УДК 681.3.06

І. Д. ГОРБЕНКО, д-р техн. наук, Д. В. ШЕВЧЕНКО

КІЛЬЦЕВИЙ ПІДПИС НА ОСНОВІ УДОСКОНАЛЕНОГО КРИПТОПРИМІТИВУ ЗВЕДЕННЯ МНОЖИНИ ЗНАЧЕНЬ В ОДНЕ

Вступ

Недоліком більшості алгоритмів кільцевого підпису на сьогоднішній день є залежність розміру підпису від розміру групи. Для вирішення цієї задачі Нгюєн [1] запропонував реалізацію абстрактного математичного опису криптопримітиву зведення множини значень в одне (надалі криптопримітив зведення), а також кільцевий підпис з фіксованим розміром на її основі. З проведеного аналізу в роботі [2] видно, що за швидкісними характеристиками запропонований Нгюєном кільцевий підпис є фаворитом у порівнянні з кільцевими підписами, що сформовані на інших методах побудови підписів. Недоліками даного підпису є велика кількість сеансовий ключів, що використовуються при формуванні підпису, а також 11 складових підпису, які необхідно передавати разом з повідомленням. Згідно [1] криптопримітив зведення має експонентну складність підробки зведеного значення, тому може використовуватися як основа для розроблення нових підписів. Таким чином актуальною задачею є продовження напрямку розробки кільцевих підписів на основі криптопримітиву зведення запропонованого Нгюєном, що залучає:

– розроблення алгоритму кільцевого підпису з фіксованим розміром, зменшеною кількістю складових підпису та сеансовий ключів;

– проведення аналізу стійкості розробленого кільцевого підпису.

Аналіз стійкості розробленого кільцевого підпису повинен залучати:

– аналіз стійкості до підробки зведеного значення удосконаленого криптопримітива зведення Нгюєна;

– аналіз складності обчислення слабких місць складових підпису;

– аналіз стійкості до атаки екзестеційної підробки фактичним підписувачем;

– аналіз можливості формування підпису не користувачем групи;

– аналіз стійкості до атаки екзестеційної підробки зловмисником.

Запропонований кільцевий підпис на удосконаленому криптопримітиві зведення

Даний підпис розробляється для роботи в системі на ідентифікаторах, де існує уповноважений на генерування особистих ключів PKG (надалі уповноважений PKG), який формує ключ користувача групи, використовуючи свій особистий ключ та ідентифікаційні дані користувача групи. Таким чином уповноваженим PKG формуються такі загальносистемні параметри

$$params_{PKG} = (Q, Q_{pub}, G_1, p) \qquad (1)$$

де Q – базова точка адитивної групи G_1 простого порядка p, $Q_{pub} = s_m Q$ – відкритий ключ уповноваженого PKG, $s_m \in_R Z_p^*$ – випадкове значення особистого ключа уповноваженого PKG.

Пропонується удосконалення криптопримітиву зведення Нгюєна, яке полягає у введенні додаткового зв'язку між базовою точкою Q та точкою P, що використовується для формування загальносистемних параметрів криптопримітиву зведення. Таким чином зв'язок представлений рівнянням $P = cQ$, де $c \in_R Z_p^*$, дозволяє пов'язати вхідні дані для формування підпису, що в свою чергу дозволить виконати вимоги до кільцевих підписів представлених у роботах [3,4,5]. Більш детально застосування даного удосконалення обговорюється далі. Удосконалення криптопримітиву зведення змінює опис властивості "ефективність генерування".

