УДК 681.3.06:519.248.681

С.И. ЗБИТНЕВ

ПРОЕКТИВНАЯ ГЕОМЕТРИЯ – НЕ ВСЕ ТАК ГЛАДКО

Введение

По современным взглядам разрешение ряда противоречий несимметричной криптографии может быть осуществлено за счет использования криптографических преобразований в группах точек эллиптической кривой [15]. Если эллиптическая кривая (ЭК) удовлетворяет условию MOV [1,2] и FR-условию [3] и свободна от p-делителя над F_{p^r} [4,5,6], то для криптопреобразований в группах точек ЭК известны три атаки на дискретный логарифм в группах точек ЭК – методы ρ-Полларда[7,8], Полига-Хелмана [9] и малых – больших шагов [9, 17]. Криптосистемы на основе эллиптических кривых с длиной ключа 160 бит имеет одинаковую стойкость с криптосистемами ElGamal и RSA с длиной ключа 1024 бита [16]. По этой причине криптосистемы на ЭК обсуждались в ISO/IEC CD 14883-3, ISO/IEC DIS 11770-3, ANSI ASC X.9.63, X.9.62, IEEE p1363 [2], ГОСТ-34.2001 РФ и NESSIE и в настоящее время получили развитие.

Несмотря на уменьшения длины блока преобразования, основные операции в группах точек ЭК требуют значительных вычислительных затрат. Поэтому важным является уменьшение вычислительной сложности преобразований в группах точек ЭК. Наиболее распространенными методами уменьшения вычислительной сложности являются:

- Использование специфических кривых, в которых в ущерб стойкости мы достигаем существенного повышения быстродействия [18,19,20];
- Использование эллиптических кривых, определенных над F_q. При программной реализации достигается максимальная производительность, если $q = p$, а при $q = 2^m$ достигается существенное ускорение аппаратной реализации криптопреобразования [2];
- Использование различных базисов представления элементов поля для $E(F_{2^m})$. Полиномиальное представление эффективней при программной реализации преобразований на ЭК, а нормальный базис Гауса предпочтительней при аппаратной реализации [2];
- Различное представление точек на ЭК [2,10-14].

Последний способ позволяет повысить производительность на порядок, без ущерба безопасности криптосистем, и поэтому, возможно, является основным в решении задач уменьшения сложности преобразований в группе точек ЭК.

Целью настоящей статьи является проведение сравнительного анализа вычислительной сложности операций сложения в группах точек ЭК в различных известных координатных базисах, а также определение основных ограничений и условий применения различных координатных базисов при выполнение криптографических преобразований в группах точек эллиптических кривых.

1. Представление точек на эллиптической кривой

Точка на эллиптической кривой может быть представлена в нескольких координатных базисах. Основными из них являются аффинные координаты [10], проективные координаты [11], якобиановые координаты [12,13], координаты Чудновского(Chudnovsky Jacobian) [12] и модифицированные якобиановые координаты [14].

Метрика сложения в аффинных координатах [10]. Пусть

$$E: y^2 = x^3 + ax + b\left(a, b \in \mathrm{F}_p, 4a^3 + 27b^2 \neq 0\right) - \tag{1}$$

уравнение эллиптической кривой E над F_p. Пусть даны точки $P_1 = (x_1, y_1) \in E(\mathrm{F}_p)$ и $P_2 = (x_2, y_2) \in E(\mathrm{F}_p)$, тогда суммой двух точек P_1 и P_2 называется точка $P_3 \in E(\mathrm{F}_p)$, такая что $P_3 = P_1 + P_2 = (x_3, y_3)$. Если $P_1 \neq P_2$, то координаты точки $P_3 = (x_3, y_3) = P_1 + P_2 = (x_1, y_1) + (x_2, y_2)$ образуются как в [10]

$$x_3 = \lambda^2 - x_1 - x_2 \pmod p,\ y_3 = \lambda(x_1 - x_3) - y_1 \pmod p, \tag{2}$$

где $\lambda = (y_2 - y_1)/(x_2 - x_1) \pmod p$.

Если $P_1 = P_2$, то операцию $P_1 + P_2$ называют удвоением и вычисляется как $P_3 = (x_3, y_3) = 2P_1 = 2(x_1, y_1)$, причем

$$x_3 = \lambda^2 - 2x_1 \pmod p,\ y^3 = \lambda(x_1 - x_3) - y_1 \pmod p, \tag{3}$$

где $\lambda = (3x_1^2 + a)/(2y_1) \pmod p$.

