УДК 519.252

Д.В. ШЕВЧЕНКО

ЗАТ «Інститут Інформаційних Технологій», Україна

КІЛЬЦЕВІ ПІДПИСИ ТА ЇХ ВЛАСТИВОСТІ

Розглянуто основні методи побудови кільцевих підписів. Проведено аналіз стійкості кожного методу, визначені його недоліки та розглянуті напрямки удосконалення. Проведено порівняльний аналіз даних методів та визначені переваги.

кільцеві групові підписи, комбінуючі функції, функції акумулювання

Вступ

Платіжні системи, системи електронних торгів, електронні виборчі системи пред'являють вимоги, які можуть бути виконані при використанні групових підписів [1 – 3]. Суттєві переваги в класі групових підписів мають кільцеві підписи. На нинішній час актуальним є завдання теоретичного узагальнення та дослідження якраз кільцевих підписів. Аналіз ряда робіт відносно кільцевих підписів [4 – 10] дозволив відмітити триосновні методі побудови кільцевих підписів: 1) на основі побудування кільця з функціями *trapdoor* ; 2) на основі маскування особистого та сеансового ключів; 3) на основі використання криптографічних примітивів, що дозволяють зводити множину у одне значення.

Метою цієї статті є класифікація та порівняльний аналіз кільцевих підписів при умові що відомі вимоги до цифрового підпису.

1. Алгоритм формування цифрового підпису на основі функції trapdoor

Функцією *trapdoor* називають функцію, що має такі властивості [1]:

– поліноміальна складність прямого перетворення;

– експонентна складність зворотного перетворення без знання особистого ключа;

– поліноміальна складність зворотного перетворення зі знанням особистого ключа.

Аналіз алгоритмів цифрового підпису [2, 4] показав, що загальна ідея побудови кільця полягає у обчисленні елементів кільця за допомогою функції *trapdoor* , використовуючи у якості вхідних даних випадкове значення та відкритий ключ користувача. У загальному вигляді кільце можна представити комбінуючою функцією:

$$z = C_{k,v}(y_1,...,y_r), \qquad (1)$$

де y_i – вихідні значення функції *trapdoor* $y_i = g(x_i)$ від випадкових значень x_i; k – ключ комбінуючої функції; v – ініціююче випадкове значення комбінуючої функції. Для замикання кільця у загальному випадку значення $z = v$. Для формування кільця використовується функція *trapdoor* від випадкових значень x_i, $\forall i = 1,...,r$, причому для виконання умови $z = v$ обчислювати одне значення $x_s = g^{-1}(y_s)$. Графічна інтерпретація кільця наведена на рис. 1.

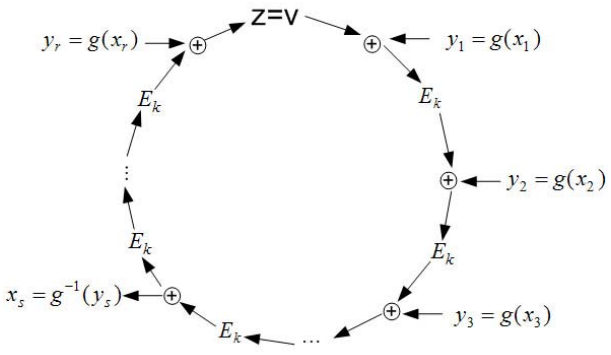

Рис. 1. Загальне представлення комбінуючої функції

Комбінуюча функція пов'язує множину значень

$y_1,...,y_r$ з випадковим ініціюючим значенням v, розгорнутий вид такої функції можна представити у вигляді залежності:

$$z = C_{k,v}(y_1,...,y_r) = \\ = E_k(y_r \oplus E_k(y_{r-1} + E_k(...\oplus E_k(y_1 + v)))), \quad (2)$$