Ефективність генерування: Для генерування параметрів криптопримітиву зведення використовуються загальносистемні параметри, що надані уповноваженим PKG. Генеруються випадкові значення $c, s \in_R Z_p^*$, обчислюється точка $P = cQ$, та формується параметр

$t = (p, G_1, G_M, e, P)$, де G_1 – адитивна група еліптичної кривої, G_M – мультиплікативна група поля, $e: G_1 \times G_1 \to G_M$ – білінійне відображення декартового множення елементів адитивної групи у мультиплікативну групу. Згідно з властивостями адитивних груп еліптичних кривих, в групі, що має простий порядок, кожний елемент групи є генератором. Таким чином точка $< P >= G_1$ простого порядку p. Далі обчислюється значення $t' = (P, P_{pub} = sP, ..., s^q P)$, де q є верхньою границею числа елементів, що акумулюються криптопримітивом зведення. Після формування відкритого параметру t' необхідно зробити перевірку на рівність $Q \stackrel{?}{=} s^i P$, де $i \in \{1, ..., q\}$. При виконанні такого рівняння необхідно згенерувати нове значення $s \in_R Z_p^*$ і знов сформувати відкритий параметр t'. Відповідні функції f, g для параметрів t, t' визначаються таким чином:

$$g(f(u, X)) = \prod_{i=1}^{k} (x_i + s) uP, \tag{2}$$

де $X = \{x_1, ..., x_k\}$ – множина геш-значень ідентифікаційних даних, значення u є відкритим параметром. Геш-функції $H: \{0,1\}^* \to Z_p^*$, яка необхідна для одержання геш-значень від ідентифікаційних даних користувачів групи, та $H_2: \{0,1\}^* \to Z_p^*$, яка необхідна для одержання геш-значення від повідомлення. Використання двох різних геш-функцій підвищує стійкість до колізій як зазначено у [6].

Значення c є таємним значенням, використовується при формуванні підпису і може зберігатися упродовж існування групи, або знижується після формування підпису.

Загальносистемні параметри що надаються ФП:

$$params = (t, t', Q, Q_{pub}, f, g.u) \tag{3}$$

Формування підпису складається з формування відкритого ключа групи, формування таємного ключа групи, та формуванням складових підпису. При цьому при формуванні декількох підписів від незмінної групи обчислюються тільки значення таємного ключа групи та складових підпису.

Формування геш-значення від повідомлення

$$h = H_2(M) \tag{4}$$

Формування відкритого ключа групи :

$$gpk = V = g(f(u, X)) = \prod_{i=1}^{k} (x_i + s) uP, \tag{5}$$

де елементи групи є геш-значення ідентифікаційних даних користувачів групи, що представлені множиною $X = \{H(ID_i)\}_{i=1}^{k}$.

Формування таємного ключа групи :

$$X' = X \setminus \{x_j\}, \tag{6}$$

де геш-значення ідентифікаційних даних ФП

$$x_j = H(ID_j). \tag{7}$$

$$W = g(f(u, X')) = \prod_{i=1, i \neq j}^{k} (x_i + s) u P, \tag{8}$$

та особистий ключ ФП

$$s_j = R_{ID_j} = \frac{1}{x_j + s_m} Q \tag{9}$$

Складова підпису для маскування ідентифікаційних даних ФП:

$$R_1 = c^{-1} \cdot hW = c^{-1} \cdot h \cdot u \cdot \prod_{i=1, i \neq j}^{k} (x_i + s) P \tag{10}$$

Єднальний елемент

$$s_1 = (x_j + s) \cdot c \tag{11}$$

Складова підпису. що надає гарантію дійсності повідомлення

$$S_2 = h \cdot zR_{ID_j}, \tag{12}$$

де $z \in_R Z_p^*$ – сеансовий ключ.

Перевірочні елементи

$$R_2 = sS_2 = s \cdot h \cdot zR_{ID_j} = \frac{s \cdot h \cdot z}{x_j + s_m} Q. \tag{13}$$

$$R_3 = z \cdot hQ \tag{14}$$

Умова виконання першого перевірочного рівняння надає гарантії використання при формуванні кільцевого підпису ідентифікаційних даних всіх користувачів групи.

$$e(s_1 R_1, P) = e(V, P)^h \tag{15}$$

$$e(s_1 R_1, P) = e(P, P)^{(x_1+s)\,c\,c^{-1}\,h\,u \prod_{i=1, i\neq j}^{t}(x_i+s)} = e(P, P)^{h\,u \prod_{i=1}^{t}(x_i+s)} \tag{16}$$

$$e(V, P)^h = e(P, P)^{h\,u \prod_{i=1}^{t}(x_i+s)} \tag{17}$$

Умова виконання другого перевірочного рівняння надає гарантії дійсності повідомлення та особистого ключа ФП, гарантії належності ФП групі X.

