



ДЕРЖАВНА СЛУЖБА
ІНТЕЛЕКТУАЛЬНОЇ
ВЛАСНОСТІ
УКРАЇНИ

УКРАЇНА

(19) **UA** (11) **84278** (13) **U**
(51) МПК (2013.01)
H03M 13/00

(12) ОПИС ДО ПАТЕНТУ НА КОРИСНУ МОДЕЛЬ

(21) Номер заявки: u 2013 06329	(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 ВИРОБЛЕННЯ ТА ПЕРЕВІРЯННЯ ЦИФРОВОГО ПІДПИСУ У ВИГЛЯДІ ЕЛЕКТРОННОГО КОДУ НА ОСНОВІ РЕКУРЕНТНИХ ПОСЛІДОВНОСТЕЙ

(57) Реферат:

Спосіб вироблення та перевіряння цифрового підпису у вигляді електронного коду на основі рекурентних послідовностей включає процедури вироблення та перевіряння цифрового підпису у вигляді електронного коду, секретний ключ та обчислений на його основі відкритий ключ підписанта. Для отримання цифрового підпису у вигляді електронного коду використовують обчислення елементів рекурентних послідовностей з заданим індексом.

UA 84278 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 цифрового підписування, що базується на використанні операції піднесення до степеня великих чисел за модулем (Т. ElGamal, "A Public-Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms", Advances in Cryptology: Proceedings of CRYPTO 84, Springer Verlag, 1985, pp. 1-18.)

Суть способу полягає в тому, що на попередньому етапі центр довіри або відправник (підписант) вибирає і відкрито публікує просте число p та ціле число g , $1 < g < p$. Потім він вибирає випадкове число a , $1 \leq a \leq p-2$, як секретний ключ та обчислює $y = g^a \bmod p$ - відкритий ключ, який передається одержувачу (перевірятьнику). Після цього протокол цифрового підписування реалізується таким чином.

На етапі формування підпису підписант вибирає випадкове число k , $1 \leq k \leq p-2$ і $\text{НОД}(k, p-1) = 1$, та обчислює $r = g^k \bmod p$ (ці обчислення можуть бути виконані і попередньо). Потім він обчислює $s = k^{-1}(h(M) - a \cdot r) \bmod (p-1)$, де h - функція хешування, і надсилає повідомлення M з підписом (r, s) одержувачу.

На етапі перевірки підпису перевіряльник спочатку перевіряє чи $0 < r < p$ та $0 < s < p-1$ і, якщо хоча б одна умова не виконується, то підпис відкидається. А потім, якщо обидві ці умови виконуються, підпис приймається тоді і лише тоді коли виконується рівняння $g^{h(M)} \bmod p = y^r r^s \bmod p$.

Стійкість способу базується на складності вирішення задачі дискретного логарифмування.

Обчислювальна складність способу в основному визначається складністю виконання операцій піднесення до степеня великого числа за модулем. Всього згідно способу необхідно виконати чотири таких операції - по дві на кожному боці: з боку відправника обчислення на попередньому етапі відкритого ключа $y = g^a \bmod p$ та значення $r = g^k \bmod p$, з боку одержувача - $y^r \bmod p$ та $r^s \bmod p$.

Відомий спосіб цифрового підписування, що базується на використанні операції піднесення до степеня великих чисел за модулем (C.P. Schnorr, "Efficient Signature Generation for Smart Cards". Advances CRYPTO '89 Proceedings, Springer-Verlag, 1990, pp. 239-252).

Суть способу полягає в тому, що він базується на тих же обчисленнях, що і розглянутий перед цим спосіб Ель-Гамала і є одним з варіантів цього способу.

На попередньому етапі центр довіри або відправник вибирає і відкрито публікує два простих числа p і q : $q \mid p-1$ та число $g \neq 1$: $g^q \equiv 1 \pmod{p}$. 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 $k < q$ та обчислює $x = g^k \bmod p$; (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 $s = (k + a \cdot r) \bmod q$ і надсилає повідомлення M з підписом (r, s) одержувачу.

