УДК 621.391.2

Горицький В.М., Снєжок О.В.
Височіненко М.С.

ГЕНЕРАЦІЯ ВИПАДКОВИХ ПОСЛІДОВНОСТЕЙ ДЛЯ СИСТЕМ УПРАВЛІННЯ КЛЮЧАМИ

В статті дається аналіз стану та розвитку засобів формування випадкових послідовностей для криптографічних застосувань із метою підвищення їх ефективності за критерієм стійкості. Розглянуто підходи до підвищення властивостей випадкових послідовностей (ВП) на основі обробки первинних ВП від фізичних джерел. Викладені підходи до зменшення кореляційних властивостей первинних ВП шляхом ймовірнісно-криптографічних перетворень на основі кодування у суміжних класах $(n, n-k)$ кодів V.

Ключові слова: випадкові послідовності, управління ключами, криптографія, криптостійкість, ймовірнісно-криптографічні перетворення.

Постановка завдання. Безпека інформації в інформаційно-комунікаційних технологіях (ІКТ) забезпечується сукупністю організаційних та інженерно-технічних заходів, засобів і методів захисту інформації, що утворюють комплексну систему захисту інформації (КСЗІ) [1]. Найважливішими складовими частинами КСЗІ є криптографічні системи (КС). Сучасні ІКТ потребують від криптографічних систем забезпечення стійкості та надійності захисту інформації при заданих умовах функціонування.

Криптостійкість (КрС) більшості сучасних КС, згідно принципу О.Кергофса, повинна забезпечуватися лише параметрами (ключовими даними) криптографічного перетворення (криптоалгоритму), тому стійкість КС прямо залежить від ефективності функціонування ключових систем (систем управління ключами).

Генерація якісної випадкової послідовності – найбільш складна частина багатьох криптографічних операцій [2]. В [3] показано, що для забезпечення стійкості шифрування необхідно забезпечити надійний ключ, а це в свою чергу, досягається шляхом використання криптографічно якісних генераторів випадкових послідовностей (ГВП).

Аналіз існуючих підходів отримання випадкових послідовностей. Сучасні методи генерування ключових даних припускають використання генератора (генераторів) випадкової послідовності і засобів формування та тестування ключів криптографічної системи.

Існуючи методи генерування криптографічно якісних ВП умовно можна поділити на: *істинновипадкові*, *псевдовипадкові* та *квазівипадкові* послідовності.

Істинновипадкові послідовності (ІВП). Для отримання *істинновипадкових послідовностей (ІВП)* в якості джерел ентропії використовують фізичні явища природи. У деяких криптографічних застосуваннях можуть використовуватися екзотичні (неспеціалізовані) методи отримання первинної ентропії [3], наприклад:

- тривалість натискання клавіш на клавіатурі («миші») та періоди між натисканням;
- параметри локальної (глобальної) комп'ютерної мережі;
- коливання часу доступу до жорсткого диску у зв'язку із турбулентністю повітря в його корпусі [1];
- шуми звичайної цифрової камери, розміщеної у темряві (проект «Lavarnd» online: http://lavarnd.org) тощо.

Але такі генератори мають малу ентропію, низьку продуктивність та характеризуються високою кореляцією вихідної послідовності, тому не можуть бути використані у прямому застосуванні, а лише як криптографічно слабкі джерела для отримання початкових даних (ініціалізації) квазівипадкових та псевдовипадкових ГВП.

Спеціалізовані криптографічно сильні генератори ІВП в якості джерел ентропії використовують радіоактивний розпад, фізичні явища оптично-квантової механіки, електричні шуми.

Радіоактивний розпад є одним із «фундаментальних» фізичних процесів, що використовується для отримання криптографічно якісних випадкових послідовностей [1].