де E_k необхідна для уникнення колізій, коли декільком вхідним множинам $Y_1 \neq Y_2$ відповідає одне значення z. У якості функції E_k можуть бути функції симетричного шифрування або геш-функції. Значення ключа k комбінуючої функції беруть у загальному випадку як геш-значення від повідомлення m. При використанні функцій симетричного шифрування рух навколо кола виконується у двох напрямках, при використанні геш-функції рух навколо кола виконується тільки у одному напрямку, що підвищує стійкість від підробок. При використанні геш-функції комбінуюча функція може бути представлена як:

$$z = \\ = H\left(m \| \left(g(x_r) \oplus H\left(m \| \left(g(x_{r-1}) \oplus ... H\left(m \| \left(g(x_1) \oplus v\right)\right)...\right)\right)\right)\right), \quad (3)$$

де m – повідомлення, що підписується.

Для наочності даний вид комбінуючої функції представлено на рис. 2.

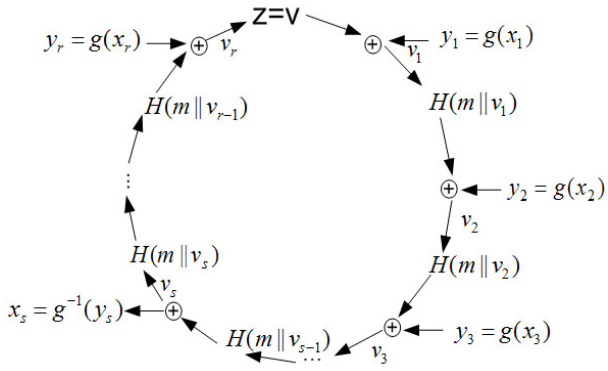

Рис. 2. Загальне представлення комбінуючої функції з використанням геш-функцій

Аналіз показав [2, 4], що до комбінуючи функцій пред'являються такі вимоги:

1. Перестановка кожного вхідного значення. Для кожного $s \in \{1,...,r\}$, та для будь-яких фіксованих значень y_i, де $i \neq s$, функція взаємооднозначно відображує y_s у вихідне значення z.

2. Ефективне розв'язання функції відносно будь-якого одиничного вхідного значення. Для кожного $s \in \{1,...,r\}$, даних значення z та вхідних значень y_i, за винятком y_s, що мають довжину b біт, необхідно забезпечити ефективне обчислювання значення y_s довжини b біт, яке задовольняє рівнянню $C_{k,v}(y_1, y_2,..., y_r) = z$.

3. Неможливість розв'язання перевіряючого рівняння без знання особистого ключа користувача для зворотного перетворення функцій $y_i = g_i(x_i)$ (trapdoor). Це означає, що для даних значень k, v та z зловмисник не може вирішити рівняння $C_{k,v}(g_1(x_1), g_2(x_2),..., g_r(x_r)) = z$ відносно x_1, x_2,..., x_r (навіть якщо зловмисник має доступ до кожної функції g_i та E_k), якщо він не може знайти рішення x_i хоча б для однієї з функцій $g_1, g_2,..., g_r$.

Стійкість комбінуючої функції, що розглядається, базується на стійкості функцій *trapdoor*. Шамір та Рівест [2] запропонували використовувати для реалізації *trapdoor* функції RSA перетворення

$$g_i(x) = x^{e_i} \bmod n_i, \quad (4)$$

з відкритим ключем користувача $P_i = (n_i, e_i)$. Проведені дослідження дозволили виділити ряд недоліків застосування RSA:

1. Якщо відомі значення $g_i(x)$, e_i та n_i, то задача знаходження x зводиться до вирішення рівняння $d = e^{-1} \bmod \varphi(n)$. При цьому знаходження функції Ейлера, тобто факторизація великого числа n є задачею субекспоненційної складності.

2. Функція $g(x_i)$ для різних користувачів групи буде видавати значення y_i різної довжини навіть при використанні однакових за довжиною значень n_i. Це робить складним комбінування y_i, тому ви-

магається, щоб всі функції мали однакову довжину вихідного значення над $\{0,1\}^b$.

