УДК 681.3.067

Ю. Є. Яремчук

ФОРМУВАННЯ ТА ПЕРЕВІРЯННЯ ЦИФРОВОГО ПІДПИСУ НА ОСНОВІ РЕКУРЕНТНИХ ПОСЛІДОВНОСТЕЙ

Запропоновано метод та протокол формування і перевіряння цифрового підпису, що базуються на математичному апараті рекурентних V_k –послідовностей. У порівнянні з відомими аналогами метод має простішу процедуру завдання параметрів, а також забезпечується можливість змінювати стійкість методу залежно від порядку послідовності. Перевагою методу перед аналогами, що базуються на математичному апараті V_k –послідовностей, є те, що в ньому розмір цифрового підпису визначається лише певним числом, а не елементами послідовності з індексом цього числа.

Ключові слова: захист інформації, криптографія, автентифікація, цифрове підписування, рекурентні послідовності.

Вступ

Використання криптографічних протоколів [1–4] на основі симетричних методів передбачає, що обидві сторони довіряють один одному. Криптографічні системи з відкритим ключем (асиметричні криптосистеми) [1, 2] дозволяють реалізувати протоколи взаємодії сторін, які не довіряють один одному. Найважливішим прикладом таких систем є системи електронного цифрового підписування [1–4], що реалізують таку можливість.

В загальному випадку цифровий підпис являє собою деяке число специфічної структури, яке допускає перевірку за допомогою відкритого ключа того факту, що воно було вироблено для деякого повідомлення з використанням секретного ключа.

Цифрове підписування передбачає два етапи: формування та перевіряння цифрового підпису, що реалізується за певним протоколом [1]. Серед існуючих протоколів цифрового підписування найбільшого поширення отримали ті, що реалізують рандомізовані схеми з додаванням повідомлення, зокрема це методи Ель-Гамаля, Шнорра, DSA, ГОСТ 34.10, ECDSA [1–3]. При цьому актуальним залишається питання підвищення криптографічної стійкості методів цифрового підписування.

Так в роботі [5] представлено метод цифрового підписування, який базується на рекурентних V_k –послідовностях і забезпечує підвищення стійкості у порівнянні з відомими аналогами. Однак даний метод має збільшений розмір цифрового підпису, оскільки в ньому цифровий підпис являє собою набір з k елементів V_k –послідовності ($v_{s+i,k} \bmod p$, $i = \overline{-1, k-2}$), а не одне число s як у відомих аналогах.

Тому актуальною є розробка методу формування та перевіряння цифрового підпису підвищеної стійкості на основі рекурентних V_k –послідовностей, в якому б розмір цифрового підпису був принаймні того ж порядку, що й у відомих аналогах.

Метод формування та перевіряння цифрового підпису на основі рекурентних V_k –послідовностей.

В [6] розглянуто V_k –послідовність, яка складається з V_k^+ –послідовності та V_k^- –послідовності.

V_k^+ –послідовністю називається послідовність чисел, що обчислюються за формулою

$$v_{n,k} = g_k v_{n-1,k} + g_1 v_{n-k,k} \qquad (1)$$

для початкових значень $v_{0,k} = 1$, $v_{1,k} = g_2$ для $k = 2$; $v_{0,k} = v_{1,k} = \ldots = v_{k-3,k} = 0$, $v_{k-2,k} = 1$, $v_{k-1,k} = g_k$ для $k > 2$; де g_1, g_k – цілі числа; n і k – цілі додатні.

Обчислення елементів цієї послідовності для спадних n, починаючи з деякого значення $n = l$, буде здійснюватись таким чином

$$v_{n,k} = \frac{v_{n+k,k} - g_k \cdot v_{n+k-1,k}}{g_1}. \qquad (2)$$

V_k^- –послідовністю називається послідовність чисел, що обчислюються за формулою (2) для n – від'ємних при початкових значеннях $v_{-1,k} = 0$, $v_{-2,k} = g_1^{-1}$ для $k = 2$; $v_{-1,k} = 0$, $v_{-2,k} = g_1^{-1}$, $v_{-3,k} = v_{-4,k} = ... = v_{-k,k} = 0$ для $k > 2$.

