m \in [0, \ldots, M-1]$ точками эллиптической кривой $E(K)$:

$$A = \{a_0, a_2, \ldots, a_{M-1}\} \to \{0, \ldots, M-1\} \to \\ \to \{P_0(x, y), \ldots, P_{M-1}(x, y)\} \in E(K).$$

Заметим, что любой открытый текст есть набор символов некоторого конечного алфавита, тем самым, закодировав символы алфавита точками эллиптической кривой, мы закодируем весь текст. Затем к полученному набору точек применим одну из стандартных эллиптических крипосистем (см. [1]), в результате чего мы получаем шифротекст пригодный для передаче по открытому каналу связи. Сложность расшифровки этого текста есть сложность решения задачи дискретного логарифмирования на эллиптической кривой (см. [1, 2]). На сегодняшний день не существует детерминированного, полиномиального по времени алгоритма, решающего задачу дискретного логарифмирования в общем случае. Поэтому расшифровать такой шифротекст в режиме реального времени в общем случае не под силу даже современным компьютерам, что подчеркивает важность изучения таких криптосистем.

Для построения детерминированного алгоритма кодирования алфавитов точками эллиптических кривых нам потребуется несколько классических фактов из теории эллиптических кривых. Введем операцию сложения точек эллиптической кривой над конечным полем K (подробное описание операции сложения см. в [1, 2]).

Пусть $P = (x_1, y_1) \in E(K)$, тогда $-P = (x_1, -y_1)$. Если $Q = (x_2, y_2) \in E(K)$ $Q \neq -P$, то $P + Q = (x_3, y_3)$, где

$$x_3 = \lambda^2 - x_1 - x_2;$$
$$y_3 = \lambda(x_1 - x_3) - y_1;$$
$$\lambda = \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1}, & \text{если } P \neq Q, \\ \dfrac{3x_1^2 + a}{2y_1}, & \text{если } P = Q. \end{cases}$$

Теорема 1. $\{E(\mathbb{F}_q), +\}$ — *множество точек на эллиптической кривой является абелевой группой относительно введенной выше операции сложения.*

Теорема 2 (Хассе). *Пусть* $\#E(K)$ — *число точек на эллиптической кривой в форме (1), определенной над конечным полем* K, $\operatorname{char} K \neq 2, 3$. *Тогда* $|\#E(K) - (1 + p)| \leqslant 2\sqrt{p}$.

Доказательства этих теорем можно найти в [3]. Теперь введем определение дуальных эллиптических кривых.

Определение 2. Две эллиптические кривые:

$$E_{ab} : y^2 = x^3 + ax + b \quad \text{и} \quad E_{a'b'} : y^2 = x^3 + a'x + b',$$

заданные над конечным полем K, $\operatorname{char} K \neq 2, 3$, $a, b, a', b' \in K$ называются дуальными (twists), если имеет место следующее соотношение:

$$\begin{cases} a' = v^2 a, \\ b' = v^3 b, \end{cases}$$

где $v \in K$ — квадратичный невычет по модулю p.

Обозначим через $\#E(K)$ — количество точек на эллиптической кривой $E(K)$.

Теорема 3. *Пусть* $E_{ab}(\mathbb{F}_p)$, *и* $E_{a'b'}(\mathbb{F}_p)$ — *две дуальные эллиптические кривые над конечным полем* $\mathbb{F}_p$, $p \neq 2, 3$. *Тогда*

$$\#E_{ab}(\mathbb{F}_p) + \#E_{a'b'}(\mathbb{F}_p) = 2p + 2.$$

Доказательство. Пусть у нас есть дуальные эллиптические кривые над полем $\mathbb{F}_p$ вида:

$$E_{ab}(\mathbb{F}_p) : y^2 = g(x), \quad \text{где} \quad g(x) = x^3 + ax + b,$$
$$E_{a'b'}(\mathbb{F}_p) : y^2 = g_v(x), \quad \text{где} \quad g_v(x) = x^3 + a'x + b'.$$

Лемма 1.

$$g_v(x) = v^3 g\left(\frac{x}{v}\right).$$

Доказательство.

$$g_v(x)=x^3+a'x+b'=x^3+v^2ax+v^3b=v^3\left(\left(\frac{x}{v}\right)^3+a\left(\frac{x}{v}\right)+b\right)=v^3g\left(\frac{x}{v}\right).$$

Лемма доказана.

