УДК 681.324.067: 681.3.06

Ю.І. Горбенко[1], Т.О. Гріненко[2], О.П. Нарєжній[3]

[1] *Приватне акціонерне товариство «Інститут інформаційних технологій», Харків*
[2] *Харківський національний університет радіоелектроніки, Харків*
[3] *Харківський національний університет імені В.Н. Каразіна, Харків*

АНАЛІЗ СТАТИСТИЧНИХ ВЛАСТИВОСТЕЙ АПАРАТНОГО ГЕНЕРАТОРА ВИПАДКОВИХ ПОСЛІДОВНОСТЕЙ

Наводяться результати експериментальних досліджень властивостей випадкових послідовностей апаратного генератора. Відмічається доцільність застосування в сучасних обчислювальних системах фізичних датчиків шуму на основі резисторів або датчиків на основі кремнієвих діодів.

Ключові слова: *генератор випадкових послідовностей, детермінований генератор випадкових послідовностей, ключ, ключові дані, тестування.*

Вступ

Однією з основних умов забезпечення необхідного рівня гарантій криптографічної стійкості є застосування та відповідне управління ключовими даними. Рівень гарантій криптографічної стійкості дозволяє надавати з необхідною якістю такі базові послуги безпеки, як конфіденційність, цілісність, автентичність (справжність), неспростовність, доступність тощо.

В криптографічних системах створюються спеціальні підсистеми – джерела ключових даних і ключової інформації, а також здійснюється управління ключовими даними (ключами) [1].

Під ключовими даними (ключами) розуміється сукупність випадкових або псевдовипадкових значень змінних параметрів криптографічного перетворення інформації, за рахунок яких досягається мета цього перетворення (наприклад, зашифрування, розшифрування, обчислення криптографічного контрольного значення, обчислення електронного цифрового підпису, перевіряння електронного цифрового підпису, формування сертифікату відкритого ключа тощо).

Задача генерації випадкових і псевдовипадкових послідовностей, які використовуються в криптографії в якості ключів, загальносистемних параметрів та ін. вирішується за допомогою застосування високошвидкісних генераторів випадкових та псевдовипадкових послідовностей.

При цьому сучасна класифікація даних генераторів відображає як методи їх побудови, так і обрану термінологію. Відмінністю чисто випадкових послідовностей від псевдовипадкових є те, що псевдовипадкова послідовність може бути відновлена у просторі й часі.

Від якості випадковості формування ключів, ключової інформації та системних параметрів суттєво залежить криптографічна стійкість.

Аналіз стану генерування та тестування ключів

Загальним підходом до генерування ключів, ключової інформації та параметрів є стандартизація методів, механізмів і алгоритмів їх генерування. Вимоги до алгоритмів та реалізацій методів і засобів генерування і тестування послідовностей випадкових чисел визначаються:

– міжнародним стандартом ISO/IEC 18031 «Information technology – Random number generation» [2], який визначає алгоритми генерування псевдовипадкових і випадкових чисел, а також визначає статистичні тести перевірки генераторів;

– національним стандартом ДСТУ ISO/IEC 19790 «Інформаційна технологія – Методи захисту – Вимоги щодо захисту криптографічних модулів» [3];

– промисловими стандартами США (FIPS 140-3, ANSI X9.31, X9.44 та ін.).

Одним із важливих і необхідних напрямків досліджень і створення ефективних генераторів випадкових послідовностей (ГВП) та генераторів псевдовипадкових послідовностей (ГПВП) є розробка методів і засобів оцінки статистичних властивостей випадкових послідовностей (ВП). Статистичні показники мають вагомий вплив на загальну оцінку ГВП. По суті, статистичні показники та побудовані на їх основі критерії оцінки є інструментом перевірки правильності технічних рішень щодо побудови ГВП та забезпечення якості їх нерозрізнюваності.

Генеровані послідовності щонайменше мають бути випадковими, рівноймовірними, незалежними і формуватися на основі однорідних процесів. Розроблено значне число тестів, за допомогою яких можна визначити, чи є послідовність випадковою, але ніякий кінцевий набір тестів не вважають достатнім. Також результати статистичного тесту мають інтерпретуватися з деякою обережністю і застереженням, для того

щоб уникнути невірних висновків для певного генератора. На цей час найбільш доведеними та практичними до використання є методики тестування NIST STS [4], FIPS PUB 140-3, AIS 20 та AIS 31.

