УДК 004.056.55

ПЕРІОДИЧНІ ВЛАСТИВОСТІ КРИПТОГРАФІЧНО СТІЙКИХ ПСЕВДОВИПАДКОВИХ ПОСЛІДОВНОСТЕЙ

О. О. КУЗНЕЦОВ, А. С. КІЯН, Д. І. ПРОКОПОВИЧ-ТКАЧЕНКО, В. П. ЗВЄРЄВ, Е. В. КОТУХ, Т. Ю. КУЗНЕЦОВА

У цій роботі розглянуто доказово стійкі генератори псевдовипадкових послідовностей, завдання криптоаналізу яких зводиться до вирішення добре відомої і надзвичайно складної математичної задачі, що належить до класу NP-складних. Зокрема, розглянуто генератори Blum-Blum-Shub, Rivest-Shamir-Adleman, Dual Elliptic Curve і генератор на синдромному декодуванні (Pseudo-Random Generator Provably as Secure as Syndrome Decoding). Досліджено періодичні властивості формованих псевдовипадкових послідовностей. Показано, що розглянуті генератори не дозволяють сформувати послідовності максимального періоду. Крім того, для кожного генератора існують початкові стану (слабкі ключі), що призводять до катастрофічно малих довжин періодів формованих послідовностей.

Ключові слова: модель доказової безпеки, генератор псевдовипадкових чисел, періодичні властивості.

ВСТУП

Важливим напрямком сучасної криптографії є побудова криптографічно стійких (англ. Cryptographically Strong) генераторів псевдовипадкових послідовностей (ПВП), які відповідають вимогам моделі доказової безпеки (англ. Provable Security Model) [1]. Сутність цієї моделі полягає у зведенні задачі криптоаналізу до вирішення добре відомої і надзвичайно складної математичної проблеми (що належить до класу NP-складних), наприклад, факторизації, дискретного логарифмування тощо. [1]. Криптографічні примітиви, які відповідають такій моделі безпеки, прийнято називати доказово безпечними, тому що їх криптоаналіз можна порівняти з рішенням NP-складної математичної проблеми.

Обґрунтування безпеки доказово стійких генераторів базується на прийняття припущення про існування так званих односторонніх функцій [1, 2]. Одностороння функція $f: x \to y$, задана на безлічі x з областю значень в безлічі y володіє двома властивостями:

– існує поліноміальний алгоритм обчислення $f(x)$;

– не існує поліноміальною алгоритму інвертування функції $f(x)$, тобто розв'язання рівняння $f(x) = y$.

Виконання другої властивості на сьогоднішній день не доведено ні для однієї з можливих функцій $f(x)$, тобто не доведено саме існування односторонніх функцій (як є бездоказовим і припущення $P \neq NP$ в теорії складності). Водночас, на використанні різних кандидатів на односторонню функцію будуються практично всі відомі криптосистеми з відкритим ключем [2]. До претендентів на односторонню функцію належать розкладання цілих чисел на множники, проблему обчислення дискретних логарифмів або обчислення квадратного кореня за модулем складеного числа, задачу синдромного декодування, дискретного логарифмування в групі точок еліптичної кривої тощо [1–7]. Метою цієї статті є дослідження періодичних властивостей криптографічно стійких ПВП, які формуються доказово безпечними генераторами. Зокрема, в цій роботі досліджуються такі генератори: Blum-Blum-Shub (BBS) [5], Micali-Schnorr та Rivest-Shamir-Adleman (RSA) [3, 4], Dual Elliptic Curve Deterministic Random Bit Generator [6], Code-based Pseudorandom Generator [7].

2. ДОКАЗОВО СТІЙКІ ГЕНЕРАТОРИ ПВП

2.1. Генератор BBS

Найбільш важлива одностороння функція, використовувана в ході побудови генераторів ПВП, – є факторизація цілих чисел [1, 2]. Широко відомим криптопримітивом, заснованим на цій проблемі, є генератор BBS [5], запропонований в 1986 р. Ленором Блюмом, Мануелем Блюмом і Майклом Шубом.

Обчислення ПВП у генераторі BBS описується виразом:

$$x_n = x_{n-1}^2 \bmod N,$$

де $N = pq$ є добутком двох великих простих p і q і які можуть бути обидва порівнянні з числом 3 за модулем 4.

На кожному кроці алгоритму формують один біт ПВП шляхом взяття біта парності числа x_n (або одного найменш значущого біту).