$$e(s_1 P + Q_{pub}, S_2) = e(R_2 + R_3, Q) \tag{18}$$

$$e(s_1 P + Q_{pub}, S_2) = e((x_j + s) \cdot cP + Q_{pub}, \frac{h \cdot z}{x_j + s_m} Q) =$$

$$= e((x_j + s)Q + s_m Q, \frac{h \cdot z}{x_j + s_m} Q) = \tag{19}$$

$$= e(Q, Q)^{\frac{h \cdot z \cdot (x_j+s)}{x_j+s_m} + \frac{h \cdot z \cdot s_m}{x_j+s_m}} = e(Q, Q)^{h \cdot z} \cdot e(Q, Q)^{\frac{z\,h\,s}{x_j+s_m}}$$

$$e(R_2 + R_3, Q) = e(Q, Q)^{h \cdot z} \cdot e(Q, Q)^{\frac{z \cdot h \cdot s}{x_j + s_m}} \tag{20}$$

Значення підпису формується таким чином:

$$\sigma = (R_1, R_2, S_1, S_2, V, X) \tag{21}$$

При роботі з однією групою декілька разів замість передачі всіх ідентифікаційних даних можна передавати строку, яка посилається на визначену множину X, при цьому скорочується розмір підпису і стає дійсно фіксованим.

Аналіз складності обчислення слабких місць складових підпису

Насамперед необхідно перевірити складність обчислення єднального елемента $s_1 = (x_j + s) \cdot c$ при невідомих зловмиснику значеннях s, c і можливістю перебрати всі значення $x_j \in X$. Випадкові значення $s, c \in_R Z_p^*$, де значення p мінальну довжину порядка 2^{163}, згідно до сучасних вимог до стійкості [ДСТУ4145]. Довжина групи X мінімально дорівнює 10. Тоді кількість наслідків для $x_j = C_{10}^1 = 10$. Кількість наслідків для значень s та c дорівнює $C_{2^{163}}^1 = 2^{163}$. Таким чином максимальна кількість наслідків для одержання значення s_1 дорівнює

$$C_{10}^1 \cdot C_{2^{163}}^1 \cdot C_{2^{163}}^1 = 1{,}36 \cdot 10^{99}, \tag{22}$$

тоді максимальна складність обчислення значення s_1 дорівнює

$$I = 1{,}36 \cdot 10^{99} I_{add} + 1{,}36 \cdot 10^{99} I_{mul}, \tag{23}$$

де I_{add} – складність додавання двох елементів поля, I_{mul} – складність множення двох елементів поля.

Порівнювати будемо зі складністю вирішення дискретного логарифму еліптичної кривої з порядком адитивної групи 2^{163} повним перебором. Складність однієї операції додавання та подвоєння точок дорівнює

$$I_{add\_p} = 2I_{mul} + I_{inv} + I_{sqr} + 9I_{add} \text{ та} \tag{24}$$

$$I_{dbl\_p} = I_{inv} + 2I_{mul} + I_{sqr} + 7I_{add}, \tag{25}$$

відповідно, тоді складність вирішення дискретного логарифму повним перебором

$$I_{EC} = 7 \cdot 10^{49} I_{add} + 2 \cdot 10^{49} I_{mul} + 10^{49} I_{inv} + 10^{49} I_{sqr} + \\ + (n-1)(9 \cdot 10^{49} I_{add} + 2 \cdot 10^{49} I_{mul} + 10^{49} I_{inv} + 10^{49} I_{sqr}), \tag{26}$$

