УДК 004.032.2

Н. И. Кушниренко, **В. Д. Буряк**,
В. Я. Чечельницкий, д-р техн. наук

МЕТОД ПОСТРОЕНИЯ ГАММА-ПОСЛЕДОВАТЕЛЬНОСТИ ДЛЯ ШИФРОВАНИЯ ПОТОКОВ ДАННЫХ

Аннотация. *В работе для решения задачи шифрования больших потоков данных в реальном времени предлагается использовать гамма-последовательность, которая построена на базе совершенных двоичных решеток. Гамма-последовательность удовлетворяет требованиям стандарта FIPS 140-1.*

Ключевые слова: *потоковое шифрование, гамма-последовательность, совершенные двоичные решетки, стандарт FIPS 140-1*

N. Kushnirenko, **V. Buriak,**
V. Chechelnytskyi, ScD.

METHOD OF CONSTRUCTING GAMMA SEQUENCE FOR STREAM ENCRYPTION

Abstract. *In the paper the use of gamma sequence based on perfect binary arrays is proposed to solve the problem of encryption of big data streams in real time. The gamma sequence meets the requirements of FIPS 140-1.*

Keywords: *stream encryption, gamma sequence, perfect binary arrays, FIPS 140-1*

Н. И. Кушніренко, **В. Д. Буряк**,
В. Я. Чечельницький, д-р техн.наук

МЕТОД ПОБУДОВИ ГАММА-ПОСЛІДОВНОСТІ ДЛЯ ШИФРУВАННЯ ПОТОКІВ ДАНИХ

Анотація. *У роботі для розв'язання завдання шифрування великих потоків даних в реальному часі пропонується використовувати гамма-послідовність, яка побудована на базі досконалих двійкових решіток. Гамма-послідовність задовольняє вимогам стандарту FIPS 140-1.*

Ключові слова: *потокове шифрування, гамма-послідовність, досконалі двійкові решітки, стандарт FIPS 140-1*

Введение. Проблема шифрования больших сообщений и потоков данных возникла сравнительно недавно с появлением средств мультимедиа и сетей мультимедиа с высокой пропускной способностью, обеспечивающих передачу этих данных. Так как передача оцифрованной звуковой, графической информации и видеоконференции во многих случаях требует конфиденциальности, то возникает проблема шифрования огромных информационных массивов. Для интерактивных систем типа телеконференций, ведения аудио и видеосвязи, такое шифрование должно осуществляться в реальном масштабе времени и по возможности быть «прозрачным» для пользователей. Отсюда встает проблема разработки современных технологий шифрования больших потоков данных в реальном времени.

Целью работы является разработка метода построения гамма-последовательности для потокового шифрования данных.

Основная часть. Решить проблему шифрования больших потоков данных в реальном времени можно на основе гаммирования, когда осуществляется сложение по модулю два битов открытого текста (X) с битами гамма-последовательности (Γ): $Y = X \oplus \Gamma$. На приемной стороне, для получения исходного сообщения (X), осуществляется сложение по модулю два полученных битов (Y) с битами той же гамма-последовательности: $Y \oplus \Gamma = X$.

При использовании метода гаммирования ключом шифрования является последовательность, с которой производится сложение – гамма.

Клод Шеннон доказал, что если гамма обладает определенными свойствами, то этот метод шифрования является абсолютно стойким. Вот некоторые из требуемых свойств: гамма должна содержать одинаковое количество нулей и единиц, длина гаммы должна быть не меньше длины сообщения, которое необходимо шифровать, гамма не должна повторяться, т.е. для передачи нового сообщения необходимо генерировать новую гамму.

Обычно для генерации гаммы используются конгруэнтные генераторы псевдослучайных чисел [1]. Также широко применяются генераторы m-последовательностей [2], генераторы последовательностей Голда и Кассами [3], генераторы больших систем бинарных кодовых слов на основе последовательностей Голда [4].

В настоящей работе предлагается в качестве гаммы использовать псевдослучайную последовательность (ПСП) построенную на базе совершенных двоичных решеток (СДР).