Головною перевагою генератору BBS є те, що для отримання числа x_n необов'язково обчислювати всі $n-1$ попередніх чисел. Необхідно лише знати початковий стан генератора, тобто число x_0 (яке задається, наприклад, секретним ключем), а також числа p і q. Будь-який елемент послідовності описується виразом:

$$x_n = x_0^{2^n \bmod ((p-1)(q-1))} \bmod N.$$

2.2. Генератори Micali-Schnorr та RSA

Стійкість генераторів Micali-Schnorr та RSA заснована на теоретико-складній задачі обчислення *дискретних логарифмів* [1, 2]. Кожен елемент ПВП у генераторі *Micali-Schnorr* описується відповідно до виразу [2–4]:

$$x_n = x_{n-1}^e \bmod N \,. \qquad (1)$$

Початковий стан генератора, тобто число x_0, задається, наприклад, секретним ключем. На кожному кроці формується r біт ПВП шляхом зчитування r найменш значущих біт числа x_n, причому [2–4]:

$$r = \lfloor \lg(pq) \rfloor + 1 - \left\lfloor (\lg(pq)+1)(1-\frac{2}{e}) \right\rfloor$$

де

$$e \in \begin{cases} 1 < e(p-1)(q-1); \\ НОД(e,(p-1)(q-1) = 1; \\ 80e \le \lfloor \lg(pq) \rfloor + 1; \end{cases}$$

p і q – прості числа.

У генераторі *RSA* кожен елемент ПВП описується виразом (1), але на відміну від генератора *Micali-Schnorr* на вихід поступає один найменш значущий біт (біт парності) числа x_n [2–4].

2.3. Генератор Dual Elliptic Curve

У національному стандарті США NIST Special Publication 800-90A [6] визначено рекомендації щодо побудови генераторів ПВП із застосуванням різних математичних методів, у тому числі, із застосуванням перетворень у групі точок еліптичної кривої. І хоча в оновленні версії стандарту [8] цей генератор було виключено через певні недоліки, ми розглянемо алгоритм формування ПВП з метою дослідження його періодичних властивостей.

Метод формування псевдовипадкових послідовностей із використанням перетворень на еліптичних кривих, який запропоновано в рекомендаціях NIST SP 800-90, засновано на застосуванні двох скалярних множень точок еліптичної кривої та відображенні відповідних x-координат отриманих результатів у ненульове ціле значення.

Перше скалярне множення на фіксовану (базову) точку P виконується для формування проміжного стану s_i, яке циклічно оновлюється на кожній ітерації в ході функціонування відповідного генератору. Таким чином значення стану s_i залежить від значення попереднього стану s_{i-1} (на попередній ітерації) та від значення базової точки P:

$$s_i = \phi(x(s_{i-1}P)), \qquad (2)$$

де $x(A)$ – є x-координатою точки A, $\phi(x)$ – функція відображення елементів поля у ненульові цілі числа.

Початкове значення параметра s_0 формується із використанням процедури ініціалізації, яка включає введення секретного ключа (*Key*), що задає початкову ентропію (невизначеність), та хешування введеного ключа із форматуванням отриманого результату до визначеної довжини бітів. Отримане таким чином значення *Seed* засіює (ініціює) початкове значення параметра: $s_0 = Seed$.

Друге скалярне множення на фіксовану (базову) точку Q виконується для формування проміжного стану r_i, яке після відповідного перетворення і задає значення формованих псевдовипадкових бітів. Значення параметру r_i залежить від сформованого у результаті першого скалярного множення параметра s_i та від значення базової точки Q:

$$r_i = \phi(x(s_i Q)), \qquad (3)$$

Отримане таким чином значення r_i є вихідним для формування псевдовипадкових бітів, які формуються шляхом зчитування блоку з найменш значущих (правих) бітів числа r_i. ПВП формується шляхом конкатенації зчитаних бітів формованих чисел r_i.

Значення фіксованих (базових) точок задаються у вигляді констант і під час формування ПВП не змінюються.

Таким чином, розглянутий метод формування псевдовипадкових послідовностей застосовує перетворення у групі точок еліптичної кривої для формування проміжних станів s_i і r_i. Причому зворотна дія, тобто формування s_{i-1} за відомим s_i, та/або формування s_i та відомим r_i пов'язано з вирішенням теоретико-складного завдання дискретного логарифмування у групі точок еліптичної кривої. Схему формування проміжних станів генератора подано на рис. 1.

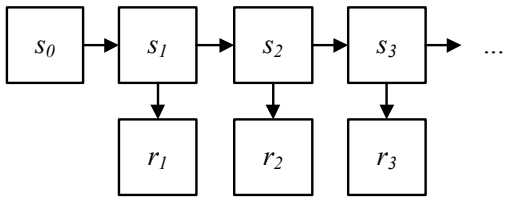

Рис. 1. Схема формування проміжних станів генератору

Як видно з рис. 1 послідовність станів $\ldots s_{i-1}$, s_i, $\ldots s_{i+1} \ldots$ формується із початкового значення $s_0 = Seed$, яке в свою чергу формується із даних секретного ключа. Кожне наступне значення s_i залежить від попереднього значення s_{i-1} і формується за допомогою скалярного множення базової точки еліптичної кривої за формулою (2).

