ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ТЕХНОЛОГИЙ ПЕРЕДАЧИ И ОБРАБОТКИ ИНФОРМАЦИИ И СИГНАЛОВ

УДК 621.391; 681.3

ОБОСНОВАНИЕ ТРЕБОВАНИЙ К ВЫБОРУ ПАРАМЕТРОВ ЭЛЛИПТИЧЕСКОЙ КРИВОЙ В АЛГОРИТМАХ КОДИРОВАНИЯ АЛФАВИТА ТОЧКАМИ ЭЛЛИПТИЧЕСКОЙ КРИВОЙ

Червяков Н.И., Кияшко Е.С.

В статье проанализированы существующие алгоритмы кодирования алфавита точками эллиптической кривой над F_p. Найдены недостатки данных алгоритмов и предложены методы их решения.

Ключевые слова: Эллиптическая кривая, кодирование алфавита точками эллиптической кривой.

Введение. Постановка задачи

Эллиптические кривые применяются в криптографии с 1985 года, причем как для факторизации чисел и проверки простоты, так и для построения криптографических протоколов. Интерес к ним обусловлен, с одной стороны, тем, что они являются богатым источником абелевых групп, обладающих полезными структурными свойствами, так и тем, что на их основе обеспечиваются те же криптографические свойства, которыми обладают числовые или полиномиальные криптосистемы, но при существенно меньшем размере ключа.[7] Эллиптическая кривая *E* над простым полем F_p, где $p > 3$, задана уравнением в форме Вейерштрассе:

$$E(F_p): y^2 = x^3 + ax + b, \text{ где } 4a^3 + 27b^2 \neq 0. \quad (1)$$

Представление информации в виде набора точек на эллиптической кривой используют большинство эллиптических криптосистем, но переход от алфавита к точкам эллиптической кривой нужно еще осуществить.

Поставка задачи: необходимо провести анализ существующих алгоритмов кодирования алфавитов точками эллиптической кривой над F_p, определить недостатки с целью их устранения и предложить методы их решения.

Алгоритмы кодирования алфавитов

Существует два алгоритма кодирования алфавитов: вероятностный и детерминированный. Проанализируем вероятностный алгоритм кодирования алфавита точками эллиптической кривой (1), предложенный в 1985 г. Н. Коблиц [3].

Алгоритм 1. Кодирование алфавита точками эллиптической кривой.

Вход. Простое число p, $a, b \in F_p$, M – мощность алфавита, который мы кодируем точками эллиптической кривой, и k – число, причем обычно значение $k = 20$ или $k = 50$.

Выход. Закодированный алфавит точками эллиптической кривой P_i, где $i \in [0,..., M-1]$.

1. $i = 0$

2. Пока $i < M$, выполнять:

2.1. $j = 1$

2.2. Пока $j < k + 1$, выполнять:

2.2.1.Если $\left(\frac{(i \cdot k + j)^3 + a(i \cdot k + j) + b}{p}\right) = 1$, то

2.2.1.1.

$P_0 = (i \cdot k + j, \text{sqrtmod}((i \cdot k + j)^3 + a(i \cdot k + j) + b))$

2.2.1.2. Переходим к пункту 2.3.

2.2.2. $j = j + 1$

2.3. $i = i + 1$

3. Вывод P_i для всех $i = 0,..., M-1$.

Функция $\text{sqrtmod}(a)$ вычисляет корень квадратный из числа a по модулю *p*.

Рассмотрим алгоритм декодирования.

Алгоритм 2. Декодирование символа из точки эллиптической кривой.

Вход. Точка $P_i = (x, y)$ эллиптической кривой и число *k*.

Выход. Число i

1. Если $x \bmod k = 0$, то $i = \frac{x - k}{k}$

2. Если $x \bmod k > 0$, то $i = \frac{x - x \bmod k}{k}$

3. Вывод i

Преимущество данного алгоритма состоит в том, что для вычисления, числа *i* необходимо держать в памяти только точку $P_i = (x, y)$ и число k.