де n – порядок адитивної групи еліптичної кривої приблизно дорівнює 2^{163}, I_{inv} – складність одержання зворотного елемента мультиплікативної групи. I_{sqr} – складність одержання квадратичного елемента мультиплікативної групи. Згідно [7] $I_{inv} \approx 10,5 I_{mul}$ та $I_{sqr} \approx 0,11 I_{mul}$ і тоді зводимо рівняння (25) до рівняння обчислення складності додавання та множення елементів в полі:

$$I_{EC} = (1.05 \cdot 10^{99} + 7 \cdot 10^{49}) I_{add} + (1,48 \cdot 10^{99} + 12.61 \cdot 10^{49}) I_{mul} \tag{27}$$

Таким чином можна зробити виводи, що складність визначення значення s_1 простим перебором для невідомих значень $c, s \in Z_p^*$, де $p = 2^{163}$, та $X = \{x_1, ..., x_{10}\} \subset Z_p^*$ порівняно зі складністю рішення дискретного логарифму в групі точок еліптичних кривих над полями Z_p простим перебором.

Аналіз стійкості удосконаленого криптопримітива зведення

Згідно [1] стійкість криптопримітива зведення Нгюєна заснована на задачі $q - SDH$:

$$\Pr[(A(t,t') = (x_i, \frac{1}{x_i + s} P)) \wedge (x_i \in Z_p)] \tag{28}$$

де $t' = (P, P_{pub} = sP, s^2 P, ..., s^q P)$ та $t = (p, G_1, G_M, e, P)$, q – граничне значення криптопримітива. Тобто якщо є можливість одержання значення $(x_i, \frac{1}{x_i + s} P)$, тоді можна одержати трійку значень (x_i, W, X), де $W \in G_1, X = \{x_1, ..., x_k\} \subset Z_p \setminus \{-s\}$ таких, що виконується $(x_i \in Z_p \setminus X) \wedge ((x_i + s)W = \prod_{i=1}^{k} (x_i + s) uP)$. Формально це можна записати $f(g^{-1}(W), x_i) = f(u, X)$, або $f(g^{-1}(W), x_i) = (x_i + s) \cdot g^{-1}(W) = (x_i + s) \cdot u_1$, де $u_1 = g^{-1}(W)$. Таким чином $(x_i + s) \cdot u_1 = \prod_{i=1}^{k} (x_i + s) \cdot u$ і значення $W = u_1 P = (x_i + s)^{-1} \cdot \prod_{i=1}^{k} (x_i + s) \cdot uP$.

Удосконалення даного криптопримітиву визначається обчисленням точки

$$P = cQ \tag{29}$$

де $< Q >= G_1$ – простого порядку p, $c \in_R Z_p^*$. Удосконалення робить зв'язок між двома перевірочними рівняннями і забезпечує можливість надання гарантій щодо "належності ФП групі". Задача визначення таємного значення c дорівнює складності вирішення дискретного логарифму на еліптичній кривій. Удосконалення вимагає деяких обмежень стосовно випадкового значення $s \in_R Z_p^*$, яке полягає у додатковій перевірці рівняння значень відкритого параметру $t' = (P, P_{pub} = sP, ..., s^q P)$ базовій точці Q. У випадку рівняння будь-якого значення відкритого параметру t' з базовою точкою Q необхідно обрати нове значення $s \in_R Z_p^*$, обчислити нове значення t' та знов виконати перевірку. Таким чином стійкість удосконаленого криптопримітиву зведення не відрізняється від стійкості криптопримітиву, що запропонова-

но Нгюєном. Недоліком є додання додаткових вимог щодо випадкового значення s, але перевагами є зв'язок вхідних значень підпису, а відповідно і зв'язок двох перевірочних рівнянь, що дозволить виконання певних вимог [3,4,5].