Для будь-яких цілих додатних n, m та k отримано таку аналітичну залежність [6]

$$v_{n+m,k} = v_{m+(k-2),k} \cdot v_{n,k} + g_1 \cdot \sum_{i=1}^{k-1} v_{m+(k-2)-i,k} \cdot v_{n-k+i,k}. \qquad (3)$$

Для будь-яких цілих додатних n і m, таких що $1 \le m < n$ та будь-якого цілого додатного k існує така залежність [6]

$$v_{n-m,k} = v_{-m+(k-2),k} \cdot v_{n,k} + g_1 \cdot \sum_{i=1}^{k-1} v_{-m+(k-2)-i,k} \cdot v_{n-k+i,k}. \qquad (4)$$

Представлені рекурентні послідовності, а також отримані залежності дозволяють запропонувати такий метод формування та перевіряння цифрового підпису на їх основі.

Суть методу цифрового підписування, що пропонується (заявка на корисну модель № u 2013 06332 від 22.05.2013 р.), базується на використанні властивості (3) V_k –послідовності, яка дозволяє використовувати її для обчислення елементу $v_{n+m,k}$, а також для обчислення елементу $v_{-n+m,k}$. Крім того властивість (3) дозволяє реалізувати процедуру обчислення елементу $v_{n \cdot m,k}$. Так само на основі властивості (4) можна реалізувати процедуру обчислення елементу $v_{-n \cdot m,k}$. Все це дає можливість створення такого методу цифрового підписування.

Спочатку відправник-підписант (або центр довіри) виконує попередню процедуру вибору параметрів та обчислення ключів. При цьому він випадковим чином вибирає секретний ключ a, за допомогою якого обчислює, а потім передає одержувачу-перевіряльнику відкритий ключ $v_{-a+i,k}$, $i = \overline{-k,-1}$.

При формуванні цифрового підпису для повідомлення M відправник-підписант вибирає випадкове число b, обчислює $v_{b,k}$, визначає значення r як $r = v_{b,k}$. Далі він визначає значення s як $s = b \cdot h(M) + a \cdot r$ за допомогою обраної функції хешування h від повідомлення M. Після цього отриману множину цілих чисел $\{r; s\}$ він перетворює у цифровий підпис вигляду $DS = (0 \| r \| 0 \| s)$ і передає його разом з повідомленням M одержувачу.

При перевірці цифрового підпису одержувач спочатку обчислює $v_{-a \cdot r+i,k}$, $i = \overline{-(k-1),0}$, на основі відкритого ключа – елементів $v_{-a+i,k}$, $i = \overline{-k,k-2}$, та отриманого від підписанта значення r, а потім на основі обчислених щойно елементів та отриманого від підписанта значення s він обчислює елементи $v_{s+i,k}$, $i = \overline{-1,k-2}$.

Після цього на основі усіх обчислених підписантом елементів він обчислює елемент $v_{b \cdot h(M),k}$ як $v_{b \cdot h(M),k} = v_{-a \cdot r+s,k}$, використовуючи залежність (3), а потім обчислює значення r' як $r' = v_{\left\lfloor \frac{b \cdot h(M)}{h(M)} \right\rfloor,k}$ та перевіряє, чи виконується $r \stackrel{?}{=} r'$. Якщо так, то підпис приймається, в іншому випадку – відкидається.

Не важко пересвідчитись, що для підпису, згенерованого згідно цього методу, перевірка $r \overset{?}{=} r'$ завжди буде виконуватись.

Виходячи з цього схема формування та перевіряння цифрового підпису за даним методом буде мати вигляд, представлений на рис. 1.

