



ДЕРЖАВНА СЛУЖБА
ІНТЕЛЕКТУАЛЬНОЇ
ВЛАСНОСТІ
УКРАЇНИ

УКРАЇНА

(19) **UA** (11) **84273** (13) **U**
(51) МПК (2013.01)
H03M 13/00

(12) ОПИС ДО ПАТЕНТУ НА КОРИСНУ МОДЕЛЬ

| | |
|----------------------------------------------------------------------------|----------------------------------------------------------------|
| (21) Номер заявки: u 2013 06321 | (72) Винахідник(и): Яремчук Юрій Євгенович (UA) |
| (22) Дата подання заявки: 22.05.2013 | (73) Власник(и): Яремчук Юрій Євгенович, |
| (24) Дата, з якої є чинними права на корисну модель: 10.10.2013 | вул. Воїнів-Інтернаціоналістів, 9-а/63, м. Вінниця, 21021 (UA) |
| (46) Публікація відомостей про видачу патенту: 10.10.2013, Бюл.№ 19 | |

(54) СПОСІБ АВТЕНТИФІКАЦІЇ СУБ'ЄКТІВ (ОБ'ЄКТІВ) ВЗАЄМОДІЇ НА ОСНОВІ ЕЛЕКТРОННОГО КОДУ

(57) Реферат:

Спосіб автентифікації суб'єктів (об'єктів) взаємодії на основі електронних кодів базується на доведенні з нульовим розголошенням знання і включає процедури доведення та перевірки автентичності на основі електронних кодів, секретний ключ та обчислений на його основі відкритий ключ суб'єкта (об'єкта), що доводить свою автентичність. В процедурах доведення та перевірки автентичності на основі електронних кодів використовують обчислення елементів рекурентних послідовностей з заданим індексом, а саме рекурентної послідовності.

UA 84273 U

Корисна модель належить до техніки криптографічного захисту інформації і може використовуватися в системах захисту інформації, комп'ютерних мережах, банківських та електронних платіжних системах, системах стільникового зв'язку та інших інформаційно-обчислювальних і телекомунікаційних системах.

Відомий спосіб автентифікації суб'єктів (об'єктів) взаємодії, на основі електронних кодів що базується на доведенні з нульовим розголошенням знання (A. Fiat and A. Shamir, "How to Prove Yourself: Practical Solutions to Identification Signature Problems", Advances in Cryptology CRYPTO '86 Proceedings, Springer - Verlag, 1987. - P. 186-194).

Спосіб базується на операції піднесення у квадрат за модулем, коли модуль є добутком двох простих чисел. Суть способу така. На попередньому етапі центр довіри вибирає два великих простих числа p і q , які він тримає у секреті, і публікує велике число $n : n = pq$, $n \geq 512$ біт (рекомендується обирати $n \sim 1024$). Далі претендент (сторона, яка доводить свою автентичність) вибирає свій секретний ключ s , причому таким чином, щоб виконувались такі умови $(s, n) = 1$, $1 \leq s \leq n-1$. Після цього обчислюється відкритий ключ v претендента як $v = s^2 \pmod n$, який разом з модулем схеми n стає відомий усім суб'єктам (об'єктам) взаємодії.

На етапі безпосередньої автентифікації виконуються такі дії:

- претендент вибирає випадкове число r , $r < n$, обчислює $x = r^2 \pmod n$ і відправляє його перевіряльнику (стороні, яка перевіряє автентичність);
- перевіряльник вибирає випадковий біт $e \in \{0, 1\}$ і надсилає його претенденту;
- якщо $e = 0$, то претендент відправляє перевіряльнику число r , інакше, якщо $e = 1$, він відправляє число $y = r \cdot s \pmod n$;
- перевіряльник перевіряє, якщо $y \neq 0$ (якщо $y = 0$, доведення повинно бути недейсним, тому що $r = 0$); якщо ця умова виконується, то перевіряється рівняння $y^2 \equiv x \cdot v^e \pmod n$ і у випадку його виконання доведення приймається перевіряльником.

Вказані дії при безпосередній автентифікації повторюються у циклі t разів. Ймовірність обману претендентом перевіряючого (тобто ймовірність помилкового рішення) при однократному виконанні вказаних дій дорівнює $1/2$, відповідно при виконанні циклу t разів ймовірність дорівнює $1/2^t$. Число t називається параметром безпеки протоколу, його рекомендується обирати на рівні 20...40. Вважається, що перевіряльник пройшов автентифікацію, якщо перевірка порівняння на останньому кроці в усіх t циклах завершилась з позитивним результатом.