Окремі біти ПВП формуються шляхом зчитування бітів послідовності чисел … r_{i-1}, r_i, r_{i+1},…, тобто шляхом зчитування даних, отриманих у результаті скалярного множення іншої базової точки на відповідні значення станів … s_{i-1}, s_i, … s_{i+1} … за формулою (3).

Оскільки таємний ключ *Key*, який задає правило формування послідовностей, після певних перетворень визначає початкове значення параметру s_0, відповідна стійкість розглянутого генератора базується на зведенні завдання відновлення секретних ключових даних до вирішення добре відомого і надзвичайно складного математичного завдання дискретного логарифмування у групі точок еліптичної кривої. Крім того окремі фрагменти псевдовипадкової послідовності також пов'язані між собою скалярним множенням точки еліптичної кривої, тобто, для того, щоб відновити будь-який фрагмент псевдовипадкової послідовності за якимось іншим, відомим фрагментом, потрібно вирішити завдання дискретного логарифмування у групі точок еліптичної кривої. І навпаки, якщо для розглянутого генератора за відомим фрагментом псевдовипадкової послідовності вдається відновити інший, будь-який невідомий фрагмент, або вдається відновити значення секретного ключа (або хоча б значення елементів послідовності … s_{i-1}, s_i, … s_{i+1} …) це означає, що вдається вирішити завдання дискретного логарифмування в групі точок еліптичної кривої, тобто інвертована функція (2) або (3).

2.4. Генератор синдромного декодування

Побудову цього генератора засновано на використані блокового (n,k,d) коду, який заданий своєю перевірною матрицею H розміром n стовпців і $n-k$ рядків. У теорії кодування відома NP-складна проблема синдромного декодування [9, 10]:

– за відомим вектором-синдромом s довжини $n-k$ і відомою матрицею H знайти такий вектор помилки e довжини n, що $s = e \cdot H^T$, причому вага Хеммінга (число ненульових елементів) вектору e дорівнює $w(e) = t = \left\lceil \frac{d-1}{2} \right\rceil$, де $\lceil x \rceil$ – найменше ціле число, що не менше x.

Величина t визначає здатність (n,k,d) коду, тобто це гарантоване число помилок, які можливо виправити, застосувавши метод максимальної правдоподібності. Для деяких кодів (зі спеціальною структурою матриці H) відомі швидкі алгоритми алгебраїчного декодування, тобто знаходження вектора e є поліноміально вирішуване завдання. Однак для кодів загального положення (без спеціальної структури матриці H) завдання знаходження вектора e є надзвичайно складним, найкращі алгоритми засновані на переборному пошуку.

В роботі [7] запропоновано генератор ПВП, стійкість якого заснована на вирішенні проблеми синдромного декодування (Pseudo-Random Generator Provably as Secure as Syndrome Decoding). Для формування ПВП в цьому генераторі використовується двійковий (n,k,d) код і наступне рекурентне правило: $s_i = e_i \cdot H^T$, де: e_i – двійковий вектор довжини n, $w(e_i) = t = \left\lceil \frac{d-1}{2} \right\rceil$; s_i – двійковий вектор довжини $n-k$; H – двійкова перевірна матриця (n,k,d) коду. Початковий стан e_0 генератора задається за допомогою рівноважного кодування ініційованої послідовності y_0 довжини $m = \left\lfloor \log_2 \left(\frac{n!}{t!(n-t)!} \right) \right\rfloor$ біт.

Наприклад, за допомогою секретного ключа, тобто $y_0 = Key$. Рівноважне кодування перетворює двійковий вектор y_0 довжини m у двійковий вектор e_0 довжини n, причому $w(e_0) = t$.

Черговий стан генератора e_{i+1} також формується за допомогою рівноважного кодування. Для цього двійковий вектор s_i розбивається на дві частини: $s_i = y_{i+1} \| z_{i+1}$ (тут $\|$ – символ конкатенації), причому довжина двійкового вектора y_{i+1} дорівнює m. Решта $n-k-m$ біт утворюють вектор z_{i+1}, який подається на вихід генератора як елемент ПВП. Рівноважне кодування вектора y_{i+1} дозволяє сформувати стан e_{i+1} і обчислення повторюються.

Таким чином, на кожному кроці алгоритму формуються $n-k-m$ біт ПВП, причому завдання знаходження стану e_i генератора за відомим фрагментом ПВП пов'язане з вирішенням теоретико-складної проблеми синдромного декодування.

3. РЕЗУЛЬТАТИ ДОСЛІДЖЕНЬ

В ході експериментальних досліджень ставилося завдання оцінити період формованих ПВП. Для цього розглянуті вище генератори були програмно реалізовані для невеликих параметрів і виконано повний перебір всіх можливих векторів ініціалізації (секретних ключів). Для кожної ініціалізації сформована ПВП, оцінено її період. В результаті ми маємо повний набір всіх довжин періодів ПВП, які можуть бути породжені кожним генератором для відповідних вхідних параметрів.

