Криптопреобразования в группах точек эллиптических кривых

Лекция

Ревизия: 0.1

Последняя модификация: Vlad Kovtun

Дата последней модификации: 31.01.2011 21:25:00

История изменений

29.03.2009 – Версия 0.1. Первичный документ. Владислав Ковтун

Содержание

Лекция 5. Криптопреобразования в группах точек эллиптических кривых. Часть 2

Вопросы

1. Группы. Кольца. Конечные поля.
2. Эллиптическая кривая. Представления кривых.
3. Метрика операций на ЭК.
4. Примеры.

Краткое отступление

Группой называется алгебраическая система $\langle G,\circ\rangle$, в которую входит некоторое множество G, а также одна бинарная операция $\circ$, которая удовлетворяет следующим условиям:

- Замкнутость: $\forall\, x, y \in G$, $\exists\, z = x \circ y$, верно $z \in G$.
- Ассоциативность: $\forall\, x, y, z \in G$, верно $(x \circ y) \circ z = x \circ (y \circ z)$.
- Существует нейтральный элемент: $\exists\, e \in G$, $\forall x \in G$, верно $x \circ e = e \circ x = x$.
- Существует обратный элемент: $\exists\, y \in G$, $\forall x \in G$, верно $x \circ y = y \circ x = e$.

Абелева группа, в дополнение удовлетворяет условию:

- Коммутативность: $\forall\, x, y \in G$, верно $x \circ y = y \circ x$.

Конечным полем называется алгебраическая система $\langle F, +, \times\rangle$, которая состоит из конечного множества F и двух бинарных операций $+$ и $\times$, удовлетворяющим следующим условиям:

- $\langle F, +\rangle$ является Абелевой группой.
- $\langle F \setminus \{0\}, \times\rangle$ является группой.
- Дистрибутивность: $\forall\, x, y, z \in F$ верно $x \times (y + z) = (x \times y) + (x \times z)$ и $(x + y) \times z = (x \times z) + (y \times z)$.

Порядком $\mathrm{ord}(F)$ поля F, называется число элементов в поле (во множестве F).

Фундаментальным является следующее условие: конечное поле порядка $q = \mathrm{ord}(F)$ существует, тогда и только тогда, когда число q является простым, такое поле обозначается $\mathbf{F}_q$ или $\mathbf{GF}(q)$.

В криптографии широкое распространение получили поля $\mathbf{GF}(p)$, p - простое и их расширения $\mathbf{GF}(p^m)$. Расширенные поля в свою очередь делятся по характеристике на $\mathbf{GF}(2^m)$ и $\mathbf{GF}((2^m - c)^n)$ с характеристикой в виде псевдо Мерсеновых чисел. По степени расширения: на $\mathbf{GF}(2^m)$, m - простое и композитные $\mathbf{GF}((2^m)^n)$. Также следует выделить простые поля с характеристикой в виде псевдо Мерсеновых чисел и обобщенных Мерсеновых чисел. Каждый из приведенных полей нашли свое применение в криптографии, т.к. являются предпочтительными при реализации на различных платформах.

Одним из наиболее интересных полей, считается Optimal Extension Field (OEF), по причине высокопроизводительной арифметики. На рис. 1 приводится, некоторая, классификация.