Для дальнейшего сравнения сложности операций сложения и удвоения введем переменные $t(B+B)$ и $t(2B)$, сложение и удвоение точек соответственно, где B – координатный базис. Сложность операций сложения и удвоения выражаются в количестве умножений (M), возведение в квадрат (S) и инверсий (I), операция суммирования игнорируется в силу незначительной сложности. В результате получим, что $t(A+A) = I + 2M + S$ и $t(2A) = I + 2M + 2S$, где A – аффинный базис представления точки на ЭК.

Проведенный анализ показал, что при программной реализации $I \in [9M, 30M]$ и $S \approx 0.8M$.

Метрика сложения в проективных координатах [11]. Для проективных координат $x = X/Z$ и $y = Y/Z$, а уравнение ЭК имеет вид:

$$E_P: Y^2Z = X^3 + aXZ^2 + bZ^3. \tag{4}$$

Пусть даны точки $P_1 = (X_1, Y_1, Z_1) \in E_P(\mathrm{F}_p)$ и $P_2 = (X_2, Y_2, Z_2) \in E_P(\mathrm{F}_p)$, тогда суммой двух точек P_1 и P_2 называется точка $P_3 \in E_P(\mathrm{F}_p)$ такая, что $P_3 = P_1 + P_2 = (X_3, Y_3, Z_3)$. Если $P_1 \neq P_2$, то координаты точки $P_3 = (X_3, Y_3, Z_3) = P_1 + P_2 = (X_1, Y_1, Z_1) + (X_2, Y_2, Z_2)$ образуются как в [11]

$$X_3 = vA \pmod p,\ Y_3 = u\left(v^2X_1Z_2 - A\right) - v^3Y_1Z_2 \pmod p,\ Z_3 = v^3Z_1Z_2 \pmod p, \tag{5}$$

где $u = Y_2Z_1 - Y_1Z_2 \pmod p$; $v = X_2Z_1 - X_1Z_2 \pmod p$; $A = u^2Z_1Z_2 - v^3 - 2v^2X_1Z_2 \pmod p$.

Если $P_1 = P_2$, то операцию $P_1 + P_2$ называют удвоением и $P_3 = (X_3, Y_3, Z_3) = 2P_1 = 2(X_1, Y_1, Z_1)$, причем [11]

$$X_3 = 2hs \pmod p,\ Y_3 = w(4B - h) - 8Y_1^2s^2 \pmod p,\ Z_3 = 8s^3 \pmod p, \tag{6}$$

где $w = aZ_1^2 + 3X_1^2 \pmod p$; $s = Y_1Z_1 \pmod p$; $B = X_1Y_1s \pmod p$; $h = w^2 - 8B \pmod p$.

Время выполнения операции сложения $t(P+P) = 12M + 2S$ и удвоения $t(2P) = 7M + 5S$, где P обозначает проективное представление точки.

Метрика сложения в якобиановых координатах [12,13]. Для якобиановых координат $x = X/Z^2$ и $y = Y/Z^3$, а уравнение ЭК имеет вид:

$$E_J : Y^2 = X^3 + aXZ^4 + bZ^6. \tag{7}$$

Пусть даны точки $P_1 = (X_1, Y_1, Z_1) \in E_J(\mathrm{F}_p)$ и $P_2 = (X_2, Y_2, Z_2) \in E_J(\mathrm{F}_p)$, тогда суммой двух точек P_1 и P_2 называется точка $P_3 \in E_J(\mathrm{F}_p)$ такая, что $P_3 = P_1 + P_2 = (X_3, Y_3, Z_3)$. Если $P_1 \neq P_2$, то координаты точки $P_3 = (X_3, Y_3, Z_3) = P_1 + P_2 = (X_1, Y_1, Z_1) + (X_2, Y_2, Z_2)$ образуются как в [12, 13]

$$X_3 = -H^3 - 2U_1H^2 + r^2 \pmod p,\ Y_3 = -S_1H^3 + r(U_1H^2 - X_3) \pmod p,\ Z_3 = Z_1Z_2H \pmod p, \tag{8}$$

где $U_1 = X_1Z_2^2 \pmod p$, $U_2 = X_2Z_1^2 \pmod p$, $S_1 = Y_1Z_2^3 \pmod p$, $S_2 = Y_2Z_1^3 \pmod p$, $H = U_2 - U_1 \pmod p$, $r = S_2 - S_1 \pmod p$.

