Додаток А

ОСНОВНІ ПОЛОЖЕННЯ ТА МАТЕМАТИЧНІ МЕТОДИ КРИПТОГРАФІЧНИХ ПЕРЕТВОРЕНЬ У ГРУПІ ТОЧОК ЕЛІПТИЧНИХ КРИВИХ

Вступ

У цьому додатку наведено основні положення й математичні методи криптографічних перетворень у групі точок еліптичних кривих, які є теоретичним підґрунтям реалізації відповідних криптографічних методів, механізмів і протоколів, а також криптографічних систем і засобів криптографічних перетворень. При викладенні матеріалу ми орієнтуємось здебільшого на ті методи перетворень у групі точок ЕК, що використовуються на практиці або є перспективними, наприклад, спарювання точок ЕК тощо. Здебільшого вони різною мірою стандартизовані та містяться в міжнародних і національних стандартах, перш за все ДСТУ ISO/IEC 15946-1, 3; ISO/IEC 15946-1,4; ISO/IEC 14888-2; ISO/IEC-9796-3; ГОСТ Р 34 10-2001; ДСТУ 4145-2002. У цьому додатку наводяться тільки математичні методи криптографічних перетворень у групі точок ЕК і методи, на яких ґрунтується доведення криптографічної стійкості та інших властивостей.

Терміни і визначення

У цьому додатку також використовуються такі терміни і визначення:

Кінцеве поле Галуа – будь-яке поле Галуа, що містить кінцеве число елементів.

Примітка. Справедливим є те що для будь-якого позитивного цілого m і простого p існує кінцеве поле, що містить точно p^m елементів. Це поле є унікальним аж до ізоморфізму і позначається як $F(p^m)$, де p називається характеристикою $F(p^m)$.

Еліптична крива – будь-яка кубічна крива E без будь-якої сингулярної точки.

Примітка. Безліч точок E є абелевою групою. Поле, яке містить усі коефіцієнти рівняння, що описує E, називається полем визначення E. Ми будемо розглядати тільки кінцеві поля F. Коли явно описується поле визначення F кривої E, тоді ми ідентифікуємо криву як E/F, тобто в загальному випадку криву над полем Галуа $F(p^m)$.

Криптографічне білінійне відображення e_n, що задовольняє властивості невиродженості, білінійності та можливості його практичного обчислення.

Позначення

У цьому додатку використовується така система позначень:

d – Особистий ключ користувача (d – випадкове ціле число в безлічі $[2, n-2]$);
E – Еліптична крива, задана або рівнянням вигляду
$Y^2 = X^3 + aX + b$
над полем $F(p^m)$ для $p > 3$, або рівнянням вигляду
$Y^2 + XY = X^3 + aX^2 + b$
над полем $F(2^m)$, або рівнянням вигляду
$Y^2 = X^3 + aX^2 + b$
над полем $F(3^m)$, разом із допоміжною точкою 0_E, що називається точкою на нескінченності. Крива позначається як
$E/F(p^m)$, $E/F(2^m)$ або $E/F(3^m)$ відповідно;
$E(F(q))$ – безліч $F(q)$-значних точок E і 0_E;
$\#E(F(q))$ – порядок (або потужність) $E(F(q))$;
$E[n]$ – група n-кручення E, тобто $\{Q \in E \mid nQ = 0_E\}$;
$|F|$ – бітовий розмір кінцевого поля F;
$F(q)$ – кінцеве поле, що містить точно q елементів. Це включає випадки $F(p)$, $F(2^m)$ і $F(p^m)$;
$F(q)^* F(q) \backslash \{0_F\}$, тобто кінцеве поле без точки нескінченності;
G – базова точка на E з порядком n;
$< G >$ – група, що генерує G з потужністю n;
kQ – k-й множник деякої точки Q кривої E, тобто
$kQ = Q + ... + Q$ (k доданків), якщо $k > 0$,
$kQ = (-k)(-Q)$, якщо $k < 0$, і $kQ = 0_E$, якщо $k = 0$;
μ_n – циклічна група порядку n, що містить n–x коренів одиничного елемента в алгебраїчному замиканні $F(q)$;
n – простий дільник $\#E(F(q))$.;
0_E – точка еліптичної кривої на нескінченності;
P – просте число;
Q – відкритий ключ користувача, причому Q – точка еліптичної кривої групи $<G>$;
q – простий ступінь, p_m для деякого простого p та деякого цілого $m \geq 1$;
Q – точка на E з координатами (x_Q, y_Q);
$(Q_1 + Q_2)$ – сума двох точок Q_1 і Q_2 еліптичної кривої;
x_Q – x-координати $Q \neq 0_E$;
y_Q – y-координати $Q \neq 0_E$;
$[0, k]$ – безліч цілих чисел від 0 до k включно;
0_F – одиничний елемент $F(q)$ для складання;
1_F – одиничний елемент $F(q)$ для множення.

А.1. ПОЛЯ ГАЛУА

А.1.1. Прості кінцеві поля $F(p)$

Для будь-якого простого p існує кінцеве поле, що складається точно з p елементів. Це поле унікально визначається з точністю до ізоморфізму і називається кінцевим простим полем $F(p)$.

Елементи кінцевого простого поля $F(p)$ можуть бути ідентифіковані за допомогою безлічі $[0, p-1]$ усіх позитивних цілих чисел, тобто менших за p. Для $F(p)$ визначено дві операції – складання і множення, що мають такі властивості:

$F(p)$ – абелева група відносно операції складання «+».

Для $a, b \in F(p)$ сума $a + b$ задається як $a + b := r$, де $r \in F(p)$ – залишок від ділення суми цілих $a + b$ на p.

$F(p)\backslash\{0\}$ позначається як $F(p)^*$ – абелева група відносно операції множення «×».

Для $a, b \in F(p)$ результат множення $a \times b$ отримується як $a \times b := r$, де $r \in F(p)$ є залишком від ділення цілого $a \times b$ на p. Операція множення × як правило упускається й використовується позначення ab або $a \cdot b$.

А.1.2. Кінцеві поля $F(p^m)$

Для будь-якого позитивного цілого m і простого p існує кінцеве поле з точно p^m елементів. Це поле унікальне й визначається з точністю до ізоморфізму та називається кінцевим полем $F(p^m)$. Необхідно враховувати, що $F(p_m)$ – це загальне позначення, його частковими випадками є поле $F(p)$ для $m = 1$ і поле $F(2^m)$ для $p = 2$. Якщо $p = 2$, то елементи поля можуть бути ідентифіковані за допомогою бітових рядків довжини m, і сума двох елементів поля визначається як побітове XOR (сума за модулем 2) двох бітових рядків.

Кінцеве поле $F(p^m)$ може бути визначене (ідентифіковано) за допомогою безлічі p-рядків довжини m наступним чином. Кожне кінцеве поле $F(p^m)$ містить щонайменше один такий базис $\{\xi_1, \xi_2, \cdots, \xi_m\}$ над полем $F(p)$, що кожен елемент $\alpha \in F(p^m)$ має унікальне подання вигляду $\alpha = a_1 \xi_1 + a_2 \xi_2 + \cdots + a_m \xi_m$, причому $a_i \in F(p)$ для всіх $i = 1, 2, \cdots, m$. За такої умови елемент α може бути визначений за допомогою p-рядка $(a_1, a_2, \cdots, a_m)$. Вибір базису виходить за межі цього додатку. Для поля $F(p^m)$ задані дві операції – складання і множення, що задовольняють таким умовам:

1) $F(p^m)$ – це абелева група відносно операції складання «+».

Для $\alpha = (a_1, a_2, \cdots, a_m)$ і $\beta = (b_1, b_2, \cdots, b_m)$ сума $a + \beta$ задається за допомогою $a + \beta := \gamma = (c_1, c_2, \cdots, c_m)$, де $c_i = a_i + b_i$ – сума у $F(p)$. Одиничним елементом для складання є $0_F = (0, \cdots, 0)$;

2) $F(p^m)\backslash\{0\}$, позначена як $F(p^m)^*$, є абелевою групою відносно операції множення «×».

Для $\alpha = (a_1, a_2, \cdots, a_m)$ і $\beta = (b_1, b_2, \cdots, b_m)$ результат $\alpha \times \beta$ задається p-рядком $a \times \beta := \gamma = (c_1, c_2, \ldots, c_m)$, де $c_i = \sum 1_{\le j,k \le m} a_j b_k d_{i,j,k}$ для $\xi_j \xi_k = d_{1,j,k} \xi_1 + d_{2,j,k} \xi_2 + \ldots + d_{m,j,k} \xi_m$ $(1 \le j, k \le m)$. Як правило, знак операції множення × упускається й використовується позначення ab. Базис може бути вибраний таким чином, щоб одиничний елемент для множення був $1_F = (1, 0, \cdots, 0)$.

А.1.3. Квадрати і неквадрати в полі $F(q)$

Нехай характеристика $F(q) > 2$. Елемент $a \in F(q)^*$, називається квадратом у $F(q)^*$, якщо існує елемент $b \in F(q)^*$ – такий, що $a = b^2$. Чи є $a \in F(q)^*$ квадратом у полі, можна визначити, використовуючи еквівалентність твердження: a є квадратом у $F(q)^*$, якщо $\Leftrightarrow a^{(q-1)/2} = 1_F$.

Пошук квадратних коренів можна здійснювати, використовуючи різні методи [32].

А.2. ЕЛІПТИЧНІ КРИВІ

А.2.1. Визначення еліптичних кривих

А.2.1.1. Еліптичні криві над $F(p^m)$

Нехай $F(p^m)$ є кінцевим полем з простим $p > 3$ і позитивним цілим m. Тоді існує еліптична крива E, яка описується афінним рівнянням Вейєрштраса вигляду [32]

$$Y^2 = X^3 + aX + b, \tag{А.1}$$

причому $a, b \in F(p^m)$, якщо виконується умова що $4a^3 + 27b^2 \neq 0_F$ у полі $F(p^m)$.

Якщо $4a^3 + 27b^2 = 0_F$ у полі, то крива називається сингулярною і не є еліптичною кривою.

Уся безліч $F(p^m)$-значних точок E задається як

$$E(F(p^m)) = \{Q = (x_Q, y_Q) \in F(p^m) \times F(p^m) \,|\, {y_Q}^2 = {x_Q}^3 + ax_Q + b\} \cup \{0_E\},$$

де 0_E – допоміжна точка, що називається точкою нескінченності кривої E.

