УДК 004.056; 004.421.5

В.Н. Максымовыч, М.Н. Мандрона, О.И. Гарасимчук, Ю.М. Костив

ИССЛЕДОВАНИЕ ХАРАКТЕРИСТИК МОДИФИЦИРОВАННОГО АДДИТИВНОГО ГЕНЕРАТОРА ФИБОНАЧЧИ С ЗАПАЗДЫВАНИЕМ

Введение

Генераторы псевдослучайных последовательностей используются в различных областях науки и техники, в частности при моделировании различных процессов в сложных информационных системах, в аппаратных и программных системах защиты информации, в средствах криптографического преобразования информации.

С развитием информационно-телекоммуникационных систем актуальным остается вопрос обеспечения защищенности данных при передаче их по каналам связи. В настоящее время обеспечение конфиденциальности, целостности или доступности данных решается с использованием криптографических методов защиты информации, в том числе различных алгоритмов шифрования, цифровых подписей, кодов аутентификации сообщений и др.

Один из основных элементов криптографических систем, от характеристик которых зависит качество всей криптографической системы, — средства генерирования ключей или генераторы псевдослучайных последовательностей (ГПП). Установлено, что характеристики систем безопасности зависят от характеристик их криптографических подсистем, которые определяются не только использованными методами, но и качественными показателями использованных псевдослучайных последовательностей. Поскольку безопасность криптосистемы сосредоточена на ключе, то при использовании ненадежного процесса генерации ключей вся криптосистема становится уязвимой [1]. Поэтому актуальны вопросы формирования новых алгоритмов генерации псевдослучайных последовательностей.

Цель данной публикации — исследование периодов повторения и статистические характеристики псевдослучайной битовой последовательности для прогнозирования эффективного (статистически безопасного) ключевого пространства генераторов на основе модифицированного аддитивного генератора Фибоначчи с запаздыванием (МАГФЗ).

Исследование классических и модифицированных аддитивных генераторов Фибоначчи с запаздыванием

Среди различных типов генераторов псевдослучайных битовых последовательностей (ГПБП) можно выделить аддитивные генераторы Фибоначчи с запаздыванием (АГФЗ) [2–5], преимущества которых — простота построения и быстродействие.

В общем виде работа АГФЗ описывается уравнением

$$X_i = (X_{i-b} + X_{i-c} + X_{i-d} + \cdots + X_{i-m}) \bmod M, \qquad (1)$$

где X_i — текущее значение числа, X_{i-b}, X_{i-c}, X_{i-d}, …, X_{i-m} — предыдущие значения псевдослучайных чисел на определенных выбранных тактах.

© В.Н. МАКСЫМОВЫЧ, М.Н. МАНДРОНА, О.И. ГАРАСИМЧУК, Ю.М. КОСТИВ, 2016

При аппаратной реализации для упрощения построения генератора принимают $M = 2^n$, где n — количество двоичных разрядов структурных элементов схемы: регистров и комбинационных сумматоров. При этом статистические характеристики выходной псевдослучайной последовательности ухудшаются.

В работах [6–8] предложены ГПБП на основе МАГФЗ, работающих в соответствии с уравнением

$$X_i = (X_{i-b} + X_{i-c} + X_{i-d} + ... + X_{i-m} + a) \bmod 2^n. \quad (2)$$

Здесь значение переменной a определяется логическим уравнением

$$a = a_0 \oplus a_1 \oplus a_2 \oplus ... \oplus a_z, \quad (3)$$

где a_i ($i = 0, 1, ..., z$) — значение двоичных разрядов числа X_i.

Введение в процесс генерирования последовательностей числа a вызывает определенную путаницу — зависимость каждого бита числа X_i, а также и младшего бита от всех других его битов, что позволяет значительно улучшить статистические характеристики ГПБП.