Если $P_1 = P_2$, то операцию $P_1 + P_2$ называют удвоением и $P_3 = (X_3, Y_3, Z_3) = 2P_1 = 2(X_1, Y_1, Z_1)$, причем

$$X_3 = T \pmod p,\ Y_3 = -8Y_1^4 + M(S - T) \pmod p,\ Z_3 = 2Y_1Z_1 \pmod p, \tag{9}$$

где $S = 4X_1Y_1^2 \pmod p$; $M = 3X_1^2 + aZ_1^4 \pmod p$; $T = -2S + M^2 \pmod p$.

Время выполнения составляет $t(J+J) = 12M + 4S$ и $t(2J) = 4M + 6S$, где J обозначает якобиановое представление точки.

Метрика сложения в координатах Чудновского [12]. Для координат Чудновского $x = X/Z^2$ и $y = Y/Z^3$, а уравнение ЭК имеет вид:

$$E_{J^c} : Y^2 = X^3 + aXZ^4 + bZ^6. \tag{10}$$

Пусть даны точки $P_1 = (X_1, Y_1, Z_1, Z_1^2, Z_1^3) \in E_{J^c}(\mathrm{F}_p)$ и $P_2 = (X_2, Y_2, Z_2, Z_2^2, Z_2^3) \in E_{J^c}(\mathrm{F}_p)$, тогда суммой двух точек P_1 и P_2, называется точка $P_3 \in E_{J^c}(\mathrm{F}_p)$ такая, что $P_3 = P_1 + P_2 = (X_3, Y_3, Z_3, Z_3^2, Z_3^3)$. Если $P_1 \neq P_2$, то координаты точки $P_3 = (X_3, Y_3, Z_3, Z_3^2, Z_3^3) = P_1 + P_2 = (X_1, Y_1, Z_1, Z_1^2, Z_1^3) + (X_2, Y_2, Z_2, Z_2^2, Z_2^3)$ образуются как в [12]

$$X_3 = -H^3 - 2U_1H_2 + r^2 \pmod p,\ Y_3 = -S_1H^3 + r(U_1H^2 - X_3) \pmod p,\ Z_3 = Z_1Z_2H \pmod p,$$

$$Z_3^2 = Z_3^2 \pmod p,\ Z_3^3 = Z_3^3 \pmod p, \tag{11}$$

где $U_1 = X_1(Z_2^2) \pmod p$; $U_2 = X_2(Z_1^2) \pmod p$; $S_1 = Y_1(Z_2^3) \pmod p$; $S_2 = Y_2(Z_1^3) \pmod p$; $H = U_2 - U_1 \pmod p$; $r = S_2 - S_1 \pmod p$.

Если $P_1 = P_2$, то операцию $P_1 + P_2$ называют удвоением и $P_3 = \left(X_3, Y_3, Z_3, Z_3^2, Z_3^3\right) = 2P_1 = 2\left(X_1, Y_1, Z_1, Z_1^2, Z_1^3\right)$, причем:

$$X_3 = T \pmod p,\ Y_3 = -8Y_1^4 + M(S-T) \pmod p,\ Z_3 = 2Y_1Z_1 \pmod p,\ Z_3^2 = Z_3^2 \pmod p,$$

$$Z_3^3 = Z_3^3 \pmod p, \tag{12}$$

где $S = 4X_1Y_1^2 \pmod p$; $M = 3X_1^2 + a\left(Z_1^2\right)^2 \pmod p$; $T = -2S + M^2 \pmod p$.

Время выполнения составляет $t\left(J^c + J^c\right) = 11M + 3S$ и $t\left(2J^c\right) = 5M + 6S$, где J^c обозначает представление точки в координатах Чудновского.