А.2.1.2. Еліптичні криві над полем $F(2^m)$

Нехай $F(2^m)$, для деякого $m \geq 1$ буде кінцевим полем. Тоді існує еліптична крива E, яка описується афінним рівнянням Вейєрштраса вигляду [32]

$$Y^2 + XY = X^3 + aX^2 + b, \tag{А.2}$$

причому $a, b \in F(2^m)$, якщо тільки $b \neq 0_F$ у $F(2^m)$.

У криптографічних застосуваннях m повинне бути простим, оскільки за таких умов забезпечується запобігання певним видам атак на криптосистему.

Якщо $b = 0_F$, то така крива називається сингулярною кривою і не є еліптичною кривою.

Уся безліч $F(2^m)$-значних точок E задається як

$$E(F(2^m)) = \{Q = (x_Q, y_Q) \in F(2^m) \times F(2^m) \,|\, {y_Q}^2 + x_Q y_Q = {x_Q}^3 + a{x_Q}^2 + b\} \cup \{0_E\},$$

де 0_E – допоміжна точка, що називається точкою нескінченності кривої E.

А.2.1.3. Еліптичні криві над $F(3^m)$

Нехай $F(3^m)$ буде кінцевим полем, де m – позитивне ціле. Тоді існує еліптична крива E, яка описується афінним рівнянням Вейєрштраса вигляду [32]:

$$Y^2 = X^3 + aX^2 + b \text{ з } a, b \in F(3^m), \tag{А.3}$$

якщо $a, b \neq 0_F$ у полі $F(3^m)$.

Якщо a або $b = 0_F$, то така крива називається ***сингулярною кривою*** і відповідно не є еліптичною кривою.

Уся безліч $F(3^m)$-значних точок E задається як

$$E(F(3^m)) = \{Q = (x_Q, y_Q) \in F(3^m) \times F(3^m) \mid y_Q^2 = x_Q^3 + ax_Q^2 + b\} \cup \{O_E\},$$

де O_E – допоміжна точка, що називається точкою на нескінченності E.

А.3. ГРУПОВИЙ ЗАКОН ДЛЯ ЕЛІПТИЧНИХ КРИВИХ Е НАД $F(q)$ З $p>3$

А.3.1. Огляд систем координат

Зазвичай еліптична крива визначається в афінних координатах. Тому базова точка або відкритий ключ користувача задається в афінних координатах. Головним недоліком афінних координат є складність операції ділення в полі $F(q)$ при виконанні як складання, так і подвоєння [32]. Зменшення складності в цілому при складанні та подвоєнні точок може досягатись засобом уникнення операції ділення, причому якомога більше. Це досягається використанням при множенні (складанні та подвоєнні точок) інших координат, таких як проективні координати, координати Якобі та модифіковані координати Якобі тощо, які є трьохмірними [32]. Причому має забезпечуватись вимога, щоб усі *і* системи координат, що використовуються, були сумісні.

А.3.2. Груповий закон в афінних координатах

Нехай $F(q)$ є кінцевим полем Галуа з $p > 3$. Нехай E є еліптичною кривою над $F(q)$, що задається «коротким рівнянням Вейєрштраса» [32],

$$Y^2 = X^3 + aX + b, a, b \in F(q), \tag{А.4}$$

а також $4a^3 + 27b^2 \neq 0_F$ у полі $F(q)$. Тоді в афінних координатах груповий закон складання та подвоєння на еліптичній кривій (А.4) задається таким чином:

1) точка на нескінченності 0_E є одиничним елементом до операції додавання «+»;

2) усі точки $R = (x, y)$ є такими, що $R \neq 0_E$;

3) якщо $R_1 = (x_1, y_1)$ і $R_2 = (x_2, y_2)$ є дві різні точки на E – такі, що $R_1 \neq \pm R_2$ і R_1, $R_2 \neq 0_E$, то сумою точок R_1 та R_2 є точка $R_3 = (x_3, y_3)$, координати якої визначаються як:

$$x_3 = r^2 - x_1 - x_2;$$
$$y_3 = r(x_1 - x_3) - y_1,$$

причому

$$r = (y_2 - y_1) / (x_2 - x_1); \tag{А.5}$$

якщо $R = (x, y)$ є точка на E – така, що $R \neq 0_E$ і $y \neq 0_F$, то її подвоєнням є точка $2R = (x_3, y_3)$, координати якої визначаються як:

$$x_3 = r^2 - 2x;$$
$$y_3 = r(x - x_3) - y,$$

причому

$$r = (3x^2 + a) / (2y). \tag{А.6}$$

У разі якщо $R = (x, 0_F)$, подвоєнням цієї точки є точка $2R = 0_E$.

А.3.3. Груповий закон у проективних координатах

Особливістю проективного базису є те, що при використанні проективних координат необхідно виконувати більше операцій множення, але немає операції ділення за модулем (інверсії). Після виконання скалярного множення в проективному базисі необхідно зробити зворотне перетворення на афінні координати. Але при виконанні перетворення з проективних координат на афінні, необхідне одне ділення в полі.

Проективний аналог короткого афінного рівняння Вейєрштраса (А.4) визначається однорідним кубічним рівнянням [32]

$$Y^2Z = X^3 + aXZ^2 + bZ^3,\ a, b \in F(q). \qquad (A.7)$$

Безліч усіх трійок еквівалентна (X, Y, Z) і позначається як $(X, Y, Z)/\sim$.

Еліптична крива, що задається в проективних координатах, складається з усіх точок $R = (X, Y, Z)$ рівняння (А.7) так, що трійка (X, Y, Z) є рішенням рівняння.

Існує співвідношення між точками Q кривої E, коли крива задана в афінних координатах, а точка R – у проективних координатах. У цьому випадку справедливі твердження:

1) якщо $Q = (X_Q, Y_Q)$ є точка в афінних координатах, то $R = (X_Q, Y_Q, 1_F)$ є відповідною точкою в проективних координатах;

2) якщо $R = (X, Y, Z)$ (з $Z \neq 0_F$) є рішенням (А.7), то $Q = (X/Z, Y/Z)$ є відповідною точкою в афінних координатах кривої E;

3) існує тільки одне рішення (А.7) із $Z = 0$, а саме: точка $(0_F, 1_F, 0_F)$, яка відповідає 0_E.

У проективних координатах груповий закон задається таким чином:

1) точка $(0_F, 1_F, 0_F)$ є одиничним елементом 0_E відносно операції «+»;

2) точка $R = (X, Y, Z) \neq (0_F, 1_F, 0_F)$ є точкою на E, що задана в проективних координатах, тоді точка $-R = (X, -Y, Z)$;

3) нехай $R_1 = (X_1, Y_1, Z_1)$ і $R_2 = (X_2, Y_2, Z_2)$ є дві відмінні точки на E – такі, що $R_1 \neq R_2$ і $R_1, R_2 \neq (0_F, 1_F, 0_F)$, тоді сума R_1 та R_2 є $R_3 = (X_3, Y_3, Z_3)$. Координати X_3, Y_3 і Z_3 можуть бути обчисленні за допомогою таких формул:

$$\begin{aligned} X_3 &= -su, \\ Y_3 &= t(u + s^2X_1Z_2) - s^3Y_1Z_2, \\ Z_3 &= s^3Z_1Z_2, \end{aligned} \qquad (A.8)$$

де $s = X_2Z_1 - X_1Z_2$, $t = Y_2Z_1 - Y_1Z_2$, і $u = s^2(X_1Z_2 + X_2Z_1) - t^2Z_1Z_2$.

Якщо $R = (X, Y, Z) \neq (0_F, 1_F, 0_F)$ є точкою на E, тоді її подвоєння є $2R = (X_3, Y_3, Z_3)$.

Координати точки $2R - (X_3, Y_3, Z_3)$ можуть бути обчислені за допомогою таких формул:

$$\begin{aligned} X_3 &= -su, \\ Y_3 &= t(u + s^2X) - s^3Y, \\ Z_3 &= s^3Z, \end{aligned} \qquad (A.9)$$

де $t = 3X^2 + aZ^2$, $s = 2YZ$ і $u = 2s^2X - t^2Z$.

А.3.4. Груповий закон у проективних координатах Якобі

Особливістю групового закону в проективних координатах Якобі є те, що скалярне множення вимагає більше множень, але не вимагає обчислення інверсій.

Аналогом рівняння Якобі в проективних координатах відносно короткого рівняння Вейерштраса (А.5) є кубічне рівняння [32]:

$$(Jac)\ Y^2 = X^3 + aXZ^4 + bZ^6,\ a, b \in F(q). \qquad (A.10)$$

Безліч усіх трійок еквівалентна (X, Y, Z) і позначається як $(X, Y, Z)/\sim$.

Існує відношення між точками Q кривої E, коли крива задана в афінних координатах, а точки R – у проективних координатах. Так, справедливими є твердження:

1) якщо $Q = (X_Q, Y_Q)$ є точкою в афінних координатах E, то $R = (X_Q, Y_Q, 1_F)$ є відповідною точкою в координатах Якобі.

2) якщо $R = (X, Y, Z)$ $(Z \neq 0_F)$ є рішенням (А.3.7), тобто в координатах Якобі, то $Q = (X/Z^2, Y/Z^3)$ є відповідною точкою в афінних координатах точки E.

3) існує тільки одне рішення (А.10) зі значенням $Z = 0_F$, а саме точка $(1_F, 1_F, 0_F)$, яка відповідає 0_E.

