УДК 621.391.7

Ю. Є. Яремчук, канд. техн. наук, доц.

МЕТОД АВТЕНТИФІКАЦІЇ СУБ'ЄКТІВ (ОБ'ЄКТІВ) ВЗАЄМОДІЇ НА ОСНОВІ РЕКУРЕНТНИХ ПОСЛІДОВНОСТЕЙ

Запропоновано метод автентифікації суб'єктів (об'єктів) взаємодії на основі математичного апарату рекурентних V_k-послідовностей. Аналіз показав, що в цілому метод має приблизно такий самий рівень криптографічної стійкості та обчислювальної складності, як і відомі аналоги, але за певних умов метод забезпечує значне підвищення швидкості виконання процедури перевірки автентичності, а також підвищення стійкості всього процесу автентифікації. Існує також можливість перетворення методів автентифікації на основі V_k-послідовності в методи цифрового підписування.

Вступ

На сьогодні задача забезпечення цілісності є досить актуальною і вирішується за допомогою криптографічних протоколів, які бувають двох типів — автентифікації та цифрового підписування [1, 2]. В схемі автентифікації суб'єктів (об'єктів) взаємодії [1] існує два учасника — претендент — той, хто доводить свою автентичність, та перевіряльник — той, хто цю автентичність повинен перевірити. В схемі автентифікації з нульовим розголошенням знання претендент має два ключі — загальнодоступний K_1 та секретний K_2 і довести свою автентичність він повинен таким чином, щоб можна було переконатись, що претендент знає K_2 і при цьому це можна було б перевірити, знаючи лише K_1.

Найвідомішими методами автентифікації є методи Фейге-Фіата-Шаміра, Гіллоу-Куіскуотера та Шнорра [1, 2]. Ці методи базуються на операції піднесенні до степеня, яка вимагає виконання досить складних обчислень, що впливає на швидкість роботи методу у його практичній реалізації. При цьому найбільшою проблемою є те, що у вказаних методах автентифікації складні обчислення виконуються саме в процедурі перевірки автентичності, зокрема, в методі автентифікації Шнорра, необхідно виконувати два піднесення до степенів великих чисел за модулем. Це створює певні труднощі під час використання методів автентифікації в задачах, де процедуру перевірки автентичності необхідно здійснювати в реальному часі від великої кількості претендентів. В таких випадках перевіряльник за одиницю часу може отримувати велику кількість запитів на перевірку автентичності, що, в свою чергу, може створювати для нього проблему перенавантаження. 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, автентифікації в безпровідних мережах, організації банківських трансакцій, організації мобільної комерції, авторизації електронних повідомлень та інші.

В цьому зв'язку певний інтерес викликає апарат на основі рекурентних послідовностей [3, 4], який дозволяє за певних умов спрощувати обчислення під час розв'язання криптографічних задач. Так в роботі [5] викладено метод автентифікації сторін взаємодії, який базується на рекурентних V_{κ}^{+}- та U_k-послідовностях і який, у порівнянні з відомим методами, дозволяє суттєво спростити обчислення. Однак описаний метод не задовольняє усім вимогам до протоколів автентифікації, оскільки не дозволяє використовувати претенденту сеансовий ключ. В роботі [6] описано метод, який задовольняє усім сучасним вимогам щодо забезпечення автентифікації з нульовим розголошенням знання, при цьому він забезпечує ще й підвищення стійкості у порівнянні з відомими методами автентифікації. Однак, запропонований метод не вирішує проблему спрощення обчислень процедури перевірки автентичності.

Виходячи з цього, актуальним є дослідження рекурентних послідовностей щодо розробки такого методу автентифікації, який би забезпечував спрощення обчислень процедури перевірки автентичності при забезпеченні достатнього рівня криптостійкості.

Метод автентифікації на основі рекурентних V_k- послідовностей

В [4] розглянуто V_k-послідовність, яка складається з V_k^+ - послідовності та V_k^- - послідовності.

