УДК 681.324.067

МЕТОДИ ТА ЗАСОБИ ГЕНЕРУВАННЯ ПСЕВДОВИПАДКОВИХ ПОСЛІДОВНОСТЕЙ

Ю.І. ГОРБЕНКО, Н.В. ШАПОЧКА, Т.О. ГРІНЕНКО, А.В. НЕЙВАНОВ, Р.І. МОРДВІНОВ

Наводиться класифікація генераторів випадкових послідовностей, обґрунтовуються критерії та показники оцінки якості випадкових послідовностей, викладаються основні підходи до визначення випадкових та псевдовипадкових послідовностей, математичне визначення випадкових послідовностей.

Ключові слова: випадкова послідовність, псевдовипадкова послідовність, генератор випадкових послідовностей, детермінований генератор випадкових послідовностей.

ВСТУП

Незалежно від виду криптографічного перетворення, необхідними умовами забезпечення криптографічної стійкості є використання при генеруванні ключів, ключової інформації та загальних параметрів випадкових послідовностей (ВП) [1]. Вони використовуються для побудови довгострокових та разових ключів в симетричних та асиметричних криптографічних системах, ключової інформації, гам шифрування, ключів сеансів зв'язку, векторів ініціалізації (синхро послідовностей), генерації випадкових кортежів загальних параметрів тощо. В табл. 1 в якості прикладу наведено характеристики ключових даних та параметрів асиметричних криптографічних перетворень, які повинні також генеруватись випадково.

Методи генерування ключів, параметрів та ключової інформації, а також отримані з їх використанням послідовності можна поділити на 2 великих класи – випадкові (фізично) та псевдовипадкові [2]. Крім того, у залежності від використовуваної основи алфавіту m, символи генерованих послідовностей будемо називати бітами (m=2) *або числами* (m≥3). *Відповідно засоби, що забезпечують генерацію випадкових послідовностей чисел або бітів, будемо називати генераторами випадкових послідовностей (ГВП), а генератори, що забезпечують генерацію псевдовипадкових послідовностей (ПВП) – детермінованими генераторами випадкових послідовностей (ДГВП).*

Основними вимогами, що висуваються до ДГВП, є необоротність, нерозрізнюваність, непередбачуваність, просторова та тимчасова складність, відновлюваність в просторі і часі, гарантований період повторення, основа алфавіту тощо [3]. На наш погляд, на даний час задачі аналізу ДГВП залишаються не вирішеними, а також не визначені вимоги до ДГВП та ПВП. Зважаючи на складність вирішення цих задач та їх осмислення, вказані проблемні задачі і шляхи їх вирішення викладаються в серії статей, серед яких ця є першою.

Метою цієї статті є класифікація ГВП та ДГВП, аналіз стану стандартизації, визначення основних вимог до них, обґрунтування та вибір критеріїв та показників оцінки якості, викладення основних підходів до визначення випадкових та псевдовипадкових послідовностей, математичне визначення випадкових послідовностей, узагальнений порівняльний аналіз псевдовипадкових послідовностей, а також обґрунтування методичних основ дослідження (аналізу) псевдовипадкових послідовностей.

1. КЛАСИФІКАЦІЯ ТА МОДЕЛІ ГЕНЕРАТОРІВ ВИПАДКОВИХ ПОСЛІДОВНОСТЕЙ

У загальному сенсі, генератори випадкових послідовностей можна розділити на два типи у залежності від вибору джерела ентропії – змінного або фіксованого. Взагалі визначається два типи генераторів: випадкові (або не детерміновані) і детерміновані генератори випадкових послідовностей.

Генератори випадкових послідовностей. Генератор випадкових послідовностей – це механізм генерації випадкових послідовностей, у якому для

Таблиця 1

Ключі та загальні параметри асиметричні криптографічних перетворень

Параметри та вид перетворення	Особистий ключ	Відкритий ключ (сертифікат)	Асиметрична пара (ключ)	Загальні параметри	Сертифікати
Перетворення в кільці (RSA)	E_i	D_i	(E_i, D_i)	$N = PQ$	D_i
Перетворення в полі Галуа $F(P)$ (DSA)	X_i	$Y_i=g^{X}{}_i(\mathrm{mod}\ P)$	(X_i, Y_i)	P, q, g	Y_i
Перетворення в групі точок еліптичних кривих $E(F(q))$	d_i	$Q_i=d_iG(\mathrm{mod}q)$	(d_i, Q_i)	$a, b, G, n, f(x)(P), h$	Q_i

генерації випадкового потоку використовується джерело ентропії [4], що ґрунтується на фізично випадкових явищах чи випадковому явищі.

Класичним представником ГВП є фізичний генератор випадкових послідовностей. Фізичний ГВП – пристрій, який генерує випадкові послідовності на основі фізичного процесу (тепловий шум, фотоелектричний ефект або квантові явища тощо) [5], який являється абсолютно непередбаченим. Такий генератор містить внутрішнє фізичне джерело шуму. Частіше за все він виробляє аналоговий сигнал, який надалі дискретизується. Дискретизований шумовий сигнал при подальшій обробці перетворюється на внутрішню випадкову послідовність, щоб поліпшити розподіл ймовірності дискретизованої послідовності від шумових сигналів. Хороше фізичне джерело шуму може без додаткової обробки передавати дискретизований шумовий сигнал безпосередньо у вихідний блок. В ньому внутрішня випадкова послідовність відповідає дискретизованій послідовності шумового сигналу. Вихідний блок синхронізує безперервну або аперіодичну видачу внутрішньої випадкової послідовності з видачею символів випадкової послідовності. Ентропія випадкової послідовності, що видається джерелом шуму, підвищується з генерацією кожного символу випадкової послідовності. В цьому випадку ГВП представляється ідеальним ГВП [6]. Генератори випадкових послідовностей можуть будуватись на основі чисто фізичних явищ чи додатково з програмною реалізацією.

На рис. 1 показана функціональна блок-схема ГВП, яка визначена міжнародним стандартом ISO/IEC 18031 [7]. На блок-схемі пунктирні лінії вказують додаткові компоненти, які можуть включатися до складу ГВП в залежності від різних чинників. Показані компоненти не обов'язково мають бути реалізовані як фактичні фізичні компоненти, але вони мають реалізуватися функціонально [2]. До кожного з компонентів у стандарті висуваються вимоги, виконання яких дозволить забезпечити необхідний рівень захисту та забезпечити відсутність вразливостей, що пов'язані з генерацією випадкових послідовностей та можуть виникнути в криптографічних застосуваннях і середовищах.

Прикладами фізичних явищ можуть бути [8]:

1) теплові шуми з напівпровідникового діода або резистора;

2) час, що минув між емісією частинок під час радіоактивного розпаду;

3) частотна нестійкість осцилятора в режимі вільних генерацій;

4) ємність напівпровідникового конденсатора типу метал-ізолятор, що заряджається за фіксований період часу.

Генератори на базі перших двох явищ повинні бути побудовані зовні у вигляді пристроїв з використанням випадкових послідовностей і, отже, можуть піддаватися спостереженням або маніпуляціям зловмисника. Генератори на базі осциляторів і конденсаторів можуть бути побудовані на надвисоких інтегральних схемах – пристроях, що можуть бути захищені від несанкціонованого втручання.