Воспользуемся формулой для подсчета количества точек на эллиптической кривой вида (1), заданной над простым полем. Согласно [4, 5] она имеет вид

$$\#E(\mathbb{F}_p)=1+\sum_{x \pmod p}\left(\left(\frac{x^3+Ax+B}{p}\right)+1\right).$$

В нашем случае получаем, что

$$\#E_{ab}(\mathbb{F}_p)=1+\sum_{x \pmod p}\left(\left(\frac{g(x)}{p}\right)+1\right), \tag{2}$$

$$\#E_{a'b'}(\mathbb{F}_p)=1+\sum_{x \pmod p}\left(\left(\frac{g_v(x)}{p}\right)+1\right). \tag{3}$$

Проанализируем эти формулы: если для некоторого $x\in\mathbb{F}_p$ выполнено $g_v(x)=0$, то $g\left(\frac{x}{v}\right)=0$, так как имеет место соотношение $g_v(x)=v^3g\left(\frac{x}{v}\right)$. Этот случай добавляет по единице как в сумму (2), так и в сумму (3). Допустим теперь, что $g_v(x)$ — ненулевой квадратичный вычет по модулю p. Тогда так как v — квадратичный невычет по модулю p, то v^3 будет невычетом, так как:

$$\left(\frac{v^3}{p}\right)=\left(\frac{v^2}{p}\right)\left(\frac{v}{p}\right)=(1)(-1)=-1.$$

Далее заметим, что если l — невычет, то l^{-1} — невычет. Действительно, $ll^{-1}\equiv 1 \pmod p$, поэтому

$$\left(\frac{ll^{-1}}{p}\right)=\left(\frac{l}{p}\right)\left(\frac{l^{-1}}{p}\right)=(-1)(s)=1\Leftrightarrow s=-1.$$

Основываясь на этом, можно сделать вывод, что $\dfrac{1}{v^3}$ — невычет. Поэтому, так как $g\left(\dfrac{x}{v}\right) = \dfrac{g_v(x)}{v^3}$, то $g\left(\dfrac{x}{v}\right)$ — квадратичный невычет. Этот случай добавляет две единицы в (3) и ничего не добавляет в (2). Пусть теперь наоборот, $g_v(x)$ — квадратичный невычет, тогда $g\left(\dfrac{x}{v}\right)$ — вычет, что добавляет две единицы в (2) и ничего не добавляет в (3). Перебирая все элементы в поле $\mathbb{F}_p$, получаем $\#E_{ab} + \#E_{a'b'} = 2p + 2$. Теорема доказана.

Пример 1. В качестве иллюстрации теоремы 3 выпишем всевозможные дуальные кривые над полем $\mathbb{F}_5$:

$E_{01} : y^2 = x^3 + 0x + 1 \quad \#E_{01} = 6 \quad \to E_{03} : y^2 = x^3 + 0x + 3 \quad \#E_{03} = 6,$
$E_{02} : y^2 = x^3 + 0x + 2 \quad \#E_{02} = 6 \quad \to E_{01} : y^2 = x^3 + 0x + 1 \quad \#E_{01} = 6,$
$E_{03} : y^2 = x^3 + 0x + 3 \quad \#E_{03} = 6 \quad \to E_{04} : y^2 = x^3 + 0x + 4 \quad \#E_{04} = 6,$
$E_{04} : y^2 = x^3 + 0x + 4 \quad \#E_{04} = 6 \quad \to E_{02} : y^2 = x^3 + 0x + 2 \quad \#E_{02} = 6,$
$E_{10} : y^2 = x^3 + 1x + 0 \quad \#E_{10} = 4 \quad \to E_{40} : y^2 = x^3 + 4x + 0 \quad \#E_{40} = 8,$
$E_{11} : y^2 = x^3 + 1x + 1 \quad \#E_{11} = 9 \quad \to E_{43} : y^2 = x^3 + 4x + 3 \quad \#E_{43} = 3,$
$E_{12} : y^2 = x^3 + 1x + 2 \quad \#E_{12} = 4 \quad \to E_{41} : y^2 = x^3 + 4x + 1 \quad \#E_{41} = 8,$
$E_{13} : y^2 = x^3 + 1x + 3 \quad \#E_{13} = 4 \quad \to E_{44} : y^2 = x^3 + 4x + 4 \quad \#E_{44} = 8,$
$E_{14} : y^2 = x^3 + 1x + 4 \quad \#E_{14} = 9 \quad \to E_{42} : y^2 = x^3 + 4x + 2 \quad \#E_{42} = 3,$
$E_{20} : y^2 = x^3 + 2x + 0 \quad \#E_{20} = 2 \quad \to E_{30} : y^2 = x^3 + 3x + 0 \quad \#E_{30} = 10,$
$E_{21} : y^2 = x^3 + 2x + 1 \quad \#E_{21} = 7 \quad \to E_{33} : y^2 = x^3 + 3x + 3 \quad \#E_{33} = 5,$
$E_{22} : y^2 = x^3 + 2x + 2 \quad \#E_{22} = 7 \quad \to E_{31} : y^2 = x^3 + 3x + 1 \quad \#E_{31} = 5,$
$E_{23} : y^2 = x^3 + 2x + 3 \quad \#E_{23} = 7 \quad \to E_{34} : y^2 = x^3 + 3x + 4 \quad \#E_{34} = 5,$
$E_{24} : y^2 = x^3 + 2x + 4 \quad \#E_{24} = 7 \quad \to E_{32} : y^2 = x^3 + 3x + 2 \quad \#E_{32} = 5,$
$E_{30} : y^2 = x^3 + 3x + 0 \quad \#E_{30} = 10 \quad \to E_{20} : y^2 = x^3 + 2x + 0 \quad \#E_{20} = 2,$
$E_{31} : y^2 = x^3 + 3x + 1 \quad \#E_{31} = 5 \quad \to E_{23} : y^2 = x^3 + 2x + 3 \quad \#E_{23} = 7,$
$E_{33} : y^2 = x^3 + 3x + 3 \quad \#E_{33} = 5 \quad \to E_{24} : y^2 = x^3 + 2x + 4 \quad \#E_{24} = 7,$
$E_{34} : y^2 = x^3 + 3x + 4 \quad \#E_{34} = 5 \quad \to E_{22} : y^2 = x^3 + 2x + 2 \quad \#E_{22} = 7,$
$E_{40} : y^2 = x^3 + 4x + 0 \quad \#E_{40} = 8 \quad \to E_{10} : y^2 = x^3 + 1x + 0 \quad \#E_{10} = 4,$
$E_{41} : y^2 = x^3 + 4x + 1 \quad \#E_{41} = 8 \quad \to E_{13} : y^2 = x^3 + 1x + 3 \quad \#E_{13} = 4,$
$E_{42} : y^2 = x^3 + 4x + 2 \quad \#E_{42} = 3 \quad \to E_{11} : y^2 = x^3 + 1x + 1 \quad \#E_{11} = 9,$
$E_{43} : y^2 = x^3 + 4x + 3 \quad \#E_{43} = 3 \quad \to E_{14} : y^2 = x^3 + 1x + 4 \quad \#E_{14} = 9,$
$E_{44} : y^2 = x^3 + 4x + 4 \quad \#E_{44} = 8 \quad \to E_{12} : y^2 = x^3 + 1x + 2 \quad \#E_{12} = 4.$

