УДК 004.421.5

М. Мандрона[1], В. М. Максимович[2], Ю. М. Костів[2], О. І. Гарасимчук[3]
Національний університет "Львівська політехніка"
[1]Львівський державний університет безпеки життєдіяльності
кафедра управління інформаційною безпекою,
[2]кафедра безпеки інформаційних технологій,
[3]кафедра захисту інформації

ПРОЕКТУВАННЯ ГЕНЕРАТОРІВ ПСЕВДОВИПАДКОВИХ БІТОВИХ ПОСЛІДОВНОСТЕЙ ЗА СИСТЕМНО-ТЕОРЕТИЧНИМ ПІДХОДОМ

Проаналізовано підходи до проектування генераторів псевдовипадкових бітових послідовностей. За допомогою системно-теоретичного підходу спроектовано модифікований адитивний генератор Фібоначчі та наведено результати його дослідження, зокрема періоду повторення, статистичних характеристик, лінійної складності, об'єму ключової інформації (довжини ключа) і швидкодії.

Ключові слова: криптографічні пристрої, потокові шифри, генератори псевдовипадкових послідовностей, статистичні характеристики.

The approaches to designing the pseudorandom bit sequences generators are analyzed. By means of system-theoretical approach the modified additive Fibonacci's generator is projected and results of it research are given, in particular: period of repetition, statistical characteristics, linear complication, volume of key information (key length) and swiftness.

Key words: cryptographic devices, stream ciphers, generators of pseudorandom sequences, statistical characteristics.

Вступ

Сучасна наука широко використовує генератори псевдовипадкових бітових послідовностей (ГПВБП) у різних системах. У сфері захисту інформації псевдовипадкові числа використовують як у технічних, так і у криптографічних засобах захисту інформації. Відомо, що характеристики систем безпеки залежать від характеристик їх підсистем, які визначаються не тільки використаними алгоритмами, але й якісними показниками використаних псевдовипадкових послідовностей. Оскільки безпеку криптосистеми зосереджено на ключі, то з використанням ненадійного процесу генерації ключів уся криптосистема стає вразливою. Тому актуальним є питання побудова якісних, надійних ГПВБП.

Метою роботи було проаналізувати різні способи проектування генераторів псевдовипадкових послідовностей та використати системно-теоретичний підхід для побудови модифікованого адитивного генератора Фібоначчі (МАГФ).

Підходи до проектування генераторів псевдовипадкових бітів

У роботах [1, 2] зазначено, що існує чотири різні підходи до проектування потокових шифрів, які повною мірою можна віднести і до проектування ГПВБП – невід'ємної складової цих шифрів:

- системно-теоретичний підхід;
- інформаційно-теоретичний підхід;
- складнісно-теоретичний підхід;
- рандомізований підхід.

За системно-теоретичним підходом криптограф розробляє ГПВБП із характеристиками безпеки, які можна перевірити – періодом повторення, статистичними характеристиками, лінійною складністю тощо. Криптограф також вивчає різні методи криптоаналізу цих генераторів і перевіряє їх стійкість до зламу.

За інформаційно-теоретичним підходом допускається, що криптоаналітик має необмежений час і обчислювальну потужність. Єдиним потоковим шифром, що практично є незламним для криптоаналітика і реалізується за таким підходом, є одноразовий блокнот чи, інакше кажучи, одноразовий рядок. При цьому для шифрування і дешифрування використовується ідентичний потік бітів. Якщо бітовий потік є випадковим і використовується тільки один раз, безпека буде абсолютною. Однак одноразовість використання бітового потоку і є основним недоліком такого підходу.

Відповідно до складнісно-теоретичного підходу криптограф використовує теорію складності для доведення безпеки генераторів. Отже, генератори повинні бути якомога складнішими, базуватись на тих самих проблемах, що й криптографія з відкритими ключами (обчислення дискретних логарифмів, розкладання на множники тощо). Такі генератори мають невисоку швидкодію і, при апаратній реалізації, є громіздкими.

За допомогою рандомізованого потокового шифру криптограф намагається створити для криптоаналітика проблему, що практично не вирішується. Для цього, зберігаючи невеликий розмір секретного ключа, криптограф значно збільшує кількість бітів, з якими доведеться мати справу криптоаналітику. Це може бути реалізовано завдяки використанню при шифруванні і дешифруванні великого опублікованого випадкового рядка. При цьому ключ вказує, які частини рядка буде використано.