Метрика сложения в модифицированных якобиановых координатах [14]. Для модифицированных якобиановых координат $x = X/Z^2$ и $y = Y/Z^3$, а уравнение ЭК имеет вид:

$$E_{J^m} : Y^2 = X^3 + aXZ^4 + bZ^6. \tag{13}$$

Пусть даны две точки $P_1 = \left(X_1, Y_1, Z_1, aZ_1^4\right) \in E_{J^m}\left(\mathrm{F}_p\right)$ и $P_2 = \left(X_2, Y_2, Z_2, aZ_2^4\right) \in E_{J^m}\left(\mathrm{F}_p\right)$, тогда суммой двух точек P_1 и P_2 называется точка $P_3 \in E_{J^m}\left(\mathrm{F}_p\right)$ такая, что $P_3 = P_1 + P_2 = \left(X_3, Y_3, Z_3, aZ_3^4\right)$. Если $P_1 \neq P_2$, то координаты точки $P_3 = \left(X_3, Y_3, Z_3, aZ_3^4\right) = P_1 + P_2 = \left(X_1, Y_1, Z_1, aZ_1^4\right) + \left(X_2, Y_2, Z_2, aZ_2^4\right)$ образуются как в [14]:

$$X_3 = -H_3 - 2U_1H^2 + r^2 \pmod p,\ Y_3 = -S_1H^3 + r(U_1H^2 - X_3) \pmod p,\ Z_3 = Z_1Z_2H \pmod p,$$

$$aZ_3^4 = aZ_3^4 \pmod p, \tag{14}$$

где $U_1 = X_1Z_2^2 \pmod p$; $U_2 = X_2Z_1^2 \pmod p$; $S_1 = Y_1Z_2^3 \pmod p$; $S_2 = Y_2Z_1^3 \pmod p$; $H = U_2 - U_1 \pmod p$; $r = S_2 - S_1 \pmod p$.

Если $P_1 = P_2$, то операцию $P_1 + P_2$ называют удвоением и $P_3 = \left(X_3, Y_3, Z_3, aZ_3^4\right) = 2P_1 = 2\left(X_1, Y_1, Z_1, aZ_1^4,\right)$, причем:

$$X_3 = T \pmod p,\ Y_3 = M(S-T) - U \pmod p,\ Z_3 = 2Y_1Z_1 \pmod p,\ aZ_3^4 = 2U\left(aZ_1^4\right) \pmod p, \tag{15}$$

где $S = 4X_1Y_1^2 \pmod p$, $U = 8Y_1^4 \pmod p$, $M = 3X_1^2 + \left(aZ_1^4\right) \pmod p$, $T = -2S + M^2 \pmod p$.

Время выполнения составляет $t\left(J^m + J^m\right) = 13M + 6S$ и $t\left(2J^m\right) = 4M + 4S$, где J^m обозначает представление точки в модифицированных якобиановых координатах.

Анализируя время выполнения каждого алгоритма, однозначно видно неэффективность применения "чистых" аффинных координат в криптопреобразования в группах точек ЭК. Что касается проективных, якобиановых, координат Чудновского и модифицированных якобиановых координат, то тут нет явного лидера, некоторые координатные базисы выигрывают при удвоении точки, но проигрывают при сложении, некоторые наоборот.

2. Сложность и особенности выполнения преобразований в проективных координатах

Пусть дана эллиптическая кривая E над F_q, коэффициенты уравнения ЭК $a,b \in \mathrm{F}_q$, порядок ЭК $\#E(\mathrm{F}_q)$, базовая точка $G \in E(\mathrm{F}_q)$, порядок базовой точки n ($nG = \mathrm{O}$) и секретный ключ d. В криптосистемах, основанных на эллиптических кривых, основной операцией является скалярное умножение, т.е. выполняется операции умножения большого целого числа d на базовую точку G с координатами $X,Y,Z \in \mathrm{F}_q$. В результате вычисляется открытый ключ Q, представляющий собой для $E(\mathrm{F}_{2^m})$ точку на ЭК.

$$Q = d \cdot G(\mathrm{mod}\, f(x),\ 2) \text{ для } q = 2^m, \tag{16}$$

$$Q = d \cdot G(\mathrm{mod}\, p) \text{ для } q = p, \tag{17}$$

где $f(x)$ – примитивный полином степени m над полем F_2.

Значение Q вычисляется посредством многократного выполнения операций сложения и удвоения, одна из реализаций алгоритма скалярного умножение приведена ниже.

Вход: большое целое число d и точка на эллиптической кривой G.

Выход: точка на эллиптической кривой $Q = d \cdot G(\mathrm{mod}\, f(x),\ 2)$.

1. Если $d = 0$, выдать O и остановить алгоритм.

2.Если $d < 0$, установить $R \leftarrow (-G)$ и $k \leftarrow (-d)$, иначе $R \leftarrow G$ и $k \leftarrow d$.