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

Стійкість способу базується на складності вирішення задачі дискретного логарифмування. Обчислювальна складність способу, як і в попередньому способі, в основному визначається складністю виконання операцій піднесення до степеня великого числа за модулем, яких так само необхідно виконувати чотири - по два на кожному боці.

Відомий спосіб цифрового підписування, що базується на використанні математичного апарату рекурентних послідовностей (P. Smith, C. Skinner, A public-key cryptosystem and a digital signature system based on the Lucas function analogue to discrete logarithms, in Advances in Cryptology - Asiacrypt 1994, Lect. Notes in Comp. Sci. 917. Springer, Berlin, 1995, 357-364.) (найближчий аналог).

Суть способу (його іноді називають LUCELG DS) полягає у використанні рекурентної функції Люка і заміні піднесення до степеня за модулем, як це робиться в способі Ель-Гамала та його варіантах, на обчислення елементу рекурентної послідовності Люка за модулем простого числа p з певним індексом.

- 5 В способі використовуються рекурентні послідовності $\{T_n\}$, що отримуються з лінійного рекурентного співвідношення другого порядку такого вигляду

$$T_n = P \cdot T_{n-1} - Q \cdot T_{n-2}, \quad (1)$$

де P і Q взаємно прості числа.

Серед набору послідовностей $\{T_n\}$, що породжуються рекурентним співвідношенням (1),

- 10 виділяють послідовності $\{c_1\alpha^n + c_2\beta^n\}$, де c_1 , і c_2 - будь-які числа, із значеннями початкових елементів $T_0 = c_1 + c_2$ та $T_1 = c_1\alpha + c_2\beta$.

Спосіб базується на математичному апараті двох конкретних представників цієї послідовності, які позначаються $\{U_n\}$ та $\{V_n\}$ і визначаються таким чином:

$$U_n = \frac{\alpha^n - \beta^n}{\alpha - \beta}, \text{ відповідно } c_1 = \frac{1}{\alpha - \beta} = -c_2;$$

- 15 $V_n = \alpha^n + \beta^n$, відповідно $c_1 = 1 = c_2$.

Це є послідовності цілих чисел, оскільки їх початкові елементи приймають такі значення $U_0 = 0$, $U_1 = 1$, $V_0 = 2$, і $V_1 = P$.

Ці послідовності залежать тільки від цілих чисел P і Q , а функції, що їм відповідають, називають функціями Люка P і Q . Іноді їх записують як $U_n(P, Q)$ та $V_n(P, Q)$, щоб підкреслити

- 20 їхню залежність від P і Q .

Для цих послідовностей отримано такі аналітичні залежності:

$$V_{n+k}(P, 1) = V_n(V_k(P, 1), 1), \quad (2)$$

$$2V_{n+m} = V_n V_m + D U_n U_m = 2(\alpha^{n+m} + \beta^{n+m}). \quad (3)$$

- 25 Спосіб цифрового підписування базується на даному математичному апараті і по суті є еквівалентом способу Ель-Гамала. Основу способу складають аналітичні залежності (2) і (3), що дозволяють обчислювати елементи $V_n(P, Q)$ та $U_n(P, Q)$ - послідовностей різними шляхами.

На попередньому етапі цифрового підписування центр довір або відправник генерує та публікує просте число p , використовуючи такий генератор, що $V_{(p+1)/t}(\lambda, 1) \not\equiv 2 \pmod p$ для кожного

- 30 $t > 1$ поділеного на $(p+1)$. Потім він вибирає випадкове число $x < p$ як секретний ключ та отримує відкритий ключ у вигляді двох значень y та y' , що обчислюються як $y \equiv V_x(\lambda, 1) \pmod p$ та $y' \equiv U_x(\lambda, 1) \pmod p$, які передаються одержувачу. Після цього протокол цифрового підписування реалізується таким чином.