Функцію *trapdoor* можна удосконалити таким чином. Спочатку обчислюються q та r, де $0 \le r < n$, які відповідають рівнянню $x = qn + r$. Далі обчислюється функція

$$g(x) = \begin{cases} qn + f(r), & \text{при умові } (q+1)n \le 2^b; \\ x. \end{cases} \quad (5)$$

де b є деякою степеню двійки, яка більше ніж всі модулі n_i.

Подальше підвищення стійкості такої функції виконується за рахунок заміни рівняння $z = v$ на $z = v \oplus E_k(v)$.

2. Кільцеві підписи, у яких маскуються значення особистого та сеансового ключів

Аналіз [6, 10, 11] показав, що основним математичним перетворення для реалізації даної концепції є білінійні відображення на сингулярних кривих $G \times G \to Z_p$.

Ці перетворення мають такі властивості:

1) невиродженість: $e(P,P) \ne 1$, $e(P,P) = \gamma$, де $< P >$ є генератором групи G порядка p, а γ є генератором мультиплікативної групи Z_p;

2) білінійність: $e(aP,bP) = e(P,P)^{ab}$, де $a,b \in Z_p$;

3) асоціативність:

$$e(aP + bP, P) = e(aP, P) \times e(bP, P).$$

Загальна ідея цього методу [6, 10] полягає у формуванні підпису у вигляді множини значень $\sigma_1,...,\sigma_r$. При цьому значення σ_i, $i \ne s$ обчислюється в загалі звичайним множенням значень відкритих ключів користувачів на випадкові значення. Тоді як у значення σ_s фактичного підписувача закладаються протилежні значення елементів σ_i, $\forall i \ne s$, які при обчисленні перевірочного рівняння скорочуються. Друга частина значення σ_s формується із особистого ключа фактичного підписувача та повідомлення. Вона безпосередньо залежить від перевірочного рівняння підпису.

Розглянемо цей метод на прикладі схеми підпису [10].

Процес генерування ключів. Відкриті ключі користувачів кільця обчислюються як $U_i = x_i P$, $V_i = y_i P$, де $< P >$ – генератор групи G порядку p, x_i та y_i – особисті ключі користувачів кільця $\forall i = 1,...,r$.

Процес формування кільцевого цифрового підпису.

Підписувач S:

1) обчислює геш-значення від повідомлення $m = H(M) \in Z_p^*$;

2) обирає випадкове значення $n \in Z_p^*$, та випадкові значення $a_i \in Z_p^*$, $\forall i \ne s$;

3) обчислює кільцевий підпис таким чином:

$$\sigma_s = \frac{1}{m + x_s + y_s n}(P - \sum_{i \ne s} a_i (mP + U_i + nV_i)), \quad (6)$$

при виконанні умови $m + x_s + y_s n = 0$ обирається інше значення $n \in Z_p^*$ і повторюється обчислення σ_s.

$$\sigma_i = a_i P, \quad \forall i \ne s. \quad (7)$$

В цілому цифровий підпис повідомлення M має вигляд:

$$\sigma = (\sigma_1, \sigma_2, ..., \sigma_n, n). \quad (8)$$

Для перевірки підпису необхідно вирішити рівняння:

$$\prod_{i=1}^{r} e(mP + U_i + nV_i, \sigma_i) = e(P,P). \quad (9)$$

Вирішивши рівняння (9), маємо:

$$\prod_{i \ne s} \gamma^{ma_i + a_i x_i + a_i y_i r} \times \prod_{i \ne s} \gamma^{\frac{1}{a_i m} + \frac{1}{a_i x_i} + \frac{1}{a_i y_i r}} \times \gamma = \gamma. \quad (10)$$

Аналіз цього методу з урахуванням можливих атак [6, 10, 11] дозволив визначити його недоліки:

1) використання відкритих ключів учасників підпису без втручання самих учасників, але можлива організація обчислення значень $\sigma_i, i \neq s$ самими учасниками. Наприклад використовуючи замість випадкових значень a_i свої особисті ключі;

2) довжина підпису залежить від кількості учасників підпису;

3) атака з можливістю додання користувачів групи у сформований підпис у більшості таких підписів.