В роботі для тестування апаратного ГВП використовується методика NIST STS. Методика NIST STS застосовується як засіб комплексного контролю. Вибір цієї методики зумовлений тим, що вона містить необхідний набір статистичних тестів, сукупність яких обґрунтована, пропонує критерії прийняття рішення відносно не тільки окремої послідовності, але й відносно всього ГВП. Додатковим фактором вибору цієї методики є позитивний досвід її використання при дослідженні статистичних властивостей алгоритмів блокового і потокового шифрування, що висувалися на національний стандарт США і держав ЄС, а також власний досвід використання методики при тестуванні ГВП.

Фізичні генератори випадкових послідовностей

Складовим чи основним елементом генераторів ключів є фізичний генератор випадкових чисел. Фізичний генератор випадкових чисел (ФГВЧ) – пристрій, який генерує випадкові числа на основі фізичного процесу (тепловий шум, фотоелектричний ефект або квантові явища), який є абсолютно непередбачуваним. У деяких джерелах ФГВЧ називають недетермінованим генератором випадкових чисел (НГВЧ) або генератором випадкових чисел (ГВЧ).

Аналіз показав, що в сучасних криптографічних системах швидкість генерації випадкових послідовностей повинна перевищувати 1Мбіт/сек. Такі параметри можуть бути реалізовані на основі електронних датчиків шуму з широким спектром частот [1,5]. Випадкові зміни параметрів (тепловий шум) спостерігаються в усіх електронних компонентах при температурах вище абсолютного нуля за Кельвіном. Тому як фізичні датчики шуму можуть бути використані будь-які електронні компоненти.

В якості фізичного датчика шуму можна використовувати датчики шуму на основі резисторів, які генерують випадковий сигнал у смузі частот від одиниць Гц до сотень МГц з амплітудами вихідної напруги не більше 0,1 мВ [1,5]. Тому для сполучення з цифровими пристроями необхідно застосовувати підсилювачі з коефіцієнтом посилення за напругою в декілька тисяч разів. Споживна потужність такого датчика визначається в основному потужністю підсилювача і становить від десятків до сотень мВт при напрузі живлення від 5 до 15В. Перевагами датчиків шуму на основі резисторів є малі габаритні параметри, невеликі економічні витрати на виготовлення фізичного датчика шуму.

В якості генератора шумових напруг можна використовувати діод в діапазоні зворотних струмів [1,5]. Напівпровідниковий шумовий діод – це напівпровідниковий прилад, що є джерелом шуму із заданою спектральною щільністю в певному діапазоні частот. Наприклад, датчики шуму на основі кремнієвих діодів Зенеровського пробою (стабілітрони) генерують випадковий сигнал з рівномірним спектром від одиниць Гц до десятків МГц і амплітудами в десятки мВ. Такі прилади розроблені і випускаються як спеціалізовані шумові діоди із Зенеровським пробоєм (наприклад, КГ401). Вони при напрузі 8-9 В і струмі від 50 до 100 мкА генерують широкий спектр (до десятків МГц) випадкових імпульсів з амплітудами від 0,1 до 1В. Споживна потужність таких датчиків шуму менше 1 мВт при напрузі живлення від 10 до 20 В, що дозволяє легко вбудовувати їх в обчислювальні системи. Малогабаритні та економічні показники датчиків шуму на основі шумових діодів із Зенеровським пробоєм є одними з найкращих при реалізації в інтегральному виконанні на одному кристалі з обчислювальною системою.

Експериментальні дослідження властивостей випадкових послідовностей апаратного генератора електронного ключа «Кристал-1»

Одними з функцій пристрою електронний ключ (ЕК) «Кристал-1» є такі:

– генерація особистих і відкритих ключів для алгоритму ЕЦП;

– генерація особистих і відкритих ключів для протоколу розподілу ключів;

– генерація ключів для алгоритму шифрування та генерація випадкових послідовностей на основі апаратного генератора.