У проективних координатах Якобі груповий закон для (А.10) задається таким чином [32]:

1) точка $(1_F, 1_F, 0_F)$ є одиничним елементом 0_E щодо «+»;

2) якщо $R = (X, Y, Z) \neq (1_F, 1_F, 0_F)$ є точкою на E, заданою в координатах Якобі, тоді точка $-R = (X, -Y, Z)$;

3) якщо $R_1 = (X_1, Y_1, Z_1)$ і $R_2 = (X_2, Y_2, Z_2)$ є дві відмінні точки на E, але такі, що $R_1 \neq R_2$ і $R_1, R_2 \neq (1_F, 1_F, 0_F)$, тоді сумою точок R_1 та R_2 є точка $R_3 = (X_3, Y_3, Z_3)$. Координати X_3, Y_3 і Z_3 можуть бути обчислені за допомогою таких формул:

$$\begin{aligned} X_3 &= -h^3 - 2u_1h^2 + r^2, \\ Y_3 &= -s_1h^3 + r(u_1h^2 - X_3), \\ Z_3 &= Z_1Z_2h, \end{aligned} \qquad (A.11)$$

де $u_1 = X_1Z_2^2$, $u_2 = X_2Z_1^2$, $s_1 = Y_1Z_2^3$, $s_2 = Y_2Z_1^3$, $h = u_2 - u_1$, і $r = s_2 - s_1$;

4) якщо $R = (X, Y, Z) \neq (1_F, 1_F, 0_F)$ є точкою на E, тоді її подвоєння є $2R = (X_3, Y_3, Z_3)$. Координати X_3, Y_3 і Z_3 можуть бути обчислені за допомогою таких формул:

$$\begin{aligned} X_3 &= t, \\ Y_3 &= -8Y^4 + m(s - t), \\ Z_3 &= 2YZ, \end{aligned} \qquad (A.12)$$

де $s = 4XY^2$, $m = 3X^2 + aZ^4$ і $t = -2s + m^2$.

А.3.5. Груповий закон у модифікованих координатах Якобі

Згідно з тим же кубічним рівнянням (А.10) груповий закон у модифікованих координатах Якобі задається шляхом представлення координат Якобі четвіркою координат (X, Y, Z, aZ^4). Таке представлення забезпечує найменшу складність операції подвоєння для еліптичної кривої E $(F(q))$.

У модифікованих координатах Якобі груповий закон на еліптичній кривій задається таким чином [32]:

1) якщо $R_1 = (X_1, Y_1, Z_1, aZ^4_1)$ і $R_2 = (X_2, Y_2, Z_2, aZ^4_2)$ є дві відмінні точки на E – такі, що $R_1 \neq R_2$ і $R_1, R_2 \neq (1_F, 1_F, 0_F, 0_F)$, тоді сумою є точка $R_3 = (X_3, Y_3, Z_3, aZ^4_3)$. Координати X_3, Y_3 і Z_3 можуть бути обчислені за допомогою таких формул:

$$X_3 = -h^3 - 2u_1h^2 + r^2,$$
$$Y_3 = -s_1h^3 + r(u_1h^2 - X_3),$$
$$Z_3 = Z_1Z_2h,$$
$$aZ^4_3 = aZ^4_3, \qquad \text{(A.13)}$$

де $u_1 = X_1Z^2_2$, $u_2 = X_2Z^2_1$, $s_1 = Y_1Z^3_2$, $s_2 = Y_2Z^3_1$, $h = u_2 - u_1$, і $r = s_2 - s_1$;

2) якщо $R = (X, Y, Z, aZ^4) \neq (1_F, 1_F, 0_F, 0_F)$ є точкою на E, тоді її подвоєння позначається як $2R = (X_3, Y_3, Z_3, aZ^4_3)$. Координати X_3, Y_3 і Z_3 можуть бути обчислені за допомогою формули:

$$X_3 = t,$$
$$Y_3 = m(s - t) - u,$$
$$Z_3 = 2YZ,$$
$$aZ^4_3 = 2u(aZ^4), \qquad \text{(A.14)}$$

де $s = 4XY^2$, $u = 8Y^4$, $m = 3X^2 + (aZ^4)$, і $t = -2s + m^2$.

A.3.6. Змішані координати

Представлення точки еліптичної кривої в афінних, проективних координатах, координатах Якобі або модифікованих координатах Якобі має обчислювальні переваги й недоліки. Немає ніякої системи координат, яка забезпечує обидва як швидкі складання, так і швидкі подвоєння. Можливо змішування різних координат, тобто додання двох точок, де перша задається в деякій одній системі координат, а друга – в деякій іншій системі координат. Ми можемо також вибрати систему координат результату. Оскільки ми маємо чотири різні види систем координат, це надає велике число можливостей. Змішані координати надають кращу комбінацію систем координат для подвоєнь або складань для мінімізації часу для піднесення до ступеня еліптичної кривої. Змішані координати діють найефективніше в алгоритмі попереднього обчислення [32].

A.4. КРИПТОГРАФІЧНЕ БІЛІНІЙНЕ ВІДОБРАЖЕННЯ

A.4.1. Існування спарювання

Криптографічне білінійне відображення e_n використовується в таких криптографічних застосуваннях як схеми цифрового підпису, направленого шифрування, криптографічні протоколи тощо. Криптографічне білінійне відображення e_n (спарювання) реалізоване шляхом обмеження області спарювання Вейла або Тейта таким чином:

$$e_n : <G1> \times <G2> \to \mu n.$$

Криптографічне білінійне відображення e_n задовольняє таким властивостям:

– білінійність: $e_n(aG_1, bG_2) = e(G_1, G_2)^{ab}$, де $a, b \in [0, n-1]$).

– невиродженість: $e_n(G_1, G_2) \neq 1$.

– обчислюваність: існує ефективний алгоритм для обчислення e_n.

Примітка. Існує два типи спарувань:

1) випадок $G_1 = G_2$; 2) випадок $G_1 \neq G_2$.

Нехай E є еліптичною кривою над $F(q)$, де $q = p^m$, і нехай n буде відносно простим числом для характеристики p функції $F(q)$. Група n-кручення генерується двома точками, коли n – відносно просте число до p. $E(F(q))$ включає точку n-кручення G_1, тому що $\#E\,(F(q))$ кратне простому n. Відзначимо, що цей факт не має на увазі $E(F(q)) \supset E[n]$. Спарювання Вейла і Тейта є невиродженими білінійними відображеннями, визначеними над еліптичною кривою E для μ_n. Спарювання Вейла визначається над групою n-кручення $E[n]$, і тому вимагає $E(F(q^B))$ таке, щоб $E(F(q^B)) \supset E[n]$. З іншого боку, спарювання Тейта можливе тільки якщо $E(F(q^B)) \ni G_1$ і $F(q^B) \supset \mu_n$. Тому обчислення спарувань Тейта ефективніше, ніж обчислення спарювання Вейла.

А.4.2. Визначення спарувань Вейла і Тейта

Нехай E/F є еліптичною кривою, n є простим дільником порядку кривої $\#E\,(F(q))$, і $E[n]$ є групою n-крутіння. Вважатимемо, що n є відносно простим числом до q. Тоді $E[n]$ містить дві точки G_1 і G_2 – такі, що $E[n] = <G1> \times <G2>$. Нехай B є найменшим цілим числом – таким, що $q^B - 1$ кратне n. Тоді $E[n] \subseteq E(F(qB))$.

Спарювання Вейла є спарюванням $e_n : E[n] \times E[n] \to \mu_n$,

а спарювання Тейта є спарюванням $E(F(q^B))[n] \times E(F(q^B)) \,/\, nE(F(q^B)) \to \mu_n$.

Детальна інформація про спарювання Вейла і Тейта наведена в [32,54,55].

А.4.3. Криптографічне білінійне відображення

Криптографічне білінійне відображення e_n реалізується через обмеження області спарувань Вейла або Тейта, які задовольняють умовам невиродженості, білінійності й допустимої складності обчислення. У криптографічних застосуваннях криптографічні білінійні відображення e_n описуються двома способами:

1) $e_n : <G_1> \times <G_2> \to \mu_n$;

2) $e_n : <G_1> \times <G_1> \to \mu_n$,

де $<G_1>$ та $<G_2>$ є циклічними групами порядку n,

μ_n є циклічною групою n-х коренів з одиниці.

А.5. ФУНКЦІЇ ПЕРЕТВОРЕННЯ

А.5.1. Перетворення рядків октетів на бітові рядки OS2BSP і навпаки BS2OSP

Примітиви OS2BSP і BS2OSP для перетворення між рядків октетів на бітові рядки та навпаки визначаються таким чином:

Функція OS2BSP (x) приймає рядок октетів x як вхідні дані, інтерпретує його як бітовий рядок y (природним чином) і виводить бітовий рядок y.

Функція BS2OSP (y) приймає бітовий рядок як вхідні дані, довжина яких кратна 8, і виводить унікальний рядок октетів x – такий, що y = OS2BSP (x).

Примітка. Безліч кінцевих бітових рядків є $\{0, 1\}^*$. Безліч кінцевих рядків октетів є $\{0, 1\}^{8*}$.

А.5.2. Перетворення бітових рядків на цілі числа BS2IP і навпаки I2BSP

Примітиви BS2IP і I2BSP призначені для перетворення бітових рядків на цілі числа і навпаки та визначаються таким чином:

Функція BS2IP (x) відображає бітовий рядок x в ціле значення x' таким чином: якщо $x = \langle x_{l-1}, \ldots, x_0 \rangle$, де $x_0, \ldots, x_{l-1}$ є біти, то значення x' визначається як $x' = \sum_{0 \le i < l,\, x_i = 1} 2^i$, i.

Функція I2BSP (m, l) приймає як вхідні дані два ненегативні цілі m і l і виводить унікальний бітовий рядок x довжини l – такий, що BS2IP (x) = m, якщо таке x існує. Інакше функція виводить повідомлення про помилку.

Вважається, що бітовою довжиною ненегативного цілого m є число бітів у його бінарному поданні, тобто $\lceil \log 2\,(m+1) \rceil$.

У подальшому для зручності позначення Oct (m) визначається як Oct (m) = I2BSP (m, 8).

Примітка. Перетворення I2BSP (m, l) не може бути виконаним, якщо, і тільки якщо бітова довжина m є більшою за довжину l.

А.5.3. Перетворення рядків октетів на цілі числа OS2IP і навпаки I2OSP

Примітиви OS2IP і I2OSP призначені для перетворення рядків октетів на цілі числа, і навпаки – цілих чисел на рядки октетів і визначаються таким чином:

Функція OS2IP (x) приймає як вхідні дані рядок октетів x і виводить ціле число BS2IP (OS2BSP (x)).

Функція I2OSP (m, l) приймає як вхідні дані два ненегативних цілих числа m та l і виводить унікальний рядок x октетів довжини l – такий, що OS2IP (x) = m, якщо існує таке x. Інакше функція виводить повідомлення про помилку.

Довжина ненегативного цілого m в октетах дорівнює числу розрядів у його поданні за основою 256, тобто $\lceil \log 256\,(m+1) \rceil$.