3. Підписи на криптографічних примітивах, що дозволяють акумулювати множину значень у одне значення

Основна ідея цього методу полягає у можливості зведення множини значень у одне значення з визначеної групи для подальшого використання у криптографічних примітивах.

Аналіз [5, 6] дозволив вибрати математичну реалізацію методу, та представити конкретну реалізацію [5]. Функцією акумулювання називають пару $(\{F_l\}_{l\in N}, \{X_l\}_{l\in N})$, де F_l є сімейством функцій типа $f: U_f \times X_f{}^{расш} \to U_f$, де $X_f{}^{расш} \supseteq X_l$ та $\{X_l\}$ – значення домену для функції акумулювання. Основними властивостями даного абстрактного апарату є ефективність генерування та обчислення, а також квазікомутативність.

Ефективність генерування – властивість, що гарантує існування ефективного алгоритму G генерування випадкової функції $f \in F_l$, можливо разом з додатковою інформацією a_f, використовуючи у якості вхідного значення параметр безпеки 1^l.

Ефективність обчислення – властивість що гарантує обчислення функції $f \in F_l$ за поліноміальний час l.

Квазікомутативність – властивість, що гарантує виконання рівняння $f(f(u,x_1),x_2) = f(f(u,x_2),x_1)$ для кожного $l \in N$, $f \in F_l$, $u \in U_f$ та $x_1, x_2 \in X_l$.

Для будь-яких значень $l \in N$, де N – максимальна кількість можливих учасників підпису, функції $f \in F_l$ та набору $X = \{x_1,...,x_s\} \subset X_l$, акумульованим значенням набору X над u буде

$$v = f(...f(u,x_1)...,x_s).$$

Завдяки властивості квазі-комутативності значення v не залежить від того, у якому порядку значення x_i, $i = 1,...,s$ поступають у функцію v, тому її можна записати $v = f(u,X)$.

Стійкість функції акумулювання визначається теоремою 1 [7].

Теорема 1. Функція акумулювання визначається колізійно-стійкою [7], коли для кожного імовірно поліноміального алгоритму, який для згенерованих значень $f \in F_l$ та $u \in U_f$ обчислює значення (x,w,X) такі, що виконується рівняння

$$(X \subseteq X_l) \wedge (w \in U_f) \wedge$$
$$\wedge (x \in X_f{}^{расш} \setminus X) \wedge (f(w,x) = f(u,X)),$$

зі зневажено малою ймовірністю, тобто можна записати таким чином:

$$\Pr\left[\begin{array}{l|l} f \leftarrow F_l & (X \subseteq X_l) \wedge (w \in U_f) \\ u \leftarrow U_f & \wedge (x \in X_f{}^{расш} \setminus X) \\ (x,w,X) \leftarrow A(f,U_f,u) & \wedge (f(w,x) = f(u,X)) \end{array}\right] = \nu(1), \quad (11)$$

де $\nu(l)$ зневажено мала функція. Тобто для $l \in N$ та $f \in F_l$ доказом факту що $x \in X_l$ акумульовано за допомогою $v \in U_f$ є $w \in U_f$ кожен раз, коли $f(w,x) = v$.

Доведення теореми наведено в [5].

Додатково функція акумулювання може мати властивості додавання та видалення елементів, що зведені у акумульоване значення.