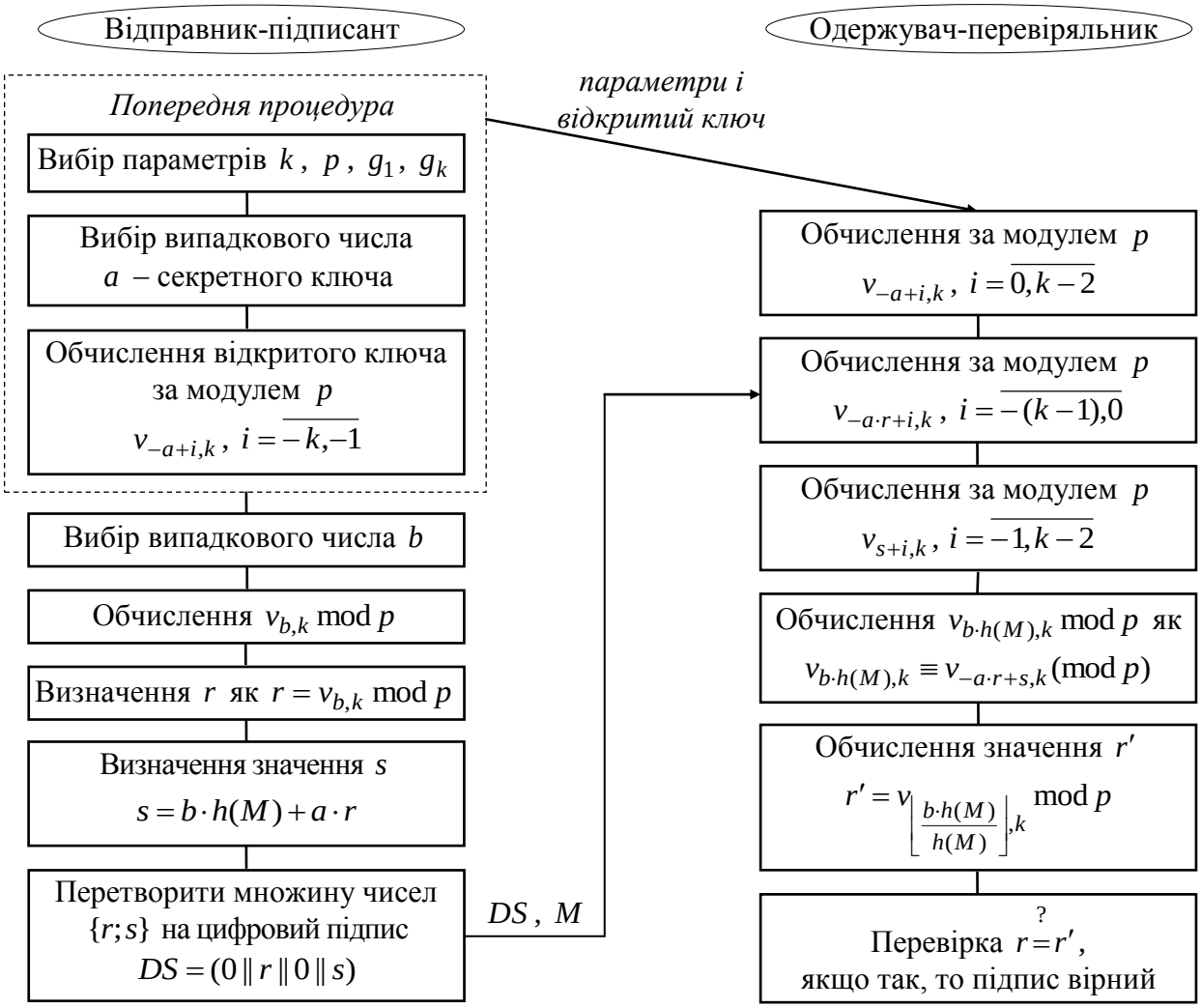

Рис. 1. Схема формування та перевіряння цифрового підпису на основі елементів V_k –послідовності.

Операція за модулем в схемі цифрового підписування використовується для обмеження розрядності чисел під час виконання арифметичних операцій. Обчислення елементу $v_{b,k} \bmod p$ відправник може виконати попередньо, заздалегідь до безпосереднього формування цифрового підпису з повідомлення M.

