УДК 621.3.06

АНАЛІЗ ГЕНЕРАТОРА ПСЕВДОВИПАДКОВИХ ПОСЛІДОВНОСТЕЙ ЗАСНОВАНОГО НА БАГАТОРАЗОВОМУ ГЕШУВАННІ

Ю.І. ГОРБЕНКО, Д.Е. ХРЯПІН

Наводиться опис генератора псевдовипадкових послідовностей заснованого на багаторазовому гешуванні, визначеному в стандарті X9.98. Приводяться результати дослідження колізійних властивостей методу генерування. Продемонстровано доказ стійкості генератору проти атак різного виду та надаються рекомендації, щодо зміни конструкції генератора. Наводяться результати визначення швидкості генерації псевдовипадкових послідовностей. Надаються висновки, щодо використання методу генерування в системах захисту інформації.

Ключові слова: детермінований генератор випадкових послідовностей, гешування, статистичний портрет, швидкість генерування послідовностей.

ВСТУП

Суттєвими складовими інформаційних та інформаційно-телекомунікаційних систем, від властивостей яких залежить якість надання криптографічних послуг, є засоби генерування ключів та параметрів. Існуючі методи генерування ключів та параметрів можна розділити на два великих класи – генератори випадкових послідовностей (ГВП) та генератори псевдовипадкових послідовностей(ГПВП). Для двійкового алфавіту ГПВП в [1, 2] названо детермінованим генератором випадкових бітів (ДГВБ). Обидва вказані класи генераторів знаходять застосування, але більш широко використовуються ДГВП, по крайній мірі в частині інтенсивності їх використання.

До ДГВП висувається ряд вимог. В загальному ДГВП та ПВП, що ним генеруються, повинні задовольняти вимогам необоротності, нерозрізнюваності та непередбачуваності [1, 2]. Згідно вказаних вимог період повторення lz повинен бути не менше припустимого ln, ентропія джерела ключів $H(k)$ та безпечний час $t_б$ також не менше припустимих значень, тобто $H(k) \geq Hp(K)$ та $t_б \geq t_р$. Крім того, реалізація ПВП Yi повинна задовольняти вимогам випадковості, рівноймовірності, незалежності та однозначності, а також забезпечувати генерування бітів з допустимою складністю (швидкодією).

Проведений аналіз показав, що ДГВП, які засновані на функціях гешування, мають ряд переваг. Так, ДГВП можуть використовувати будь-яку криптографічну функцію гешування за умови забезпечення достатньої ентропії для початкового значення. Але для таких ДГВП необхідно генерувати, в тому числі згідно ключів (ключа), символи прообразів з довільним алфавітом послідовності прообразу, з завідомо заданим періодом повторення $l_р$, допустимою швидкодією (складністю) v генерування символів та стійкістю проти визначення закону генерування ДГВП, яку називають непередбачуваністю.

1. ІНСТАЛЯЦІЯ ПОЧАТКОВОГО СТАНУ ТА ГЕНЕРУВАННЯ ПВП

В [1, 2] розглянуті методи генерування ПВП, які спираються на двокаскадну схему. В них перший каскад забезпечує генерування послідовності з необхідним алфавітом та періодом повторення, а другий забезпечує необхідні властивості непередбачуваності, нерозрізнюваності та необоротності. В стандарті X9.98 [1] наведене криптографічне забезпечення системи NTRU, в тому числі математична модель двох каскадного ДГВП, в якому обидва каскади грунтуються на використанні функцій гешування. В цілому в стандарті визначено чотири рівня безпеки, кожен з яких визначається мінімальною ентропією початкової або повторної ініціалізації. Ці рівні безпеки можуть бути реалізовані засобом використання функцій гешування. В таблиці 1 наведено класифікацію та визначення функцій гешування у залежності від рівня безпеки. Рекомендовано використовувати функції гешування сімейства SHA (Secure hash) [2, 3].