Ефективність додавання – властивість, що гарантує існування поліноміальних алгоритмів D_a, W_a, таких що $v = f(u,X)$, $x \in X, x' \notin X$ та $f(w,x) = v$ виконуються такі вимоги:

$$D_a(a_f, v, x') = v', \text{ де } v' = f(u, X \cup \{x'\}); \quad (12)$$

$$W_a(f, v, v', x, x', w) = w', \text{ де } f(w', x) = v'. \quad (13)$$

Ефективне видалення – властивість, що гарантує існування поліноміальних алгоритмів D_d, W_d, таких, що при $v = f(u, X)$, $x, x' \in X$, $x \neq x'$ та $f(w, x) = v$ виконуються такі вимоги:

$$D_d(a_f, v, x') = v', \text{ де } v' = f(u, X \setminus \{x'\}); \quad (14)$$

$$W_d(f, v, v', x, x', w) = w', \text{ де } f(w', x) = v'. \quad (15)$$

Нгюен запропонував [5] реалізацію сімейства функцій $\{F_l\}$ з використанням білінійних відображень для можливості створення криптографічних примітивів. У цілому динамічна функція акумулювання $(\{X_l\}_{l \in N}, \{F_l\}_{l \in N})$ має такі властивості:

Ефективність генерування: Використовуючи таємний параметр l, генерується

$$t = (p, G_1, G_M, e, P), \; s \in Z_p^*,$$

де $< P >$ – генератор адитивної групи G_1 порядку p, та білінійне відображення $e: G_1 \times G_1 \to G_M$.

Обчислюється значення $t' = (P, sP, ..., s^q P)$, де q являє верхню границю числа елементів, що зводяться функцією акумулювання.

Нгюєн пропонує використання двох функцій. Функція f необхідна для зведення множини у єдине значення, а функція g виконує відображення одержаного значення у необхідну групу елементів, яка потім використовується у криптографічних примітивах. Відповідні функції $(f, g) \in F_l$ для t, t' визначають як:

$$f: Z_p \times Z_p \to Z_p \text{ та } g: Z_p \to G_1;$$

$$f: (u, x) \to (x + s)u; \quad g: u \to uP. \quad (16)$$

Елементи для зведення у єдине значення представлені множиною

$$X = \{x_1, ..., x_k\} \subset Z_p \setminus \{-s\},$$

де $k \leq q$. Для перевірки запису $t' = (P, sP, ..., s^q P)$ вирішується рівняння

$$e(P, s^q P) = e(sP, s^{q-1} P) = e(s^2 P, s^{q-2} P) = ... \quad (17)$$

Запропоновані в [5] функції відповідають основним вимогам щодо сімейства функцій функції акумулювання.

Квазікомутативність. При обчисленні функції f виконується рівняння

$$f(f(u, x_1), x_2) = f(u, \{x_1, x_2\}) = (x_1 + s)(x_2 + s)u,$$

тобто виконується властивість квазікомутативності.

Ефективність обчислення. При одержання значення функції акумулювання необхідно обчислити функцію $g(f(u, X)$ відносно $u \in Z_p$ та множини вхідних значень $X = \{x_1, x_2, ..., x_k\}$:

$$g(f(u, X)) = \prod_{i=1}^{k} (x_i + s) \times uP. \quad (18)$$

При розв'язанні рівняння (18) одержуємо різні степені s^i, де $i = 1, ..., k$, які підставляються зі запису

$$t' = (P, sP, ..., s^q P),$$

при цьому становиться необов'язковим знання значення s.

Ефективність додаткових властивостей, таких як додання та видалення, можна пояснити так.

Ефективне додавання. Припустимо, що

$$V = g(f(u, X)), x \in X, x' \notin X \text{ та}$$

$$g(f(g^{-1}(W), x)) = V,$$

тоді $V' = g(f(u, X \cup \{x'\}))$ можна обчислити як

$$V' = (x' + s)V.$$

Та значення W' можна обчислити таким чином: $W' = V + (x' - x)W$, при цьому повинно виконуватись рівняння $g(f(g^{-1}(W'), x)) = V'$.