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

$$v_{n,k} = g_k v_{n-1,k} + g_1 v_{n-k,k} \tag{1}$$

для початкових значень $v_{0,k} = 1$, $v_{1,k} = g_2$ для $k = 2$; $v_{0,k} = v_{1,k} = ... = v_{k-3,k} = 0$, $v_{k-2,k} = 1$, $v_{k-1,k} = g_k$ 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:

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

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 [3]:

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

Для будь-яких цілих додатних n і m, таких що $1 \le m < n$ та будь-якого цілого додатного k існує така залежність [4]:

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

Наведені рекурентні послідовності, а також отримані залежності дозволяють розробити метод автентифікації суб'єктів (об'єктів) взаємодії на їх основі.

Суть методу автентифікації, що пропонується (заявка на корисну модель № u 2013 06321 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 автентифікації суб'єктів (об'єктів) взаємодії.

Спочатку претендент (або центр довіри) виконує попередню процедуру обчислення ключів. Для цього він випадковим чином вибирає секретний ключ a, після цього обчислює і передає перевіряльнику відкритий ключ $v_{-a+i,k}$, $i = \overline{-k,-1}$.

Коли претендент хоче довести свою автентичність, він вибирає випадкове число b, обчислює $v_{b,k}$, визначає значення x як $x = v_{b,k}$ і передає його перевіряльнику. В цей час перевіряльник вибирає випадкове число c, передає його претенденту, після чого обчислює $v_{-a \cdot c+i,k}$, $i = \overline{-(k-1),0}$, на основі елементів $v_{-a+i,k}$, $i = \overline{-k,k-2}$, та свого сеансового ключа c.

Одночасно претендент обчислює значення $b + a \cdot c$ на основі своїх секретного ключа a та сеансового ключа b, а також сеансового ключа c, отриманого від перевіряльника, та передає обчислене значення перевіряльнику.

Після цього перевіряльник обчислює на основі отриманого значення $b + a \cdot c$ елементи $v_{b+a \cdot c+i,k}$, $i = \overline{-1,k-2}$, а потім використовує отримані елементи для обчислення x' як $x' = v_{-a \cdot c+(b+a \cdot c),k}$ згідно із залежністю (3). На завершення він перевіряє отримане значення x' зі значенням x, раніше отриманим від претендента.

Виходячи з цього схема автентифікації суб'єктів (об'єктів) взаємодії за запропонованим методом буде мати такий вигляд (рис.).

