УДК 621.391.7

Ю.Є. Яремчук[1]

[1]*к.т.н., доцент, директор Центру інформаційних технологій і захисту інформації, професор кафедри адміністративного та інформаційного менеджменту Вінницького національного технічного університету*

МЕТОД ЦИФРОВОГО ПІДПИСУВАННЯ НА ОСНОВІ РЕКУРЕНТНИХ ПОСЛІДОВНОСТЕЙ

Запропоновано метод цифрового підписування, що базується на математичному апараті рекурентних V_k –послідовностей. Проведено дослідження щодо криптографічної стійкості та обчислювальної складності, в результаті якого встановлено, що запропонований метод є більш стійким і майже вдвічі забезпечує спрощення обчислень процедури перевірки підпису, ніж відомі аналоги.

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

Вступ

Забезпечення цілісності на сьогодні є не менш актуальною задачею, ніж забезпечення конфіденційності інформації. Якщо задача конфіденційності вирішується за допомогою криптосистем, то для забезпечення цілісності інформації використовують криптографічні протоколи [1–4]. Найбільш розповсюдженими є два типи криптографічних протоколів – автентифікації та цифрового підписування [1–5]. Якщо протоколи автентифікації в основному спрямовані на забезпечення автентифікації учасників взаємодії, то протоколи цифрового підписування забезпечують автентифікацію повідомлень, що передаються, тобто гарантують, що повідомлення надсилаються від достовірного відправника і в неспотвореному вигляді. Більш того, цілісність тут розуміється у широкому розумінні, тому що одержувач повідомлення не тільки переконується в його достовірності, але й отримує електронний підпис, який в подальшому може використовувати як доказ достовірності повідомлення третім особам (арбітру) у тому випадку, коли відправник в подальшому буде намагатись відмовитись від свого підпису.

В загальному вигляді в схемі цифрового підписування [5] існує два учасника – відправник–підписант та одержувач–перевіряльник. Відправник (або центр довіри) генерує два ключа – загальнодоступний відкритий ключ K_1 та відповідний йому секретний ключ K_2. При формуванні підпису для повідомлення M відправник обчислює цифровий підпис DS від M, використовуючи ключ K_2. При перевірці підпису одержувач перевіряє підпис DS від повідомлення M, використовуючи ключ K_1.

Існуючі на сьогодні схеми цифрового підписування поділяють [1] на схеми з додаванням (with appendix) та схеми з відновленням повідомлення (with message recovery). У схемах підписування з додаванням цифровий підпис DS приєднується до повідомлення M і в такому вигляді відправляється одержувачу, а під час перевірки цього підпису необхідно мати підпис DS та саме повідомлення M. У схемах підписування з

відновленням повідомлення все повідомлення (або його частина) можуть бути відновлені безпосередньо з цифрового підпису, тому на вхід процедури перевірки підпису надходить лише цифровий підпис DS.

Кожна з цих схем цифрового підписування може бути детермінованою (deterministic) або рандомізованою (randomized) [1]. У першому випадку при подаванні на вхід однакових повідомлень формуються однакові цифрові підписи, а у другому випадку за рахунок використання певного випадкового числа (сеансового ключа) формуються різні цифрові підписи для однакових вхідних повідомлень (при використанні тих самих ключів K_1 та K_2). У свою чергу детерміновані схеми поділяють [1] на схеми одноразового (one-time) та багаторазового (multiple-use) застосування.

Серед існуючих схем цифрового підписування найбільшого поширення отримали рандомізовані схеми з додаванням повідомлення. До таких схем в першу чергу відносяться методи Ель-Гамаля [6], Шнорра [7], DSA [8], ГОСТ 34.10 [3, 4]. Ці методи базуються на операції піднесенні до степеня, яка вимагає виконання досить складних обчислень, що впливає на швидкість роботи методу при його практичній реалізації. Поряд з цим на сьогодні доволі активно досліджується проблема дискретного логарифмування, про що свідчать хоча б результати в роботі [9], тому актуальним залишається питання і підвищення стійкості цих методів цифрового підписування. Виходячи з сказаного, в цілому актуальним стає пошук та розробка таких математичних апаратів, які б могли стати основою побудови ефективних методів забезпечення цілісності інформації.