При использовании МАГФЗ в криптографических устройствах в режиме одноразового блокнота криптографическим ключом является значение начальных цифр в регистрах генератора. Величина множества этих значений будет определять криптостойкость шифров, в которых используется генератор, к атаке «грубая сила». Следовательно, существует необходимость дополнительного исследования ГПБП на основе МАГФЗ на всем множестве значений начальных чисел в регистрах. Эта задача для достаточно больших количеств регистров и их разрядов такова, что ее нельзя решить путем моделирования всех возможных вариантов исходной битовой последовательности и их исследования. Однако не исключена возможность исследовать характеристики таких устройств на определенных подмножествах начальных значений, выявляя закономерности с последующей экстраполяцией этих результатов на все множество начальных значений.

В работе исследованы периоды повторения и статистические характеристики псевдослучайной битовой последовательности для прогнозирования эффективного статистически безопасного ключевого пространства генераторов на основе МАГФЗ.

Исследования проводились для генератора, который реализует функцию

$$X_i = (X_{i-3} + X_{i-8} + a) \bmod 2^n. \quad (4)$$

Схема устройства ГПБП на основе МАГФЗ приведена на рис. 1. В его состав входят: комбинационный сумматор (КС), регистры Рг1–Рг9 и логическая схема (ЛС).

Выходная битовая последовательность снимается с выхода младшего разряда Рг1. Она формируется под влиянием следующих факторов:

— количество регистров генератора;
— определение регистров, числа в которых арифметически добавляются в КС;
— количество разрядов регистров, n;
— количество разрядов Рг1, подключенных к ЛС;
— начальные состояния Рг1–Рг9.

В данной работе первые два фактора зафиксированы неизменными в соответствии со структурой схемы устройства рис. 1.

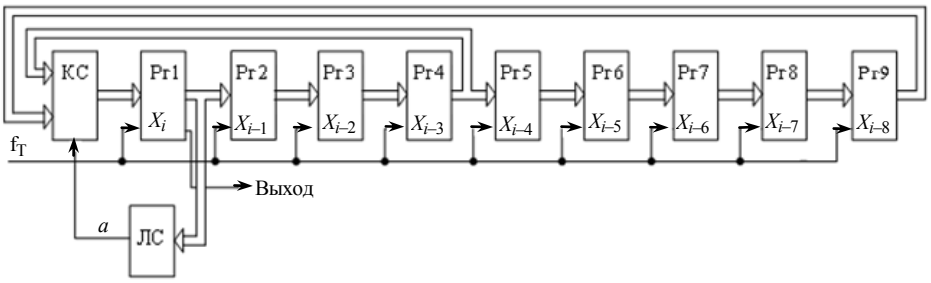


Рис. 1

На рис. 2 (*а* — $a = 0$, *б* — $a = a_0$, *в* — $a = a_0 \oplus a_1$, *г* — $a = a_0 \oplus a_1 \oplus a_2$) приведены результаты исследования периодов повторения выходной последовательности генератора при n = 3, которые определялись с помощью имитационного моделирования и фиксировались в моменты, когда повторялись начальные значения чисел во всех регистрах. При этом осуществлен перебор всех возможных комбинаций исходных чисел в регистрах Рг4 и Рг9: $X_{i-3}(0)$ и $X_{i-8}(0)$, а в других регистрах зафиксировались случайным образом выбранные начальные значения $X_i(0) = 3$, $X_{i-1}(0) = 7$, $X_{i-2}(0) = 5$, $X_{i-4}(0) = 3$, $X_{i-5}(0) = 1$, $X_{i-6}(0) = 7$, $X_{i-7}(0) = 5$. Начальные значения чисел в Рг4 и Рг9 представлены переменной $Q(0)$ и определяются уравнением

