4. Сосулин Ю.Г. Теория обнаружения и оценивания стохастических сигналов / Ю.Г. Сосулин. – М.: Сов. радио, 1978. – 320 с.

5. Левин Б.Р. Теоретические основы статистической радиотехники / Б.Р. Левин. – М.: Радио и связь, 1989. – 656 с. Теория обнаружения сигналов / [П.С. Акимов, П.А. Бакут, В.А. Богданович и др.] ; под ред. П.А. Бакута. – М.: Радио и связь, 1984. – 440 с.

6. Тихонов В.И. Статистический анализ и синтез радиотехнических устройств и систем / В.И. Тихонов, В.Н. Харисов. – М.: Радио и связь, 1991. – 608 с.

7. Шеннон К. Математическая теория связи // В кн. «Работы по теории информации и кибернетике». – С. 243-332. / К. Шеннон. – М.: ИИЛ, 1963. – 832 с.

8. Попов А.А. Информационные соотношения между элементами пространства сигналов, построенного на обобщенной булевой алгебре с мерой / А.А. Попов // Вісник Державного університету інформаційно-комунікаційних технологій. – 2007. – Т.5, № 2. – С.175-184.

9. Попов А.А. Вероятностно-статистические и информационные характеристики случайных процессов, инвариантные относительно группы взаимнооднозначных функциональных преобразований / А.А. Попов // Вісник Державного університету інформаційно-комунікаційних технологій. – 2007. – Т.5, № 1. – С. 52-62.

10. Попов А.А. Мера количества информации в пространстве сигналов, построенном на обобщенной булевой алгебре с мерой / А.А. Попов // Вісник Державного університету інформаційно-комунікаційних технологій. – 2007. – Т.5, № 3. – С.253-261.

11. Сикорский Р. Булевы алгебры / Р. Сикорский. – М.: Мир, 1969. – 376 с.

12. Общая алгебра. Т. 2 / [В.А. Артамонов, В.Н. Салий, Л.А. Скорняков и др.]; под общ. ред. Л.А. Скорнякова. – М.: Наука, 1991. – 480 с.

13. Биркгоф Г. Теория решеток / Г. Биркгоф. – М.: Наука, 1984. – 568 с.

14. Скляр Б. Цифровая связь. Теоретические основы и практическое применение / Б. Скляр. – М.: Издательский дом «Вильямс», 2003. – 1104 с.

15. Попов А.А. Инварианты групп отображений мгновенных значений случайных сигналов в метрическом пространстве со свойствами *L*-группы / А.А. Попов // Вісник Державного університету інформаційно-комунікаційних технологій. – 2013. – № 1. – С.28-38.

17. Харкевич А.А. Борьба с помехами / А.А. Харкевич. – М.: Наука, 1965. – 276 с.

УДК 681.3.067

Яремчук Ю.Є., к.т.н. (*Вінницький національний технічний університет)*

ОЦІНЮВАННЯ ОБЧИСЛЮВАЛЬНОЇ СКЛАДНОСТІ ПРОТОКОЛІВ ШИФРУВАННЯ БЕЗ ПОПЕРЕДНЬОГО РОЗПОДІЛУ КЛЮЧІВ НА ОСНОВІ РЕКУРЕНТНИХ ПОСЛІДОВНОСТЕЙ

Яремчук Ю.Є. Оцінювання обчислювальної складності протоколів шифрування без попереднього розподілу ключів на основі рекурентних послідовностей. В даній роботі проведено оцінювання обчислювальної складності протоколу шифрування інформації без попереднього розподілу ключів на основі V_k- та U_k-послідовностей і отримано його мінімальні та максимальні оцінки складності. Проведено порівняння отриманих оцінок з оцінками складності відомого протоколу шифрування без попереднього розподілу ключів Шаміра. Результати порівняння показали, що протокол шифрування на основі рекурентних послідовностей має меншу складність обчислень для будь-якого k, причому не менше ніж у 100 разів і при цьому забезпечує достатній рівень криптостійкості.

Ключові слова: ЗАХИСТ ІНФОРМАЦІЇ, КРИПТОГРАФІЯ, ШИФРУВАННЯ, РОЗПОДІЛ КЛЮЧІВ, ОБЧИСЛЮВАЛЬНА СКЛАДНІСТЬ АЛГОРИТМІВ, РЕКУРЕНТНІ ПОСЛІДОВНОСТІ

Яремчук Ю.Е. Оценивание вычислительной сложности протоколов шифрования без предварительного распределения ключей на основе рекуррентных последовательностей. В данной работе

проведено оценивание вычислительной сложности протокола шифрования информации без предварительного распределения ключей на основе V_k- и U_k-последовательностей и получены его минимальные и максимальные оценки сложности. Проведено сравнение полученных оценок с оценками сложности известного протокола шифрования без предварительного распределения ключей Шамира. Результаты сравнения показали, что протокол шифрования на основе рекуррентных последовательностей имеет меньшую сложность вычислений для любого k, причём не меньше, чем в 100 раз и при этом обеспечивает достаточный уровень криптостойкости.