3.1. Періодичні властивості генератора BBS

Для проведення досліджень періодичних властивостей розглянутих генераторів, експериментальні дослідження полягали у повному переборі всіх можливих значень вектора x_0, оцінці відповідних довжин пері-

оду L формованих ПВП та порівнянні з максимальною довжиною періоду $L_{\max} = \min\left(2^M - 1, n-1\right)$, де M – бітова довжина ключових даних (бітова довжина вектору x_0).

Під час проведення експериментальних досліджень генератора BBS було обрано такі вихідні дані.

Експеримент 1. Вихідні дані: $p = 19$, $q = 43$, $n = 817$. Як вектор x_0 обиралися всі цілі числа від 2 до 816.

Експеримент 2. Вихідні дані: $p = 131$, $q = 163$, $n = 21353$. Як вектор x_0 обиралися всі цілі числа від 2 до 21352.

Експеримент 3. Вихідні дані: $p = 523$, $q = 1031$, $n = 539213$. Як вектор x_0 обиралися всі цілі числа від 2 до 539212.

Експеримент 4. Вихідні дані: $p = 2039$, $q = 4099$, $n = 8357861$. Як вектор x_0 обиралися всі цілі числа від 2 до 8357860.

Отримані результати експериментальних досліджень узагальнені та наведені як діаграми на рис. 2–5. На діаграмах наведено розподіл кількостей K таких векторів x_0, які дають відповідне значення періоду L.

Таким чином, проведені експериментальні дослідження довели, що генератор BBS володіє істотним недоліком. Період сформованих ПВП менший за максимальний на 2–5 порядків (для введених загальних параметрів). При збільшенні бітового ініціалізуючого вектора різниця між максимальним та фактичним періодом формованих ПВП також збільшується. Слід також зазначити, що для кожного розглянутого випадку існують такі значення векторів x_0, при введені яких відповідний генератор формує катастрофічно погані послідовності з довжиною періоду, що дорівнює одиниці. Тобто можна стверджувати, що для цих значень (т .з. слабких ключів) генератор формує детерміновані послідовності і не виконує свої функції.

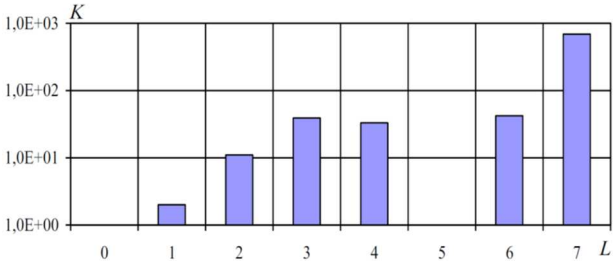

Рис. 2. Розподіл кількості K векторів x_0 по довжинах періодів формованих послідовностей (експеримент 1, $L_{\max} = 816$)

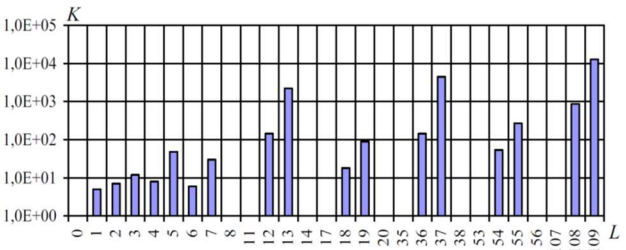

Рис. 3. Розподіл кількості K векторів x_0 по довжинах періодів формованих послідовностей (експеримент 2, $L_{\max} = 21352$)

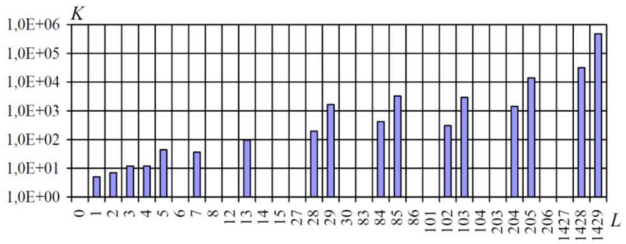

Рис. 4. Розподіл кількості K векторів x_0 по довжинах періодів формованих послідовностей (експеримент 3, $L_{\max} = 539212$)

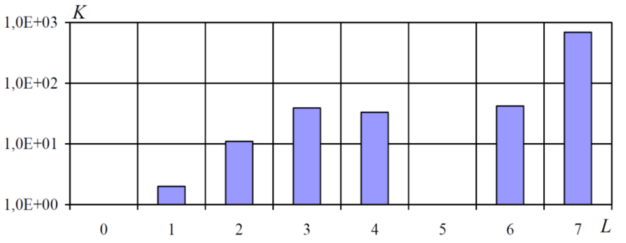

Рис. 5. Розподіл кількості K векторів x_0 по довжинах періодів формованих послідовностей (експеримент 4, $L_{\max} = 8357860$)

3.2. Періодичні властивості генератора RSA

Під час проведення експериментів обрано такі вихідні дані (рис. 6–9).