Дійсно, припустити, що атомарне ядро розпадеться в дану секунду або в іншу – доволі непередбачуване твердження. Для отримання первинної випадковості звичайно використовують періоди між щигликами в лічильнику Гейгера. Довготривалість, стабільність та непередбачуваність такого фізичного процесу – головні переваги генераторів ІВП, що використовують радіоактивний розпад. До недоліків таких генераторів відносять: необхідність використання радіоактивних матеріалів, що призводить до загальної громіздкості та складності усієї системи; технічна складність побудови чутливих датчиків Гейгера (недосконалість сучасних датчиків призводить до підвищення кореляції вихідної ВП); низька продуктивність; низька мобільність; висока собівартість.

Модерним та перспективним напрямком методів отримання випадковості є ГВП, які побудовані на властивостях квантових процесів [[1]]. Часто, для отримання ВП, квантові генератори використовують «принцип Гейзенберга». Опис генератору, побудованого на цьому принципі можна знайти в [1]. Але є і інші підходи – наприклад, генератор, описаний в [1], використовує більш спрощений метод і дозволяє отримувати істинновипадкові послідовності біт із більшою швидкістю – до 100 кбіт на секунду. Висока статистична якість та мала кореляція вихідної ВП є перевагами квантових ГВП. Недоліками є: відносно низька продуктивність; потреба у складних, високотехнологічних оптико-електронних приладах. В наслідок цього – низька загальна надійність і висока собівартість.

Найбільш доступний та простий на сьогодні спосіб отримання первинної ентропії для генерації ВП є перетворення випадкових процесів електричних шумів. Природа виникнення електричних шумів може бути обумовлена як самим механізмом протікання електричного струму так і флуктуаціями інших неелектричних величин, які перетворюються у флуктуації току та напруги [1]. Причини виникнення ряду шумів до кінця нез'ясовані.

Фундаментальні аналогові електричні шуми, що використовуються для отримання ВП, можна поділити на тепловий шум (рівноважні флуктуації, шум Найквиста) та дробовий шум. Їх співіснування породжує шуми підсилювачів, які також можуть бути використані для генерації ІВП. Особливе місце займають так звані «надлишкові шуми» (генераційно-рекомбінаційні шуми, шуми струморозподілення, вибухові та флікерні шуми). Їх існування загалом не залежить від фундаментальних шумів і деякі з них можуть добре вплинути на отримання якісної статистики шумового процесу. Але, наприклад, існування в системі флікерного шуму, який проявляються на інфранизьких частотах може призвести до погіршення статистики ГВП та внести кореляцію у вихідну ВП. Описи ГВП (для криптографічних цілей):

- на основі термального шуму – «ZRANDOM» компанії Westphal Electronic (http://home.t-online.de/home/p.westphal/zran_eng.htm);
- дробового шуму – «HG400 Series Random Number Generators» компанії Random (http://random.com.hr/products/random/manual/index.html);
- шумів підсилювача – «ComScire QNG» компанії The Quantum World Corporation (https://www55.ssldomain.com/Products).

Перевагами ІВП, отриманих за допомогою електричних шумів є: наявність глибоких теоретичних знань про механізми їх існування; простота реалізації (порівняно із іншими методами); висока продуктивність; висока мобільність та надійність; відносно низька собівартість. Головні недоліки: сильний вплив схемотехнічних, технологічних рішень та зовнішнього середовища на статистичну якість та кореляцію вихідної ВП.

Окремо можна виділити метод, який, завдяки сучасним нанотехнологіям, використовує переваги ГВП, що побудовані на процесах електричного шуму та квантової механіки. Запропонований компанією El-Mul Technologies Ltd. (http://www.el-mul.com) новітній та перспективний спосіб генерації ІВП отримує початкову ентропію з випадкового процесу дробового шуму польового транзистору, побудованого на карбонових нанотрубках. Його сполучення з наноскопічними лічильниками дозволяє збирати інформацію з точністю до окремих електронів та забезпечити продуктивність до 1 Гбіт на секунду. Окремий дискретний елемент з десятків тисяч таких ГВП може дати продуктивність до 10 терабіт на

секунду. Таке рішення дозволяє зменшити вплив зовнішнього середовища на статистику та кореляцію ГВП. Недоліки – теоретично можливий вплив зовнішнього середовища на процес генерації ВП, складність та висока собівартість технологічного процесу виготовлення таких ГВП.