Ключевые слова: ЗАЩИТА ИНФОРМАЦИИ, КРИПТОГРАФИЯ, ШИФРОВАНИЕ, РАСПРЕДЕЛЕНИЕ КЛЮЧЕЙ, ВЫЧИСЛИТЕЛЬНАЯ СЛОЖНОСТЬ АЛГОРИТМОВ, РЕКУРРЕНТНЫЕ ПОСЛЕДОВАТЕЛЬНОСТИ

Iaremchuk Iu.Ie. Evaluation of computational complexity of encryption protocols without prior key distribution based on recurrent sequences. This paper evaluated computational complexity of encryption protocol without prior keys distribution based on V_k- and U_k-sequences, and obtained its minimum and maximum complexity values. We conducted a comparison of these estimates with the estimates of the known Shamir encryption protocol without prior key distribution. The results of the comparison showed that the encryption protocol based on recurrent sequences has a lower computational complexity for any k, not less than 100 times, while providing an adequate level of reliability.

Keywords: information security, cryptography, encryption, key distribution, computational complexity of algorithms, recurrent sequences.

Вступ. В роботі [1] розглянуто метод шифрування інформації без попереднього розподілу ключів на основі рекурентних V_k- і U_k-послідовностей та їх аналітичних залежностей, особливістю якого є заміна піднесення до степеня обчисленням певного елементу U_k-послідовності. Метод має забезпечувати значне спрощення обчислень у порівнянні з відомим методом Шаміра [2] при забезпеченні достатнього рівня криптостійкості. При цьому актуальним стає отримання оцінок обчислювальної складності запропонованого методу та їх порівняння з відповідними оцінками відомого аналога.

V_k-послідовністю називається послідовність чисел, яка складається з V_k^+-послідовності та V_k^--послідовності [1].

V_k^+–послідовністю називається послідовність чисел, що обчислюються за формулою

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

для початкових значень $v_{0,k} = 1$, $v_{1,k} = g_2$ для $k = 2$; $v_{0,k} = v_{1,k} = \ldots = v_{k-3,k} = 0$, $v_{k-2,k} = 1$, $v_{k-1,k} = g_k$ для $k > 2$; 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: $$v_{n,k} = \frac{v_{n+k,k} - g_k \cdot v_{n+k-1,k}}{g_1}. \qquad \textbf{(2)}$$

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

U_k-послідовністю [3] називається послідовність чисел, що обчислюються за формулою

$$u_{n,k} = g_k u_{n-1,k} + g_1 u_{n-k,k} \qquad \textbf{(3)}$$

для початкових значень $u_{0,k} = g_1$, $u_{1,k} = g_2$, $u_{2,k} = g_3$, ... $u_{k-1,k} = g_k$; g_1, g_2, g_3, ... , g_k – цілі числа; n і k – цілі додатні числа.

Для будь-яких цілих додатних n, m та k [3]

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

Для будь-яких цілих додатних n та k, таких що $n \geq k$, в [3] представлено залежність, яка дозволяє обчислювати елементи U_k-послідовності тільки на основі елементів V_k^+ - послідовності

$$u_{n,k} = g_k \cdot v_{n-1,k} + g_1 \cdot \sum_{i=1}^{k-1} g_i \cdot v_{n-i-1,k} \cdot \quad \textbf{(5)}$$

Виходячи з формули (3) вираз для обчислення елементів $u_{n,k}$ для спадних n, починаючи з деякого $n = l$, має такий вигляд:

$$u_{n,k} = \frac{u_{n+k,k} - g_k u_{n+k-1,k}}{g_1}. \quad \textbf{(6)}$$

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

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

На основі даного математичного апарату запропоновано метод шифрування інформації без попереднього розподілу ключів [1]. При цьому актуальним залишається отримання оцінок обчислювальної складності протоколів, що реалізують запропонований метод, для можливості порівняння з відомим протоколом.

В даній роботі проводиться оцінювання обчислювальної складності протоколу шифрування інформації на основі V_k - та U_k-послідовностей, а також відомого протоколу та порівняння їх між собою.

Оцінювання обчислювальної складності протоколів шифрування без попереднього розподілу ключів. Згідно [1] шифрування інформації без попереднього розподілу ключів здійснюється за рахунок послідовного використання спочатку аналітичної залежності (4) обчислення елементу $u_{n+m,k}$, а потім залежності (7) обчислення елементу $u_{n-m,k}$. На основі цього було запропоновано метод шифрування інформації без попереднього розподілу ключів, а також протокол його реалізації, який має такий вигляд.

П.1. Задати параметр k.

П.2. Вибрати p.

П.3. Вибрати $g_1, g_2, \ldots, g_k$.