Стійкість даного способу основана на складності витягнення квадратного кореня n , коли невідомо розкладання n на прості множники.

Відомий спосіб автентифікації суб'єктів (об'єктів) взаємодії на основі електронних кодів, що базується на доведенні з нульовим розголошенням знання (U. Feige, A. Fiat, and A. Shamir. Zero Knowledge Proofs of Identity. Proceedings of the IPth Annual ACM Symposium on the Theory of Computing, 1987, pp. 210-217).

Суть способу полягає в тому, що він базується на тих же обчисленнях, що і розглянутий перед цим спосіб Фіата-Шаміра і є вдосконаленням цього способу за рахунок використання паралельної схеми обчислень, яка дозволила зменшити кількість раундів обміну між претендентом та перевіряльником при збереженні властивості нульового розголошення знань.

На попередньому етапі центром довіри вибирається число n як і в способі Фіата-Шаміра.

Далі претендент вибирає свій секретний ключ у вигляді k різних чисел $\{s_i\}_{i=1}^k$, де кожне s_i :

$(s_i, n) = 1$, $1 \leq s_i \leq n-1$. Рядок $\{v_i\}_{i=1}^k$, де $v_i = s_i^2 \pmod n$, приймається як відкритий ключ претендента.

Під час безпосередньої автентифікації виконуються такі дії:

- претендент вибирає випадкове число r , $r < n$, обчислює $x = r^2 \pmod n$ і відправляє його перевіряльнику;
- перевіряльник виробляє випадковий двійковий рядок $\{e_i\}_{i=1}^k$, $e_i \in \{0, 1\}$, і надсилає його претенденту;

- претендент обчислює $y = r \cdot \prod_{i=1}^k s_i^{e_i}$, перемножуючи лише ті s_i , які відповідають одиничним бітам вектора e , і надсилає у перевіряльнику;

- перевіряльник перевіряє, чи $x = y^2 \cdot \prod_{i=1}^k v_i^{e_i}$.

Як і в попередньому способі вказані дії при безпосередній автентифікації повторюються у циклі t разів. При цьому ймовірність помилки перевіряльника у t проходах циклу дорівнює $1/2^{kt}$. Автори способу рекомендують вибирати $k = 5$, $t = 4$.

5 Стьйкість даного способу, як і його прототипу Фіата-Шаміра, базується на складності витягнення квадратного кореня n , коли невідомо розкладання n на прості множники.

Відомий спосіб автентифікації суб'єктів (об'єктів) взаємодії, на основі електронних кодів що базується на доведенні з нульовим розголошенням знання (L.C. Guillou and J.-J. Quisquater. A Practical Zero-Knowledge Protocol Fitted to Security Microprocessor Minimizing Both Transmission and Memory. Advances in Cryptology EUROCRYPT'88 Proceedings, Springer-Verlag, 1988. - P. 123-128).

10 Суть способу базується на використанні операції піднесення до степеня за модулем великих чисел, і полягає в тому, що в ньому визначається відкритий ключ як $J = h(I_p)$ або просто $J = I_p$, де h - хеш-функція, а I_p рядок ідентифікаційних даних про претендента, що включає, 15 наприклад його ім'я, термін повноважень, номер банківського рахунку і т.п. У випадку $J = I_p$ - це по суті є вірча грамота (credentials) претендента. Центр довіри виробляє і публікує число $n = p \cdot q$, де p і q - великі прості числа (секретні), а також число v , що визначається з порівняння $J B^v \equiv 1 \pmod{n}$, де B - секретний ключ претендента. Перед початком автентифікації перевіряльник зчитує у претендента рядок J .

20 Під час безпосередньої автентифікації виконуються такі кроки:

- претендент вибирає випадкове число r , $1 < r < n-1$, обчислює $T = r^v \pmod{n}$ і відправляє його перевіряльнику;

- перевіряльник вибирає випадкове число $d \in \mathbb{Z}$, $d < 0 < v-1$, і надсилає його претенденту;

- претендент обчислює $D = r \cdot B^d \pmod{n}$ і надсилає його перевіряльнику;

25 - перевіряльник обчислює $T' = D^v \cdot J^d \pmod{n}$. Автентифікація вважається завершеною успішно, якщо $T \equiv T' \pmod{n}$.

