УДК 681.3.067

Ю. Є. Яремчук
Вінницький національний технічний університет,
вул. Хмельницьке шосе, 95, 21021 Вінниця, Україна

Метод вироблення та перевіряння цифрового підпису на основі рекурентних послідовностей

Запропоновано метод вироблення та перевіряння цифрового підпису, що базується на математичному апараті рекурентних V_k*-послідовностей, а також схему та протокол його реалізації. Аналіз запропонованого методу показав, що, у порівнянні з відомими аналогами, він є більш стійким і майже вдвічі забезпечує спрощення обчислень під час перевіряння підпису, крім того запропонований метод має значно простішу процедуру завдання параметрів.*

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

Вступ

Розвиток інформаційних технологій та засобів телекомунікації привів до зростання користувачів локальних і глобальних комп'ютерних мереж і, як наслідок, до збільшення електронного документообігу, що там циркулює. При цьому виникає проблема забезпечення цілісності та автентичності даних, що передаються та обробляються. На сьогодні найбільш ефективним вирішенням цієї проблеми є цифрове підписування [1–4], яке, окрім електронного документообігу, отримало широке застосування в таких прикладних задачах як забезпечення банківських трансакцій, забезпечення безпеки електронних платіжних систем та електронної комерції, підписування повідомлень електронної пошти, підписування цифрових сертифікатів та ін.

Цифровий підпис у цифрових документах відіграє ту ж роль, що і підпис, поставлений від руки на паперових документах, тобто це дані, що приєднуються до повідомлення, яке передається, і підтверджують, що автор підпису (відправник-підписант) склав і завірив дане повідомлення. Одержувач (перевіряльник) повідомлення або третя сторона за допомогою цифрового підпису може пересвідчитися, що автором повідомлення є саме власник підпису, і що у процесі передавання не було порушено цілісність даних.

Цифрове підписування передбачає два етапи: вироблення та перевіряння цифрового підпису, що реалізується за певним протоколом [1]. Найбільш відомими є методи цифрового підписування RSA [5], Ель-Гамаля [6], Шнорра [7], DSA [8], що базуються на математичному апараті піднесення до степеня великих цілих чисел, а також методи на основі математичного апарату еліптичних кривих (ECDSA, ДСТУ 4145-2002, ГОСТ Р34.10-2001 та інші [9–11]). Однак математичні апарати, на яких базуються ці методи, вимагають виконання досить складних обчислень, що впливає на швидкість роботи методів при їхній практичній реалізації. Тому актуальним залишається питання пошуку та використання таких математичних апаратів, які б забезпечували спрощення обчислень під час вироблення та перевіряння цифрового підпису.

Також недоліком відомих 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 би значно ускладнювали зловмиснику його спроби щодо зламу, і цим самим підвищували би стійкість цифрового підписування.

Окрім того, існують задачі, в яких процес перевірки цифрового підпису щодо складності обчислень домінує над процесом вироблення. До таких задач, у першу чергу, відносяться клієнт-серверні застосування, прикладом яких на практиці можуть бути центри сертифікації ключів, центри видачі цифрових атестатів, електронні платіжні системи та ін. У таких задачах перевіряльник за одиницю часу може отримувати велику кількість запитів на перевірку підпису, що, в свою чергу, може створювати для нього проблему перенавантаження.

Враховуючи вищесказане, слід звернути увагу на математичний апарат рекурентних послідовностей [12, 13], який дозволяє за певних умов спрощувати обчислення під час вирішення криптографічних задач і підвищувати стійкість на певних етапах криптографічних перетворень. Так у роботах [14, 15] представлено методи автентифікації сторін взаємодії, які базуються на рекурентних V_k-послідовностях і забезпечують за різних умов спрощення обчислень і підвищення стійкості.

Таким чином, актуальною є розробка методу вироблення та перевіряння цифрового підпису на основі рекурентних V_k-послідовностей, який би забезпечував прискорення процедури перевіряння підпису і при цьому забезпечував підвищення рівня криптографічної стійкості.

Метод вироблення та перевіряння цифрового підпису на основі рекурентних V_k-послідовностей

У [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

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

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 здійснюватися 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 (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 [12]:

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

Для будь-яких цілих додатних n і m, таких що $1 \le m < n$, та будь-якого цілого додатного k існує така залежність [13]:

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

Представлені рекурентні послідовності, а також отримані залежності дозволяють запропонувати наступний метод вироблення та перевіряння цифрового підпису на їхній основі.