В якості явищ, на яких можуть базуватися програмні ГВП, можуть бути [8]:

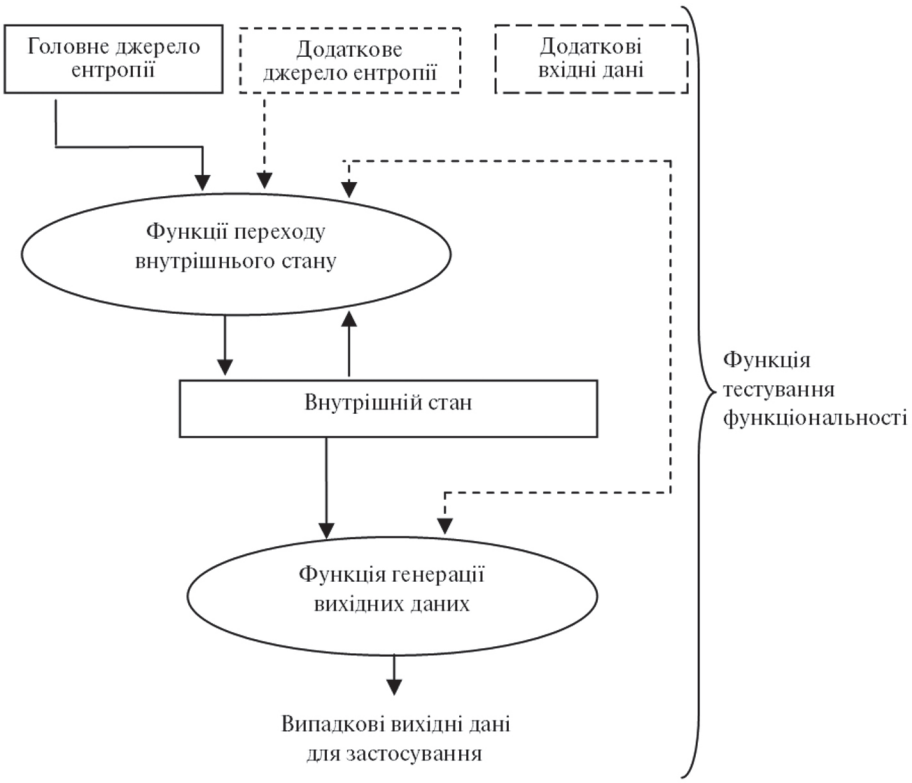

Рис. 1. Блок-схема генератора випадкових послідовностей

1) час, що минув між натисканнями клавіші або переміщенням миші;

2) системний годинник комп'ютера;

3) зміст буферів вводу/виводу;

4) параметри операційної системи, такі як системне навантаження і мережеві статистичні дані.

Детермінований генератор випадкових послідовностей. Детермінований генератор випадкових послідовностей є одним з базових примітивів для більшості криптографічних додатків, він забезпечує генерацію послідовностей, які називають псевдовипадковими. Однією з основних властивостей та переваг ДГВП є забезпечення відновлюваності послідовності в просторі і часі. В той же час ПВП повинні мати гарантовані властивості відносно періоду повторення, відновлення відрізків ПВП в просторі та часі, можливість проведення попереднього дослідження їх властивостей тощо [9].

На рис. 2 показана блок-схема функціональної моделі ДГВП [7]. Наведені елементи моделі не обов'язково мають бути реалізовані, наприклад, як фактичні окремі програмні підпрограми, але вони повинні бути функціонально реалізованими. До кожного з компонентів висуваються вимоги щодо запобігання вразливостей, що пов'язані з генерацією випадкових послідовностей та виникають у криптографічних додатках. При цьому необхідно враховувати, що ніякий детермінований алгоритм не може генерувати повністю випадкові послідовності, він може тільки апроксимувати деякі властивості випадкових послідовностей.

Клод Шеннон [10] показав, що симетрична схема шифрування (наприклад, шифр Вернама) безумовно-стійка тільки в тому випадку, якщо ключова послідовність k має рівномірний закон розподілу (будемо говорити, що вона генерується випадково, однорідно, має рівноймовірний розподіл, а біти (числа) є незалежними. Складність реалізації безумовно стійкої системи пов'язана з тим, що ключ повинен мати довжину, не меншу довжини повідомлення, що зашифровується. При використанні для зашифрування ПВП, довжина ключа суттєво зменшується, по суті на нинішній час її довжина не більше 512 бітів, а властивості ПВП близькі до фізично випадкової послідовності, тобто ПВП є практично нерозрізнюваною від випадкової послідовності. В той же час ПВП породжується деяким ДГВП на основі використання короткого ключа [9].

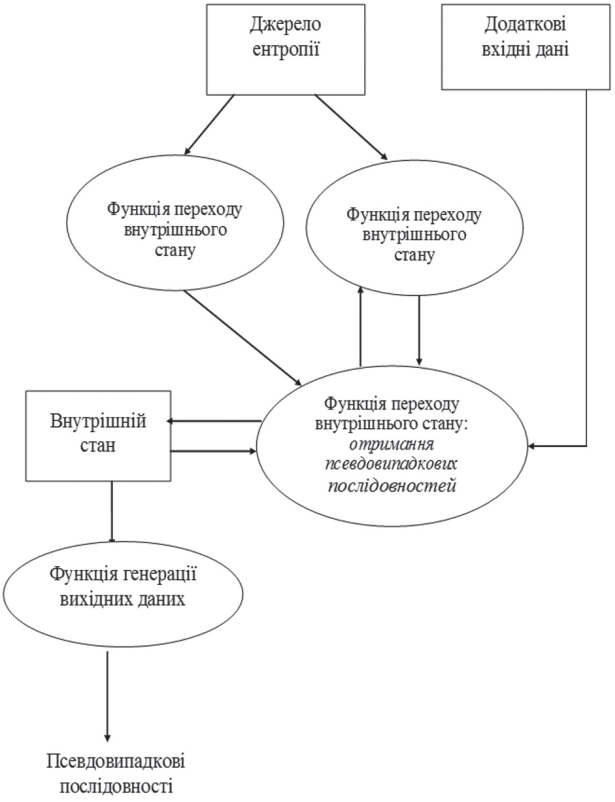

Рис. 2. Модель детермінованого генератора випадкових послідовностей

Можна говорити, що ДГВП забезпечує «розтягування» ключа в послідовність гами шифрування Γ_i. За певних умов при використанні Γ_i забезпечується криптоперетворення з гарантованим рівнем.

Більшість ДГВП мають багато серйозних недоліків, а послідовності, що ними генеруються, не відповідають вимогам, які висуваються криптографічними додатками. Основними з яких є:

– недопустимо короткий або недоведений період повторення послідовності Y_i;

– недостатній рівень необоротності відносно знаходження ключа K_i, що дозволяє вирішувати задачу знаходження Y_i з поліноміальною чи субекспоненціальною складностями, що є недопустимим;

– недостатня нерозрізнюваність Y_i, що також робить її певним чином передбачуваною «вперед та назад»;

– властивості випадковості, рівноймовірності, незалежності та однорідності не відповідають вимогам тощо.

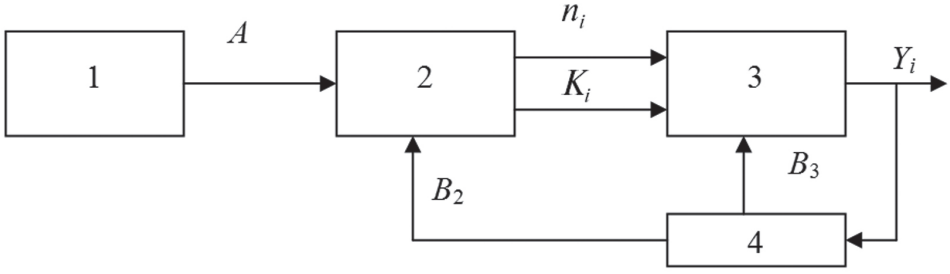

Рис. 3. Детермінований генератор випадкових послідовностей

В [11] висунуті вимоги до ДГВП та послідовностей, що ними генеруються, сутність яких зводиться до захищенності від таких основних атак, як:

– криптоаналітичні атаки знаходження початкового чи розгорнутих ключів;

– атаки, що зводяться до вирішення математичних задач, складність яких менше або суттєво менше атаки груба сила;

– атак, що засновані на вхідних даних генератора, які здійснюються засобом визначення або маніпулювання вхідними даними ГВП з метою впливу на вихідні дані (ключі, параметри тощо для інших криптографічних додатків);

– атаки, що зводяться до розповсюдження компрометованого стану генератора на інші стани – попередні чи майбутні;

– атаки, що засновуються на недопустимо обмеженому періоді повторення Y_i.