Експеримент 1. Вихідні дані: $p = 17$, $q = 37$, $n = 629$, $e = 257$. Як вектор x_0 обиралися всі цілі числа від 2 до 628.

Експеримент 2. Вихідні дані: $p = 131$, $q = 163$, $n = 21353$, $e = 1031$. Як вектор x_0 обиралися всі цілі числа від 2 до 21352.

Експеримент 3. Вихідні дані: $p = 521$, $q = 1031$, $n = 537151$, $e = 2029$. Як вектор x_0 обиралися всі цілі числа від 2 до 537150.

Експеримент 4. Вихідні дані: $p = 2053$, $q = 4099$, $n = 8415247$, $e = 2051$. Як вектор x_0 обиралися всі цілі числа від 2 до 8415246.

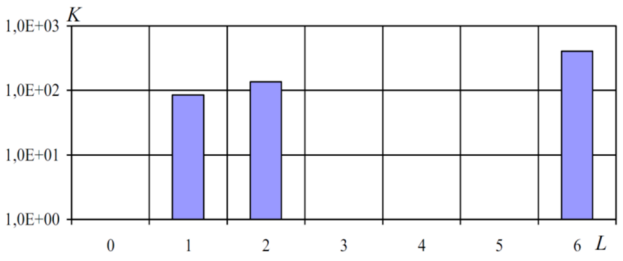

Рис. 6. Розподіл кількості K векторів x_0 по довжинах періодів формованих послідовностей (експеримент 1, $L_{\max} = 628$)

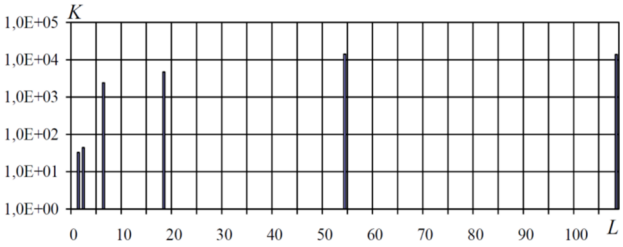

Рис. 7. Розподіл кількості K векторів x_0 по довжинах періодів формованих послідовностей (експеримент 2, $L_{\max} = 21352$)

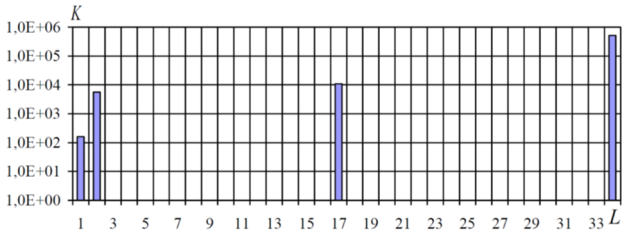

Рис. 8. Розподіл кількості K векторів x_0 по довжинах періодів формованих послідовностей (експеримент 3, $L_{\max} = 537150$)

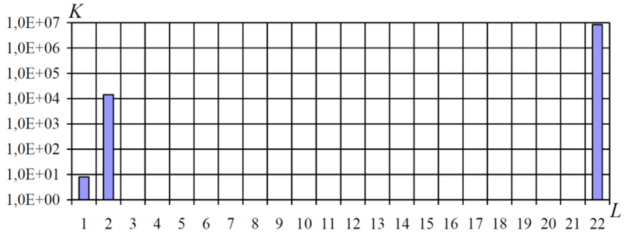

Рис. 9. Розподіл кількості ключів по довжинах періодів формованих послідовностей (експеримент 4, $L_{\max} = 8415248$)

За результатами експериментів з генератором RSA з'ясовано, що період сформованих ПВП також значно менший за максимальний. Наприклад, судячи із результатів експерименту 1 при максимальній довжині періоду $L_{\max} = 628$ фактична довжина періоду формованих послідовностей лежить у межах $L = 1..6$, тобто різниця між максимальним та фактичним періодом щонайменше у 100 разів. Судячи із експерименту 2 відповідні значення дорівнюють $L_{\max} = 21352$ і $L = 1..108$, тобто різниця між максимальним та фактичним періодом складає вже у 200 разів. У четвертому експерименті різниця між максимальним і фактичним періодом складає вже понад п'ять порядків. Генератор RSA також має слабкі ключі (вектори x_0), які призводять до катастрофічно низьких значень періоду сформованих послідовностей. Формована за допомого генератора Мікалі-Шнора ПВП за своїми періодичними властивостями не може бути кращою за ПВП, які формуються генератором RSA.