Суть методу цифрового підписування, що пропонується (заявка на корисну модель № u 2013 06324 від 22.05.2013 р.), 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 того властивість (3) дозволяє реалізувати процедуру обчислення елемента $v_{n \cdot m,k}$. Так само на основі властивості (4) можна реалізувати процедуру обчислення елемента $v_{-n \cdot m,k}$. 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 значення r як $r = (h(M) \cdot x) \bmod p$ за допомогою обраної функції хешування h від повідомлення M. 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 (3), обчислює значення r' як $r' = (h(M) \cdot x') \bmod p$ та перевіряє, чи виконується $r \overset{?}{=} r'$. Якщо так, то підпис приймається, в іншому випадку — відкидається.

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

Виходячи з цього, схема вироблення та перевіряння цифрового підпису за даним методом буде мати вигляд як показано на рисунку.

Операція за модулем у схемі вироблення та перевіряння цифрового підпису використовується для обмеження розрядності чисел під час виконання арифметичних операцій.

Обчислення елемента $v_{b,k} \bmod p$ відправник може виконати попередньо, заздалегідь до безпосереднього формування цифрового підпису з повідомлення M.

У запропонованому методі вироблення та перевіряння цифрового підпису основні обчислення виконуються згідно залежності (3). Обчислення елемента $v_{n+m,k}$ згідно цієї залежності здійснюється на основі елементів $v_{n+i,k}$, $i = \overline{-(k-1), 0}$, та елементів $v_{m+i,k}$, $i = \overline{-1, k-2}$.

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 формул (1) або (2) на основі вже отриманих.

Також у 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 $v_{-m \cdot n,k}$.

Визначивши як можуть отримуватись елементи V_k-послідовності, що використовуються в методі вироблення та перевіряння цифрового підпису, отримаємо такий протокол вироблення та перевіряння цифрового підпису.