Недостатки:

1. Вероятность того, что i будет не закодировано, равна $\frac{1}{2^k}$, а при большом выборе M вероятность не закодировать один из символов алфавита возрастает многократно. Например, при $M = 10^5$ и $k = 13$ вероятность не закодировать

алфавит равна $1-\left(1-\frac{1}{2^k}\right)^M = 0{,}7$; то есть вероятность не закодировать алфавит больше, чем вероятность его закодировать.

2. С помощью данного алгоритма можно закодировать алфавит, мощность которого равна $\left\lfloor \frac{p}{k} \right\rfloor$, что приблизительно в k раз меньше, чем число точек на эллиптической кривой согласно теореме Хассе.

Проведем анализ детерминированного алгоритма кодирования алфавитов точками эллиптических кривых, предложенного в [4]. Для рассмотрения детерминированного алгоритма кодирования алфавита точками эллиптической кривой введем понятие дуальных эллиптических кривых.

Определение. Две эллиптические кривые: $E_{ab}: \quad y^2 = x^3 + ax + b$ и $E_{a'b'}: y^2 = x^3 + a'x + b'$, заданные над конечным полем F_p, где p – простое число, $p > 3$, $a, b, a', b' \in F_p$ называются дуальными, если имеет место

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

где $v \in F_p$ – квадратичный невычет по модулю p.

Для дуальных эллиптических кривых справедлива следующая теорема.

Теорема 1 [4]. Пусть $E_{ab}(F_p)$ и $E_{a'b'}(F_p)$ – две дуальные эллиптические кривые над конечным полем F_p, $p \neq 2,3$. Тогда

$$\#E_{ab}(F_p) + \#E_{a'b'}(F_p) = 2p + 2$$

Перейдем теперь к алгоритму кодирования.

Алгоритм кодирования алфавита точками эллиптической кривой

Алгоритм 3. Кодирование алфавита точками эллиптической кривой.

Вход. Простое число p, $a, b \in F_p$ и M – мощность алфавита, который мы кодируем точками эллиптической кривой.

Выход. Закодированный алфавит точками эллиптической кривой P_i, где $i \in [0,..., M-1]$, и эллиптическая кривая.

1. Выбираем число v так, чтобы оно являлось квадратичным невычетом в F_p.

2. Вычисляем $a' = (v^2 a) \bmod p$

3. Вычисляем $b' = (v^3 b) \bmod p$

4. $\text{counterE}_{ab} = 0$. $\text{counterE}_{a'b'} = 0$

4. Для всех $i = 0,...,2M-2$ вычисляем $\left(\frac{x^3 + ax + b}{p}\right)$ – символ Лежандра.

4.1. Если $\left(\frac{i^3 + ai + b}{p}\right) \geq 0$, то

$\text{counterE}_{ab} = \text{counterE}_{ab} + 1$.

4.2. Если $\left(\frac{i^3 + ai + b}{p}\right) \leq 0$, то

$\text{counterE}_{a'b'} = \text{counterE}_{a'b'} + 1$.

5. Если $\text{counterE}_{ab} \geq M$, то

5.1. $j = 0$, $i = 0$.

5.2. До тех пор пока $j \neq M$, выполнять

5.2.1. Если $\left(\frac{i^3 + ai + b}{p}\right) = 1$, то

$P_j = (i, \text{sqrtmod}(i^3 + ai + b))$ и $j = j + 1$.

5.2.2. Если $\left(\frac{i^3 + ai + b}{p}\right) = 0$, то $P_j = (i, 0)$ и $j = j + 1$

5.2.3 $i = i + 1$

5.3. Выводим P_m и $a, b \in F_p$

5.4. Иначе $j = 0$, $i = 0$

5.5. До тех пор пока $j \neq M$, выполнять

5.5.1. Если $\left(\frac{i^3 + ai + b}{p}\right) = -1$, то

$P_j = (vi, \text{sqrtmod}(v^3 i^3 + a'iv + b'))$ и $j = j + 1$

5.5.2. Если $\left(\frac{i^3 + ai + b}{p}\right) = 0$, то $P_j = (vi, 0)$ и $j = j + 1$

5.5.3 $i = i + 1$

5.6. Выводим P_m и $a', b' \in F_p$.

