УДК. 682.142.35

М.Карпінський, докт.техн.наук; І.Якименко; І.Дуда
Тернопільська академія народного господарства
Національний технічний університет України "Київський політехнічний інститут"

ЕЛІПТИЧНА КРИВА ДЛЯ АСИМЕТРИЧНОЇ КРИПТОГРАФІЧНОЇ СИСТЕМИ

Пропонується еліптична крива, що проходить кільце Z_n для асиметричної криптографічної системи з метою підвищення її надійності щодо гомоморфічних атак. Розглядаються алгоритми для визначення порядку еліптичної групи $|E_p(a,b)|$ і комплементарної групи $\overline{|E_p(a,b)|}$ до даної еліптичної кривої $y^2=x^3+ax+b(mod\ n)$.

Відомі асиметричні криптографічні системи (АСК), які грунтуються на застосуванні еліптичних кривих і запропоновані низкою авторів – Діффі–Хельманом [1], Міллером [2], Ель–Гамалом, Мессі–Омурою, характерні рядом недоліків. Основні з них: використання лише для електронного підпису, а не для зовнішньої криптографічної системи, обмеження типів первинного тексту, що формує арифметичний модуль, і типів використовуваних еліптичних кривих.

Суть пропонованої АКС полягає у застосуванні еліптичних кривих , що проходять кільце Z_n. Алгоритм системи такий: першу координату точки P=(x,y) на еліптичній кривій $y^2=x^3+ax+b(\text{mod } n)$ з фіксованими параметрами (a та b) обчислюють шляхом комп'ютерної обробки, в результаті чого отримують x_e. Тут n – добуток двох великих простих чисел p та q, e – енкрипційний множник.

Відомо, що для простого числа p>3 і цілих чисел a та b крива не вироджується, якщо витримується умова

$$4a^3 + 27b^2 \neq 0 (\text{mod} p). \qquad (1)$$

Позначимо через $E_p(a,b)$ еліптичну групу модуля p, елементи якого (x,y) є парами чисел, що менші від p. Тоді

$$y^2 = x^3 + ax + b(\text{mod} p) \qquad (2)$$

разом з точкою нескінченності (∞).

Далі задають операцію додавання двох точок P та Q на еліптичній кривій для отримання третьої точки R, яку описують так:

$$P+Q = R, \qquad (3)$$

При чому для $P=(x_1,y_1)$ і $Q=(x_2,y_2)$, $R=(x_3,y_3)$ визначається згідно з такими правилами:

$$x_3 = \lambda^2 - x_1 - x_2 \ (\text{mod} p), \qquad (4)$$

$$y_3 = \lambda(x_1 - x_3) - y_1 \,(\mathrm{mod}\, p), \tag{5}$$

де

$$\lambda = \begin{cases} \dfrac{y_1 - y_2}{x_1 - x_2}, \text{якщо } x_1 \neq x_2 \,(\mathrm{mod}\, p) \\ \dfrac{3 * x_1^{\,2} + a}{2 y_1}, \text{якщо } x_1 \equiv x_2 \,(\mathrm{mod}\, p) \end{cases} \tag{6}$$

Якщо Q є ідентичним елементом, тоді

$$P+Q=Q+P=R. \tag{7}$$

На основі цього для $x_1=x_2$ і $y_1=-y_2(\mathrm{mod}\ p)$

$$P + Q = \infty, \tag{8}$$

зокрема P= -Q або $(x_2,-y_2) = -(x_2,y_2)$ (mod p).

Порядок еліптичної групи $\left| E_p(a,b) \right|$ визначається з такої формули:

$$\left|E_p(a,b)\right| = 1 + \sum_{x=1}^{p} \left(\left(\frac{z}{p} \right) + 1 \right), \tag{9}$$

де $\frac{z}{p}$ – символ Легендре,

а $z = x^3 + ax + b(\mathrm{mod}\, p)$. (10)

Для обчислення порядку еліптичної групи в обмеженому полі можна використати поліноміальний часовий алгоритм. Якщо p – просте число і $p \equiv 1(\mathrm{mod}4)$, r – складне число і $\frac{r}{p} \equiv 1(\mathrm{mod}(2i+2))$, а D є будь–яке ціле число, що не ділиться на p, тоді порядок еліптичної групи $E_p(-D,0)$ буде

$$\left|E_r(-D,0)\right| = p + 1 - \overline{\left(\frac{D}{r}\right)_4} \cdot r - \left(\frac{D}{r}\right)_4 \bar{r}, \tag{11}$$

де x/r – символ четвертого ступеня цілого числа r.

