УДК 621.391.7

Ю.Є. Яремчук[1]

[1]к.т.н., доцент, директор Центру інформаційних технологій і захисту інформації, професор кафедри менеджменту та безпеки інформаційних систем Вінницького національного технічного університету

МЕТОД ВІДКРИТОГО РОЗПОДІЛУ СЕКРЕТНИХ КЛЮЧІВНА ОСНОВІ РЕКУРЕНТНИХ ПОСЛІДОВНОСТЕЙ

Запропоновано метод відкритого розподілу секретних ключів, що базується на математичному апараті рекурентних V_k^+ –послідовностей. Проведено аналіз обчислювальної складності та криптографічної стійкості, який показав, що у порівнянні з відомими аналогами за певних умов запропонований метод забезпечує підвищення стійкості розподілу ключів.

Ключові слова: захист інформації, криптографія, розподіл секретних ключів, рекурентні послідовності.

Вступ

Розподіл ключів - одна з найважливіших криптографічних задач [1, 2]. На сьогодні ця задача може вирішуватись різними шляхами: передаванням вже згенерованих ключів, спільного вироблення загального ключа (відкритий розподіл ключів), а також попереднього розподілу ключів [1]. При цьому розподіл ключів може здійснюватись при безпосередній взаємодії лише двох сторін (типу «точка-точка»), так і централізовано з використанням третьої сторони, що відіграє роль довіреного центру.

Відкритий розподіл ключів дозволяє двом сторонам виробляти спільний секретний ключ шляхом динамічної взаємодії на основі обміну відкритими повідомленнями без якоїсь спільної секретної інформації, що виробляється заздалегідь. Важливою перевагою відкритого розподілу є те, що жоден з абонентів заздалегідь не може визначити значення ключа, так як ключ залежить від повідомлень, що передаються в процесі обміну.

Вперше метод відкритого розподілу секретних ключів був запропонований Діффі та Хеллманом [3]. Криптостійкість методу Діффі-Хеллмана базується на складності обчислення дискретних логарифмів, і хоч ця задача вважається на сьогодні важковирішуваною, однак можливість її вирішення досліджується доволі активно, тому пошук надійних методів відкритого розподілу секретних ключів залишається актуальним.

В роботі [4] показано можливість побудови методу Діффі-Хеллмана на основі математичного апарату еліптичних кривих, який використовує менші довжини ключів та загальносистемні параметри, і цим самим підвищує швидкість криптографічних перетворень під час розподілу ключів при забезпеченні високої обчислювальної складності цих перетворень з боку зловмисника. Незважаючи на це, слід відзначити й на наявність достатньої кількості атак на криптографічні методи, що базуються на еліптичних кривих, більшість з яких розглянуто в [5].

В роботі [6] запропоновано метод LUCDIF, який є аналогом методу Діффі-Хеллмана і використовує в своїй основі рекурентні послідовності Люка за модулем простого числа p замість модулярного піднесення до степеня. Пізніше в роботі [7] було

показано, що функції Люка, які є аналогом проблеми дискретного логарифмування, послаблюють проблему дискретного логарифмування, а сам метод не володіє якимось суттєвими перевагами в порівнянні з оригінальним методом.

В роботі [8] представлено метод відкритого розподілу секретних ключів, який базується на використанні рекурентних V_k^+ та U_k –послідовностей. У порівнянні з відомим методом розподілу ключів Діффі-Хеллмана, запропонований метод майже вдвічі спрощує обчислення, а також дозволяє встановлювати необхідний рівень криптографічної стійкості залежно від порядку послідовності k.

Однак, аналіз запропонованого в [8] методу показує, що в ньому отримання спільного ключа на завершальному етапі розподілу здійснюється за допомогою аналітичної залежності обчислення елементу послідовності з адитивною, а не мультиплікативною зміною індексу, а це могло б значно підвищити стійкість криптографічних перетворень під час розподілу ключів, оскільки отримання зловмисником складових частин індексу елемента послідовності обчисленого таким чином є більш складним, ніж отримання складових індексу елемента послідовності обчисленого за адитивним способом зміни індексу.

Виходячи з цього, актуальними є дослідження такої можливості підвищення стійкості криптографічних перетворень під час розподілу ключів для розробки методу відкритого розподілу секретних ключів підвищеної стійкості.

