УДК 681.324.067

ПОРІВНЯЛЬНИЙ АНАЛІЗ МЕТОДІВ ТА ЗАСОБІВ ТЕСТУВАННЯ ВИПАДКОВИХ ПОСЛІДОВНОСТЕЙ NIST 800-22 ТА NIST 800-90B

Р.І. МОРДВІНОВ

Проаналізовано вимоги, які висуваються у стандарті NIST 800-90B до джерела ентропії та генераторів випадкових біт. Наводиться порівняльний аналіз методик тестування, що описані у стандартах NIST 800-22 та NIST 800-90B. Описано методику тестування та їх порівняння.

Ключові слова: випадкова послідовність, псевдовипадкова послідовність, генератори випадкових послідовностей, детерміновані генератори псевдовипадкових послідовностей.

ВСТУП

У криптології безумовно визнано, що стійкість криптографічних систем суттєво залежить від якісних ключових даних, що використовуються в них. Первинною ознакою, що визначає якість ключових даних, є ентропія джерела ключів. По суті, вона визначає невизначеність початкового стану генератора ключових даних. Усі подальші властивості ключових даних, що генеруються таким генератором, залежать якраз від вказаної початкової ентропії.

У серпні 2012 року запропоновано стандарт NIST DRAFT Special publication 800-90B Recommendation for the Entropy Sources Used for Random Bit Generation [1]. У ньому описано рекомендації для джерел ентропії, які використовуються для генераторів випадкових бітів. Цей стандарт висуває ряд вимог до фізичних та детермінованих генераторів, пропонує ряд оцінок та тестів для послідовностей. Також наводяться методики для визначення мінімальної ентропії джерела. Розглянемо більш детально та зробимо порівняльний аналіз стандартів NIST 800-22 та NIST 800-90B. *Метою цієї статі є аналіз основних положень NIST DRAFT Special publication 800-90B, дослідження впливу початкової ентропії на криптографічні властивості ключових даних та розробка рекомендацій з його використання у перспективі.*

1. ОСОБЛИВОСТІ АНАЛІЗУ ВЛАСТИВОСТЕЙ ВИПАДКОВИХ ТА ПСЕВДОВИПАДКОВИХ ПОСЛІДОВНОСТЕЙ

Статистичні властивості ключових даних мають бути нерозрізнювані від випадкових послідовностей. Для визначення таких властивостей використовуються методики статистичного тестування. На сьогодні найбільш практичними та поширеними є FIPS-PUB 140-2 [2], AIS 20 [3], AIS 31 [4] та NIST STS [5].

Методика FIPS-PUB 140-2 має високу швидкість тестування, завдяки чому використовується в основному для оперативного контролю даних генератора під час його функціонування.

Методика AIS 20 використовується для даних з детермінованих генераторів випадкових послідовностей (ДГВБ). Має високу швидкість, через що може використовуватися для тестування в реальному часі.

Методика AIS 31 може використовуватися для тестування випадкових (фізичних) генераторів. Є надійною методикою та забезпечує результати, що і NIST STS. Має високу швидкість, тому може використовуватися для тестування генераторів у режимі реального часу.

NIST STS на сьогодні є одним з найпотужніших та найпоширеніших методик для тестування статистичних властивостей послідовностей. Відповідно останнього видання, до методики NIST STS входять 15 тестів, які, в ході використання всіх параметрів, на виході дають 188 результатів. Ця методика з великою ймовірністю дозволяє відбракувати псевдовипадкові дані, що не відповідають вимогам випадковим. Через велику складність в ході використання усіх тестів зі всіма параметрами, методика NIST STS не дає можливості використовувати тестування генераторів у реальному часі.

Порядок тестування послідовності згідно з NIST STS має такий вигляд:

1. Висувається нульова гіпотеза H_0 – припущення про те, що тестова двійкова послідовність є випадковою.

2. За послідовністю розраховується статистика тесту.

3. Із використанням спеціальної функції і статистики тесту розраховується значення імовірності $P \in [0,1]$.