Атака екзестеційної підробки ФП

Відкритий ключ $gpk = V = g(f(u,X))$ та множина X визначає групу користувачів. Проведемо аналіз можливості підробки повідомлення для вже сформованого підпису, тобто екзестеційну підробку. фактичним підписувачем. Для дійсного повідомлення з геш-значенням h складові підпису V, R_1, R_2, s_1, S_2, X разом з таємним значенням c, і відкритими параметрами t, t' є фіксованими значеннями. Для формування однакового підпису від двох різних повідомлень необхідно виконання рівнянь:

$$R_1 = c^{-1} \cdot hW = c^{-1} h'W', \tag{30}$$

$$S_2 = h \cdot zR_{ID_j} = h' \cdot z' R_{ID_j}, \tag{31}$$

$$R_2 = sS_2 = s \cdot h \cdot zR_{ID_j} = \frac{s \cdot h \cdot z}{x_j + s_m} Q = \frac{s \cdot h' \cdot z'}{x_j + s_m} Q. \tag{32}$$

$$R_3 = z \cdot hQ = z' \cdot h'Q \tag{33}$$

де R_{ID_j} – особистий ключ фактичного підписувача. h та h' геш-значення дійсного та підробленого повідомлення відповідно. Знаходження значення $z' = \frac{z \cdot h}{h'} \bmod p$ для рівнянь (30),(31).(32) є поліноміальною задачею, але виникає складність у вирішенні рівняння (29). Якщо визначити зв'язок між геш-значеннями повідомлень $h_1 = h' \backslash h \bmod p$, тоді рівняння (29) можна представити:

$$\prod_{i=1, i \neq j}^{k} (x_i + s)u = h_1 \prod_{i=1, i \neq j, i \neq d}^{k} (x_i + s)u \bmod p. \tag{34}$$

Розв`язок рівняння (33) можливий прн виконанні умови

$$h_1 = (x_d + s), \tag{35}$$

де $d \in \{1,...,k\} \setminus \{j\}$. Враховуючн те, що кількість можливих користувачів, які можуть бути залучені у групу для формування підпису, обмежено деякими структурами, наприклад, співробітник відділу, або робітники деякої компанії, а також властивості формуванням значень $x_i = H(ID_i)$, підбирання значення x_d для визначеного значення s є задачею перебору всіх можливих варіантів x_i. У випадку відсутності значень x_i, які відповідають умові (34) необхідно обирати нове повідомлення для підробки и знов обчислювати значення h_1. Враховуючи експоненту складність визначення заздалегідь значень h_1 та x_d, що відповідають умові (34). та розміру поля більшим за 2^{163}. перебір всіх можливих значень є задачею експонентної складності. Тоді пропонується для заздалегідь визначеного значення h_1 та будь-якого значення $x_d \in X \setminus \{x_j\}$ обчислювати значення s таким чином:

$$(x_d + s) \bmod p = h_1 \Rightarrow s = (h_1 - x_d) \bmod p \tag{36}$$

Згідно визначеного s обчислюються відкритий параметр t', Відкритий ключ групи обчислюється:

$$gpk = V = \prod_{i=1}^{k} (x_i + h_1 - x_d) \cdot uP = \prod_{i=1, i \neq d}^{k} (x_i + h_1 - x_d) \cdot h_1 \cdot uP \tag{37}$$

Таємний ключ групи обчислюється:

$$W = \prod_{i=1, i \neq j}^{k} (x_i + h_1 - x_d) \cdot uP = \prod_{i=1, i \neq j, d}^{k} (x_i + h_1 - x_d) \cdot h_1 \cdot uP \tag{38}$$

тоді згідно рівняння $W = h_1 W'$ значення W' представлено:

$$W' = \prod_{i=1, i\neq j, d}^{k} (x_i + h_1 - x_d) \cdot uP \tag{39}$$

значення особистого ключа ФП залишається незмінним

$$s_j = R_{ID_j} = \frac{1}{x_j + s_m} Q \tag{40}$$

$$gsk = (W, x_j, s_j), \text{ та} \tag{41}$$

$$gsk' = (W', x_j, s_j) \tag{42}$$

Визначення значення z' за формулою

$$z' = (h \cdot z) / h' \bmod p \tag{43}$$

Обчислення складових підпису представлено у табл.1 для геш-значень дійсного та підробленого повідомлень h та h' відповідно.