В цілому стійкість способу базується на складності вирішення задачі дискретного логарифмування, а також складності задачі факторизації розкладання модуля n на два простих числа p і q .

30 Однак стійкість способу окремо має певні слабкості. По-перше, знання двох відповідей D_1 і D_2 на два різних запита d_1 і d_2 при однаковому T еквівалентно знанню B^k , де $k = \text{НОД}(v, d_2 - d_1)$. По-друге, не важко пересвідчитись, що злоумисник може доволі легко обчислити секретний ключ B претендента. Виходячи з цього, для забезпечення стійкості претендент щоразу повинен вибирати число r таким, щоб воно не повторювалось з 35 попереднім.

Відомий спосіб автентифікації суб'єктів (об'єктів) взаємодії, на основі електронних кодів що базується на доведенні з нульовим розголошенням знання (C.P. Schnorr. Efficient Signature Generation for Smart Cards. Advances CRYPTO '89 Proceedings, Springer-Verlag, 1990. - P. 239-252) (найближчий аналог).

40 Суть способу базується на використанні операції піднесення до степеня великих чисел за модулем і полягає в тому, що на попередньому етапі центр довіри або претендент вибирає і відкрито публікує два простих числа p і q $q | p-1$ та число $a \neq 1$: $a^q \equiv 1 \pmod{p}$. Потім він вибирає випадкове число $s < q$ як секретний ключ та обчислює $d = a^{-s} \pmod{p}$ - відкритий ключ, який передається перевіряльнику. Після цього безпосередній етап автентифікації реалізується 45 таким чином:

- претендент вибирає випадкове число $r < q$, обчислює $x = a^r \pmod{p}$ і надсилає x перевіряльнику (ці обчислення можуть бути виконані і попередньо).

- перевіряльник виробляє випадкове число e : $0 < e \leq 2^t - 1$ і надсилає його претенденту.

- претендент обчислює $y = r + se \pmod{q}$ і надсилає його перевіряльнику.

50 - перевіряльник перевіряє рівняння $x = a^y d^e \pmod{p}$.

Безпека методу визначається величиною параметру t . Автори способу показують, що складність розкриття способу складає 2^t операцій і рекомендують вибирати $p \sim 512$ біт, $q \sim 140$ біт, $t = 72$ біти. Слід також зазначити, що властивість нульового розголошення для цього способу строго не доведена.

5 Стієкість способу базується на складності вирішення задачі дискретного логарифмування.

Загальним недоліком більшості розглянутих способів автентифікації на основі електронних кодів є те, що в них в процедурі перевірки автентичності виконуються складні обчислення, зокрема в найближчому аналогу, способі автентифікації Шнорра, необхідно виконувати два піднесення до степенів великих чисел за модулем без можливості виконання попередніх обчислень. Це створює певні труднощі під час використання способів 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 безпроводних мережах, організації банківських трансакцій, організації мобільної комерції, авторизації електронних повідомлень та інші. Необхідність виконання в таких задачах за існуючими способами автентифікації складних обчислень в процедурі перевірки автентичності створює перевіряльнику певні незручності, в зв'язку з чим дуже важливим є можливість прискорення виконання цієї процедури при забезпеченні достатнього рівня криптостійкості. Забезпечення останнього також є важливим, оскільки, скажімо серед існуючих способів автентифікації вказаний недолік в меншій мірі стосується способу автентифікації Фіата-Шаміра, однак при цьому спосіб Фіата-Шаміра забезпечує і менший рівень стійкості при рівних умовах порівняно з іншими існуючими аналогами, що значно обмежує галузь використання цього способу.

В основу корисної моделі поставлено задачу створення способу автентифікації суб'єктів (об'єктів) взаємодії на основі електронних кодів з можливістю доведення з нульовим розголошенням знання, в якому за рахунок використання математичного апарату рекурентних послідовностей, коли за основу обчислень береться обчислення елемента рекурентної послідовності з певним індексом, досягається можливість зменшення обчислювальної складності процедури перевірки автентичності при забезпеченні достатнього рівня криптостійкості. Крім цього забезпечується можливість збільшення стійкості пропорційно порядку рекурентних послідовностей, що лежать в основі автентифікації, а також спрощення процедури завдання параметрів.