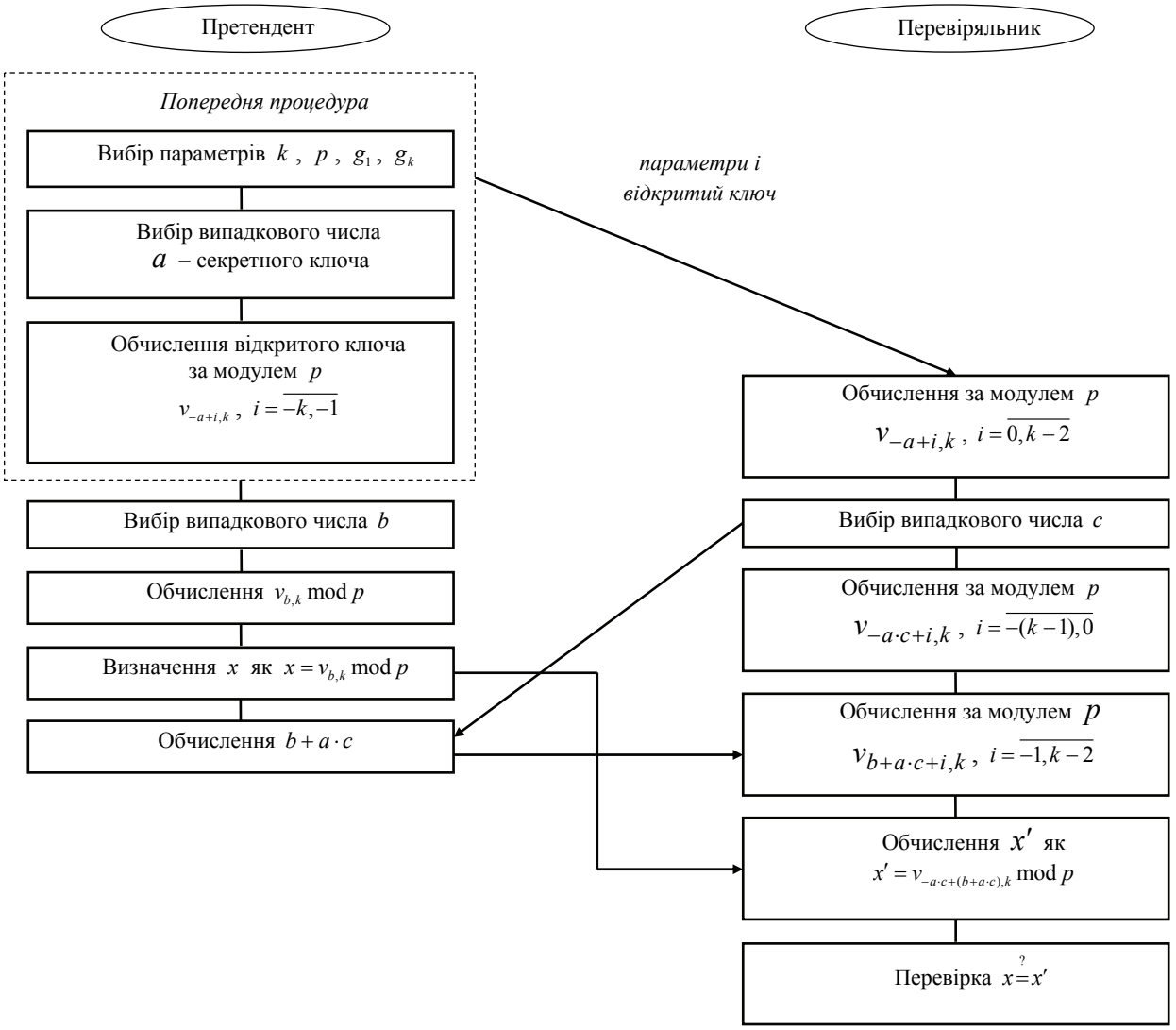

Схема автентифікації суб'єктів (об'єктів) взаємодії на основі елементів V_k-послідовності

Операція за модулем в схемі автентифікації використовується для обмеження розрядності чисел під час виконання арифметичних операцій.

Вибір числа b та обчислення елементу $v_{b,k} \bmod p$ претендентом можуть бути виконані попередньо, заздалегідь до безпосередньої автентифікації. Так само попередньо перевіряльник може вибрати число c і обчислити на основі відкритого ключа елементи $v_{-a\cdot c+i,k}$, $i=\overline{-(k-1),0}$. Попереднє обчислення цього набору елементів з боку перевіряльника дає можливість зменшити майже у два рази обчислювальну складність процедури перевірки автентичності безпосередньо під час автентифікації.

В запропонованому способі автентифікації основні обчислення виконуються згідно з залежністю (3) на основі елементів $v_{n+i,k}$, $i=\overline{-(k-1),0}$, та елементів $v_{m+i,k}$, $i=\overline{-1,k-2}$.

У 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 з формулами (1) або (2) на основі вже отриманих.

Виходячи з вищесказаного, отримано такий протокол автентифікації суб'єктів (об'єктів) взає-

модії на основі елементів V_k-послідовності.

П.1. Задати параметр k.

П.2. Вибрати p.

П.3. Вибрати g_1, g_k.

П.4. Претенденту передати параметри Перевіряльнику.

П.5. Претенденту вибрати випадкове число a — секретний ключ.

П.6. Претенденту 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. Претенденту передати відкритий ключ $v_{-a+i,k} \bmod p$, $i=\overline{-k,-1}$ Перевіряльнику.

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

П.9. Претенденту вибрати випадкове число b, а Перевіряльнику вибрати випадкове число c і передати його Претенденту.

П.10. Претенденту обчислити $v_{b,k} \bmod p$, використовуючи алгоритм прискореного обчислення елементів $v_{n,k}$ для додатних значень n, а Перевіряльнику обчислити за модулем p $v_{-a\cdot c+i,k}$, $i=\overline{-(k-1),0}$, використовуючи алгоритми прискореного обчислення елементів $v_{-m\cdot n,k}$.

П.11. Претенденту визначити x як $x=v_{b,k} \bmod p$ і передати отримане значення Перевіряльнику.