Таблиця 1

Обчислення складових підпису для дійсного та підробленого повідомлення

Дійсне повідомлення	Підроблене повідомлення
$R_1 = c^{-1} \cdot h \cdot W = c^{-1} \cdot \frac{h'}{h_1} \cdot \prod_{i=1, i\neq j, d}^{k} (x_i + h_1 - x_d) \cdot h_1 \cdot uP = c^{-1} \cdot h' \cdot \prod_{i=1, i\neq j, d}^{k} (x_i + h_1 - x_d) \cdot uP$	$R_1' = c^{-1} \cdot h' \cdot W' = c^{-1} \cdot h' \cdot \prod_{i=1, i\neq j, d}^{k} (x_i + h_1 - x_d) \cdot uP$
$S_2 = h \cdot zR_{ID_j} = \frac{h \cdot z}{x_j + s_m} Q$	$S_2' = h' \cdot z' R_{ID_j} = \frac{h' \cdot z'}{x_j + s_m} Q$
$R_2 = sS_2 = \frac{s \cdot h \cdot z}{x_j + s_m} Q = \frac{(h_1 - x_d) \cdot h \cdot z}{x_j + s_m} Q$	$R_2 = sS_2 = \frac{s \cdot h' \cdot z'}{x_j + s_m} Q = \frac{(h_1 - x_d) \cdot h' \cdot z'}{x_j + s_m} Q$
$R_3 = z \cdot hQ$	$R_3' = z' \cdot h' Q$
$s_1 = (x_j + h_1 - x_d) \cdot c$	$s_1' = (x_j + h_1 - x_d) \cdot c$

Таким чином ми одержали однакові складові підпису, але підпис приймається перевірником у випадку виконання умов перевірочних рівнянь.

Першим виконуємо церевірку підпису для дійсного повідомлення.

$$e(s_1 R_1, P) \stackrel{?}{=} e(V, P)^h \tag{44}$$

$$e(s_1 R_1, P) = e(P, P)^{(x_j + h_1 - x_d) \cdot c \cdot c^{-1} \cdot h' \cdot \prod_{i=1, i\neq j, d}^{k} (x_i + h_1 - x_d) \cdot u} =$$

$$= e(P, P)^{\prod_{i=1, i\neq d}^{k} (x_i + h_1 - x_d) \cdot h' \cdot u} \tag{45}$$

$$e(V, P)^h = e(P, P)^{\prod_{i=1, i\neq d}^{k} (x_i + h_1 - x_d) \cdot h_1 \cdot u \cdot h} =$$

$$= e(P, P)^{\prod_{i=1, i\neq d}^{k} (x_i + h_1 - x_d) \cdot h' \cdot u} \tag{46}$$

Умова першого перевірочного рівняння виконана. Перевірка другого перевірочного рівняння:

$$e(s_1 P + Q_{pub}, S_2) \stackrel{?}{=} e(R_2 + R_3, Q) \tag{47}$$

$$e(s_1 P + Q_{pub}, S_2) = e((x_j + h_1 - x_d) \cdot cP + s_m Q, \frac{h \cdot z}{x_j + s_m} Q) =$$

$$= e((x_j + h_1 - x_d) Q + s_m Q, \frac{h \cdot z}{x_j + s_m} Q) =$$

$$= e(Q,Q)^{\frac{h\cdot z\cdot(x_j+h_1-x_d)-h\cdot z\cdot s_m}{x_j+s_m}} = e(Q,Q)^{h\,z}\cdot e(Q,Q)^{\frac{h\,z\cdot(h_1-x_d)}{x_j+s_m}} \quad (48)$$

$$e(R_2+R_3,Q) = e(\frac{(h_1-x_d)\cdot h\cdot z}{x_j+s_m}Q + z\cdot hQ, Q) =$$

$$= e(Q,Q)^{h\cdot z}\cdot e(Q,Q)^{\frac{h\,z\cdot(h_1-x_d)}{x_j+s_m}} \quad (49)$$

Умова другого перевірочного рівняння виконана, таким чином підпис дійсного повідомлення з геш-значенням h приймається.