4. Значення імовірності P порівнюється із рівнем значущості α, $\alpha \in [0,001; 0,01]$. Якщо $P \geq \alpha$, то гіпотеза H_0 приймається. В іншому випадку приймається альтернативна гіпотеза.

Таким чином, у результаті тестування псевдовипадкових бітів формується вектор значень імовірності $P = \{P_1, P_2, ..., P_{188}\}$. Аналіз складових P_i даного вектора дозволяє вказати на конкретні дефекти псевдовипадкових бітів, що тестуються. У стандарті рекомендованою довжиною є вхідний блок даних 10^6 біт; в одному тестуванні використовується 100 блоків такої довжини. Таким чином довжина вхідних даних для одного тестування складає 10^8 біт. Далі кожний з цих 100 блоків проходить тестування. Результати тестування зводяться до таблиці і мають вигляд 97/100, де 97 – кількість блоків, що пройшли тестування за конкретним тестом, а 100 – загальна кількість тестів. Для зручності використовується

раціональний вид, тобто 0.97. В NIST STS використовуються 2 пороги для результатів тестування – це 0.96 та 0.99, тобто для різних рівнів значущості дозволяється, що зі 100 блоків може не пройти 4 та 1 відповідно.

2. ОСОБЛИВОСТІ ТА РЕЗУЛЬТАТИ ЗАСТОСУВАННЯ СТАНДАРТУ NIST 800-90B

У стандарті NIST 800-90B описана велика кількість тестів. Для виявлення відхилень джерела шуму чи компонентів стану від розподілу при незалежному та стабільному поводженні використовується наступна процедура.

Набір даних довжини N поділяється на 10 підмножин, що не перекриваються та мають довжину $\left\lfloor \frac{N}{10} \right\rfloor$. Кожна з цих підмножин тестується та отримує бали за такою схемою:

- оцінка стиснення – один бал за підмножину даних;
- оцінка великих/малих серій – два бали за підмножину даних;
- оцінка «відвідувань» – один бал за підмножину даних;
- оцінка направлених серій – три бали за підмножину даних;
- оцінка коваріацій – один бал за підмножину даних;
- оцінка колізій – три бали за підмножину даних;
- тест хі-квадрат – прийняття/відбракування послідовності;

У даному стандарті тест з хі-квадрат має два тести – тест на незалежність даних та тест стабільності розподілу даних. Кожен з цих тестів повертає значення ok/fail у випадках проходження/відбракування послідовності.

Першою тестується оригінальна послідовність. Після цього проводиться ще 1000 тестувань з цією ж послідовністю, але після використання перемішування Фішера-Ейтса на кожному кроці. Таким чином формується вектор оцінок. Після цього цей вектор сортується по балах і виявляється положення оригінальних даних. Якщо оцінки оригінальної множини S даних співпадають з іншими, то положення оригінальної множини береться ближче до середини, тобто якщо оцінки множин Rank [482] = 34, Rank [483] = 34, Rank [484] = 35, а Rank [S] оригінальної множини дорівнює 34, тоді її положення Rank (S) = 483, та, якщо Rank [586] = 45, Rank [587] = 46, Rank [588] = 46, Rank [589] = 47, а Rank оригінальної множини дорівнює 46, то її положення Rank (S) = 587 відповідно.

Позиція оригінальної підмножини S повинна бути в інтервалі $50 \le \text{Rank (S)} \le 950$. Таким чином, якщо $\text{Rank (S)} \le 50$ чи $\text{Rank (S)} \ge 950$, то підмножина не проходить тест. Якщо 8 чи більше підмножин оригінальної множини не проходять тести, то джерело ентропії не проходить тести. Ця серія тестів направлена на виявлення недоліків та відхилень джерела ентропії від заданого розподілу. Якщо 8 або більше підмножин не проходять тестування – джерело відкидається.

Для порівняння результатів тестування як джерело ентропії було взято детермінований генератор випадкових послідовностей, заснований на БСШ ГОСТ 28147. Для тестування використовувалися послідовності довжиною 10^8 біт. Тестові дані генерувалися на при одних і тих же ключах та вхідних даних, але на різній кількості циклів шифрування. Всі послідовності були протестовані через обидві методики тестування. Вхідні дані для генератора створювалися за допомогою лічильника та мали велику збитковість «0» бітів.