Наприклад, якщо p=13, а r=3+2i, тоді

$\left|E_{13}(-1,0)\right| = 14 - (1) * (3 + 2i) - (1) * (3 - 2i) = 8$,

$\left|E_{13}(1,0)\right| = 14 - (-1) * (3 + 2i) - (-1) * (3 - 2i) = 20$,

$\left|E_{13} - (2,0)\right| = 14 - (i) * (3 + 2i) - (-i) * (3 - 2i) = 18$,

$\left|E_{13}(2,0)\right| = 14 - (-i) * (3 + 2i) - (i) * (3 - 2i) = 10$.

Якщо ж p – просте число і $p \equiv 1(\mathrm{mod}3)$, $\frac{r}{p} \equiv 2(\mathrm{mod}3)$, а D є будь–яким цілим числом, що не ділиться на p, то порядок еліптичної групи $E_p(-D,0)$ буде

$$\left|E_p(0,D)\right| = p + 1 + \left(\frac{\overline{4D}}{r}\right)_6 + \left(\frac{4D}{r}\right)_6 * \bar{r}, \tag{12}$$

де $\left(\frac{x}{r}\right)_6$ – символ шостого ступеня цілого числа r.

Приміром, для p=13, r=-4-3ω, де $\omega=e^{2\pi i/3}$ справджується

$$|E_{13}(0,1)| = 14+(\omega^2)*(-4-3\omega)+(\omega)*(-1+3\omega)=12,$$
$$|E_{13}(0,2)| = 14+(-1)*(-4-3\omega)+(-1)*(-1+3\omega)=1,$$
$$|E_{13}(0,3)| = 14+(1)*(-4+3\omega)+(1)*(1-3\omega)=9,$$
$$|E_{13}(0,4)| = 14-(-\omega^2)*(-4-3\omega)+(-\omega)*(-1+3\omega)=16,$$
$$|E_{13}(0,6)| = 14+(-\omega)*(-4-3\omega)+(-\omega^2)*(-1+3\omega)=7.$$

Розглянемо складніший випадок, а саме для комплементарної групи до даної іптичної кривої.

Нехай p > 3 – просте число, а та b – цілі числа, що задовольняють умову (1). Тоді (a,b) позначатиме еліптичну групу модуля p, чиї елементи (x,y) задовольняють ову (2). Координата y невизначена в обмеженому полі F_p для невід'ємного цілого сла, меншого, ніж число p. Впровадимо фіксоване число V, яке є квадратним залишком модуля числа p. Операція додавання для комплементарної групи йснюється згідно з (3).

Зокрема, якщо $p=(x_1,y_1)=(x_1,u_1\sqrt{V})$, а $Q=(x_2,y_2)=(x_2,u_2\sqrt{V})$ - два елементи рупі, тоді $R=(x_3,y_3)=(x_3,u_3\sqrt{V})$ є також у групі.

Опишемо конкретну реалізацію покоординатного сумування. Для $y_1)+(x_2,y_2)=(x_3,y_3)$(mod p) за умови $x_1 \neq x_2$ (mod p)

$$x_3=\left(\frac{u_1-u_2}{x_1-x_2}\right)^2 * V - x_1 - x_2 \text{ (mod p)}, \tag{13}$$

$$y_3=\left(\left(\frac{u_1-u_2}{x_1-x_2}\right)*(x_1-x_2)-u_1\right)*\sqrt{V} \text{ (mod p)}. \tag{14}$$

Якщо ж $x_1=x_2$, а $y_1 \neq y_2$(mod p), то

$$x_3=\left(\frac{3x_1^2+a}{2u_1V}\right)^2 * V - x_1 - x_2 \text{ (mod p)}, \tag{15}$$

$$y_3=\left(\left(\frac{3x_1+a}{2u_1V}\right)*(x_1-x_3)-u_1\right)*\sqrt{V} \text{ (mod p)}. \tag{16}$$

Порядок комплементарної групи $|E_p(a,b)|$ визначиться з виразу

$$|Ep(a,b)| = 1+\sum_{x=1}^{p}\left(1-\left(\frac{z}{p}\right)\right) \tag{17}$$

Позначимо через A значення координати x, для якої (z/p)=1, через B – значення динати x, для якої (z/p)=0 і через C – значення координати x, для якої (z/p)=-1. Тоді о з (17) можна впевнитися, що координата x має перебувати в одній з можливих тей:

$$A+B+C=p \tag{18}$$
$$2A+B=p+a \tag{19}$$

Використовуючи (9) … (12), відповідно до (18) і (19) отримуємо такий порядок лементарної групи:

$$\left|E_p(a,b)\right| = 1 + 2A + B = 1 + p + a, \tag{20}$$

$$\left|\overline{E_p(a,b)}\right| = 1 + 2C + B = 1 + 2p - (2A + B) = 1 + p - a \tag{21}$$

Впровадимо поняття енкрипції щодо даної комплементарної групи, беручи до уваги множення координати точки P(x,y) на енкрипційний множник

$$(s,t)=(x,y) \# e(\text{mod } n), \tag{22}$$

де $0 \le x, s \le n-1$.

