Анализ повышения криптографической сложности систем при переходе на эллиптические кривые

В. Ю. Лёвин, В. А. Носов

Хорошо известно, что основную криптографическую сложность при взломе классических криптосистем над конечными полями дает сложность решения задачи дискретного логарифмирования. В случае классических криптосистем на основе эллиптических кривых такую сложность дает решение соответствующей задачи дискретного логарифмирования на эллиптической кривой. Стоить отметить, что большинство криптосистем позволяют перейти на эллиптические кривые. При этом происходит серьезное увеличение криптографической сложности. В данной работе проведен анализ изменения сложности при переходе на эллиптические кривые. В ходе анализа установлено, что возрастание сложности при подобном переходе не приводит к увеличению размеров ключей, а наблюдается эффект уменьшения их длин при сохранении общей криптосложности системы. В работе приведено теоретическое обоснование этого факта, построены зависимости длин ключей.

1. Понятие эллиптической кривой и ее особенности

Обозначим через K одно из полей вида $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, или $\mathbb{F}_q$, где $q = p^r$, p — простое.

Определение 1 (общая формула уравнения эллиптической кривой). Пусть $x^3 + a_2x^2 + a_4x + a_6$ — многочлен без кратных корней. Тогда

эллиптической кривой над полем K (обозначаемой далее как E(K)) называется множество точек (x, y), удовлетворяющих уравнению

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \tag{1}$$

где $a_i \in K$, $i = 1, 2, 3, 4, 6$, вместе с единственным бесконечно удаленным элементом, обозначаемым далее как O.

Схематично последнее можно записать в виде:

$$E(K) = \left\{(x, y) \in K \times K : \ y^2+a_1xy+a_3y = x^3+a_2x^2+a_4x+a_6\right\} \cup \{O\}$$

Теперь можно заметить, что если $\operatorname{char} K \neq 2$, то заменой $y + \dfrac{a_1x + a_3}{2} \to y$ уравнение (1) приводится к виду

$$y^2 = x^3 + ax^2 + bx + c$$

и заменой $x + \dfrac{1}{3}a \to x$ к виду

$$y^2 = x^3 + bx + c$$

если $\operatorname{char} K > 3$.

Заметим, что согласно определению, в обоих этих случаях многочлен справа не должен имееть кратных корней.

Если $\operatorname{char} K = 2$, то уравнение (1) приводится к виду

$$y^2 + cy = x^3 + ax + b$$

либо к виду

$$y^2 + xy = x^3 + ax^2 + b,$$

где многочлен справа не имеет кратных корней.

Замечание. Заметим, что в уравнении (1) нет коэффициента a_5. Это обясняется тем, что индексы коэффициентов имеют следующий смысл:

видим, что $y = x^{\frac{3}{2}} + o(x)$. Сделав замену

$$\begin{cases} x = t^2 + o(t) \\ y = t^3 + o(t), \end{cases}$$

можно переписать (1) в виде

$$t^6 + a_1 t^5 + a_3 t^3 = t^6 + a_2 t^4 + a_4 t^2 + a_6.$$

Теперь видно, что индекс коэффициента в сумме с соответствующей степенью t есть 6.

В работе будет использовано более компактное определение эллиптической кривой, которое является следствием того, что при $\mathrm{char}\, K > 3$ уравнение (1) можно привести к виду $y^2 = x^3 + bx + c$.

Поэтому при $\mathrm{char}\, K \neq 2, 3$ без потери общности можно рассмотреть следующее определение эллиптической кривой:

Определение 2 (уравнение эллиптической кривой в форме Вейерштрасса) Пусть K — поле, причем $\mathrm{char}\, K \neq 2, 3$ и $x^3 + ax + b$ — кубический многочлен без кратных корней $(a, b \in K)$.

Эллиптическая кривая над K $(E(K))$ — это множество точек (x, y) $x, y \in K$, удовлетворяющих уравнению

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

вместе с единственным элементом O — бесконечно удаленной точкой.