$$X(0) = X_{i-3}(0) + 2^n \cdot X_{i-8}(0). \qquad (5)$$

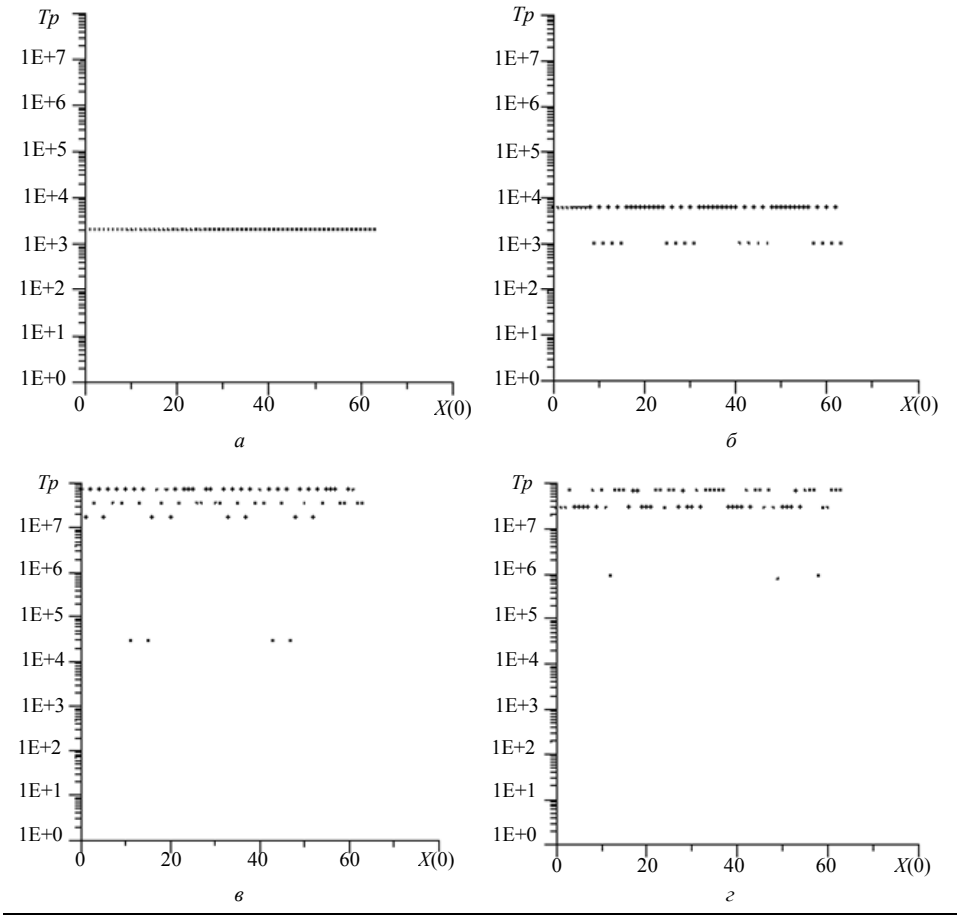


Рис. 2

Периоды повторения исследовались при различном количестве разрядов регистра Рг1, подключенных к ЛС, т.е. при различных значениях переменной *а* в соответствии с уравнением (3). Заметим, что случай *а* = 0 (рис. 2, *а*) соответствует класическому АГФЗ, в котором отсутствует ЛС.

Из анализа результатов следует, что включение в состав генератора ЛС существенно увеличивает периоды повторения выходной последовательности. При этом увеличение периодов наблюдается также с увеличением задействованных членов уравнения (3).

Дальнейшие исследования проводились при увеличении количества разрядов структурных элементов устройства при n = 4 и тех же значениях $X_i(0) = 3$, $X_{i-1}(0) = 7$, $X_{i-2}(0) = 5$, $X_{i-4}(0) = 3$, $X_{i-5}(0) = 1$, $X_{i-6}(0) = 7$, $X_{i-7}(0) = 5$. Результаты исследований МАГФЗ (в сокращенном виде) приведены в таблице, где $Tp_{\min}$ и $Tp_{\max}$ — минимальное и максимальное значение Tp на всем множестве значений начальных состояний регистров Рг4 и Рг9.