Результати тестування занесені у таблиці 1–4. У лівій колонці зазначені тести, що були використані, у правій колонці результати у такому вигляді:

– для NIST STS 130/188 (69%), де 130 – кількість пройдених тестів для відповідного рівня значущості (0.96 чи 0.99), 188 – загальна кількість тестів, 69% – відсоток пройдених тестів;

– для NIST 800-90B 8/10, де 8 – кількість оцінок, для яких $50 \le \text{Rank (S)} \le 950$, 10 – загальна кількість результатів тесту.

Перша вхідна послідовність була взята на другому циклі шифрування. Результати тестування наведені у табл. 1.

Таблиця 1

Результати тестування 1-ї послідовності

NIST STS	Результати
Рівень значущості 0.99	0/188 (0%)
Рівень значущості 0.96	0/188 (0%)
NIST 800-90B	
оцінка стиснення	(9/10)
оцінка великих/малих серій	(4/10) (6/10)
оцінка «відвідувань»	(4/10)
оцінка направлених серій	(1/1) (1/1) (1/1)
оцінка коваріацій	(3/10)
оцінка колізій	(1/10) (5/10) (8/10)
тест хі-квадрат (незалежність даних)	FAIL
тест хі-квадрат (стабільності розподілу даних)	FAIL

Друга вхідна послідовність була взята на шостому циклі шифрування. Результати тестування наведені у табл. 2.

Таблиця 2

Результати тестування 2-ї послідовності

NIST STS	Результати
Рівень значущості 0.99	34/188 (18%)
Рівень значущості 0.96	89/188 (47%)
NIST 800-90B	
оцінка стиснення	(10/10)
оцінка великих/малих серій	(3/10) (7/10)
оцінка «відвідувань»	(8/10)
оцінка направлених серій	(1/1) (1/1) (1/1)
оцінка коваріацій	(4/10)
оцінка колізій	(9/10) (10/10) (9/10)
тест хі-квадрат (незалежність даних)	OK
тест хі-квадрат (стабільності розподілу даних)	FAIL

Третя вхідна послідовність була взята на сьомому циклі шифрування. Результати тестування наведені у табл. 3.

Таблиця 3

Результати тестування 3-ї послідовності

NIST STS	Результати
Рівень значущості 0.99	108/188 (57%)
Рівень значущості 0.96	174/188 (93%)
NIST 800-90B	
оцінка стиснення	(10/10)
оцінка великих/малих серій	(10/10) (10/10)
оцінка «відвідувань»	(10/10)
оцінка направлених серій	(1/1) (1/1) (1/1)
оцінка коваріацій	(7/10)
оцінка колізій	(10/10) (10/10) (10/10)
тест хі-квадрат (незалежність даних)	OK
тест хі-квадрат (стабільності розподілу даних)	FAIL

Четверта вхідна послідовність була взята з повноциклової версії шифру. Результати тестування наведені у таблиці 4.

Таблиця 4

Результати тестування 4-ї послідовності

NIST STS	Результати
Рівень значущості 0.99	145/188 (77%)
Рівень значущості 0.96	188/188 (100%)
NIST 800-90B	
оцінка стиснення	(10/10)
оцінка великих/малих серій	(10/10), (10/10)
оцінка «відвідувань»	(10/10)
оцінка направлених серій	(1/1) (1/1) (1/1)
оцінка коваріацій	(10/10)
оцінка колізій	(10/10) (10/10) (10/10)
тест хі-квадрат (незалежність даних)	OK
тест хі-квадрат (стабільності розподілу даних)	OK

ВИСНОВКИ ТА ПРОПОЗИЦІЇ ВІДНОСНО NIST 800-90B

– Деякі тести з NIST 800-90B не відображують дійсну картину статистичних властивостей вхідної послідовності. Це зумовлено тим, що результати тестування оригінальної послідовності порівнюються не з еталонними значеннями чи межами, а з тією ж самою послідовністю, у якій переставлені значення. Для послідовності, у якій кількість «0» та «1» бітів приблизно рівна, ця методика працюватиме, але при тестуванні послідовностей зі збитковістю тих чи інших – результати оригінальної послідовності не виділяються на фоні «перемішаних» послідовностей.