Поставлена задача вирішується тим, що використання в основі автентифікації обчислень елементів рекурентних послідовностей з певними індексами та властивостей цих послідовностей дозволяє під час автентифікації на основі електронних кодів в процедурі перевірки автентичності певні обчислювання елементів рекурентних послідовностей виконувати попередньо, тим самим зменшуючи майже у два рази обчислювальну складність процедури перевірки автентичності безпосередньо під час автентифікації.

Зокрема пропонується як математичний апарат рекурентних послідовностей використовувати апарат рекурентних V_k -послідовностей, які є узагальненими рекурентними послідовностями, при обчисленні елементів яких використовуються рекурентні залежності з коефіцієнтами, що пов'язані з початковими елементами послідовностей.

V_k -послідовністю назовемо послідовність, яка складається з

V_k^+ -послідовності та V_k^- -послідовності.

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

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

для початкових значень $v_{0,k} = 1$, $v_{1,k} = g_2$ для $k = 2$; $v_{0,k} = v_{1,k} = \dots = v_{k-3,k} = 0$, $v_{k-2,k} = 1$,

50 $v_{k-1,k} = g_k$ 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

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

V_k^- -послідовністю назвемо 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 $k = 2$; $v_{-1,k} = 0$, $v_{-2,k} = g_1^{-1}$, $v_{-3,k} = v_{-4,k} = \dots = v_{-k,k} = 0$ для $k > 2$.

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

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

5 Для будь-яких цілих додатних n і m , таких що $1 \leq m < n$ та будь-якого цілого додатного k отримано таку залежність

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

Суть способу автентифікації на основі електронних кодів, що пропонується, базується на використанні властивості (3) V_k^- -послідовності, яка дозволяє використовувати її для обчислення елемента $v_{n+m,k}$, а також для обчислення елемента $v_{-n+m,k}$. Крім цього властивість (3) дозволяє реалізувати процедуру обчислення елемента $v_{n-m,k}$. Так само на основі властивості (4) можна реалізувати процедуру обчислення елемента $v_{-a+i,k}$. Все це дає можливість створення такого способу автентифікації.

Спочатку претендент (або центр довіри) виконує попередню процедуру обчислення ключів у вигляді електронних кодів. Для цього він випадковим чином вибирає секретний ключ a , після чого 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 $v_{-a-c+i,k}$, $i = \overline{-(k-1), 0}$, на основі елементів $v_{-a+i,k}$, $i = \overline{-k, k-2}$, та свого сеансового ключа c .

Потім претендент обчислює значення $b+c \cdot a$ 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 $b+c \cdot a$ елементи $v_{b+c \cdot a+i,k}$, $i = \overline{-1, k-2}$, а потім використовує отримані елементи для обчислення x' як $x' = v_{-a-c+(b+c \cdot a),k}$ згідно залежності (3). На завершення він перевіряє отримане значення x' зі значенням x , яке він раніше отримав від претендента.

Загальна схема способу автентифікації на основі електронних кодів та математичного апарату рекурентних послідовностей, що пропонується, буде мати вигляд представлений на кресленні.

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

Вибір числа b та обчислення елемента $v_{b,k} \bmod p$; претендентом можуть бути виконані попередньо, заздалегідь до безпосередньої автентифікації. Так само попередньо перевіряльником може бути вибрано число c і обчислені на його основі та відкритого ключа елементи $v_{-a-c+i,k}$, $i = \overline{-(k-1), 0}$. Можливість попереднього 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 залежності (3). Обчислення елемента $v_{n+m,k}$ згідно з цією залежністю, 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.

Виходячи з вищесказаного, отримуємо такий протокол автентифікації на основі електронних кодів та елементів V_k^- -послідовності.