Особливості системно-теоретичного підходу

Розглянуто адитивні генератори Фібоначчі при їх апаратній реалізації на елементній базі цифрової техніки. Під час проектування таких генераторів природним є використання системно-теоретичного підходу.

Це пояснюється тим, що, по-перше, алгоритм роботи генераторів Фібоначчі не можна віднести до теоретично складних. По-друге, інформаційно-теоретичний і рандомізований підходи до проектування використовують для проектування генераторів Фібоначчі для потокових шифрів типу одноразового рядка, що не є предметом досліджень у цій роботі. Однак це не заперечує можливість адаптації запропонованих генераторів до потокових шифрів згаданого типу.

За системно-теоретичним підходом до проектування ГПВБП необхідно їх перевіряти на відповідність таким критеріям [1, 2]:

– великий період повторення;
– велика лінійна складність;
– статистичні характеристики;
– плутанина: кожний біт вихідного потоку повинен бути складним перетворенням усіх чи більшості бітів ключа;
– дифузія: надлишковість в структурних елементах повинна розсіюватись, спричиняючи більш “розмазану” статистику;
– критерії нелінійності для логічних функцій, таких як відсутність кореляції m-го порядку, відстань до лінійних функцій тощо.

Розробляючи нові ГПВБП, треба пам’ятати, що криптографія – це суміш математики і плутанини, і без плутанини математика може бути використана проти вас [2].

Головною проблемою генераторів, розроблених за допомогою системно-теоретичного підходу, є неможливість доведення їх безпеки. ГПВБП може відповідати усім правилам розробки, але бути небезпечним – некрипостійким. Інший може бути цілком безпечним. Отже, процес проектування ГПВБП є достатньо евристичним [2].

За системно-теоретичним підходом до проектування ГПВБП їх оцінюють за такими параметрами:

– період повторення при різних початкових станах структурних елементів;
– статистичні характеристики;
– лінійна складність;
– об’єм ключової інформації (довжина ключа);
– швидкодія.

Дослідження характеристик ГПВБП на основі МАГФ

Дослідження генератора на відповідність сформульованим вище вимогам запропоновано нами в роботах [3–4]. Цей генератор є базовим і може розглядатись як окрема ланка для створення складніших багатоланкових пристроїв. Правила побудови багатоланкових генераторів є окремою задачею, яка подібна до задачі побудови РЗЛЗЗ і генераторів з використанням R-блоків на основі примітивних поліномів [5].

Структурну схему ГПВБП на основі МАГФ наведено на рис. 1 [3–4].

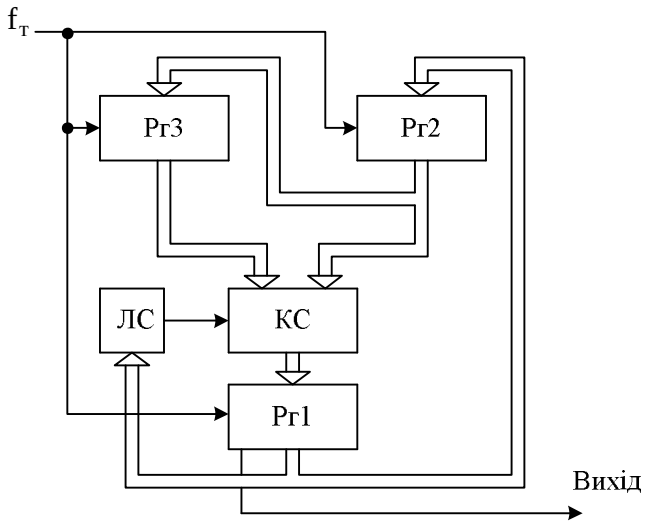

Рис. 1. Структурна схема ГПВБП на основі МАГФ

До його складу входять регістри Рг1-Рг3, комбінаційний суматор КС і логічна схема ЛС. Роботу генератора описують рівняннями:

$$\begin{aligned} Q_1(t+1) &= [\,Q_2(t)+Q_3(t)+a\,]\ mod\ 2^n, \\ Q_2(t+1) &= Q_1(t), \\ Q_3(t+1) &= Q_2(t), \end{aligned} \qquad (1)$$

де $Q_1(t)-Q_3(t)$ і $Q_1(t+1)\text{-}Q_3(t+1)$ – числа в регістрах Рг1 – Рг3 в поточному і наступному тактах роботи, значення змінної “а” визначається рівнянням

$$a = a_0\ xor\ a_1\ xor\ a_2 \ldots xor\ a_z, \qquad (2)$$

де a_i $(i=0,1,...,z;\ z\le n\text{-}1)$, в даному випадку, значення двійкових розрядів числа Q_1 в регістрі Рг1, а n – кількість двійкових розрядів Рг1 – Рг3 і КС.

