УДК 681.3.067

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

Метод автентифікації учасників взаємодії на основі рекурентних послідовностей

Запропоновано метод автентифікації учасників взаємодії на основі рекурентних V_k *-послідовностей та їхніх залежностей. Аналіз криптографічної стійкості та обчислювальної складності показав, що запропонований метод є більш стійким при забезпеченні в цілому приблизно такого ж рівня складності обчислень, що й відомі аналоги. Перевагою запропонованого методу є те, що він забезпечує значне спрощення обчислень процедури перевірки автентичності.*

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

Вступ

Задача забезпечення цілісності на сьогодні є не менш актуальною, ніж забезпечення конфіденційності, і вирішується за допомогою криптографічних протоколів, які бувають двох типів — автентифікації та цифрового підписування [1, 2].

У схемі автентифікації учасників взаємодії [1] існує з одного боку претендент — той, хто повинен довести свою автентичність, а з другого боку — перевіряльник — той, хто цю автентичність повинен перевірити. Претендент має два ключи — загальнодоступний K_1 та секретний K_2. При доведенні автентичності з нульовим розголошенням знання претенденту необхідно довести, що він знає K_2, причому зробити це таким чином, щоб це доведення можна було би перевірити, знаючи лише K_1.

Теоретичні основи схем автентифікації були закладені в роботі Сіммонса [3]. Найбільш відомими методами автентифікації є методи Фейге-Фіата-Шаміра, Гіллоу-Куіскуотера та Шнорра [1, 2]. Дані методи базуються на операції піднесення до степеня, яка вимагає виконання досить складних обчислень, що впливає на швидкість роботи методу при його практичній реалізації.

Загальним недоліком відомих методів автентифікації є те, що в них на певних етапах автентифікації між учасниками взаємодії передаються лише числа, які

представляють собою, скажімо, степені, а не результати піднесення до цих степенів, або результати інших обчислень над цими числами, які би значно ускладнювали зловмиснику його спроби щодо зламу, і цим самим підвищували би стійкість криптографічних перетворень під час автентифікації.

Окрім цього, суттєвим недоліком є те, що у вказаних методах автентифікації необхідно виконувати доволі складні обчислення 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 у задачах, де процедуру перевірки автентичності необхідно здійснювати в реальному часі від великої кількості претендентів. У 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 і в системах стільникового зв'язку, забезпечення веб-трансакцій між клієнтом і сервером, автентифікації у безпровідних мережах, організації банківських трансакцій, організації мобільної комерції, авторизації електронних повідомлень та інші.

У цьому зв'язку певний інтерес викликає апарат на основі рекурентних послідовностей [4, 5], який дозволяє за певних умов спрощувати обчислення під час вирішення криптографічних задач. Так, у роботі [6] представлено метод автентифікації сторін взаємодії, який базується на рекурентних V_k^+- та U_k-послідовностях і який, порівняно з відомим методами, дозволяє суттєво спростити обчислення. Однак представлений метод не задовольняє усім вимогам до протоколів автентифікації, оскільки не дозволяє використовувати претенденту сеансовий ключ. У роботі [7] представлено метод, який задовольняє усім сучасним вимогам щодо забезпечення автентифікації з нульовим розголошенням знання, при цьому він забезпечує ще й підвищення стійкості порівняно з відомими методами автентифікації. Однак запропонований метод не вирішує проблему спрощення обчислень процедури перевірки автентичності.

Виходячи з цього, актуальними є дослідження рекурентних послідовностей щодо розробки такого методу автентифікації, який би забезпечував підвищення стійкості криптографічних перетворень під час автентифікації і при цьому спрощення обчислень процедури перевірки автентичності.

Метод автентифікації на основі рекурентних V_k-послідовностей

У [5] 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 [4]:

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

Для будь-яких цілих додатних n і m, таких що $1\le m<n$ та будь-якого цілого додатного k існує така залежність [5]:

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

Представлені рекурентні послідовності, а також отримані залежності дозволяють розробити метод автентифікації учасників взаємодії на їхній основі.

Суть методу автентифікації, що пропонується (заявка на корисну модель № u 2013 06320 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 автентифікації учасників взаємодії.

Спочатку претендент (або центр довіри) виконує попередню процедуру обчислення ключів. 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 пре-

тендентові, 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.

У цей же час претендент обчислює $v_{b+a\cdot c+i,k}$, $i=\overline{-1,k-2}$, на основі своїх секретного ключа a та сеансового ключа b, а також сеансового ключа c, отриманого від перевіряльника, та передає обчислені елементи перевіряльнику.

Далі перевіряльник використовує отримані елементи для обчислення x' як $x'=v_{-a\cdot c+(b+a\cdot c),k}$ згідно залежності (3) і перевіряє отримане значення зі значенням x, яке він раніше отримав від претендента.

Виходячи з цього схема автентифікації учасників взаємодії за даним методом буде мати вигляд, як показано на рисунку.