Генератори ІВП на сьогодні залишаються основним методом отримання первинної ентропії для потреб сучасних криптографічних систем. Їх переваги – можливість отримання універсальних та незміщених змінних [3], унеможливлення передбачення наступних випадкових елементів та повторення всієї ВП. Але такого результату можна досягти лише при спеціальних умовах використання ГВП із забезпеченням стабільних параметрів навколишнього середовища (температурні, тиску, електромагнітні, радіаційні тощо), спеціалізованих технічних, технологічних рішень та забезпеченню протидії атакам на ГВП. Це, як правило, призводять до значного підвищення складності та собівартості генератора. Наявність будь-якого слабкого місця генератора ІВП, негайно призводить до втрати криптостійкості всієї КС – це головний недолік генераторів ІВП.

Псевдовипадкова послідовність (ПВП). *Псевдовипадкова послідовність* (ПВП) називається такою, якщо вона виглядає як безсистемна та імовірнісна, хоча в дійсності створювалася засобами цілком детермінованого процесу, який називається псевдовипадковий генератор [1]. Такі генератори починають свою роботу із первинної ІВП, яка називається «*початковою»* (або «*вектор ініціалізації*»), і детерміновано виробляє за її допомогою набагато більшу за довжиною ПВП. Генерація ПВП – альтернативний, поширений спосіб отримання ВП для потреб КС [2,10].

Класичні генератори ПВП, які докладно описані в [1] аналізуються лише на предмет статистичної випадковості і страждають від багатьох недоліків (з точки зору криптографічної якості): дуже малий період/періоди; послідовні значення не є незалежними; деякі біти менш випадкові ніж інші; нерівномірний одномірний розподіл; зворотність тощо.

Особливої уваги заслужив генератор ПВП «Mersenne twister» запропонований у 1997 році Мацумото та Нішімурою. Його перевагами є: великий період $\left(2^{19937}-1\right)$; рівномірне розподілення у 623 вимірах (лінійний конгруентний метод дає більш-менш рівномірний розподіл від сили у 5 вимірах); швидка генерація випадкових чисел (у 2-3 рази швидше, ніж стандартні конгруентні лінійні методи). Однак існують складні алгоритми, які дозволяють розпізнавати послідовність, яка породжується за допомогою «Mersenne twister», як невипадкову (алгоритм Ріда-Слоана). Це робить «Mersenne twister» негідним та небезпечним для використання у криптографічних цілях [3, 12].

Для криптографічно сильних генераторів ПВП, висуваються більш жорсткі вимоги. Якісний генератор ПВП, який використовується в КС, повинен задовольняти вимогам: забезпечення криптографічної стійкості; мати добрі статистичні властивості; великий період послідовності, що генерується; мати ефективну програмну та апаратну реалізацію [1]. Криптостійкість генератора ПВП характеризує спроможність протистояти криптоаналізу, який направлений на розкриття закону формування ПВП.

Навіть при знанні алгоритму роботи генератора ПВП, всієї послідовності, яка виробляється цим генератором, але без знання *початкової*, криптоаналітик немає можливості визначити наступний елемент послідовності кращим способом, ніж жеребкування. Таке визначення криптографічно сильних генераторів ПВП має назву «непредикативність вліво» та вперше було введене Мануелем Блюмом (Manuel Blum) та Сільвіо Мікелі (Silvio Micali) [1], а доведено Ендрю Яо (Andrew Yao) в [1].

Сучасні криптографічні підходи вироблення ПВП можна класифікувати за типами генераторів, побудованих на:

- функціях шифрування поточних шифрів;
- функціях шифрування блочних шифрів;
- використанні однобічних функцій;
- стохастичному перетворення інформації.

Прикладами генераторів ПВП, які використовують функції поточного шифрування можна навести: RC4, ГОСТ 28147-89 у режимі гамування та йому подібні, поточні шифри із використанням регістрів зсуву із лінійними зворотними зв'язками та нелінійними вузлами ускладнення для вироблення гами – A5, PANAMA, SOBER, SNOW, ISAAC, SEAL та інші.

