УДК 681.3.06

Р.В. Корольов

Харківський університет Повітряних Сил ім. І. Кожедуба, Харків

ДОСЛІДЖЕННЯ ПЕРІОДИЧНИХ ВЛАСТИВОСТЕЙ ГЕНЕРАТОРІВ ПСЕВДОВИПАДКОВИХ ЧИСЕЛ, ЗАСНОВАНИХ НА ВИКОРИСТАННІ НАДМІРНИХ БЛОКОВИХ КОДІВ

Розглядаються методи формування послідовностей псевдовипадкових чисел (ППВЧ), стійкість яких заснована на теоретико-складовій проблемі синдромного декодування. Досліджуються періодичні властивості генераторів, встановлено, що формовані послідовності не володіють максимальним періодом.

Ключові слова: *генератор псевдовипадкових чисел, псевдовипадкові числа.*

Вступ

1. Постановка проблеми в загальному вигляді і аналіз літератури. У роботі [1] проведені дослідження статистичної безпеки найбільш поширених генераторів ППВЧ: генератор на основі алгоритму SHA-1 [2, 3], лінійний конгруентний генератор [3, 4], генератор RC4[3], квадратичний конгруентний генератор[4], генератор на основі алгоритму DES, генератор на основі алгоритму 3-DES [5], генератор Blum-Blum-Shub [3 – 5], національний алгоритм шифрування США AES (FIPS-197) в режимі лічильника [6], доказово стійкий генератор, заснований на проблемі синдромного декодування [7] (Generator Provably as Secure as Syndrome Decoding – (GPSSD)) [8]. Проведені дослідження показали, що розглянуті генератори володіють високими показниками статистичної безпеки. Найвищі результати показав генератор GPSSD – доказово безпечний генератор ППВЧ, стійкість якого обгрунтовується теоретико-складовим завданням синдромного декодування.

Результати досліджень

Таким чином, на підставі отриманих в [1] експериментальних результатів можна стверджувати, що GPSSD є найбільш перспективним по критерію статистичної безпеки. Окрім найбільшої кількості тестів, що пройшли по методиці NIST STS [9], даний генератор належить до групи алгоритмів, до яких застосовне поняття «Доказова безпека» (Provably Security), детально досліджене в [10]. Практично воно означає, що завдання криптоаналізу (обчислення секретного ключа) генератора ППВЧ може бути зведена до однієї з відомих теоретико-складових задач, наприклад, факторизації, дискретному логарифмуванню та ін. У цей час недослідженим залишається проблема оцінки ефективності генератора GPSSD за іншими показниками безпеки (довжина періоду формованих послідовностей, структурна скритність та ін.). ***Метою даної статті*** є дослідження періодичних властивостей генератора GPSSD, оцінка довжин періодів формованих ППВЧ.

2. Структура і особливості реалізації методу GPSSD. Метод формування ППВЧ на основі надмірних код вперше запропонован в роботі [8]. Він заснован на формуванні фрагмента ППВЧ по синдромной послідовності надмірного блокового коду, яка у свою чергу формується за рекурентним правилом як функція від секретного ключа. Стійкість генератора GPSSD заснована на зведенні завдання знаходження секретного ключа до рішення задачі синдромного декодування. Структурна схема методу GPSSD приведена на рис. 1.

На першому етапі з використанням методів надмірного (перешкодостійкого) кодування нелінійними блоковими кодами по введеній ключовій послідовності формуються рівноважні посилки, відповідні введеним секретним ключовим даним. На другому етапі з використанням методів надмірного (перешкодостійкого) кодування лінійними блоковими кодами по сформованих рівноважних посилках формуються синдромні послідовності. На третьому, завершальному етапі по сформованих синдромних послідовностях з використанням методів теорії ймовірності і математичної статистики формується фрагмент ППВЧ і сеансовий ключ, який використовується в подальших ітеративних процедурах генератора на вході першого етапу методу. У [8] запропоновано використовувати просте розділення сформованої синдромної послідовності на дві частини: перша – використовується в подальших ітеративних процедурах як сеансовий ключ, друга – береться за результат формування фрагмента ППВЧ.