3.3. Періодичні властивості генератора Dual Elliptic Curve

Проаналізуємо роботу генератора ПВП, який використовує перетворення групи точок еліптичної кривої. Як приклад розглянемо випадок еліптичної кривої, яка задана рівнянням

$$y^2 \equiv x^3 - 3x + 4 \pmod 7,$$

причому виконується умова

$$4a^3 + 27b^2 = 2 (\text{mod } 7) \neq 0 (\text{mod } 7).$$

Ненульові точки (x_i, y_i) цієї кривої наведено у таблиці 1.

Таблиця 1

Множина ненульових точок еліптичної кривої

i	1	2	3	4	5	6	7	8	9
(x_i, y_i)	(0,2)	(0,5)	(1,3)	(1,4)	(3,1)	(3,6)	(4,0)	(5,3)	(5,4)

Припустимо, що як базові точки P і Q використовуються точки максимального порядку, наприклад, точки $P = (3,1)$ і $Q = (0,1)$. Побудуємо послідовність внутрішніх станів (2) та (3) та оцінимо періодичність цих послідовностей. Для спрощення вважатимемо, що функцію $\varphi(x)$ відображення елементів поля x у ненульові цілі числа задано як $\varphi(x) = x + 1$. Це припущення не накладає певних обмежень щодо кількості можливих неоднакових результатів відображення φ, оскільки за визначенням маємо функціональне співвідношення аргументу (елементи поля) та значення функції $\varphi(x)$ (деяке ціле число), тобто відображення є бієктивним і воно може бути подане як звичайна перестановка елементів поля. Додавання одиниці виключає формування нульового значення, виникнення якого переводить роботу генератора у вироджений стан (формується детермінована послідовність тільки нульових значень).

Отримані результати роботи генератора (значення внутрішніх станів) для всіх можливих початкових значень $s_0 = Seed$ наведено у табл. 2. Значення станів наводяться до першого повторення, бо решта значень є циклом. В останній колонці наведено період L фор-

мованих послідовностей станів, тобто найменша кількість елементів ПВП, через яку починається повторення.

Як видно із наведених даних періодичні властивості генератора ПВП незадовільні. Дійсно, отримані послідовності мають дуже малі значення періодів, в більшості послідовностей період дорівнює $L=2$, одна із послідовностей має період $L=1$, тобто на виході генератора формується одне й те саме значення. Хоча з огляду на порядок базових точок P і Q очікуване значення періоду дорівнює $L_{\max}=10$.

Таблиця 2

Внутрішні стани генератора та довжини періодів

$s_0 \setminus i$	i	**1**	**2**	**3**	**4**	**5**		***L***
$s_0=1$	s_i	4	2	6	2			2
	r_i	2	6	2	6			2
$s_0=2$	s_i	6	2	6				2
	r_i	2	6	2				2
$s_0=3$	s_i	1	4	2	6	2		2
	r_i	4	2	6	2	6		2
$s_0=4$	s_i	2	6	2				2
	r_i	6	2	6				2
$s_0=5$	s_i	5	5					1
	r_i	5	5					1
$s_0=6$	s_i	2	6	2				2
		6	2	6				2
		1	4	2	6	2		2
		4	2	6	2	6		2
		6	2	6				2
		2	6	2				2
		4	2	6	2			2
		2	6	2	6			2

3.4. Періодичні властивості генератора синдромного декодування

Для проведення експериментів були використані циклічні коди з наступними параметрами.

Експеримент 1. Вихідні дані: перевірна матриця довічного (15, 7, 5) коду. Як ініційована послідовність обиралися всі двійкові вектори довжини біт.

Експеримент 2. Вихідні дані: перевірна матриця довічного (15, 5, 7) коду. Як ініційована послідовність обиралися всі двійкові вектори довжини біт.

Експеримент 3. Вихідні дані: перевірна матриця довічного (31, 16, 7) коду. Як ініційована послідовність обиралися всі двійкові вектори довжини біт.

Експеримент 4. Вихідні дані: перевірна матриця довічного (31, 11, 5) коду. Як ініційована послідовність обиралися всі двійкові вектори довжини біт.

Отримані результати наведено як діаграми на рис. 10–13. На діаграмах наведено розподіли числа K різних векторів , які дають відповідне значення періоду ПВП. Максимальна (очікувана) довжина періоду становить біт.