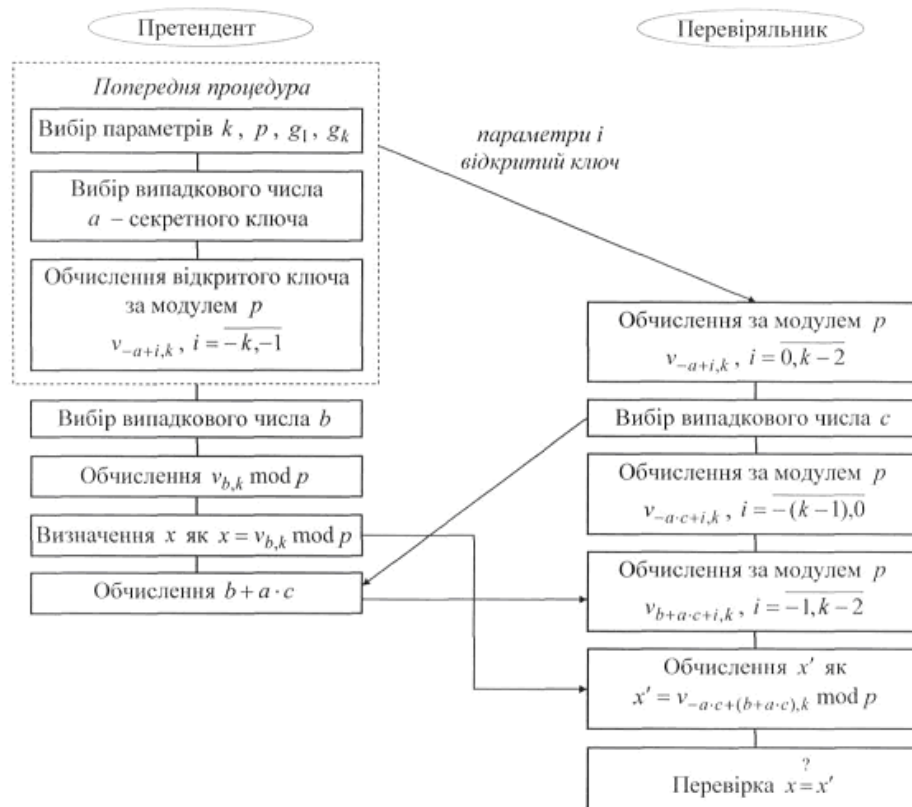
- Крок 1. Задати параметр k .
- Крок 2. Вибрати p .
- Крок 3. Вибрати g_1, g_k .
- Крок 4. Претенденту передати параметри Перевіряльнику.
- 5 Крок 5. Претенденту вибрати випадкове число a - секретний ключ.
- Крок 6. Претенденту обчислити відкритий ключ за модулем p $v_{-a+i,k}$, $i = \overline{-k, k-2}$, використовуючи алгоритм прискореного обчислення елементів $v_{n,k}$ для від'ємних значень n .
- Крок 7. Претенденту передати відкритий ключ $v_{-a+i,k} \bmod p$, $i = \overline{-k, -1}$, Перевіряльнику.
- Крок 8. Перевіряльнику обчислити за модулем p $v_{-a+i,k}$, $i = \overline{-0, k-2}$, за формулою (1).
- 10 Крок 9. Претенденту вибрати випадкове число b , а Перевіряльнику вибрати випадкове число c і передати його Претенденту.
- Крок 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
- 15 $v_{-m \cdot n, k}$.
- Крок 11. Претенденту визначити x як $x = v_{b,k} \bmod p$ і передати отримане значення Перевіряльнику.
- Крок 12. Претенденту обчислити значення $b + c \cdot a$ і передати отримане значення Перевіряльнику.
- 20 Крок 13. Перевіряльнику обчислити за модулем p $v_{b+c \cdot a + i, k}$, $i = \overline{-1, k-2}$, використовуючи алгоритм прискореного обчислення елементів $v_{n,k}$ для додатних значень n .
- Крок 14. Перевіряльнику обчислити $x' = v_{-a \cdot c + (b+c \cdot a), k} \bmod p$ за формулою (3) та порівняти отримане значення з x , тобто перевірити $x = x'$.
- 25 Технічний результат: спрощено процедуру завдання параметрів; зменшено майже у два рази обчислювальну складність процедури перевірки автентичності безпосередньо під час автентифікації на основі електронних кодів і, як наслідок, збільшено швидкість безпосередньої перевірки автентичності, що значно розширює галузь використання таких способів.