Процес формування ППВЧ методом GPSSD формалізується сукупністю наступних аналітичних співвідношень:

– на першому етапі вводяться секретні ключові дані

$$K_i = K_{i_0} \quad K_{i_1} \quad \dots \quad K_{i_{m-1}} \; ; \; K_i \in K \subseteq GF^M \; q \; ;$$

$$K_{i_j} \in GF \; q \; ;$$

По заданій послідовності зворотного зв'язку

$$S^*_{K_i} = S^*_{Ki_0} \quad S^*_{Ki_1} \quad \dots \quad S^*_{Ki_{m-1}} \; ;$$

$$S^*_{Ki} \in S^*_K \subseteq GF^M \; q \; , \; S^*_{Ki_j} \in GF \; q \; ;$$

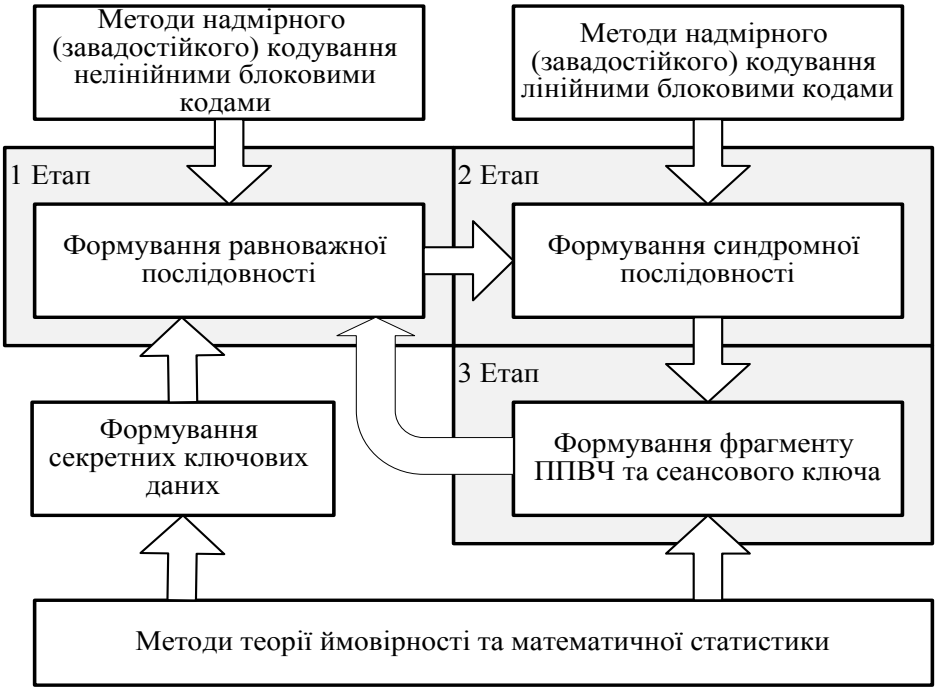

Рис. 1. Структурна схема методу GPSSD

(на першому раунді $S^*_{K_i} = K_i$) з використанням рівності

$$S^*_{K_i} = \sum_{j=0}^{n-1} \begin{pmatrix} j \\ C^*_{K_{i_j}} \end{pmatrix},$$