Тоді декрипцію можна визначити з таких співвідношень

$$(x,y)=(s,t) \# d^i \pmod n \quad . \tag{23}$$

За умов

$$(e,d^i) = 1 (\text{mod. } N_i),\ 1 \le i \le 4 \tag{24}$$

і

$$d(e,Ni)=1,\ 1 \le i \le 4 \tag{25}$$

Отримаємо послідовність обчислення шуканих координат

$$N_1 = lem(p+1+a, q+1+\beta), \text{ якщо} \left(\frac{W}{p}\right) = 1 \text{ і } \left(\frac{W}{q}\right) = 1 \tag{26}$$

$$N_2 = lem(p+1+a, q+1-\beta), \text{ якщо} \left(\frac{W}{p}\right) = 1 \text{ і } \left(\frac{W}{q}\right) \ne 1 \tag{27}$$

$$N_3 = lem(p+1-a, q+1+\beta), \text{ якщо} \left(\frac{W}{p}\right) \ne 1 \text{ і } \left(\frac{W}{q}\right) = 1 \tag{28}$$

$$N_4 = lem(p+1-a, q+1-\beta), \text{ якщо} \left(\frac{W}{p}\right) \ne 1 \text{ і } \left(\frac{W}{q}\right) \ne 1 \tag{29}$$

Треба відзначити, що в (26) – (29) a, b, p і q вибрані так, що $\alpha = \beta = 0$, тобто N_i=lem(p+1,q+1) є фіксованим для всіх i. Внаслідок цього декрипція не залежить від символів Легендре $\left(\frac{W}{p}\right)$ та $\left(\frac{W}{q}\right)$.

За аналогією з

$$z=x^3+ax+b \pmod n \tag{30}$$

$$y = \sqrt{z} \tag{31}$$

Причому для першої координати s, що належить до (21), справджується:

$$W=s^3+as+h \pmod n \text{ і}, \tag{32}$$

де $\sqrt{W} = 1$. (33)

Нехай s_1 та s_2 відповідають повідомленням x_1 і x_2, а y_1 і y_2 – відповідно повідомленням t_1 і t_2. Згідно з визначенням гомоморфізму можна записати

$$(s,1)=(s_1,t_1)+(s_2,t_2), \tag{34}$$

звідки отримуємо $t_1 = \sqrt{W_1}$, $t_2 = \sqrt{W_2}$, (35)

де $W_1 = s_1^3 + as_1 + b (\text{mod} n)$,

$W_2 = s_2^3 + as_2 + b (\text{mod} n)$.

Вилучивши один з індетермінантів, наприклад t_2, маємо

$$t_1 = u\sqrt{W_1} \tag{36}$$

З урахуванням вищенаведеного, для першої координати s

$$s = \left(\frac{1-u}{S_1 - S_2}\right)^2 \omega_1 \equiv S_1 - S_2 (\mathrm{mod} n) \tag{37}$$

На підставі цього можна визначити $u = \sqrt{\frac{W_2}{W_1}} (\mathrm{mod} n)$.

Отже, запропонована еліптична крива дозволяє суттєво підвищити надійність АСК щодо гомоморфічних атак.

There are proposed elliptical curve Z_n multitude for skew cryptographical system with aim of increasing its reliability relatively to homomorphy attacks. There are considered algorithms for determination of order of elliptical group $|E_p(a,b)|$ *and complementary group* $\overline{|E_p(a,b)|}$ *to the given elliptical curve* $y^2 = x^3 + ax + b (mod\ n)$.

Література

1. Diffie W., Hellman M.. New Directions in Cryptography // IEEE Transactions on Information Theory. – 1976. Vol. 22. – Pp. 644-654.
2. Miller V.S.. Use of Elliptic Curves in Cryptography // Advances in Cryptology: Proceedings of CRYPTO 85, Lecture Notes in Computer Science. – 1986. – Vol. 218. – Pp. 417-426.

Одержано 10.04.01 р.