УДК 621.396

Масштабирование псевдослучайных последовательностей в нечетко определенных границах

Г.А. Валюк, А.В. Кондрашов, В.В. Перепеловский

Санкт-Петербургский государственный электротехнический университет «ЛЭТИ»

Аннотация: Рассмотрены перспективные направления получения псевдослучайных последовательностей (ПСП) на основе систем в режиме динамического хаоса. Решена задача получения ПСП изолированных натуральных чисел. Под ограниченной последовательностью изолированных псевдослучайных чисел (ИПСП) понимается последовательность, элементы которой, разделены промежутками, в которых нет возможных псевдослучайных чисел (ПСЧ). Данные последовательности могут применяться для вторичного использования каналов связи, например, в стеганографии для выбора пикселя в фотографических изображениях. Для уменьшения искажений первоначальной информации целесообразно сохранять содержимое одного из рядом расположенных элементов множества(пикселя). Впервые в работе предложен способ преобразования ПСП, позволяющие получать ИПСП. Основой преобразования является нелинейное сжатие промежутков между ПСЧ в нечетко определенных границах масштабирования.

Ключевые слова: вторичное использование каналов связи, детерминированный хаос, изолированные псевдослучайные числа, случайные числа, нечеткие множества, криптография, стеганография, FIPS-140, уравнения Лоренца.

1. Введение

Последовательности псевдослучайных чисел широко используются в целях шифрования [1]. Ключевым аспектом шифрования становится система генерации ПСП. В ряде работ исследовались возможности получения ПСП целых чисел [2,3]. Однако получение изолированных натуральных псевдослучайных последовательностей (ИПСП) не были рассмотрены до настоящего времени. Данные последовательности могут применяться для выбора элементов множеств, нумеруемых целыми числами, например, при выборе пикселя в шифровании фотографических изображений, в частном случае стеганографии. В процессе стеганографии информация вводится в некоторое множество путем частичного или полного изменения содержимого выбранных элементов множества. Для уменьшения искажения первоначальной информации целесообразно сохранять содержимое одного из рядом расположенных элементов множества, следовательно, требуются ПСП изолированных натуральных чисел.

2. Алгоритм построения ИПСП

Данная работа посвящена преобразованию ПСП в ИПСП. Под последовательностью изолированных псевдослучайных чисел понимается последовательность, элементы которой, удалены одни от другого на промежутки R, в которых нет возможных псевдослучайных чисел. Параметр R будем называть радиусом изоляции. Под ограниченностью ИПСП понимается существование такого числа (min), которое определяет область наиболее вероятных значений ИПСП слева, и существование такого числа (max), которое определяет область наиболее вероятных значений ИПСП справа.

Для образования первоначальной ПСП целесообразно использовать уравнения динамического хаоса. Одна система из 3-х дифференциальных уравнений Лоренца позволяет получить три вещественных ПСЧ. В задачах пакетной передачи данных, требуется большее число ПСЧ [4]. Одним из способов решения такой задачи является использования нескольких систем уравнений динамического хаоса с различными

коэффициентами и начальными условиями [5]. Множество ПСЧ получаемых за один шаг решения нескольких уравнений Лоренца, назовем – сетом. На рис.1 приведена часть исходной ПСП полученной 9-ю уравнениями Лоренца. ПСЧ относящиеся к одному сету располагаются по вертикале. Заметны области близких значений ПСЧ выделенные прямоугольниками.