Для тестування статистичних властивостей випадкових послідовностей ЕК «Кристал-1» використовувалася методика NIST STS [4], рекомендована Національним інститутом по стандартизації й технологіям США, розроблена для статистичного тестування алгоритмів-кандидатів на AES (NIST SP 800-22). Пакет NIST STS містить у собі 16 статистичних тестів. Ці тести використовуються для перевірки гіпотези про випадковість двійкових послідовностей довільної довжини, породжуваних ГВП або ГПВП. По сукупності результатів всіх тестів приймається рішення про те, чи буде задана послідовність нулів і одиниць «випадковою» чи ні.

З використанням методики NIST STS було здійснено тестування випадкової послідовності ГВЧ ЕК «Кристал-1(Д)» і ГВЧ ЕК «Кристал-1(Т)», а також проведене порівняння властивостей цих послідовностей із властивостями ПВП генератора псевдовипадкових чисел BBS [4] (тестова вибірка, рекомендована NIST). Для здійснення тестування були обрані такі параметри:

1. Довжина послідовності, що тестується $n = 10^6$ біт.

2. Кількість послідовностей, що тестується $m = 100$. Таким чином, обсяг вибірки, що тестується, склав $N = 10^6 \times 100 = 10^8$ біт.

3. Рівень значимості $\alpha = 0{,}01$

4. Кількість тестів $q = 189$. Таким чином, статистичний портрет генератора містить 18900 значень ймовірності P.

В ідеальному випадку при $m = 100$ і $\alpha = 0{,}01$ може бути відкинута тільки одна послідовність зі ста, тобто коефіцієнт проходження кожного тесту повинен становити 99%. Але це занадто тверде правило. Тому застосовується правило на основі довірчого інтервалу для r_j [4]. Нижня границя в цьому випадку складе значення $r_{min} = 0{,}96015$. Із цих позицій проаналізуємо результати тестування, що представлені на рис. 1 – 3. На рис. 1 – 3 представлені статистичні портрети генераторів ВП та ПВП.

У табл. 1 наводяться дані по проходженню ВП тестів за правилом 1 [4]. У табл. 2 представлені зведені результати по проходженню генераторами тестів за правилом 2 [4].

Таблиця 1

Дані по проходженню тестів за правилом 1

Генератор	Кількість тестів, у яких тестування пройшли більше 99% послідовностей	Кількість тестів, у яких тестування пройшли більше 96% послідовностей
BBS	134 (70,8%)	189 (100%)
ГВП ЕК Кристал-1(Д)	134 (70,8%)	187 (98,9%)
ГВП ЕК Кристал-1(Т)	142 (75,13%)	189 (100%)

Таблиця 2

Дані по проходженню тестів за правилом 2

Генератор	Кількість тестів, у яких значення ймовірності $P \le 0{,}01$	Кількість тестів, у яких значення ймовірності $P \le 0{,}001$
BBS	0	0
ГВП ЕК Кристал-1(Д)	0	0
ГВП ЕК Кристал-1(Т)	0	0

.

