УДК 681.324

І.В. Васильцов[*], Б.З. Карпінський[*], А.Ю. Федоров[#]
[*]Тернопільська академія народного господарства,
кафедра безпеки інформ. технологій
[#]College of William and Mary, Department of Computer Science

ДОСЛІДЖЕННЯ СТАТИСТИЧНИХ ХАРАКТЕРИСТИК ГЕНЕРАТОРА ПСЕВДОВИПАДКОВИХ ПОСЛІДОВНОСТЕЙ ПОБУДОВАНОГО НА БАЗІ РЕГІСТРА ЗСУВУ

Розглянуто результати дослідження статистичних характеристик генератора псевдовипадкових послідовностей побудованого на базі регістра зсуву. Отримані результати дають змогу розробити методику експериментальних досліджень для криптоаналізу апаратної реалізації поточних шифрів.

In this paper the results of the investigation of the statistical parameters of the linear feedback shift register (LFSR) generator have been considered. Obtained results allow to develop the techniques of the experimental investigation for differential analysis of the flow chippers.

Стрімкий розвиток сучасних комп'ютерних систем обробки інформації зумовлює підвищення актуальності задач захисту інформаційних ресурсів від різних типів несанкціонованого доступу. Суть криптографічних засобів захисту інформації полягає у використанні спеціальних методів та алгоритмів перетворення вихідних даних в шифр-текст. Такі перетворення дають змогу вирішити дві основні задачі захисту інформації: конфіденційності та цілісності інформаційних ресурсів. З іншого боку, зрозуміло, що об'єми інформаційних ресурсів, котрі необхідно захищати від зловмисних впливів, також постійно зростають, а тому ефективне вирішення задач захисту інформації можливе лише за умови використання апаратних засобів, що реалізують ті чи інші криптоалгоритми. Тому сучасні системи захисту інформації, як правило, завжди володіють такими апаратними засобами, які побудовані на сучасній елементній базі мікроелектроніки.

Разом з тим, розвиваються методи та засоби криптоаналізу, які дають змогу отримати доступ до інформації (чи порушити її цілісність) за відсутності ключової інформації. Одним із нових та досить ефективних методів криптоаналізу є диференційний аналіз помилок, який передбачає навмисну фізичну дію на шифруючий пристрій з метою формування апаратних похибок в регістрах, що містять перетворювані дані [1]. Досвід показує, що застосування цього методу криптоаналізу дає позитивні результати при атакуванні як симетричних, так і асиметричних криптосистем захисту інформації [2]. Реалізація такого методу базується на використанні: а) вмонтованих апаратних закладок у шифруючому пристрої, які реагують на певну кодову комбінацію; б) зовнішніх впливів, що призводять до виникнення збоїв у шифруючому пристрої.

Формування задачі аналізу базується на таких припущеннях: криптоаналітик має вільний доступ до шифруючого пристрою з ключами, криптоаналітик також має можливість впливати на шифруючий пристрій за допомогою зовнішніх дестабілізуючих

факторів, щоб викликати збої. Цей напрям активно досліджується, проте розробляється в основному етап побудови спеціалізованих алгоритмів обробки статистичної інформації [3], причому приймається *a priori*, що задача отримання статистичних даних в режимі виникнення збоїв успішно вирішена. Відомо, що мікроелектронні пристрої, виготовлені на основі напівпровідникових матеріалів, характеризуються чутливістю до зовнішніх дестабілізуючих факторів. У якості таких факторів найчастіше виступають температура навколишнього середовища, нестабільність напруги живлення та електромагнітне випромінювання [4]. Про те, як правильно вибрати параметри такого впливу, як довго та як інтенсивно піддавати впливу, щоб отримати ефективні результати, у відкритій літературі інформації не наведено. Тому завдання дослідження впливу параметрів зовнішніх дестабілізуючих факторів на ефективність криптоатаки на основі апаратних помилок є важливим та актуальним, оскільки результати таких досліджень дадуть змогу розробити рекомендації щодо побудови нових методів, алгоритмів та пристроїв захисту інформації, стійких до цього виду атак.

Раніше [5] авторами була розроблена структура макета для дослідження криптоатаки на основі апаратних помилок. У якості досліджуваного пристрою вибрано апаратну реалізацію алгоритму гамування, оскільки цей алгоритм достатньо добре вивчений і просто реалізується, а також нечутливий до розмноження похибок під час процедури шифрування/дешифрування інформації. Окрім того, цей клас шифрів характеризується високими швидкісними показниками, що дає змогу застосовувати його в системах реального часу.

На рис. 1. зображено узагальнену структуру макета для експериментального дослідження стійкості пристрою гамування до криптоатаки на основі апаратних помилок. За допомогою такого макета можна досліджувати вплив температури, нестабільності напруги живлення та електромагнітного випромінювання на функціональні вузли пристрою гамування (генератор псевдовипадкових послідовностей (ГПВЧ), регістри ключів, лінії зв`язку регістра ключів із іншими функціональними вузлами).