В той же час відомо, що будь-який ДГВП з обмеженими ресурсами може генерувати ПВП з наперед відомим періодом, можливо недопустимо коротким. Довжина циклів ДГВП залежить від самого генератора і в середньому складає приблизно $2^{n/2}$, де n – розмір внутрішнього стану в бітах, хоча лінійні конгруентні і LFSR-генератори забезпечують максимальні періоди порядку 2^n. Якщо ДГВП може сходитися до дуже коротких циклів, навіть з деякою ймовірністю, то такий ДГВП стає передбаченим і є непридатним.

2. ЕТАПИ СТВОРЕННЯ, ВИМОГИ ДО ДГВП ТА ЗАГАЛЬНА ХАРАКТЕРИСТИКА

Теорія ДГВП вперше була розроблена Блюмом, Мікалі [12] і Яо [13] на початку 1980-х років. Блюм і Мікалі [12] висунули вимоги, розробили загальну модель криптографічно-стійких ДГВП і запропонували першу конкретну реалізацію криптографічно-стійкого ДГВП під назвою генератор Блюма — Мікалі. Потім Яо [13] показав як побудувати криптографічно-стійкий ДГВП з використанням будь-якої односторонньої перестановки.

Хастад і інші [14] узагальнили цей результат і представили схему криптографічно-стійкого ДГВП, який ґрунтується на використанні будь-якої односторонньої функції. Згідно вищевказаних робіт побудувати ДГВП з односторонньою функцією не складно, тим більше, що в [14] висунуті необхідні і достатні умови існування ДГВП. Одностороння функція – це функція, яка дозволяє не вище ніж з поліноміальною складністю обчислити образ, а прообраз тільки з експоненційною складністю. Проте на сьогоднішній день не відомо про існування теоретично досконалих односторонніх функцій. Кращими видами односторонньої функції в реальності вважаються функції блокового шифрування і криптографічні геш-функції. Якщо послабити вимогу ефективного обчислення ДГВП, то можна знайти криптографічно-стійкі ДГВП, які проходять всі тестування поліноміального часу [15].

Келсі і інші [16] розглянули можливі криптографічні атаки на запропоновану модель ДГВП. Вони досліджували ДГВП з точки зору зловмисника і представили сильні і слабкі сторони чотирьох реальних ДГВП: ANSI X9.17, DSA, RSAREF і CryptoLib. Проте аналіз Келсі і інших був здебільшого спеціалізований і заснований на евристичних аргументах. Дісай, Хеві і Інь [17] надали загальну структуру захисту для ДГВП, об'єднавши атаки, про які зазвичай піклуються користувачі, і проаналізували генератори ANSI X9.17 і FIPS 186. В їх структурі захисту ДГВП розглядалися з точки зору доказового захисту, подібно тлумаченню захисту Беларе та інших [18, 19]. В роботі Десая-Хеві-Іня надається конкретний аналіз захисту для ДГВП, заснованих на ефективних криптографічних примітивах, таких як блокові шифри і геш-функції [15].

ДГВП, що засновані на геш-функціях, базуються на тому, що геш-функції є важко оборотними, практично мають експоненційну складність. Вказані ДГВП можуть використовувати будь-яку ISO/IEC криптографічну геш-функцію, що відповідає ISO/IEC 10118-3 [20], і можуть використовуватися застосуваннями, що вимагають різні рівні захисту за умови використання відповідної геш-функції і забезпечення достатньої ентропії для початкового значення [21]. Нині на міжнародному рівні проводиться заключний етап проекту створення перспективної геш-функції, значну перспективу мають кандидати на стандарт Skein і Blake [21].

До ДГВП, що засновуються на геш-функціях, висуваються такі припущення:

– вихідні дані геш-функції є випадковими для різних вхідних даних;

– початкове значення має відповідну ентропію, що заснована на необхідних бітах захисту, аж до максимуму бітової довжини вихідних даних геш-функції;

– ДГВП, що заснований на геш-функції, проектується відповідно різним рівням захисту в залежності від геш-функції, що використовується [21];

– довжина початкового значення дорівнює найбільшому розміру блоку гешованих вихідних даних;

– повинна існувати можливість використання геш-функції декілька разів, включаючи процеси ініціалізації і пере ініціалізації;

– повинна завжди використовуватися однакова геш-функція, яка відповідає або перевищує бажану стійкість, що висувається криптографічним додатком.

У табл. 2 наведено приклад затвердженої геш функції з ілюстрацією стійкості захисту, необхідної мінімальної ентропії і довжини початкового значення.

Загальна характеристика оцінки ДГВП, що засновані на блоковому шифрі, ґрунтується на використанні стандартизованих алгоритмів бло-

кового шифрування. ДГВП, що засновані на блоковому шифрі, описані в стандарті ISO/IEC 18031 [7]. При цьому, для обчислення геш-значення може використовуватись будь-який стандарт блокового шифрування, який відповідає вимогам, наприклад, ISO/IEC 18033-3 [22]. Причому при застосуванні блокових шифрів різного рівня стійкості може забезпечуватись і різний рівень стійкості ДГВП.

В табл. 3 надано вимоги до стійкості захисту, ентропії і початкового значення, якщо використовується AES із ISO/IEC18033-3.

ДГВП, заснований на блоковому шифрі, повинен ґрунтуватись на алгоритмі блокового шифрування в режимі лічильника, згідно вимог ISO/IEC 10116 [23]. Зрозуміло, що для всіх операцій повинні використовуватися одні і ті ж алгоритми блокового шифрування і довжина ключа.

ДГВП, що ґрунтуються на складності вирішення теоретико-числових задач (наприклад, задача дискретного логарифма, в тому числі в групі точок еліптичних кривих), має як певні особливості і переваги, так і певні недоліки. Якщо генератор розроблений з урахуванням властивостей асиметричного криптоперетворення, то характеристики випадковості і/або непередбачуваності такого генератора будуть гарантуватися складністю пошуку рішення такої задачі. До такого типу генераторів можна віднести подвійний ДГВП на еліптичній кривій і ДГВП Майклі-Шнорра [24].

Подвійний ДГВП на еліптичній кривій засновано на наступній важкій задачі [24], іноді відомій як «задача дискретного логарифму еліптичної кривої»: для заданих точок P і Q на еліптичній кривій порядку n необхідно знайти таке a, що $Q=aP$. Для ініціювання генерації *blocksize*-бітових псевдовипадкових послідовностей в подвійному ДГВП на еліптичній кривій використовується початкове значення m-бітової довжини, а безпосередньо генерування ПВП виконується з використанням операції скалярного множення двох точок в групі точок еліптичних кривих. Такий алгоритм є необоротним навіть у випадку компрометації його внутрішнього стану. Пряма секретність також забезпечується, але тільки при аналізі з використанням даних, що доступні за межами ДГВП.

ДГВП Майклі-Шнорра є варіантом так званого RSA генератора, який ґрунтується на криптографічному перетворенні в кільці. Його сутність полягає у наступному. Нехай $\gcd(x,y)$ є найбільший загальний дільник цілих x і y, і $\phi(n)$ є функція Ейлера. Позначимо n – добуток двох різних великих простих чисел; і e – позитивне ціле число, таке, що $\gcd(e,\phi(n))=1$. Визначимо $f(y)=y^e \bmod n$. Починаючи з початкового числа y_0 утворюємо послідовність $y_{i+1}=f(y_i)$ і виводимо рядок, що складається з $k=\lg\lg(n)$ найменших значущих бітів кожного y_i. Як відомо, ці біти (асимптотичні в n) захищені настільки, наскільки захищена RSA функція крипто перетворення f.