В цьому зв'язку певний інтерес викликає робота [10] авторів Сміта і Скіннера, які запропонували використовувати рекурентні функції Люка і замінили піднесення до степеня за модулем, як це робиться в методі Ель-Гамаля та його варіантах, на обчислення елементу рекурентної послідовності Люка за модулем простого числа p з певним індексом (метод називають LUCELG DS). Перевагою методу LUCELG DS є те, що його стійкість, яка базується на математичному апараті рекурентних послідовностей, не залежить від спроб криптоаналізу, що існують в задачах дискретного логарифмування. При цьому метод має певні слабкості щодо стійкості, зокрема, розглянуті функції Люка є вразливими до екзистенційної підробки. Не зважаючи на це, вважається, що методи, які базуються на цих функціях, в цілому є більш стійкими, ніж ті, що базуються на математичному апараті еліптичних кривих [3]. Однак, основним недоліком методу LUCELG DS є те, що він має велику обчислювальну складність, оскільки потребує значно більшої кількості обчислень елементів рекурентних послідовностей, ніж навіть аналоги, що базуються на операції піднесенні до заданого степеня. І, що є ще більш незручним і обмежує його використання – розглянутий метод на основі функцій Люка потребує досить складних обчислень при перевірці цифрового підпису.

Загальним недоліком методів цифрового підписування є те, що одна з частин підпису являє собою число (у більшості методів значення s), а не, скажімо, результат піднесення до степеня, що визначається цим числом (як, наприклад, інша частина підпису r у більшості методів), або результат інших обчислень над цими числами, які б значно ускладнювали зловмиснику його спроби щодо зламу і цим самим підвищували б стійкість цифрового підписування. Крім того, існують задачі, в яких процедуру перевірки підпису необхідно здійснювати в реальному часі від великої кількості власників і тому необхідність виконання складних обчислень в існуючих методах цифрового підписування створює перевіряльнику в таких випадках певні незручності. До такого роду задач відносяться задачі авторизації та ідентифікації під час здійснення трансакцій в електронних платіжних системах та в системах стільникового зв'язку, забезпечення веб-трансакцій між клієнтом та сервером, організації банківських трансакцій, організації мобільної комерції, авторизації електронних повідомлень та інші. В таких задачах перевіряльник за одиницю часу може отримувати велику кількість запитів на перевірку

підпису, що, в свою чергу, може створювати для нього проблему перенавантаження.

Таким чином, актуальним є розробка такого методу цифрового підписування, який би прискорював виконання процедури перевірки підпису при забезпеченні достатнього рівня криптографічної стійкості.

Математичний апарат на основі рекурентних V_k –послідовностей

Певна слабкість методу цифрового підписування LUCELG DS, запропонованого у роботі [10], не означає, що рекурентні послідовності як математичний апарат не можуть ефективно використовуватись для побудови криптографічних протоколів, оскільки рекурентні послідовності, що використовуються в даному методі, є лише окремим випадком більш узагальнених рекурентних послідовностей.

Рекурентні послідовності в загальному вигляді породжуються таким співвідношенням [11]

$$u_n = a_1 \cdot u_{n-1} + a_2 \cdot u_{n-2} + \ldots + a_k \cdot u_{n-k}, \quad (1)$$

де $a_1, a_2, \ldots, a_k$ – коефіцієнти, k – порядок послідовності, виходячи з початкових елементів $u_0, u_1, \ldots, u_k$.

Певну цікавість представляють послідовності, в яких початкові елементи пов'язані з коефіцієнтами. Найпростішим прикладом в цьому випадку є послідовність, елементи якої обчислюються за формулою

$$u_n = a_1 \cdot u_{n-1}. \quad (2)$$

Якщо $u_1 = q$, $a_1 = q$, то $u_n = q^n$. Тобто, в цьому випадку, рекурентне співвідношення породжує степеневу послідовність.