Таблиця 1

Рівні безпеки у залежності від довжини геш значення

Рівень захисту	112	128	192	256
SHA-1	+	+	–	–
SHA-224	+	+	+	-
SHA-256	+	+	+	+
SHA-384	+	+	+	+
SHA-512	+	+	+	+

Вхідними даними алгоритму для генерування ПВП є:

– бітова строчка, з використанням якої отримують внутрішній стан генератора;

– додаткові дані – бітова строчка, яка призначена для внесення додаткової ентропії в внутрішній стан на протязі циклу роботи генератора;

– необхідний рівень захисту – ціле число яке вказує на рівень захисту, який повинен забезпечувати ДГВП (фактично вибір функції гешування та максимальної кількості запитів на генерацію за один сеанс);

– необхідна кількість бітів для генерації – ціле число, яке вказує на довжину бітової строчки, що повинна бути генерована на виході ДГВП.

З урахуванням вказаного алгоритм генерації може бути представленим у наступному вигляді:

1) *Ініціалізація внутрішнього стану*. Під час ініціалізації перевіряються усі значення

параметрів довжин на відповідність заданому рівню захисту, розраховуються наступні значення внутрішнього стану:

$$V = hash(0x01 \| seed\_length \| entropy\_input \| \| personalization\_string) \| \| \| hash(0x02 \| seed\_length \| \| entropy\_input \| personalization\_string) \| .... \| \| hash(seed\_length / hash\_outlen) \| \| \| seed\_length \| \| entropy\_input \| personalization\_string)$$

$$C = hash(0x01 \| seed\_length \| 0x00 \| V) \| \| hash(0x02 \| seed\_length \| 0x00 \| V) \| \| ..... \| hash(seed\_length / hash\_outlen \| \| seed\_length \| 0x00 \| V)$$

2) *Генерування вихідного значення.* Після отримання запиту на генерація та генерування ПВП на вихід подається наступне значення.

$$output = hash(V) \| hash(V+1) \| ... \| hash(V + + requested\_number\_of\_bits / hash\_outlen)$$

3) *Оновлення внутрішнього стану.* Якщо кількість оброблених запитів більш ніж максимально дозволена встановленим рівнем захисту, то внутрішній стан оновлюється за наступними згідно таких перетворень

$$V = hash(0x01 \| seed\_length \| 0x01 \| V \| entropy\_input \| \| additional\_input) \| \| \| hash(0x02 \| seed\_length \| 0x01 \| \| V \| entropy\_input \| additional\_input) \| ..... \| \| hash(seed\_length / hash\_outlen \| seed\_length \| 0x01 \| \| V \| entropy\_input \| additional\_input)$$

$$C = hash(0x01 \| seed\_length \| 0x00 \| V) \| \| hash(0x02 \| seed\_length \| 0x00 \| V) \| \| .... \| hash(seed\_length / hash\_outlen \| \| seed\_length \| 0x00 \| V)$$

В цілому перетворення, що подані 1) – 3) можна представити в вигляді алгоритму, блок-схема якого наведеної на рис. 1.

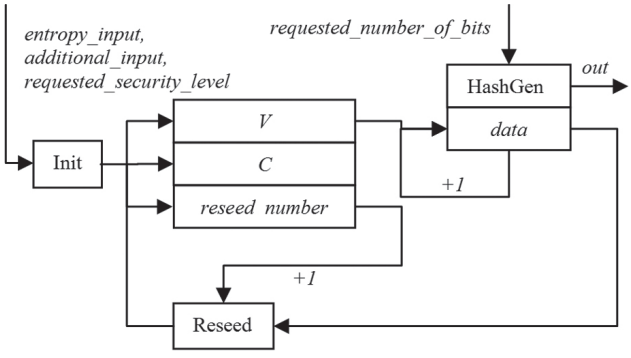

Рис. 1. Блок-схема генератора

1. АНАЛІЗ СТІЙКОСТІ ГЕНЕРАТОРА ПРОТИ АТАК

Проведемо аналіз стійкості ГПВП, що представлений на рис. 1, поклавши що він застосовується для генерації ключових даних, загально системних параметрів та даних в механізмах встановлення, узгодження, транспортування тощо ключів. Для вказаних криптографічних додатків було розроблено багато методів криптографічного аналізу генераторів. Тому актуальною є задача оцінки криптографічних якостей нерозрізнюваності, необоротності непередбачуваності та періоду повторення ПВП.