Примітка 1. Застосування примітиву I2OSP (m, l) є невдалим, якщо, і тільки якщо, довжина m в октетах є більшою за l.

Примітка 2. Довжина ненегативного цілого m в октетах позначається як L (m).

А.5.4. Перетворення елементів кінцевого поля на цілі числа $\mathrm{FE2IP}_F$

Примітив $\mathrm{FE2IP}_F$ призначений для перетворення елементів кінцевого поля $F_в$ на цілі числа і визначається таким чином:

Функція $\mathrm{FE2IP}_F$ відображає елемент $a \in F_в$ на ціле значення a' таким чином: якщо елемент $a \in F_в$ m-кортежем $(a_1, \ldots, a_m)$, де порядок $F_в$ $q = p^m$ і $a_i \in [0, p-1]$ для $1 \le i \le m$, то значення a' визначається як $a' = \sum_{1 \le i \le m} a_i p^{i-1}$.

А.5.5. Перетворення рядків октетів на елементи кінцевого поля: OS2FEPF, і навпаки FE2OSPF

Примітиви $\mathrm{OS2FEP}_F$ та $\mathrm{FE2OSP}_F$ призначені для взаємного перетворення рядків октет на елементи поля і навпаки та визначаються таким чином:

Функція $\mathrm{OS2FEP}_F(x)$ приймає як вхідні дані рядок октетів x і виводить (унікальний) елемент поля $a \in F$ – такий, що $\mathrm{FE2OSP}_F(a) = x$, якщо таке a існує, а інакше невдача.

Примітка 1. $\mathrm{OS2FEP}_F(x)$ зазнає невдачі, якщо, і тільки якщо, x не має довжину точно $\lceil \log_{256} |F| \rceil$, або $\mathrm{OS2IP}(x) \geq |F|$.

Функція $\mathrm{FE2OSP}_C(a)$ приймає як вхідні дані елемент a поля F і виводить рядок октетів $\mathrm{I2OSP}(a', l)$, де $a' = \mathrm{FE2IP}_F(a)$ та $l = L(|F|-1)$. Тому вихідні дані $\mathrm{FE2OSP}_F(a)$ завжди будуть рядком октетів довжини точно $\lceil \log_{256} |F| \rceil$.

Примітка 2. $L(x)$ є довжиною цілого x в октетах (ненегативне ціле число).

А.5.6. Перетворення точок еліптичної кривої на октетові рядки: EC2OSPE, і навпаки OS2ECPE

Стислі точки еліптичної кривої

Нехай E є еліптичною кривою над явно заданим кінцевим полем F, де поле F має характеристику p. Точка $P \neq O_E$ може бути подана в будь-якій стислій, нестислій або гібридній формі. Якщо $P = (x, y)$, то (x, y) є нестислою формою P. Стислою формою P є пара $(x, \tilde{y})$, де $\tilde{y} \in \{0, 1\}$ і визначається таким чином:

1. Якщо $p \neq 2$ і $y = 0_E$, то $\tilde{y} = 0$.

Якщо $p \neq 2$ і $y \neq 0_E$, то $\tilde{y} = ((y'/p^r) \bmod p) \bmod 2$, де $y' = \mathrm{FE2IP}_F(y)$, і де F є найбільше ненегативне ціле – таке, щоб $p^r \mid y'$.

Примітка 1. Якщо $p \neq 2$ та $y = (y_1, \ldots, y_m) \neq 0_F$, що еквівалентно, то нехай j є найменший індекс з $yj \neq 0$, тоді $\tilde{y} = yj \bmod 2$.

2. Якщо $p = 2$ і $x = 0_E$, то $\tilde{y} = 0$.

Якщо $p = 2$ і $x \neq 0_E$, то $\tilde{y} = \lfloor z'/2^r \rfloor \bmod 2$, де $z = y/x$, де $z' = \mathrm{FE2IP}_F(z)$, і де F є найбільше ненегативне ціле – таке, що 2^r кратне $\mathrm{FE2IP}_F(1_F)$.

Примітка 2. Якщо $p = 2$ і $x \neq 0$, то це еквівалентно твердженню, що $y/x = (z_1, \ldots, z_m)$, і тоді визначимо $\tilde{y} = z_1$.

Гібридною формою $P = (x, y)$ є трійка $(x, \tilde{y}, y)$, де $\tilde{y}$ є таким, як у попередньому параграфі.

Алгоритми відбудови точок

Існують ефективні процедури відбудови точок, тобто обчислення y з $(x, \tilde{y})$. Сутність процедур полягає в такому.

1. Якщо $p \neq 2$ і нехай $(x, \tilde{y})$ буде стислою формою (x, y). Точка (x, y) задовольняє рівнянню Вейєрштраса $y^2 = F(x)$, визначеному в п. 5.1.1 або 5.1.3 [9796-3]. Якщо $F(x) = 0_F$, то існує тільки один можливий варіант для y, а саме: $y = 0_F$. Інакше, якщо $F(x) \neq 0_F$, то існує два можливих варіанти y, які відрізняються тільки знаком, і правильний вибір визначається як $\tilde{y}$. Існують добре відомі алгоритми для обчислення квадратних коренів у кінцевих полях, і тому два варіанти y легко обчислюються.

2. Якщо $p = 2$ і нехай $(x, \tilde{y})$ буде стислою формою (x, y). Точка (x, y) задовольняє рівнянню $y^2 + xy = x^3 + ax^2 + b$. Якщо $x = 0_F$, то ми маємо $y^2 = b$, тому y унікально визначається й легко обчислюється. Інакше, якщо $x \neq 0_F$, то встановлюючи $z = y/x$, ми маємо $z^2 + z = g(x)$, де $g(x) = x + a + bx^{-2}$. Значення y унікально визначається й легко обчислюється зі значень z і x, і тому цього достатньо для обчислення z. Для обчислення z відзначимо, що для фіксованого x, якщо z є одним рішенням для рівняння $z^2 + z = g(x)$, існує точно одне інше рішення, а саме: $z + 1_F$. Легко обчислити ці два кандидати значень z, і, як легко побачити, правильний вибір z визначається через $\tilde{y}$.

Функції перетворення

Нехай E є еліптичною кривою над явно заданим кінцевим полем F.

Примітиви $EC2OSP_E$ і $OS2ECP_E$ для перетворення між точками на еліптичній кривій E і рядками октетів визначаються таким чином:

1) Функція $EC2OSP_E(P, f_{mt})$ приймає як вхідні дані точку P на E і специфікатор формату f_{mt}, який представляється одним із символічних значень, стислим, нестислим або гібридним. Вихідними даними є рядок октетів EP, обчислений таким чином:

– якщо $P = 0_E$, то $EP = \text{Oct}(0)$;

– якщо $P = (x, y) \neq 0_E$, зі стислою формою $(x, \tilde{y})$, то $EP = H \| X \| Y$, де

H є одинарний октет виду $\text{Oct}(4U + C \cdot (2 + \tilde{y}))$, а

$U = 1$ якщо f_{mt} є нестислим або гібридним, інакше $U = 0$;

$C = 1$ якщо f_{mt} є стислим або гібридним, інакше $C = 0$.

Причому:

X є рядок октетів $FE2OSP_F(x)$;

Y є рядок октетів $FE2OSP_F(y)$, якщо f_{mt} є нестислим або гібридним, а інакше Y є нульовим рядком октетів.

2) Функція $OS2ECP_E(EP)$ приймає як вхідні дані рядок октетів EP. Якщо існує точка P на кривій E і специфікатор формату f_{mt} – такий, що $EC2OSP_E(P, f_{mt}) = EP$, то функція виводить P (у нестислій формі), а інакше функція зазнає невдачі. Відзначимо, що точка P, якщо існує, унікально визначається, і тому функція $OS2ECP_E(EP)$ є цілком визначеною.

Примітка. Якщо формат fmt є нестислим, то використовуються обидві координати – x та y, тому значення $\tilde{y}$ обчислювати не потрібно.

Перетворення цілих чисел на точки еліптичної кривої I2ECP

Нехай E є еліптичною кривою над явно заданим кінцевим полем F. Примітив I2ECP для перетворення з цілих чисел на точки еліптичної кривої визначається таким чином:

Функція $I2ECP(x)$ приймає як вхідні дані ціле;

Здійснюється перетворення цілого числа x на рядок октетів

$$X = I2OSP(x, L(|F|-1)).$$

Якщо існує точка P на кривій E – така, що $EC2OSP_E(P, \text{стисла}) = 03 \| X$, то функція виводить P, інакше функція зазнає невдачі.

Примітка 1. Вихідні дані для точки P, якщо вона існує, унікально визначаються.

Примітка 2. Функція I2ECP на вхідному x дасть негативну відповідь, якщо точка P не належить кривій E і точка P така, що

$$EC2OSPE(P, \text{стисла}) = 03 \| X.$$

Примітка 3. Діапазон значень I2ECP складає приблизно половину $E(F)$, тому I2ECP завжди виводить точки еліптичної кривої $P = (x, y)$ із стислою формою $(x, 1)$. Вона не виводить ні точку на нескінченності, ні точку на еліптичній кривій $P = (x, y)$ зі стислою формою $(x, 0)$.

Примітка 4. У деяких застосуваннях, заснованих на еліптичній кривій, може бути потрібною функція відображення рядків октетів в точки еліптичної кривої. Функція I2ECP використовується як компонент разом з OS2IP або функцією гешування.

А.6. ПАРАМЕТРИ ОБЛАСТІ ЕЛІПТИЧНОЇ КРИВОЇ ТА ВІДКРИТИЙ КЛЮЧ

А.6.1. Параметри області еліптичної кривої над $F(q)$

Параметри еліптичної кривої над $F(q)$, включаючи особливі випадки $F(p)$ і $F(2^m)$, повинні визначати:

– розмір поля $q = p^m$, який визначає базове кінцеве поле $F(q)$, де p повинно бути простим числом, і вказує на базис, що використовується для представлення елементів поля у випадку $m > 1$;

– якщо $q = p^m$, *причому* $p > 3$, два елементи поля a і b у $F(q)$, які визначають рівняння еліптичної кривої

$$E: y^2 = x^3 + ax + b;$$

– якщо $q = 2^m$, то два елементи поля a і b у $F(2^m)$, які визначають рівняння еліптичної кривої

$$E: y^2 + xy = x^3 + ax^2 + b;$$

– якщо $q = 3^m$, то два елементи поля a і b у $F(3^m)$, які визначають рівняння еліптичної кривої

$$E: y^2 = x^3 + ax^2 + b;$$

– елементи поля x_G і y_G у $F(q)$, які визначають базову точку $G = (x_G, y_G)$ порядку n на еліптичній кривій E;

– порядок n базової точки G;

– значення кофактора $h = \#E(F(q))/n$, якщо воно вимагається базовою схемою криптографічного перетворення.