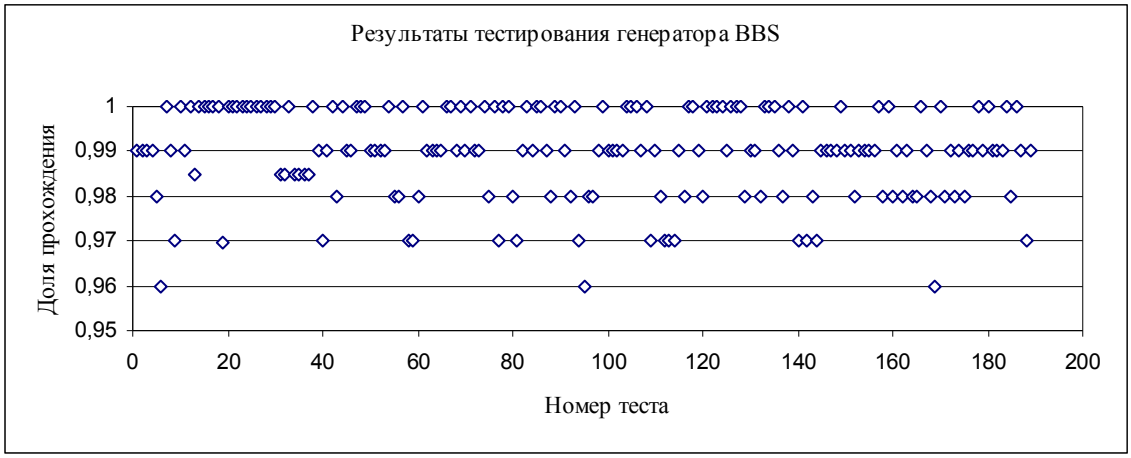

Рис. 1. Статистичний портрет генератора BBS

Рис. 2. Статистичний портрет генератора «Кристал-1 (D)»

Рис. 3. Статистичний портрет генератора «Кристал-1 (Т)»

Аналіз результатів тестування статистичних властивостей послідовностей показав, що генератор випадкових послідовностей ЕК «Кристал-1(Д)» пройшов 187 зі 189 тестів, а генератор ВП ЕК «Кристал-1(Т)» пройшов всі тести. Якщо застосовувати жорсткий критерій, тобто коли може бути відкинута лише одна послідовність зі ста, то кращий результат показав ЕК «Кристал-1(Т)».

Порівняльний аналіз результатів тестування статистичних властивостей послідовностей із властивостями ПВП генератора псевдовипадкових чисел BBS (тестова вибірка, рекомендована NIST) показав, що генератор ЕК «Кристал-1(Т)» має кращі характеристики.

Висновок

Аналіз основоположних джерел дозволяє зробити висновок, що необхідною умовою забезпечення криптографічної стійкості є формування ключів, ключової інформації та певних параметрів, що досягається використанням одночасно як засобів формування фізично випадкових, так і детермінованих випадкових послідовностей. Алгоритми генерації і тестування послідовностей випадкових чисел є базовими алгоритмами, що забезпечують дійсну криптографічну стійкість алгоритмів і механізмів криптографічного захисту інформації.

Аналізуючи отримані результати, можна зробити висновок про доцільність застосування в сучасних обчислювальних системах фізичних датчиків шуму на основі резисторів або датчиків на основі кремнієвих діодів. Їх малогабаритні та економічні показники є одними з найкращих при реалізації в інтегральному виконанні на одному кристалі з обчислювальною системою.

Список літератури

1. Горбенко І.Д. Прикладна криптологія. Теорія. Практика. Застосування. Монографія / І.Д. Горбенко, Ю.І. Горбенко. – Х.:Форт, 2012. – 878 с.

2. ISO/IEC 18031 Information technology — Security techniques — Random bit generation, 2005.

3. ISO/IEC 19790:2006. Information technology – Security techniques – Security requirements for cryptographic modules.

4. Ruhkin A.A. (2010). Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications. NIST Special Publication 800-22rev1a.

5. Торба А.А. Математические модели датчиков шума / А.А. Торба, В.А. Бобух, А.А. Торба // Прикладна радіоелектроніка. – 2007. – Т. 6, № 2. – С. 277-282.

Надійшла до редколегії 1.10.2015

Рецензент: д-р техн. наук, проф. Р.В. Олійников, Харківський національний університет ім. В.Н. Каразіна, Харків.

АНАЛИЗ СТАТИСТИЧЕСКИХ СВОЙСТВ АППАРАТНОГО ГЕНЕРАТОРА СЛУЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ

Ю.И. Горбенко, Т.А. Гриненко, А.П. Нарежний

Приводятся результаты экспериментальных исследований свойств случайных последовательностей аппаратного генератора. Отмечается целесообразность применения в современных вычислительных системах физических датчиков шума на основе резисторов или датчиков на основе кремниевых диодов.

Ключевые слова: *генератор случайных последовательностей, детерминированный генератор случайных последовательностей, ключ, ключевые данные, тестирование.*

ANALYSIS OF STATISTICAL PROPERTIES OF RANDOM SEQUENCES GENERATOR

U.I. Gorbenko, T.A. Grinenko, A.P. Narezshny

The experimental results of the random sequences generator hardware properties are showed below. The usefulness of modern computing systems of physical noise sensors based on resistors or sensors based on silicon diodes.

Keywords: *random sequence generator, deterministic random sequence generator, key, key data, testing.*