Дослідження періоду повторення. Період повторення ГПВБВ на основі МАГФ досліджували за допомогою імітаційної моделі. Період фіксували в моменти повторення значень чисел у регістрах Рг1 – Рг3. Складність дослідження полягає в тому, що період повторення потрібно визначати для усіх можливих комбінацій значень початкових чисел у регістрах. При достатньо великих кількостях двійкових розрядів структурних елементів пристрою ця задача практично не вирішується через неприйнятно великий час моделювання. Так, наприклад, при $n=10$ для повного перебору необхідно $2^{3n}=2^{30}\approx 10^9$ кроків (тактів). Якщо частота кроків перебору дорівнює $f_п=10^9$ Гц, час повного дослідження займе одну секунду. Якщо $n=20$, для повного перебору потрібно $2^{3n}=2^{60}\approx 10^{18}$ кроків, що за тієї самої частоти перебору займе 10^9 с, або приблизно 32 роки.

Тому прийняли рішення дослідити періоди повторення генератора для малих значень n, виявити певні закономірності, які можна перенести на велику кількість розрядів.

На рис. 2 наведено результати дослідження періодів повторення генератора – T_p для кількох значень n. Тут

$$Q_0 = Q_{3\_0} + Q_{2\_0} \cdot 2^n + Q_{1\_0} \cdot 2^{2n}, \qquad (3)$$

де Q_{1_0}, Q_{2_0} і Q_{3_0} – початкові числа в Рг1, Рг2 і Рг3.