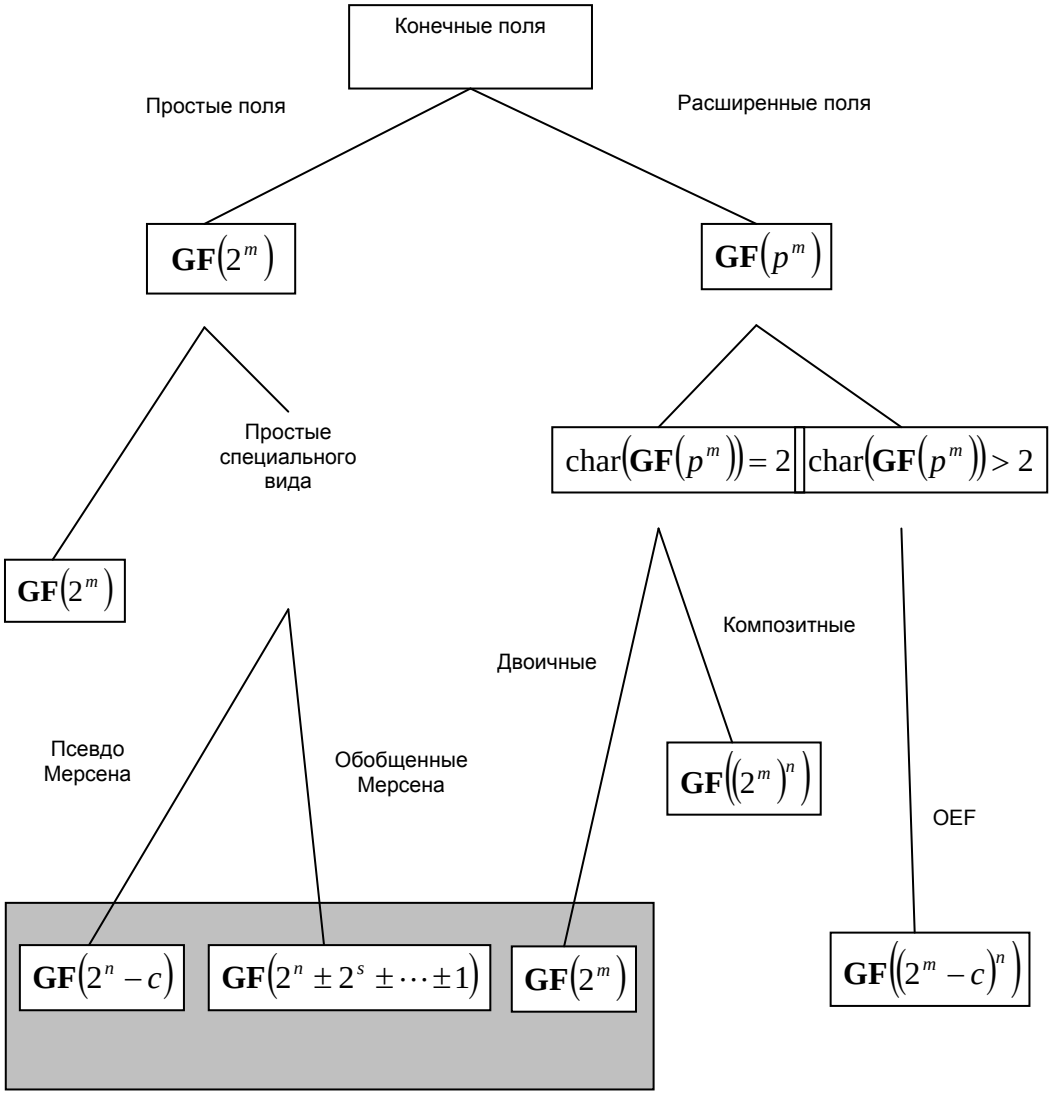


Рис. 1. Конечные поля, которые предлагаются для использования в криптографических приложениях

Отдельно стоит остановиться на представлении элементов поля. Как правило, поля чисел $\mathbf{GF}(p)$ представляются двоичным вектором (массив машинных слов двоичной длиной W): $b_{l-1}2^{l-1}+b_{l-2}2^{l-2}+\cdots+b_1 2^1+b_0=a_{n-1}2^{(n-1)W}+a_{n-2}2^{(n-2)W}+\cdots+a_1 2^W+a_0$, где $n=\lceil \frac{l}{W} \rceil$ - число машинных слов необходимых для представления числа двоичной длины l; b_i - двоичные коэффициенты; a_j - машинные слова.