П.12. Претенденту обчислити значення $b+a\cdot c$ і передати отримане значення Перевіряльнику.

П.13. Перевіряльнику обчислити за модулем p $v_{b+a\cdot c+i,k}$, $i=\overline{-1,k-2}$, використовуючи алгоритм прискореного обчислення елементів $v_{n,k}$ для додатних значень n.

П.14. Перевіряльнику обчислити $x'=v_{-a\cdot c+(b+a\cdot c),k} \bmod p$ за формулою (3) та порівняти отримане значення з x, тобто перевірити $x \overset{?}{=} x'$.

У п. 2 проводиться вибір параметра p, який є модулем у обчисленнях в поданому 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 автентифікації необхідно здійснювати обчислення елементу $v_{b,k} \bmod p$, а у п. 13 обчислення за модулем p елементів $v_{b+a\cdot c+i,k}$, $i=\overline{-1,k-2}$. Ці обчислення можна здійснювати за одним з алгоритмів прискореного обчислення елементів $v_{n,k}$ для додатних n, які описані в роботі [4].

Так само можна здійснювати обчислення за модулем p елементів $v_{-a+i,k}$, $i=\overline{-k,k-2}$, що виконуються у п. 6 протоколу автентифікації, на основі одного з запропонованих у тій же роботі [4] алгоритмів прискореного обчислення елементів $v_{n,k}$ для від'ємних n.

У п. 10 протоколу автентифікації необхідно здійснювати обчислення за модулем p елементів $v_{-a\cdot c+i,k}$, $i=\overline{-k+1,0}$, на основі елементів $v_{-a+i,k}$, $i=\overline{-k,k-2}$, та сеансового ключа c перевіряльника. Ці обчислення можна здійснювати за алгоритмом прискореного обчислення елементів $v_{-m\cdot n,k}$, описаного в роботі [6].

Здійснювати криптоаналіз запропонованого методу автентифікації суб'єктів (об'єктів) взаємодії на основі V_k-послідовності, зловмисник може на основі відомих параметрів k, p, g_1, g_k, відкритого ключа $v_{-a+i,k} \bmod p$, $i=\overline{-k,-1}$, а також $v_{b,k} \bmod p$ і $b+a\cdot c$, які передаються від претендента до перевіряльника, а також числа c, яке передається від перевіряльника до претендента. Приблизно так само у відомих методах, зокрема у методі Шнорра зловмиснику відомі параметри

p, q, g, відкритий ключ $g^{-a} \bmod p$, а також $g^b \bmod p$ та $b + a \cdot c (\bmod q)$, які передаються від претендента до перевіряльника, а також число *c*, яке передається від перевіряльника до претендента. З [3] видно, що складність отримання зловмисником індексу елементу рекурентної V_k-послідовності, обчисленого за модулем, є принаймні не меншою, ніж отримання числа степеня з результату модулярного піднесення до степеня. Враховуючи це, можна стверджувати, що криптографічна стійкість запропонованого методу знаходиться приблизно на тому ж рівні, принаймні є не меншою, ніж й відомого аналогу.

Перевагою запропонованого методу автентифікації 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 автентифікації. Окрім цього, до переваг запропонованого методу автентифікації слід віднести й те, що він має значно простішу процедуру задання параметрів, оскільки їх вибір не потребує проведення складних обчислень над великими числами.

Аналіз запропонованого та відомого методів автентифікації щодо обчислювальної складності показує, що згідно р запропонованим методом необхідно чотири рази проводити обчислення елементів V_k-послідовності за прискореним алгоритмом (по два рази кожному боці), а саме — обчислення за модулем p різних наборів елементів з $v_{-a,k}$, $v_{b,k}$, $v_{-a \cdot c,k}$ та $v_{b+a \cdot c,k}$. За відомим методом Шнорра необхідно виконувати стільки ж, чотири, піднесення до степеня за модулем p: g^{-a}, g^b, g^y, $(g^{-a})^c$, і так само по два рази на кожному боці. З [4] видно, що складність обчислення елементу V_k-послідовності із заданим індексом має приблизно такий самий рівень як і піднесення до заданого степеня того ж порядку, що й індекс. Виходячи з цього, в цілому обчислювальна складність запропонованого методу автентифікації має приблизно такий самий рівень складності обчислень, що й відомий метод Шнорра.