Отсутствие кратных корней в правых частях уравнений можно сформулировать используя понятие дискриминанта $\triangle$ эллиптической кривой (1).

Введем обозначение: $b_2 = a_1^2 + 4a_2$, $b_4 = 2a_4 + a_1 a_3$, $b_6 = a_3^2 + 4a_6$, $b_8 = a_1^2 + 4a_2 a_6 - a_1 a_3 a_4 + a_2 a_3^2 - a_4^2$

Теперь для поля K определим дискриминант $\triangle$ кривой (1) формулой

$$\triangle = -b_2^2 b_8 - 8b_4^3 - 27b_6^2 + 9b_2 b_4 b_6.$$

Определив понятие дискриминанта, мы можем сказать, что кубическая кривая, заданная уравнением (1), является **особой** тогда и только тогда, когда ее дискриминант $\triangle$ равен 0. Заметим, что если эллиптическая кривая задана уравнением (2), то формула для вычисления дискриминанта имеет вид

$$\triangle = 4a^3 + 27b^2.$$

Значения дискриминантов некоторых эллиптических кривых приведены ниже:

Эллиптическая кривая	Значение дискриминанта $\triangle$
$y^2 + y = x^3 - x$	-11
$y^2 + xy = x^3 - 2x^2 + x$	-15
$y^2 + xy + y = x^3$	-26
$y^2 + xy - y = x^3$	-28
$y^2 + y = x^3 + x^2 - x$	-35
$y^2 + y = x^3 + x^2$	-43
$y^2 + xy + y = x^3 - x^2$	-53
$y^2 + xy = x^3 - x^2 + x$	-55
$y^2 + xy = x^3 + x$	-63
$y^2 + 7xy + 2y = x^3 + 4x^2 + x$	15
$y^2 + 3xy = x^3 + x$	17
$y^2 + y = x^3 - x$	37
$y^2 + 2xy - 3y = x^3 - 1$	37
$y^2 + xy = x^3 - x$	65
$y^2 + 3xy - y = x^3 - x^2$	79
$y^2 = x^3 + x^2 - x$	80
$y^2 + xy = x^3 + x^2 - x$	89

Основной интерес в теории эллиптических кривых представляет структура группы точек эллиптической кривой. В качестве полей над которыми задаются эллиптические кривые, в криптографии чаще всего рассматривают поля из q элементов $\mathbb{F}_q$. Такие поля называются **простыми** , если q — простое число.

В дипломной работе будут рассматриваться как простые поля, так и поля из p^n элементов, то есть поля вида $\mathbb{F}_q$, $q = p^n$, $p > 3$ — простое число.

1.1. Структура группы точек эллиптической кривой над полем $\mathbb{F}_q$

Определение 3. Аддитивной абелевой группой называется множество A с операцией сложения, обладающей следующими свойствами:

1) $a + b = b + a \ \forall a, b \in A$ (коммутативность);
2) $(a + b) + c = a + (b + c) \ \forall a, b \in A$ (ассоциативность);

3) В множестве A существует такой элемент O (нуль), что $a + O = a$ $\forall a \in A$;

4) Для любого элемента $a \in A$ существует такой элемент $-a \in A$ (противоположный элемент), что $a + (-a) = O$.

Рассмотрим эллиптическую кривую (2), то есть множество точек вида

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

Введем закон сложения точек на эллиптической кривой.

Определение 4. Пусть $E(K)$ — эллиптическая кривая над полем K, P, Q — две точки на $E(K)$. Определим точки $-P$, $P + Q$:

1) Если $P = O$, то $-P = O$ и $P + Q = Q$ то есть O — тождественный элемент по сложению. Далее полагаем, что ни точка P, ни точка Q не являются точками в бесконечности.