На етапі формування підпису відправник вибирає випадковим чином секретне число k , $0 < k < p$, для кожного повідомлення (або блоку повідомлення) m і обчислює $r \equiv V_k(\lambda, 1) \pmod p$

- 35 та $r' \equiv U_k(\lambda, 1) \pmod p$. Потім він обчислює s як $s \equiv k^{-1}(m - x \cdot r) \pmod{(p+1)}$ і надсилає цифровий підпису вигляді (m, r, r', s) одержувачу.

На етапі перевірки підпису одержувач, по аналогії із способом Ель-Гамала, спочатку обчислює ліву частину (LHS) як $LHS \equiv V_m(\lambda, 1) \pmod p$, потім, дещо складніше ніж в Ель-Гамала, обчислює праву частину (RHS) як

- 40 $RHS \equiv \{V_r(y, 1)V_s(r, 1) + Dy'U_r(r, 1)r'U_s(r, 1)\} / 2 \pmod p$,

$$\text{де } D \equiv \lambda^2 - 4 \pmod p.$$

Якщо $RHS = LHS$, тоді четвірка (m, r, r', s) вважається справжнім підписом способу LUCELG DS, інакше - підпис відкидається.

- 45 Стійкість способу базується на складності обчислення індексу рекурентної послідовності з обчисленого елементу цієї послідовності. Ця задача за обчислювальною складністю є аналогом задачі дискретного логарифмування. Тому спосіб має схожі характеристики з тими способами цифрового підписування, що базуються на дискретному логарифмуванні. Однак перевагою є те, що стійкість способів цифрового підписування на основі розглянутого математичного апарату рекурентних послідовностей не залежить від спроб криптоаналізу, що існують в задачах
- 50 дискретного логарифмування.

Недоліком цього способу цифрового підписування, який є найближчим аналогом, є те, що він має певні слабкості щодо стійкості, зокрема розглянуті функції Люка є вразливими до екзистенційної піддробки. Хоча при цьому вважається, що способи, які базуються на цих функціях, в цілому є більш стійкими, ніж ті, що базуються на математичному апараті еліптичних кривих. Однак, основним недоліком цього способу 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 спосіб на основі функцій Люка потребує досить складних обчислень при перевірці цифрового підпису.

Загальним недоліком розглянутих способів цифрового підписування є те, що одна з частин підпису являє собою число (у більшості способів значення s), а не, скажімо, результат піднесення до степеня, що визначається цим числом (як, наприклад, інша частина підпису r у більшості способів), 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 способах цифрового підписування створює перевіряльнику в таких випадках певні незручності, в зв'язку з чим важливим є прискорення виконання процедури перевірки підпису при забезпеченні достатнього рівня криптостійкості. До такого роду задач відносяться задачі авторизації та ідентифікації під час здійснення транзакцій в електронних платіжних системах та в системах стільникового зв'язку, забезпечення веб-транзакцій між клієнтом та сервером, організації банківських транзакцій, 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.

В основу корисної моделі покладено задачу створення способу цифрового підписування на основі математичного апарату більш узагальнених рекурентних послідовностей, ніж розглядалися раніше при побудові способів такого типу, коли для отримання цифрового підпису у вигляді електронного коду використовуються обчислення елементів рекурентних послідовностей з певним індексом на основі узагальнених рекурентних залежностей з коефіцієнтами, що пов'язані з початковими елементами послідовностей, в яких коефіцієнти рекурентних залежностей, початкові елементи та елементи послідовностей, що породжуються цими залежностями, можуть бути будь-якими цілими числами без додаткових умов та обмежень. За рахунок цього досягається можливість підвищення стійкості цифрового підписування, а також зменшення обчислювальної складності процедури перевірки підпису. Крім того забезпечується можливість збільшення стійкості пропорційно порядку рекурентних послідовностей, що лежать в основі цифрового підписування, а також спрощення процедури завдання параметрів.