Метод відкритого розподілу секретних ключів на основі рекурентних V_k^+ –послідовностей

Для побудови методу розподілу секретних ключів підвищеної стійкості пропонується використовувати математичний апарат тільки на основі рекурентних V_k^+ –послідовностей, що дасть можливість користувачам на завершальному етапі розподілу ключів обчислювати спільний ключ як результат обчислень елементу цієї послідовності за мультиплікативним способом зміни індексу.

V_k^+ –послідовністю [8] 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

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

Для будь-яких цілих додатних n, m та k отримано таку аналітичну залежність [9]

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

Суть методу відкритого розподілу секретних ключів, що пропонується (заявка на корисну модель № u 2013 08385 від 04.07.2013 р.), базується на використанні властивості (3) V_k^+ –послідовності, яка забезпечує можливість реалізувати процедури прискореного обчислення елементів V_k^+ –послідовності для великих значень індексів, а саме процедури прискореного обчислення елементів $v_{n,k}$ та $v_{n\cdot m,k}$.

Спочатку центр довіри (або користувач A чи користувач B) вибирає і відкрито публікує ціле додатне число p ($p > 2$) та цілі числа g_1, g_k.

Під час безпосереднього розподілу ключів користувач A вибирає випадкове число a, $1 < a < p$, а користувач B вибирає випадкове число b, $1 < b < p$. Потім користувач A обчислює за модулем p $v_{a+i,k}$, $i = \overline{-(k-1),0}$, а користувач B – за модулем p $v_{b+i,k}$, $i = \overline{-(k-1),0}$, після чого вони обмінюються обчисленими значеннями. Далі користувачі A і B розширюють отриманий один від одного набір елементів, використовуючи формулу (1), обчислюючи за модулем p відповідно набори елементів $v_{b+i,k}$, $i = \overline{1,k-1}$, та $v_{a+i,k}$, $i = \overline{1,k-1}$. Після цього вони обчислюють спільний ключ K відповідно як $K = v_{b\cdot a,k} \bmod p$ та $K = v_{a\cdot b,k} \bmod p$, використовуючи свої секретні числа a і b.

Виходячи з цього схема відкритого розподілу секретних ключів за даним методом буде мати вигляд представлений на рис. 1.

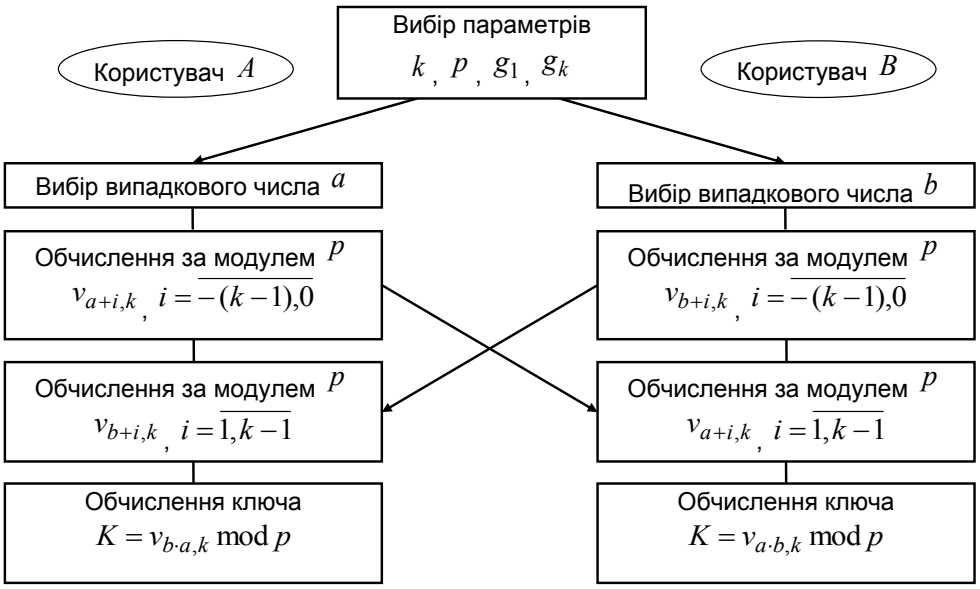

Рис. 1. Схема відкритого розподілу секретних ключів на основі елементів V_k^+ –послідовності.

Операція за модулем в схемі відкритого розподілу секретних ключів використовується для обмеження розрядності чисел під час виконання арифметичних операцій.

Користувачі можуть вибирати числа a і b та обчислювати за модулем p елементи $v_{a+i,k}$ і $v_{b+i,k}$ для $i=\overline{-(k-1),0}$ попередньо, заздалегідь до безпосереднього розподілу секретних ключів.