2) Если $P = (x, y)$, то $-P = (x, -y)$. (из уравнения $y^2 = x^3 + ax + b$ следует, что точка $(x, -y) \in E(K)$)

3) Если P и Q имеют различные x-координаты, тогда прямая PQ имеет с $E(K)$ еще одну точку пересечения R (За исключением двух случаев: а) прямая PQ касательная в точке P, тогда полагаем $R = P$; б) прямая PQ касательная в точке Q, тогда полагаем $R = Q$). Определяем точку $P + Q = -R$.

4) Если $Q = -P$, то $P + Q = O$.

5) Если $Q = P$, то считаем, что прямая PQ касательная к $E(K)$ в точке P. Положим $PQ \cap E(K) = R$ (единственная другая точка пересечения). Тогда $P + Q = -R$ (в качестве R берем P, если P есть точка перегиба кривой).

Заметим, что здесь под тем, что точка (x, y) принадлежит кривой $E(K)$, понимаемся, что $x, y \in K$ и в этом поле имеет место соотношение (2). Можно вывести закон сложения точек на эллиптической кривой $E(K)$ в виде формул.

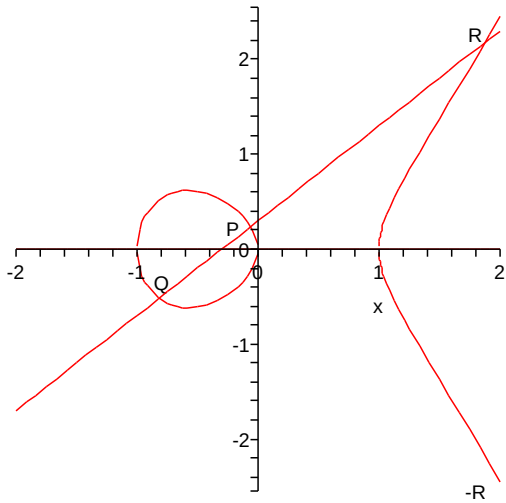

Рис. 1. Сложение точек на эллиптической кривой $y^2 = x^3 - x$ над полем $\mathbb{R}$.

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

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

Подробный вывод этих законов можно найти в [4, гл. 5, §1], поэтому мы не будем подробно останавливаться на нем.

Сейчас уместно пояснить, почему мы не рассматриваем кривые, у которых многочлен в правой части имеет кратные корни, действительно, рассмотрим вырожденные случаи вида:

$y^2 = x^3$
$y^2 = x^3 - x^2$
$y^2 = x^3 + x^2$

У всех этих кривых 0 — особая точка, поэтому понятие касательной в ней не определено и операция сложения точек на эллиптической кривой не имеет смысла.

Существует более общее определение операции сложения точек на эллиптической кривой.

Определение 5 (Метод Пуанкаре определения суммы точек на произвольной эллиптической кривой). Зафиксируем произвольную эллиптическую кривую. Отметим на ней произвольную точку E. Теперь чтобы сложить две точки кривой A и B, проведем прямую AB. Она пересечет кривую в некоторой точке X. Точку пересечения прямой XE с кубической кривой будем считать суммой точек A и B.

Теорема 1. *Множество точек на эллиптической кривой — это абелева группа относительно введенной выше операции сложения.*

Доказательство. Теорема утверждает, что $\{E(\mathbb{F}_q), +\}$ — абелева группа по сложению, которое мы определили выше. Как легко заметить, бесконечно удаленный элемент O является тождественным элементом по сложению. Коммутативность операции сложения очевидна. Доказательство ассоциативности можно найти в [3, гл. 1, §1].

Со сложением мы разобрались. Умножение точеки на целое число k понимается как сложение точки с собой k раз:

$$\underbrace{P + P + \ldots + P}_{k} = kP.$$

Определение 6. Порядком точки P на эллиптической кривой называется наименьшее натуральное число N, такое что $NP = O$.

Такое число всегда существует если мы рассматриваем кривые над полями $\mathbb{F}_q$. Заметим, что так как $O + O = O$, то порядок единичного элемента группы $E(\mathbb{F}_q)$ равен единице.