А.6.2. Генерація ключів еліптичної кривої

Для заданого дійсного набору параметрів еліптичної кривої особистий ключ і відповідний відкритий ключ можуть бути генеровані таким чином:

1) обирається випадкове або псевдовипадкове ціле d на відрізку $[2, n-2]$, яке має бути захищене від несанкціонованого розкриття й бути непередбачуваним;

2) обчислюється точка $P = (x_P, y_P) = dG$;

3) як ключова пара вибирається (P, d), де P – відкритий ключ, і d – особистий ключ.

У деяких застосуваннях відкритий ключ обчислюється як eG, за умови, що $de = 1 \bmod n$.

А.7. ОСНОВНА ІНФОРМАЦІЯ ЩОДО ЕЛІПТИЧНИХ КРИВИХ

У цьому підрозділі подані відомості щодо еліптичних кривих, які необхідні для асиметричних криптографічних перетворень у групі точок еліптичної кривої.

А.7.1. Властивості еліптичних кривих

Порядок еліптичної кривої

Еліптична крива E над полем $F(q)$ має бінарною операцією «+» складання точок $E \times E \to E$, для якої двом точкам Q_1, Q_2 на E може бути обчислена третя точка $Q_1 + Q_2$ на E. Еліптична крива E є абелевою групою щодо операції «+».

Число точок еліптичної кривої E (включаючи точку нескінченності 0_E) називається порядком E і позначається як $\#E(F(q))$. Порядок кривої $\#E(F(q))$ визначається згідно з теоремою Хасе:

$$q+1-2\sqrt{q} \le \#E(F(q)) \le q+1+2\sqrt{q}. \qquad \text{(A.15)}$$

Ціле число t, визначене як $t = q+1-\#E(F(q))$, називається ***слідом***. Теорема Хасе визначає межу по сліду.

А.7.2. Аномальні та суперсингулярні криві

Еліптична крива E, що визначена над полем $F(q)$ з порядком $\#E(F(q))=p^m$, де $q=p^m$, називається ***аномальною***.

Еліптична крива E, визначена над $F(q)$ зі слідом t, кратним p, називається ***суперсингулярною***.

Аномальні криві вразливі до атак з використанням алгоритмів Аракі-Сатока [13], Смарта [15] і Сімаіва [14].

Відносно суперсингулярних кривих існують вразливості, засновані на алгоритмах Фрея-Рюка та Менезіса-Окамото-Ванстона [32].

А.7.3. Груповий закон для еліптичних кривих над полем $F(2^m)$

А.7.3.1. Груповий закон в афінних координатах

Нехай $F(2^m)$ для деякого $m \ge 1$ є кінцевим полем. Нехай E є еліптичною кривою над $F(2^m)$, що задана рівнянням:

$$Y^2 + XY = X^3 + aX^2 + b \qquad \text{(A.16)}$$

з $a, b \in F(2^m)$ – такими, що $b \ne 0_F$.

В афінних координатах груповий закон на еліптичній кривій (А.16) визначається таким чином:

1) точка на нескінченності є одиничним елементом 0_E щодо «+»;

2) якщо $R=(x, y) \ne 0_E$ є точкою на E, що задана в афінній системі координат, то $-R=(x, x+y)$;

3) для точок $R_1=(x_1, y_1)$ та $R_2=(x_2, y_2)$ – таких, що $R_1 \ne \pm R_2$ і $R_1, R_2 \ne 0_E$ існує сума у вигляді точки $R_3=(x_3, y_3)$, де:

$$x_3 = r^2 + r + x_1 + x_2 + a;$$
$$y_3 = r(x_1 + x_3) + x_3 + y_1, \qquad \text{(A.17)}$$

причому

$$r = (y_2 + y_1) / (x_2 + x_1).$$

4) якщо $R=(x, y)$ є точка на E – така, що $R \ne 0_E$ та $x \ne 0$, то її подвоєнням є точка $2R=(x_3, y_3)$, де:

$$x_3 = r^2 + r + a;$$
$$y_3 = x^2 + (r + 1_F)\, x_3, \qquad \text{(A.18)}$$

причому

$$r = x + (y / x).$$

У разі коли $R=(0_F, y)$, її подвоєнням є $2R=0_E$.

При обчисленні згідно з (А.18) необхідно виконувати операцію ділення за модулем, що вимагає значних потужностей. Складність обчислень може бути пониженою при виконанні групових операцій у проективних координатах.

А.7.3.2. Груповий закон у проективних координатах над полем $F(2^m)$

Проективний аналог афінного рівняння (А.16) визначається над $П_{\text{proj}}(F(2^m))$ і задається однорідним кубічним рівнянням:

$$Y^2Z + XYZ = X^3 + aX^2Z + bZ^3 \text{ з } a, b \in F(2^m). \qquad (А.19)$$

Безліч усіх трійок, еквівалентних (X, Y, Z), позначається як $(X, Y, Z)/\sim$.

Еліптична крива, задана в проективних координатах, складається з усіх точок $R = (X, Y, Z)$ функції $F(2^m) \times F(2^m) \times F(2^m) \setminus \{(0_F, 0_F, 0_F)\}$ – таких, що трійка (X, Y, Z) є рішенням рівняння (А.19).

Коли еліптична крива задається в афінних координатах, а точка R – у проективних координатах, то справедливі твердження:

1) якщо $Q = (x_Q, y_Q)$ є афінною точкою E, то $R = (x_Q, y_Q, 1_F)$ є відповідною точкою в проективних координатах;

2) якщо $R = (X, Y, Z)$ (з $Z \neq 0_F$) є рішенням (А.19), то $Q = (X/Z, Y/Z)$ є відповідною афінною точкою E;

3) Існує тільки одне рішення (А.19) з $Z = 0_F$, а саме $(0_F, 1_F, 0_F)$. Ця точка відповідає 0_E.

У проективних координатах груповий закон на еліптичній кривій, що задана для (А.19), формулюється таким чином:

1) точка $(0_F, 1_F, 0_F)$ є одиничним елементом 0_E щодо операції «+»;

2) якщо $R = (X, Y, Z) \neq (0_F, 1_F, 0_F)$ є точкою на E, заданою в проективних координатах, то:

$R = (X, X + Y, Z)$.

Нехай $R_1 = (X_1, Y_1, Z_1)$ та $R_2 = (X_2, Y_2, Z_2)$ є дві точки на E – такі, що $R_1 \neq R_2$ і $R_1, R_2 \neq (0_F, 1_F, 0_F)$, тоді суму цих точок як точку $R_3 = (X_3, Y_3, Z_3)$ можна обчислити за допомогою таких формул:

$$X_3 = su;$$

$$Y_3 = t(u + s^2X_1Z_2) + s^3Y_1Z_2 + su; \qquad (А.20)$$

$$Z_3 = s^3Z_1Z_3,$$

де $s = X_2Z_1 + X_1Z_2$, $t = Y_2Z_1 + Y_1Z_2$, і $u = (t^2 + ts + as^2)Z_1Z_2 + s^3$.

Нехай $R = (X, Y, Z) \neq (0_F, 1_F, 0_F)$ є точка на E, тоді її подвоєння $2R = (X_3, Y_3, Z_3)$ можуть бути обчислені за допомогою таких формул:

$$X_3 = st;$$

$$Y_3 = X^4s + t(s + YZ + X^2); \qquad (А.21)$$

$$Z_3 = s^3,$$

де $s = XZ$ і $t = bZ^4 + X^4$.

А.7.4. Груповий закон для еліптичних кривих над полем $F(3^m)$

А.7.4.1. Груповий закон в афінних координатах

Нехай $F(3^m)$ для деякого цілого $m \geq 1$ є кінцевим полем. Нехай також E є еліптичною кривою над полем $F(3^m)$, що задана рівнянням:

$$Y^2 = X^3 + aX^2 + b, \text{ з } a, b \in F(3^m), \qquad (А.22)$$

причому $a, b \neq 0_F$.

В афінних координатах груповий закон на еліптичній кривій, що задана як (7.7), визначається таким чином:

1) точка на нескінченності є одиничним елементом 0_E щодо операції «+»;

2) якщо $R = (x, y) \neq 0_E$ є точкою на E, що задана в афінній системі координат, тоді

$$R = (x, x + y);$$

3) якщо $R_1 = (x_1, y_1)$ та $R_2 = (x_2, y_2)$ є дві відмінні точки на кривій E – такі, що $R_1 \neq \pm R_2$ і $R_1, R_2 \neq 0_E$, тоді їх сумою є точка $R_3 = (x_3, y_3)$, де:

$$x_3 = r^2 - a - x_1 - x_2,$$

$$y_3 = r(x_1 - x_3) - y_1, \qquad \text{(A.23)}$$

причому

$$r = (y_2 - y_1) / (x_2 - x_1);$$

4) якщо $R = (x, y)$ є точка на кривій E – така, що $R \neq 0_E$ та $y \neq 0_F$, то її подвоєнням є точка $2R = (x_3, y_3)$, координати якої визначаються згідно з формулами:

$$x_3 = r^2 - a + x,$$

$$y_3 = r(x - x_3) - y, \qquad \text{(A.24)}$$

причому $r = ax / y$ (окрім випадків, коли $R = (x, 0_F)$, то її подвоєнням є $2R = 0_E$.

А.7.4.2. Груповий закон у проективних координатах

Проективний аналог афінного рівняння (А.22) визначається над $\Pi_{\text{proj}}(F(3^m))$ і задається однорідним кубічним рівнянням:

$$Y^2Z = X3 + aX^2Z + bZ^3 \text{ з } a, b \in F(3^m). \qquad \text{(A.25)}$$

Еліптична крива, задана в проективних координатах, складається з усіх точок $R = (X, Y, Z)$ для $F(3^m) \times F(3^m) \times F(3^m) / \{(0_F, 0_F, 0_F)\}$ – таких, що трійка (X, Y, Z) є розв'язком рівняння (А.25).