Совершенными двоичными решетками называются двумерные матрицы размера $N \times N$, которые имеют идеальную двумерную периодическую автокорреляционную функцию [5]. Совершенные двоичные решетки состоят из элементов «+1» и «−1» и имеют разбаланс элементов $|K^{(+)} - K^{(-)}| = N$, где $K^{(+)}$ – число символов (+1), а $K^{(-)}$ – число символов

(–1) в структуре СДР. Существуют совершенные двоичные решетки порядков $N = 2^k$ и $N = 3 \cdot 2^k$, где k – простое натуральное число.

Построению СДР посвящено множество статей, например [5 – 9]

Принцип построения ПСП состоит в следующем. Строится ансамбль СДР определенного порядка. С помощью конкатенации строк каждой СДР строится бинарная последовательность. Путем замены элементов полученной последовательности « +1 » на «0» и « –1 » на «1» получаем ПСП. Например, из СДР

$$\mathbf{P} = \begin{bmatrix} + & + & + & - \\ - & + & + & + \\ - & + & - & - \\ + & + & - & + \end{bmatrix}$$

путем конкатенации строк получается следующая бинарная последовательность

$$+ + + - - + + + - + - - + + - +,$$

а после замены элементов – следующая ПСП

$$0\,0\,0\,1\,1\,0\,0\,0\,1\,0\,1\,1\,0\,0\,1\,0.$$

Таким же образом из каждой совершенной двоичной решетки полного класса строятся отдельные ПСП, а затем с помощью операции конкатенации получается полная ПСП, которую необходимо использовать в качестве гаммы.

При генерации ПСП СДР можно переставлять, при этом количество таких перестановок определяется факториалом $Z = \Psi!$, где Ψ – мощность полного класса СДР. Для совершенных двоичных решеток порядка $N = 2^k$ мощность полного класса можно вычислить по формуле [8]

$$\Psi = \begin{cases} 7^{(k-1)/2} \cdot 3^{(k-1)/2} \cdot 2^{2^{k+1}-1}, & \text{если } k \text{ нечетное;} \\ 7^{(k-2)/2} \cdot 3^{k/2} \cdot 2^{2^{k+1}-1}, & \text{если } k \text{ четное.} \end{cases}$$

При увеличении порядка СДР их мощность растет по экспоненциальному закону (рис. 1).

Для ориентации, что эти мощности действительно большие, можно привести данные популярного сайта Википедия (http://ru.wikipedia.org) на котором приводится число молекул в известной части вселенной, которое определяется значениями $10^{79} \ldots 10^{81}$.

Длины гамма-последовательности (периоды) достаточно большие и соответствуют объему современных потоков данных (табл. 1). Если же длины гамма-последовательности не достаточно для шифрования потока данных, то можно всегда перейти к СДР большего порядка.

1. Периоды гамма-последовательностей

Порядок СДР	Период последовательности
8	5,25 Мбайт
12	72,98 Гбайт
16	1,34 Тбайт
24	$9{,}93 \cdot 10^5$ Тбайт

Существует буквально бесконечное число тестов, которые можно использовать для проверки того, является ли последовательность случайной [1; 10]. К сожалению, в доступных источниках не было обнаружено отечественных стандартов, которые бы определяли требования к характеристикам (свойствам)

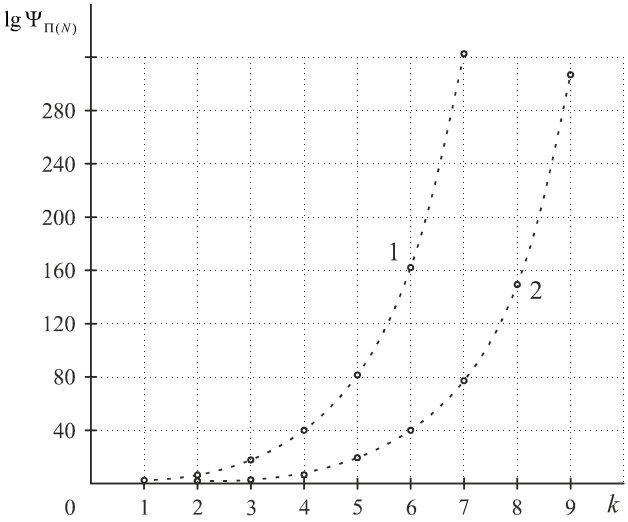


Рис. 1. Десятичные логарифмы мощностей полных классов СДР разных порядков *N:*
$1 - N = 2^k$; $2 - N = 3 \cdot 2^k$

псевдослучайной последовательности, которую можно использовать в криптографических приложениях.