Аналогичное представление используется и для элементов расширенных полей $\mathbf{GF}(p^m)$, в частности для двоичных полей, где $p=2$ полином может быть представлен:

- В полиномиальном базисе: посредством задания неприводимого полинома $p(t)$ степени l. Любой элемент поля может быть представлен $b_{l-1}x^{l-1}+b_{l-2}x^{l-2}+\cdots+b_1x^1+b_0=a_{n-1}2^{(n-1)W}+a_{n-2}2^{(n-2)W}+\cdots+a_1 2^W+a_0$, $n=\lceil \frac{l}{W} \rceil$ - число машинных слов необходимых для представления числа двоичной длины l; b_i - двоичные коэффициенты у полнома; a_j - машинные слова.
- В нормальном базисе (оптимальном нормальном базисе): посредством задания нормального полинома $p(t)$ степени l. Любой элемент поля может быть представлен $b_{l-1}\Theta^{2^{l-1}}+b_{l-2}\Theta^{2^{l-2}}+\cdots+b_1\Theta^{2^1}+b_0=a_{n-1}2^{(n-1)W}+a_{n-2}2^{(n-2)W}+\cdots+a_1 2^W+a_0$, $n=\lceil \frac{l}{W} \rceil$ - число машинных слов необходимых для представления числа двоичной длины l; b_i - двоичные коэффициенты у полнома; Θ - является корнем полинома $p(t)$; a_j - машинные слова

Простые поля. Рассмотрение начнем с простых полей, модуль которых является псевдо-Мерсеновыми и обобщенными Мерсеновыми числами вида $p = \beta^t - c$, где c - небольшое целое.

В таблице 1 приведем сложности операции приведения по известным простым модулям в операциях процессора.

Таблица 1. Теоретические оценки сложности операции приведения по известным простым модулям в операциях процессора

№	Модуль	Сложность в полевых операциях	Сложность в операциях процессора
1	Псевдо-Мерсеново число общего вида, $p = \beta^t - c$		$(tl + l^2)M_{CPU}$, t - двоичная длина модуля p, причем $l = \log_2 c \le \frac{t}{2}$, k - двоичная длина числа, которое приводится
2	Псевдо-Мерсеново число общего вида, $p = \beta^t - c$, когда c размещается в одном машинном слове		$(t+1)M_{CPU}$, t - двоичная длина модуля p, причем $l = \log_2 c \le \frac{t}{2}$, k - двоичная длина числа, которое приводится
3	Псевдо-Мерсеново число $p = 2^{192} - 2^{64} - 1$	$2A_{F_p}$	$12A_{CPU}$, $W = 32$
4	Псевдо-Мерсеново число $p = 2^{224} - 2^{96} + 1$	$7A_{F_p}$	$49A_{CPU}$, $W = 32$
5	Псевдо-Мерсеново число $p = 2^{256} - 2^{224} + 2^{192} + 2^{96} - 1$	$15A_{F_p}$	$120A_{CPU}$, $W = 32$
6	Псевдо-Мерсеново число $p = 2^{384} - 2^{128} - 2^{96} + 2^{32} - 1$	$15A_{F_p}$	$180A_{CPU}$, $W = 32$
7	Псевдо-Мерсеново число $p = 2^{521} - 1$	$\frac{3}{2}A_{F_p} + 17X_{CPU} + 33Sh_{CPU}$	$25{,}5A_{CPU} + 17X_{CPU} + 33Sh_{CPU}$, $W = 32$
8	Сложение, без приведения по модулю		kA_{CPU}
9	Вычитание, без приведения по модулю		kA_{CPU}
10	Умножение Montgomery [17], без приведения по модулю		$(2k^3 + 2k)M_{CPU} + (4k^2 + 6k + 2)A_{CPU}$
11	Умножение КСМ [17], без приведения по модулю		$(k^2 + k + X_1)M_{CPU} + (2k^2 + 4k + 1 + X_2)A_{CPU}$
12	Умножение [22], без приведения по модулю		$(k(k-1) + t)(3A_{CPU} + M_{CPU})$
13	Возведение в квадрат [22], без приведения по модулю		$(k(2k-1) + t)(4A_{CPU} + \frac{1}{2}M_{CPU})$

Далее рассмотрим сложность операции возведения в степень, в таблице 2 приведены интересующие нас аналитические выражения.