Наступним за складністю є випадок, коли два коефіцієнти відрізняються від нуля. В цьому випадку елементи послідовності обчислюються за такою формулою

$$u_n = a_1 \cdot u_{n-1} + a_k \cdot u_{n-k}. \quad (3)$$

В [12] розглянуто V_k–послідовність, яка складається з V_k^+–послідовності та V_k^-–послідовності.

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

$$v_{n,k} = g_k v_{n-1,k} + g_1 v_{n-k,k} \quad (4)$$

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

$$v_{n,k} = \frac{v_{n+k,k} - g_k \cdot v_{n+k-1,k}}{g_1}. \quad (5)$$

V_k^- –послідовністю називається послідовність чисел, що обчислюються за формулою (5) 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 [13]

$$v_{n+m,k} = v_{m+(k-2),k} \cdot v_{n,k} + g_1 \cdot \sum_{i=1}^{k-1} v_{m+(k-2)-i,k} \cdot v_{n-k+i,k}. \quad (6)$$

Для будь-яких цілих додатних n і m, таких що $1 \le m < n$ та будь-якого цілого додатного k існує така залежність [12]

$$v_{n-m,k} = v_{-m+(k-2),k} \cdot v_{n,k} + g_1 \cdot \sum_{i=1}^{k-1} v_{-m+(k-2)-i,k} \cdot v_{n-k+i,k}. \quad (7)$$

Представлені рекурентні послідовності, а також отримані залежності дозволяють розробити методи цифрового підписування на їх основі.

Методи цифрового підписування на основі рекурентних V_k –послідовностей

Відомо [2], що будь-який метод автентифікації, що базується на технології відкритого ключа, може бути перетворений у метод цифрового підписування шляхом заміни перевіряльника однонаправленою хеш-функцією. При цьому повідомлення не хешується перед підписанням, замість цього хеш-функція включається в сам алгоритм цифрового підписування.

Виходячи з цього, запропонований в [14] метод автентифікації на основі V_k –послідовності може бути перетворений в такий метод цифрового підписування (заявка на корисну модель № u 2013 06322 від 22.05.2013 р.).

Суть методу цифрового підписування, що пропонується, базується на використанні властивості (6) 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 (6) дозволяє реалізувати процедуру обчислення елементу $v_{n \cdot m,k}$. Так само на основі властивості (7) 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 x як $x=v_{b,k}$ та обчислює хеш-значення r як $r=h(x,M)$ за допомогою обраної функції хешування h від повідомлення M та значення x. Далі він визначає значення s як $s=b+a\cdot r$ і обчислює для нього елементи $v_{s+i,k}$, $i=\overline{-1,k-2}$. Після цього отриману множину цілих чисел $\{r;v_{s+i,k},i=\overline{-1,k-2}\}$ він перетворює у цифровий підпис вигляду $DS=(0\|r\|0\|v_{s-1,k}\|0\|v_{s,k}\|...0\|v_{s+(k-2),k})$ 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. Потім він обчислює x' як $x'=v_{-a\cdot r+s,k}$, використовуючи залежність (6), обчислює хеш-значення r' як $r'=h(x',M)$ та перевіряє, чи виконується $r\overset{?}{=}r'$. 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 цифрового підписування за даним методом буде мати такий вигляд (рис.1).

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 цифрового підписування основні обчислення виконуються згідно залежності (6). 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 (4) або (5) на основі вже отриманих.

Також в методі одержувачу слід виконувати обчислення елементів $v_{-a\cdot r+i,k}$, $i=\overline{-(k-1),0}$, які можна здійснювати згідно представленого в роботі [14] методу обчислення елементів $v_{-m\cdot n,k}$.