Для генераторів ПВП, які побудовані для поточного шифрування, можна зауважити: кожен елемент вихідної інформаційної послідовності шифрується на своєму елементі ключової послідовності (ПВП); результат перетворення окремих елементів залежить від їх позиції у вихідній послідовності; мають ефективну апаратну та програмну реалізацію; їм властива висока продуктивність – швидкість генерації залежить лише від обчислювальної потужності апаратно-програмних засобів ГВП.

Приклади реалізації генераторів ПВП блочного шифрування: ГОСТ 28147-89 у режимі заміни, AES-128, DES та йому подібні тощо. Особливості блочного шифрування: шифруванню піддаються порції інформації фіксованої довжини (блоки); кожен блок вихідної послідовності шифрується незалежно від інших на одному і тому ж ключі; низька швидкодія, так як функція шифрування любого сучасного блочного криптоалгоритму є багатократне повторення однієї рондомізованої операції.

Для сучасних КС, як правило, в основу генераторів ПВП покладено використання функцій поточного шифрування.

Криптографічно стійкі генератори ПВП можуть бути побудовані на використанні так званих однобічних функцій. Такі функції є базовим поняттям для криптографії з відкритим ключем [1].

Однобічною функцією із секретом називається функція $F_k : X \to Y$, залежна від параметру k, і має наступні властивості:

– при любому k існує поліноміальний алгоритм обчислення значень $F_k(x)$;

– при невідомому k не існує поліноміального алгоритму інвертування F_k;

– при відомому k існує поліноміальний алгоритм інвертування F_k.

На теперішній час ні для однієї з функції, кандидата на звання однобічної, не доведена друга властивість, але відомо, що задача інвертування еквівалентна деякій добре вивченій та давно відомій важкій математичній задачі. Це означає, що друга вимога до однобічної функції із секретом замінюються більш слабкою умовою: при невідомому k, *імовірно*, не існує поліноміального алгоритму інвертування F_k^{-1}.

В [1] показано, що взагалі, криптографічно стійкий генератор ПВП, за визначенням Яо, можна побудувати на будь-якій однобічній функції із секретом. Існують реалізації генераторів, побудованих на криптоалгоритмах RSA, Ель-Гамаля та еліптичних кривих [1] та їм подібних.

Гарним прикладом генератора ПВП, побудованого на однобічній функції є генератор Е.Блюм, М.Блюм, М.Шуба (M.Schub) (BBS-генератор) [3].

Елемент послідовності, що генерує BBS-генератор, визначається як:

$$x_{n+1} = (x_n)^2 \bmod M$$

де: M – добуток двох великих простих чисел q та p, $p \neq q$, $p \equiv 3 \bmod 4$, $q \equiv 3 \bmod 4$ (число M ще називають цілим числом Блюма); x_n – попереднє число послідовності.

Функція зведення у квадрат по модулю M є перестановкою квадратичних відрахувань по модулю числа M, та вважається, що вона є однобічною функцією із секретом. Доведено, що складність інвертування такої функції еквівалентно обчисленню розкладення M на множники і вважається складною обчислювальною задачею.

Послідовність будується з перших t значущих бітів b_i послідовності чисел $x_1, x_2, \ldots, x_n$, отриманих за формулою : $BBS_{M,t}(x_0) = b_0 b_1 b_2 \ldots b_{t-1}$.

BBS-генератор є непредикативним вліво, це означає, що ніхто не може відгадати знаючи M та $b_0 b_1 b_2 \ldots b_{t-1}$.

Важливі якості цього генератора полягають в тому, що для всіх, хто знає розкладання M на множники, згідно теореми Ейлєра, є можливим *пряме визначення* тих окремих бітів, які в ньому вироблюються. До недоліків BBS-генератора відносять дуже низьку продуктивність, тому його використання в реальних КС не поширене.

Сучасні криптографічні генератори ПВП, побудовані на однобічних функціях, з точки зору статистичних властивостей, мають досить непогані характеристики і в деяких випадках кращі, ніж у спеціалізованих апаратних генераторах істинновипадкових біт.