Генератор Майклі-Шнорра використовує одні і ті ж значення e і n для формування більшої кількості випадкових бітів на ітерацію, в той же час виключаючи багаторазове одночасне використання бітів як вихідних даних і як початкового числа. Кожне $y_i \in [0,n)$ представляється як конкатенація $s_i \| z_i$ r – бітового числа s_i і k – бітового числа z_i (де $k=\lg(n)-r$). s_i використовується для розподілу цілої послідовності: $y_{i-1}=s_i^e \bmod n$; z_i виводяться як випадкові біти. Відмітимо, що r повинно бути як мінімум $2(\min\{strenght, \lg(n)/e\})$, де $strenght$ є необхідною стійкістю захисту генератора, і $e \geq 3$. Випадкове r-бітове seed s_0 використовується для ініціації процесу. Довжини r і k, RSA-модуль n і значення експоненти e є змінними в певних межах. Межі засновані на бажаній стійкості вироблюваних бітів. Для максимальної ефективності з точки зору складності (швидкості) e повинно бути малим, а k – великим.

Таблиця 2

Значення стійкості, необхідної мінімальної ентропії і довжини початкового значення геш-функції

Геш-функція	Стійкість захисту	Мінімальна необхідна ентропія	Довжина початкового значення
Secure Hash	80	120	256
	112	120	256
	128	128	256
	192	192	256
	256	256	256

Таблиця 3

Значення стійкості захисту, ентропії і початкового значення для ISO затвердженого блокового шифру

Алгоритм блокового шифрування	Стійкості захисту	Необхідна мінімальна ентропія	Довжина початкового числа (у бітах)
AES-128	80, 112, 128	128	256
AES-192	80, 112, 128, 192	192	320
AES-256	80, 112, 128, 192, 256	256	384

3. АНАЛІЗ СТАНУ СТАНДАРТИЗАЦІЇ ГЕНЕРАТОРІВ ВИПАДКОВИХ ПОСЛІДОВНОСТЕЙ

На нинішній час загальним підходом до методів, механізмів та засобів генерування ключів, ключової інформації та параметрів є їх стандартизація та уніфікація. Причому, як можна судити із ряду джерел [1, 25-27], ці методи, механізми та алгоритми стараються захистити від розповсюдження, особливо в частині генерування випадкових послідовностей. Таке ж відношення до початку XXI століття було і відносно псевдовипадкових послідовностей. В останні роки, у зв'язку із суттєвим розвитком інфраструктури відкритих ключів, виникла потреба в створенні апаратних, апаратно-програмних та програмних засобів генерування ключів. Розроблені та прийняті спочатку регіональні [6, 28, 29], а потім і міжнародні стандарти [7, 30], в яких були визначені вимоги, методи, механізми та алгоритми реалізації ДГВП. Причому, у зв'язку з необхідністю відновлення ключів та ключової інформації в просторі і часі, в указаних джерелах в повному обсязі розглядаються ДГВП, що генерують відповідно псевдовипадкові послідовності.

Кращими, і, як наслідок, визнаними на міжнародному рівні, є три різні методи і ДГВП, побудовані на їх основі, що викладені в ISO/IEC 18031 [7]. Вони базуються на використанні: алгоритмів блокового симетричного шифрування; функцій гешування певної послідовності символів та застосування асиметричних крипто перетворень, наприклад, перетворення в групі точок еліптичних кривих (ЕК), а також за необхідності гешування координат точок еліптичних кривих тощо.

Існує декілька підходів до визначення вимог до рівнів гарантій ДГВП. Перший підхід пов'язаний з тестуванням ПВП на нерозрізнюваність, для чого, наприклад, застосовуються федеральні стандарти FIPS 140-1, FIPS 140-2, FIPS 140-3. Більш детальними є вимоги та механізми реалізації, що визначені в AIS 20, що дозволяє реалізувати різні рівні гарантій – K1, K2, K3, K4 [29]. При цьому самим вищим рівнем гарантій являється рівень K4. В AIS 31 відносно випадкових послідовностей визначено два рівня гарантій P1 і P2, в яких, по суті, P1 дещо еквівалентний K1, K2, а P2 еквівалентний K3, K4. У випадку рівня гарантій K4 вимагається, щоб ПВП мали статистичні властивості, подібні до статистичних властивостей ПВП, що генеровані ідеальним ДГВП, а також була заданою ентропія джерела ключів (тобто наявність та певна довжина ключа генератора є обов'язковими), а також повинна бути практично виключена можливість обчислення попередніх та наступних послідовностей генератора при знанні поточного стану, тобто задані нерозрізнюваність, необоротність та непередбачуваність. В табл. 4 наведено порівняння функціональних класів з використанням AIS 20, що призначений якраз для оцінки ДГВП.

4. КРИТЕРІЇ ТА ПОКАЗНИКИ ОЦІНКИ ЯКОСТІ ДЕТЕРМІНОВАНИХ ГЕНЕРАТОРІВ ВИПАДКОВИХ ПОСЛІДОВНОСТЕЙ

Під критерієм будемо розуміти ознаку, на основі якої здійснюється оцінка, визначення чи класифікація чого-небудь, тобто, по суті, будемо розуміти мірило оцінки. Попередні дослідження дозволили зробити висновок, що порівняння криптографічних перетворень можна здійснити з використанням двох сукупностей критеріїв: безумовних та умовних. З урахуванням попереднього досвіду, оцінку криптоперетворень типу ДГВП рекомендується виконувати в 2 етапи. На першому етапі перевіряється їх відповідність безумовним критеріям, а на другому отримуються відповідні інтегральні оцінки з використанням умовних критеріїв.

До безумовних критеріїв будемо відносити ті критерії, виконання яких для ДГВП є обов'язковим, тобто безумовним. Аналіз стану застосування, досвід розроблення й оцінки властивостей ДГВП, досягнуті результати при практичному розв'язанні задач крипто аналізу та реалізації різних атак дозволяють в якості основних вибрати, як мінімум, такі безумовні критерії оцінки:

– надійність математичної бази, що застосовується в ДГВП;

– практична захищеність ДГВП від відомих атак;

– реальна захищеність ДГВП від усіх відомих та потенційно можливих крипто аналітичних атак;

– статистична безпечність ДГВП;

Таблиця 4

Порівняння функціональних класів ДГВП

Функціональний клас	Вимоги до ДГВП	Криптографічні додатки, у яких застосовуються ДГВП відповідного класу
K1	K1(i)	Інтерактивні криптопротоколи встановлення ключів, автентифікації, розподілу таємниці тощо
K2	K1(i)+ K2(ii)	Симетричні потокові шифри
K3	K1(i)+ K2(ii)+ K3(iii)+ K3(iv)	Генерація ключів сеансу, цифрового підпису чи направленого шифрування (секретний ключ *x* або випадкове число *k DSA*, *EC DSA*), генерація паролів тощо
K4	K1(i)+ K2(ii)+ K3(iii)+ K3(iv)+ K4(v)	Генерація ключів сеансу, цифрового підпису чи направленого шифрування (секретний ключ *x* або випадкове число *k DSA*, *EC DSA*), генерація паролів, генерація ключів сеансу для симетричних криптографічних механізмів тощо

– непередбачуваність ПВП (вперед і назад), що генеруються ДГВП;

– відсутність слабких таємних (особистих) ключів;

– складність генерування носить не вище за поліноміальний характер.

Розглянемо більш детально ці критерії, як у частині понять та визначень, так і в частині особливостей застосування.

1. Надійність математичної бази, у розумінні відсутності в порушника можливостей здійснювати атаки типу «універсальне розкриття» за рахунок недосконалості математичної бази ДГВП або слабкостей, що можуть бути закладені за рахунок специфічних властивостей загальних параметрів і ключів. При цьому критерієм оцінки надійності математичної бази є той факт, що складність атаки «універсальне розкриття» $I_{\text{ур}}$ має експоненційний характер, а критерієм ненадійності – субекспоненційний або поліноміальний характер складності. Будемо позначати цей критерій $W_{\delta 1}$.