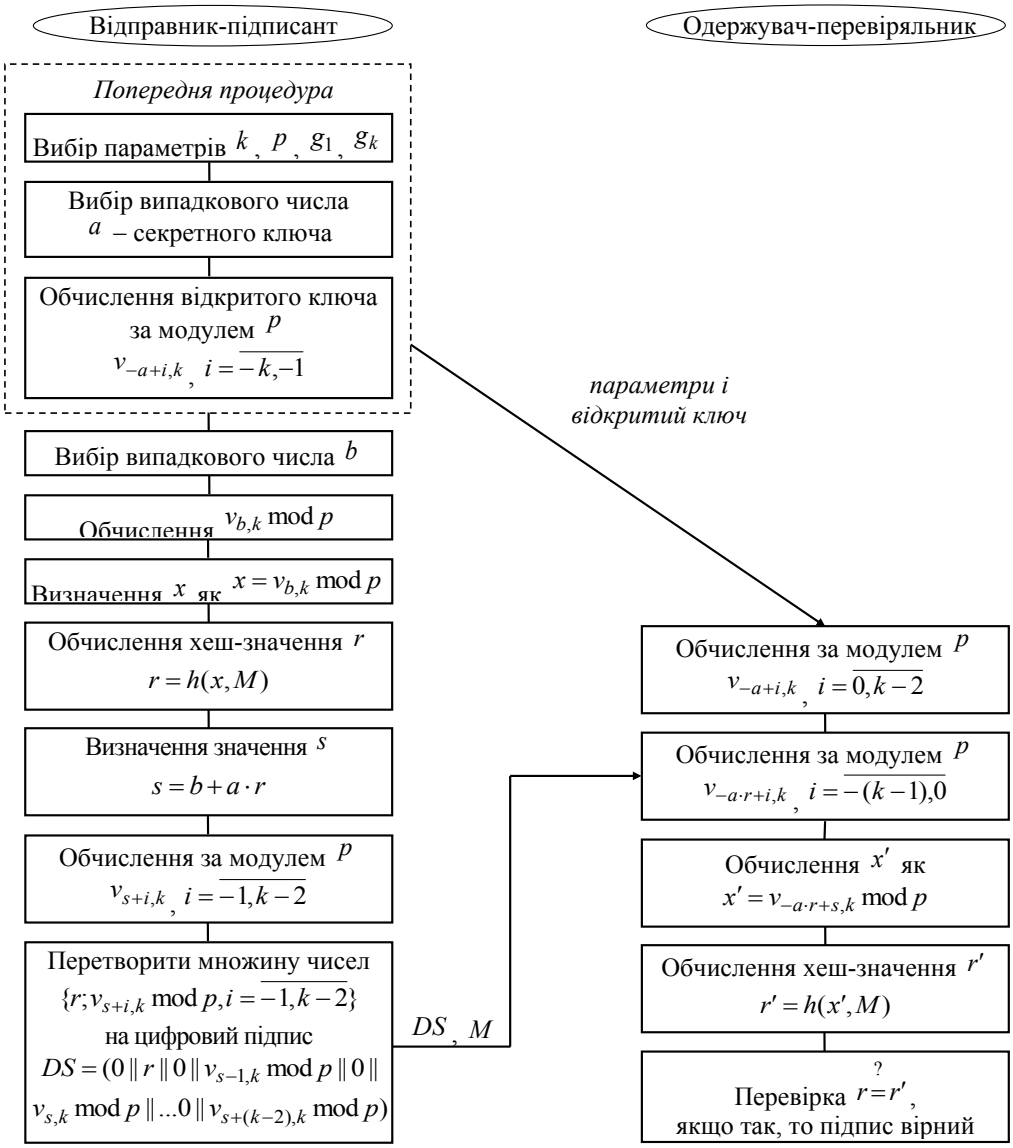

Рис. 1. Схема цифрового підписування на основі елементів V_k –послідовності.

Визначивши як можуть отримуватись елементи V_k –послідовності, що використовуються в методі цифрового підписування, отримаємо такий протокол цифрового підписування.

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 (4).

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 x як $x = v_{b,k} \bmod p$.

П.12. Відправнику обчислити хеш-значення r як $r = h(x, M)$ за допомогою обраної функції хешування h від повідомлення M та значення x.

П.13. Відправнику визначити значення s як $s = b + a \cdot r$.