П.4. Опублікувати параметри.

П.5. Передавачу вибрати випадкове число a, а Приймачу вибрати випадкове число b.

П.6. Передавачу обчислити $v_{a+i,k}$ за модулем p, а Приймачу обчислити $v_{b+i,k}$ за модулем p для $i = \overline{-(k-1),k-2}$, використовуючи алгоритм прискореного обчислення елементів $v_{n,k}$ для додатних значень n.

П.7. Передавачу обчислити $v_{a+i,k}$, $i = \overline{-2k+1,-k}$, за модулем p, а Приймачу обчислити $v_{b-k,k}$ за модулем p, використовуючи формулу (2).

П.8. Передавачу обчислити $v_{-a+i,k}$ за модулем p, а Приймачу обчислити $v_{-b+i,k}$ за модулем p для $i = \overline{-k,k-2}$, використовуючи алгоритм прискореного обчислення елементів $v_{n,k}$ для від'ємних значень n.

П.9. Передавачу обчислити $u_{a-i,k}$, $i = \overline{0,k-1}$, за модулем p, використовуючи (5).

П.10. Передавачу обчислити $y_i' = M \cdot u_{a-i} \bmod p$, $i = \overline{0,k-1}$.

П.11. Передавачу передати y_i', $i = \overline{0,k-1}$ Приймачу.

П.12. Приймачу обчислити y_i'', $i = \overline{0,k-1}$ за модулем p, використовуючи (4).

П.13. Приймачу передати y_i'', $i = \overline{0,k-1}$ Передавачу.

П.14. Передавачу обчислити y_i''', $i=\overline{0,k-1}$ за модулем p, використовуючи (7).

П.15. Передавачу передати y_i''', $i=\overline{0,k-1}$ Приймачу.

П.16. Приймачу дешифрувати повідомлення M за формулою

$$M=\frac{y^{IV}}{u_{0,k}}\bmod p=(y^{IV}\cdot g_1^{-1})\bmod p,$$

де y^{IV} обчислюється за модулем p за формулою (7), використовуючи дані отримані ним в п. 8 та дані, що передав Передавач у п.15.

Визначимо тепер обчислювальну складність представленого протоколу шифрування без попереднього розподілу ключів. Складність N протоколу складається з $N^{ПРД}$ та $N^{ПРМ}$ – складностей виконання операцій відповідно Передавачем та Приймачем. Тобто

$$N=N^{ПРД}+N^{ПРМ}.$$

Передавач основні обчислення проводить в пп. 6–10, 14, а Приймач в пп. 6–8, 12, 16. Складність обчислення елементів в п.6 з боку Передавача, як і з боку Приймача визначається N_{V+}. Так само, для кожного, складність обчислення елементів в п.8 визначається складністю N_{V-} прискореного обчислення елементів $v_{n+i,k}$ для $i=\overline{-k,k-2}$, для від'ємних значень n. Виходячи з цього

$$N^{ПРД}=N_{V+}+N_{V-}+N_{дод}^{ПРД}+N_{від}^{ПРД}+N_{мн}^{ПРД}, \qquad \textbf{(8)}$$

де $N_{дод}^{ПРД}$, $N_{від}^{ПРД}$, $N_{мн}^{ПРД}$ – кількість операцій додавання, віднімання та множення відповідно, які виконує Передавач в пп. 7, 9, 10, 14;

$$N^{ПРМ}=N_{V+}+N_{V-}+N_{дод}^{ПРМ}+N_{від}^{ПРМ}+N_{мн}^{ПРМ}, \qquad \textbf{(9)}$$

де $N_{дод}^{ПРМ}$, $N_{від}^{ПРМ}$, $N_{мн}^{ПРМ}$ – кількість операцій додавання, віднімання та множення відповідно, які виконує Приймач в пп. 7, 12, 16.

Визначимо складність виконання операцій кожного вказаного пункту.

В п.7 Передавач обчислює k елементів, а Приймач один елемент за формулою (2). Тобто в цьому пункті Передавач виконує $2k$ множень та k віднімань, а Приймач виконує два множення та одне віднімання.

В п.9 Передавач обчислює k елементів за формулою (5), тобто виконує $k(k+1)$ множень та $k(k-1)$ додавань.

В п.10 Передавач здійснює об'єднання відкритого повідомлення M з елементами U_k –послідовності. При цьому k елементів об'єднуються з M за допомогою операції множення, тобто всього тут виконується k множень.

В п.12 Приймач обчислює k елементів за формулою (4), тобто виконує k^2+k множень та k^2-k додавань.

В п.14 Передавач обчислює k елементів за формулою (7), яка, в свою чергу, потребує для обчислення одного елементу виконання $k+1$ множень та $k-1$ додавань. Тоді всього в п.14 виконується $k(k+1)$ множень та $k(k-1)$ додавань.