Воспользуемся Федеральным стандартом США FIPS 140-1 [11], который утвержден National Institute of Standards and Technjlogy 11 января 1994 года. Псевдослучайная последовательность считается прошедшей тестирование по стандарту FIPS 140-1, если произвольная ее последовательность из 20000 бит удовлетворяет всем четырем требованиям, которые приведены в стандарте. Приведем эти требования и проанализируем ПСП, построенные на базе совершенных двоичных решеток.

Монобитный тест. Суть данного теста состоит в подсчете количества единиц или нулей. Тест считается пройденным, если количество единиц (нулей) лежит в диапазоне $9654 < n_1 < 10346$. Псевдослучайная последовательность построенная на основе СДР всегда содержит одинаковое количество единиц или нулей ($n_1 = 10\,000$), поскольку всегда можно выбрать равное количество опорных СДР как с положительным разбалансом $K^{(+)} - K^{(-)} = N$, так и с отрицательным разбалансом $K^{(+)} - K^{(-)} = -N$, где $K^{(+)}$ – число символов (+1), а $K^{(-)}$ – число символов (–1) в структуре СДР.

Блоковый тест (тест Покера). Последовательность разбивается на 5000 блоков по 4 бита каждый, после чего производится подсчет частот $q[0] \ldots q[15]$ появления каждого из сегментов от «0000» до «1111» соответственно. Тест считается пройденным, если критерий χ^2 – он имеет, так называемое, статистическое распределение «хи-квадрат», лежит при таком построении выборки в диапазоне $1{,}03 < \chi^2 < 57{,}4$, где

$$\chi^2 = (16/5000) \cdot \left(\sum_{i=0}^{15} q[i]^2 \right) - 5000 .$$

Результаты выполнения теста для СДР разных порядков приведены в табл. 2.

2. Результаты блокового теста

Порядок СДР	χ^2
8	6,0416
12	4,7294
16	3,6024

Тест серий. Под серией понимается последовательность одинаковых символов (нулей и единиц) в ПСП. Количество непрерывных последовательностей длины *K* должно лежать в определенных диапазонах. В таблицах 3 и 4 приведены требования к диапазонам и результаты выполнения теста для СДР разных порядков. Таким образом, данный тест состоит из двенадцати независимых требований.

3. Результаты теста серий (количество серий единиц)

Порядок СДР	Длина серий (допустимый диапазон)					
	1 (2267–273)	2 (1079–1421)	3 (502–748)	4 (223–402)	5 (90–223)	≥ 6 (90–22)
8	2428	1211	662	320	204	112
12	2493	1212	612	316	143	169
16	2472	1267	635	328	142	142

4. Результаты теста серий (количество серий нулей)

Порядок СДР	Длина серий (допустимый диапазон)					
	1 (2267–2733)	2 (1079–1421)	3 (502–748)	4 (223–402)	5 (90–223)	$6 \geq$ (90–223)
8	2503	1158	633	281	214	143
12	2459	1176	676	299	171	158
16	2527	1275	607	299	164	147