Однак, важливою перевагою запропонованого методу на основі V_k-послідовностей є те, що за необхідністю процедуру перевірки автентичності можна значно спростити, якщо обчислення елементів $v_{b+c \cdot a+i,k} \bmod p$, $i = \overline{-1, k-2}$, здійснювати не перевіряльнику, а претенденту, і передавати потім ці елементи перевіряльнику замість індексу $b + c \cdot a$ (заявка на корисну модель № u 2013 06320 від 22. 05. 2013 р.). Тоді претенденту необхідно буде передавати більшу кількість чисел і виконувати три обчислення елементів V_k-послідовності за прискореним алгоритмом замість двох. Однак при цьому такий варіант методу буде мати дві суттєвих переваги, по-перше, підвищиться стійкість методу, оскільки тепер зловмиснику замість індексу $b + c \cdot a$ буде відомий набір елементів $v_{b+c \cdot a,k} \bmod p$, обчислених за цим індексом, і, по-друге, значно спроститься процедура перевірки автентичності, оскільки в такому випадку перевіряльнику необхідно буде виконувати лише одне обчислення елементів V_k-послідовності за прискореним алгоритмом, причому здійснювати ці обчислення він зможе навіть попередньо, а не під час безпосередньої автентифікації.

В разі необхідності існує можливість ще більшого підвищення стійкості запропонованого методу автентифікації [6], якщо перевіряльнику замість індексу c обчислювати і передавати претенденту елементи $v_{c+i,k} \bmod p$, $i = \overline{-(k-1), 0}$ (заявка на корисну модель № u 2013 06319 від 22. 05. 2013 р.), але такий варіант методу не дає можливості спрощувати обчислення.

Відомо [2], що будь-який метод автентифікації, який 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 саму схему цифрового підписування. Виходячи з цього, запропоновані методи автентифікації на основі V_k — послідовності можуть бути перетворені в методи цифрового підписування (заявки на корисну модель № u 2013 06322 та № u 2013 06323 від 22. 05. 2013 р.).

Висновки

Запропоновано метод автентифікації суб'єктів (об'єктів) взаємодії на основі математичного апарату рекурентних V_k-послідовностей, в якому відбувається заміна піднесення до степеня обчисленням елементу рекурентної послідовності з певним індексом. Наведено протокол реалізації методу, а також проведено аналіз його криптографічної стійкості та обчислювальної складності у

порівнянні з відомим аналогом.

Аналіз показав, що в цілому криптографічна стійкість і обчислювальна складність запропонованого методу знаходяться приблизно на тому ж рівні, що й відомого аналога, але при цьому запропонований метод за певних умов дозволяє значно спрощувати обчислення процедури перевірки автентичності, а також підвищувати стійкість всього процесу автентифікації.

Крім того, в запропонованому методі забезпечується можливість збільшення стійкості пропорційно порядку рекурентних послідовностей, що лежать в основі автентифікації, а також спрощення процедури завдання параметрів.

Існує також можливість перетворення методів автентифікації на основі V_k-послідовності в методи цифрового підписування.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Menezes A. J. Handbook of Applied Cryptography / 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 / Б. Шнайер. — М. : Триумф, 2002. — 816 с.

3. Яремчук Ю. Є. Використання рекурентних послідовностей для побудови криптографічних методів з відкритим ключем / Ю. Є. Яремчук // Захист інформації. — 2012. — № 4. — С. 120—127.

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

5. Яремчук Ю. Є. Метод автентифікації сторін взаємодії на основі рекурентних послідовностей / Ю. Є. Яремчук // Сучасний захист інформації. — 2013. — № 1. — С. 4—10.

6. Яремчук Ю. Є. Методи автентифікації на основі рекурентних послідовностей / Ю. Є. Яремчук // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. — 2013. — Вип. 1(25). — С. 39—48.

Рекомендована кафедрою адміністративного та інформаційного менеджменту

Стаття надійшла до редакції 8.05.2013
Рекомендована до друку 20.05.2013

Яремчук Юрій Євгенович — професор кафедри адміністративного та інформаційного менеджменту.
Вінницький національний технічний університет, Вінниця