Поставлена задача вирішується тим, що використання в основі цифрового підписування більш узагальнених рекурентних послідовностей та їх властивостей дозволяє під час цифрового підписування обчислювати підписанту і передавати перевіряльнику одну з частин підпису у вигляді не самого числа, як це робиться у відомих аналогах (у більшості аналогів це значення s), а у вигляді елемента рекурентної послідовності з індексом, що визначається цим числом. Враховуючи, що рівень складності обчислень певного елемента рекурентної послідовності є не меншим, ніж, скажімо, піднесення до заданого степеня, це дає можливість значно підвищити стійкість схеми цифрового підписування до атак зловмисника. В той же час, використання математичного апарату більш узагальнених рекурентних послідовностей в основі цифрового підписування, ніж у найближчому аналозі, надає більші можливості щодо спрощення обчислень, що, в першу чергу, може бути використано для спрощення обчислень процедури перевірки підпису при розробці способу цифрового підписування.

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

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

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

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

V_k^- -послідовністю назовемо 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 $k = 2$;

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

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

$$10 \quad v_{n+m,k} = v_{m+(k-2),k} \cdot v_{n,k} + g_1 \cdot \sum_{i=1}^{k-1} v_{m+(k-2)-i,k} \cdot v_{n-k+i,k} \quad (6)$$

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

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

Суть способу 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 $v_{n-m,k}$. Так само на основі властивості (7) можна реалізувати процедуру обчислення елементу $v_{-n-m,k}$. Все це дає можливість створення такого способу цифрового підписування.

20 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-перевірятьнику відкритий ключ $v_{-a+i,k}, i = \overline{-k, -1}$.

25 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 вибраної функції хешування h від повідомлення M , і обчислює для s елементи $v_{s+i,k}, i = \overline{-k, -2}$. Після цього отриману множину цілих чисел $\{r; v_{s+i,k}, i = \overline{-1k, -2}\}$ він перетворює у цифровий підпис вигляду

$$DS = (0 \| r \| 0 \| v_{s-1,k} \| 0 \| v_{s,k} \| \dots 0 \| v_{s+(k-2),k}) \text{ і передає його разом з повідомленням } M \text{ одержувачу.}$$

30 При перевірці цифрового підпису одержувач спочатку обчислює $v_{-a+r+i,k}, i = \overline{-(k-1), 0}$, на основі відкритого ключа - елементів $v_{-a+i,k}, i = \overline{-k, k-2}$, та отриманого від підписанта значення r . Потім він обчислює елемент $v_{b \cdot h(M),k}$ як $v_{b \cdot h(M),k} = v_{-a+r+s,k}$ використовуючи залежність (6), і обчислює значення r' як $r' = v \left[\frac{b \cdot h(M)}{h(M)} \right]$ та перевіряє, чи виконується $r = r'$. Якщо так, то підпис приймається, в іншому випадку - відкидається.

35 Не важко пересвідчитись, що для підпису, згенерованого згідно цього методу, перевірка $r = r'$ завжди буде виконуватись.

Загальна схема способу цифрового підписування на основі математичного апарату рекурентних послідовностей, що пропонується, буде мати вигляд представлений на кресленні.

40 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.

Виходячи з вищесказаного отримаємо такий протокол цифрового підписування на основі елементів V_k -послідовності.

Крок 1. Задати параметр k .

Крок 2. Вибрати p .

Крок 3. Вибрати g_1, g_k .

Крок 4. Відправнику передати параметри Одержувачу.

Крок 5. Відправнику вибрати випадкове число a - секретний ключ.

Крок 6. Відправнику обчислити відкритий ключ за модулем p $v_{-a+i,k}, i = \overline{-k, k-1}$, використовуючи алгоритм прискореного обчислення елементів $v_{n,k}$ для від'ємних значень n .

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

Крок 8. Одержувачу обчислити за модулем p $v_{-a+i,k}, i = \overline{-0, k-2}$, за формулою (4).