2. Практична захищеність ДГВП від відомих силових і аналітичних атак, яка досягається за рахунок вибору розмірів загальних параметрів і ключів. Тобто критерієм практичної захищеності ДГВП є вибір таких розмірів загальних параметрів і ключів, за яких складність атаки $I_{\text{са}}$ суттєво (на необхідне число порядків) перевищує існуючу потужність крипто аналітичних систем на рівні технологічно розвинутих держав (порушника третього рівня), у тому числі з урахуванням прогнозу збільшення потужності крипто аналітичних систем за рахунок розвитку математичного та програмного забезпечення тощо. Позначимо цей безумовний критерій $W_{\delta 2}$.

3. Реальна захищеність ДГВП від усіх відомих та потенційно можливих крипто аналітичних атак, де під захищеністю розуміють той факт, що всі відомі крипто аналітичні атаки типу «повне розкриття» мають експоненційну складність $I_{\text{ес}}$, а під критерієм незахищеності – субекспоненційний $I_{\text{се}}$ і нижче характер складності атаки «повне розкриття». Будемо позначати цей безумовний критерій $W_{\delta 3}$ та розуміти під ним оцінку необоротності.

4. Статистична безпечність ДГВП, під якою розуміють статистичну незалежність вихідних значень (виходу) генератора, наприклад, від вхідних. Будемо позначати цей безумовний критерій $W_{\delta 4}$.

5. Непередбачуваність «вперед та назад», під якою розуміється відсутність атак, що пов'язані з визначенням як майбутніх та минулих ПВП, складність яких менша, ніж складність атаки типу «повне розкриття». Цей безумовний критерій будемо позначати $W_{\delta 5}$.

6. Відсутність слабких особистих (таємних) ключів ДГВП, за яких складність крипто аналітичних атак типу «повне розкриття» та «універсальне розкриття» є меншою, ніж складність атаки «повне розкриття» для інших (не слабких) особистих ключів. Позначимо цей безумовний критерій як $W_{\delta 6}$.

7. Складність генерування $I_{\text{ген}}$ носить поліноміальний характер і не перевищує допустимої величини $I_{\text{д}}'$. Позначимо цей безумовний критерій також $W_{\delta 7}$.

Так як наведені часткові критерії є безумовними, то інтегральним критерієм добору є логічна зміна так/ні (1/0), і безумовний критерій можна записати у вигляді:

$$(W_{\delta 1}, W_{\delta 2}, W_{\delta 3}, W_{\delta 4}, W_{\delta 5}, W_{\delta 6}, W_{\delta 7}) \in (1,0). \quad (1)$$

З урахуванням наведених вище часткових безумовних критеріїв $W_{\delta 1} - W_{\delta 7}$ та умови (1) функцію відповідності крипто перетворення в групі точок еліптичних кривих може бути записано у вигляді:

$$f_{\text{фв}}(\ ) = W_{\delta 1} \wedge W_{\delta 2} \wedge W_{\delta 3} \wedge W_{\delta 4} \wedge \wedge W_{\delta 5} \wedge W_{\delta 6} \wedge W_{\delta 7}. \quad (2)$$

де символ «$\wedge$» позначає операцію кон'юнкції булевих змінних.

Таким чином, якість ДГВП (ПВП) може бути оцінена з використанням безумовного інтегрального критерію – функції відповідності ДГВП вимогам, що $f_{\text{фв}}(\ ) \in (0;1)$ та при $f_{\text{фв}}(\ ) = 1$ ДГВП, що оцінюється, відповідає безумовним вимогам.

Якісне й кількісне порівняння криптографічних перетворень в групі точок еліптичних кривих можна здійснити, використовуючи узагальнений критерій переваги [99, 109]. Для цього необхідно вибрати сукупність умовних критеріїв та показників оцінки, визначити їх та згорнути в інтегральний умовний критерій.

Відмітимо тільки, що кількісна оцінка генераторів може бути зроблена з використанням таких показників, як:

– складність обернення генератора ПВП, тобто знаходження ключа, що використовується;

– ентропія джерела ключів $H_{\text{к}}$, в тому числі для випадку, коли ДГВП використовується як джерело ключів;

– період l_n (довжина) повторення ПВП та безпечний час t_b;

– основа алфавіту m послідовності, що генерується;

– ймовірність перекриття в просторі або в часі двох сегментів бітів Y_r та Y_{μ}, тобто в різних абонентів або в одного абонента протягом часу, так, що $Y_r = Y_{\mu}$;

– відстань рівнозначності l_0 конкретної послідовності бітів Y_{υ};

– просторова $I_{\text{п}}$ та часова складності $I_{\text{ч}}$ формування послідовності бітів Y тощо.

5. ОСНОВНІ ПІДХОДИ ДО ВИЗНАЧЕННЯ ПСЕВДОВИПАДКОВИХ ПОСЛІДОВНОСТЕЙ

Питанням вивчення природи випадковості присвячено значне число робіт [8, 9]. Існують різні підходи до визначення випадкових послідовностей. Але в криптографічних системах однією з необхідних умов є забезпечення криптографічної

стійкості генерування ключів, ключової інформації та параметрів з використанням випадкових та псевдовипадкових послідовностей.

Вперше систематичні дослідження випадкових послідовностей здійснив Борель (Borel) [31, 32]. У своїх працях Борель стверджує, що у істинної випадкової послідовності кожний символ зустрічається приблизно з однією частотою. Крім цього, вказана властивість повинна розповсюджуватись і на відносно довгі послідовності.

Нехай $N_i(x)$ – кількість символів a_i, що містяться у послідовності x, $1 \le i \le Q$. Відповідно коефіцієнт $\frac{N_i(x)}{|x|}$ є відносна частота появи символу a_i у послідовності x. Визначимо алфавіт A^*, наприклад, $A = \{0,1\}$, $A^2 = \{00,01,10,11\}$.

Визначення 1. Не пуста послідовність $x \in A^*$ називається ε-обмеженим, де ε є додатне реальне число, якщо для всіх $1 \le i \le Q$, x задовольняє нерівності

$$\left| \frac{N_i(x)}{|x|} - Q^{-1} \right| \le \varepsilon . \qquad (3)$$

Починаючи з цих робіт дослідники приділяють значну увагу визначенню випадковості.

У 60-х роках академік Колмогоров [33] формує обчислювальний або обчислювально-складнісний підхід до визначення випадковості. Він дав таке визначення випадковості.

Визначення 2. Послідовність x є випадковою (за Колмогоровим), якщо

$$\max_{|x|=n} K(x) = |x| + O(1) . \qquad (4)$$

Тобто, послідовність x є випадковою за Колмогоровим, якщо її довжина $|x|$ дорівнює довжині $K(x)$ самого найкоротшого алгоритму (програми), що породжує x. Із цього слідує, що для формування випадкової послідовності необхідно розробити алгоритм, довжина входу якого дорівнює довжині випадкової послідовності. Це визначення розширюють, а саме послідовність x є t – випадковою за Колмогоровим, якщо

$$K(x) \ge |x| - t . \qquad (5)$$

На основі визначення (3) та (4) можна ввести поняття складності випадкової послідовності. По відношенню до неї підхід Колмогорова за природою є «онтологічним».

Практично одночасно з Колмогоровим концепцію визначення випадковості запропонував Чейтін (Chaitin) [34]. Він також розвинув обчислювально-складнісний та запропонував інформаційно-складнісний підходи до визначення випадковості послідовності.

Сутність інформаційно-складнісного підходу в тому, що випадкова послідовність не може бути алгоритмічно стиснута, тобто має максимальну ентропію. Чейтін увів міру складності *H*, яка залежить від ентропії джерела послідовності [34]. Цей підхід є розвитком не тільки ідей Колмогорова, але й положень Шеннона щодо визначення кількості інформації.