6. Конец

Рассмотрим применения алгоритма 3 к кодированию алфавита точками эллиптических кривых из работы [5], которые рекомендованы в США.

Пример 1. Эллиптическая кривая E_{ab}: $y^2 = x^3 - 3x + b$ задана над полем F_n, где p – простое число. Закодировать числа $m \in [0,...,7]$

1. Рассмотрим эллиптическую кривую $P-192$:

$b = 153447221625558988608768369/$

$/6998407365480692536381144252 65$

$p = 627710173538668076383578942 3/$

$/2076664160839087003903249612 79$

Так как p – простое число вида $p = 4k + 3$, то $p - 1$ является квадратичным невычетом в F_p и, значит,

$v = p - 1 = 627710173538668076383578 9/$
$/42320766641608390870039032496 1278$.

Вычислим a' и b':

$a' = 627710173538668076383578 9423/$
$/20766641608390870039032496 1276$
$b' = 612365451376112177522702 1053/$
$/50782567953583944675221053 6014$

Найдем, для каких значений $i \in [0...14]$ значение выражения $x^3 - 3x + b$ является квадратичным вычетом в F_p, а для каких – невычетом в F_p. Результат вычисления оформим в виде таблицы, где знаком «+» обозначается квадратичный вычет в F_p, а знаком «–» обозначается квадратичный невычет в F_p.

Таблица 1.

i	$E_{ab}(i)$	iv	$E_{a'b'}(iv)$
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	–	$13v$	+
14	–	$14v$	+

Мы получили, что в столбце эллиптической кривой E_{ab} число плюсов равно 5, а в столбце эллиптической кривой $E_{a'b'}$ – 10 плюсов. Таким образом, кодирование будет осуществляться с помощью эллиптической кривой $E_{a'b'}$.

Для кодирования числа «0» воспользуемся строкой с номером 2. Этой строке соответствует точка

$\left(2v, \text{sqrtmod}((2v)^3 - a \cdot (2v) + b)\right) = (627710173538/$
$/66807638357894232076664160839087003903 2496/$
$/1277, 12344909704434357094945483249892753 11/$
$/0013110430180582923 50).$

Таким образом, «0» будет закодирован точкой
(627710173538668076383578942 32/
/07666416083908700390324961277,
12344909704434357094945483249 8/
/92753110013110430180582923 50).

Для краткости будем записывать это так:

$0 \to 2 \to$ (627710173538668076383578942 39/
/42320766641608390870039032496 1277,
12344909704434357094945483249 8/
/92753110013110430180582923 50);
$1 \to 3 \to$ (627710173538668076383578942/
/32076664160839087003903249612 76,
54832218508459406110542237790339/
/52398269531847958561436381);
$2 \to 4 \to$ (627710173538668076383578942 32/
/07666416083908700390324961275,
30388726966587001182122894950 1/
/03407742449436272629166026 92);
$3 \to 5 \to$ (627710173538668076383578 9/
/42320766641608390870039032496 1274,
29094583868224251897675922597/
/97524831389360823444734508543);
$4 \to 6 \to$ (627710173538668076383578 9/
/42320766641608390870039032496 1273,
36396065120665209936203129571/
/74687570291106189790410801368);
$5 \to 9 \to$ (627710173538668076383578 9/
/42320766641608390870039032496 1270,
28523371345875919144088584494/
/22488889087567985269024248608);
$6 \to 10 \to$ (627710173538668076383578 9/
/42320766641608390870039032496 1269,
18810379573679683598797288572/
/41544647527486465809863097482);
$7 \to 12 \to$ (627710173538668076383578 9/
/42320766641608390870039032496 1267,
50738792504375883144992815027/
/02009951896015994137612734228).