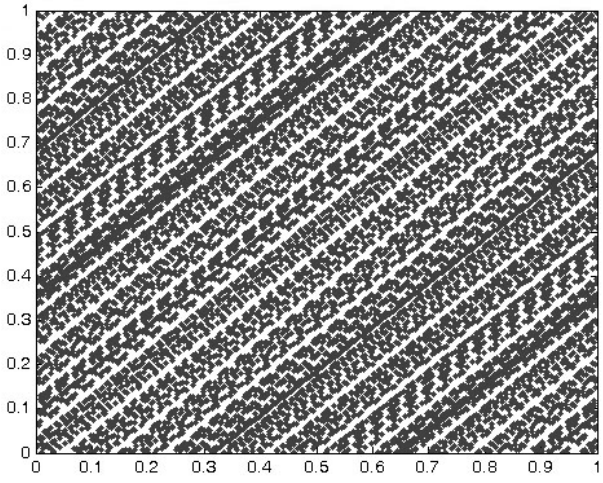
Тест длин серий. Суть теста состоит в том, что необходимо проверить максимальную длину серии одинаковых элементов, и она не должна превышать значения 34 элемента. Результаты выполнения этого теста приведены в табл. 5.

5. Результаты теста длин серий

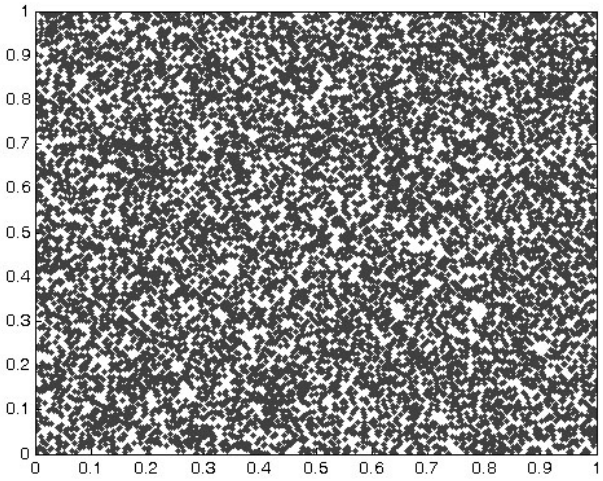
Порядок СДР	Максимальная длина серии
8	8
12	10
16	11

В результате выполнения исследования установлено, что все протестированные ПСП, которые построены на базе СДР, удовлетворяют требованиям стандарта FIPS 140-1, т.е. являются криптографически пригодными. Кроме того, из данных приведенных в таблицах 1; 2; 3 и 4 видно, что с ростом порядка СДР статистические свойства ПСП последовательности улучшаются.

Кроме статистических тестов существуют и графические тесты, например, тест «Распределение на плоскости» [10]. Данный тест предназначен для определения зависимостей между элементами исследуемой последовательности.



а



б

Рис. 2. Распределение на плоскости:
а – для конгруэнтного генератора ПСП;
б – ПСП построенной на базе СДР

Построение распределения на плоскости осуществляется следующим образом. На поле размером $(2^R-1)\times(2^R-1)$ (R – разрядность чисел исследуемой последовательности) наносятся точки с координатами (b_i, b_{i+1}), где b_i – элементы исследуемой последовательности b; $i=\overline{1,n-1}$; n – длина последовательности.

Далее анализируются полученные рисунки. Если между элементами последовательности отсутствуют зависимости, то точки на рисунке расположены хаотично (рис. 2, б). Если на рисунке присутствуют зависимости, наблюдаются «узоры» – последовательность не является случайной (рис. 2, а).

На рис. 2, а показано распределение на плоскости для конгруэнтного генератора ПСП работающего по формуле

$$b_{i+1} = (363x_i^3 + 99x_i^2 + 430x_i + 2531) \bmod 11979$$

и ПСП построенной на базе СДР порядка N=16 (рис. 2, б)

Выводы. Зашифрованный текст Y в приведенном случае является достаточно трудным для раскрытия, в силу следующих свойств гамма-последовательности.

1. Гамма шифра по построению содержит одинаковое количество символов 0 и 1, то есть вероятность $p(0) = p(1) = 0,5$.

2. Гамма шифра не содержит повторяющихся битовых последовательностей, поскольку структура опорных СДР различна и неповторяема;

3. Гамма шифра изменяется фактически случайным образом для каждого шифруемого слова, причина этого – случайный выбор порядка следования рабочих СДР из $\psi = \Psi!$ всевозможных перестановок;

4. Период гаммы $|\Gamma| \geq |X|$, где $|X|$ – длина открытого текста. В табл. 1 приведены периоды ПСП построенных из полного класса СДР разных порядков выраженные в байтах.