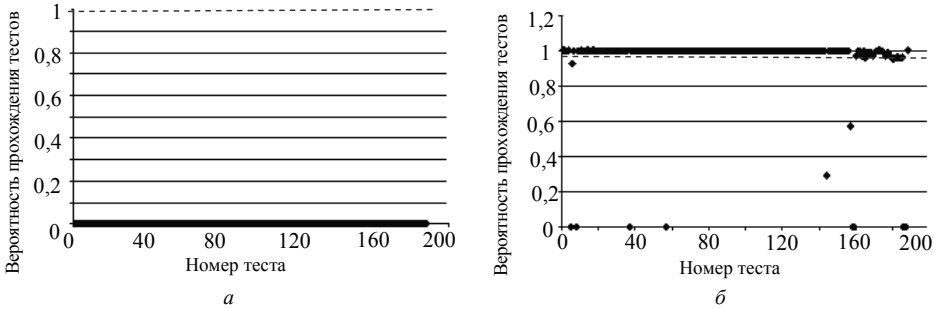
Таблица

A	$Tp_{\min}$		$Tp_{\max}$	
	Значения	NIST	Значения	NIST
0	4088	—	4088	—
a_0	2044	—	6132	—
$a_0 \oplus a_1$	58254	—	144438238	—
$a_0 \oplus a_1 \oplus a_2$	55889092	—	$>10^9$	+
$a_0 \oplus a_1 \oplus a_2 \oplus a_3$	750109555	—	$>10^9$	+

Для отдельных значений $Tp_{\min}$ и $Tp_{\max}$ исследовались статистические характеристики исходной последовательности генератора с помощью статистических тестов NISN [9], поскольку они используются для определения качественных и количественных свойств случайных последовательностей. Набор NIST содержит 15 статистических тестов, в том числе тест определения линейной сложности. Во время тестирования вычисляется 188 значений вероятности P, которые можно рассматривать как результат работы отдельных тестов. По полученным результатам формируют статистический портрет (рис. 3: *а* — $a = a_0$, *б* — $a = a_0 \oplus a_1$, *в* — $a = a_0 \oplus a_1 \oplus a_2$, *г* — $a = a_0 \oplus a_1 \oplus a_2 \oplus a_3$), в котором пунктирными линиями отмечены границы доверительного интервала [8, 10]. Если результаты тестирования попадают в эти пределы, то делаем вывод, что исследуемый генератор соответствует требованиям случайности, т.е. статистически безопасный.

На рис. 3 приведены результаты исследования статистических характеристик МАГФЗ при n = 4 и $Tp_{\min}$. Из статистических портретов четко видно, как влияет ЛС на статистические характеристики генератора.

Протестирована битовая последовательность длиной 10^9 бит, которая снималась с младшего разряда регистра Рг1. При этом зафиксировано, что при $Tp > 10^9$ в большинстве случаев исследуемая последовательность проходит все тесты (отмечено символом + в таблице), а в случае, когда $Tp \le 10^9$, она не проходит все тесты. Заметим, что при n = 4 и $a = a_0 \oplus a_1 \oplus a_2$ период Tp не превышает 10^9 для 12-ти значений $X(0)$ из 256, а при n = 4 и $a = a_0 \oplus a_1 \oplus a_2 \oplus a_3$ — только для трех значений $X(0)$ из тех же 256.