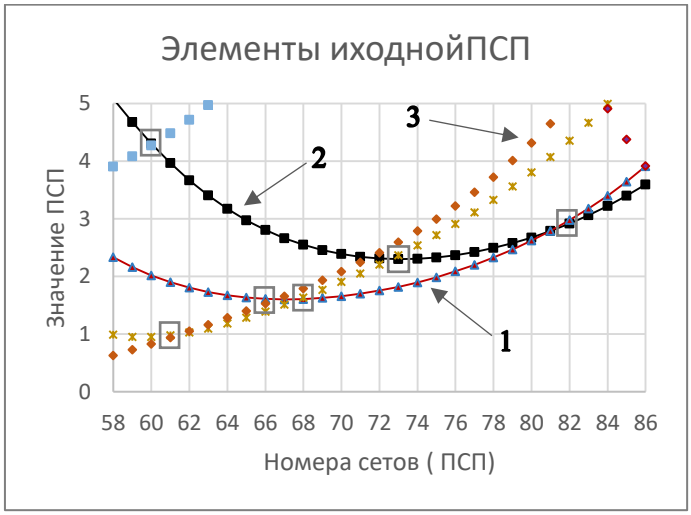

Рисунок 1. Прямоугольниками выделены области совпадения ПСЧ одного сета: 1) ПСП 1-ой системы уравнений Лоренца (переменная x), 2) ПСП 2- ой системы уравнений Лоренца (переменная x), 3) ПСП 2- ой системы уравнений Лоренца (переменная y). Другие графики имеют аналогичный смысл ПСП.

Переход к целочисленному представлению решений систем Лоренца, приводит к большему числу близких ПСЧ. Преобразование решающее возникшую проблемы состоит из нескольких этапов. Рис.2. схематично иллюстрирует действие каждого этапа преобразования на ПСП.

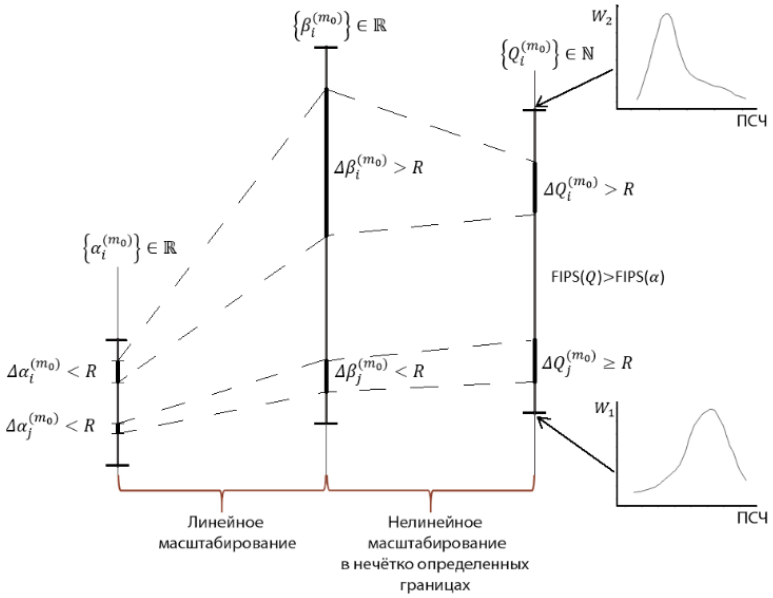

Рисунок 2. Масштабирование псевдослучайной последовательности в нечетко определенных границах одного сета (m_0).

На первом этап требуется получить ПСП как результат решения H уравнений Лоренца - $\left\{\alpha_i^{(m)}\right\}$, где $m \in [0,1,..]$ - номер сета; $i \in [1,2,...,3H]$ - номер ПСЧ в одном сете. На рисунке представлено преобразование одного сета. Полученную последовательность обозначим - $\left\{\alpha_i^{(m_0)}\right\}$. В ПСП существуют ПСЧ, интервалы между которыми меньше заданного R, что показано на рис.2. Выполняя линейное масштабирование получаем последовательность $\left\{\beta_i^{(m_0)}\right\}$.

Второй этап - нелинейное сжатие в нечетко определенных границах. В результате этого этапа получаем последовательность $\left\{Q_i^{(m_0)}\right\}$. Под нечетко определенными границами, понимаем задание минимального и максимального предела ПСП в виде распределения плотности вероятности W_1 и W_2 соответственно. Управление распределением плотности вероятности позволяет изменять хаотичность полученной ИПСП $\left\{Q_i^{(m_0)}\right\}$, что анализировалось на основе тестов FIPS-140. На рис. 3 показан результат масштабирования - увеличение промежутков между ПСЧ, т.е. получение ПСЧ с заданным радиусом изоляции R.