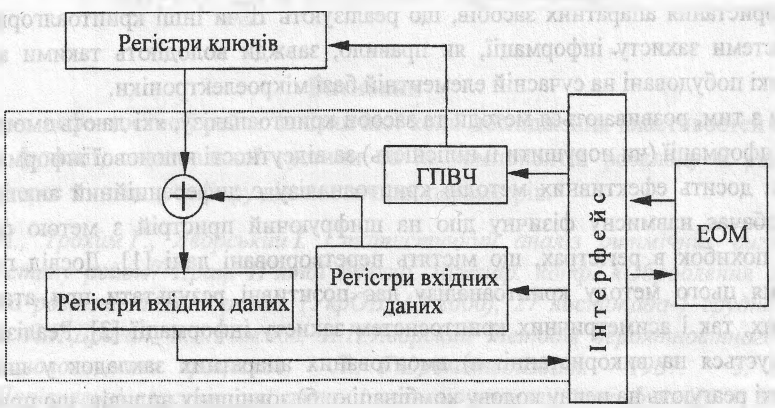


Рис. 1. Узагальнена структура макету

Одним із ключових функціональних вузлів цього макета є генератор псевдовипадкових послідовностей. Для генерації псевдовипадкових послідовностей

існують різні методи [6, 7], проте до всіх цих методів ставляться однакові вимоги: простота генерування послідовності, великий період, рівномірний розподіл. Оптимальним методом у всіх трьох аспектах вважається метод, що базується на використанні лінійних рекурентних співвідношень. Саме цей метод було вибрано для генерації псевдовипадкових чисел. Для реалізації цього методу використовують лінійні регістри зсуву з оберненим зв'язком.

Генератор складається із лінійного регістра зсуву із зворотними зв'язками (linear feed-back shift register – LFSR), об'єднаними за модулем 2 з одиничним значенням суматора [8]. Кожному такому LFSR регістру довжиною n можна поставити у відповідність поліном зворотних зв'язків h(x) із двійковими коефіцієнтами вигляду:

$$h(x) = h_n x_n + h_{n-1} x_{n-1} + ... + h_1 x + h_o \qquad (1)$$

Також слід зауважити, що h_n дорівнює 1, оскільки в іншому випадку зменшиться степінь полінома, що призведе до отримання вихідної послідовності псевдовипадкових чисел з меншим періодом.

Поліноми зворотних зв'язків степеня n називають також породжуючими поліномами.

Відомо, що за умови, коли $h(x)$ є примітивним поліномом степеня n, то кожен з $2^n - 1$ початкових станів регістра зсуву генерує вихідну послідовність максимально можливого періоду $2^n - 1$ [8, 9].

Для побудови методики проведення експерименту слід попередньо оцінити статистичні характеристики генератора псевдовипадкових послідовностей. У відкритій літературі наведено математичні співвідношення, що дають змогу побудувати генератори лише з максимальним періодом на базі сильно розріджених поліномів [9]. В той час як для проведення експерименту необхідно проаналізувати ефективність використання диференційного аналізу LFSR генератора, побудованого на основі довільних поліномів.

Для реалізації макета запропоновано використати стандартний паралельний інтерфейс ЕОМ з вісьмома лініями даних [5], тому за предмет дослідження вибрано 8-бітні поліноми. На рис. 2 зображено залежність періоду генерування псевдовипадкової послідовності чисел на базі регістра зсуву від полінома, представленого у вигляді десяткового числа при нульовому ініціалізуючому векторі.

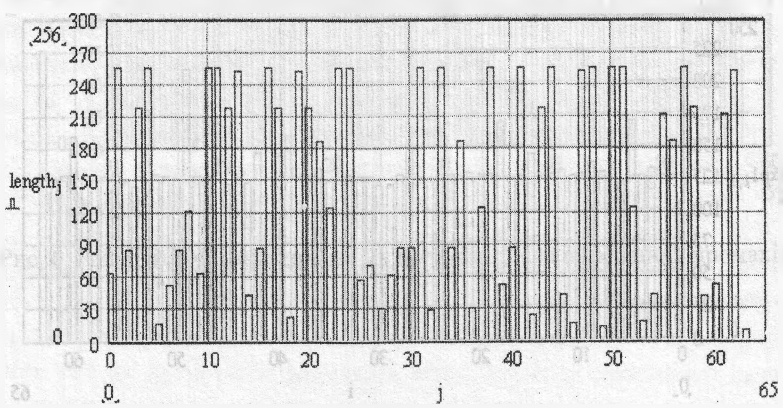
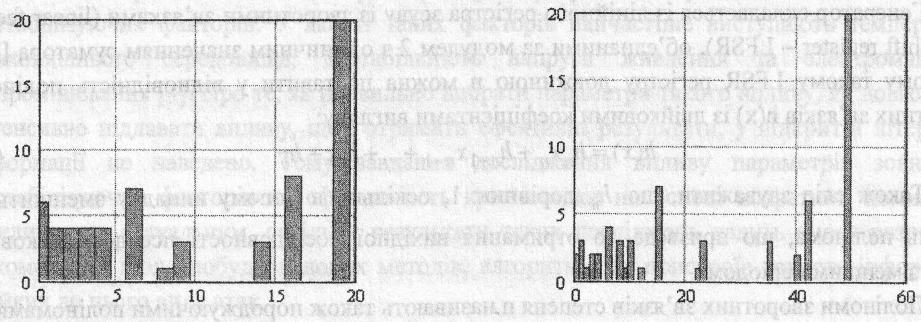