Якщо еліптична крива задається в афінних координатах, а точка R – у проективних координатах, то справедливі твердження:

1) якщо $Q = (x_Q, y_Q)$ є афінною точкою E, то $R = (x_Q, y_Q, 1_F)$ є відповідною точкою в проективних координатах;

2) якщо $R = (X, Y, Z)$ (з $Z \neq 0_F$) є рішенням (7.10), то $Q = (X/Z, Y/Z)$ є відповідною точкою в афінних координатах;

3) існує тільки одне рішення рівняння (А.25) з $Z = 0_F$, а саме: точка $(0_F, 1_F, 0_F)$, що відповідає 0_E.

У проективних координатах груповий закон на еліптичній кривій, що задана для (А.25), є таким:

1) точка $(0_F, 1_F, 0_F)$ є одиничним елементом 0_E щодо операції «+».

2) якщо $R = (X, Y, Z) \neq (0_F, 1_F, 0_F)$ є точкою на кривій E, що задана в проективних координатах, то й $R = (X, X + Y, Z)$.

3) якщо $R_1 = (X_1, Y_1, Z_1)$ та $R_2 = (X_2, Y_2, Z_2)$ є дві відмінні точки на кривій E, але такі, що $R_1 \neq \pm R_2$ і $R_1, R_2 \neq (0_F, 1_F, 0_F)$, тоді їх сума $R_3 = (X_3, Y_3, Z_3)$ може бути обчислена за допомогою формул:

$$X_3 = st^2Z_1Z_2 - s^3u;$$

$$Y_3 = t(sX_1Z_2 - t^2Z_1Z_2 + s^2u) - s^3Y_1Z^2;$$
$$Z_3 = s^3Z_1Z_2, \qquad \text{(A.26)}$$

причому $s = X_2Z_1 - X_1Z_2$, $t = Y_2Z_1 - Y_1Z_2$, та $u = aZ_1Z_2 + X_1Z_2 + X_2Z_1$;

Якщо $R = (X, Y, Z) \neq (0_F, 1_F, 0_F)$ є точкою на кривій E, тоді її подвоєння $2R = (X_3, Y_3, Z)$, тобто координати X_3, Y_3 і Z_3 можуть бути обчислені за допомогою таких формул:

$$X_3 = tY;$$
$$Y_3 = s(XY^2 - t) - Y^4;$$
$$Z_3 = Y^3Z,$$

причому

$$s = aX \text{ і } t = s^2Z - aY^2Z + XY^2.$$

Виконання операцій додавання та подвоєння при скалярному множенні вимагає виконання складної операції ділення за модулем над полем $F(3^m)$. Цей недолік деякою мірою усувається при застосуванні проективних базисів.

А.7.5. Умови існування еліптичної кривої

А.7.5.1. Порядок еліптичної кривої, що визначена над полем $F(P)$

Слід кривої E над полем $F(p)$ згідно з теоремою Хасе обмежений відрізком $[-2\sqrt{p}, 2\sqrt{p}]$. Також згідно з теоремою Вотерхауза для t в діапазоні $[-2\sqrt{p}, 2\sqrt{p}]$ існує еліптична крива E над $F(p)$ зі слідом t.

Теорема Вотерхауза. Кожне ціле n в інтервалі, що заданий згідно з теоремою Хасе, є порядком деякої еліптичної кривої, визначеної над $F(p)$.

А.7.5.2. Порядок еліптичної кривої, що визначена над полем $F(P^m)$

Слід кривої E над полем $F(2^m)$ згідно теореми Хасе обмежений відрізком $[-2\sqrt{2^m}, 2\sqrt{2^m}]$. Згідно з теоремою Вотерхауза для t в діапазоні $[-2\sqrt{2^m}, 2\sqrt{2^m}]$ існує еліптична крива E над $F(2^m)$ із слідом t.

Теорема Вотерхауза. Нехай t є цілим числом, де $|t| \leq 2\sqrt{2^m}$, тоді існує еліптична крива, що визначена над полем $F(2^m)$, порядку $2^m + 1 - t$, якщо, і тільки якщо, виконується одна з таких умов:

– t непарне;

– $t = 0$;

– m непарне і $t^2 = 2^{m+1}$;

– m парне і $t^2 = 2^{m+2}$ або $t^2 = 2^m$.

А.7.5.3. Порядок еліптичної кривої, що визначена над полем $F(3^m)$

Слід E над полем $F(p^m)$ згідно з теоремою Хасе обмежений відрізком $[-2\sqrt{3^m}, 2\sqrt{3^m}]$. Згідно з теоремою Вотерхауза для t в діапазоні $[-2\sqrt{3^m}, 2\sqrt{3^m}]$ існує еліптична крива E над $F(3^m)$ зі слідом t.

Теорема Вотерхауза. Нехай t є ціле, де $|t| \leq 2\sqrt{3^m}$. Тоді існує еліптична крива, визначена над $F(3^m)$ порядку $3^m + 1 - t$, якщо, і тільки якщо, дотримується одна з таких умов:

1) t не кратне 3;

2) m непарне і виконується одна з умов:

– $t = 0$;

– $t^2 = 3^{m+1}$ та $p = 3$.

3) m парне і виконується одна з умов:

– $t^2 = 4 \cdot 3^m$;

– $t^2 = 3^m \cdot 3$;

– $t = 0$.

Нехай E є еліптичною кривою над $F(q)$, де $q = p^m$, і нехай n буде відносно простим числом для характеристики p функції $F(q)$. Група n-кручення генерується двома точками, коли n – відносно просте число до p. $E(F(q))$ включає точку n-кручення G_1, оскільки $\#E(F(q))$ кратне простому n. Відзначимо, що цей факт не має на увазі $E(F(q)) \supset E[n]$. Спарювання Вейла і Тейта є не виродженими білінійними $\supset$ відображеннями, визначеними над еліптичною кривою E для μ_n. Спарювання Вейла визначається над групою n-кручення $E[n]$ і тому вимагає $E(F(q^B))$ таке, щоб $E(F(q^B)) \supset E[n]$. З іншого боку, спарювання Тейта можливе тільки, якщо $E(F(q^B)) \in G_1$ і $F(q^B) \supset \mu_n$. Тому обчислення спарувань Тейта ефективніше, ніж обчислення спарювання Вейла.

А.8. БАЗОВА ІНФОРМАЦІЯ ЩОДО КРИПТОСИСТЕМ, ЩО ҐРУНТУЮТЬСЯ НА ЕЛІПТИЧНИХ КРИВИХ

У цьому розділі наведено інформацію щодо стійкості та складності криптографічних перетворень у групі точок еліптичних кривих. Щодо стійкості мають на увазі стійкість проти атаки «Повне розкриття», а щодо складності – складність виконання основних арифметичних операцій та окремих етапів криптографічних перетворень.

А.8.1. Основні задачі при атаках на особисті ключі

А.8.1.1. Задача дискретного логарифмування в групі точок еліптичної кривої (ECDLP)

Для еліптичної кривої E над полем $F(q)$, відомої базової точки $G \in E(F(q))$ з порядком n, і точки $Q \in E(F(q))$, задачею дискретного логарифмування в групі точок еліптичної кривої є пошук цілого $x \in [0, n-1]$ – такого, що $Q = x\,G$, якщо таке ціле x, тобто особистий ключ, існує. При правильному виборі загальних параметрів та їх розмірів, складність дискретного логарифмування носить експоненційний характер.

А.8.1.2. Обчислювальна задача Діффі-Геллмана в групі точок еліптичної кривої (ECDHP)

Для еліптичної кривої E над полем $F(q)$, відомої базової точки $G \in E(F(q))$ з порядком n, а також точок $aG, bG \in E(F(q))$, обчислювальною задачею еліптичної кривої Діффі-Геллмана є обчислення точки еліптичної кривої abG. При виборі загальних параметрів та їх розмірів у відповідності з рекомендаціями складність обчислювальної задачі носить експоненційний характер або близький до нього.

А.8.1.3. Вирішувальна задача Діффі-Геллмана в групі точок еліптичної кривої (ECDDHP)

Для еліптичної кривої E над полем $F(q)$, відомої базової точки $G \in E(F(q))$ з порядком n і точок $aG, bG, Y \in E(F(q))$, вирішувальною задачею еліптичної

кривої Діффі-Геллмана є задача визначення, чи виконується рівняння $Y = abG$, чи ні. При виборі загальних параметрів та їх розмірів відповідно до рекомендацій складність вирішувальної задачі носить експоненційний характер або близький до нього.

А.8.1.4. Білінійна задача Діффі-Геллмана (BDH)

Білінійна задача Діффі-Геллмана відповідно до криптографічного білінійного відображення описується двома способами:

1) для двох груп $< G_1 >$ та $< G_2 >$ з порядком n, криптографічним білінійним відображенням e_n: $< G_1 > \times < G_2 > \to \mu_n$, aG_1, $bG_1 \in < G_1 >$ та aG_2, $cG_2 \in < G_2 >$, білінійною задачею Діффі-Геллмана є задача обчислення $e_n (G_1, G_2)^{abc}$;

2) для групи $< G_1 >$ з порядком n, криптографічним білінійним відображенням e_n: $< G_1 > \times < G_1 > \to \mu_n$, та aG_1, bG_1 $cG_1 \in < G_1 >$, білінійна задача Діффі-Геллмана є задачею обчислення $e_n (G_1, G_1)^{abc}$.

А.8.2. Алгоритми визначення дискретних логарифмів у групі точок еліптичної кривої

А.8.2.1. Складність дискретного логарифмування в групі точок еліптичної кривої (ECDLP)

Складність задачі ECDLP залежить від вибору еліптичних кривих $E/F(q)$ і розміру n порядку базової точки G. Нижче наводиться короткий огляд алгоритмів оцінки складності вирішення задачі дискретного логарифмування ECDLP. При цьому еліптична крива E над полем $F(q)$ повинна бути вибрана відповідно визначеним цілям захисту від можливих атак та загроз.

Розмір n має бути встановлений відповідно до визначених цілей захисту проти алгоритму «малий крок – великий крок» різних варіантів алгоритму Полларда ρ.

Мінімальна величина порядку точки n для досягнення достатнього захисту має становити 160 або більше бітів.