3. Пусть $h_l h_{l-1} \ldots h_1 h_0$ - бинарное представление числа $3k$, где самый крайний бит h_l равняется 1.

4. Пусть $k_l k_{l-1} \ldots k_1 k_0$ - бинарное представление числа k.

5. Установить $S \leftarrow R$.

6. Цикл i от $l-1$ до 1 делать:

6.1. Установить $S \leftarrow 2S$.

6.2. Если $h_i = 1$ и $k_i = 0$, вычислить $S \leftarrow S + R$

6.2. Если $h_i = 0$ и $k_i = 1$, вычислить $S \leftarrow S + (-R)$

7. Выдать результат S.

После нахождения Q в проективных координатах значение этой точки необходимо преобразовать в аффинные координаты. Эта операция выполняется один раз в конце скалярного умножения.

Из пункта 6.1 алгоритма скалярного умножения следует, что количество удвоений точки зависит от длины множителя, то есть удвоение производиться $l-2$ раз. По теории вероятности в случайном числе распределение битов 1 и 0 равновероятностное, следовательно, количество единиц в случайном числе приблизительно $l/2$, следовательно, и количество пар $h_i = 1$, $k_i = 0$ и $h_i = 0$, $k_i = 1$ приблизительно $l/2$. Этот факт дает возможность утверждать, что количество удвоений точки выполняется приблизительно в два раза чаще, чем сложение в группе точек ЭК.

Для построения криптосистем на основе ЭК предпочтительным является использование представления точек в модифицированных якобиановых координатах, так как они обеспечивают минимизацию сложности операции удвоения точки на ЭК. Но при большом количестве единиц в бинарном представлении множителя необходимо использовать более сбалансированное представление координат – якобианово представление (ниже все примеры

приведены в якобиановом и аффинном представлениях точки над расширенным полем Галуа).

Использование одного координатного базиса не всегда позволяет достичь максимальной производительности. Перспективным направлением является использование смешанных координат. К примеру, на этапах 6.2 и 6.3 алгоритма скалярного умножения сложность суммирования в модифицированных координатах составляет $t\left(J^m + J^m\right) = 13M + 6S$. Если перед выполнением алгоритма скалярного умножения представить точки R и $-R$ в аффинном базисе, мы получим суммирование в смешанных координатах и сложность такой операции составляет $t\left(J^m + A\right) = 9M + 5S$, при условии представления результата в базисе J^m. В табл. 1 приведены всевозможное использование смешанных координат и их сложность.

Таблица 1

Удвоение		Сложение	
Операция	Временные затраты	Операция	Временные затраты
$t(2P)$	$7M + 5S$	$t\left(J^m + J^m\right)$	$13M + 6S$
$t\left(2J^c\right)$	$5M + 6S$	$t\left(J^m + J^c = J^m\right)$	$12M + 5S$
$t(2J)$	$4M + 6S$	$t\left(J + J^c = J^m\right)$	$12M + 5S$
$t\left(2J^m = J^c\right)$	$4M + 5S$	$t(J + J)$	$12M + 4S$
$t\left(2J^m\right)$	$4M + 4S$	$t(P + P)$	$12M + 2S$
$t\left(2A = J^c\right)$	$3M + 5S$	$t\left(J^c + J^c = J^m\right)$	$11M + 4S$
$t\left(2J^m = J\right)$	$3M + 4S$	$t\left(J^c + J^c\right)$	$11M + 3S$
$t\left(2A = J^m\right)$	$3M + 4S$	$t\left(J^c + J = J\right)$	$11M + 3S$
$t(2A = J)$	$2M + 4S$	$t\left(J^c + J^c = J\right)$	$10M + 2S$
		$t\left(J + A = J^m\right)$	$9M + 5S$
		$t\left(J^m + A = J^m\right)$	$9M + 5S$
		$t\left(J^c + A = J^m\right)$	$8M + 4S$
		$t\left(J^c + A = J^c\right)$	$8M + 3S$
		$t(J + A = J)$	$8M + 3S$
		$t\left(J^m + A = J\right)$	$8M + 3S$
		$t\left(A + A = J^m\right)$	$5M + 4S$
		$t\left(A + A = J^c\right)$	$5M + 3S$
$t(2A)$	$2M + 2S + I$	$t(A + A)$	$2M + S + I$

Рассмотрим пример вычисления открытого ключа.