Нехай N – множина натуральних чисел, $N_+ = N \setminus \{0\}$. Зафіксуємо $A = \{a_1,...,a_Q\}, Q \ge 2$ як кінцеву абетку. Через A^* позначимо вільний моноід, який генерується за допомогою A шляхом конкатенації. Елемент моноіду A^* є послідовність; λ – пустий рядок. Для x в A^*, $|x|$ – довжина послідовності x. Зрозуміло, що $|\lambda| = 0$. Для деякого m в N, $A^m = \{x \in A^* \,||x| = m\}$. Для кожного $x \in A^*$, та натурального n припустимо $x = xx...x$ (тобто n - разів); $x^0 = \lambda$.

Кожне загальне упорядкування на A, припустимо $a_1 < a_2 < ... < a_Q$, породжує квазілексографічний порядок на A:

$$\lambda < a_1 < ... < a_Q < a_1a_1 < ... < a_1a_Q < a_Qa_Q < ... < a_1a_1a_1 < ...$$

Позначимо через $x(n)$ n-ий рядок в A^* у відповідності до квазі лексографічного порядку. Чейтін уводить поняття спеціального комп'ютера (комп'ютер Чейтіна) – це частково рекурсивна функція $C: A^* \times A^* \xrightarrow{0} A$ с префікс-вільними доменами, яка здійснює стиск послідовності x зі складністю H.

Визначення 3. Послідовність $x \in A^*$ є m-випадковою за Чейтіном, де m – натуральне число, якщо

$$H(x) \ge \sum(|x|) - m . \qquad (6)$$

Послідовність x є випадковою за Чейтіном, якщо вона є 0-випадковою.

Таким чином, при інформаційно-складнісному підході випадковість зв'язується виключно з неможливістю стиснути послідовність. Фахівці вважають, що модель випадковості Чейтіна є адекватнішою за модель Колмогорова. Вона дозволяє будувати методи щодо перевірки можливості стиску послідовності.

Альтернативою обчислювально-складнісному та інформаційно-складнісному підходам до визначення випадковості є біхевіористичний підхід. У цьому підході замість розгляду «тлумачення» явища випадковості розглядається вплив цього явища на середовище. Тобто послідовність, що генерована ДГВП, вважається псевдовипадковою, якщо не існує ефективного алгоритму, який зможе її відрізнити від дійсно випадкової послідовності тієї ж самої довжини. Основоположним постулатом є те, що об'єкти, які не можуть бути розрізнені один від одного за допомогою будь-яких ефективних процедур, розглядаються як еквівалентні, хоча вони можуть бути і різними за природою. Розглянутий підхід призводить до концепції детермінованого випадкового генератора, який є фундаментальним поняттям у більшості криптографічних додатків.

Базовими елементами біхевіористичного підходу є поняття обчислювальної нерозрізненості та непередбаченості.

Визначення 4. Два ансамблі $X=\{X_n\}_{n\in N}$ та $Y=\{Y_n\}_{n\in N}$ є нерозрізнюваними за поліноміальний час, якщо для будь-якого імовірнісного поліноміального алгоритму D, будь-якого поліному $P(\bullet)$ та для всіх достатньо великих n

$$\left|\Pr_{t\in X_n}\left(D(t)=1\right)-\Pr_{t\in Y_n}\left(D(t)=1\right)\right|<\frac{1}{P(n)}. \qquad (7)$$

Тут $t\in X_n$ позначає, що $t\in\{0,1\}^n$ та t обрано відповідно із X_n.

Таким чином із (7) слідує, що для достатньо довгих рядків не існує ефективної процедури D, яка може вирішити – рядок належить до X_n чи до Y_n. Під поліноміально-часовим алгоритмом D частіше за все розуміють статистичні тести, які виконуються за поліноміальний час.

Концепція обчислювальної нерозрізненості є удосконаленням традиційних підходів із теорії імовірності. Два ансамблі $X=\{X_n\}_{n\in N}$ та $Y=\{Y_n\}_{n\in N}$ є статистично близькими, якщо їх статистична різниця незначна, де статистична різниця між X та Y, відома також як відстань зміни, визначається як функція

$$\Delta(n)\overset{def}{=}\sum_{\alpha}\left|\Pr ob(X_n=\alpha)-\Pr ob(Y_n=\alpha)\right|. \qquad (8)$$

Ключовою властивістю псевдовипадкової послідовності, особливо тієї, яка використовується у криптографічних додатках, є її непередбаченість. Послідовність $\{X_n\}$ є непередбаченою, якщо не існує ефективного алгоритму, який за відомим відрізком послідовності $t_1,t_2,..,t_i$ може визначити наступний елемент t_{i+1} з імовірністю, більшою за $1/2$.

Визначення 5. Ансамбль $X=\{X_n\}_{n\in N}$ є непередбаченим за поліноміальний час, якщо для будь-якого імовірнісного поліноміального алгоритму D, для будь-якого поліному $P(\bullet)$ та для всіх достатньо великих n

$$\Pr_{t\in X_n}\left[D(t_1,t_2,..,t_p)=t_{p+1}\right]>\frac{1}{2}+\frac{1}{P(n)}. \qquad (9)$$

Формула (9) є основою розробки так званих тестів на наступний біт (Next bit test).

Таким чином, біхевіористичний підхід формує концепцію ДГВП, які породжують послідовності, що можуть розглядатися як випадкові будь-яким підготовленим спостерігачем. З цього слідує, що результати ДГВП можуть використовуватися замість випадкових послідовностей для будь-яких прикладних задач.

Найбільш поширеним на практиці підходом до визначення псевдовипадковості є евристичний підхід. В цьому підході ДГВП розглядається як програма (алгоритм), яка породжує бітову послідовність $s=s_0,s_1,..,s_{n-1}$ скінченої довжини n, що проходить деякі особливі статистичні тести. Таким чином, властивості випадкової або псевдовипадкової послідовності можуть бути охарактеризовані та описані у імовірнісному сенсі.

Існує безліч тестів, що дають оцінку, чи є послідовність випадковою. Але ніякий закінчений кінцевий набір тестів не вважають достатнім. Крім того, результати статистичного тесту мають інтерпретуватися із деякою обережністю і застереженням для того, щоб уникнути невірних висновків відносно певного генератору. Але основне, що необхідно підкреслити, це те, що нерозрізнюваність та непередбачуваність є основними характеристиками ВП та ПВП.

6. МАТЕМАТИЧНЕ ВИЗНАЧЕННЯ ГЕНЕРАТОРІВ ВИПАДКОВИХ ПОСЛІДОВНОСТЕЙ

Вимогою мінімального захисту для ДГВП [11] є вимога достатньо великої довжини *k* випадкового початкового числа, але такої, щоб пошук на 2^k елементах був нездійсненним для порушника. Основними загальними вимогами до ДГВП є такі:

– вимога нерозрізнюваності вихідних послідовностей ДГВП від істинно випадкових послідовностей;

– вимога непередбаченості вихідних бітів для порушника з обмеженими обчислювальними ресурсами [16];

– вимога необоротності генератора у змісті наперед визначеної малої ймовірності компрометації ключа самого ДГВП.

Визначення 6. Вважається, що ДГВП проходить всі статистичні тестування поліноміального часу, якщо жоден алгоритм поліноміального часу не може правильно відрізнити вихідну послідовність генератора від істинної випадкової послідовності тієї ж довжини з ймовірністю, значно більшою, ніж $1/2$ [15].

Визначення 7. Вважається, що ДГВП проходить тестування наступного біту, якщо немає жодного алгоритму поліноміального часу, який при введені перших *l* бітів вихідної послідовності *s*, може передбачити (*l*+1)-й біт *s* з ймовірністю, значно більшою, ніж $1/2$ [15].