В п.16 Приймач обчислює один елемент за формулою (7) та виконує одну операцію множення при дешифруванні, тобто виконує всього $k+2$ множення та $k-1$ додавань.

Зазначимо, що оскільки повідомлення M зазвичай розбивають на певну кількість Q частин M_1, M_2, ... , M_Q фіксованого розміру, кожна з яких шифрується окремо, то пп.10, 14 з боку Передавача та пп. 12, 16 з боку Приймача будуть виконуватись Q разів. Відповідно кількість операцій в указаних пунктах буде теж збільшена в Q разів.

Враховуючи це, отримаємо: $N_{дод}^{ПРД}=Q(k^2-k)+k^2-k$, **(10)** $N_{від}^{ПРД}=k$, **(11)**

$$N_{мн}^{ПРД} = Q(k^2+2k)+k^2+3k, \quad \textbf{(12)} \qquad N_{дод}^{ПРМ} = Q(k^2-1), \quad \textbf{(13)}$$

$$N_{від}^{ПРМ} = 1, \quad \textbf{(14)} \qquad N_{мн}^{ПРМ} = Q(k^2+2k+2)+2. \quad \textbf{(15)}$$

Таким чином отримано оцінки складності протоколу шифрування без попереднього розподілу ключів як з боку Передавача згідно оцінки (8), так і з боку Приймача згідно оцінки (9) з врахуванням кожної арифметичної операції з великими числами, що використовуються в протоколі. Оскільки кожна така операція має різну складність виконання, отримані результати ще не дають можливості провести порівняльний аналіз розглянутого протоколу з відомим. Відкритим також залишається питання визначення оцінки N_{V+} прискореного обчислення елементів $v_{n+i,k}$ для $i = \overline{-(k-1),k-2}$, для додатних значень n, а також оцінки N_{V-} прискореного обчислення елементів $v_{n+i,k}$ для $i = \overline{-k,k-2}$ для від'ємних значень n.

В роботі [4] представлено алгоритми прискореного обчислення елементів V_k–послідовності як для додатних так і для від'ємних значень n. Причому для кожного випадку розглянуто по два можливих варіанти алгоритмів - на основі бінарного методу з використанням адитивного ланцюжка та на основі методу з розкладанням індексу елементу послідовності, що забезпечило спрощення обчислень за рахунок зберігання проміжних результатів попередніх обчислень в пам'яті.

Крім того, згідно [5] проведено оцінювання складності обчислень таких алгоритмів виконання арифметичних операцій над числами великої розрядності як цілочисельне додавання, віднімання та операції за модулем додавання, віднімання, обчислення мультиплікативно оберненої величини, лишку Монтгомері та множення за Монтгомері. З метою прискорення криптографічних перетворень усі ці алгоритми реалізовані на низькому програмному рівні.

В результаті оцінювання алгоритмів виконання операцій над числами великої розрядності встановлено, що оцінки складності операцій додавання та віднімання великих чисел за модулем на рівні машинних одиниць інформації збігаються і становлять кожна $3(H+2)$ операцій, де H – кількість машинних одиниць інформації для зберігання великого числа. В результаті оцінювання також визначено, що складність виконання операції множення великих чисел за модулем дорівнює $6H(H+1)$.

Враховуючи вищесказане, в роботі [4] отримано оцінки складності прискореного обчислення елементу $v_{n,k}$, які показали, що складність виконання алгоритмів на основі бінарного методу для додатних та від'ємних значень n є однаковою, так само і складність виконання алгоритмів на основі методу з розкладанням індексу як для додатних, так і для від'ємних значень індексу n також є однаковою. В результаті мінімальні та максимальні оцінки складності алгоритмів на основі бінарного методу та методу з розкладанням індексу і для додатних і для від'ємних значень n мають такий вигляд:

$$S_{БМ\min} = H^2 q\cdot[6H(k^2+3k-2)+3(3k^2+6k-5)], \quad \textbf{(16)}$$

$$S_{БМ\max} = H^2 q\cdot[6H(k^2+3k)+9(k^2+2k)], \quad \textbf{(17)}$$

$$S_{PI\min} = H\cdot[6H(k^2+k)+3(3k^2+k)], \quad \textbf{(18)}$$

$$S_{PI\max} = H^2 q\cdot[6H(k^2+k)+3(3k^2+k)], \quad \textbf{(19)}$$

де q – кількість розрядів машинної одиниці інформації.

Слід зазначити, що під час реалізації криптографічних методів в сучасних комп'ютерних системах оперують ключами, що мають розмір 1024 і більше розрядів ($Hq \geq 1024$), зокрема розмір ключа може бути 4096 розрядів.