Загальні вимоги до криптографічних генераторів ПВП, їх різновидів та методів їх побудови можна знайти в [1].

Загалом до переваг генераторів ПВП відносять: незалежність від умов навколишнього середовища; зумовленість статистики, як наслідок – відсутність спеціальної схеми контролю виходу генератора; просте управління та реалізація.

Обов'язкова необхідність початкової ініціалізації високоякісною істинновипадковою послідовністю та базування крипостійкості на обчислювальній складності – головні недоліки генераторів ПВП [1].

Квазівипадкові послідовності (КВП). До генераторів *квазівипадкових послідовностей* (КВП) можна віднести широкий клас методів, метою яких є отримання рівномірно розподілених, незалежних біт, із джерел випадковості, які мають деякі статистичні та кореляційні дефекти. Методи, які перетворюють послідовності із незалежними, але нерівноімовірним розподіленням біт відносять, як правило, до методів статистичного перетворення [1].

Джон фон Нейман (John von Neumann) вперше розглянув в [1] задачу із перетворення послідовності, що породжується бернулієвським джерелом із алфавіту $\{0,1\}$ та ймовірностями $1-p$ та p відповідно, $0 < p < 1$, причому p може бути невідомим. Необхідно перетворити (закодувати) цю послідовність в таку, де ймовірність появи нуля або одиниці в послідовності рівні (іноді таку послідовність називають абсолютно випадковою). Суть запропонованого методу в наступному: вхідна послідовність ділиться на блоки довжиною 2, які кодуються по наступному правилу:

$$00 \to \Lambda,\ 01 \to 0,\ 10 \to 1,\ 11 \to \Lambda,$$

де Λ – пусте слово.

Так як імовірності слів 01 та 10 співпадають (рівні $p(1-p)$ та $(1-p)p$ відповідно), то за правилом кодування отримуємо абсолютно випадкову послідовність. Легко помітити недолік такого методу – при вхідній послідовності довжиною t трансформована послідовність складається з $tp(1-p)$ символів, тобто навіть якщо $p \to 0,5$ довжина вихідної послідовності буде рівна $t/4$.

Елаєсом (Peter Elias) [1] був запропонований метод перетворення, якій більш економно витрачає символи вхідної послідовності, що досягається за рахунок переходу до кодування блоків довжиною N, більше двох (при $N = 2$ методи Елаєса та фон Неймана співпадають). Верхня границя ефективності методу є ентропія джерела послідовності $h(p)$ за Шеноном [3], тобто

$$h(p) = -\left(p \log p + (1-p)\log(1-p)\right).$$

Метод ефективний при зростанні N, але потребує зберігання всіх 2^N кодових слів, тому розмір пам'яті кодеру зростає по експоненті. В роботі [2] пропонується метод, заснований на алгоритмі Елаєса, в якому об'єм пам'яті та часу, витраченого на обробку одного символу, по експоненті менші, ніж у попередніх алгоритмів, але складність апаратної реалізації та орієнтованість подібних алгоритмів (алгоритми стиснення Шеннона, Хаффмена, Ходака, Лемпеля-Зіва [2] тощо) на модель бернулієвського джерела випадковості (тобто без урахування кореляційних залежностей) є недостатнім для використання їх у якості методу перетворення виходу реальних фізичних ГВП.

У роботі М. Санта (Miklos Santha) та Ю. Вазірані (Umesh Vazirani) [2] вперше розглядається математична проблема генерації випадкових послідовностей за допомогою фізичних джерел шуму (із найбільш поширених – діоди Зенера). У таких фізичних джерел первинної ентропії вихідні біти *не тільки зміщені, але й залежні*. Надзвичайно узагальненою моделлю виходу такого «напіввипадкового» («недосконалого») джерела, розглядають підкидання монети із зміщенням δ $(0<\delta<1)$, яке може змінюватися із плином часу. В роботі також дається поняття квазівипадкового генератора: це джерело, таке що для кожного $t>0$, для достатньо великого n, и для кожного функціонального статистичного тесту f : $\left|\mu_f(n)-\mu_f^*(n)\right|<1/n^t$,

де:

– $\mu_f(n)=1/2^n\sum_{|x|=n} f(x)$ – середнє значення f істинновипадкової послідовності x довжини n;

– $\mu_f^*(n)=\sum_{|x|=n} p_n(x)f(x)$ – середнє значення f випадкової послідовності x із ймовірністю $p_n(x)$, довжини n, що генерується джерелом.