Крок 9. Відправнику вибрати випадкове число b .

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

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

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

Крок 13. 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 .

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

Крок 15. Одержувачу обчислити за модулем p $v_{-a+r+i,k}, i = \overline{-(k-1), 0}$, використовуючи алгоритм прискореного обчислення елементів $v_{-m,n,k}$.

Крок 16. Одержувачу обчислити $v_{b \cdot h(M),k} \bmod p$ як $v_{b \cdot h(M),k} \equiv v_{-a \cdot r + s,k} \pmod{p}$ згідно залежності (6).

Крок 17. Одержувачу обчислити значення r' як $r' = v_{\left[\begin{smallmatrix} b \cdot h(M) \\ h(M) \end{smallmatrix} \right]} \bmod p$, використовуючи алгоритм прискореного обчислення елементів $v_{-m,n,k}$.

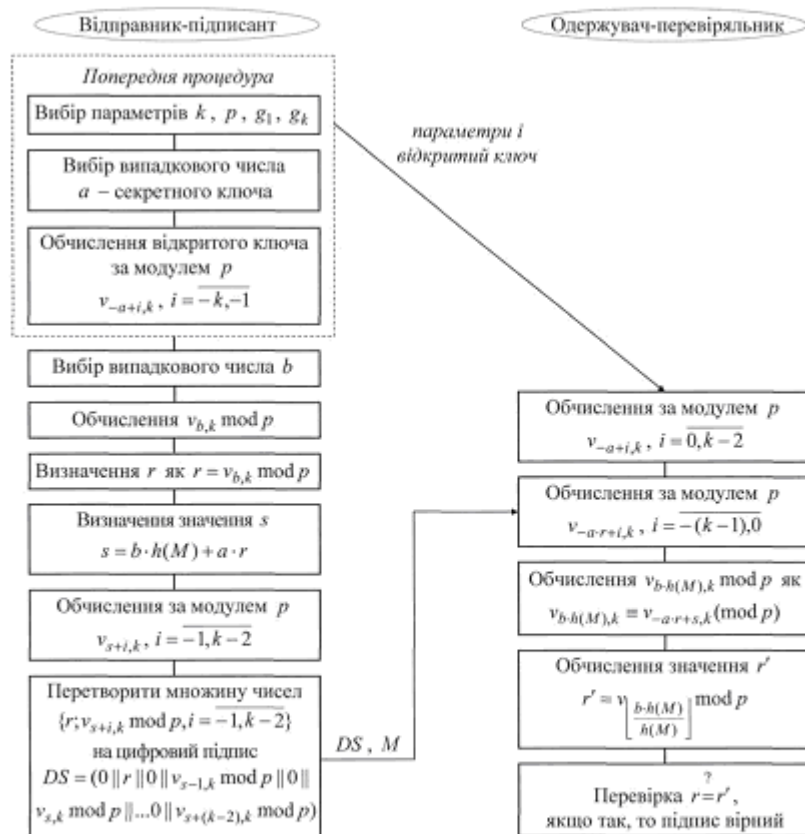
Крок 18. Одержувачу перевірити, чи виконується $r = r'$, якщо так, то підпис вважати вірним.

Технічний результат: підвищується стійкість та достовірність цифрового підписування, забезпечується можливість збільшення стійкості пропорційно порядку рекурентних послідовностей, що лежать в основі цифрового підписування; спрощується процедура завдання параметрів; зменшується майже вдвічі обчислювальна складність процедури перевірки підпису і, як наслідок, суттєво збільшується швидкодія процедури перевірки підпису, що дає можливість розширення галузі використання таких способів цифрового підписування.