Теорема 4. *Пусть $n \leqslant [2\sqrt{p}]$ — целое число, $E(\mathbb{F}_p)$ — эллиптическая кривая в форме (1) над простым полем $\mathbb{F}_p$, $p \neq 2, 3$, причем $\#E(\mathbb{F}_p) = p + 1 - n$. Тогда*

$$\#E_v(\mathbb{F}_p) = \begin{cases} p+1+n, & \textit{если } v \textit{ — невычет;} \\ p+1-n, & \textit{если } v \textit{ — вычет,} \end{cases}$$

где $E_v(\mathbb{F}_p)$ — эллиптическая кривая в форме (1), полученная заменой

$$\begin{cases} a' = v^2 a, \\ b' = v^3 b. \end{cases}$$

Доказательство. Рассмотрим несколько случаев. Пусть v — квадратичный невычет. Тогда по определению кривые $E(\mathbb{F}_p)$ и $E_v(\mathbb{F}_p)$ являются дуальными. Следовательно, по предыдущей теореме, $\#E(\mathbb{F}_p) + \#E_v(\mathbb{F}_p) = 2p + 2$, откуда получаем, что

$$\#E_v(\mathbb{F}_p) = 2p + 2 - p - 1 + n = p + 1 + n.$$

Если v — вычет, то аналогично, анализируя формулу для подсчета количества точек на эллиптической кривой, можно в терминах предыдущей теоремы заметить, что если $g_v(x)$ — вычет, то и $g\left(\dfrac{x}{v}\right)$ — вычет, верно и наоборот. Теперь остается перебрать все элементы поля $\mathbb{F}_p$ и заметить что

$$\#E(\mathbb{F}_p) = \#E_v(\mathbb{F}_p) = p + 1 - n.$$

Теорема доказана.

Теорема 5. *Пусть $n \leqslant [2\sqrt{p}]$ — целое число. Тогда количество эллиптических кривых в форме (1) над $\mathbb{F}_p$, $p \neq 2, 3$, имеющих $p+1-n$ точек равно количеству эллиптических кривых в форме (1) над тем же полем, имеющих $p+1+n$ точек.*

Доказательство. Нужно показать, что соответствие

$$E_{ab} \to E_{a'b'}$$

взаимнодназначное, то есть у двух различных эллиптических кривых в форме (1) не может быть одинаковой дуальной кривой. Предположим противное. Рассмотрим две кривые $E_{a_1 b_1}$, $E_{a_2 b_2}$, $a_1, b_1, a_2, b_2 \in \mathbb{F}_p$,

пусть $b_1 = b_2$, a_1 несравнимо с a_2 по модулю p и обе эти кривые при замене

$$\begin{cases} a' = v^2 a, \\ b' = v^3 b \end{cases}$$

переходят в кривую $E_{a'b'}$. Заметим, что условие того, что кривые перешли в одну равносильно условию $a_1 v^2 \equiv a_2 v^2 \pmod{p}$, но тогда $a_1 \equiv a_2 \pmod{p}$.

Последнее невозможно, так как мы рассматривали кривые у которых a_1 несравнимо с a_2 по модулю p (то есть заданные разными многочленами). Пришли к противоречию. Теорема доказана.

Из доказаных теорем следует, что если перебрать все эллиптические кривые над текущем полем, считая количество точек на каждой из них, то эллиптических кривых на которых p точек будет столько же, сколько эллиптических кривых на которых $p + 2$ точки; эллиптических кривых на которых $p - 1$ точка будет столько же, сколько эллиптических кривых на которых $p + 3$ точки, и так далее. Обнаруженная симметрия позволяет построить новый, детерминированный алгоритм представления открытых текстов.