Пример 1. Найти порядок точки $P = (2, 3)$ на $y^2 = x^3 + 1$. Применяя формулы сложения точек на эллиптической кривой, находим $2P = (0, 1)$; потом по аналогии находим, что

$$4P = 2(2P) = (0, -1) \Rightarrow 4P = -2P \Rightarrow 6P = O.$$

Следовательно, порядок точки P может быть равен $2, 3, 6$. Но замечаем, что $2P = (0, 1) \neq O$, а если бы точка P имела порядок 3, то было бы равенство $3P = O$, что неверно. Значит, $\Rightarrow P$ имеет порядок 6.

Пример 2. Пусть эллиптическая кривая задана уравнением $y^2 = x^3 + x + 1$ над $\mathbb{Z}_{23}$. Тогда $|E(\mathbb{Z}_{23})| = 28$, группа $E(\mathbb{Z}_{23})$ циклическая с образующим элементом $P = (0, 1)$. Ниже показаны точки, полученные умножением из точки P:

$P = (0, 1)$	$2P = (6, -4)$	$3P = (3, -10)$	$4P = (-10, -7)$
$5P = (-5, 3)$	$6P = (7, 11)$	$7P = (11, 3)$	$8P = (5, -4)$
$9P = (-4, -5)$	$10P = (12, 4)$	$11P = (1, -7)$	$12P = (-6, -3)$
$13P = (9, -7)$	$14P = (4, 0)$	$15P = (9, 7)$	$16P = (-6, 3)$
$17P = (1, 7)$	$18P = (12, -4)$	$19P = (-4, 5)$	$20P = (5, 4)$
$21P = (11, -3)$	$22P = (7, -11)$	$23P = (-5, -3)$	$24P = (-10, 7)$
$25P = (3, 10)$	$26P = (6, 4)$	$27P = (0, -1)$	$28P = O$

Пример 3. Перечислить все точки и их порядки для кривой $y^2 = x^3 + 3x + 3$ над полем $\mathbb{F}_{11}$.

Дискриминант данной кривой $\triangle = 351$. Следовательно данная кривая не является особой и она пригодна для вычислений. Всего на данной кривой 8 точек, то есть $|E(\mathbb{F}_{11})| = 8$.

Точки эллиптической кривой:	Порядки точек:
O	1
$(0, 5)$	4
$(0, 6)$	4
$(5, 0)$	2
$(7, 2)$	4
$(7, 9)$	4
$(8, 0)$	2
$(9, 0)$	2

Пример 4. Перечислить все точки и их порядки для кривой $y^2 = x^3 + 3x + 3$ над полем $\mathbb{F}_7$.

Дискриминант данной кривой $\triangle = 351$. Всего на данной кривой уже 6 точек, то есть $|E(\mathbb{F}_{11})| = 6$

Точки эллиптической кривой:	Порядки точек:
O	1
$(1, 0)$	2
$(3, 2)$	3
$(3, 5)$	3
$(4, 3)$	6
$(4, 4)$	6

В завершение параграфа стоит еще раз отметить то, что точки эллиптической кривой над K — образуют абелеву группу. Если K есть $\mathbb{F}_q$, $q = p^n$, p — простое, то она не обязательно циклическая, но она всегда представляет собой произведение двух циклических групп:

$$G \cong \prod_{t|N} \frac{\mathbb{Z}}{t^\alpha \mathbb{Z}} \times \frac{\mathbb{Z}}{t^\beta \mathbb{Z}}$$

где произведение берется по всем простым делителям N (здесь $\alpha > 0$, $\beta > 0$.)

2. Анализ криптографической сложности при переходе на эллиптические кривые

Рассмотрим конечное поле F_p, p — простое число.

Определение 7. Задачей дискретного логарифмирования (DLP) с основанием $q \in F_p^*$ называется нахождение для данного $p \in F_p^*$ целого числа x, такого что $q^x = p$.