Таблица 2. Теоретические оценки сложности операции возведения в степень в полевых операциях

№	Название	Размер пред-вычислений	Средняя сложность
1	Метод «Возведение в квадрат и умножение»	-	$\frac{1}{2}lM_{F_p} + lS_{F_p}$
2	Метод с фиксированной шириной окна предвычислений	2^{w-1}	$\left(\left\lfloor\frac{l-1}{w}\right\rfloor\left(w+1-2^{-w}\right)+1-2^{-((l-1)\bmod w)}\right)M_{F_p}$
3	Метод с адаптируемой шириной окна (скользяще окно) предвычислений	2^{w-1}	$\left(2^{w-1}+\frac{l}{w+1}+l-w\right)M_{F_p}$
4	Метод Lim-Lee	$v\left(2^h-1\right)$	$\left(\frac{2^h-1}{2^h}a-2\right)M_{F_p}+bS_{F_p}$

Окончательный выбор того или иного алгоритма будет производиться на основе не только теоретической оценки сложности, но и экспериментальной оценки.

Эллиптическая кривая

Эллиптической кривой E над полем k называется гладкая кривая, которая описывается множеством решений $(x, y)\in k^2$ уравнения в обобщенной форме Вейерштрасса:

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,\ a_1, a_2, a_3, a_4, a_6 \in k, \quad (1)$$

и находится в аффинной плоскости $\mathbf{A}^2\left(\bar{k}\right)=\bar{k}\times\bar{k}$ с точкой O на ∞.

Альтернативным, является следующее определение. **Эллиптическая кривая** – гладкая кривая E из $\mathbf{P}^2$ над полем k из семейства кривых из $\mathbf{P}^2$ над полем k, образованных двумя кубиками $x_0x_1x_2=0$ и $x_0^3+x_1^3+x_2^3=0$ в форме Хассе, предложено Фриумом в 2001 году:

$$E_{(a,b)}: ax_0x_1x_2 + b\left(x_0^3 + x_1^3 + x_2^3\right) = 0,\ (a, b)\in \mathbf{P}^1. \quad (2)$$

С точки зрения практической реализации, следует рассматривать конкретные кривые, заданные над полями четной и нечетной характеристики.

Криптография на эллиптических кривых

Точкой отсчета криптографических преобразований на ЭК принято считать доклады Нила Коблица и Виктора Миллера, сделанные ими независимо:

- **N. Koblitz, Elliptic curve cryptosystems, in Mathematics of Computation 48, 1987, pp. 203–209. В университете Вашингтона.**
- **V. Miller, Use of elliptic curves in cryptography, CRYPTO 85, 1985. В компании IBM.**

Основной идеей, которая эксплуатировалась в работах, была особенность, которой обладали точки ЭК – **образовывать группу**. Не сложно провести аналогию между задачей дискретного логарифма в поле чисел (полиномов) и точками ЭК, что бы понять открывшиеся перспективы.

Как было указано ранее, точки ЭК образуют группу по операции сложения, другим словами точки ЭК могут складываться.

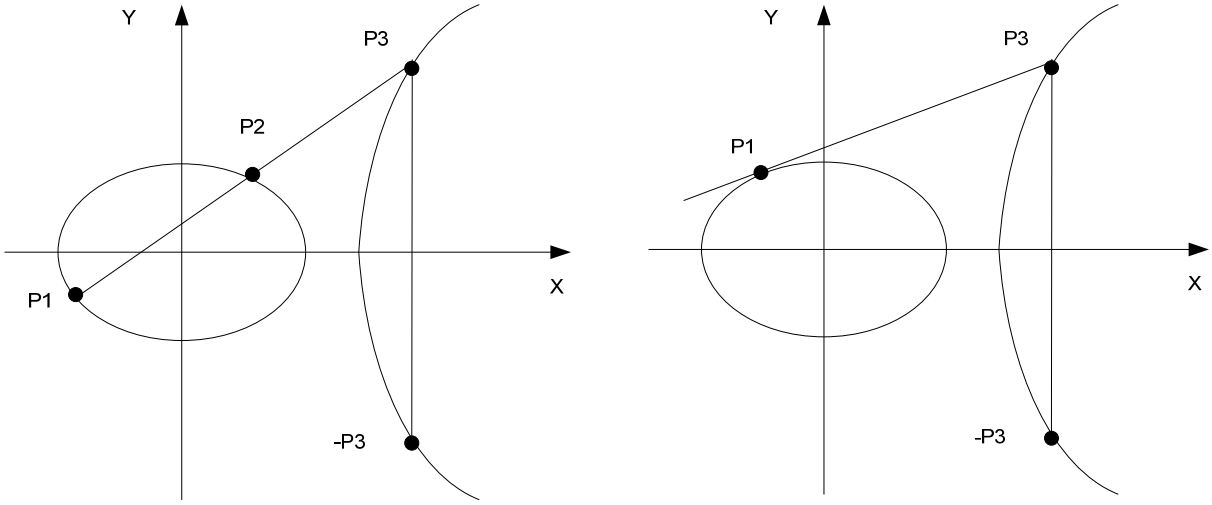
Перечислим основные свойства группового закона:

$$P_1 + P_2 + P_3 = O\,. \tag{15}$$

Другими словами:

$$P_1 + P_2 = -P_3 = P_4\,.$$

На рис. 2 представлена графическая интерпретация такого сложения.



а) графическая интерпретация сложения различных точек

б) графическая интерпретация операции сложения двух одинаковых точек (удвоение)

Рис. 2. Геометрическая интерпретация сложения точек ЭК

На рис. 3 рассмотрим иерархию операций, которые применяются при реализации скалярного умножения точек ЭК.

Рис. 3. Обобщенная иерархия операций при скалярном умножении в группе точек эллиптической кривой

Более подробная иерархия операций при скалярном умножении может быть представлена виде рис. 4.

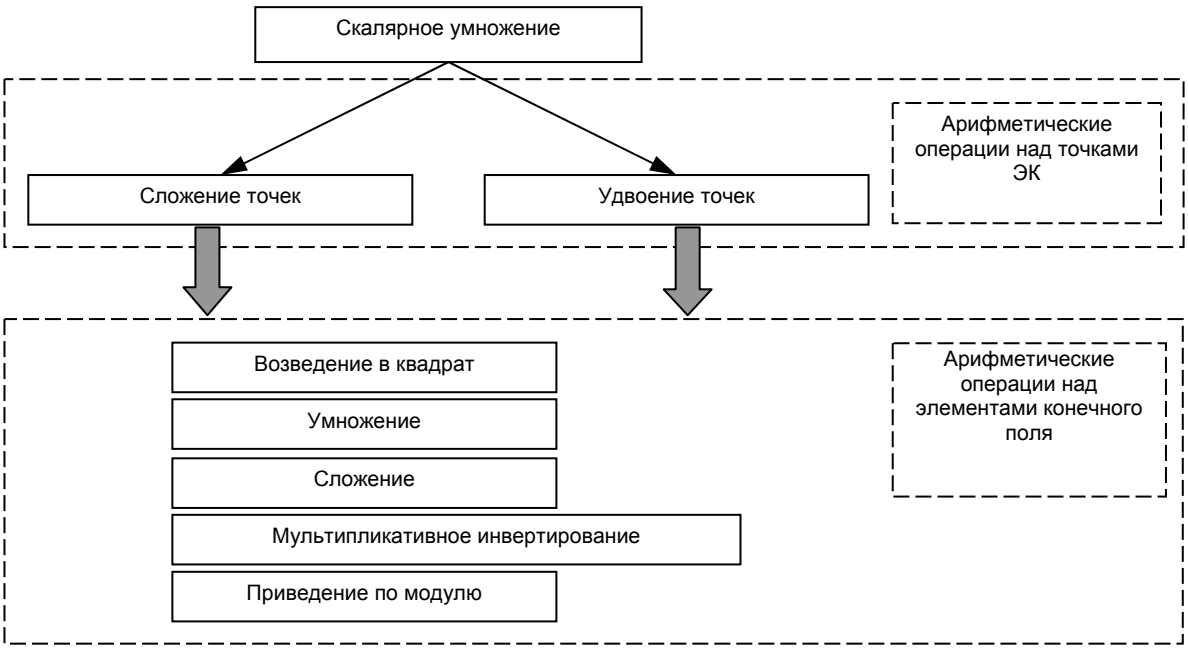


Рис. 4. Иерархия операций используемых для скалярного умножения точек эллиптической кривой