П.14. Відправнику 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.15. Відправнику перетворити множину цілих чисел $\{r; v_{s+i,k} \bmod p, i = \overline{-1,k-2}\}$ у цифровий підпис вигляду $DS = (0 \| r \| 0 \| v_{s-1,k} \bmod p \| 0 \| v_{s,k} \bmod p \| ... 0 \| v_{s+(k-2),k} \bmod p)$ і передати його разом з повідомленням M Одержувачу.

П.16. 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.17. Одержувачу обчислити $x' = v_{-a \cdot r+s,k} \bmod p$ згідно залежності (6).

П.18. Одержувачу обчислити хеш-значення r' як $r' = h(x', M)$.

П.19. 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 цифрового підписування відправнику необхідно здійснювати обчислення $v_{b,k} \bmod p$, а у п.14 – 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 [12].

Так само можна здійснювати обчислення за модулем p елементів $v_{-a+i,k}$, $i=\overline{-k,k-2}$, що виконуються у п.6 протоколу цифрового підписування, на основі одного з запропонованих у тій же роботі [12] алгоритмів прискореного обчислення елементів $v_{n,k}$ для від'ємних n.

У п.16 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 [14].

Не важко помітити, що у випадку, якби $k=1$, запропонований метод цифрового підписування став би дуже подібним на метод Шнорра.

Згідно відомого протоколу цифрового підписування Шнорра [7] центр довіри або відправник вибирає і відкрито публікує два простих числа p і q: $q \mid p-1$ та число $g\neq 1$: $g^q \equiv 1(\mathrm{mod}\, p)$. Потім він вибирає випадкове число $a<q$ як секретний ключ та обчислює $y=g^{-a} \bmod p$ – відкритий ключ, який передається одержувачу. Після цього протокол цифрового підписування реалізується таким чином.

На етапі формування підпису відправник вибирає випадкове число $b<q$ та обчислює $x=g^b \bmod p$ (ці обчислення можуть бути виконані і попередньо). Далі, з отриманого значення x та повідомлення M, що підписується, він здійснює хешування за допомогою функції h, обчислюючи значення $r=h(x,M)$. Потім відправник обчислює $s=(b+a\cdot r) \bmod q$ і надсилає повідомлення M з підписом (r,s) одержувачу.

На етапі перевірки підпису одержувач обчислює $x'=g^s \cdot y^r \bmod p$ і перевіряє, чи виконується рівняння $r \stackrel{?}{=} h(x',M)$. Якщо так, то підпис приймається, інакше – відкидається.

Проведемо аналіз запропонованого методу цифрового підписування на основі елементів V_k –послідовності та порівняємо його з відомим методом цифрового підписування Шнорра.

Спочатку проведемо аналіз щодо криптографічної стійкості.

Здійснювати криптоаналіз запропонованого методу цифрового підписування на основі V_k –послідовності зловмисник може на основі відомих параметрів k, p, g_1, g_k, відкритого ключа $v_{-a+i,k} \bmod p$, $i=\overline{-k,-1}$, набору чисел $\{r; v_{s+i,k} \bmod p, i=\overline{-1,k-2}\}$ цифрового підпису та повідомлення M, які передаються від відправника до одержувача. Відповідно згідно методу Шнорра зловмиснику відомі параметри p, q, g, відкритий ключ $g^{-a} \bmod p$, а також повідомлення M з підписом (r,s), які передаються одержувачу відправником.

В роботі [13] досліджувалась стійкість криптографічних перетворень, що базуються на використанні елементів V_k^+ та U_k – послідовностей, з яких видно, що складність отримання зловмисником індексу елемента рекурентної послідовності, обчисленого за модулем, є принаймні не меншою, ніж отримання числа степеня з результату модулярного піднесення до степеня. Тобто можна вважати, що ці обчислення знаходяться приблизно на одному ж рівні.

Виходячи з цього можна стверджувати, що метод цифрового підписування на основі V_k–послідовності криптографічно є більш стійким, ніж відомий метод Шнорра, оскільки в ньому замість передавання від відправника до одержувача числа s як частини підпису відповідно передаються елементи $v_{s+i,k} \bmod p$, $i = \overline{-1, k-2}$, тобто не саме число-індекс, а елементи рекурентної послідовності, обчислені для заданого індексу.