Определение 8. Задачей дискретного логарифмирования на эллиптической кривой (ECDLP) $E(F_p)$ с основанием $q \in E(F_p)$ называется нахождение для данного $p \in E(F_p)$ целого числа x, такого что $xq = p$ (если оно существует).

Важно заметить, что решение ECDLP может и не существовать. Это связано с тем, что группа точек на эллиптической кривой не всегда является циклической группой. Однако, ее можно всегда представить в виде произведения двух циклических групп. Что касается DLP, то ее решения существует всегда, так как хорошо известно, что мультипликативная группа поля является циклической. Для исследования криптографической стойкости нам потребуется понятие сложности алгоритма. В основном под сложностью алгоритма понимается количество выполняемых им арифметических операций. Представим сложность в виде функции от длины входа, то есть от количества бит n, требуемых для записи входных данных. Если эта функция многочлен от n, то говорят что алгоритм имеет полиномиальную сложность, если эта функция имеет вид e^{Cn}, $c = \text{const}$, то говорят, что алгоритм имеет экспоненциальную сложность.

Определим функцию

$$L_p(\mu, c) = \exp\left(c(\ln p)^{\mu}(\ln \ln p)^{1-\mu}\right).$$

При $\mu = 0$, эта функция полиномиальна по $\ln p$, если $\mu = 1$ — то экспоненциальна. Поведение этой функции при $0 < \mu < 1$ назовем субъекспоненциальным.

Наилучший из известных на сегодняшний день алгоритмов решения DLP в F_p имеет сложность $L_p(1/3, c_0)$, $c_0 \approx \left(\frac{64}{9}\right)^{1/3} \approx 1.92$. Этот алгоритм был предложен Широкауаром и реализован в виде программы Вебером. Основная идея состоит в некой модификации алгоритма просеивания числового поля.

Теперь заметим, что наилучший среди известных на настоящий момент алгоритмов по решению ECDLP имеет сложность $O(\sqrt{p})$ операций сложения в группе $\langle E(F_p, +)\rangle$. Например для получения этой оценки можно использовать метод Полларда или рассмотреть следующие теоремы:

Теорема 2. *Пусть n, r — натуральные числа, $r^2 \geqslant n$. Для любого целого x можно указать целые числа s и t такие, что*

$$x \equiv sr + t \pmod{n};\ 0 \leqslant s < r,\ 0 \leqslant t < r.$$

Доказательство. Можно предполагать, что $0 \leqslant x < n$. Пусть $s = \left[\frac{x}{r}\right]$, $t = x - sr$. Следовательно можно записать

$$0 \leqslant s \leqslant \left[\frac{x}{r}\right] < \left[\frac{n}{r}\right] \leqslant r.$$

С другой стороны,

$$0 \leqslant s \leqslant \left[\frac{x}{r}\right] < s + 1,$$

поэтому $sr \leqslant x < sr + r$, или $0 \leqslant x - sr = t < r$. Теорема доказана.

После этого можно заметить, что для вычисления кратного $n * m$, где m — элемент некоторого кольца, а n — натуральное число, достаточно выполнить не более $2\,[\log_3 n]$ операций сложения. Для установления этого факта можно применить бинарный метод построения аддитивных цепочек.

Теорема 3. *Пусть $\langle E(F_p, +)\rangle$ — конечная группа точек эллиптической кривое над конечным полем $\mathbb{F}_p$. Q, P — элементы этой группы, n — порядок элемента P,*

$$kP = Q.$$

Тогда число k можно найти выполнив не более, чем $2(\sqrt{n} + \log_2 n) - 1$ операций сложения в группе $\langle E(F_p, +)\rangle$.