ФОРМУЛА КОРИСНОЇ МОДЕЛІ

- 30 Спосіб автентифікації суб'єктів (об'єктів) взаємодії на основі електронних кодів, що базується на доведенні з нульовим розголошенням знання і включає процедури доведення та перевірки автентичності на основі електронних кодів, секретний ключ та обчислений на його основі відкритий ключ суб'єкта (об'єкта), що доводить свою автентичність, який **відрізняється** тим, що
- 35 в процедурах доведення та перевірки автентичності на основі електронних кодів використовують обчислення елементів рекурентних послідовностей з заданим індексом, а саме рекурентної V_k -послідовності, яка складається з V_k^+ -послідовності та V_k^- -послідовності, V_k^+ -послідовність визначається як послідовність чисел, що обчислюються за формулою $v_{n,k} = g_k v_{n-1,k} + g_1 v_{n-k,k}$, для початкових значень $v_{0,k} = 1$, $v_{1,k} = g_2$ для порядку послідовності
- 40 $k = 2$, $v_{0,k} = v_{1,k} = \dots = v_{k-3,k} = 0$, $v_{k-2,k} = 1$, $v_{k-1,k} = g_k$ для $k > 2$, де g_1, g_k - цілі числа, n і k - цілі додатні числа, V_k^- -послідовність визначається як послідовність чисел, що обчислюються за формулою $v_{n,k} = \frac{v_{n+k,k} - g_k \cdot v_{n+k-1,k}}{g_1}$ для n - від'ємних при початкових значеннях $v_{-1,k} = 0$,
- $v_{-2,k} = g_1^{-1}$ для $k = 2$, $v_{-1,k} = 0$, $v_{-2,k} = g_1^{-1}$, $v_{-3,k} = v_{-4,k} = \dots = v_{-k,k} = 0$ для $k > 2$, елементи V_k^- -послідовності $v_{n+m,k}$ для будь-яких цілих n та m розраховуються за формулою
- 45 $v_{n+m,k} = v_{m+(k-2),k} \cdot v_{n,k} + g_1 \cdot \sum_{i=1}^{k-1} v_{m+(k-2)-i,k} \cdot v_{n-k+i,k}$ елементи V_k^- -послідовності $v_{n-m,k}$ для будь-яких цілих n та m обчислюються за допомогою способу прискореного обчислення цих елементів з використанням бінарного способу розкладання індексу m та формули обчислення

- елементів $v_{n+m,k}$, при цьому доведення та перевірка автентичності на основі електронних кодів відбувається таким чином: спочатку претендент (або центр довіри) виконує попередню процедуру вибору параметрів та обчислення ключів у вигляді електронних кодів, для цього він вибирає параметр p як ціле додатне число, $p > 2$, яке потім використовується як модуль під час обчислень елементів V_k - послідовності, далі претендент випадковим чином вибирає секретний ключ a , $1 < a < p$, після чого обчислює відкритий ключ $v_{-a+i,k} \bmod p$, $i = \overline{-k, -1}$, за допомогою способу прискореного обчислення елементів $v_{n,k}$ з використанням бінарного способу розкладання індексу n , і передає перевіряльнику обчислений відкритий ключ, коли претендент хоче довести свою автентичність, він вибирає випадкове число b , $1 < b < p$, обчислює за модулем p , $v_{b+i,k}$, $i = \overline{-k, k-2}$, за допомогою способу прискореного обчислення елементів $v_{n,k}$, визначає з цього набору елементів значення x як $x = v_{b,k} \bmod p$ і передає його перевіряльнику, в цей час перевіряльник вибирає випадкове число c , $1 < c < p$, передає його претенденту, після чого обчислює за модулем p елементи $v_{-a \cdot c+i,k}$, $i = \overline{-(k-1), 0}$, на основі елементів $v_{-a+i,k} \bmod p$, $i = \overline{-k, k-2}$ та значення c за допомогою способу прискореного обчислення елементів $v_{n \cdot m,k}$, в цей час претендент обчислює значення $b + c \cdot a$ на основі свого секретного ключа a та значення b , а також значення c отриманого від перевіряльника, та передає обчислене значення перевіряльнику, після цього перевіряльник, використовуючи щойно отримане значення, обчислює за модулем p елементи $v_{b+a \cdot c+i,k}$, $i = \overline{-1, k-2}$, за допомогою способу прискореного обчислення елементів $v_{n,k}$, а потім перевіряльник використовує раніше обчислені ним елементи $v_{-a \cdot c+i,k} \bmod p$, $i = \overline{-(k-1), 0}$, та щойно обчислені елементи для обчислення x' як $x' = v_{-a \cdot c + (b + a \cdot c),k} \bmod p$, використовуючи формулу обчислення елементів $v_{n+m,k}$, на завершення він перевіряє щойно отримане значення x' зі значенням x , яке він раніше отримав від претендента.

25



Комп'ютерна верстка М. Ломалова

Державна служба інтелектуальної власності України, вул. Урицького, 45, м. Київ, МСП, 03680, Україна

ДП "Український інститут промислової власності", вул. Глазунова, 1, м. Київ – 42, 01601