Вероятностный алгоритм кодирования алфавитов открытых текстов точками эллиптической кривой

Н. Коблиц в 1985 году предложил вероятностный алгоритм представления (кодирования) открытых текстов. В качестве объекта представления Н. Коблиц предложил рассмотреть символы произвольного алфавита $A = \{a_0, a_2, \ldots, a_{M-1}\}$. Суть этого алгоритма заключается в следующем. Поставим в соответствие каждой букве алфавита A её номер m. Теперь закодируем произвольный номер m точкой $P_m(x, y)$ на эллиптической кривой вида (1). Тем самым мы переводим буквы алфавита A в набор точек на эллиптической кривой. Отображение которое будет построено является инъективным, однако оно будет обладать тем свойством, что зная координаты точки $P_m(x, y)$ можно однозначно восстановить какому числу m они соответствуют. Таким образом возможен обратный процесс (процесс декодирования). Предполагается, что далее к полученному набору то-

чек будет применена одна из ECC (Elliptic Curve Cryptology)-криптосистем. В результате применения такой криптосистемы пользователь получает зашифрованный текст, пригодный для передачи другому пользователю.

Рассмотрим $E(\mathbb{F}_q)$, где поле $\mathbb{F}_q$ фиксировано. Положим $q = p^r$. Далее положим, что q — большое нечетное число и $q > M\kappa$, где κ — достаточно большое целое число. Последнее число характеризует вероятность неудачи, то есть вероятность того, что алгоритм не сможет представить букву (символ) алфавита точкой на эллиптической кривой. Эта вероятность равна $\dfrac{1}{2^\kappa}$. Например часто полагают, что $\kappa = 20$ или $\kappa = 50$.

Записываем числа от 1 до $M\kappa$ в виде $m\kappa + j$, $1 \leqslant j \leqslant \kappa$, и устанавливаем взаимооднозначное соответствие между такими числами и некоторым множеством элементов в $\mathbb{F}_q$. Например, можно записать это число как r-значное число в p-ичной системе исчисления, и отождествить числа этой записи с элементами $\mathbb{F}_p \cong \dfrac{\mathbb{Z}}{p\mathbb{Z}}$ рассмотрев их как коэффициенты многочлена степени не выше чем $r-1$ над $\mathbb{F}_p$, соответствующие элементу поля $\mathbb{F}_q$:

$$(a_{r-1}a_{r-2}\dots a_1a_0)_p \to \sum_{i=0}^{r-1} a_i x^i.$$

Значит при данном m $\forall j = 1, 2 \dots \kappa$ мы получаем элемент x из $\mathbb{F}_q$, соответствующий $m\kappa + j$. Для такого x вычисляем правую часть уравнения $y^2 = f(x) = x^3 + ax + b$ и пытаемся найти квадратный корень из $f(x)$. Если мы находим такой $y : y^2 = f(x)$, то полагаем $P_m = (x, y)$; если y не оказывается квадратом, то увеличиваем j на 1 и повторяем попытку с соответствующим значением x. Если мы находим x такой, что $f(x)$ — квадрат, прежде чем j превысит κ, то мы можем восстановить m по формуле

$$m = \left[\frac{\tilde{x} - j}{\kappa}\right],$$

где $\tilde{x}$ — целое число, соответствующее x при отображении $\mathbb{Z}$ и $\mathbb{F}_q$, а вероятность того, что мы найдем такое x равна $1 - \dfrac{1}{2^\kappa}$. Важно отме-

тить, что здесь x, y — элементы поля, то есть многочлены степени не выше $r-1$.

Следует отметить, что данный алгоритм является классическим, и его краткое описание изложено в [1, гл. 5,§2].

Модификация вероятностного алгоритма кодирования алфавитов открытых текстов в случае простого поля $\mathbb{F}_p$

Если рассмотривать простое поле, то вероятностный алгоритм представления открытых текстов можно описать следующим образом. Рассотрим алфавит $A = \{a_0, a_2, \ldots, a_{M-1}\}$, символы которого мы хотим представить точками на эллиптической кривой. Как и в предыдущем случае, поставим в соответствие символу алфавита его номер, и без ограничения общности можно считать, что мы кодируем числа $m \in [0, \ldots, M-1]$ точками эллиптической кривой. Возмем число κ, простое поле $\mathbb{F}_p : p \leqslant M\kappa$, и эллиптическую кривую $E(\mathbb{F}_p)$.