Тепер, коли визначено усі необхідні оцінки для оцінювання протоколу шифрування інформації без попереднього розподілу ключів на основі U_k–послідовностей, отримаємо

такі мінімальні та максимальні оцінки протоколу, причому як для випадку з використанням бінарного методу так і з використанням методу розкладання індексу n:

$$S_{\min(БМ)} = QH \cdot [12H(k^2+2k+1)+3(6k^2+7k+3)] + 4H^2q \cdot [6H(k^2+3k-2)+3(3k^2+6k-5)], \quad \textbf{(20)}$$

$$S_{\max(БМ)} = QH \cdot [12H(k^2+2k+1)+3(6k^2+7k+3)] + 4H^2q \cdot [6H(k^2+3k)+9(k^2+2k)], \quad \textbf{(21)}$$

$$S_{\min(PI)} = QH \cdot [12H(k^2+2k+1)+3(6k^2+7k+3)] + H \cdot [6H(5k^2+7k+2)+15(3k^2+2k+1)], \quad \textbf{(22)}$$

$$S_{\max(PI)} = QH \cdot [12H(k^2+2k+1)+3(6k^2+7k+3)] + 4H^2q \cdot [6H(k^2+k)+3(3k^2+k)]. \quad \textbf{(23)}$$

Порівняємо тепер отримані оцінки складності розглянутого протоколу на основі U_k-послідовностей з відповідними оцінками відомого протоколу шифрування інформації без попереднього розподілу ключів Шаміра.

Основною операцією, що виконується в методі Шаміра є піднесення до степеня за модулем. Ця операція може здійснюватись за методом Монтгомері [5], який має меншу складність обчислень, ніж відомий бінарний метод [6]. Метод піднесення до степеня за Монтгомері оснований на множенні за методом Монтгомері. Виходячи з цього, алгоритм піднесення до степеня за Монтгомері та обчислення усіх необхідних для цього операцій і величин можна розробити на основі розроблених алгоритмів обчислення лишку Монтгомері та множення за Монтгомері, що використовуються для реалізації розглянутого протоколу шифрування без попереднього розподілу ключів на основі рекурентних послідовностей.

В результаті отримано оцінки складності виконання операції піднесення до степеня за модулем за Монтгомері, які наведено в [4]. Аналіз отриманих оцінок показав, що обчислення певного елементу U_k-послідовності має той же порядок, що і складність піднесення до заданого степеня.

Використовуючи отримані оцінки, отримаємо такі мінімальні та максимальні оцінки складності для відомого протоколу шифрування без попереднього розподілу ключів Шаміра

$$S_{Ш\min} = 24QH^2q(H+1), \quad \textbf{(24)} \qquad S_{Ш\max} = 48QH^2q(H+1). \quad \textbf{(25)}$$

На основі отриманих оцінок (20)…(23) для розглянутого протоколу шифрування без попереднього розподілу ключів на основі U_k–послідовностей побудуємо графіки залежності $S = f(Q)$ для різних значень H. При цьому розглянемо випадки, коли $q = 32$, k дорівнює 2 або 3 і для прискореного обчислення елементу $v_{n,k}$ застосовується метод з розкладанням індексу n.

На рис. 1(а) та 2(а) представлено графіки залежностей для максимальної, а на рис. 1(б) та 2(б) – для мінімальної оцінки складності розглянутого протоколу на основі U_k-послідовностей та відомого протоколу Шаміра.

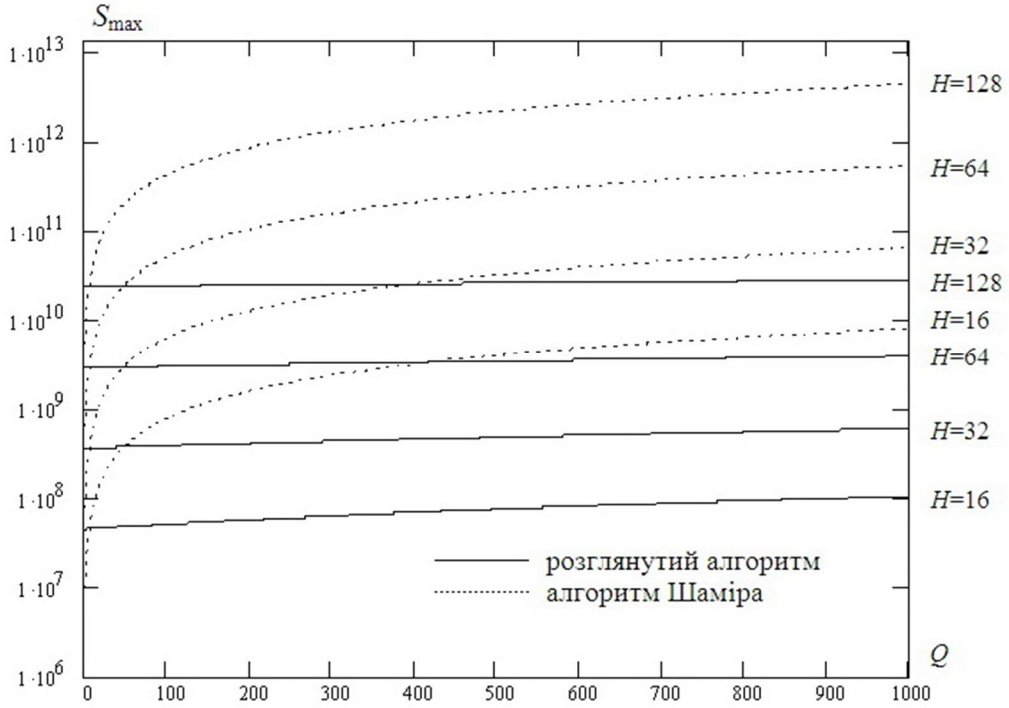
Аналіз графіків представлених на рис. 1, 2 показує, що максимальна оцінка складності розглянутого протоколу шифрування інформації без попереднього розподілу ключів на основі U_k–послідовностей для $Q > 100$ приблизно у 10^2 разів менша ніж для відомого, а мінімальна оцінка менша ніж для відомого приблизно у 10^3.