Для доказу стійкості генератора, що заснований на багаторазовому гешуванні, докажемо теореми для загального випадку (генератор заснованій на перетвореннях в підгрупах полів Галуа), а потім виконаємо змаштабування отриманих результатів на ДНВП, що досліджується. При розгляді будемо використовувати модель випадкового оракулу. В рамках цієї моделі криптоаналітик може знаходитися в декількох початкових станах, які будемо ранжувати за критерієм кількості відомої інформації про систему, тобто її ентропію. Криптоаналітик може находитись в наступних початкових умовах:

– відомі тільки загальносистемні параметри;
– відомі ЗСП та одне вихідне значення;
– відомі ЗСП та n вихідні значення;
– відомі ЗСП, n вихідних значений та один прообраз вихідного значення;
– відомі ЗСП, n вихідних значень и m прообразів вихідних значень.

Криптоаналітик може діяти, ставлячи перед собою одну з наступних цілей:

– отримати певне значення ;
– отримати значення сеансового ключа ;
– отримати значення начального ключа

Теорема 1 [1]. Якщо криптоаналітик володіючи максимальними знаннями про ДГВП на основі перетворень в підгрупі поля Галуа намагається отримати певне значення, то оракул, який він використовує для досягнення цією мети, можна використовувати для криптоаналізу циклової функції.

Доказ. Спираючись на структурну схему ДГВП на основі перетворень в підгрупі поля Галуа, що наведена на рис. 2, вихідне значення можна отримати використовуючи такий вираз

$$a_i = g^{K_k} f(a_{i-1}) \bmod p . \quad (1)$$

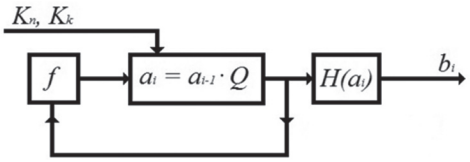

Рис. 2. Спрощена структурна схема ДГВП

Далі, вираз (1) можна перетворити до наступного вигляду:

$$g^{K_k} = \frac{a_i}{f(a_{i-1})}, \quad (2)$$

$$a_{i+k} = \frac{a_i f(a_{i+k-1})}{f(a_{i-1})} . \quad (3)$$

Аналіз (2) показує, що за умови використання не захищеної циклічної функції, складність отримання значення пошуку зводиться до

пошуку двох прообразів геш-значень. Такі задачі носять поліноміальний характер. При цьому, використовуючи (3), можна обчислити спираючись на знання трьох прообразів, довільний попередній, або наступний стан генератора. Так, якщо у аналітика є оракул, то можна отримати

$$f(a_{i-1}) = g^{K_k} \cdot a_i .$$

Але якщо в якості циклової функції використовується криптографічно стійка функція (стійке криптографічне перетворення, наприклад симетричне шифрування), то оракул аналітика виконує ефективний криптоаналіз симетричного шифру. Що у випадку використання, наприклад симетричного шифру, суперечить сучасному стану вирішення цієї задачі.

Теорема 2 [1]. Якщо криптоаналітик володіючи максимальними знаннями про ДГВП на основі перетворень в підгрупі поля Галуа намагається отримати значення, то оракул, який він використовує для досягнення цією мети, можна використовувати для вирішення дискретного логарифму в полі.

Доказ. Оракул, який може визначити сеансовий ключ генератора заснованого на перетвореннях в підгрупі поля Галуа та гешуванні можна використати для вирішення дискретного логарифму. Для цього на вхід оракулу необхідно подати ряд значень, що обчислюються за правилом:

$$a_0 = g^{K_k} ,$$

$$a_i = g^{K_k} \cdot f(a_{i-1}) .$$

Ця послідовність емітує послідовності, яку було генеровано ДГВП, у якого початковий і ключ сеансу не відрізняються. Таким чином оракул криптоаналітика, вирішує задачу дискретного логарифму в полі, що суперечить сучасному стану вирішення цієї задачі.

Таким чином загальна двокаскадна конструкція генератора є стійкою проти усіх можливих видів атак. Але використання менш стійкого перетворення на першому каскаді, зменшує рівень стійкості до поліноміального.