– Тести великих та малих серій, відвідувань та коваріацій дають більш чітку картину відносно статистичних властивостей послідовності. Перші 2 також є у методиці NIST STS.

– Згідно з алгоритмом в NIST 800-90B тест направлених серій виконується для всієї множини вхідних даних, без розбиття на 10 блоків, як робиться в інших тестах. Через це для відкидання джерела ентропії достатньо, щоб лише один з критеріїв не входив до заданого інтервалу.

– Тести для оцінки колізій виявили відхилення лише у послідовності з великою збитковістю «0» бітів. Коли кількість «0» та «1» бітів ставала приблизно рівною, оцінки тестування майже нічого не показували.

– Тести з використанням хі-квадрат критерію єдині, що порівнюються за еталонними результатами, через що лише вони вказували на статистичні властивості послідовності, а не порівнюють її з результатами цієї ж послідовності, в якій переставлені значення. Тести, що використовують критерій хі-квадрат, також використовуються методикою NIST STS.

– Методика тестування NIST 800-90B підходить для генераторів, в яких розподіл «0» та «1» бітів рівноймовірний. В іншому випадку деякі тести показують не зовсім правильну картину статистичних даних. Більш того, в стандарті написано, що ймовірність вийти за межі заданого інтервалу дорівнює 10%, а в деяких тестах, через те, що значення Rank (S) береться ближче до середини, будуть ще менші. Для відбракування джерела ентропії необхідно, щоб 8 або більше підмножин не пройшли тестування. Через це можна сказати, що, використовуючи лише оцінки, можна відбракувати тільки неякісні джерела ентропії, а послідовності 2 та 3 були відбраковані лише завдяки тестам з використанням критерію хі-квадрат.

Література

[1] NIST 800-90 b Recommendation for the Entropy Sources Used for Random Bit Generation, 2012.

[2] FIPS-PUB-140-2 security requirements for cryptographic modules, 1999.

[3] AIS20 Functionality Classes and Evaluation Methodology for Deterministic Random Number Generators, BSI, 1999.

[4] AIS31 Functionality classes and evaluation methodology for true (physical) random number generators, BSI, 2001.

[5] NIST 800-22 A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications, 2000.

Надійшла до редколегії 23.04.2013

Мордвінов Руслан Ігорович, аспірант кафедри БІТ Харківського національного університету радіоелектроніки. Наукові інтереси: розробка та застосування методів генерації випадкових послідовностей.

УДК 681.324.067

Сравнительный анализ методов и средств тестирования случайных последовательностей NIST 800-22 и NIST 800-90B / Р.И. Мордвинов // Прикладная радиоэлектроника: науч.-техн. журнал. – 2013. – Том 12. – № 2. – С. 250–253.

Проанализированы требования, описанные в стандарте NIST 800-90B к источнику энтропии и генераторам случайных бит. Приводится сравнительный анализ методик тестирования, которые описаны в стандартах NIST 800-22 и NIST 800-90B. Описана методика тестирования и сравнение.

Ключевые слова: случайная последовательность, псевдослучайная последовательность, генератор случайной последовательности, детерминированный генератор случайной последовательности.

Табл.: 4. Библиогр.: 5 назв.

UDC 681.324.067

Comparative analysis of methods and tools for testing random sequences NIST 800-22 and NIST 800-90B / R.I. Mordvinov // Applied Radio Electronics: Sci. Journ. – 2013. – Vol. 12. –№ 2. – P. 250–253.

The paper analyzes requirements of the standard NIST 800-90B to an entropy source and random bit generators. A comparative analysis of the testing techniques which are described in the standards NIST 800-22 and NIST 800-90B is conducted. The methodology of testing and comparison of testing methods is described.

Keywords: random sequence, pseudo-random sequence, random sequence generator, deterministic random sequence generator.

Tab.: 4. Ref.: 5 items.