А.8.2.2. Методи дискретного логарифмування в групі точок еліптичної кривої

Вважаються ефективними такі методи для визначення дискретних логарифмів на еліптичній кривій:

1) алгоритм Покліга-Сільвера-Геллмана. Це є метод «розділяй і володарюй», який зводить задачу дискретного логарифма для еліптичної кривої E, визначеної над полем $F(q)$, до завдання дискретного логарифма в циклічних підгрупах простого порядку, кратного $\#E(F(q))$;

2) алгоритм «малий крок – великий крок» і різні варіанти алгоритму Полларда;

3) алгоритм Фрея-Рюка й алгоритм Менезиса-Окамото-Ванстона, які обидва зводять задачу дискретного логарифмування в циклічній підгрупі E з простим порядком n до задачі дискретного логарифмування в розширеному полі $F(q^B)$, але $F(q)$ такого, що n кратне $(q^B - 1)$ (вважається, що алгоритм Фрея-Рюка є найбільш слабким (складнішим), ніж алгоритм Менезиса-Окамото-Ванстоуна);

4) алгоритми Аракі-Сатоха, Смарта і Семайва, які можуть бути застосовані для вирішення задачі дискретного логарифмування відносно еліптичної кривої E, визначеної над полем $F(p^m)$ (у цьому випадку $\#E(F(p^m)) = p^m$).

А.8.2.3. MOV умова

Нехай n є порядком точки еліптичної кривої, причому n є також простим дільником порядку еліптичної кривої $\#E(F(q))$. Значення B задається як найменше ціле число – таке, що n кратне $q^B - 1$. Як указано у 8.2.2, алгоритми Фрея-Рюка і Менезиса-Окамото-Ванстона зводять завдання дискретного логарифмування в групі точок еліптичної кривої над полем $F(q)$ до завдання дискретного логарифма в кінцевому полі $F(q^B)$. Тобто задача дискретного логарифмування в групі точок еліптичної кривої $E/F(q)$ зводиться до вирішення завдання дискретного логарифма в кінцевому полі $F(qB)$. Таким чином MOV-дозволяє вибрати ступінь B, який гарантує еквівалентність складності розв'язання задачі дискретного логарифмування в групі точок еліптичної кривої та задачі дискретного логарифма у випадку кінцевого поля. Для застосувань, що засновані на використанні спарувань Вейла і Тейта, рекомендується використовувати розумно малі значення B, наприклад 6.

А.8.3. Алгоритми скалярного множення точок еліптичної кривої

Основною, й по суті єдиною, операцією в групі точок еліптичної кривої є операція скалярного множення, при якій ціле число, наприклад k, множиться на точку G, тобто обчислюється точка

$$Q = kG.$$

Зрозуміло, що потрібно мінімізувати складність скалярного множення. Тому вирішенню цієї важливої задачі приділяється значна увага. Розглянемо один із основних алгоритмів скалярного множення, що називається базовим алгоритмом.

А.8.3.1. Базові алгоритми скалярного множення

Скалярне множення точки еліптичної кривої виконується за допомогою добре відомого алгоритму «подвоєння та складання» [31–32]. Нехай k є довільним l-бітовим позитивним цілим числом і нехай $k = k_{l-1}2^{l-1} + \ldots + k_1 2 + k_0$ є бінарним представленням k, де $k_{l-1} = 1$. Тоді обчислення точки $Q = kG$ можна виконати за таким алгоритмом:

1) Присвоїти $Q := G$.

2) У циклі від $i = l - 2$ до $i = 0$ виконати:

а) $Q := 2Q$;

б) якщо $k_i = 1$, то $Q := Q + G$.

Таким чином, при довільно вибраному k для обчислення kG необхідно виконати $(l-1)$ подвоєнь еліптичної кривої та близько $l/2$ складань точок на еліптичній кривій.

Скалярне множення цілого числа на точку еліптичної кривої також може бути виконане з використанням алгоритму «складання – віднімання», заснованого на застосуванні несуміжної форми (NAF). NAF форма представлення числа k визначена в [7]. При NAF представленні довжина числа k приймає значення l або $l + 1$. Нехай також k є довільним l-бітовим позитивним цілим числом і має $k = k_l 2^l + k_{l-1}2^{l-1} + \ldots + k_1 2 + k_0$ значно-бінарне подання k, для якого $k_i = 0, +1, -1$, і ніякі два значення k_i і k_{i+1} обидва разом є не ненульовими.

Тоді скалярне множення, тобто знаходження $Q = kG$, можна виконати з використанням такого алгоритму:

Присвоїти $Q := O_E$.

У циклі від $i = l - 2$ до $i = 0$ виконати такі дії:

1) обчислити $Q := 2Q$;

2) якщо $k_i = 1$, то обчислити $Q := Q + G$;

3) якщо $k_i = -1$, то обчислити $Q := Q - G$.

При застосуванні цього алгоритму для випадково вибраного k для обчислення точки kG необхідно виконати щонайбільше l подвоєнь і близько $l/3$ складань точок на еліптичній кривій.

А.8.3.2. Алгоритм скалярного множення з попередньо обчисленою таблицею

Скалярне множення на еліптичній кривій ефективно реалізується з використанням алгоритму «вікна» [32]. Алгоритм «вікна» складається з двох частин: попереднього обчислення та основного циклу. На етапі попереднього обчислення значення точки $G_i = iG$ обчислюються для деякого $w > 0$ для непарних $i \in [1, 2^w - 1]$, де w визначає розмір попередньо обчисленої таблиці. На етапі основного циклу kG обчислюється за допомогою попередньо обчисленої точки. Розглянемо алгоритм більш детально.

Нехай k є довільним позитивним цілим числом і представлено в бінарному вигляді $k = k_{l-1} 2^{l-1} + \ldots + k_1 2 + k_0$, причому $k_{l-1} = 1$. Тоді обчислення точки $Q = kG$ можна виконати за таким алгоритмом.

Попереднє обчислення

1. Присвоїти $G_1 := G$, $G_2 := 2G$.

2. Для $i = 1$ до $2^{w-1} - 1$ виконати $G_{2i+1} := G_{2i-1} + G_2$.

Основний цикл

1. Присвоїти $j := l - 1$, $Q := G$.

2. Поки $j \geq 0$, виконати:

а) якщо $k_j = 0$, то присвоїти $Q := 2Q$ та $j := j - 1$;

б) інакше обчислити $h := \sum_{j \geq i \geq t} k_i 2^{i-t}$, $Q := 2^{j-t+1} Q + G_h$ для найменшого цілого t – такого, що

$$j - t + 1 \leq w, k_t = 1 \text{ і } j := t - 1.$$

Аналіз показує, що для попереднього обчислення потрібне одне подвоєння та $2^{w-1} - 1$ складань. Для головного циклу щонайменше потрібне $(l - 1)$ подвоєнь і близько $(l / (w + 1)$ складань. Таким чином, для випадково вибраного k складність обчислення точки kG можна оцінити як $(l - 1)$ подвоєнь та близько $(l / (w + 1) + 2^{w-1} - 1)$ складань точок еліптичної кривої.

А.8.4. Алгоритми обчислення спарювань точок ЕК

Для обчислення значень точок еліптичних кривих, що спарюють, переважно застосовують методи Вейла або Тейта. Тому розглянемо їх детально.

А.8.4.1. Допоміжні функції обчислень

Допоміжні функції використовуються при обчисленні спарювань методами Вейла і Тейта. Тому спочатку розглянемо їх.

Для обчислення спарувань застосовуються дві допоміжні функції – *Fmag*.

Функція $F(P, Q, R)$ визначається для $E(F(q^B)) \ni P = (x_P, y_P)$, $Q = (x_Q, y_Q)$, $R = (x_R, y_R)$ таким чином.

Для еліптичної кривої E з рівнянням $Y_2 = X_3 + aX + b$ над полем $F(p^m)$ $(p > 3)$:
1) якщо $P = 0_E$ і $Q = 0_E$, то $F(P, Q, R) = 1_F$;
2) якщо $P = 0_E$, то $F(P, Q, R) = x_R - x_Q$;
3) якщо $Q = 0_E$, то $F(P, Q, R) = x_R - x_P$;
4) якщо $x_P \neq x_Q$, то $F(P, Q, R) = (x_Q - x_P)y_R - (y_Q - y_P)x_R - x_Q y_P + x_P y_Q$;
5) якщо $y_P \neq y_Q$, то $F(P, Q, R) = x_R - x_P$;
6) якщо $b = 0_F$ і $x_P = y_P = x_Q = y_Q = 0_F$, то $F(P, Q, R) = x_R$;
7) якщо, то $F(P, Q, R) = (-3x_P{}^2 - a)(x_R - x_P) +$
$+ 2y_P(y_R - y_P) = -(y_R - y_P)^2 + (x_{R-} x_P)^2 (2x_P + x_R)$.

Для еліптичної кривої E з рівнянням $Y^2 + XY = X^3 + aX^2 + b$, над полем $F(2^m)$:
1) якщо $P = 0_E$ і $Q = 0_E$, то $F(P, Q, R) = 1_F$;
2) якщо $P = 0_E$, то $F(P, Q, R) = x_R + x_Q$;
3) якщо $Q = 0_E$, то $F(P, Q, R) = x_R + x_P$;
4) якщо $x_P \neq x_Q$, то $F(P, Q, R) = (x_Q + x_P)y_R + (y_Q + y_P)x_R + x_Q y_P + x_P y_Q$;
5) якщо $y_P \neq y_Q$, то $F(P, Q, R) = x_R + x_P$;
6) якщо $x_P = x_Q = 0_F$ і $y_P = y_Q = \sqrt{b}$, то $F(P, Q, R) = x_R$
інакше $F(P, Q, R) = (y_P + x_P{}^2)(x_R + {}_{xP}) + xP(y_R + y_P) =$
$= (y_R + y_P)^2 + (x_R + x_P)(y_R + y_P + (x_R + x_P)(a + x_R))$.

