ОБГРУНТУВАННЯ ВИМОГ ДО МЕТОДІВ ГЕНЕРУВАННЯ ПСЕВДОВИПАДКОВИХ ПОСЛІДОВНОСТЕЙ

Гріненко Т.О., Мордвінов Р.І.
Харківський національний університет радіоелектроніки
61166, Харків, пр. Леніна, каф. Безпеки інформаційних технологій, тел. (057) 702-14-25,
E-mail: bit@kture.kharkov.ua, факс (057)7021425

It is grounded requirements to pseudorandom number generators. The research results concerning provided methods are based on hash functions, block cipher algorithms and number theoretic problems.

Генератори випадкових чисел, ймовірно, є одним із самих основних елементів криптографічних примітивів. Вони широко використовуються для генерування ключів, паролів, загальносистемних параметрів та ін. На практиці реалізацію отримали два основних методи генерування ключів – на основі використання випадкових чисел, що формуються з використанням фізичних випадкових процесів, та які не можуть бути відновлені в просторі та часі, та на основі використання псевдовипадкових чисел, що можуть бути відновленими в просторі і часі.

До детермінованих генераторів випадкових послідовностей (ДГВП) та методів, за якими формуються псевдовипадкові послідовності (ПВП) висунуто ряд вимог. Основними з них є: пряма та зворотна непередбачуваність чисел або структурна скритність, складність або швидкодія генерування, необоротність функції генерування ключа, під якою розуміється обчислювальна складність визначення ключа ДГВП, що застосовується, захищеність генератора від впливу на процес генерування ключа, а також забезпечення заданого періоду повторення ПВП. При цьому рівень гарантій в суттєвій мірі залежить від ентропії джерела ключів і на сьогодні вона повинна складати від 80 до 512 бітів. На наш погляд, цим вимогам значною мірою можуть задовольняти генератори ПВП, які розроблені з використанням переваг теоретико-числових задач (наприклад, задачі дискретного логарифма в групі точок еліптичних кривих) [1]. При забезпеченні вимог випадковості і/або непередбачуваності такого генератора рішення задачі криптоаналіза буде експоненційно складним. У загальному випадку для побудови генератора ПВП використовується однобічна функція. Для побудови таких однобічних функцій використовуються функції, складність яких ґрунтується на складності дискретного логарифму або на складності факторизації великого числа.

Зважаючи на актуальність та необхідність якісного забезпечення перелічених вимог на світовому та національному рівнях застосовується практика стандартизації вимог до методів, механізмів та засобів генерації та тестування ПВП [2-7].

Серед стандартів генерування випадкових послідовностей бітів уже визнаними на міжнародному рівні є ISO 19790 [2], ISO/IEC 18031 [3] та ANSI X9.98 [4]. В них з різною мірою деталізації визначені вимоги до ДГВП, методи та алгоритми їх реалізації на основі теоретико-числових задач, блокових симетричних шифрів та на основі перетворення з використанням необоротних колізійно стійких функцій.

Спираючись на описані в стандарті ДСТУ ISO/IEC 18031 схеми генераторів випадкових бітів були реалізовані генератори випадкових бітів на геш-функціях та в групі точок ЕК і перевірено їх статистичні характеристики за допомогою методики NIST STS. Результати тестування розглянутих ДГВП підтвердили високий рівень випадковості послідовностей, що були згенеровані в процесі досліджень.

Основними обмеженнями методів, що викладені в ISO 19790 та ISO/IEC 18031, є відсутність доведення стійкості генератора до компрометації ключа, що використовує цей генератор та непередбачуваності як до раніше, так і після генеруємих псевдовипадкових бітів. Необхідно також відмітити і недоліки конкретних методів генерування послідовностей ПВБ, що представлені в стандарті ISO/IEC 18031, тобто на основі блокових шифрів, вирішення теоретико-числових задач та гешування. При застосуванні методу, що

базується на використанні колізійно стійких функцій гешування залишаються проблемними питання визначення значення величини періоду повторення.

У табл. 1 наводяться дані по проходженню ПВП тестів за Правилом 1.

Таблиця 1.