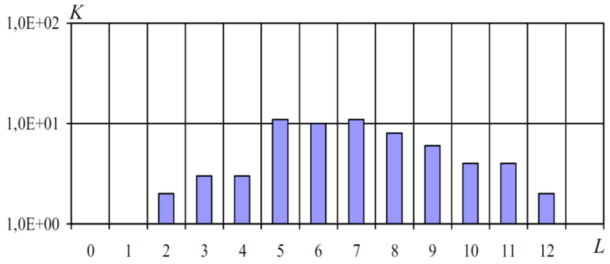

Рис. 10. Розподіл кількості ключів по довжинах періодів формованих послідовностей (експеримент 1, $L_{\max}=64$)

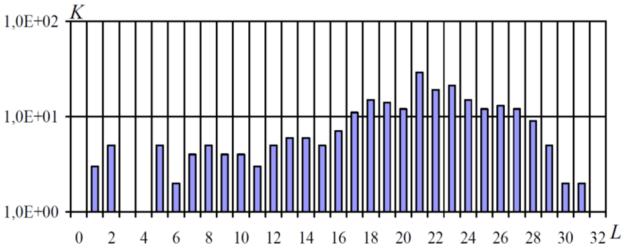

Рис. 11. Розподіл кількості ключів по довжинах періодів формованих послідовностей (експеримент 2, $L_{\max}=256$)

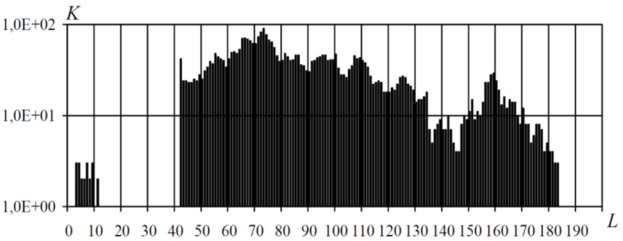

Рис. 12. Розподіл кількості ключів по довжинах періодів формованих послідовностей (експеримент 3, $L_{\max}=4096$)

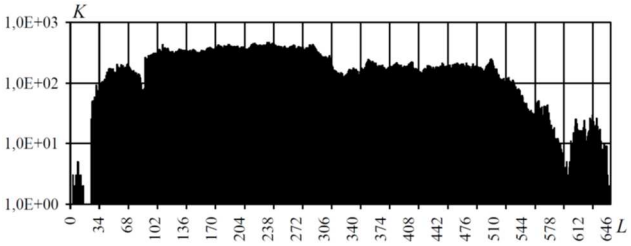

Рис. 13. Розподіл кількості ключів по довжинах періодів формованих послідовностей (експеримент 4, $L_{\max}=131072$)

Отримані результати показують, що генератор ПВП, заснований на проблемі синдромного декодування, також формує послідовності, період яких істотно нижче максимального. Це спостерігається у всіх розглянутих випадках і зі збільшенням довжини ініційованого вектора розбіжності між очікуваним і фактичним періодом збільшуються. Наприклад, для останнього випадку фактичний період менше максимального більш ніж в 200 разів.

4. ВИСНОВКИ

За результатами проведених експериментальних досліджень встановлено, що відомі доказово стійкі генератори ПВП володіють певними недоліками. Зок-

рема періоди формованих ПВП значно менші за максимальні. З підвищенням довжини вектора ініціалізації підвищується і розходження між очікуваною (максимальною) довжиною періоду і фактично спостерігаючими у формованих ПВП.

Таким чином, з огляду на високі криптографічні властивості доказово стійких генераторів актуальним є питання їх подальшого удосконалення з метою формування ПВП максимального періоду. Найбільш привабливим виглядає удосконалення генератора на синдромному декодуванні, оскільки він здатен протистояти квантовим методам криптографічного аналізу [11].

Література

[1] "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.

[2] *Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanstone.* Handbook of Applied Cryptography, CRC Press, 1997, 794 p.

[3] *A. Shamir.* "On the generation of cryptographically strong pseudorandom sequences". ACM Transactions on Computer Systems, vol. 1., 1983, pp. 38–34.

[4] *M. Blum, S. Micali.* "How to generate cryptographically strong sequences of pseudo-random bits". SIAM Journal on Computing, vol. 13, 1984, pp. 850–864.

[5] *L. Blum, M. Blum, M. Shub.* "A simple unpredictable pseudorandom number generator". SIAM Journal on Computing, vol. 15, 1986, pp. 364–383.

[6] *Elaine Barker and John Kelsey.* "Recommendation for random number generation using deterministic random bit generators". National Institute of Standards and Technology, January 2012, 124 p. [On-line]. Internet: https://doi.org/10.6028/NIST.SP.800–90A

[7] *Jean-Dernard Fisher, Jacques Stern.* "An efficient Pseudo-Random Generator Provably as Secure as Syndrome Decoding". EUROCRYPT'96 Proceeding, LNCS 1070, p. 245–255.

[8] *Elaine Barker and John Kelsey.* "Recommendation for random number generation using deterministic random bit generators". National Institute of Standards and Technology, June 2015, 101 p. [On-line]. Internet: https://doi.org/10.6028/NIST.SP.800-90Ar1

[9] *F. J. MacWilliams and N. J. A. Sloane.* The theory of error-correcting codes. North-Holland, Amsterdam, New York, Oxford, 1977, 762 p.