Для еліптичної кривої E з рівнянням $Y^2 = X^3 + aX^2 + b$, над полем $F(3^m)$:
1) $P = 0_E$ і $Q = 0_E$, то $F(P, Q, R) = 1F$;
2) якщо $P = 0_E$, то $F(P, Q, R) = x_R - x_Q$;
3) якщо $Q = 0_E$, то $F(P, Q, R) = x_R - x_P$;
якщо $x_P \neq x_Q$, то $F(P, Q, R) = (x_Q - x_P)y_R - (y_Q - y_P)x_R - x_Q y_P + x_P y_Q$;
якщо $y_P \neq y_Q$, то $F(P, Q, R) = x_R - x_P$;
якщо $b = 0_F$ і $x_P = y_P = x_Q = y_Q = 0_F$, то $F(P, Q, R) = x_R$;
якщо, то $F(P, Q, R) = (y_R - y_P)^2 - (x_R - x_P)^2 (2x_P + a + x_R)$.

Функція $g(P, Q, R)$ визначається для
$P, Q, R \in E(F(q^B))$ як $g(P,Q,R) = F(P, Q, R) / F(P + Q, -P - Q, R)$.

Функція $d_n(P, Q)$ для двох точок P і Q на кривій E з порядком $n > 2$ обчислюється з використанням такого алгоритму.
1) Нехай $n = n_{l-1}2^{l-1} + \cdots + n_1 2 + n_0$ $(n_{l-1} \neq 0)$ є бінарним представленням, де $n_i = 0,1$.
2) Присвоїти $Y := P$, $h := 1$.
3) для $i = l - 2$ до 0 виконати:
а) $h := h^2 \cdot g(Y, Y, Q)$, $Y := 2Y$;
б) $P_{n_i} \neq 0$ то
$h := h \cdot g(Y, P, Q)$;
$Y := Y + P$.
4) Вивести h як $d_n(P, Q)$.

А.8.4.2. Алгоритм обчислення спарювання Вейла

Нехай G_1 і G_2 є точки на кривій E з $nG_1 = nG_2 = 0_E$. Спарювання Вейла $e_n(G_1, G_2)$ обчислюється через виконання таких кроків:

1) Випадково вибрати точки R на E так, щоб усі точки O_E, G_2, R, $G_1 + R$ були відмінними.

2) Обчислити значення $e_n(G_1, G_2) = (d_n(G_2, G_1 + R)\, d_n(G_1, -R)) / (d_n(G_2, R)\, d_n(G_1, G_2 - R))$.

3) Якщо в процесі обчислень виникає ділення на нуль, то необхідно повторити обчислення з новою точкою R.

А.8.4.3. Алгоритм обчислення спарювання Тейта

Нехай G_1 і G_2 є точки на кривій E з $nG_1 = nG_2 = 0_E$. Спарювання Тейта $e_n(G_1, G_2)$ обчислюється через виконання таких кроків:

1) Випадково вибрати точки R на кривій E.

2) Обчислити значення $e_n(G_1, G_2) = d_n(G_1, G_2 - R) / d_n(G_1, -R)$.

3) Якщо в процесі обчислень виникає ділення на нуль, то необхідно повторити обчислення з новою точкою R.

А.8.5. Перевірка достовірності загальних параметрів еліптичної кривої та відкритого ключа

У цьому підрозділі наведено перелік загальних параметрів ЕК, вимоги та порядок їх перевірки за критерієм достовірності. Якщо набір параметрів області, що перевіряється, є недійсним, то необхідно вважати, що криптографічна система є непрацездатною, усі припущення щодо її захищеності потрібно анулювати, включаючи всі криптографічні операції, а також конфіденційні й особисті ключі. Зазначене вимагає, щоб перед кожним використанням набору загальних параметрів ЕК користувач мав гарантію, що набір є дійсним.

Гарантія дійсності може бути досягнута за умови, що:

– загальні параметри ЕК були генеровані користувачем або для користувача довірчою третьою стороною;

– параметри ЕК були явно затверджені користувачем або довірчою третьою стороною.

А.8.5.1. Перевірка достовірності загальних параметрів *ЕК* над полем $F(q)$

При перевірці загальних параметрів на достовірність необхідно виконати такі операції:

1) перевірити, що q є простим ступенем p^m;

2) перевірити, що коефіцієнти ЕК a та b, а також базова точка ЕК (x_G, y_G) є елементами базового поля;

3) перевірити, що $4a^3 + 27b^2 \neq 0$, якщо $q = p^m$ з $p > 3$, $b \neq 0$, якщо $q = 2^m$, і $a, b \neq 0$, якщо $q = 3^m$;

4) якщо еліптична крива була генерована з використанням SEED, то перевірити, що a і b були вироблені з використанням відповідного значення SEED;

5) якщо $q = p^m$ з $p > 3$, то перевірити, що $y_G{}^2 = x_G{}^3 + ax_G + b$ в полі $F(p^m)$. Якщо $q = 2^m$, то перевірити, що $y_G{}^2 + x_G y_G = xG^3 + ax_G{}^2 + b$ в полі $F(2^m)$. Якщо $q = 3^m$, то перевірити, що $y_G{}^2 = x_G{}^3 + ax_G{}^2 + b$ в полі $F(3^m)$;

6) перевірити, що порядок базової точки n є простим і що $n > 4\sqrt{q}$;

7) перевірити, що $nG = O_E$;

8) обчислити $h' = \lfloor (\sqrt{q} + 1)^2 / n \rfloor$ та перевірити, що $h = h'$;

9) перевірити ЕК на можливість застосування та виключення відомих слабких кривих, у тому числі:

– перевірити, що MOV умова виконується, тобто складність вирішення дискретного логарифму в полі $F(q^B)$ є достатньою для забезпечення необхідного рівня стійкості, коли задача дискретного логарифмування на еліптичній кривій ECDLP над $E/F(q)$ зводиться до DLP дискретного логарифмування над полем $F(q^B)$, наприклад, з використанням алгоритму Фрея-Рюка або Менезиса-Окамото-Ванстона;

– перевірити, що ЕК не є аномальною, тобто що порядок кривої не співпадає з порядком поля, $\#E(F(q)) \neq q$.

Якщо хоча б одна вимога не виконується, то загальні параметри вважаються недійсними.

А.8.5.2. Перевірка достовірності відкритого ключа

Для заданого дійсного набору параметрів еліптичної кривої та відкритого ключа Q, який має певне значення, достовірність відкритого ключа може бути перевірена таким чином:

1) перевірити, що Q не є точкою на нескінченності 0_E;

2) перевірити, що координати точки x_Q і y_Q є елементами в полі $F(q)$;

3) якщо $q = p^m$ з $p > 3$, то перевірити, що $y_Q^2 = x_Q^3 + ax_Q + b$ в полі $F(q)$;

4) якщо $q = 2^m$, то перевірити, що $y_Q^2 + x_Q y_Q = x_Q^3 + ax_Q^2 + b$ в полі $F(2^m)$;

5) якщо $q = 3^m$, то перевірити, що $y_Q^2 = x_Q^3 + ax_Q^2 + b$ в полі $F(3^m)$;

6) перевірити, що $nQ = 0_E$.

У разі невдачі при будь якій перевірці відкритий ключ повинен вважатися недійсним. Ніякі криптографічні операції з ним не можуть виконуватись. Тому перед використанням відкритого ключа користувач повинен пересвідчитись, що він дійсний, наприклад, мати гарантію, що:

– достовірність відкритого ключа була явно перевірена користувачем;

– достовірність відкритого ключа була явно перевірена для користувача третьою довірчою стороною.

Примітка. Неверифікований відкритий ключ за певних умов може використовуватися, якщо він був генерований або явно затверджений об'єктом, що заслуговує довіру користувача, протягом життєвого циклу ключа.

А.9. СКЛАДНІСТЬ ОБЧИСЛЕНЬ У РІЗНИХ СИСТЕМАХ КООРДИНАТ

У цьому розділі наводяться оцінки складності виконання операцій в різних системах координат [31–32].

У разі коли $E(F(q))$ з $p > 3$, існує п'ять систем координат: афінні координати, проективні координати, координати Якобі, модифіковані координати Якобі та змішані координати. У випадках $E(F(2^m))$ і $E(F(3^m))$ існує дві системи координат: афінні координати та проективні координати.

Позначимо відповідно афінні координати, проективні координати, координати Якобі й модифіковані координати Якобі символами A, P, J і J_m; час складання точок в координатах C_1 і C_2 з результатом в координатах C_3 як $t(C_1 + C_2 = C_3)$; час подвоєння точки в координатах C_1 з результатом в координатах C_2 як $t(2C_1 = C_2)$; і множення точок (зворотне та зведення у квадрат) у полі $F(q)$ як M (відповідно I та S). У таблиці А.1 надаються характеристики системи координат $E(F(q))$ з $p > 3$. У таблиці А.2 надаються характеристики системи координат $E(F(2^m))$. У таблиці А.3 надаються характеристики системи координат $E(F(3^m))$.

Таблиця А.1. **Характеристики системи координат $E(F(q))$ з $p > 3$**

Подвоєння		Складання	
Операція	Складність обчислення	Операція	Складність обчислення
$t(2P)$	$7M + 5S$	$t(Jm + Jm)$	$13M + 6S$
$t(2J)$	$4M + 6S$	$t(J + J)$	$12M + 4S$
$t(2Jm)$	$4M + 4S$	$t(P + P)$	$12M + 2S$
$t(2Jm = J)$	$3M + 4S$	$t(J + A = Jm)$	$9M + 5S$
$t(2A = Jm)$	$3M + 4S$	$t(Jm + A = Jm)$	$9M + 5S$
$t(2A = J)$	$2M + 4S$	$t(J + A = J)$	$8M + 3S$
–	–	$t(Jm + A = J)$	$8M + 3S$
–	–	$t(A + A = Jm)$	$5M + 4S$
$t(2A)$	$2M + 2S + I$	$t(A + A)$	$2M + S + I$

Таблиця А.2. **Характеристики системи координат $E(F(2^m))$**

Подвоєння		Складання	
Операція	Складність обчислення	Операція	Складність обчислення
$t(2P)$	$7M + 5S$	$t(P + P)$	$16M + 2S$
$t(2A)$	$2M + S + I$	$t(A + A)$	$2M + I$

Таблиця А.3. **Характеристики системи координат $E(F(3^m))$**

Подвоєння		Складання	
Операція	Складність обчислення	Операція	Складність обчислення
$t(2P)$	$9M + 3S$	$t(P + P)$	$15M + 2S$
$t(2A)$	$3M + S + I$	$t(A + A)$	$2M + S + I$