Генератор	Кількість тестів, у яких тестування пройшли більше 99% послідовностей	Кількість тестів, у яких тестування пройшли більше 96% послідовностей
BBS	134 (71%)	189 (100%)
SHA1 (ISO/IEC 18031)	132 (69%)	188 (99%)
SHA2 256 (ISO/IEC 18031)	130 (68%)	187 (98%)
SHA2 384 (ISO/IEC 18031)	133 (70%)	189 (100%)
SHA2 512 (ISO/IEC 18031)	141 (74%)	189 (100%)
AES (ISO/IEC 18031)	138 (73%)	189 (100%)
DES (ISO/IEC 18031)	132 (69%)	188 (99%)
ГОСТ 28-147 (ISO/IEC 18031)	132 (69%)	188 (99%)
TDES (ISO/IEC 18031)	135 (71%)	189 (100%)
ДГВП на ЕК (ISO/IEC 18031)	129 (68,25%)	189 (100%)

У табл. 2 представлені зведені результати по проходженню генераторами тестів за Правилом 2.

Таблиця 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
SHA1 (ISO/IEC 18031)	0	0
SHA2 256 (ISO/IEC 18031)	0	0
SHA2 384 (ISO/IEC 18031)	3	0
SHA2 512 (ISO/IEC 18031)	0	0
AES (ISO/IEC 18031)	0	0
DES (ISO/IEC 18031)	4	1
ГОСТ 28-147 (ISO/IEC 18031)	1	0
TDES (ISO/IEC 18031)	3	0
ДГВП на ЕК (ISO/IEC 18031)	1	0

У [1] наведено удосконалений метод і алгоритми побудови ДГВП на основі використання криптографічних перетворень в групі точок ЕК над простими і розширеннями полів Галуа та застосування стійких до колізій функцій гешування, використання якого дозволить формувати ПВП з необхідними властивостями нерозрізнюваності та необоротності.

Задача оцінки необоротності запропонованого генератора у цілому по суті зводиться до послідовного вирішення двох задач – спочатку знаходження по відомому виходу генератора (геш-значення) його прообразу, а потім по відомому прообразу до вирішення задачі дискретного логарифмування в групі точок еліптичних кривих з визначенням секретного ключа генератора. Доказано, що складність обернення генератора ПВП на основі застосування гешування носить експоненційний характер. При цьому складність суттєво зменшується, якщо криптоаналіз здійснюється на основі створення колізій. Найбільш

складною є атака знаходження прообразу. Генератор ПВП, що ґрунтується на використанні як скалярного множення на еліптичній кривій так і гешування, має складність обернення більшу ніж атака «груба сила». Це означає, що для цього методу атака типу «груба сила» є найбільш ефективною з точки зору криптоаналітика.

Запропонований у [1] математичний апарат дозволяє також зробити оцінки ймовірностей виникнення колізій геш-значень точок еліптичних кривих, а також вибрати довжини геш-значень, наприклад, допустимі значення. При цьому необхідно враховувати, що на практиці довжини геш-значень є стандартизованими – 160, 256, 384 та 512 бітів, а також знайти обмеження на число символів випадкової послідовності бітів, які можуть генеруватись на одному і тому ж ключі.

Увага до генераторів псевдовипадкових послідовностей на ЕК з боку криптологів зростає. На наш погляд, для систем захисту інформації з доказовим рівнем стійкості та систем, які не потребують жорстких часових обмежень, найбільш придатним для застосування є генератор на еліптичній кривій, оскільки він має доказовий теоретичний рівень стійкості. Застосування математичного апарата груп точок ЕК дозволяє побудувати різні генератори ПВП. Основними методами формування ПВП є методи, що засновані на операціях додавання й множення в групах точок ЕК.

Література:

1. Гріненко Т.О., Горбенко Ю.І., Мордвінов Р.І. Властивості та перспективи застосування генераторів псевдовипадкових послідовностей на еліптичних кривих. – Системи обробки інформації. ХУПС. Вип. 2(92) – 2011. – С.76-80.

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

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

4. American National Standard for Financial Services ANSI X9.98 - 2010 Lattice-Based Polynomial Public Key Establishment Algorithm for the Financial Services Industry, 2010.

5. ANSI/X9 X9.82-3:2007. Random Number Generation, Part 3: Deterministic Random Bit Generators. Accredited Standards Committee X9 Incorporated, 11-Sep-2007 – 113 pages.

6. AIS 20. Functionality classes and evaluation methodology for Deterministic random number generators. BSI. 1999.

7. AIS 31. Functionality classes and evaluation methodology for true (physical) random number generators. BSI. 2001.