Висновок. Проведено оцінювання обчислювальної складності протоколу шифрування інформації без попереднього розподілу ключів на основі U_k–послідовностей, в результаті чого отримано мінімальні та максимальні оцінки складності цього протоколу, причому як для випадку використання бінарного методу прискореного обчислення елементів V_k–послідовності, так і методу з використанням розкладання індексу n.

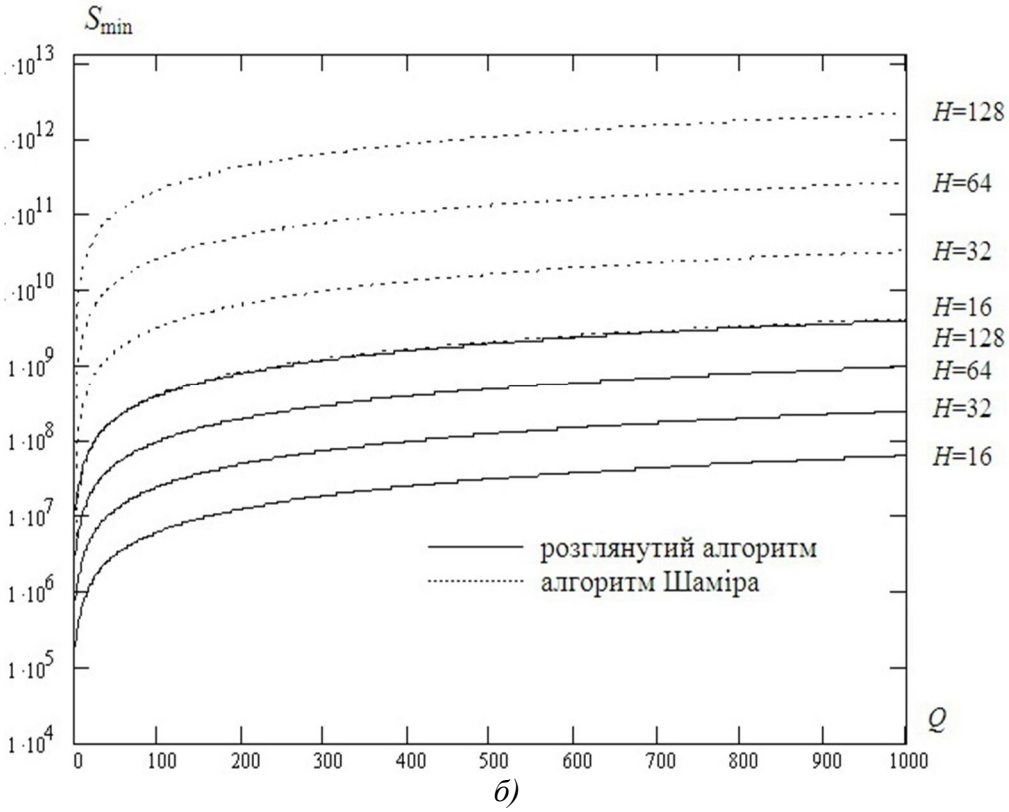
З метою можливості порівняння, проведено оцінювання обчислювальної складності відомого протоколу шифрування інформації без попереднього розподілу ключів Шаміра. Для порівняння отриманих оцінок з розглянутим протоколом на основі рекурентних

послідовностей отримано графіки залежностей $S = f(Q)$ для різних значень H та коли k дорівнює 2 або 3.

Аналіз отриманих оцінок показав, що протокол шифрування без попереднього розподілу ключів на основі рекурентних V_k та U_k –послідовностей має меншу складність обчислень для будь-якого k не менше ніж у 10^2 разів у порівнянні з відомим протоколом Шаміра і при цьому забезпечує достатній рівень криптостійкості.