Представляем числа от 1 до $M\kappa$ в виде $m\kappa + j$ $j \in [1, \ldots, \kappa]$. После чего считаем символ Лежандра $\left(\dfrac{f(m\kappa+j)}{p}\right)$, если он равен 1, то мы нашли соответствующую точку $P_m(m\kappa+j, \bar{y})$. При этом $\bar{y}$ — это такое число, что

$$\bar{y}^2 \equiv f(m\kappa + j) \pmod{p}.$$

А если он равен -1, то увеличиваем j на единицу и повторяем процесс. С вероятростью $1-\dfrac{1}{2^\kappa}$ мы такое представление найдем. Этот процесс можно записать в виде схемы:

$$\begin{array}{l} 1 \\ 2 \\ 3 \\ \vdots \\ m \quad m\kappa + j \to f(m\kappa + j) \to \begin{array}{l} \text{если} \quad \left(\dfrac{f(m\kappa+j)}{p}\right) = 1 \to P_m(m\kappa + j, \bar{y}) \\ \text{иначе} \quad j \to j+1 \end{array} \\ \vdots \\ M\kappa \end{array}$$

Получается кодирование каждого числа $m \in [1, \ldots, M]$ происходит не более чем за κ попыток. Вот почему данный алгоритм назван вероятностным.

Пример 2. Закодируем предложение «veni vidi vici» над полем F_{6421} точками эллиптической кривой $y^2 = x^3 + 123x + 3456$. При этом будем интерпретировать латинские буквы как их ASCII коды (числа от 0 до 255). Также положим, что $\kappa = 25$.

$$\begin{gathered}\text{veni vidi vici}\\ \downarrow\\ (2951{,}6054)(2527{,}4044)(2752{,}140)(2625{,}1007)(801{,}4067)(2951{,}6054)(2625{,}1007)\\ (2500{,}4398)(2625{,}1007)(801{,}4067)(2951{,}6054)(2625{,}1007)(2476{,}2074)(2625{,}1007)\end{gathered}$$

Теперь опишем обратный процесс (процесс декодирования $P_m(x, y) \to m$). Восстановление происходит по формуле

$$m = \begin{cases} \dfrac{x - x \pmod{\kappa}}{\kappa} & \text{если } j \neq \kappa, \\ \dfrac{x - \kappa}{\kappa} & \text{если } j = \kappa. \end{cases}$$

Заметим, что декодер может держать у себя в памяти только число κ, и это уже позволит ему, получив точку $P_m(x, y)$, восстановить исходное число m.

Описание детерминированного алгоритма кодирования алфавитов точками эллиптических кривых

Более подробное описание детерминированного алгоритма см. в [6].

$$\boxed{\begin{array}{l} m \in [0, \ldots, M-1], \quad M, K, E(K), \\ v \in K \text{ — невычет} \end{array}} \quad \to \quad \begin{array}{l} P_m(x, y) \\ \text{кривая } E(K), \\ \text{либо } E_v(K) \\ \text{подстановка.} \end{array}$$

Возмем произвольный невычет $v \in K$, и рассмотрим две кривые: E_{ab} и к ней дуальную $E_{a'b'}$ заданные над полем K.

$m \in [0, \ldots, M-1]$ — число которое мы хотим закодировать точкой на эллиптической кривой. Рассмотрим удвоенный отрезок: $[0, \ldots, 2M-2]$.

Пусть $g(x) = x^3 + ax + b$, $g_v(x) = x^3 + a'x + b'$ — правые части уравнений эллиптических кривых E_{ab} и $E_{a'b'}$ соответственно.

Последовательно, начиная с 0 до $2M - 2$ проверяем является ли $g(m)$ вычетом или нет. При этом можно показать, что если $g(m)$ — вычет, то $g_v(mv)$ — невычет, и наоборот, если $g(m)$ — невычет, то $g_v(mv)$ — вычет.

Свойство быть вычетом или невычетом здесь равносильно существованию на соответствующей эллиптической кривой точки $P_m(x, y)$ в которую мы переводим число m. Информацию о том, является ли $g(m)$ и $g_v(mv)$ вычетом/невычетом удобно представить в виде таблицы, где + означает, что $g(m)$ или $g_v(mv)$ — вычет, а − — невычет.