Рис. 2. Період генерування псевдовипадкових чисел

Як видно з рис. 2 для 8-бітного LFSR-генератора можна побудувати доволі багато поліномів з великим періодом генерування чисел. Зокрема виявлено, що для періоду L>211 можна використати 28 поліномів. На рис. 3 зображено гістограми розподілу періоду генерування залежно від кількості інтервалів у діапазоні чисел.



а б

Рис. 3. Гістограма періоду генерування:
а) при кількості інтервалів 20;
б) при кількості інтервалів 50

Аналіз рис. 3. показує, що розподіл періодів генерування має яскраво виражений характер і в обидвох випадках кількість поліномів з максимальним періодом рівна 20.

Окремо необхідно дослідити рівномірність розподілу стосовно нулів та одиниць, оскільки в [7, 8, 9] показано, що ключі з рівномірним розподілом нулів і одиниць характеризуються максимальною криптостійкістю.

На рис. 4 та рис. 5 зображено розподіли кількості значень типу нуль та одиниця для максимального періоду при нульовому значенні ініціалізуючого вектора. Слід звернути увагу, що розподіли значень "нуль" мають більшу вагу для даного полінома. З іншого боку, для ТТЛ-логіки запас завадостійкості для сигналу типу "логічний нуль" є меншим [4]. Цю особливість необхідно враховувати при проведенні експериментальних досліджень.

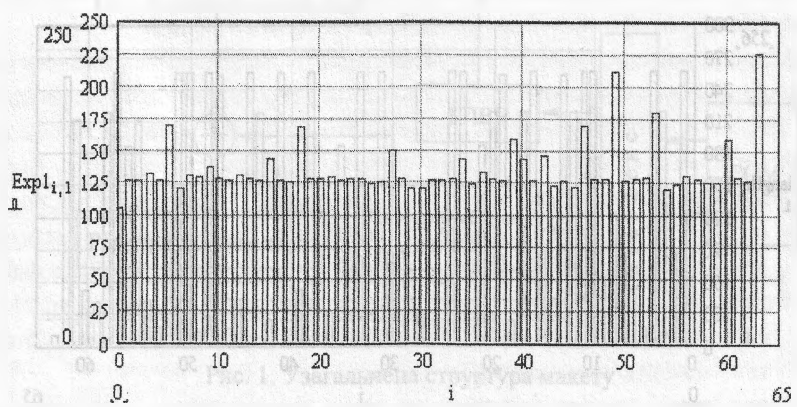


Рис. 4. Розподіл нульових значень в поліномі залежно від кодової комбінації

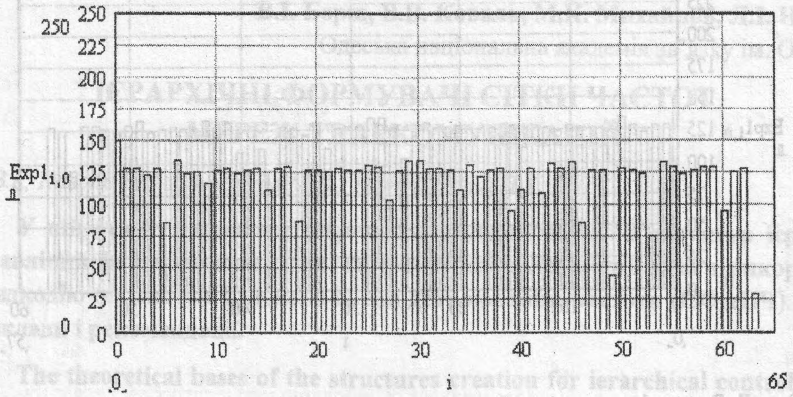


Рис. 5. Розподіл одиничних значень в поліномі в залежності від кодової комбінації

Отримані співвідношення симулювалися за умови використання максимально можливої довжини ключа для 8-бітного регістра зсуву. Оскільки деякі поліноми не є примітивними, то відповідні їм згенеровані результати будуть виродженими. Тому для підвищення адекватності оцінки рівномірності розподілу необхідно провести робастну обробку результатів експерименту. Для відкидання промахів використано критерій Шовене [10]. На рис. 6 та рис. 7 зображено результати експерименту після двократного застосування критерію Шовене.