Метрика операций на ЭК

Сложение различных точек

Исходя из графической интерпретации закона сложения точек ЭК, постараемся сформулировать его в терминах координат точек, которые складываются.

$$P_1 = (x_1, y_1),\ P_2 = (x_2, y_2),\ P_3 = (x_3, y_3).$$

$$x_3 = \lambda^2 - x_1 - x_2,\ y_3 = \lambda(x_1 - x_3) - y_1,\ \lambda = \frac{y_2 - y_1}{x_2 - x_1}. \tag{16}$$

Продемонстрируем вывод координат результирующей точки $P_3 = (x_3, y_3)$: основу вывода составляет тот факт, что прямая, которая проходит через точки: P_1, P_2, P_3 и уравнения ЭК E - пересекаются, т.е. имеют общие точки. Другими словами, мы можем сформулировать систему уравнений:

$$\begin{cases} y = \lambda x + c \\ y^2 = x^3 + ax + b \end{cases}.$$

Причем известны 2 корня из 3-х – точки P_1, P_2. Коэффициент λ и c в уравнении кривой легко вычислить, зная точки P_1, P_2: $\lambda = \frac{y_2 - y_1}{x_2 - x_1}$, $c = y_1 - \lambda x_1$ (либо $c = y_2 - \lambda x_2$).

Подставим $y_3 = \lambda x_3 + c$ в уравнение кривой $y_3^2 = x_3^3 + ax_3 + b$. Полученное однородное уравнение может быть представлено $(x - x_1)(x - x_2)(x - x_3) = 0$. Согласно теореме Виета [4]: x_1, x_2, x_3 - корни кубического уравнения $ax^3 + bx^2 + cx + d = 0$, то

$$x_1 + x_2 + x_3 = -\frac{b}{a},\ x_1x_2 + x_1x_3 + x_2x_3 = \frac{c}{a},\ x_1x_2x_3 = -\frac{d}{a}. \quad (17)$$

Можно выразить x_3 через x_1 и x_2: $x_3 = -\frac{b}{a} - x_1 - x_2$, в наших обозначениях:

$$x_3 = \lambda^2 - x_1 - x_2.$$

Подставив в уравнение прямой, полученную координату x_3, можно вычислить y_3:

$$y_3 = \lambda x_3 + c,\ y_3 = \lambda(x_1 - x_3) - y_1.$$

Удвоение

Исходя из графической интерпретации закона удвоения точек ЭК, постараемся сформулировать его в терминах координат точек, которые удваиваются.

$$P_1 = (x_1, y_1),\ P_3 = (x_3, y_3).$$

$$x_3 = \lambda^2 - x_1 - x_2,\ y_3 = \lambda(x_1 - x_3) - y_1,\ \lambda = \frac{3x_1^2 + a}{2y_1}. \quad (16)$$

Продемонстрируем вывод координат результирующей точки $P_3 = (x_3, y_3)$: основу вывода составляет тот факт, что прямая, которая проходит через точки: P_1, P_3 и уравнения ЭК E - пересекаются, т.е. имеют общие точки. Другими словами, мы можем сформулировать систему уравнений:

$$\begin{cases} y = \lambda x + c \\ y^2 = x^3 + ax + b \end{cases}.$$

Причем известны 2 корня (один корень кратности 2) из 3-х – точки P_1. Коэффициент λ и c в уравнении кривой легко вычислить, зная точку P_1. Для этого необходимо вычислить производную обоих уравнений, по x: $2yy' = 3x^2 + a$ и $y' = \lambda$. Значение коэффициента λ в точке x_1, легко вычислить $\lambda = \frac{3x_1^2 + a}{2y_1}$, и свободный член $c = y_1 - \lambda x_1$.