Найдем $\#E_{a'b'}$. Так как
$\#E_{ab} = 627710173538668076383578 94/$
$/23176059013767194773182842284081$,
то, используя теорему 1, получим, что

$$\#E_{a'b'} = 627710173538668076383578 94/$$
$$/232392738184006226275978076384 79 =$$
$$= 23 \cdot 10864375060560251605900 6777/$$
$$/43 \cdot 251204017934436899364791 25511.$$

Из того, что максимальный множитель в разложении $\#E_{a'b'}$ равен

$$251204017934436899364791 25511,$$

следует, что методом Полларда задачу дискретного логарифмирования можно решить за

$$\sqrt{251204017934436899364791 25511} =$$
$$= 158494169588170$$

операций с точками на эллиптической кривой [6]. При условии, что современная техника может производить 10^{10} операций с точками на эллиптической кривой, то задачу дискретного логарифмирования на эллиптической кривой можно решить за 4 часа 30 минут. На основе этих данных мы можем сделать вывод, что данная эллиптическая кривая непригодна к использованию в криптографических целях.

Из примера 1 видно, что детерминированный метод кодирования алфавита точками эллиптической кривой приводит к понижению криптостойкости эллиптических кривых *P*–192 на дуальные, но не криптостойкие кривые. В связи с этим на эллиптическую кривую нужно накладывать дополнительные условия.

Таким образом, во избежание недостатков данных алгоритмов, используемая эллиптическая кривая $y^2 = f(x)$ над простым полем F_p должна удовлетворять, следующим условиям:

1. p – простое число длины 256 бит.
2. Полином $f(x)$ не должен иметь кратных корней, то есть его дискриминант должен быть отличен от нуля по модулю p.
3. j – инвариант кривой должен быть отличен от 0 и 1728.
4. Число точек $\#E(F_p)$ и $2p+2-\#E(F_p)$ должно иметь простой делитель r длины от 254 до 256 бит.
5. $\#E(F_p) \neq p$.
6. $p^k \neq 1 (\mathrm{mod}\, r)$ для $k = 1; 2; 3 \ldots 31$.

Выводы

В статье проведен анализ алгоритмов кодирования алфавитов точками эллиптической кривой. Показано, что вероятностный метод кодирования обладает двумя существенными недостатками:

- при большой мощности алфавита вероятность его не закодировать возрастает и становится больше, чем вероятность его закодировать.
- с его помощью возможно закодировать алфавит в k раз меньше, чем количество точек на эллиптической кривой.

Рассмотрен детерминированный метод кодирования алфавита, который использует дуальную эллиптическую кривую. Показано, что переход от криптостойкой эллиптической кривой к дуальной кривой может привести к некриптостойкой эллиптической кривой, что следует из приведенного примера 1, задачу дискретного логарифмирования можно решить за 4 ч 30 мин. при условии, что современная техника может выполнять 10^{10} операций в секунду с точками эллиптической кривой.

Наложены дополнительные требования, которым должна удовлетворять эллиптическая кривая для применения алгоритма Левина.

Литература

1. Menezes A., van Oorchot P., Vanstone S. Handbook of applied cryptography. CRC press, 1997. – 816 p.
2. Ростовцев А.Г. Маховенко Е.Б. Два подхода к логарифмированию на эллиптической кривой: URL: http://www.ssl.stu.neva.ru/ssl/archieve/lift1.pdf
3. Коблиц Н. Курс теории чисел и криптографии. М.: Изд. ТВП, 2001. – 254 с.
4. Левин В.Ю. Кодирование алфавитов точками эллиптических кривых // Интеллектуальные системы. Т.11, 2007. – С. 171-183.
5. Recommended Elliptic Curves for Federal Government Use: URL: http://csrc.nist.gov/groups/ST/toolkit/documents/dss/NISTReCur.pdf
6. Ростовцев А.Г., Маховенко Е.Б. Теоретическая криптография. СПб: АНО НПО «Профессионал», 2005. – 720 с.
7. Болотов А.А., Гаршков С.Б., Фролов А.Б., Часовских А.А. Алгоритмические основы эллиптической криптографии. М: Изд. МЭИ, 2004. – 499 с.