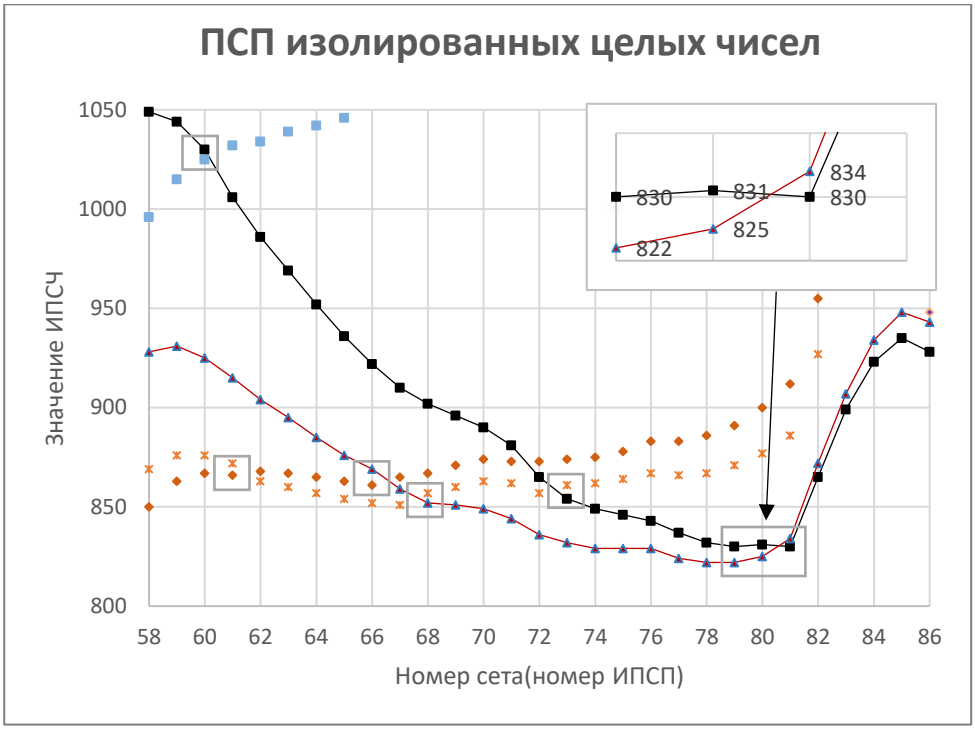

Рисунок 3. Результаты нелинейное масштабирования с нечетко заданными границами – изолированные целые ПСЧ одного сета.

3. Заключение

Решена задача получения ПСП изолированных натуральных чисел. Предложен метод обеспечивающий значительную регулировку параметров, получаемых ПСП и отличается от существующих ранее методов, возможностью создавать последовательности изолированных псевдослучайных натуральных чисел с возможностью управления уровнем хаотичности. Полученные ИПСП исследовались по критериям FIPS-140.

Список литературы

1. Ünal Ç. et al. The design and implementation of hybrid RSA algorithm using a novel chaos based RNG // Chaos, Solitons & Fractals. – 2017. – Т. 104. – С. 655 – 667.
2. Lynnyk V. et al. Pseudo random number generator based on the generalized Lorenz chaotic system // IFAC-PapersOnLine. – 2015. –Т. 48. – С. 257 – 261.
3. Aleksandra V. et al. Adaptive chaotic maps and their application to pseudo-random numbers generation // Chaos, Solitons & Fractals. – 2020. – Т. 133. – С. 109615.
4. Гребенев М. С. и др. Передача двоичных данных на хаотически сформированных несущих частотах. // Известия высших учебных заведений России. Радиоэлектроника. – 2018. – Т. 5. – С. 5 – 12.
5. Kondrashov A. V. et al. Application of hyper-chaotic Lorenz system for data transmission» // Journal of Physics: Conference Series. – 2019. – Т. 1400. – С. 044033.