Доказательство. Полагаем $r = [\sqrt{n}] + 1$. Рассмотрим ряды $0 * P = O,\ 1 * P = P, 2 * P, \ldots, (r-1) * P$ и $Q, Q + (1 * (-r)) * P, Q + (2 * (-r)) * P, \ldots, Q + ((r-1) * (-r)) * P$. После этого заметим, что если уравнение $kP = Q$ разрешимо относительно k то по предыдущей теореме, учитывая что $r^2 \geqslant n^2$, представим k в виде

$$k \equiv t + sr \pmod{n},\ 0 \leqslant t < r.$$

Так как n — порядок элемента P, то $kP = (sr + t)P = Q$ в том случае если

$$tP = Q + (-sr)P,$$

то есть когда найдется элемент второго ряда, совпадающий с некоторым элементом первого ряда. При вычислении элементов первого ряда потребуется выполнить не более $r - 2$ сложение в группе

$\langle E(F_p,+)\rangle$. Для вычисления $(-r*P)=(n-r)*P$ в силу предыдущей теоремы потребуется выполнить не более $2\log_2 n$ умножений. Так же остается заметить, что для вычисления членов второго ряда нужно выполнить не более $r-1$ операции сложения. Таким образом, общее число групповых операций для нахождения натурального числа k не превышает

$$2r-3+2\log_2 n \leqslant 2(\sqrt{n}+\log_2 n)-1.$$

Теорема доказана.

Вот почему, наилучший среди известных на настоящий момент алгоритмов по решению ECDLP имеет сложность $O(\sqrt{p})$ операций сложения в группе $\langle E(F_p,+)\rangle$. Стоит заметить, что эта оценка в случае использования суперсингулярных эллиптических кривых может быть понижена, однако такие эллиптические кривые не используют на практике.

Введем в рассмотрение число $n=[\log_2 p]$ (оно характеризует число бит в записи числа p). Отбросив константы можно проследить, что

$$\sqrt{p}=2^{\log_2\sqrt{p}}=2^{(\log_2 p)/2}=2^{n/2}.$$

Введем в рассмотрение функцию $C_{ECDLP}(n)$ — сложность решения ECDLP в зависимости от количества бит во входе, аналогично введем функцию $C_{DLP}(l)$ — сложность решения DLP в зависимости от количества бит во входе. Следовательно

$$C_{ECDLP}(n)=2^{n/2}$$

Итак

$$L_p(1/3,c_0)=\exp\left(c_0(\ln p)^{1/3}(\ln\ln p)^{2/3}\right).$$

Положим $l=\log_2 p$, имеем $\log_2 p=\ln p/\ln 2 \;\Rightarrow \ln p=\log_2 p\ln 2$. Следовательно

$$L_p(1/3,c_0)=\exp\left(c_0(\log_2 p\ln 2)^{1/3}(\ln(\log_2 p\ln 2))^{2/3}\right)\approx$$
$$\approx\exp\left(c_0(l\ln 2)^{1/3}(\ln(l\ln 2))^{2/3}\right).$$

Теперь положим $C_{DLP}(l) = \exp\left(c_1(l)^{1/3}(\ln(l\ln 2))^{2/3}\right)$, $c_1 = c_0(\ln 2)^{1/3}$. В итоге мы получили следующее:

$$C_{ECDLP}(n) = 2^{n/2},\ C_{DLP}(l) = \exp\left(c_1(l)^{1/3}(\ln(l\ln 2))^{2/3}\right).$$

Теперь мы можем проанализировать разницу в длинах ключей при одинаковом уровне криптографической безопасности в конечных полях (DLP) и на эллиптических кривых (ECDLP). Имеем $C_{ECDLP}(n) \approx C_{DLP}(l)$, поэтому $n = 2\left(\log_2\left(\exp\left(c_1 l^{1/3}\left(\ln(l\ln 2)\right)^{2/3}\right)\right)\right)$.