[10] *R.E. Blahut.* Theory and Practice of Error Control Codes. Addison Wesley Publishing Company, Inc., Reading, Massachusetts, 1983, 1983, 500 p.

[11] *D. Bernstein, J. Buchmann and E. Dahmen*. Post-Quantum Cryptography. Springer-Verlag, Berlin-Heidleberg, 2009, 245 p.

Надійшла до редколегії 10.10.2018

Кузнецов Олександр Олександрович, доктор технічних наук, професор, заступник головного конструктора ПАТ «ІІТ», професор кафедри безпеки інформаційних систем і технологій Харківського національного університету ім. В.Н. Каразіна. Галузь наукових інтересів – криптографія та автентифікація, алгебраїчна теорія кодів, обробка, передача та захист інформації.

Кіян Анастасія Сергіївна, магістрант кафедри безпеки інформаційних систем і технологій Харківського національного університету ім. В.Н. Каразіна. Галузь наукових інтересів – криптографія та автентифікація, алгебраїчна теорія кодів та кодові криптосистеми.

Прокопович-Ткаченко Дмитро Ігоревич, кандидат технічних наук, завідувач кафедри кібербезпеки Університету митної справи та фінансів. Заступник Голови Державної служби спеціального зв'язку та захисту інформації України (2013 – 2014 р.). Галузь наукових інтересів – інформаційна та кібербезпека держави, автентифікація та безпека безпроводових мереж.

Звєрєв Володимир Павлович, кандидат технічних наук, старший науковий співробітник, Помічник Голови Національної поліції України, Голова Державної служби спеціального зв'язку та захисту інформації України (2014 – 2015 р.). Галузь наукових інтересів – інформаційна та кібернетич-на безпека держави.

Котух Євген Володимирович, кандидат технічних наук, доцент, доцент кафедри кібербезпеки Університету митної справи та фінансів. Галузь наукових інтересів – кодова криптографія і автентифікація, обробка, передача та захист інформації.

Кузнецова Тетяна Юріївна, науковий співробітник кафедри безпеки інформаційних систем і технологій Харківського національного університету імені В.Н. Каразіна. Галузь наукових інтересів – криптографія і автентифікація, обробка, передача та захист інформації.

УДК 004.056.55

Кузнецов А. А. **Периодические свойства криптографически стойких псевдослучайных последовательностей /** А. А.Кузнецов, А. С. Киян, Д. И. Прокопович-Ткаченко, В. П. Зверев, Е. В. Котух, Т. Ю. Кузнецова // Прикладная радиоэлектроника: науч. – техн. журнал. – 2018. – Том 17, №. 3, 4. – С. 96–103.

В данной работе рассмотрены доказуемо стойкие генераторы псевдослучайных последовательностей, задача криптоанализа которых сводится к решению хорошо известной и очень сложной математической задачи, относящейся к

классу NP-сложных. В частности, рассмотрены генераторы Blum-Blum-Shub, Rivest-Shamir-Adleman, Dual Elliptic Curve и генератор на синдромном декодировании (Pseudo-Random Generator Provably as Secure as Syndrome Decoding). Исследованы периодические свойства формируемых псевдослучайных последовательностей. Показано, что рассмотренные генераторы не позволяют сформировать последовательности максимального периода. Кроме того, для каждого генератора существуют начальные состояния (слабые ключи), которые приводят к катастрофически малым длинам периодов формируемых последовательностей.

Ключевые слова: модель доказуемой безопасности, генератор псевдослучайных чисел, периодические свойства.

Табл. 2. Ил. 13. Библиогр.: 11 наим.

UDC 004.056.55

Kuznetsov O. O. **Periodic properties of cryptographically secure pseudorandom sequences** / O. O. Kuznetsov, A. S. Kian, D. I. Prokopovich-Tkachenko, V. P. Zverev, E. V. Kotuh, T. Yu. Kuznetsova // Applied Radio Electronics: Sci. Journ. – 2018. – Vol. 17, № 3, 4. – P. 96–103.

This paper considers evidentially secure pseudorandom sequences generators whose problem of cryptanalysis is reduced to solving a well-known and extremely complex mathematical problem that belongs to a NP-complex class. In particular, Blum-Blum-Shub, Rivest-Shamir-Adleman, Dual Elliptic Curve generators and that which is based on syndrome decoding (Pseudo-Random Generator Provably as Secure as Syndrome Decoding) are considered. The periodic properties of molded pseudorandom sequences are investigated. It is shown that the considered generators do not enable to form maximum period sequences. In addition, for each generator there are initial states (weak keys), which lead to catastrophically small lengths of periods of molded sequences.

Keywords: proof-security model, pseudorandom number generator, periodic properties.

Tabl. 2, Fig. 13. Ref.: 11 items.