Визначення ймовірнісного статистичного тесту поліноміального часу в такому контексті стає більш строгим ніж концепція статистичного тесту представленого у Яо в [14].

Суть запропонованого методу генерації квазівипадкової послідовності полягає у наступному: для m послідовностей біт, кожна довжиною n:

$$x_{11},\ldots,x_{1n},$$
$$x_{k1},\ldots,x_{kn},$$

$$x_{m1},\ldots,x_{mn},$$

отримуємо вихідну послідовність $y=y_1,\ldots,y_n\in\{0,1\}^n$, де кожен біт вихідної послідовності y_i є результатом функції парності: $y_i=parity(x_{1i}+\ldots x_{mi})$. Для отриманої послідовності кожен біт буде мати зміщення в межах $\left[1/2-(1-2\delta)^m,1/2+(1-2\delta)^m\right]$, тобто

$$\left|\Pr(y_i=0|y_1,\ldots,y_{i-1}=u)-\Pr(y_i=1|y_1,\ldots,y_{i-1}=u)\right|<(1-2\delta)^m.$$

Легко помітити, що якість виходу такого квазівипадкового ГВП експоненційно залежить від кількості окремих, незалежних джерел випадковості, що для апаратної реалізації в КС може виявитися досить дорого (кожне таке джерело повинно представляти собою окремий фізичний ГВП).

Дослідження такого підходу було розвинуто та узагальнено у роботах Коуена (Cohen), Голдрейча (Goldreich) та Віджерсона (Widgerson) [2] та закінчено Цукерманом (Zuckerman) в

[4], який ввів поняття (засноване на min-ентропії) «слабких випадкових джерел» та конструкцій екстракторів (хоча термін «екстрактор» був запропонований пізніше Наомом Нісаном (Naom Nisan) та Цукерманом в [5]).

Взагалі проблема отримання незалежної та рівноімовірної послідовності із невеликого набору взаємно незалежних слабковипадкових послідовностей $X_1,\ldots,X_k$ вважалася нерозв'язаною [5] до недавньої роботи Барака (Barak) та інших [5], зробивший, можливо, крупне досягнення в комбінаториці [6]. Зараз це направлення активно досліджується [6,6].

Інше направлення, яке дозволяє отримувати криптографічно якісну ВП, розглянуто в [6] і притримується моделі єдиної вхідної слабковипадкової послідовності X, та розглядається наступне: наприклад, ми маємо високоякісний рандомізований алгоритм (із здатністю робити дійсно випадкові вибори) і маємо вхідну послідовність X. Чи можемо ми стверджувати, що вихід $A(X)$ – може бути рівноімовірним та некорельованим?

Така постановка питання вирішується існуючим на теперішній час широким класом так званих екстракторів та диспергаторів. Дослідження з цього направлення, визначення, існуючі реалізації та їхні класифікації, аналіз, порівняння та ефективне застосування можна знайти у роботах [6].

Із зробленого аналізу сучасних методів та засобів генерації ВП у криптографічних додатках можна зробити висновки:

– для ефективного функціонування, підвищенні стійкості та криптоживучості сучасні КС потребують генераторів ВП із сильними криптографічними якостями, здатні працювати у різних умовах експлуатації;

– проблема генерації високоякісних ВП із подальшим криптографічним застосуванням – складна теоретико-практична задача, яка торкається різних областей знань: квантової механіки, теорії ймовірностей, теорії інформації, теорії складності тощо;

– відсутнє існування єдиного уніфікованого підходу до побудови якісних криптографічних ГВП, які б мали з одного боку просту, недорогу та надійну технічну реалізацію, а з іншого – можливість генерувати стабільну, рівноімовірну та незалежну ВП;

– для усіх підходів генерації ВП необхідна наявність одного або декілька первинних датчиків невизначеності, тобто фізичних ГВП.