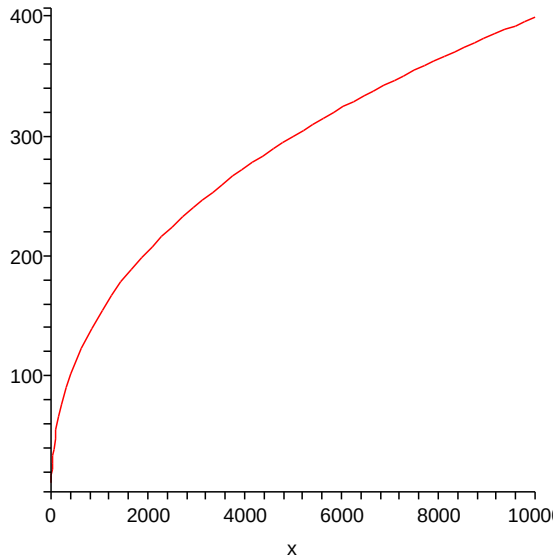

Рис. 2. соотношение длин ключей в криптосистемах над конечными полями (горизонтальная ось) и криптосистемами на основе эллиптических кривых (вертикальная ось) имеющих одинаковый уровень безопасности.

Из вышеописанных вычислений можно усмотреть, что

$$C_{ECDLP}(n) \approx C_{DLP}(sn),\ s = O\left(\frac{n^2}{(\ln 2)^2}\right).$$

Где ECDLP рассматривается над полем F_p, а DLP над полем F_{p^s}. Следовательно произошло увеличение сложности (а как следствие криптостойкости системы) на нелинейный множитель $s = O\left(\frac{n^2}{(\ln 2)^2}\right)$ только за счет перехода на язык эллиптических кривых. Стоить заметить, что эллиптические кривые являются универсальным средством обобщения, это означает что большинство имеющихся криптосистем могут быть переведены на эллиптические кривые, в следствии чего мы получим существенный выигрыш в криптостойкости. Заметим что переход на эллиптические кривые в чем-то эквивалентны взятию расширения поля степени s.

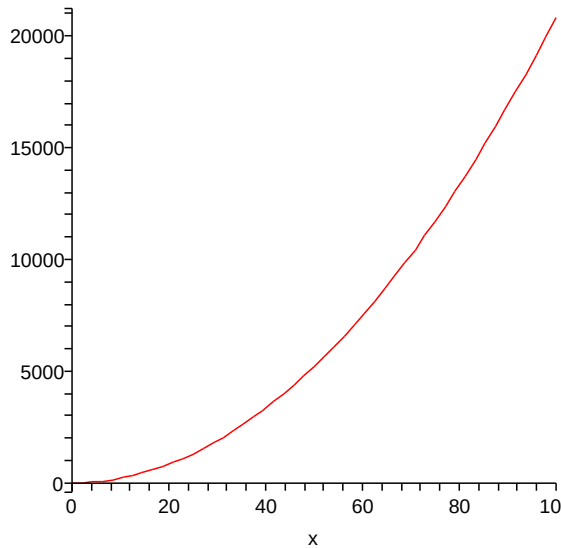

Рис. 3. Коэффициент расширения поля (вертикальная ось), длины бит (горизонтальная ось).

Следует заметить, что оперирование в полях со столь большим расширением невозможно для современных требований криптографии (где требуется скорость и возможность работы всей системы в режиме реального времени). Исходя из вышесказанного, преимуще-

ство использования эллиптических кривых очевидно. Мы получаем серьезный уровень криптографической безопасности пользуясь ключами существенно меньшей длины, чем могли бы пользоваться оставшись в рамках конечных полей и их расширений.

Ниже приведем выводы касающиеся соотношений длин ключей в стандартных системах. Стоит отметить, что согласно ГОСТ 34.11–94 длина ключа в DLP системах, подобных системе Эль-Гамаля, полагается равной 512 бит. При одинаковом уровне криптографической стойкости при переходе на эллиптические кривые длина ключа составляет около 100 бит.