В запропонованому методі розподілу секретних ключів основні обчислення виконуються згідно залежності (3). 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 (1) або (2) на основі вже отриманих.

Протокол розподілу секретних ключів згідно запропонованого методу буде мати такий вигляд.

Крок 1. Задати параметр k.

Крок 2. Вибрати p, $p>2$.

Крок 3. Вибрати g_1, g_k.

Крок 4. Опублікувати параметри.

Крок 5. Користувачу A вибрати випадкове число a, $1<a<p$, а користувачу B вибрати випадкове число b, $1<b<p$.

Крок 6. Користувачу A обчислити за модулем p $v_{a+i,k}$, $i=\overline{-(k-1),0}$, а користувачу B обчислити за модулем p $v_{b+i,k}$, $i=\overline{-(k-1),0}$, використовуючи спосіб прискореного обчислення елементів $v_{n,k}$ для додатних значень n, після чого передати один одному обчислені елементи.

Крок 7. Користувачу A обчислити за модулем p $v_{b+i,k}$, $i=\overline{1,k-1}$, а користувачу B обчислити за модулем p $v_{a+i,k}$, $i=\overline{1,k-1}$, використовуючи формулу (1).

Крок 8. Користувачам A і B обчислити спільний ключ K відповідно як $K=v_{b\cdot a,k} \bmod p$ та $K=v_{a\cdot b,k} \bmod p$, використовуючи спосіб прискореного обчислення елементів $v_{n\cdot m,k}$.

У п.2 проводиться вибір параметру p, який є модулем при обчисленнях в 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.6 протоколу розподілу ключів користувачам необхідно здійснювати обчислення за модулем p елементів $v_{a+i,k}$ і $v_{b+i,k}$ для $i = \overline{-(k-1),0}$, коли індекси цих елементів приймають великі значення. Ці обчислення можна здійснювати за одним з алгоритмів прискореного обчислення елементів $v_{n,k}$ для додатних n, які представлено в роботі [9].

У п.8 протоколу користувачам необхідно здійснювати обчислення за модулем p елементів $v_{b\cdot a,k}$ та $v_{a\cdot b,k}$ для великих значень індексів. Для цього можна використати алгоритм прискореного обчислення елементів $v_{m\cdot n,k}$, який представлено в роботі [10].

Аналіз запропонованого методу та відомого методу Діффі-Хеллмана щодо обчислювальної складності показує, що згідно запропонованого методу необхідно по два рази на кожному боці проводити за прискореними алгоритмами обчислення елементів V_k^+–послідовності для великих значень індексів, а саме обчислення за модулем p елементів $v_{a,k}$ ($v_{b,k}$) та $v_{b\cdot a,k}$ ($v_{a\cdot b,k}$). За відомим методом Діффі-Хеллмана необхідно виконувати так само, по два рази на кожному боці, обчислення за модулем n: g^a (g^b) та $g^{b\cdot a}$ ($g^{a\cdot b}$). З [9] видно, що складність обчислення елементу 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 відкритого розподілу секретних ключів має приблизно такий же рівень складності обчислень, що й відомий метод Діффі-Хеллмана.

Проведемо тепер аналіз цих методів щодо криптографічної стійкості. Здійснювати криптоаналіз запропонованого методу розподілу ключів на основі V_k^+–послідовності зловмисник може на основі відомих параметрів k, p, g_1, g_k, а також елементів $v_{a+i,k} \bmod p$ та $v_{b+i,k} \bmod p$ для $i = \overline{-(k-1),0}$, які передаються між користувачами. Приблизно так само у відомому методі Діффі-Хеллмана зловмиснику відомі параметри n, g, а також $g^a \bmod n$ та $g^b \bmod n$, що передаються між користувачами. З [8] 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, можна стверджувати, що криптографічна стійкість запропонованого методу знаходиться приблизно на тому ж рівні, принаймні є не меншою, ніж відомого методу Діффі-Хеллмана.

Однак перевагою запропонованого методу розподілу ключів на основі рекурентної V_k^+–послідовності перед методом Діффі-Хеллмана щодо стійкості є можливість змінювати параметр k, що, в свою чергу, дає можливість підвищувати криптостійкість за рахунок збільшення складності виконання протоколу розподілу ключів.