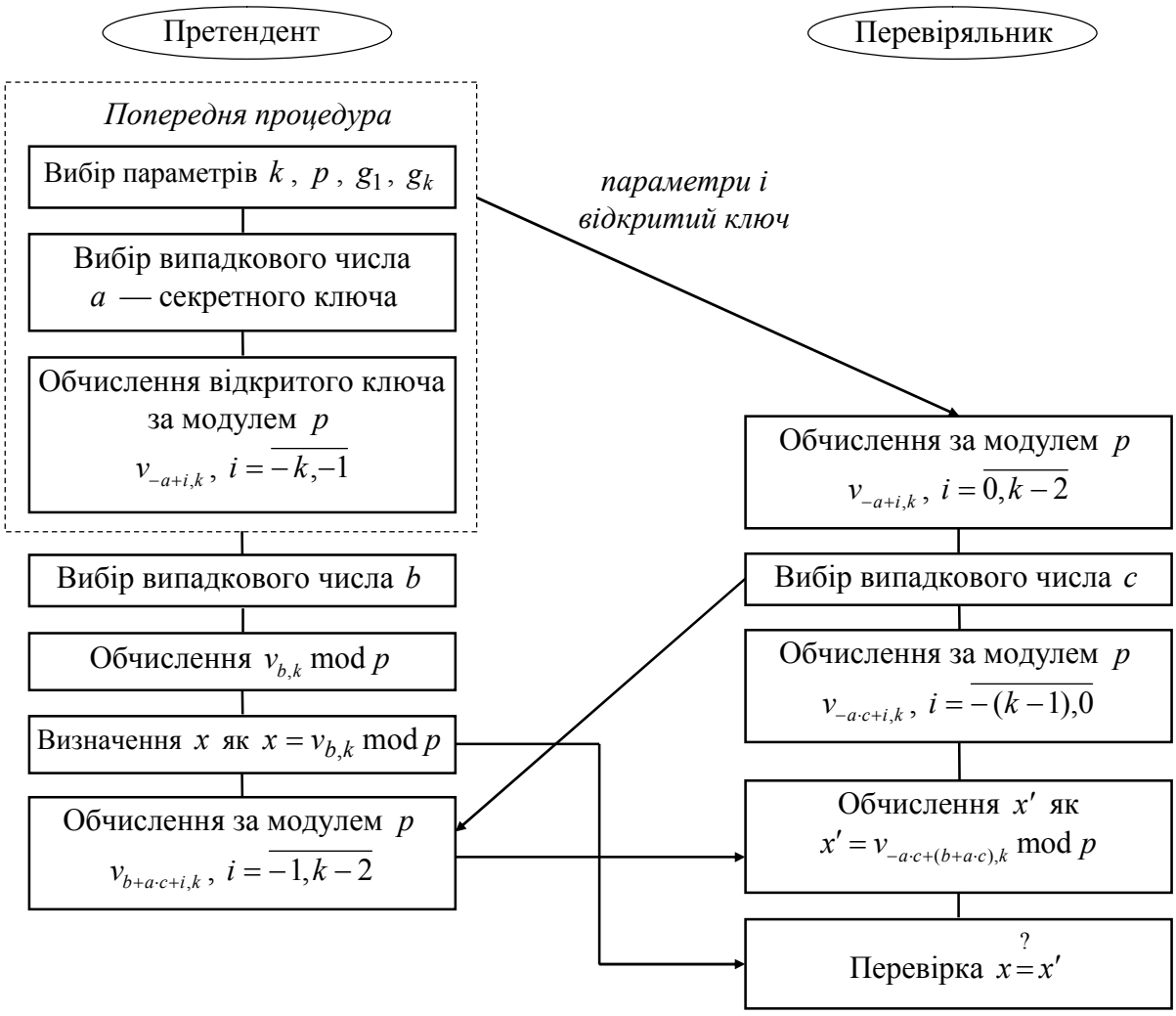

Схема автентифікації учасників взаємодії на основі елементів V_k-послідовності

Операція за модулем у 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 перевіряльник може вибрати число c й обчислити на його основі та відкритого ключа елементи $v_{-a\cdot c+i,k}$, $i = \overline{-(k-1),0}$.

У запропонованому способі автентифікації 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.

Виходячи з вищесказаного, отримаємо такий протокол автентифікації учасників взаємодії 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 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, і передати отримані елементи Перевіряльнику.

П. 13. 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 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 автентифікації необхідно здійснювати обчислення елемента $v_{b,k} \bmod p$, а у п.12 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 представлено в роботі [5].

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 із запропонованих у тій же роботі [5] 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 $v_{-m\cdot n,k}$, представленого в роботі [7].