Перевагою запропонованого методу цифрового підписування на основі рекурентних послідовностей перед відомими методами щодо стійкості є також можливість змінювати параметр k, що, в свою чергу, дає можливість підвищувати криптостійкість за рахунок збільшення складності виконання протоколу цифрового підписування.

Також перевагою запропонованого методу цифрового підписування є те, що він має значно простішу процедуру завдання параметрів, оскільки їх вибір не потребує проведення складних обчислень над великими числами.

Проведемо більш детальний аналіз запропонованого методу цифрового підписування щодо обчислювальної складності.

З результатів дослідження складності обчислення елементів V_k–послідовності, які наведено в роботі [12], видно, що складність обчислення елементу V_k–послідовності за алгоритмом його прискореного обчислення є значно більшою, ніж за будь-якою аналітичною залежністю обчислення елементів цієї послідовності. Так само у відомому методі автентифікації Шнорра обчислювальна складність операції піднесення до степеня є значно більшою, ніж будь-якої іншої операції, що використовується в даному методі.

Аналіз запропонованого та відомого методів автентифікації показує, що згідно запропонованого методу необхідно чотири рази проводити обчислення елементів V_k –послідовності за прискореним алгоритмом, а саме обчислення за модулем p різних наборів елементів з $v_{-a,k}$, $v_{b,k}$, $v_{s,k}$ та $v_{-a\cdot r,k}$. Стільки ж, чотири, необхідно виконувати піднесень до степеня за модулем p згідно відомого методу Шнорра: g^{-a}, g^b, g^s та y^r.

В роботі [12] проведено дослідження складності виконання алгоритмів прискореного обчислення елементів V_k–послідовності, з якого видно, що складність обчислення елементу цієї послідовності із заданим індексом має приблизно такий же рівень як і піднесення до заданого степеня того ж порядку, що й індекс.

Виходячи з цього, запропонований метод цифрового підписування на основі V_k –послідовності в цілому має приблизно такий же рівень обчислювальної складності, що і відомий метод Шнорра. При цьому слід відзначити, що розмір цифрового підпису згідно відомого методу є меншим, оскільки відправник передає лише саме число s, а не набір з k елементів $v_{s+i,k} \bmod p$, $i = \overline{-1, k-2}$, як у запропонованому методі. Правда, цей недолік, може бути усунутий за рахунок зменшення криптографічної стійкості запропонованого методу до рівня відомого методу шляхом зменшення розміру чисел та еле-

ментів послідовності, який в основному визначається параметром p методу. Тоді зменшиться і розмір цифрового підпису і, як наслідок, зменшиться і обчислювальна складність запропонованого методу.

І все ж таки, окрім підвищеної стійкості, важливою перевагою запропонованого методу є суттєве, майже в два рази, спрощення обчислювальної складності процедури перевірки підпису, оскільки тут замість двох піднесень до степеня згідно відомого методу тепер необхідно виконувати лише одне обчислення набору елементів $v_{-a\cdot r,k}$ за прискореним алгоритмом обчислення елементів V_k –послідовності. Правда, це досягається необхідністю при формуванні підпису виконувати три обчислення елементів V_k –послідовності за прискореним алгоритмом, замість двох піднесень до степеня згідно відомого методу. Однак, велика кількість задач, в яких перевірку цифрового підпису необхідно здійснювати значно частіше, ніж його формування, і перевіряти підпис від великої кількості його власників, як то в клієнт-серверних задачах, дає суттєву перевагу запропонованому методу перед відомими аналогами.

Слід також сказати і про те, що в запропонованому методі обчислення елементів $v_{s+i,k} \bmod p$, $i = \overline{-1, k-2}$, можна здійснювати і на стороні одержувача, при цьому, по аналогії з відомим методом, відправник буде передавати лише саме число-індекс s (заявка на корисну модель № u 2013 06323 від 22.05.2013 р.). Тоді рівень криптографічної стійкості знизиться приблизно до рівня відомого методу, при цьому обчислювальна складність як взагалі методу, так і з боку кожної із сторін, також стане приблизно такого ж рівня, що й відомого аналогу. Однак такий варіант методу не буде забезпечувати можливість прискорення процедури перевірки підпису.