Порівнюючи запропонований метод розподілу ключів на основі V_k^+ –послідовності з методом розподілу ключів на основі V_k^+ та U_k –послідовностей, представленого в роботі [8], слід відзначити, що хоча запропонований метод на основі V_k^+ –послідовності і має вищу складність обчислень, однак при цьому він забезпечує і вищу криптографічну стійкість розподілу ключів, оскільки на завершальному етапі розподілу ключів спільний ключ обчислюється як результат обчислень елементу $v_{n\cdot m,k}$ V_k^+ –послідовності, тобто за мультиплікативним способом зміни індексу, а не за адитивним способом зміни індексу при обчисленні елементу $u_{n+m,k}$ U_k –послідовності, як це робиться згідно методу представленого в роботі [8].

Висновки

На основі математичного апарату рекурентних V_k^+ –послідовностей запропоновано метод відкритого розподілу секретних ключів, в якому відбувається заміна піднесення до степеня обчисленням елементу рекурентної послідовності з певним індексом. Представлено протокол реалізації методу, а також проведено аналіз його обчислювальної складності та криптографічної стійкості у порівнянні з відомими аналогами.

Аналіз показав, що в цілому криптографічна стійкість і обчислювальна складність запропонованого методу знаходяться приблизно на тому ж рівні, що і відомого методу Діффі-Хеллмана, однак у порівнянні з відомими аналогами запропонований метод за певних умов дозволяє підвищувати стійкість криптографічних перетворень підчас розподілу ключів. Крім того, запропонований метод дозволяє змінювати стійкість методу залежно від параметру k –порядку послідовності.

Література

1. Основы криптографии / А. П. Алферов, А. Ю. Зубов, А. С. Кузьмин, А. В. Черемушкин. – М: Гелиос АРВ, 2002. – 480 с.
2. Н.Смарт. Криптография. – М.: Техносфера, 2005. – 528 с.
3. W. Diffie, M.E. Hellman. New directions in cryptography // IEEE Transactions on Information Theory. – №22, 1976. – Pp. 644–654.
4. Smart N. The Discrete Problem on Elliptic Curves of Trace One. Journal of Cryptology, 12. – 1999. – Pp. 29–34.
5. Ростовцев А.Г., Маховенко Е.Б. Подпись и шифрование на эллиптической кривой: анализ безопасности и безопасная реализация // Проблемы информационной безопасности. Компьютерные системы, СПб. – №1, 2003. – С. 64–73.
6. Smith P. and Skinner C. A public-key cryptosystem and a digital signature system based on the Lucas function analogue to discrete logarithms // In Advances in Cryptology Asiacrypt '94, Springer-Verlag. – 1995. – Pp. 357–364.
7. Bleichenbacher D., Bosma W., and Lenstra A. Some remarks on Lucas-based cryptosystems // In Advances in Cryptology Crypto '95, Springer-Verlag. – 1995. – Pp.386–396.
8. Яремчук Ю.Є. Використання рекурентних послідовностей для побудови криптографічних методів з відкритим ключем // Захист інформації. – №4, 2012. – С. 120–127.
9. Яремчук Ю.Є. Розробка алгоритмів прискореного обчислення елементів рекурентних послідовностей для криптографічних застосувань // Реєстрація, зберігання і обробка даних. – Т. 15, №1, 2013. – С. 14–22.
10. Яремчук Ю.Є. Методи автентифікації на основі рекурентних послідовностей // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – Випуск 1(25), 2013. – С. 39–48.

Надійшла до редколегії 19.04.2013 р.

Рецензент: д.т.н., проф. Пархуць Л.Т.

Яремчук Ю.Є.

МЕТОД ОТКРЫТОГО РАСПРЕДЕЛЕНИЯ СЕКРЕТНЫХ КЛЮЧЕЙ НА ОСНОВЕ РЕКУРРЕНТНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ

Предложен метод открытого распределения секретных ключей, который основывается на математическом аппарате рекуррентных V_k^+ –последовательностей. Проведен анализ вычислительной сложности и криптографической стойкости, который показал, что по сравнению с известными аналогами при определённых условиях предложенный метод обеспечивает повышение стойкости распределения ключей.

Ключевые слова: защита информации, криптография, распределение секретных ключей, рекуррентные последовательности.

Yaremchuk Yu.

METHOD OF PUBLIC DISTRIBUTION OF SECRET KEYS BASED ON RECURRENT SEQUENCES

We have suggested a method of public distribution of secret keys based on the mathematical apparatus of recurrent V_k^+ sequences. We have conducted an analysis of computational complexity and cryptography reliability, which shows that compared with the known counterparts under certain conditions the proposed method enhances the reliability of key distribution.

Keywords: information security, cryptography, distribution of secret keys, recurrent sequences.