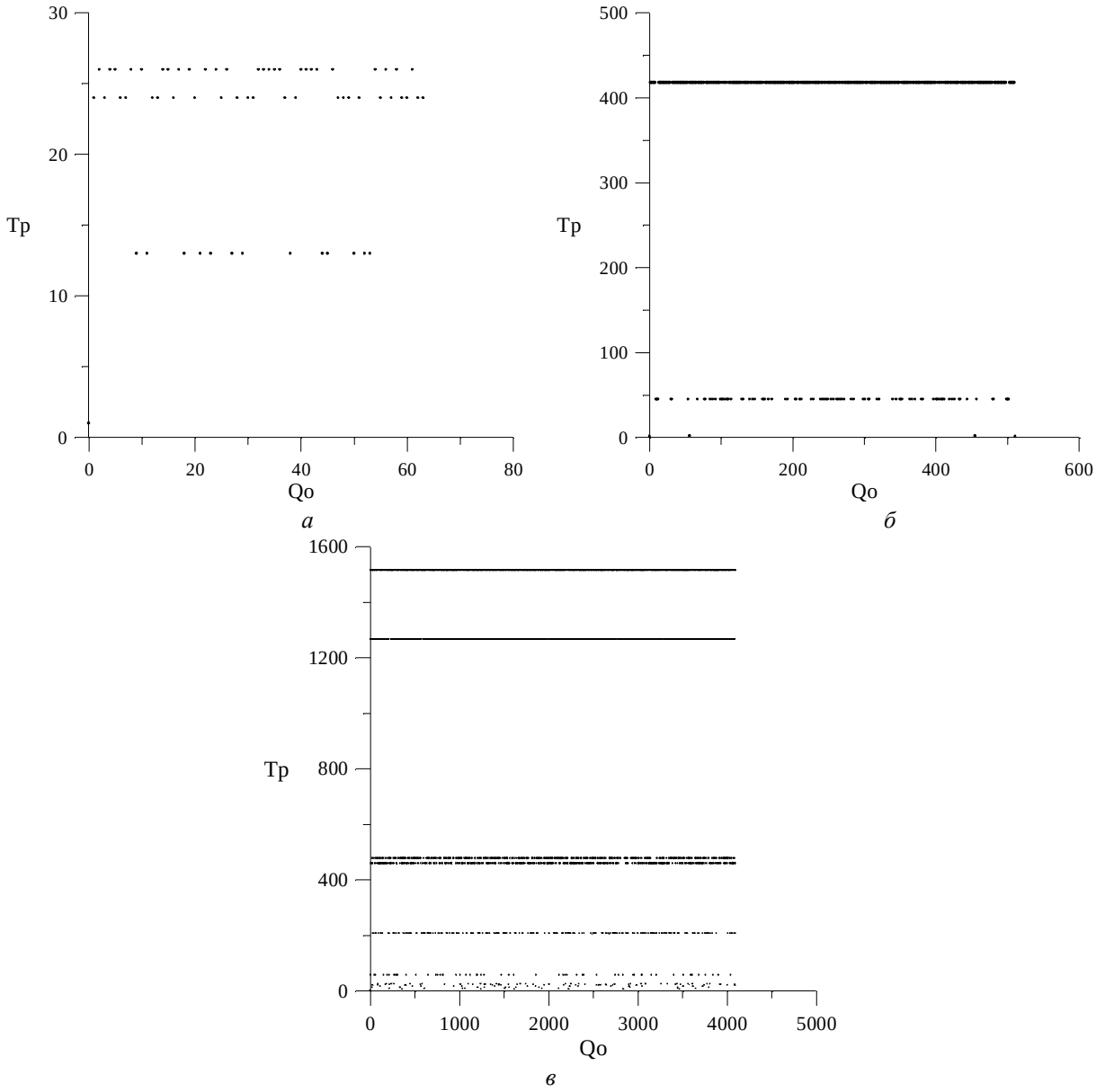

Рис. 2. Залежності періодів повторення T_p від початкових станів Q_0 регістрів Рг1 - Рг3: а – $n = 2$; б – $n = 3$; в – $n = 4$

Наведені результати дають змогу зробити такі висновки стосовно ГПВБП на основі МАГФ:

– період повторення T_p істотно залежить від початкових станів регістрів Q_0 (аналогічна залежність спостерігається і в інших ГПББП, наприклад, на основі РЗЛЗЗ чи R-блоків [6]);

– максимальні значення T_p з ростом числа розрядів n швидко збільшуються;

– понад половини значень T_p є близькими до максимальних (50 з 63 перевищують 23 при n=2, 418 з 511 перевищують 417 при n=3, 2783 з 4095 перевищують 1266 при n=4).

Надалі досліджували період повторення генератора таким чином. При $1 \le n \le 6$ визначали максимальне значення T_p при переборі усіх можливих значень Q_{1_0}, Q_{2_0} і Q_{3_0}. При $7 \le n \le 8$ фіксували значення Q_{1_0}=0, Q_{2_0}=0 і здійснювали повний перебір значень Q_{3_0}. При $n \ge 9$ було зафіксовано значення Q_{1_0}=0, Q_{2_0}=0, Q_{3_0}=2. Значення Q_{1_0}, Q_{2_0} і Q_{3_0}, що фіксували, враховуючи результати попередніх досліджень з метою досягнення максимально можливих значень T_p.

Результати дослідження максимальних значень T_p наведено в таблиці.

Результати дослідження ГПВБП на основі МАГФ

Кількість розрядів n	Множина значень $Q_0^M = 2^{3n}$	Максимальне значення періоду повторення		Результати тестування (тести NIST)	Статистично безпечна множина $Q_0{}^c = 2^{3n-1}$
		$T_{p_{max}}$	Умови визначення		
1	2^3	4	Перебір Q_{1_0}, Q_{2_0} і Q_{3_0}	-	–
2	2^6	26		-	–
3	2^9	418		-	–
4	2^{12}	1516		-	–
5	2^{15}	17320		-	–
6	2^{18}	226256		-	–
7	2^{21}	878868	Q_{1_0}=0, Q_{2_0}=0 перебір Q_{3_0}	-	–
8	2^{24}	11984790		-	–
9	2^{27}	49559052	Q_{1_0}=0, Q_{2_0}=0 і Q_{3_0}=2	-	–
10	2^{30}	727654100		-	–
11	2^{33}	$>10^9$		-	–
12	2^{36}	$>10^9$		-	–
13	2^{39}	$>10^9$		-	–
14	2^{42}	$>10^9$		-	–
15	2^{48}	$>10^9$		-	–
16	2^{48}	$>10^9$		-	–
17	2^{51}	$>10^9$		-	–
18	2^{54}	$>10^9$		-	–
19	2^{57}	$>10^9$		-2	–
20	2^{60}	$>10^9$		-1	–
21	2^{63}	$>10^9$		-1	–
22	2^{66}	$>10^9$		-1	–
23	2^{69}	$>10^9$		+	2^{68}
24	2^{72}	$>10^9$		+	2^{71}

Дослідження статистичних характеристик включно з лінійною складністю. Статистичні характеристики досліджували за допомогою тестів NIST [6], що містять і визначення лінійної складності. Тестували бітову послідовність завдовжки 10^9 бітів, яку знімали з молодшого розряду регістра Рг1. Результати тестування наведено в таблиці. Тут прийнято такі позначення: "-" – більшість тестів не пройдено; "-2", "-1" – не пройдено 2 чи1 тести; "+" – усі тести пройдено.