Название криптосистемы:	Длина ключа в случае DLP:	Длина ключа в случае ECDLP:
система Эль-Гамаля	512 бит	112 бит
система Месси–Омуры	512 бит	112 бит
система Диффи–Хеллмана	512 бит	112 бит
система Эль-Гамаля	1024 бит	152 бит
система Месси–Омуры	1024 бит	152 бит
система Диффи–Хеллмана	1024 бит	152 бит
система Эль-Гамаля	2048 бит	206 бит
система Месси–Омуры	2048 бит	206 бит
система Диффи–Хеллмана	2048 бит	206 бит

Принимая во внимание стандарт на цифровую подпись DSA (RSA) приведем выигрыш при переходе на эллиптические кривые (ECDSA ГОСТ 34.10–2001) в этом случае.

Система на основе эллиптической кривой ECDSA:	Система на основе RSA/DSA
106 бит	512 бит
132 бит	768 бит
160 бит	1024 бит
224 бит	2048 бит

Как мы видим из последней таблицы 1024 битная схема цифровой подписи DSA может быть легко заменена на 160 битную схему электронной цифровой подписи на эллиптических кривых ECDSA. При этом происходит серьезное уменьшение размеров ключа.

Производительность вычислительных устройств с недавнего времени принято оценивать в MIPS (Million Instruction Per Second): 1 MIPS = 10^6 опер./с. MIPS год по сути характеризует сложность алгоритма, которая требует годовой работы компьютера чтобы вскрыть соответствующий шифр. По отношению к эллиптическим кривым производительность 1 MIPS соответствует примерно $4 * 10^4$ операций сложения кривой в секунду, поскольку длина ключа существенно превышает длину единицы данных. Устойчивость алгоритмов криптографии принято оценивать в MIPS годах. Иначе говоря, устойчивость — это число лет непрерывной работы, необходимое вычислителю с производительностью 1 MIPS, чтобы взломать данный шифр. В связи с этим представляется целесообразным привести MIPS характеристики в последнем случае.

Время на взлом MIPS лет	Размер ключа RSA/DSA	Размер ключа ECC	Отношение длин ключей RSA/DSA vs ECC
10^4	512 бит	106 бит	5:1
10^8	768 бит	132 бит	6:1
10^{11}	1024 бит	160 бит	7:1
10^{20}	2048 бит	210 бит	10:1

Список литературы

[1] Кудрявцев В. Б., Алешин С. В., Подколзин А. С. Введение в теорию автоматов. М.: Наука, 1985.

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

[3] Прасолов В. В., Соловьев Ю. П. Эллиптические функции и алгебраические уравнения. Изд-во «Факториал», 1997.

[4] Коблиц Н. Курс теории чисел и криптографии. Изд-во «ТВП», 2001.

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

[6] Koblitz N., Menezis A., Vanstone S. The State of Elliptic Curve Cryptography. 2000.

[7] Secure Hash Standard. FIBS PUB 180–1. 1993. May, 11.

[8] Schoof R. Ellitic curves over finite fields and computation of square roots. Vol. 44. No. 170. P. 283–494. Apr. 1985.

[9] Schoof R. Counting points on elliptic curves over finite fields. 1995.

[10] Kiyomichi A., Takakazu S., Shinji M. Overview of curva cryptography.

[11] Нечаев В. И. Элементы криптографии: основы теории защиты информации. Изд-во «Высшая школа», 1999.

[12] Винберг Э. Б. Курс алгебры. Изд-во «Факториал Пресс», 2002.

[13] Курош А. Г. Курс высшей алгебры. 2003.

[14] Виноградов И. М. Основы теории чисел. Гос. изд-во технико-теоретической литературы, 1952г.

[15] Koblitz N. Elliptic curve cryptosistems // Mathematics of Computation. 48 (1987). P. 203–204.

[16] Miller V. Uses of elliptic curves in cryptography // Advances in Cryptology: Proceedings of Crypto'85. Lecture Notes in Computer Science. 218 (1986). Springer-Verlag. P. 417–426.