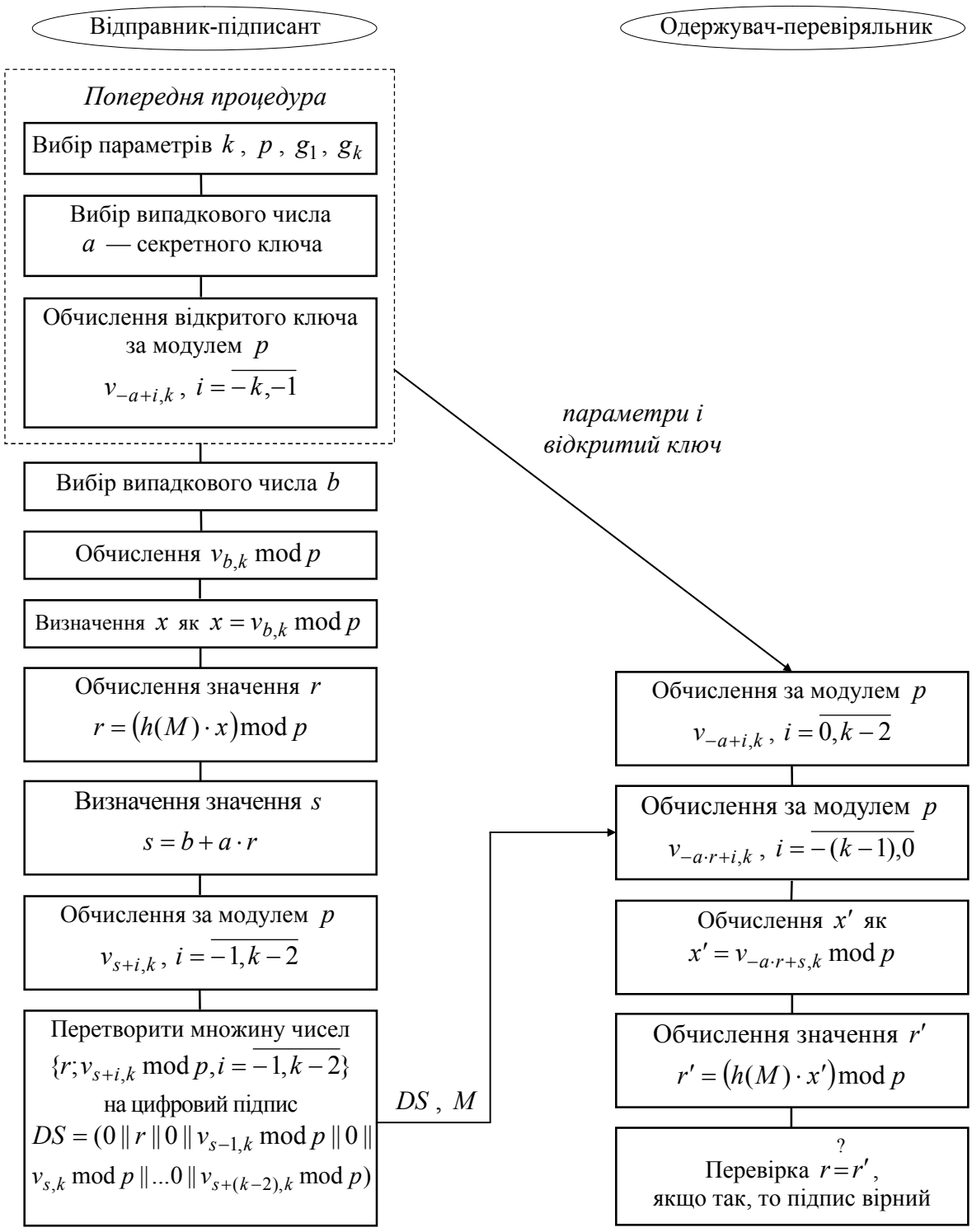

Схема вироблення та перевіряння цифрового підпису на основі елементів V_k-послідовності

П. 1. Задати параметр k.

П. 2. Вибрати p.

П. 3. Вибрати g_1, g_k.

П. 4. Відправнику передати параметри Одержувачу.

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

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

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

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

П. 9. Відправнику вибрати випадкове число b.

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

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

П. 12. Відправнику обчислити значення r як $r = \big(h(M)\cdot x\big) \bmod p$ за допомогою обраної функції хешування h від повідомлення M.

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 із 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 (3).

П. 18. Одержувачу обчислити значення r' як $r' = \big(h(M)\cdot x'\big) \bmod p$.

П. 19. Одержувачу перевірити, чи виконується $r \overset{?}{=} r'$, якщо так, то підпис вважати вірним.

У п. 2 проводиться вибір параметра p, який є модулем при обчисленнях у 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 вироблення та перевіряння цифрового підпису 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 [13].

Так само можна здійснювати обчислення за модулем p елементів $v_{-a+i,k}$, $i = \overline{-k,k-2}$, що виконуються у п. 6 протоколу вироблення та перевіряння цифрового підпису, на основі одного із запропонованих у тій же роботі [13] 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].

Аналіз запропонованого методу вироблення та перевіряння цифрового підпису з використанням рекурентної V_k-послідовності щодо криптографічної стійкості показує, що зловмисник може здійснювати криптоаналіз методу 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.

У роботі [12] показано, що складність отримання зловмисником індексу елемента рекурентної V_k-послідовності, обчисленого за модулем, є принаймні не меншою, ніж отримання числа степеня з результату модулярного піднесення до степеня, тобто ці обчислення знаходяться приблизно на одному ж рівні. Виходячи з цього, запропонований метод цифрового підписування на основі V_k-послідовності криптографічно є більш стійким, ніж відомі аналоги, 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.

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

Аналіз запропонованого методу вироблення та перевіряння цифрового підпису щодо обчислювальної складності показує, що в ньому 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 $v_{-a\cdot r,k}$. Приблизно стільки ж необхідно виконувати піднесень до степеня за модулем і у відомих аналогах.

Оскільки в роботі [13] показано, що складність обчислення елемента V_k-послідовності із заданим індексом має приблизно такий же рівень як і піднесення до заданого степеня того ж порядку, що й індекс, то запропонований метод цифрово-

го підписування на основі V_k-послідовності в цілому має приблизно такий же рівень обчислювальної складності, що й відомі аналоги. При цьому слід відзначити, що розмір цифрового підпису згідно відомих аналогів 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 відомих аналогів шляхом зменшення розміру чисел та елементів послідовності, який в основному визначається параметром p методу, тоді зменшиться і розмір цифрового підпису і, як наслідок, зменшиться і обчислювальна складність запропонованого методу.