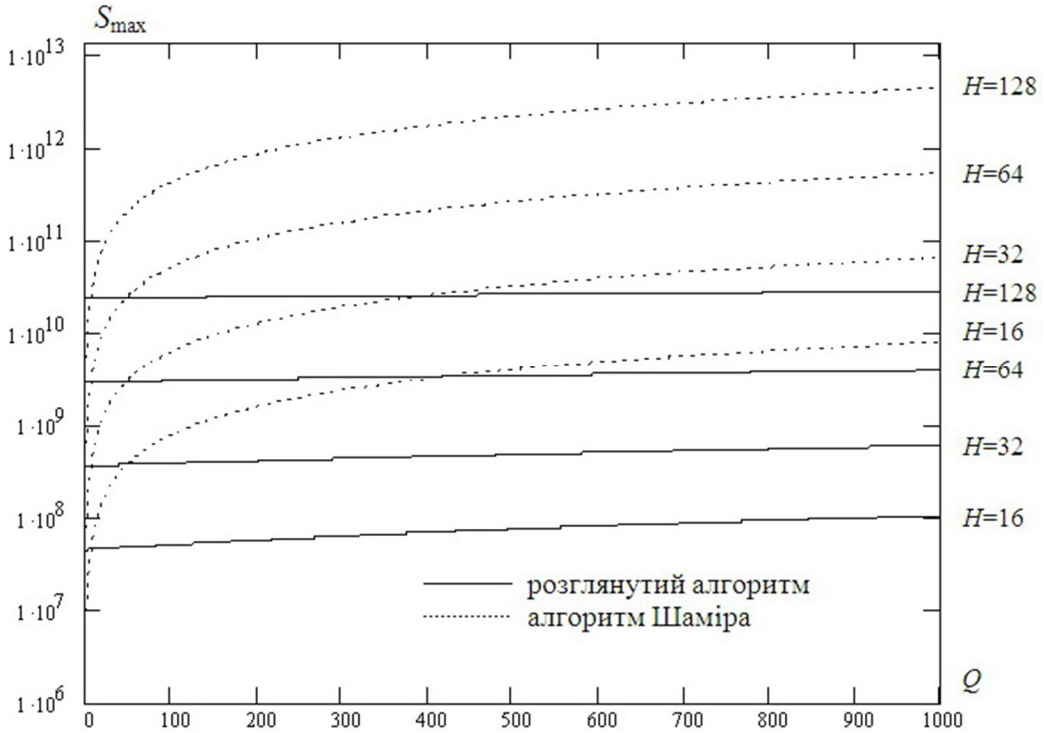


а)

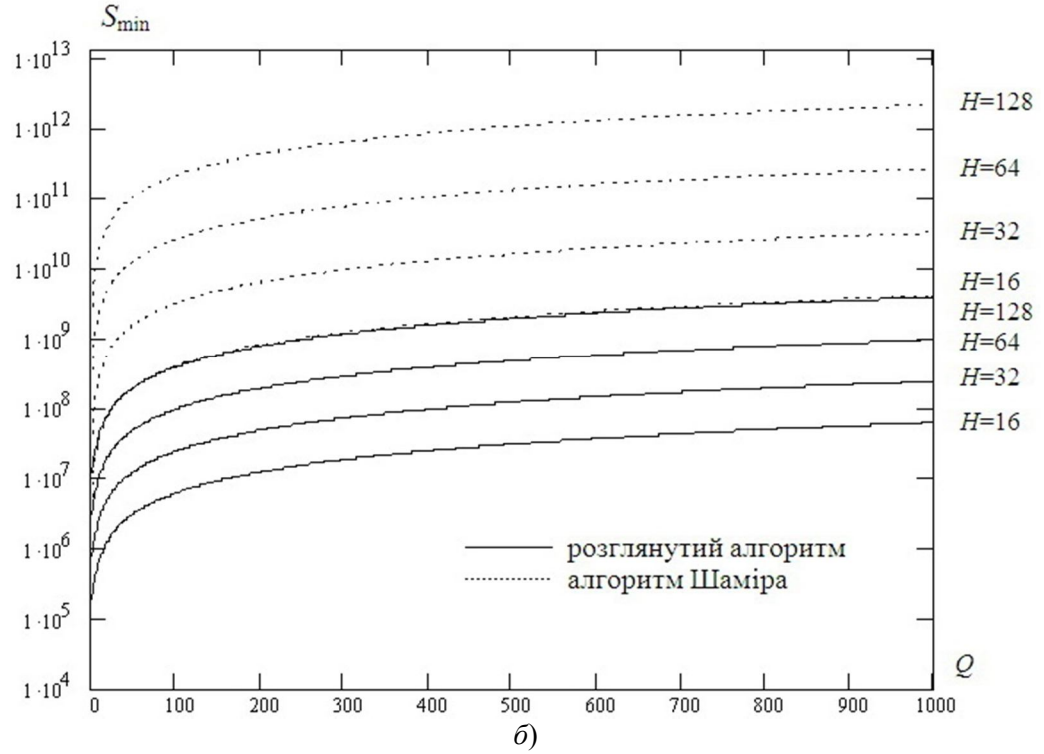


б)