3. АНАЛІЗ ШВИДКОДІЇ ТА СТАТИСТИЧНИХ ВЛАСТИВОСТЕЙ ДГВП

Однією з основних вимог, що практично висуваються до ДГВП, та зрозуміло і до ПВП, є складність (швидкодія) її генерування. Для дослідження швидкодії було розроблено програмну модель ДГВП згідно математичної моделі, що мається в стандарті X9.98. В табл. 2 наведені дані відносно швидкодії такого ДГВП.

Порівняння даних табл. 2 з даними відносно швидкодії інших ДГВП такого ж призначення [4, 5], дозволяє зробити висновок, що вказаний генератор задовольняє вимогам відносно його до швидкодії. В той же час існує можливість оптимізації ДГВП по критерію швидкодії, в тому числі на рівні програмної моделі.

Таблиця 2

Швидкість генерації (Мгбіт /сек)

Геш-функція	SHA-1	SHA-256	SHA-512
Швикдоція	15,5	21,4	47,5

Зрозуміло, що основним критерієм безпеки відносно ДГВП є його характеристики нерозрізнюваності. Для дослідження якості нерозрізнюваності було використано NIST STS 800-22 [5]. На рис. 3–5 наведені фазові портрети ПВП

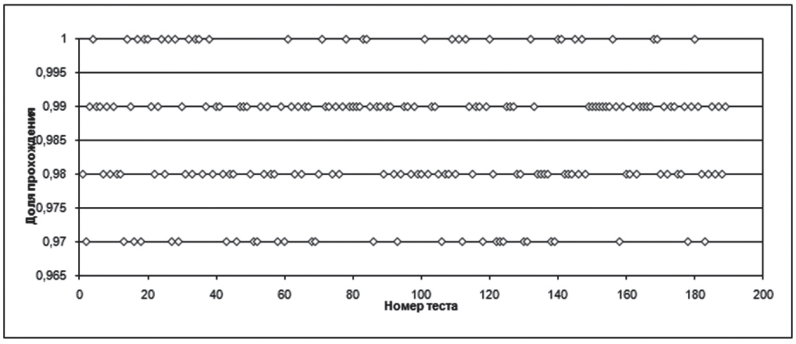

Рис. 3. ДГВП з геш-функцією SHA-1

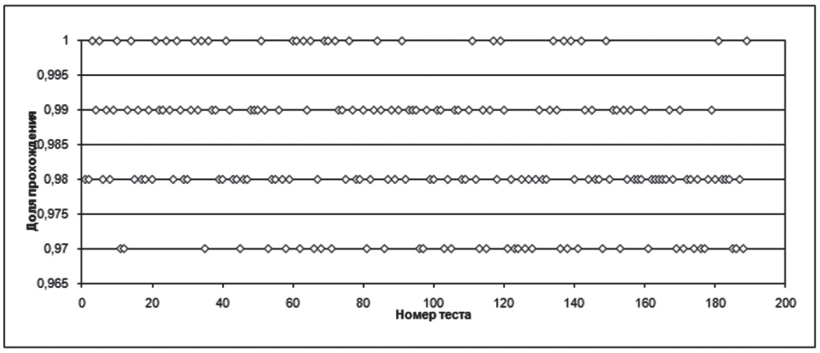

Рис. 4. ДГВП з геш-функцією SHA-256

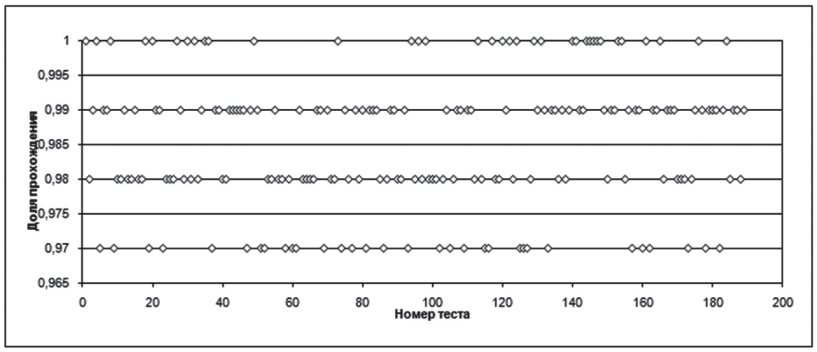

Рис. 5. ДГВП з геш-функцією SHA-512

ДГВП з різними функціями гешування, з застосуванням методики, що визначена в NIST STS. Їх порівняльний аналіз з даними відносно інших ДГВП [4], дозволяє зробити висновок що пропонуємий в стандарті X9.98 ДГВП є одним із кращих по критерію нерозрізнюваності.