Теорема 1. ДГВП проходить тестування наступного біту, якщо він проходить всі статистичні тестування поліноміального часу [15].

Блюм-Мікалі ввели поняття криптографічно-стійкого ДГВП, еквівалентне наступному визначенню [15].

Визначення 8. ДГВП, який проходить тестування наступного біту, називається криптографічно-стійким ДГВП [15].

Таким чином, ПВП повинна мати деякі статистичні властивості [11], що присутні в істинно випадкових послідовностях. Багато статистичних властивостей лінійної конгруентної псевдовипадкової числової послідовності $x_{i+1}=a\cdot x_i+b(\mathrm{mod}\,n)$

досліджені Кнутом [35]. Проте, на відміну від істинних випадкових послідовностей, наступний біт в лінійній конгруентній послідовності може бути легко обчислений з попередніх бітів, навіть коли x_0, a, b або n не задані. Хоча лінійні конгруентні генератори проходять деякі статистичні тестування, вони є передбаченими, і тому цілком незахищеними з точки зору криптографії.

ДГВП, що засновані на детермінованих алгоритмах, відповідають наступній структурі, узятій з Ля Екюера (1994): ДГВП є структурою (S, μ, f, U, g), де S – кінцева множина станів (простір станів), μ – розподіл ймовірності на S станів, що використовується для вибору початкового стану (або початкового числа) s_0, $f: S \to S$ є функція переходу, U – є вихідний простір, і $g: S \to U$ є вихідна функція. Зазвичай, $U = (0,1)$. Стан ДГВП формується згідно рекурентності $s_i = f(s_{i-1})$ для $i \geq 1$, а вихідними даними на кроці i є $u_i = g(s_i) \in U$. Вихідні значення $u_0, u_1, u_2 \ldots$ є так званими випадковими бітами, виробленими ДГВП.

Принциповою відмінністю ДГВП та ГВП [11] для стохастичних моделювань і криптографічних застосувань є те, що в криптографічних системах вони додатково повинні забезпечувати стійкість проти здійснення різного роду атак. Як показав аналіз, атаки в криптографічних системах на ДГВП можуть здійснюватись для [4]:

– знаходження невідомих вихідних даних (ключів, ключової інформації та параметрів, що генеруються для інших криптографічних застосувань);

– знаходження інформації про внутрішній стан, в першу чергу значення ключа безпосередньо самого генератора;

– маніпулювання вихідними даними генератора.

Згідно [11] потенційно можливі атаки можна розділити на три таких класи:

– крипто аналітичні атаки, що зводяться до вирішення математичних задач обернення генератора, складність яких менше або суттєво менше атаки груба сила;

– атаки, що засновані на вхідних даних генератора;

– атаки, що засновуються на недостатніх показниках непередбачуваності.

По особливостям впливу порушника потенційно можливі атаки можна розділити на дві великі групи [4]:

– пасивні атаки, при здійсненні яких порушник відслідковує джерело шуму і частини вихідних даних генератора. Якщо він зможе виявити будь-які кореляції між цими двома потоками, то він зможе використовувати ці знання для прогнозування майбутніх вихідних даних, тобто ключів та/або параметрів;

– активні атаки, при здійсненні яких порушник може вплинути на джерело шуму і, таким чином, мати можливість впливу на послідовність бітів, що генерується генератором. Даний вид атаки є особливо ефективним, тому що зловмисник може спробувати адаптувати вхідні шуми з характерними властивостями ДГВП для отримання передбачуваних вихідних даних.

ВИСНОВКИ ТА ПРОПОЗИЦІЇ

Більшість ДГВП хоча й мають прийнятну швидкодію, але мають багато серйозних недоліків, основними з яких є :

– недопустимо короткий або недоведений період повторення;

– послідовні значення бітів не є незалежними, що робить його передбачуваним;

– оборотність відносно визначення закону формування (ключа), що також робить його передбачуваним;

– властивості випадковості, рівноймовірності, незалежності та однорідності не відповідають вимогам, а значить властивості нерозрізнюваності не відповідають вимогам.

ДГВП повинні бути захищеними від таких основних атак, як:

– криптоаналітичні атаки, що зводяться до вирішення математичних задач, складність яких менше або суттєво менше атаки груба сила;

– атаки, що засновані на вхідних даних генератора, які здійснюються засобом визначення або маніпулювання вхідними даними ГВП з метою впливу на вихідні дані (ключі, параметри тощо для інших криптографічних додатків);

– атаки, що зводяться до розповсюдження компрометованого стану генератора на інші стани – попередні чи майбутні.

Безумовними вимогами до ДГВП є необхідність запобігання будь-яким атакам, які дозволяють зловмиснику отримати інформацію про його внутрішній стан.

У зв'язку з виявленими протиріччями та проблемними питаннями, на наш погляд, в подальшому повинні бути вирішеними такі проблемні питання.

1. Обґрунтування та побудування ДГВП на основі біхевіористичного підходу, при якому послідовність, що генерується ДГВП, вважається псевдовипадковою, якщо не існує ефективного алгоритму, який зможе її відрізнити від дійсно випадкової послідовності тієї ж самої довжини, тобто з добрими властивостями нерозрізнюваності.

2. Удосконалення методів та засобів оцінки як самого генератора, так і статистичних властивостей псевдовипадкових послідовностей, а також порівняльний аналіз ДГВП та ПВП, що ним генеруються, як по окремим, так і інтегральним критеріям та показникам.

3. У зв'язку з тим, що на сьогоднішній день розроблені і широко використовуються ряд методик тестування статистичних властивостей псевдовипадкових послідовностей, таких як NIST STS [36], FIPS PUB 140-1 [28], FIPS PUB 140-2 [37], AIS 20 [29] та AIS 31 [6], необхідно розробити методику дослідження властивостей ДГВП, за-

сновану на комплексному контролі ефективності функціонування ДГВП.

4. Заслуговує уваги та подальшого розвитку ряд нових та удосконалених методів побудування ДГВП, в тому числі на основі спарювання точок еліптичних кривих, результат якого визначає підгрупи розширення поля F_{q^k} з наперед відомим гарантованим періодом, кожен елемент якого гешується.

7. Теоретичні дослідження методів та ДГВП, що ґрунтуються на рекурентному формування елементів полів і підполів Галуа та їх перетворенні методом гешування в ПВП з необхідними властивостями необоротності, нерозрізнюваності, непередбачуваності та швидкодії.

Вирішення поставлених задач представлено в серії наступних статей.

Література

[1] *Б. Шнаер.* Прикладная криптографія / Б. Шнаер // 2-е издание.

[2] *Горбенко І.Д.* Аналіз генераторів випадкових бітів згідно стандарту ISO/IEC 18031 та рекомендації щодо його застосування в Україні / Горбенко І.Д., Шапочка Н.В. // Міжнародний симпозіум «Вопросы оптимизации вычислений». – Кацивелі. – 2009. – С.164-170.

[3] *Потий А.В.* Декомпозиция требований, предъявляемых к генераторам случайных и псевдослучайных чисел, на основе классификации специальных даннях / Потий А.В., Пестерев А.К, Олейников Р.В. // Матеріали науково-практичної конференції «Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні». – Київ: НТУУ "КПІ". – 1998. – С. 194.

[4] *Andrea Rock.* Pseudorandom Number Generators for Cryptographic Applications / Andrea Rock // Diplomarbeit zur Erlangung des Magistergrades an der Naturwissenschaftlichen Fakultat der Paris-Lodron-Universitat Salzburg. – Salzburg. – 2005.

[5] *Торба А.А.* Генерация равновероятных случайных последовательностей на основе физических датчиков / Торба А.А., Елаков С.Г., Степченко А.З. // Всеукр. межвед. науч.-техн. сб. Радиотехника. – Вып. 119. – 2001. – С.108-114.