Рис. 1. Графіки залежностей $S_{\max} = f(Q)$ та $S_{\min} = f(Q)$ для $k = 2$, $q = 32$



а)



б)

Рис. 2. Графіки залежностей $S_{\max} = f(Q)$ та $S_{\min} = f(Q)$ для $k = 3$, $q = 32$

Література

1. Яремчук Ю.Є. Спеціалізовані процесори шифрування інформації без попереднього розподілу ключів на основі рекурентних послідовностей / Ю.Є. Яремчук // Радіотехніка. – 2013. – Вип. 172. – С. 112-120.

2. Месси Д.Л. Введение в современную криптологию / Д.Л. Месси // ТИЭИР. – 1988. – Т.76, №5. – С. 2442.

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

4. Яремчук Ю.Є. Оцінювання обчислювальної складності алгоритмів прискореного обчислення елементів рекурентних послідовностей / Ю.Є. Яремчук // Вісник СНУ ім. В. Даля. – 2012. – №12 (183), Ч. 2. – С. 113-121.

5. Menezes A.J., van Oorschot P.C., Vanstone S.A. Handbook of Applied Cryptography. – CRC Press, 2001. – 816 p.

6. Кнут Д. Искусство программирования для ЭВМ, том 2. Получисленные алгоритмы / Д. Кнут. – М.: Вильямс, 2004. – 832 с.

УДК 621.396.662.072.078

Сайко В.Г., д.т.н. ; **Дакова Л.В.** асп.; **Бондарчук А.П.,** к.т.н.
(Государственный университет информационно-коммуникационных технологий)

РЕКУРЕНТНЫЙ МЕТОД ОПРЕДЕЛЕНИЯ ГЛУБИНЫ ЗАМИРАНИЙ МНОГОЛУЧЕВЫХ СИГНАЛОВ ДЛЯ ЗАЩИЩЕННЫХ РАДИОСИСТЕМ

Сайко В.Г., Дакова Л.В., Бондарчук А.П. Рекурентний метод визначення глибини завмирань багатопроменевих сигналів для захищених радіосистем. Запропоновано новий метод визначення глибини завмирань багатопроменевих сигналів мереж рухомого радіозв'язку, що відрізняється простотою технічної реалізації і дозволяє зменшити середньоквадратичну похибку і варіабельність оцінки в середньому на 9-14%.

Ключові слова: ЗАВМИРАННЯ СИГНАЛІВ, ВІДНОШЕННЯ СИГНАЛ/МУМ

Сайко В.Г., Дакова Л.В., Бондарчук А.П. Рекуррентный метод определения глубины замираний многолучевых сигналов для защищенных радиосистем. Предложен новый метод определения глубины замираний многолучевых сигналов сетей подвижной радиосвязи, отличающийся простотой технической реализации и позволяющий уменьшить среднеквадратическую погрешность и вариабельность оценки в среднем на 9-14 %.

Ключевые слова: ЗАМИРАНИЯ СИГНАЛОВ, ОТНОШЕНИЕ СИГНАЛ/ШУМ

Saiko V.H., Dakova L.V., Bondarchuk A.P. Recursive method for determining the depth of fading multipath signals for secure radio communications. A new method for determining the depth of fading multipath signals of mobile radio technology which is easy to implement and allows to reduce the mean squared error and variability of estimates by an average of 9-14%.

Keywords:: FADING SIGNALS, SIGNAL / NOISE RATIO

В системах мобильной связи нового поколения ряд задач обнаружения и различения многолучевых сигналов на фоне помех с априорно неизвестными статистическими характеристиками можно успешно решить с помощью систем, адаптирующихся к наиболее информативным параметрам **статистик второго порядка** принимаемого сигнала с замираниями. К таким параметрам относятся, например, среднее число пересечений одного или нескольких относительных уровней анализа за фиксированное время, распределение длительностей выбросов за уровень и пауз между ними, распределение времени пребывания сигнала в заданных границах. Полезной может оказаться информация о законе распределения интервала времени между произвольным моментом и первым пересечением сигналом нулевого уровня, о среднем интервале между экстремумами сигнала [1]. Самыми изученными параметрами **статистик второго порядка** являются их средние длительности за уровень и, отчасти, дисперсии длительностей, а также начальные участки плотностей распределения длительностей выбросов. Ввиду сложности строго решения ряда задач в области теории выбросов случайных процессов, полезными оказываются приближенные результаты, которые удается довести до инженерных приложений [2].

Постановка задачи. Проведенный анализ методов определения характеристик замираний сигнала из-за многолучевости (канальных статистических параметров второго порядка и глубины замираний) показал, что при непараметрической априорной