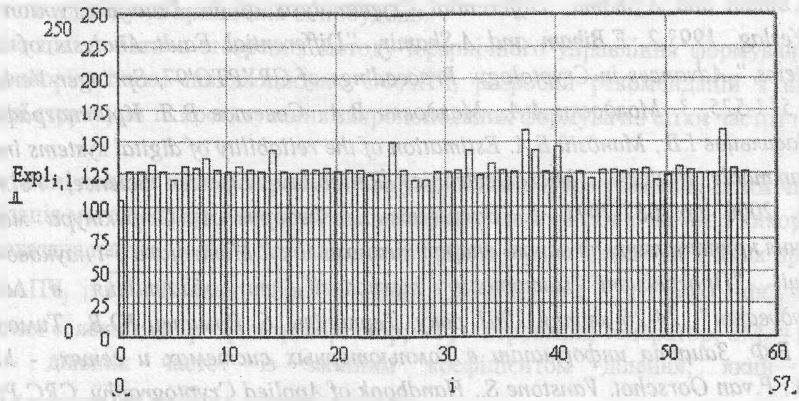


Рис. 6. Розподіл нульових значень в поліномі після відкидання промахів

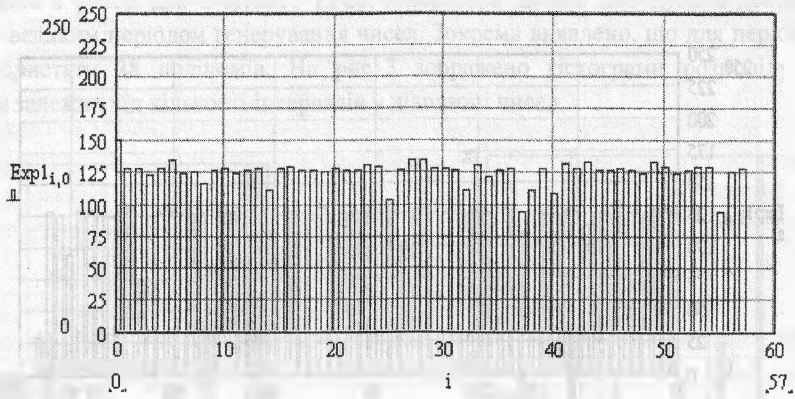


Рис. 7. Розподіл одиничних значень в поліномі після відкидання промахів

Для оцінки рівномірності розподілу отриманих результатів використано критерій χ^2. Аналіз показав, що для розподілу нульових значень можна прийняти гіпотезу про рівномірний закон розподілу з імовірністю 0.995, а для розподілу одиничних - з імовірністю 0,928.

Отримані статистичні результати дають змогу оцінити розподіли генерованих чисел. Це, своєю чергою дозволить побудувати ефективну методику проведення експериментальних досліджень для диференційного аналізу криптопристроїв гамування на основі LFSR-генератора.

1. E.Biham and A.Shamir, Differential Cryptanalysis of the Data Encryption Standard, Springer-Verlag, 1993.2. E.Biham and A.Shamir, "Differential Fault Analysis of Secret Key Cryptosystems," Advances in Cryptology: Proceedings of CRYPTO'97, Springer-Verlag, August 1997, pp. 513-525. 3. Молдовян А.А., Молдовян В.А., Советов В.Я. Криптография.– Спб., 2000. 4. Васильцов І.В., Мандзій Б.А. Estimation of the reliability of digital systems implemented on programmable devices . Microelectronics Reliability, Elsevier Science, Vol:40 Iss:12, November, 2000 pp.2087-2093. 5. Васильцов І., Федоров А. Структура макету для дослідження криптоатаки на основі апаратних помилок // Матеріали 5-ї науково-технічної конференції "Прогресивні матеріали, технології та обладнання в машино- і приладобудуванні", 24-26 квітня 2001 року, Тернопіль. 6. Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф. Защита информации в компьютерных системах и сетях, - М., 1999.7. Menezes A., P.van Oorschot, Vanstone S., Handbook of Applied Cryptography, CRC Press, 1996. 8. Гундарь К.Ю., Гундарь А.Ю., Янишевський Д.А. Защита Информации в компьютерных системах. К., 2000г. 9. http://www.unix.kg/cgi-bin/document.pl?lang=rus&id=17. 10. Дж.Тейлор. Введение в теорию ошибок. М., 1985.