Такой шифр можно раскрыть только прямым перебором.

На приемную сторону необходимо передавать не всю ПСП, а только параметры генератора СДР, что резко сокращает объем информации, который необходимо передать по секретному каналу.

Список использованной литературы

1. Кнут Д. Э. Искусство программирования: том 2. Получисленные алгоритмы / Д. Э. Кнут. – М. : Вильямс, 2005.– 832 с.

2. Кузнецов В. М. Генераторы равновероятностных псевдослучайных последовательностей на регистрах сдвига / В. М. Кузнецов, В. А. Песошин // Известия высших учебных заведений. Поволжский регион.– 2012.– № 1. – С. 21 – 28.

3. Столингс В. Беспроводные линии связи и сети / В. Столингс [Пер. с англ]. – М. : Издательский дом «Вильямс», 2003. – 640 с.

4. Мрачковський О. Д. Формування та властивості послідовностей Голда / О. Д. Мрачковський, А. А. Часник, В. А. Ганзенко // Вісник Національного технічного університету України «КПІ», Серія – Радіотехніка. Радіоапаратобудування. – 2011. – К. : № 45. – С. 52 – 57.

5. Чечельницкий В. Я. Полный класс совершенных двоичных решеток на 144 элемента / В. Я. Чечельницкий // Радиоэлектроника (Изв. вузов). – К. : – 2009. – Т. 52. – № 2.– С. 29 – 35.

6. Чечельницкий В. Я. Порождающий класс совершенных двоичных решеток размера 12x12 для защиты информации / В. Я. Чечельницкий // Сучасний захист інформації. – К. : – 2010. – № 4. – С. 44 – 52.

7. Чечельницкий В. Я. Метод построения полного класса совершенных двоичных решеток порядка *N*=8x8 / В. Я. Чечельницкий // Радиоэлектроника (Изв. вузов). – К. :– 2005.– Т. 48. – № 11.– С. 65 – 72.

8. Чечельницкий В. Я. Метод построения полного класса совершенных двоичных решеток порядка $N=2^k$ / В. Я. Чечельницкий // Радиоэлектроника (Изв. вузов). – К. :– 2006.– Т. 49. – № 9.– С. 44 – 53.

9. Чечельницкий В. Я. Метод построения полного класса совершенных двоичных решеток порядка N=6 / В. Я. Чечельницкий // Збірник наукових праць Одеського ордена Леніна інституту сухопутних військ. – К. :– 2007.– № 13. – С. 129 – 132.

10. Иванов М. А. Теория, применение и оценка качества генераторов псевдослучайных последовательностей / М. А. Иванов, И. В. Чугунков. – М. : КУДИЦ-ОБРАЗ, 2003. – 240 с.

11. Federal Information Processing Standards. FIPS PUB 140-1. Security Requirements for Cryptographic Modules (In English) Available at: (http://csrc.nist.gov/publications/fips/fips140-1/fips1401.pdf) (accessed 11.01.1994).

Получено 30.05.2015

References

1. Knut D. E. Iskusstvo programmirovaniya. Tom 2. Poluchislennyie algoritmyi [The Art of Computer Programming. Volume 2. Seminumerical Algorithms], (2005), *Vilyams*, Moscow, Russian Federation [In Russian], URL: http://www.ex.ua/get/7967343.

2. Kuznetsov V.M., and Pesoshin V.A. Generatoryi ravnoveroyatnostnyih psevdosluchaynyih posledovatelnostey na registrah sdviga [Pseudorandom Number Generators Based on Linear Feedback Shift Registers], (2012), *Izvestiya Vyisshih Uchebnyih Zavedeniy. Povolzhskiy Region*, Russian Federation [In Russian], Url: http://izvuz_tn.pnzgu.ru/files/izvuz_tn.pnzgu.ru/3112.pdf.