Подставим $y_3 = \lambda x_3 + c$ в уравнение кривой $y_3^2 = x_3^3 + ax_3 + b$. Полученное однородное уравнение может быть представлено $(x - x_1)^2(x - x_3) = 0$. Согласно теореме Виета [4]: x_1, x_3 - корни кубического уравнения $ax^3 + bx^2 + cx + d = 0$, то

$$2x_1 + x_3 = -\frac{b}{a},\ x_1^2 + x_1x_3 + x_1x_3 = \frac{c}{a},\ x_1^2x_3 = -\frac{d}{a}. \quad (17)$$

Можно выразить x_3 через x_1: $x_3 = -\frac{b}{a} - 2x_1$, в наших обозначениях:

$$x_3 = \lambda^2 - 2x_1 .$$

Подставив в уравнение прямой, полученную координату x_3, можно вычислить y_3:

$$y_3 = \lambda x_3 + c ,\ y_3 = \lambda(x_1 - x_3) - y_1 .$$

В случае рассмотрения ЭК над двоичным полем, полученные выражения могут быть упрощены.

Примеры

Пример 1

Пусть имеется ЭК $y^2 = x^3 + x + 1$ над полем $\mathbf{GF}(23)$. Коэффициенты кривой: $a = 1$, $b = 1$ и модуль преобразований $p = 23$.

1. Проверить, что следующие точки: (1,7), (1,16), (3,10), (3,13), (4,0), (5,4), (5,19), (6,4), (6,19), (7,11), (7,12), (9,7), (9,16), (17,3), (17,20), (18,20), (19,5), (13,16) принадлежат ЭК.

2. Зная $P_1 = (3, 10)$, $P_2 = (9, 7)$, следует найти $P_3 = P_1 + P_2$.

Пример 2

Найдем все точки ЭК E: $y^2 = x^3 + x + 6 \bmod 11$.

Порядок ЭК (количество точек) ЭК: $\#E = 13$.

Генератором группы является $\alpha = (2, 7)$, все точки могут быть получены из генератора:

$2\alpha = (2, 7) + (2, 7) = (x_3, y_3).$

$$\lambda = \frac{3x_1^2 + a}{2y_1} = (2 \cdot 7)^{-1}(3 \cdot 4 + 1) = 3^{-1}13 \equiv 4 \cdot 2 \equiv 8 \bmod 11$$

$$x_3 = \lambda^2 - x_1 - x_2 = 60 \equiv 5 \bmod 11$$

$$y_3 = \lambda(x_1 - x_3) - y_1 = 8(2 - 5) - 7 = -24 - 7 = -31 \equiv 2 \bmod 11$$

$2\alpha = (2, 7) + (2, 7) = (5, 2)$

$3\alpha = 2\alpha + \alpha = (5, 2) + (2, 7) = \ldots$

…

$12\alpha = 11\alpha + \alpha = (2, 4)$

$13\alpha = 12\alpha + \alpha = (2, 4) + (2, 7) = (2, 4) + (2, -4) = O$

$14\alpha = 13\alpha + \alpha = O + (2, 7) = (2, 7)$

…

Все 12 ненулевых элементов, вместе с точкой на бесконечности, формируют циклическую группу.

Литература

1. Криптографическая защита информации в АСУ СН. Курс лекций. В.И. Долгов. ХВУ. 1998.

2. Криптографическая защита информации в информационных системах. Курс лекций. И.Д. Горбенко. ХНУРЭ. 2002.

3. Криптопреобразования с открытым ключом. Текущее состояние. Обзор. В.Ю. Ковтун. 2006.

4. Теорема Виета для представления коэффициентов многочлена через его корни. http://ru.wikipedia.org/wiki/Формулы_виета

5. Ковтун В.Ю. Криптография с открытым ключом. http://www.nrjetix.com/fileadmin/doc/publications/additional_info/public_key_cryptography_-_lecture.pdf

6. Таня Ланге. База арифметических операций в группе точек ЭК. http://www.hyperelliptic.org/EFD/

7. http://ru.wikipedia.org/wiki/Однородные_координаты