ФОРМУЛА КОРИСНОЇ МОДЕЛІ

Спосіб вироблення та перевіряння цифрового підпису у вигляді електронного коду на основі рекурентних послідовностей, що включає процедури вироблення та перевіряння цифрового підпису у вигляді електронного коду, секретний ключ та обчислений на його основі відкритий

- ключ підписанта, який **відрізняється** тим, що для отримання цифрового підпису у вигляді електронного коду 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 визначають 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 $k=2$, $v_{0,k} = v_{1,k} = \dots = v_{k-3,k} = 0$, $v_{k-2,k} = 1$, $v_{k-1,k} = g_k$ для $k > 2$, де g_1, g_k - цілі числа, n і k - цілі додатні числа, V_k^- -послідовність визначають 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 розраховують за формулою $v_{n+m,k} = v_{m+(k-2),k} \cdot v_{n,k} + g_1 \cdot \sum_{i=1}^{k-1} v_{m+(k-2)-i,k} \cdot v_{n-k+i,k}$, елементи V_k -послідовності $v_{n-m,k}$ для будь-яких цілих n та m обчислюють за допомогою способу прискореного обчислення цих елементів з використанням бінарного способу розкладання індексу m та формули обчислення елементів $v_{n+m,k}$, при цьому вироблення та перевіряння цифрового підпису у вигляді електронного коду відбувається таким чином: спочатку відправник-підписант (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 він випадковим чином вибирає секретний ключ a , $1 < a < p$, який він використовує для обчислення відкритого ключа $v_{-a+i,k} \bmod p$, $i = \overline{-k, -1}$, за допомогою способу прискореного обчислення елементів $v_{n,k}$ з використанням бінарного способу розкладання індексу n , i передає одержувачу-перевіральному обчислений відкритий ключ, при виробленні цифрового підпису у вигляді електронного коду для повідомлення M відправник-підписант вибирає випадкове число b , $1 < b < p$, обчислює елемент $v_{b,k} \bmod p$ за допомогою способу прискореного обчислення елементів $v_{n,k}$, i визначає значення r , представлене у вигляді електронного коду, як $r = v_{b,k} \bmod p$, далі він визначає значення s як $s = b \cdot h(M) + a \cdot r$ за допомогою вибраної функції хешування h у діапазоні чисел, що обмежуються $p-1$, від повідомлення M та значення x , i обчислює для цього значення за модулем p елементи $v_{s+i,k}$; $i = \overline{-1, k-2}$, за допомогою способу прискореного обчислення елементів $v_{n,k}$, після цього отриману множину цілих чисел $\{r; v_{s+i,k} \bmod p, i = \overline{-1, k-2}\}$ він перетворює у цифровий підпис як електронний код у вигляді $DS = (0 \| r \| 0 \| v_{s-1,k} \bmod p \| 0 \| v_{s,k} \bmod p \| \dots \| 0 \| v_{s+(k-2),k} \bmod p)$ і передає його разом з повідомленням M одержувачу, при перевірці цифрового підпису у вигляді електронного коду одержувач спочатку обчислює за модулем p елементи $v_{-a+r+i,k}$, $i = \overline{-(k-1), 0}$, на основі відкритого ключа - елементів $v_{-a+i,k} \bmod p, i = \overline{-k, k-2}$, та отриманого від підписанта значення r за допомогою способу прискореного обчислення елементів $v_{n-m,k}$, потім він обчислює елемент $v_{b \cdot h(M),k} \bmod p$ як $v_{b \cdot h(M),k} \equiv v_{-a \cdot r + s,k} \pmod{p}$, використовуючи формулу обчислення елементів $v_{n+m,k}$, i обчислює значення r' у вигляді електронного коду як $r' = v_{\left[\frac{b \cdot h(M)}{h(M)} \right]} \bmod p$, використовуючи спосіб прискореного обчислення на основі способу прискореного обчислення елементів $v_{n-m,k}$, але з відніманням від індексу $n \cdot m$ числа $n \cdot m - 1$ разів, після цього він перевіряє, чи виконується рівняння $r = r'$, якщо так, то підпис приймається, в іншому випадку - відкидається.



Комп'ютерна верстка А. Крулевський

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