Пример 1. Пусть дана точка $G = (23, 0, 1)$, которая принадлежит кривой

$$Y^2 + XYZ = X^3 + aX^2Z^2 + bZ^6 \left(\mathrm{mod}\, f(x), 2\right),$$

где $a=1$; $b=3$; $n=38$; $m=5$; $f(x)=x^5+x^2+1$. Необходимо найти скалярное умножение $Q=dG$, причем $d=7$.

Используя алгоритм скалярного умножения, мы получим $Q=(2,29,25)$, в аффинных координатах эта точка имеет вид $Q=(28,2)$.

Заметим, что при использовании различных алгоритмов скалярного умножения можно получить различные значения точки Q. Так при семикратном сложении точки G самой с собой получим $Q'=(31,16,2)$, которая в аффинных координатах имеет вид $Q'=(28,2)$.

Из выше приведеного видно, что точки Q и Q' в проективном представлении принадлежат одному классу точек, так как в аффинном представлении это одна и таже точка. Этот эффект обусловлен тем, что порядок кривой в проективном представлении [21] $\#E_p(\mathrm{F}_{2^m})=(2^m-1)(\#E_a(\mathrm{F}_{2^m}))$. Если известна хотя бы одна точка в проективном представлении (и в других представлениях, кроме аффинного), то все множество точек, принадлежащее одному классу, можно получить как (tX,tY,tZ), где $t\le n$ есть простое число.

Пример 2. Подсчитать количество точек (порядок кривой), удовлетворяющих уравнениям:

1. $y^2+xy=x^3+x^2+3(\mathrm{mod}\, f(x),2)$.
2. $Y^2+XYZ=X^3+aX^2Z^2+bZ^6(\mathrm{mod}\, f(x),2)$,

где $a=1$; $b=3$; $n=38$; $m=5$; $f(x)=x^5+x^2+1$. Причем второе уравнение получено из первого, используя соответствующие формулы перехода.

Учитывая, что порядок поля небольшой, можно перебрать все возможные комбинации (x,y) в первом уравнении и (X,Y,Z) во втором. Получим:

1. $\#E=37+1$.
2. $\#E=1147+1$.

Если проанализировать полученный результат в проективном представлении, то мы увидим 37 классов точек. Точки принадлежат одному классу, если при переходе в аффинное представление мы получаем одну и туже точку. Из табл. 2 следует, что точке $(5,14)$ в аффинных координатах соответствует 31 различная точка в проективных координатах.

Таблица 2

Проективное преставление 1	Аффинн. представление 1	Проективное преставление 2	Аффинн. представление 2	Проективное преставление 1	Аффинн. представление 1	Проективное преставление 2	Аффинн. Представление 2
x:1 y:16 z:28	x:5 y:14	x:17 y:6 z:3	x:5 y:14	x:1 y:29 z:25	x:14 y:2	x:17 y:9 z:18	x:14 y:2
x:2 y:24 z:9	x:5 y:14	x:18 y:3 z:22	x:5 y:14	x:2 y:1 z:17	x:14 y:2	x:18 y:22 z:26	x:14 y:2
x:3 y:1 z:21	x:5 y:14	x:19 y:29 z:10	x:5 y:14	x:3 y:17 z:8	x:14 y:2	x:19 y:30 z:3	x:14 y:2
x:4 y:20 z:29	x:5 y:14	x:20 y:18 z:2	x:5 y:14	x:4 y:19 z:23	x:14 y:2	x:20 y:26 z:28	x:14 y:2
x:5 y:11 z:1	x:5 y:14	x:21 y:10 z:30	x:5 y:14	x:5 y:10 z:14	x:14 y:2	x:21 y:27 z:5	x:14 y:2
x:6 y:19 z:20	x:5 y:14	x:22 y:31 z:11	x:5 y:14	x:6 y:11 z:6	x:14 y:2	x:22 y:25 z:13	x:14 y:2
x:7 y:5 z:8	x:5 y:14	x:23 y:14 z:23	x:5 y:14	x:7 y:31 z:31	x:14 y:2	x:23 y:21 z:20	x:14 y:2
x:8 y:30 z:18	x:5 y:14	x:24 y:12 z:13	x:5 y:14	x:8 y:8 z:7	x:14 y:2	x:24 y:18 z:12	x:14 y:2
x:9 y:2 z:14	x:5 y:14	x:25 y:23 z:17	x:5 y:14	x:9 y:7 z:30	x:14 y:2	x:25 y:5 z:21	x:14 y:2
x:10 y:28 z:27	x:5 y:14	x:26 y:4 z:4	x:5 y:14	x:10 y:15 z:22	x:14 y:2	x:26 y:14 z:29	x:14 y:2
x:11 y:9 z:7	x:5 y:14	x:27 y:22 z:24	x:5 y:14	x:11 y:13 z:15	x:14 y:2	x:27 y:20 z:4	x:14 y:2
x:12 y:8 z:15	x:5 y:14	x:28 y:13 z:16	x:5 y:14	x:12 y:28 z:16	x:14 y:2	x:28 y:3 z:27	x:14 y:2
x:13 y:27 z:19	x:5 y:14	x:29 y:25 z:12	x:5 y:14	x:13 y:23 z:9	x:14 y:2	x:29 y:16 z:2	x:14 y:2
x:14 y:21 z:6	x:5 y:14	x:30 y:26 z:25	x:5 y:14	x:14 y:2 z:1	x:14 y:2	x:30 y:6 z:10	x:14 y:2
x:15 y:15 z:26	x:5 y:14	x:31 y:7 z:5	x:5 y:14	x:15 y:4 z:24	x:14 y:2	x:31 y:24 z:19	x:14 y:2
x:16 y:17 z:31	x:5 y:14			x:16 y:12 z:11	x:14 y:2		