ВИСНОВКИ

1) Більшість існуючих генераторів мають недоліки пов'язані з швидкодією генерації, або рівнем криптографічної стійкості методу генерації послідовностей. Перспективними для подальшого розвитку та актуальними для досліджень є генератори що засновуються на двокаскадній схемі. А саме отримання послідовності з необхідними властивостями та подальше гешування елементів цієї послідовності.

2) Представлений ДГВП має двокаскадну схему, яка складається з каскаду підготовки елементів та каскаду вхідного перетворення.

3) Проаналізований метод володіє високими показниками швидкодії, які зумовлені тим, що в якості фінального перетворення використовується геш функція.

4) Представлений ДГВП має високу криптографічну стійкість від атак різного вигляду. Це зумовлено тим, що криптографічна його стійкість спирається на складність вирішення криптографічних задачі пошуку прообразу геш значення.

5) Порівнюваний генератор володіє колізійними властивостями які задовольняють найжорсткішим вимогам дійсних стандартів в галузі безпеки інформації України та світовим вимогам.

Література

[1] American national standard for financial services (ANSI) X9.98. Lattice Based Polynomial Public Key Establishment Algorithm for the Financial Services Industry. – approved 2010-10-15. – ANSI, 2010. – 297 pages.

[2] Federal Information Processing Standards Publication (FIPS PUB) 180-2. Secure hash standard. – approved 2002-08-01. – NIST, 2002. – 76 pages.

[3] Federal Information Processing Standards Publication (FIPS PUB) 180-3. Secure hash standard (SHS). – approved 2008-10. – NIST, 2008. – 32 pages.

[4] *Горбенко І.Д.* Метод побудування випадкових бітів на основі спарювання точок кліптичних кривих / І.Д. Горбенко, Н.В. Шапочка, К.А. Погребняк // Журн. Прикладная радиоэлектроника. – 2010. – Т. 9, №3. – С. 386-394.

[5] NIST SP 800-22. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications. – 2001-09. – 164 pages.

Надійшла до редколегії 12.04.2012

Хряпін Дмитро Едуардович, магістрант кафедри БІТ ХНУРЕ. Область наукових інтересів: аналіз асиметричних криптосистем, методів генерування випадкових послідовностей і функцій гешування, генератори ПВП, асиметричні криптопримітиви в групі точок еліптичних кривих.

Горбенко Юрій Іванович, кандидат технічних наук, технічний директор ЗАТ «ІІТ», науковий співробітник НІЦ «Z» каф. БІТ ХНУРЕ. Область наукових інтересів: захист інформації в інформаційно-телекомунікаційних системах.

УДК 621.3.06

Анализ генератора псевдослучайных последовательностей основанного на многократном хешировании / Ю.И. Горбенко, Д.Э. Хряпин // Прикладная радиоэлектроника: науч.-техн. журнал. – 2012. – Том 11. № 2. – С. 184–187.

Проводится анализ генератора псевдослучайных последовательностей основанного на многократном хешировании. Приводятся результаты оценки криптографической стойкости генератора против атак разного вида, показатели быстродействия генерации последовательностей, и их статистические свойства.

Ключевые слова: детерминированный генератор случайных последовательностей, хеширование, статистический портрет, скорость генерации последовательностей..

Табл. 2. Ил. 5. Библиогр.: 5 назв.

UDC 621.3.06

Analysis of pseudorandom sequence generator based on multiple hashing / Yu.I. Gorbenko, D.E. Khriapin // Applied Radio Electronics: Sci. Journ. – 2012. Vol. 11. № 2. – P. 184–187.

Analysis of a pseudorandom number generator based on multiple hashing is performed. The paper presents results of evaluating cryptographic resistance of a generator against various kinds of attacks, indications of sequence generation speed and their statistical properties.

Keywords: determined random sequence generator, hashing, statistical portrait, sequence generation speed.

Tab. 2. Fig. 5. Ref.: 5 items.