що встановлює правило рівноважного кодування, тобто перетворення послідовності сеансового ключа в послідовність біноміального коду, формується рівноважна послідовність

$$C^*_{K_i} = C^*_{Ki_0} \quad C^*_{Ki_1} \quad \dots \quad C^*_{Ki_{n-1}} \ ;$$

$$C^*_{Ki} \in C^*_K \subseteq GF^n \ \ q \ ;$$

$$C^*_{Ki_j} \in GF \ \ q \ ;$$

$$w \ \ C^*_{Ki} = w \ ;$$

– на третьому етапі по сформованій рівноважній послідовності і перевірочної матриці H надмірного лінійного блокового (n, k, d) коду з використанням рівності

$$S_{K_i} = C^*_{K_i} \cdot H^T$$

формується синдромна послідовність лінійної блокового n, k, d коду $r = n - k$:

$$S_{K_i} = S_{Ki_0} \quad S_{Ki_1} \quad \dots \quad S_{Ki_{r-1}} \ ;$$

$$S_{Ki} \in S_K \subseteq GF^r \ \ q \ ;$$

$$S_{Ki_j} \in GF \ \ q \ ;$$

– на четвертому етапі по сформованій синдромній послідовності за допомогою усікання елементів формується фрагмент ППВЧ і послідовність зворотнього зв'язку,

$$S^*_{K_i} = S^*_{Ki_0} \quad S^*_{Ki_1} \quad \dots \quad S^*_{Ki_{m-1}} \ ;$$

$$S^*_{Ki} \in S^*_K \subseteq GF^M \ \ q \ ;$$

$$S^*_{Ki_j} \in GF \ \ q \ ,$$

яка використовується на наступному циклі (раунді) першого етапу запропонованого методу.

Таким чином, як показали проведені дослідження, на кожному раунді перетворень з використанням методів нелінійного (рівноважного) і лінійного кодування формується фрагмент ППВЧ, як вибірка (усікання) синдромної послідовності лінійного блокового коду. Частина синдромної послідовності, що залишилася, поступає на перший етап наступного раунду перетворень.

Методика досліджень і основні отримані результати

Для проведення досліджень періодичних властивостей генератора GPSSD розроблена програмна модель, що реалізовує процес формування ППВЧ з використанням надмірних блокових даних. Як початкові дані використовувався двійковий код з параметрами (64, 24, 16). Відповідна довжина секретного ключа склала $m = 24$ біта, довжина синдромної послідовності $m = 40$ біт, довжина сеансового ключа $m = 24$ біта, довжина формованого на кожній ітерації фрагмента ППВЧ 40-24 = 16 біт. Очікувана довжина періоду $L = 2^{24} - 1$.

В ході проведення досліджень протестована робота генератора GPSSD на повній безлічі ненульових ключових даних (всього $2^{24} - 1$ тестів). У

кожному тесті оцінювалася довжина періоду L. В результаті проведення експерименту підрахований розподіл числа послідовностей N по довжинах періодів L, представлене на рис. 2.

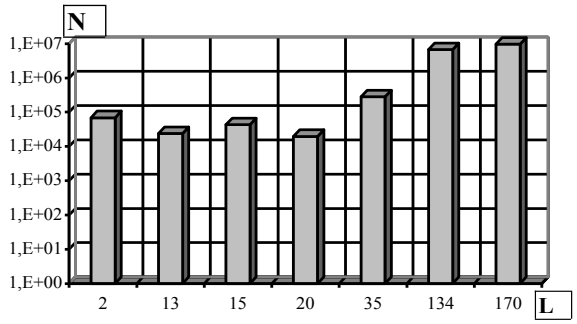

Рис. 2. Розподілення числа послідовностей по довжинам періодів

Як слідує з приведених на рис. 2 даних, генератор GPSSD формує послідовності з малою довжиною періоду L = 2÷170. Найбільше число послідовностей (>97%) мають період 134 або 170. У теж час деякі послідовності володіють надзвичайно малим періодом (L = 2÷35). Аналіз показує, що найбільший період послідовностей, який дозволяє сформувати генератор GPSSD із заданими параметрами складає L = 170, що на п'ять порядків менше максимального ($L = 2^{24} - 1$). Таким чином можна констатувати, що доказово стійкий генератор GPSSD, що має покращенні показники по статистичній безпеці [1] і швидкодії [8] не забезпечує формування послідовностей максимального періоду.