[6] Application Notes and Interpretation of the Scheme (AIS) 31. Functionality classes and evaluation methodology for physical random number generators. Certification body of the BSI in context of certification scheme. BSI, 2001.

[7] ISO/IEC 18031:2005(E). Information technology – Security techniques – Random bit generation.

[8] *Чайковский Ю.В.* О природе случайности / Чайковский Ю.В. // Монография. 2-е изд., Испр. и доп. Вып. 27. «Ценологические исследования» -М.: Центр системных исследований – институт истории естествознания и техники РАН. – 2004. – С.280.

[9] *Птицын Н.* Приложение теории детерминированного хаоса в криптографии / Птицын Н. // - Москва. – 2002.

[10] *C.E. Shannon.* A mathematical theory of communication / C.E. Shannon. // Bell System Technical Journal, №27. – 1948. – P.379-423, 623-525.

[11] *Шапочка Н.В.* Аналіз атак на генератори випадкових бітів / Шапочка Н.В. // Радіоелектронні і комп'ютерні системи. – 2010. – С. 99-105.

[12] *M. Blum.* How to generate cryptographycally strong sequences of pseudorandom bits / M. Blum, S. Micali // SIAM Journal on Computing. – Vol. 1. – 1986. P.850-864.

[13] *A.C. Yao.* Theory and applications of trapdoor functions / A. C. Yao //23rd IEEE FOCS. – 1982. – P.80-91.

[14] *J. Hastad.* Pseudorandom number generators from any one-way function / J. Hastad, R. Impagliazzo, L.A. Levin, M. Luby // SIAM Journal on Computing. – Vol. 28. – 1999. – P.1364-1396.

[15] *Ju-Sung Kang.* Security frameworks for pseudorandom number generators / Ju-Sung Kang // Information Center for Mathematical Sciences. – Vol.8, Number 1. – 2005. – P.1-11.

[16] *J. Kelsey.* Cryptanalytic attacks on pseudorandom number generators / J. Kelsey, B. Schneier, D. Wagner, C. Hall // FSE. – 1998.

[17] *A. Desai.* A practice-oriented treatment of pseudorandom number generators / A. Desai, A. Hevia, Y. L. Yin // EUROCRYPT. – 2002. – P.368-383.

[18] *M. Bellare.* A concrete security treatment of symmetric encryption / M. Bellare, A. Desai, E. Jokipi, P. Rogaway // FOCS. – 1997.

[19] *M. Bellare.* The security of the cipher block chaining message authentication code / M. Bellare, J. Kilian, P. Rogaway // CRYPTO'94. – 1994.

[20] ISO/IEC 10118-3:2004. Information technology – Security techniques – Hash-functions – Part 3: Dedicated hash-functions.

[21] *Шапочка Н.В.* Перспективний генератор випадкових бітів на геш - функціях та його властивості / Шапочка Н.В. // Молодіжний форум «Радіоелектроніка і молодь у XXI ст.». – Харків – 2009.

[22] ISO/IEC 18033-3:2005. Information Technology – Security Techniques – Encryption Algorithms – Part 3: Block Ciphers.

[23] ISO/IEC 10116:2006. Information technology – Security techniques – Modes of operation for an n-bit block cipher.

[24] *Daniel R. L. Brown.* A Security Analysis of the NIST SP 800-90 Elliptic Curve Random Number Generator [Електронний ресурс] / Daniel R. L. Brown, Kristian Gjosteen // – 2007. – Режим доступу: http://eprint.iacr.org/.

[25] *Горбенко І.Д.* Навчальний посібник «Захист інформації в інформаційно-телекомунікаційних системах» / І.Д. Горбенко, Т.О. Гріненко. – Х.: ХНУРЕ. – 2003. – 368 с.

[26] Введение в криптологию / Под ред. В.В. Ященко. Серия: Новые математические дисциплины. М.: МЦНМО – ЧеРо, 1998. – 271 с.

[27] *Ю.С. Харин.* Математические и компьютерные основы криптологии: Учеб. пособие / Ю.С. Харин, В.И. Берник, Г.В. Матвеев, С.В. Агиевич // Мн.: Новое знание. – 2003. – 382с.

[28] Federal Information Processing Standards Publication (FIPS PUB) 140-1. Security requirements for cryptographic modules. NIST, 1994.

[29] Application Notes and Interpretation of the Scheme (AIS) 20. Functionality classes and evaluation methodology for physical random number generators. Certifica-

tion body of the BSI in context of certification scheme. BSI, 1999.

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

[31] *Борель Е.* Вероятность и достоверность / Борель Е. // – 1969.

[32] *Борель Е.* Вероятности, ошибки / Борель Е., Дельтейль Р., Юрон Р // –1972.

[33] *S. C. Evans.* Kolmogorov complexity estimation and analysis / S. C. Evans, J. E. Hershey, and G. Saulnier // Technical Information Series 2002GRC177, GE Global Research. – 2002.

[34] *Gregory Chaitin.* Information, Randomness & Incompletenes / Gregory Chaitin // World Scientific. – 1987.

[35] *Дональд Кнут.* Искусство программирования / Дональд Кнут // Получисленные алгоритмы. The Art of Computer Programming. – Vol.2. Seminumerical Algorithms. – 3-е изд. – М.: «Вильямс»/ – 2007. – С. 832.

[36] NIST IR 6390. A Statistical Test Suite for the Validation of Random Number Generators and Pseudo Random Number Generators for Cryptographic Applications, 2000.

[37] Federal Information Processing Standards Publication (FIPS PUB) 140-2. Security requirements for cryptographic modules. NIST, 1999. Federal Information Processing Standards Publication (FIPS PUB) 140-2. Security requirements for cryptographic modules. NIST, 1999.

Надійшла до редколегії 18.05.2011

Шапочка Наталя Вікторівна, асистент кафедри безпеки інформаційних технологій Харківського національного університету радіоелектроніки. Область наукових інтересів: розробка та застосування методів генерації випадкових послідовностей.

Нейванов Андрій Вікторович, аспірант кафедри безпеки інформаційних технологій Харківського національного університету радіоелектроніки. Область наукових інтересів: розробка та застосування методів генерації випадкових послідовностей.

Мордвінов Руслан Ігоревич, магістрант кафедри БІТ Харківського національного університету радіоелектроніки. Область наукових інтересів: розробка та застосування методів генерації випадкових послідовностей.

Гріненко Тетяна Олексіївна, асистент кафедри Безпеки інформаційних технологій. Область наукових інтересів: методи та засоби криптографічного захисту інформації.

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 681.324.067

Методы и средства генерирования псевдослучайных последовательностей / Ю.И. Горбенко, Н.В. Шапочка, Т.А. Гриненко, А.В. Нейванов, Р.И. Мордвинов // Прикладная радиоэлектроника: науч.-техн. журнал. – 2011. Том 10. № 2. – С. 141–152.

Приводится классификация генераторов случайных последовательностей, обосновываются критерии и показатели оценки качества случайных последовательностей, излагаются основные подходы к определению случайных и псевдослучайных последовательностей, математическое определение случайных последовательностей.

Ключевые слова: случайная последовательность, псевдослучайная последовательность, генератор случайных последовательностей, детерминированный генератор случайных последовательностей.

Табл. 4. Ил. 03. Библиогр.: 37 назв.

UDK 681.324.067

Methods and means for generating pseudorandom sequences / Yu.I. Gorbenko, N.V. Shapochka, T.A. Grinenko, A.V. Neivanov, R.I. Mordvinov // Applied Radio Electronics: Sci. Journ. – 2011. Vol. 10. № 2. – P. 141–152.

The paper presents a classification of random sequence generators, justifies criteria and indicators for assessing the quality of random sequences, gives an account of the main approaches to the definition of random and pseudorandom sequences, provides mathematical definition of random sequences.

Keywords: random sequence, pseudorandom sequence, random sequence generator, deterministic random sequence generator.

Tab. 4. Fig. 03. Ref.: 37 items.