а *б*

ISSN 0572-2691

Продолжение рис. 3

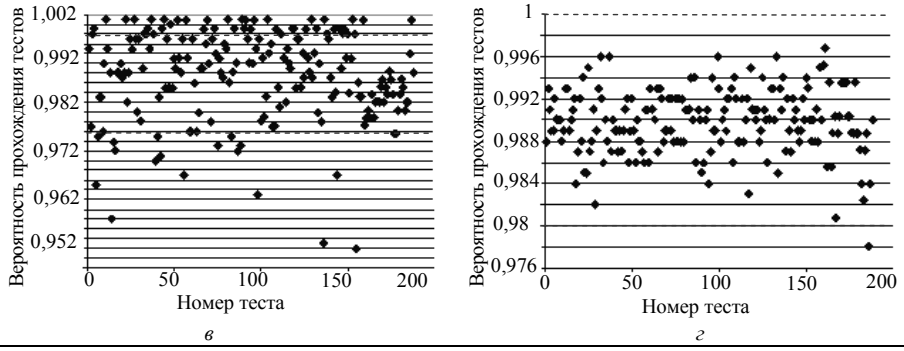


Рис. 3

На рис. 4 приведены статистические портреты для выходной псевдослучайной последовательности при $n = 4$, $a = a_0 \oplus a_1 \oplus a_2 \oplus a_3$ и указанных выше неизменных начальных значениях чисел в регистрах Рг1, Рг2, Рг3, Рг5, Рг6, Рг7, Рг8, на рис. 3, *а* — для случая когда $X_{i-3} = 10$ и $X_{i-8} = 5$, при котором был зафиксирован период $Tp = 750109555$, а на рис. 3, *б* — для $X_{i-3} = 0$ и $X_{i-8} = 0$, когда $Tp > 10^9$.

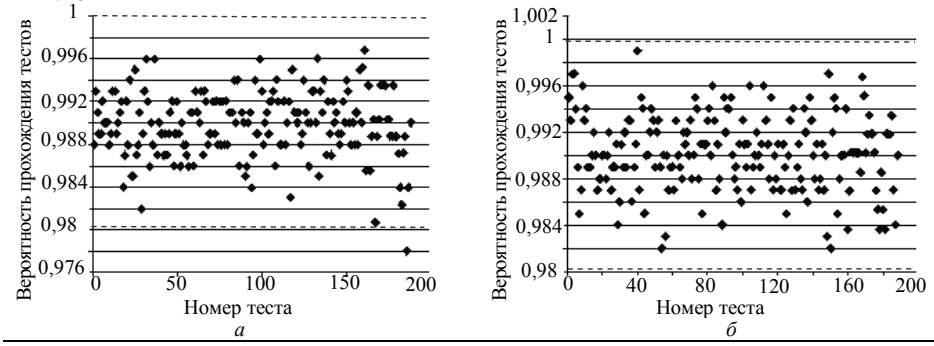


Рис. 4

Из статистических портретов видно, что практически все результаты тестирования попадают в границы доверительного интервала, что свидетельствует о случайности битовой последовательности и статистической безопасности ГПБП (рис. 4, *б*), однако на рис. 4, *а* один тест не пройден, т.е. ГПБП формирует последовательность, приближенную к случайной.

Заключение

В процессе исследования быстродействующих АГФЗ улучшены статистические характеристики и увеличены их периоды повторения за счет введения в схему классического генератора дополнительного элемента, который приводит к усложнению. При увеличении количества двоичных разрядов структурных элементов генератора и задействованных членов уравнения (3) происходит стремительное увеличение периодов повторения исходной псевдослучайной битовой последовательности и улучшение ее статистических характеристик.

При этом, однако, возникает вопрос оценки величины множества начальных значений регистров, которая определяет величину статистически безопасного ключевого пространства (длину ключа).

Исследования для $n = 4$ при полном переборе начальных значений в двух регистрах показывают, что в большинстве случаев исходная последовательность успешно проходит все статистические тесты NIST. В результате можно прогнозировать, что аналогичные результаты будут зафиксированы и при полном переборе начальных чисел во всех регистрах устройства. Логично также предположить, что при увеличении количества разрядов n статистические характеристики исходной последовательности должны улучшаться. Итак, статистически безопасное множество начальных состояний регистров генератора (см. рис. 1) будет близко к значению $2^{9 \cdot n}$, что соответствует длине ключа $9 \cdot n$.