Виводи

Проведені дослідження показали, що доказово стійкий генератор GPSSD, що побудований з використанням надмірних блокових кодів володіє покращенними показниками по статистичній безпеці і швидкодії але не забезпечує формування послідовностей максимального періоду, його періодичні властивості незадовільні, що може стати причиною появи ефективних криптографічних атак.

Перспективним напрямом подальших досліджень є розробка вдосконаленого методу на основі надмірних блокових кодів, який окрім високих показників статистичної безпеки і швидкодії дозволить формувати послідовності максимального періоду.

Список літератури

1. Кузнецов А.А., Королев Р.В., Рябуха Ю.Н. Исследование статистической безопасности генераторов псевдослучайных чисел // Системи обробки інформації. – Х., 2008. – Вип. 3(70). – С. 79-82.

2. Поповский В.В. Защита информации в телекоммуникационных системах: Учебник / В.В. Поповский, А.В. Персиков; ХНУРЭ. – Х.: ООО "Компания Смит", 2006. – 238 с.

3. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. – М.: Издательство ТРИУМФ, 2002 – 816 с.

4. Иванов М.А., Чугунков И.В. Теория, применение и оценка качества генераторов псевдослучайных последовательностей. – М.: КУДИЦ-ОБРАЗ, 2003. – 240 с.

5. Blum L. A Simple Unpredictable Pseudo-Random Number Generator / L.Blum, M.Blum, M.Shub // Siam Journal on Computing. – V. 15, n. 2. – 1986. – Pp. 364-386

6. National Institute of Standards and Technology, "FIPS-197: Advanced Encryption Standard." Nov. 2001. Available at http: //csrc.nist.gov/publications/fips/fips197/fips-197.pdf.

7. Мак-Вильямс Ф.Дж., Слоэн Н.Дж.А. Теория кодов, исправляющих ошибки. – М.: Связь, 1979. – 744 с.

8. Jean-Dernard Fisher, Jacques Stern. An efficient Pseudo-Random Generator Provably as Secure as Syndrome Decoding // EUROCRYPT'96 Proceeding, LNCS 1070. – P. 245-255.

9. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications. NIST Special Publication 800-22. Technology Administration U.S. Department of Commerce. – Washington: National Institute of Standards and Technology. – 2000. – 164 p.

10. Final report of European project number IST-1999-12324, named New European Schemes for Signatures, Integrity, and Encryption, April 19, 2004. – Version 0.15 (beta), Springer-Verlag. – 829 p.

Надійшла до редколегії 27.11.2008

Рецензент: д-р техн. наук, проф. Ю.В. Стасєв, Харківський університет Повітряних сил ім. І. Кожедуба, Харків.

ИССЛЕДОВАНИЕ ПЕРИОДИЧЕСКИХ СВОЙСТВ ГЕНЕРАТОРОВ ПСЕВДОСЛУЧАЙНЫХ ЧИСЕЛ, ОСНОВАННЫХ НА ИСПОЛЬЗОВАНИИ ИЗБЫТОЧНЫХ БЛОЧНЫХ КОДОВ

Р.В. Королев

Рассматриваются методы формирования последовательностей псевдослучайных чисел (ППВЧ), стойкость которых основана на теоретико-складовій проблеме синдромного декодирования. Исследуются периодические свойства генераторов, установлено, что формуемые последовательности не владеют максимальным периодом.

Ключевые слова: *генератор псевдослучайных чисел, псевдослучайные числа.*

RESEARCH OF PERIODIC PROPERTIES OF GENERATORS OF PSEUDOCASUAL NUMBERS, BASED ON THE USE OF SURPLUS SECTIONAL KODAS

P.B. Korol'ov

The methods of forming of sequences of pseudocasual numbers (PPVCH) firmness of which is based on theorist of intricate problem of the syndromic decoding are examined. Periodic properties of generators are probed, it is set that mouldable sequences do not own a maximal period.

Keywords: *generator of pseudocasual numbers, pseudocasual numbers.*