В запропонованому методі формування та перевіряння цифрового підпису основні обчислення виконуються згідно залежності (3). Обчислення елементу $v_{n+m,k}$ згідно цієї залежності здійснюється на основі елементів $v_{n+i,k}$, $i=\overline{-(k-1),0}$, та елементів $v_{m+i,k}$, $i=\overline{-1,k-2}$. В разі необхідності отримання певного послідовного набору елементів V_k –послідовності у кількості більшої ніж k, достатньо отримати будь-які послідовні k з них, оскільки інші можуть бути обчислені згідно формул (1) або (2) на основі вже отриманих.

Визначивши як можуть отримуватись елементи V_k–послідовності, отримаємо такий протокол генерування та перевірки цифрового підпису.

П.1. Задати параметр k.

П.2. Вибрати p.

П.3. Вибрати g_1, g_k.

П.4. Відправнику передати параметри Одержувачу.

П.5. Відправнику вибрати випадкове число a – секретний ключ.

П.6. Відправнику обчислити відкритий ключ за модулем p $v_{-a+i,k}$, $i=\overline{-k,k-2}$, використовуючи алгоритм прискореного обчислення елементів $v_{n,k}$ для від'ємних значень n.

П.7. Відправнику передати відкритий ключ $v_{-a+i,k} \bmod p$, $i=\overline{-k,-1}$, Одержувачу.

П.8. Одержувачу обчислити за модулем p $v_{-a+i,k}$, $i=\overline{0,k-2}$, за формулою (1).

П.9. Відправнику вибрати випадкове число b.

П.10. Відправнику обчислити $v_{b,k} \bmod p$, використовуючи алгоритм прискореного обчислення елементів $v_{n,k}$ для додатних значень n.

П.11. Відправнику визначити значення r як $r = v_{b,k} \bmod p$.

П.12. Відправнику визначити значення s як $s = b \cdot h(M) + a \cdot r$ за допомогою обраної функції хешування h від повідомлення M.

П.13. Відправнику перетворити множину цілих чисел $\{r; s\}$ у цифровий підпис вигляду $DS = (0 \| r \| 0 \| s)$ і передати його разом з повідомленням M Одержувачу.

П.14. Одержувачу обчислити за модулем p $v_{-a \cdot r+i,k}$, $i=\overline{-(k-1),0}$, використовуючи алгоритм прискореного обчислення елементів $v_{-m \cdot n,k}$.

П.15. Одержувачу обчислити за модулем p елементи $v_{s+i,k}$, $i=\overline{-1,k-2}$, використовуючи алгоритм прискореного обчислення елементів $v_{n,k}$ для додатних значень n.

П.16. Одержувачу обчислити $v_{b \cdot h(M),k} \bmod p$ як $v_{b \cdot h(M),k} \equiv v_{-a \cdot r+s,k} (\bmod p)$ згідно залежності (3).

П.17. Одержувачу обчислити значення r' як $r' = v_{\left\lfloor \frac{b \cdot h(M)}{h(M)} \right\rfloor,k} \bmod p$, використовуючи алгоритм прискореного обчислення елементів $v_{-m \cdot n,k}$.

П.18. Одержувачу перевірити, чи виконується $r \overset{?}{=} r'$, якщо так, то підпис вважати вірним.

У п.2 проводиться вибір параметру p, який є модулем при обчисленнях в представленому протоколі та визначає верхню межу діапазону чисел, що отримуються під час цих обчислень.

У п.3 відбувається вибір параметрів g_1, g_k. Оскільки значення будь-якого числа в розробленому протоколі обмежується параметром p, вказані параметри слід вибирати в діапазоні $[1, p-1]$. При цьому вибір можна здійснювати за допомогою будь-якого генератора випадкових чисел у вказаному діапазоні.