Важливою перевагою запропонованого методу є суттєве, майже в два рази, спрощення обчислювальної складності процедури перевіряння підпису, оскільки замість двох піднесень до степеня, як у відомих аналогах, необхідно виконувати лише одне обчислення набору елементів $v_{-a\cdot r,k}$ за прискореним алгоритмом обчислення елементів V_k-послідовності. Це досягається необхідністю при виробленні підпису виконувати три обчислення елементів V_k-послідовності за прискореним алгоритмом, замість двох піднесень до степеня згідно відомих аналогів. Однак, оскільки існує велика кількість задач, в яких перевіряння цифрового підпису необхідно здійснювати значно частіше, ніж його вироблення, і перевіряти підпис від великої кількості його власників, як то в клієнт-серверних задачах, це дає суттєву перевагу запропонованому методу перед відомими аналогами.

Слід також відзначити, 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, як і у відомих аналогах, відправник буде передавати лише саме число-індекс s (заявка на корисну модель № u 2013 06325 від 22.05.2013 р.). Тоді рівень криптографічної стійкості запропонованого методу знизиться приблизно до рівня відомих аналогів, при цьому обчислювальна складність як взагалі методу, так і з боку кожної із сторін, також стане приблизно такого ж рівня, що й відомих аналогів. Однак такий варіант методу не буде забезпечувати можливість прискорення процедури перевіряння підпису.

Висновки

Запропоновано метод вироблення та перевіряння цифрового підпису на основі математичного апарату рекурентних V_k-послідовностей, в якому відбувається заміна піднесення до степеня обчисленням елемента цієї послідовності з певним індексом.

Для запропонованого методу представлено протокол цифрового підписування, а також показано можливості реалізації цього протоколу.

Аналіз запропонованого методу цифрового підписування щодо криптографічної стійкості показав, що метод забезпечує більший рівень стійкості, ніж відомі аналоги. Крім того запропонований метод має значно простішу процедуру завдання параметрів.

Аналіз обчислювальної складності запропонованого методу показав, що він має майже вдвічі простішу процедуру перевіряння підпису порівняно з відомими аналогами, що дозволяє суттєво підвищити швидкодію виконання цієї процедури і є важливою перевагою в клієнт-серверних застосуваннях, де виникає необхідність перевіряти підпис від великої кількості його власників.

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. *Rivest R.L.* A Method for Obtaining Digital Signatures and Public-Key Cryptosystems [Текст] / R.L. Rivest, A. Shamir, L.M. Adleman // Communications of the ACM. — 1978. — Vol. 21. — P. 120–126.

6. *ElGamal T.* A Public-Key Cryptosystcm and a Signature Scheme Based on Discrete Logarithms [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. *Miller V.S.* Use of Elliptic Curves in Cryptography [Текст] / V.S. Miller // Advances in Cryptology Crypto'85. — LNCS 218, 1986. — P. 417–426.

10. *Элементарное* введение в эллиптическую криптографию. Алгебраические и алгоритмические основы [Текст] / [Болотов А.А., Машков С.Б., Фролов А.Б., Часовских А.А.]. — М.: КомКнига, 2006. — 328 с.

11. *Бессалов А.В.* Криптосистемы на эллиптических кривых: учеб. пособ. [Текст] / А.В. Бессалов, А.Б. Телиженко. — К.: ІОЦ «Видавництво «Політехніка», 2004. — 224 с.

12. *Яремчук Ю.Є.* Використання рекурентних послідовностей для побудови криптографічних методів з відкритим ключем [Текст] / Ю.Є. Яремчук // Захист інформації. — 2012. — № 4. — С. 120–127.

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

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

15. *Яремчук Ю.Є.* Метод автентифікації учасників взаємодії на основі рекурентних послідовностей [Текст] / Ю.Є. Яремчук // Реєстрація, зберігання і оброб. даних. — 2013. — Т. 15, № 2. — С. 73–81.

Надійшла до редакції 25.09.2013