Отже, при $n \geq 23$ сформована бітова послідовність відповідає вимогам статистичної безпеки.

Визначення об'єму ключової інформації (довжини ключа). Криптографічним ключем цього генератора є початковий стан регістрів Рг1 – Рг3. Повна множина значень цих станів дорівнює $Q_0 = 2^{3n}$ при довжині ключа $3n$. Однак статистично безпечною можна вважати тільки ту множину, яка відповідає вихідним бітовим послідовностям, що проходять усі тести NIST. За результатами попередніх досліджень, ця множина містить не менше $Q_0{}^c = 2^{3n-1}$ значень, що відповідає довжині ключа $3n$-1. Для конкретного окреслення цієї множини необхідно виявити закономірності впливу її значень на період повторення і статистичні характеристики вихідного сигналу за відносно малих значень n з відповідними узагальненнями на будь-які значення n.

Дослідження швидкодії. Швидкодію генератора визначають за максимальним часом, необхідним для завершення перехідного процесу в схемі – t_{nn}, який починається в момент надходження на тактовий вхід робочого фронту імпульсу і завершується формуванням нового значення числа на виході КС:

$$t_{пп} = t_{Рг} + t_{ЛС} + t_{КС}, \quad (4)$$

де $t_{Рг}$, $t_{ЛС}$ і $t_{КС}$ – час спрацювання Рг, ЛС і КС відповідно. Максимально можлива частота тактових імпульсів дорівнює:

$$f_{m_{max}} = \frac{1}{t_{пп}} = \frac{1}{t_{Рг} + t_{ЛС} + t_{КС}}. \quad (5)$$

Отже, швидкодія генератора насамперед, залежить від часу спрацювання КС і ЛС, оскільки регістри пам'яті Рг1 – Рг3 працюють синхронно, і затримка їх спрацювання дорівнює затримці спрацювання одного тригера.

Швидкодію КС можна збільшити використовуючи відомі способи побудови комбінаційних суматорів з паралельним і послідовно-паралельним перенесенням, що не впливає на період повторення генератора та його статистичні характеристики.

Час спрацювання логічної схеми ЛС залежить від схемотехніки її реалізації і від кількості членів рівняння (2), яка може бути різною. Зменшення цієї кількості дає змогу істотно підвищити швидкодію пристрою загалом. Однак, оскільки таке зменшення може вплинути на період повторення пристрою і його статистичні характеристики, необхідно проводити відповідні дослідження (визначення періоду повторення і тестування на відповідність статистичним характеристикам), що для окремих випадків реалізації ГПВБП на основі МАГФ було нами виконано в роботах [3, 4].

Висновки

Запропонований ГПВБП на основі модифікованого адитивного генератора Фібоначчі, який побудований за системно-теоретичним підходом при визначеній кількості розрядів його структурних елементів, повністю відповідає вимогам статистичної безпеки і може бути використаний у криптографічних системах.

1. Rueppel R. A. Stream Cipher, Contemporary Cryptology: The Science of Information Integrity, G. J. Simmons, ed., IEEE Press, 1992, pp. 65-134. 2. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке СИ. – М.: Изд-во "Триумф", 2002. – 797 с. 3. Мандрона М. Н. Исследование статистических характеристик модифицированных генераторов Фибоначчи / М. Н. Мандрона, В. Н. Максымовыч // Проблемы управления и информатики : межд. наук.-техн. журн. – 2014. – № 6. – С. 28–36. 4. Максимович В. М. Апаратна реалізація і дослідження модифікованих генераторів Фібоначчі / В. М. Максимович, О. І. Гарасимчук, Ю. М. Костів, М. М. Мандрона // Комп'ютерні технології друкарства : збірник наукових праць. – Львів : Вид-во Української академії друкарства. – 2013. – № 29. – С. 167–174. 5. Иванов М. А., Чугунков И. В. Криптографические методы защиты информации в компьютерных системах и сетях: учебное пособие / Под ред. М. А. Иванова. – М.: НИЯУ МИФИ, 2012. – 400 с. 6. NIST SP 800-22. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications. April, 2010.