У п.10 протоколу формування та перевіряння цифрового підпису відправнику необхідно здійснювати обчислення елементу $v_{b,k} \bmod p$, а одержувачу в п.15 – обчислення за модулем p елементів $v_{s+i,k}$, $i=\overline{-1,k-2}$. Ці обчислення можна здійснювати за одним з алгоритмів прискореного обчислення елементів $v_{n,k}$ для додатних n, які представлено в

роботі [6]. Так само можна здійснювати обчислення за модулем p елементів $v_{-a+i,k}$, $i=\overline{-k,k-2}$, що виконуються відправником у п.6 протоколу цифрового підписування, на основі одного з запропонованих у тій же роботі [6] алгоритмів прискореного обчислення елементів $v_{n,k}$ для від'ємних n.

У п.14 одержувачу необхідно обчислювати за модулем p елементи $v_{-a\cdot r+i,k}$, $i=\overline{-(k-1),0}$. Для цього можна використати алгоритм прискореного обчислення елементів $v_{-m\cdot n,k}$, який представлено в роботі [7].

У п.17 одержувачу необхідно обчислювати за модулем p елемент $v_{\left\lfloor \frac{b\cdot h(M)}{h(M)} \right\rfloor,k}$. Це можна здійснювати як обчислення елементу $v_{\left\lfloor \frac{m\cdot n}{n} \right\rfloor,k}$ по аналогії з обчисленням елементу $v_{-m\cdot n,k}$ згідно алгоритму прискореного обчислення цих елементів представленого у роботі [7], але починати обчислення не з елементів $v_{-m+i,k}$, $i=\overline{-k,k-2}$, а з елементів $v_{m\cdot n+i,k}$ для тих же значень i.

Запропонований метод формування та перевіряння цифрового підпису на основі V_k–послідовності в цілому має такий же рівень обчислювальної складності, що і метод представлений у роботі [5]. Однак, на відміну від останнього, в запропонованому методі розмір цифрового підпису є меншим, оскільки в ньому відправник передає лише саме число s, а не елементи $v_{s+i,k} \bmod p$, $i=\overline{-1,k-2}$, що визначаються індексом s.

Висновки

Запропоновано метод і протокол формування та перевіряння цифрового підпису на основі математичного апарату рекурентних V_k–послідовностей. Метод забезпечує високий рівень криптографічної стійкості, має простішу процедуру завдання параметрів у порівнянні з відомими аналогами, а також дозволяє змінювати стійкість методу залежно від порядку послідовності k.

Важливою перевагою методу перед методами-аналогами, що базуються на математичному апараті рекурентних V_k–послідовностей, є те, що в ньому розмір цифрового підпису визначається лише числом s, а не елементами V_k–послідовностей, обчисленими для цього індексу.

ЛІТЕРАТУРА

1. Menezes, A.J. Handbook of Applied Cryptography [Текст] / A.J. Menezes, P.C. van Oorschot, S.A. Vanstone. – CRC Press, 2001. – 816 p.

2. Шнайер, Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си [Текст] / Б. Шнайер. – М.: Триумф, 2002. – 816 с.

3. Молдавян, Н. А. Теоретический минимум и алгоритмы цифровой подписи [Текст] / Н. А. Молдавян. – СПб.: БХВ-Петербург, 2010. – 304 с.

4. Романец, Ю. В. Защита информации в компьютерных системах и сетях [Текст] / Ю. В. Романец, П. А. Тимофеева, В. Ф. Шаньгин. – М.: Радио и связь, 2001. – 376 с.

5. Яремчук Ю.Є. Метод генерування та перевірки цифрового підпису на основі рекурентних послідовностей [Текст] / Ю.Є. Яремчук // Сучасний захист інформації. – №3, 2013. – С. 5–12.

6. Яремчук Ю.Є. Розробка алгоритмів прискореного обчислення елементів рекурентних послідовностей для криптографічних застосувань [Текст] / Ю.Є. Яремчук // Реєстрація, зберігання і обробка даних. – Т. 15, №1, 2013. – С. 14–22.

7. Яремчук Ю.Є. Методи автентифікації на основі рекурентних послідовностей [Текст] / Ю.Є. Яремчук // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – Випуск 1(25), 2013. – С. 39–49.

Надійшла: 10.02.2014 р Рецензент: д.т.н., проф. Барабаш О.В.