Результаты таблицы можно проверить, используя формулы перехода из проективных в аффинные координаты. При этом переход из аффинных координат в проективные однозначен, каждая точка аффинного представления отображается в одну точку проективного. При обратном отображении 31 точка проективного представления должна проецироваться в одну точку аффинных координат.

В процессе выполнения арифметических операций над группой точек эллиптической кривой существует вероятность появления операции сложения двух точек из одного класса, что приводит к некорректным результатам. В этом и состоит вынесенный в название термин «не все так гладко»

Рассмотрим пример ошибочной операции из-за неоднозначности отображения между координатными базисами.

Пример 3. Пусть даны точки $G=(23,23,1)$ и $Q=(14,2,1)$, которые принадлежат кривой

$$Y^2+XYZ=X^3+aX^2Z^2+bZ^6\left(\mathrm{mod}\, f(x),2\right),$$

где $a=1$; $b=3$; $n=38$; $m=5$; $f(x)=x^5+x^2+1$. Необходимо вычислить точку $P=6G+16Q$, используя алгоритм скалярного умножения

$$P=6(23,23,1)+16(14,2,1)=(11,29,7)+(24,5,13)=(0,0,0).$$

Некорректность заключается в том, что на последнем этапе сложения точек мы использовали функцию сложения точек, так как они в проективных координатах не равны, но они принадлежат одному классу. Точки $(11,29,7)$ и $(24,5,13)$ соответствую точке $(5,14)$ в аффинных координатах, что подтверждает табл. 2.

Для получения правильного результата на последнем этапе необходимо использовать формулу удвоения любой из двух точек, тогда мы получим:

$$2(11,29,7)=(3,30,3)_{проект}=(28,2)_{аффин},$$

$$2(24,5,13)=(25,6,10)_{проект}=(28,2)_{аффин}.$$

В результате получен тот же результат, что и при вычислении $P=6G+16Q$ в аффинных координатах. Очевидно это и есть кардинальное решение, которое позволяет исключить некорректность результата сложения точек.

При реализации криптопреобразований в группах точек ЭК для повышения производительности более предпочтительным является выполнение операций сложения и удвоения в смешанных координатах, что позволяет минимизировать число операций умножения и возведения в квадрат при скалярном умножении. В таблице 2 приведены различные варианты смешанных координат и их сложность. Использование смешанных координат повышает вероятность получения некорректных результатов, и поэтому при криптопреобразованиях необходимо вводить дополнительные ограничительные условия.

В силу эпитоморфизма между множеством точек кривой E в аффинном представлении и множеством точек, удовлетворяющих уравнению кривой E в проективном представлении, в алгоритм сложения следует внести изменения: при появлении, в процессе расчета, точки $(0,0,0)$ прервать операцию сложения и выполнить операцию удвоения точки; перед операцией сложения выполнить проверку на равенство точек; пренебречь вероятностью возникновения ситуации сложения двух точек из одного класса $P=(q-1)/\#E_a(\mathrm{F}_q)$, при условии некритичности возникновения ошибки вычислений.