Виконуємо перевірку підпису для підробленого повідомлення з геш-значенням h'.

$$e(s_1R_1,P) \stackrel{?}{=} e(V,P)^{h'} \quad (50)$$

$$e(s_1R_1,P) = e(P,P)^{(x_j+h_1-x_d)\cdot z\cdot c^{-1}\cdot h'\cdot\prod_{i=1,i\neq j,d}^{k}(x_i+h_1-x_d)\cdot u} =$$

$$= e(P,P)^{h'\cdot\prod_{i=1,i\neq d}^{k}(x_i+h_1-x_d)\cdot u} \quad (51)$$

$$e(V,P)^{h'} = e(P,P)^{\prod_{i=1,i\neq d}^{k}(x_i+h_1-x_d)\cdot h_1\cdot u\cdot h'} =$$

$$= e(P,P)^{\prod_{i=1,i\neq d}^{k}(x_i+h_1-x_d)\cdot h_1\cdot u\cdot h_1\cdot h} \quad (52)$$

Умова виконання першого перевірочного рівняння не виконана. Перевірка другого перевірочного рівняння

$$e(s_1P+Q_{pub},S_2) \stackrel{?}{=} e(R_2+R_3,Q) \quad (53)$$

$$e(s_1P+Q_{pub},S_2) = e((x_j+h_1-x_d)Q+s_mQ,\frac{h'\cdot z'}{x_j+s_m}Q) =$$

$$= e(Q,Q)^{\frac{h'\cdot z'\cdot(x_j+h_1-x_d)-h'\cdot z'\cdot s_m}{x_j+s_m}} = e(Q,Q)^{h'\cdot z'}\cdot e(Q,Q)^{\frac{h'\cdot z'\cdot(h_1-x_d)}{x_j+s_m}} \quad (54)$$

$$e(R_2+R_3,Q) = e(\frac{(h_1-x_d)\cdot h'\cdot z'}{x_j+s_m}Q + h'\cdot z'Q, Q) =$$

$$= e(Q,Q)^{h'\cdot z'}\cdot e(Q,Q)^{\frac{h'\cdot z'\cdot(h_1-x_d)}{x_j+s_m}} \quad (55)$$

Умова виконання другого перевірочного рівняння виконується.

Таким чином підпис для підробленого повідомлення з геш-значенням h' не проходить перевірку.

Висновком даного аналізу є стійкість даного кільцевого підпису до атаки екзестеційної підробки зі сторони ФП за рахунок використання у звичайному виді геш-значення повідомлення у першому перевірочному рівнянні.

Атака формування підпису не користувачем групи

Зробимо аналіз можливості проведення атаки формування підпису без знання особистого ключа фактичного підписувача, тобто використовуючи особистий ключ користувача, що не входить до складу групи, замість особистого ключа фактичного підписувача. Обирається випадковий елемент $c \in_R Z_p^*$, формуються відкриті параметри t та t', обирається випадкові елементи функції $u,s \in_R Z_p^*$. Формується група, яка представлена множиною $X = \{x_1,...,x_k\}$, обирається випадковий індекс фактичного підписувача $j \in \{1,...,k\}$, при цьому робимо спробу сформувати підпис на ключі R_{ID_i}, де $x_i \notin X$.

Для сформованої групи обчислюються значення складових підпису

$$R_1 = c^{-1} \cdot h \cdot \prod_{i=1, i \neq j}^{k} (x_i + s) uP; \quad (56)$$

$$s_1 = (x_j + s) \cdot c; \quad (57)$$

$$S_2 = h \cdot zR_{ID_i}, \quad (58)$$

де $z \in_R Z_p^*$;

$$R_2 = sS_2 = s \cdot h \cdot zR_{ID_i}; \quad (59)$$

$$R_3 = z \cdot hQ.$$

Перше рівняння $e(s_1 R_1, P) = e(V, P)^h$ проходить перевірку, а друге перевірочне рівняння $e(s_1 P + Q_{pub}, S_2) = e(R_2 + R_3, Q)$ не дає можливості зробити атаку такого виду за рахунок використання єднального елемента s_1, який поєднує ідентифікаційні дані фактичного підписувача у відкритому ключі групи у першому рівнянні з ідентифікаційними даними у особистому ключі фактичного підписувача. Таким чином робимо перевірку другого перевірочного рівняння:

$$e((x_j + s)Q + s_m Q, h \cdot zR_{ID_i}) = e(Q, Q)^{\frac{(x_j + s + s_m) \cdot h \cdot z}{x_i + s_m}} \quad (60)$$

$$e(R_3 + R_2, Q) = e(z \cdot hQ + \frac{h \cdot z \cdot s}{x_i + s_m} Q, Q) = e(Q, Q)^{\frac{(x_i + s_m + s) \cdot h \cdot z}{x_i + s_m}} \quad (61)$$

Використання значення x_i при формуванні єднального елементу приведе до невиконання умови першого перевірочного рівняння $e(s_1 R_1, P) = e(V, P)^h$.

Висновком проведеного аналізу є неможливість формування підпису від імені групи, якщо фактичний підписувач не належить групі.

Проведення порівняльних характеристик

Таблиця 2

Порівняльний аналіз за кількістю операцій підписів запропонованого підпису та підпису Нгюєна

	Nguyen		Запропонований підпис	
	Форм.	Перев.	Форм.	Перев.
Додавання у групі G_1	9	6	0	2
Скалярне множення у G_1	12	8	4	2
Множення у мультиплікативній групі	10	0	$k+6$	0
Функція H_2	1	1	1	1
Відображення	6	10	0	4
Розпаралелювання	Так		Так	
Вразливість к атакам	Ні		Ні	

Висновки

В даній роботі запропоновано кільцевий підпис, який відповідає таким вимогам:

– визначення всіх можливих таємних ключів групи (у даній реалізації всіх таємних значень W) не повинно давати можливість підробити підпис, або визначити ідентифікаційні дані фактичного підписувача;

– використання при формуванні підпису чітко визначеної множини геш-значень ідентифікаційних даних всіх користувачів групи;

– можливість доказу належності ФП групі без можливості визначення його ідентифікаційних даних;

– можливість формування підпису тільки дійсним на даний час особистим ключем ФП;

– надання гарантії дійсності підписаного повідомлення.

Даний підпис має два сеансові ключі проти одинадцяти у Нгюєна, а максимальна кількість складових підпису зменшена до шести.

Проведено детальний аналіз кільцевого підпису:

– аналіз стійкості до підробки зведеного значення удосконаленого криптопримітива зведення Нгюєна;

– аналіз складності обчислення слабких місць складових підпису;

– аналіз стійкості до атаки екзестеційної підробки фактичним

– підписувачем;

– аналіз можливості формування підпису не користувачем групи;

– аналіз стійкості до атаки екзестеційної підробки зловмисником.

Таким чином одержано більш швидкій кільцевий підпис у порівнянні з підписом Нгюєна, який у результаті проведеного аналізу визначено стійким до різного виду атак.

Список литературы. 1. *Lan Nguyen* Accumulators from Bilinear Pairings and Applications to ID-based Ring Signatures and Group Membership Revocation 2. *Горбунко І.Д, Шевченко Д В.* Порівняльний аналіз групових та кільцевих підписів, методи побудови кільцевих підписів. 3. *Joseph K. Liu and Duncan S. Wong* Linkable Ring Signatures Security Models and New Schemes. 4. *Joseph K. Liu and Duncan S. Wong* On the Security of (Threshold) Ring Signature Schemes. 5. *Sherman Chow, Richard Lui, Lucas Hui, S M Yiu* Identity Based Ring Signature: Why, How and What Next. 6. *ISO/IEC 15946-2:2002,* Information technology – Security techniques – Cryptographic techniques based on elliptic curves – Part 2: Digital signatures. 7. *Darell Hankrson, Julio Lopez Hernandez, Alfred Menezes.* Software implementation of elliptic curve cryptography over binary fields. Advances in Cryptology Crypto '99. 8. *ДСТУ 4541-2002* Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що грунтується на еліптичних кривих. Формування та перевірка.

Харківський національний
університет радіоелектроніки

Надійшла до редколегії 25.04.2007