	E_{ab}:		$E_{a'b'}$:
$m \in [0, \ldots, 2M-2]$	$y^2 = x^3 + ax + b$	mv	$y^2 = x^3 + a'x + b'$
0	+	0	−
1	+	v	−
2	−	2v	+
3	−	3v	+
4	+	4v	−
5	−	5v	+
6	+	6v	−
7	−	7v	+
.	−	.	+
.	−	.	+
.	−	.	+
.	−	.	+
2M-2	+	(2M-2)v	−

После того как мы дойдем до $2M - 2$, выбираем ту кривую на которой больше или равно M плюсов то, что такая кривая найдется, следует из приведенных выше теорем. В результате работы данного алгоритма мы получим в памяти вид эллиптической кривой и соотвутствующую подстановку, по модулю которой ма закодировали символы алфавита A. Следовательно мы обошли итерации вероятностного алгоритма, а работаем детерминированно (за один шаг алгоритма мы всегда закодируем число m (букву a_m алфавита A) точкой P_m, которая будет принадлежать одной из двух рассматриваемых кривых).

Характеристики детерминированного алгоритма кодирования позволяют использовать его в системах реального времени даже при больших размерах полей.

Алгоритм реализован в виде программы, что свидетельствует об актуальности применения его на практике.

Пример 3. Рассмотрим поле $\mathbb{F}_{751}$, $M = 7$. Закодируем числа $m \in [0, \ldots, M]$ точками эллиптической кривой:

$0 < m < 2M$	$y^2 = x^3 + 748x + 749$	mv	$y^2 = x^3 + 724x + 697$
0	$-$	0	$+$
1	$-$	v	$+$
2	$+$	2v	$-$
3	$+$	3v	$-$
4	$+$	4v	$-$
5	$-$	5v	$+$
6	$+$	6v	$-$
7	$+$	7v	$-$
8	$-$	8v	$+$
9	$-$	9v	$+$
10	$+$	10v	$-$
11	$+$	11v	$-$
12	$+$	12v	$-$
13	$-$	13v	$+$

Для кодирования выбираем первую кривую с подстановкой:
$1 \to 2 \to (2, 0)$,
$2 \to 3 \to (3, 4)$,
$3 \to 4 \to (4, 186)$,
$4 \to 6 \to (6, 14)$,
$5 \to 7 \to (7, 364)$,
$6 \to 10 \to (10, 233)$,
$7 \to 11 \to (11, 36)$,

Выводы

- Построен детерминированный алгоритм, способный работать в системах реального времени. Данный алгоритм опирается на

строгий математический аппарат, некоторые теоремы которого дополняют ранее известные теоремы теории эллиптических кривых.

- Написан ряд программ, позволяющих подробно исследовать некоторые аспекты теории эллиптических кривых, что представляет собой ценность из-за вычислительной сложности работы с эллиптическими кривыми.
- Разработанный детерминированный алгоритм реализован в виде программы, как для $\mathbb{F}_p$, так и для $\mathbb{F}_{p^n}$ и может быть использован на практике.

Автор выражает признательность А. Е. Панкратьеву и В. А. Носову за научное руководство.

Список литературы

[1] Коблиц Н. Курс теории чисел и криптографии. М.: ТВП, 2001.

[2] Blake I. F., Serroussi G., Smart N. P. Elliptic curves in cryptography. 1999.

[3] Кнепп Э. Эллиптические кривые / пер. с англ. Ф. Ю. Попеленского, под ред. Ю. П. Соловьева. М.: Факториал Пресс, 2004.

[4] Koblitz Neal, Menezis Alfred, Vanstone Scott. The State of Elliptic Curve Cryptography. 2000.

[5] Schoof Rene. Counting points on elliptic curves over finite fields. 1995.

[6] Лёвин В. Ю. Кодирование алфавитов точками эллиптических кривых / Дипломная работа. 2007.