Генерація випадкових послідовностей на основі ймовірнісно-криптографічних перетворень слабковипадкових послідовностей. Одним із сучасних науково-технічних рішень задачі побудови єфективних ГВП є використання для генераторів ВП положень теорії ймовірнісно-криптографічних перетворень, яка базується на концепції відвідного каналу А Вайнера [40] та досліджена в [41-43]. Метод, який дозволяє реалізувати цей підхід, названий авторами «методом кодової генерації випадкових послідовностей (КГВП)» [38].

У запропонованому методі підвищення криптографічних властивостей ВП відбувається за рахунок використання спеціального надлишкового випадкового кодування первинних ВП у суміжних класах (СК) групового систематичного $(n,n-k)$-коду V [38].

Двійковому вектору s_i розмірністю k біт деякої випадкової послідовності ставиться у відповідність i-й (з 2^k) суміжний клас групового систематичного $(n,n-k)$-коду V. Потім, випадковим образом вибирається одне з кодових слів із цього СК. На кодове слово накладається вектор випадкової послідовності, відбувається перехід слова в інший СК. Результат такого переходу є блоком результуючої ВП.

Метод доведений до конструктивної реалізації, заснований на одержанні ВП заданої криптографічної якості на основі випадкового кодування в суміжних класах деякого коду виходів первинних джерел ентропії, які володіють, з одного боку, низькими криптографічними властивостями, а з іншого боку – прийнятними, з погляду технічної реалізації, параметрами.

Аналіз криптографічних властивостей ВП. Для аналізу ефективності ГВП необхідно проводити теоретичне та експериментальне дослідження кореляційних параметрів та

властивостей генеруемих послідовностей, що дозволить конструктивно підходити до побудови засобів генерації ВП для високоефективних криптографічних засобів.

Для об'єктивного дослідження властивостей ВП як правило використовують набори статистичних тестів. На теперішній час існує декілька наборів щодо дослідження випадкових послідовностей на різноманітні статистичні дефекти, в тому числі і на кореляційні. Із найбільш поширених та відомих наборів відносять:

– стандартизований у 1999 році спеціалістами NIST пакет Statistical Test Suite (на сьогоднішній день є найкращим);

– пакет статистичних тестів DIEHARD Джорджа Марсаглія (George Marsaglia) розроблений у 1995 році (http://stat.fsu.edu/~geo/diehard.html);

– пакет статистичних тестів CRYPT–X, розроблений Квінтсенським (Австралія) університетом технологій (http://www.isi.qut.edu.au/resources//cryptx/tests.php);

– набір статистичних тестів, заснованих на емпіричних, теоретичних та спектральних критеріях, запропонованих Д. Кнутом (Donald E. Knuth) в [15].

Треба зазначити, що деякі статистичні тести є однаковими у всіх зазначених пакетах, та для всіх пакетів існують програмні реалізації, які доступні у глобальній мережі Internet для вільного використання.

ЛІТЕРАТУРА

1. *Elias P.* The Efficient Construction of an Unbiased Random Sequence // Ann. Math. Statist. –1972. –Vol.43 № 3. –P. 864–870.

2. *Chor B., Goldreich O.* Unbiased bits from sources of weak randomness and probabilistic communication complexity // SIAM Journal on Computing. –1988. –Vol.17, № 2. –P. 230–261.

3. *Cohen A., Wigderson A*. Dispersers, deterministic amplification, and weak random sources // In Proceedings of the 30th IEEE Symposium on Foundations of Computer Science. –1989. –P. 14–19.

4. *Zuckerman D.* General weak random sources // In Proceedings of the 31st IEEE Symposium on Foundations of Computer Science. –1990. –P. 534–543.

5. *Barak B., Impagliazzo R., Wigderson A.* Extracting randomness using few independent sources // In Proceedings of the 45th IEEE Symposium on Foundations of Computer Science. –2004. –P. 384–393.

Надійшла: 16.10.2012р.

Рецензент: д.т.н., проф. Шелест Є.М.