Висновки

На основі математичного апарату рекурентних V_k –послідовностей запропоновано метод цифрового підписування, в якому відбувається заміна піднесення до степеня обчисленням елементу рекурентної послідовності з певним індексом, а також представлено протокол реалізації цього методу.

Проведено дослідження та здійснено порівняльний аналіз запропонованого методу цифрового підписування з відомим методом Шнорра щодо криптографічної стійкості та обчислювальної складності. Встановлено, що запропонований метод є більш стійким, ніж відомий аналог, при цьому він ще й дозволяє змінювати стійкість методу залежно від параметру k –порядку послідовності. Крім того метод, що запропоновано, має значно простішу процедуру завдання параметрів.

Дослідження обчислювальної складності показало, що запропонований метод має майже вдвічі простішу процедуру перевірки підпису порівняно з відомими аналогами, що дозволяє суттєво підвищити швидкодію виконання цієї процедури.

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. Петров, А. А. Компьютерная безопасность. Криптографические методы защиты [Текст] / А.А. Петров. – М.: ДМК, 2000. – 448 с.
5. Введение в криптографию [Текст] / Под общ. ред. В.Б. Ященко. – М.: МЦНМО: «ЧеРо», 2000. – 236 с.
6. ElGamal, T. A Public-Key Cryptosystcm and a Signature Scheme Based on Discrete Loga-

rithms [Текст] / T. ElGamal // Advances in Cryptology: Proceedings of CRYPTO 84. – Springer Verlag, 1985. P. 1-18.
7. Schnorr, C.P. Efficient Signature Generation for Smart Cards [Текст] / C.P. Schnorr // Advances CRYPTO '89 Proceedings. – Springer-Verlag, 1990. P. 239-252
8. National Institute of Standards and Technology, NIST FIPS PUB 186, "Digital Signature Standard," U.S. Department of Commerce, May 1994.
9. Odlyzko, A.M. Discrete logarithms: the past and the future [Текст] / A.M. Odlyzko // Designs, Codes and Cryptography. – №19, 2000. –Pp. 129–154.
10. Smith, P. A public-key cryptosystem and a digital signature system based on the Lucas function analogue to discrete logarithms [Текст] / P. Smith, C. Skinner // In Advances in Cryptology Asiacrypt '94. – Springer-Verlag, 1995. – P. 357–364.
11. Маркушевич, А.И. Возвратные последовательности [Текст] / А.И. Маркушевич. – М.: Наука, 1975. – 48 с.
12. 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.
13. Яремчук, Ю.Є. Використання рекурентних послідовностей для побудови криптографічних методів з відкритим ключем [Текст] / Ю.Є. Яремчук // Захист інформації. – 2012. – № 4. – С. 120 – 127.
14. 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. 39–48.

Надійшла до редколегії 15.02.2013 р.

Рецензент: д.т.н., проф. Дівізінюк М.М.

Яремчук Ю.Е.

МЕТОД ЦИФРОВОГО ПОДПИСАНИЯ НА ОСНОВЕ РЕКУРРЕНТНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ

Предложен метод цифрового подписания, который основывается на математическом аппарате рекуррентных V_k –последовательностей. Проведено исследование криптографической стойкости и вычислительной сложности, в результате которого установлено, что предложенный метод является более стойким и почти вдвое обеспечивает упрощение вычислений процедуры проверки подписи, чем известные аналоги.

Ключевые слова: защита информации, криптография, аутентификация, цифровое подписание, рекуррентные последовательности.

Iurii Iaremchuk

DIGITAL SIGNATURE METHOD BASED ON RECURRENT SEQUENCES

Summary. We suggested a method of digital signature based on mathematical apparatus of recurrent V_k sequences. We conducted a study on cryptographic reliability and computational complexity, whose results revealed that the proposed method is more reliable, and provides almost twice as simple a computation procedure of signature verification than the known analogues.

Keywords: informational security, cryptography, authentication, digital signature, recurrent sequences.