Здійснювати криптоаналіз запропонованого методу автентифікації учасників 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 $v_{b+a\cdot c+i,k}$, $i = \overline{-1, k-2}$, 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 [4] видно, 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. Враховуючи це, а також те, що кожному набору елементів рекурентних послідовностей, що відомі зловмиснику згідно запропонованого методу, відповідають певні результати піднесення до степеня згідно відомого методу, крім одного випадку, коли замість елементів $v_{b+a\cdot c+i,k}$, $i = \overline{-1, k-2}$, зловмиснику відомий не відповідний результат піднесення до степеня, а саме число $b + a \cdot c (\bmod q)$, можна стверджувати, що за рахунок цього криптографічна стійкість запропонованого методу є вищою, ніж 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 завдання параметрів, оскільки їхній вибір не потребує проведення складних обчислень над великими числами.

У разі необхідності існує можливість ще більшого підвищення стійкості запропонованого методу автентифікації [7], 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.

Проведемо тепер аналіз запропонованого та відомого методів автентифікації щодо обчислювальної складності. Згідно запропонованого методу необхідно чотири рази проводити обчислення елементів V_k-послідовності за прискореним алгоритмом, а саме три рази обчислювати за модулем p різні набори елементів $v_{-a,k}$, $v_{b,k}$ і $v_{b+a\cdot c,k}$ з боку претендента та один раз обчислювати за модулем p набір елементів $v_{-a\cdot c,k}$ з боку перевіряльника. За відомим методом Шнорра необхідно в цілому виконувати стільки ж, чотири, піднесення до степеня за модулем, але ці обчислення між претендентом і перевіряльником розподіляються іншим чином — по два рази на кожному боці — два обчислення $g^{-a} \bmod p$ і $g^b \bmod p$ виконуються з боку претендента, та два обчислення $g^y \bmod p$ і $(g^{-a})^c \bmod p$ виконуються з боку перевіряльника. З [5] видно, 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.

Виходячи з цього, в цілому обчислювальна складність запропонованого методу автентифікації має приблизно такий же рівень складності обчислень, що й відомий метод Шнорра. При цьому згідно запропонованого методу претенденту необхідно буде передавати більшу кількість чисел і виконувати три обчислення елементів V_k-послідовності за прискореним алгоритмом замість двох, як у відомому методі. Однак такий варіант запропонованого методу, окрім підвищеної стійкості (це було показано вище), буде забезпечувати значне спрощення процедури 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. Це дозволяє суттєво спростити процедуру перевірки автентичності порівняно з відомим методом.

Слід також вказати і про такий можливий варіант методу автентифікації, коли запропонований метод може бути дещо спрощений за рахунок зменшення криптостійкості до рівня відомого методу Шнорра, якщо претенденту не обчислювати $v_{(b+c\cdot a)+i,k} \bmod p$, $i = \overline{-1,k-2}$, а передавати перевіряльнику лише саме число $b + c \cdot a$ й обчислення відповідних елементів V_k-послідовності для цього індексу за прискореним алгоритмом здійснювати вже перевіряльнику (заявка на корисну

модель № u 2013 06321 від 22.05.2013 р.). У результаті кількість чисел, що передаються між сторонами автентифікації, стане меншою, при цьому загальна обчислювальна складність методу не зміниться — чотири обчислення елементів V_k-послідовності за прискореним алгоритмом, але тепер претендент і перевіряльник будуть виконувати по два таких обчислення на кожному боці. Тобто такий варіант не дозволить спрощувати обчислення під час перевірки автентичності.

Відомо [2], що будь-який метод автентифікації, який базується на технології відкритого ключа, може бути перетворений на 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 учасників взаємодії на основі математичного апарату рекурентних V_k-послідовностей, в якому відбувається заміна піднесення до степеня обчисленням елемента рекурентної послідовності з певним індексом. Представлено протокол реалізації методу, а також проведено аналіз його криптографічної стійкості та обчислювальної складності порівняно з відомим аналогом.

Аналіз показав, що криптографічна стійкість запропонованого методу автентифікації є вищою, ніж відомого аналогу, а обчислювальна складність запропонованого методу в цілому має приблизно такий же рівень складності обчислень, що й відомого аналогу. При цьому запропонований метод за рахунок необхідності претенденту передавати дещо більшу кількість чисел і виконувати три обчислення елементів V_k-послідовності за прискореним алгоритмом, замість двох як у відомому методі, досягається можливість в цілому майже вдвічі зменшити обчислювальну складність процедури перевірки автентичності, звести до мінімуму обчислювальну складність цієї процедури під час безпосередньої автентифікації, уникнувши взагалі в ній необхідності виконання складних обчислень елементів рекурентної послідовності. Як наслідок, це дозволило суттєво збільшити швидкість процедури перевірки автентичності як під час безпосередньої автентифікації, так і перевірку в цілому.

Окрім цього, запропонований метод автентифікації забезпечує 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.

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. *Simmons G.J.* Authentication Theory/Coding Theory / G.J. Simmons // Proc. CRYPTO'84, Lect. Notes in Comput. Sci. — 1985. — Vol. 196. — P. 411–431.

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

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

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

7. *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.

Надійшла до редакції 03.06.2013