Выводы

Использование смешанных координат позволяет повысить производительность криптопреобразований в группах точек ЭК. Криптопреобразования, построенные с использованием представления точек в аффинных координатах, крайне неэффективны из-за присутствия в алгоритмах сложения и удвоения точек операции деления в поле.

В процессе криптопреобразований в группе точек ЭК для избежания некорректного использования операции сложения необходимо ввести дополнительную проверку, либо пренебречь ею.

Перспективными направлениями изучения проективной геометрии являются нахождение новых алгоритмов скалярного умножения, расширяющие возможности использования смешанных координат и минимизирующие возможности некорректного использования операции сложения.

Список литературы: 1.*A. Menezes, T. Okamoto, S. Vanstone,* "Reducing elliptic curve logarithm to logarithm in finite field", Proceeding of the 22nd Annual ACM Symposium on The Theory of Computing (1991), 80-89. 2. IEEE P1363 Working Draft, June 16, 1998 3. *G. Frey, H.G. Ruck,* "A remark concerning m-divisibility and the discrete logarithm in the divisor class group of curves", Mathematic of computation, 62 (1994), 865-874 4. *I.A. Semaev* "Evaluation of discrete logarithm in a group of p - torsion point of an elliptic curve in characteristic p ", Mathematic of computation, 67(1998), 353-356 5. *T. Stoh, K. Araki* "Fermat quotients and polynomial time discrete logarithm for anomalous curve", Comentarii Math. Univ. St. Pauli., vol. 47 (1998), 81-92 6. *N.P. Smart* "The discrete logarithm problem on elliptic curve of trace one", to appear in J. Cryptology 7. *J. Pollard* "Monte Carlo method for index computation $(\mathrm{mod}\, p)$ ", Mathematic of computation, 32 (1978), 918-924 8. *Горбенко И.Д., Збитнев С.И., Поляков. А.А.* Криптоанализ криптографических преобразований в группах точек эллиптических кривых методом Поларда // Радиотехника: Всеукр. межвед. науч.-техн. сб. 2001. Вып. 119. С.43-50 9. *S.C. Pohlig, M.E. Hellman* "An improved algorithm for computing logarithms over $GF(p)$ and its cryptographic significance", IEEE Trans. Inf. Theory, IT-24 (1978), 106-110 10. *J.H. Silverman* "The Arithmetic of Elliptic Curve", GTM 106, Springer-Verlag, New York, 1986 11. *K. Koyama, Y. Tsuruoka* "Speeding up elliptic cryptosystem by using a signed binary window method", Advanced in Cryptology - Proceeding of Crypto'92, Lecture Notes in Computer Science, 740 (1993), Springer-Verlag, 345-357 12. *D.V. Chudnovsky, G.V. Chudnovsky* "Sequence of number generated by addition in formal group and new primality and factorization test", Advanced in Applied Math., 7 (1986), 385-434 13. *H. Cohen, A. Miyaji, T. Ono* "Efficient elliptic curve exponentiation", Advanced in Cryptology – Proceeding of ICICS'97, Lecture Notes in Computer Science, 1334 (1997), Springer-Verlag, 282-290 14. *H. Cohen, A. Miyaji, T. Ono* "Efficient elliptic curve exponentiation using mixed coordinates", Advanced in Cryptology , 1998 15. *A. Menezes,* Elliptic Curve Public Key Cryptosystems, Kluwer Academic Publishers, Boston, 1993 16. *Иванов М.А.* Криптографические методы защиты информации в компьютерных системах и сетях. М.: КУДИЦ-ОБРАЗ, 2001. 368с. 17. *R. Schoof* "Counting points on elliptic curves over finite fields", Journal de Theorie des Nombres de Bordeaux 7 (1995), 219-254 18. *N. Koblitz* "CM-Curve with good cryptographic properties", Dept. of Mathematics, 1991,279-287 19. *J. Guajardo, C. Paar* "Efficient Algorithms for Elliptic Curve Cryptosystem", GTE Corporation, Springer-Verlag, 1998, 342-356 20. *J. Solinas* "An Improved Algorithm for Arithmetic in a Family of Elliptic Curves", National Security Agency, Springer-Verlag, 1998, 357-371 21. *J.H. Silverman* "The Arithmetic of Elliptic Curves", GTM 106, Springer-Verlag, New-York, 1986

Харьковский национальный университет радиоэлектроники

Поступила в редколлегию 22.04.2002