В.М. Максимович, М.М. Мандрона, О.І. Гарасимчук, Ю.М. Костів

ДОСЛІДЖЕННЯ ХАРАКТЕРИСТИК МОДИФІКОВАНОГО АДИТИВНОГО ГЕНЕРАТОРА ФІБОНАЧЧІ ІЗ ЗАПІЗНЕННЯМ

Досліджено періоди повторення і статистичні характеристики псевдовипадкової бітової послідовності для прогнозування статистично безпечного ключового простору генераторів на основі модифікованого адитивного генератора Фібоначчі із запізненням.

V.N. Maksymovych, M.N. Mandrona, O.I. Garasimchuk, Yu.M. Kostiv

A STUDY OF CHARACTERISTICS OF FIBONACCI MODIFIED ADDITIVE GENERATOR WITH LAG

The investigation of repetition periods and statistical characteristics of pseudorandom bit sequence for predicting statistically safe key space of generators based on the modified additive lagged Fibonacci generator is performed.

1. *Горбенко І.Д., Горбенко Ю.І.* Прикладна криптографія. Теорія. Практика. Застосування. — Харків: Форт, 2012. — 870 с.
2. *Orue A.B., Montoya F., Hernández Encinas L.* Trifork, a new pseudorandom number generator based on lagged Fibonacci maps // Journal of Computer Science and Engineering. — 2010. — **2**, N 2. — P. 46–51.
3. *Parallel* pseudorandom number generation using additive lagged Fibonacci recursions / M. Mascagni, M.L. Robinson, D.V. Pryor, S.A. Cuccaro // Lecture Notes in Statistics. — 1995. — N 106. — P. 263–277.
4. *Иванов М.А., Чугунков И.В.* Теория, применение и оценка качества генераторов псевдослучайных последовательностей, — М. : КУДИЦ-ОБРАЗ, 2003. — 240 с.
5. *Иванов М.А., Чугунков И.В.* Криптографические методы защиты информации в компьютерных системах и сетях. — М.: Изд–во НИЯУ МИФИ, 2012. — 400 с.
6. *Модифікація* адитивного генератора Фібоначчі з запізненням / М.М. Мандрона, В.М. Максимович, Ю.М. Костів, О.І. Гарасимчук // Сучасний захист інформації. — 2014. — № 2. — С. 56–62.
7. *Пат.* 108586 Україна, МПК61G06F 7/58 H04L 9/20. Адитивний генератор Фібоначчі із запізненням / В.М. Максимович, М.М. Мандрона, О.І. Гарасимчук, Ю.М. Костів. — № a2014 06408 ; Заявл. 04.07.2014; Опубл. 12.05.2015, Бюл. № 9.
8. *Мандрона М.М.* Апаратні генератори псевдовипадкових бітових послідовностей з покращеними характеристиками : Дис. … канд. техн. наук : 05.13.21. — Львів, 2015. — 146 с.
9. *NIST* SP 800–22. A statistical test suite for random and pseudorandom number generators for cryptographic applications. — http://csrc.nist.gov/publications/nistpubs/800–22–rev1a/SP800–22rev1a.pdf.
10. *Дослідження* впливу параметрів генератора Голлманна на статистичні характеристики вихідного сигналу / М.М. Мандрона, В.М. Максимович, Ю.М. Костів, О.І. Гарасимчук // Вісник Кременчуцького національного університету імені Михайла Остроградського. — 2013. — Вип. 4 (81). — С. 98–103.
11. *Mandrona M.N., Maksymovych V.N* Investigation of the statistical characteristics of the modified Fibonacci generators // Journal of Automation and Information Sciences. — 2014. — **46.**i 12.60. — P. 48–53.

Получено 18.04.2016
После доработки 05.07.2016