3. Stolings V. Besprovodnyie linii svyazi i seti [Wireless Communications and Networking], (2003), *Izdatelskiy dom "Vilyams"*, Moscow, Russian Federation (In Russian), Url: http://www.williamspublishing.com/Books/5-8459-0409-9.html.

4. Mrachkovskiy O.D., Chasnik A.A., and Ganzenko V. A. Formuvannya ta vlastivosti poslidovnostey Golda [Generation and Properties of Gold's Sequence], (2011), *Visnik Natsionalnogo Tehnichnogo Universitetu Ukrayini "KPI", Seriya – Radiotehnika. Radioaparatobuduvannya*, Kiev, Ukraine, (In Ukrainian), Url: http://radap.kpi.ua/radiotechnique/article/view/80/109.

5. Chechelnitskiy V.Ya. Polnyiy klass sovershennyih dvoichnyih reshetok na 144 elementa [Complete Class of Perfect Binary Arrays for 144 Elements], (2009), *Radioelektronika (Izv. Vuzov)*, Kiev, Ukraine, (In Russian), Url: http://radio.kpi.ua/article/view/S0021347009020046.

6. Chechelnitskiy V.Ya. Porozhdayuschiy klass sovershennyih dvoichnyih reshetok razmera 12x12 dlya zaschityi informatsii [Generating Class of Perfect Binary Arrays Size of 12x12 for Information Protection], (2010), *Suchasniy Zahist Informatsiyi*, Kiev, Ukraine (In Russian).

7. Chechelnitskiy V.Ya. Metod postroeniya polnogo klassa sovershennyih dvoichnyih reshetok poryadka N=8x8 [The Method of Constructing a Complete Class of Perfect Binary Arrays of Order N=8x8], (2005), *Radioelektronika (Izv. Vuzov)*, Kiev, Ukraine (In Russian).

8. Chechelnitskiy V.Ya. Metod postroeniya polnogo klassa sovershennyih dvoichnyih reshetok poryadka $N=2^k$ [The Method of Constructing a Complete Class of Perfect Bbinary Arrays of Order $N=2^k$], (2005), *Radioelektronika (Izv. Vuzov)*, Kiev, Ukraine (In Russian), Url: http://radio.kpi.ua/article/view/S0021347006090056.

9. Chechelnitskiy V.Ya. Metod postroeniya polnogo klassa sovershennyih dvoichnyih reshetok poryadka N=6 [The Method of Constructing a Complete Class of Perfect Binary Arrays of Order N = 6], (2007), Zbirnik Naukovih Prats Odeskogo ordena LenIna Institutu Suhoputnih Viysk, Kiev, Ukraine (In Russian).

10. Ivanov M.A., and Chugunkov I.V. Teoriya, primenenie i otsenka kachestva generatorov psevdosluchaynyih posledovatelnostey [The Theory, Application and Evaluation of the Quality of Pseudo-random Sequence Generators], (2003), *KUDITS-OBRAZ*, Moscow, Russian Federation (In Russian).

11. Federal Information Processing Standards. FIPS PUB 140-1. Security Requirements for Cryptographic Modules (In English). Available at: (http://csrc.nist.gov/publications/fips/fips140-1/fips1401.pdf) (accessed 11.01.1994).

Кушниренко
Наталья Игоревна,
ст. преподаватель каф. информационной безопасности ин-та информационной безопасности, радиоэлектроники и телекоммуникаций Одесского нац. политехнического ун-та,
м.т.: +38(093)5608863.
E-mail: natalka_kni@ukr.net

Буряк
Владимир Дмитриевич,
аспирант каф. информационной безопасности ин-та информационной безопасности, радиоэлектроники и телекоммуникаций Одесского нац. политехнического ун-та,
м.т.: +38(098)2186866.
E-mail: elvis.prsl91@gmail.com

Чечельницкий
Виктор Яковлевич,
д-р техн. наук, директор ин-та информационной безопасности, радиоэлектроники и телекоммуникаций Одесского нац. политехнического ун-та, м/т.: +38(067)7314404.
E-mail: cvjonpu@ukr.net