Ефективне видалення. Припустимо, що

$$V = g(f(u, X)), \; x, x' \in X, \; x \neq x' \text{ та}$$

$$g(f(g^{-1}(W), x)) = V,$$

тоді $V' = g(f(u, X \setminus \{x'\}))$ можна обчислювати як

$$V' = 1/(x' + s)V.$$

Значення W' обчислюють таким чином: $W' = (1/(x'-x))(W - V')$, при цьому повинна виконуватись рівняння $g(f(g^{-1}(W'), x)) = V'$

Висновки

1. Основними критеріями при побудові цифрових підписів є стійкість до атак та швидкість виконання. Для кожної з наведених концепцій запропоновано конкретні реалізації, але кожна має свої недоліки.

2. Основною функцією *trapdoor* є функція на основі RSA перетворення і його модифікації, але вони мають субекспоненційну складність зворотного перетворення без знання особистого ключа користувача. Для знаходження нового виду функції *trapdoor* необхідно досліджувати математичні перетворення, наприклад можливість використання у якості функції *trapdoor* білінійних відображень на сингулярних кривих.

3. Концепція побудування кільцевих підписів на основі білінійного відображення на сингулярних кривих має два основні недоліки:

– розмір підпису залежить від кількості користувачів кільця;

– практично всі підписи піддані атаці додання нового користувача у вже сформований підпис.

4. Подальший розвиток цього напрямку лежить у зменшенні розміру підпису та протистоянні атаці додання нового користувача до вже сформованого підпису.

5. У [9] описана атака на сімейство функцій, запропонованих Нгюєном, і має поліноміальну складність виконання. Також у якості перетворення для сімейства функцій можна використовувати RSA перетворення $f(u, x) = u^x \bmod N$, де $N = P \cdot Q$ – добуток двох простих чисел. Але даний випадок має субекспоненційну складність. Основна перевага даної концепції лежить у фіксованому розмірі вихідного значення, що не залежить від кількості вхідних значень, тому даний напрямок є найбільш перспективним і потребує подальшого розвитку.

6. Основними перевагами концепцій на основі білінійного відображення та функцій акумулювання є властивість квазікомутативності, тобто незалежності від порядку входження користувачів при формуванні підпису.

Література

1. Вембо Мао. Современная криптография. Теория и практика. – М: Вильямс, 2005. – 763 с.

2. Ronald L. Rivest, Adi Shamir, Yael Tauman. How to Leak a Secret: Theory and Application of Ring Signature.

3. Patrick P. Tsang, Victor K.Wei. Short linkable ring signatures for E-voting, E-cash and Attestation.

4. Emmanuel Bresson, Jacques Ster, Michael Szydlo. Threshold Ring Signatures for Ad-hoc Groups.

5. Lan Nguyen Accumulators from bilinear pairings and applications to ID-based ring signatures and group membership revocation.

6. Sherman Chow, Richard Lui, Lucas Hui, S.M. Yiu Identity Based Ring Signature: Why, How and What Next.

7. Tsang Pak Kong Cryptography in Privacy – preserving Application / A thesis Submitted in Partial Fulfillment of the Requirement for the Degree of Master of Philosophy.

8. Patrick P.Tsang, Victor K. Wei, Tony K. Chan, Man Ho Au Separable linkable threshold ring signatures.

9. Christophe Tartary and Huaxiong Wang The Bilinear Pairing-based Accumulator Proposed at CT-RSA'05 is not Collision Resistant.

10. Jing XU, Zhenfeng Zhang, Dengguo Feng A ring signature scheme using bilinear pairings.

11. Sherman Chow, Richard Lui, Lucas Hui, S.M. Yiu Identity Based Ring Signature: Why, How and What Next.

Надійшла до редакції 27.02.2006

Рецензент: д-р техн. наук, проф. В.І. Хаханов, Харківський національний університет радіоелектроніки, Харків.