МЕТОД ОЦЕНКИ КАЧЕСТВА КРИПТОСТОЙКИХ ГЕНЕРАТОРОВ ПСЕВДОСЛУЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ

Будько М.Б.[1], Будько М.Ю.[2], Гирик А.В.[3], Грозов В.А.[4]

Цель статьи: *разработать методику обоснованного выбора генераторов псевдослучайных последовательностей (ПСП) для повышения эффективности и надежности систем криптографической защиты данных.*

Метод исследования: *методы статистического тестирования генераторов псевдослучайных последовательностей на основе стойких криптоалгоритмов, а также метод сравнительного анализа результатов численного эксперимента.*

Полученный результат: *создана методика оценки качества генераторов псевдослучайных последовательностей. Дан краткий обзор существующих подходов к оценке качества генераторов ПСП. Проведен выбор генераторов с подтвержденной высокой криптостойкостью для дальнейшего исследования. На базе этих генераторов проведен численный эксперимент с целью выявления влияния их параметров на свойства выходных последовательностей. Исследование статистических свойств выполнялось с помощью пакета статистических тестов NIST STS. Предложен способ оценки близости сгенерированных псевдослучайных последовательностей к истинно случайным с помощью заданного уровня прохождения статистических тестов. На основе указанного параметра предложен критерий «качество – скорость» для сравнения генераторов ПСП. Показано, что с помощью этого критерия можно выявить различия статистических свойств генераторов ПСП. Разработанный метод позволяет повысить уровень защищенности данных за счет выбора лучшего алгоритма генерации псевдослучайных последовательностей.*

Ключевые слова: *криптоалгоритм, пакет тестов NIST STS, последовательность битов, псевдослучайная последовательность, статистические тесты, защита данных, алгоритм генерации ПСП.*

DOI: 10.21681/2311-3456-2018-4-29-37

Введение

Обеспечение безопасного информационного обмена – важнейшая составляющая функционирования гражданской и военной техники, различных объектов энергетики, инфраструктуры, связи и т.д. Особенно острой является проблема защиты данных для все более многочисленных и разноплановых киберфизических систем (КФС): автоматизированное производство, высокотехнологичная медицина, интернет вещей, беспилотные и робототехнические устройства [1-3]. Большую опасность для таких систем представляют атаки на каналы беспроводной связи, направленные на получение несанкционированного доступа к передаваемым данным и командам управления [4-7].

Криптографические методы являются основными при защите данных. Их надежность во многом определяется качеством используемых криптографических примитивов, в том числе – генераторов случайных и псевдослучайных последовательностей [8].

Генерация истинно случайных чисел связана со многими трудностями, значительными затратами времени и ресурсов, и во многих случаях они могут быть заменены последовательностью псевдослучайных чисел, близких по своим свойствам к истинно случайным. К тому же в определенных ситуациях важным дополнительным аргументом за использование именно ПСП является возможность их точного воспроизведения.

Генераторы псевдослучайных последовательностей (ГПСП) играют значительную роль в защите данных, выполняя рандомизацию данных и алгоритмов. В условиях, когда необходимо обеспечить высокий уровень защиты данных, используются криптографически стойкие генераторы (КСГПСП), которые должны отвечать строгим требованиям. Они должны обеспечивать как непредсказуемость генерируемых выходных значений, так и неотличимость их статистических свойств от свойств истинно случайных последовательностей.

Важным этапом организации защиты данных является обоснованный выбор такого КСГПСП, который не только соответствует требованиям криптографической стойкости, но также имеет большую эффективность и является наиболее подходящим для работы в условиях конкретной задачи.

1 Будько Марина Борисовна, кандидат технических наук, доцент факультета БИТ Университета ИТМО, Санкт-Петербург, Россия. E-mail: mbbudko@corp.ifmo.ru, ORCID 0000-0001-7054-5709

2 Будько Михаил Юрьевич, кандидат технических наук, доцент факультета БИТ Университета ИТМО, Санкт-Петербург, Россия. E-mail: mbudko@corp.ifmo.ru, OCRID 0000-0002-1444-277X

3 Гирик Алексей Валерьевич, кандидат технических наук, доцент факультета БИТ Университета ИТМО, Санкт-Петербург, Россия. E-mail: avg @corp.ifmo.ru, ORCID 0000-0002-4021-7605

4 Грозов Владимир Андреевич, аспирант факультета БИТ Университета ИТМО, Санкт-Петербург, Россия. E-mail: vagrozov@corp.ifmo.ru, ORCID 0000-0002-7998-8175

Традиционно при сопоставлении ГПСП рассматривают такие параметры, как период выходной последовательности, скорость работы (производительность), а также результаты прохождения статистических тестов. При этом сравнительная оценка часто основывается на наборе разнородных характеристик генераторов, иногда не описываемых численно и поэтому трудно сопоставимых.

Использование статистических тестов в стандартном варианте не всегда дает возможность дифференцировать качество генераторов, успешно прошедших все тесты.

Однако разрабатываются и новые подходы, развивающие как способы оценки качества ГПСП, так и технику их тестирования. Следует также отметить, что существует определенная близость исследований, направленных на проверку криптостойкости ГПСП, и аналогичных работ, посвященных криптоалгоритмам.

В работах [9, 10], для сравнения генераторов по результатам статистического тестирования с помощью пакетов NIST STS и Diehard используется суммарное количество последовательностей, не прошедших тесты. Также предлагается методика ранжирования тестов пакета NIST STS. При этом выбор наиболее значимых тестов служит только сокращению затрат времени на тестирование.

Новый «легковесный» ГПСП, ориентированный на низкоресурсные устройства, используемые в сфере интернета вещей, предлагается в статье [11]. Генератор представляет собой комбинацию двух взаимно скремблированных фибоначчиевых генераторов с запаздыванием. Его сравнение с другими генераторами этого класса выполняется путем сопоставления таких характеристик, как длина ключа и аппаратная сложность (gate equivalent).

В работе [12] исследуется безопасность современных блочных шифров. В частности, изучается влияние нелинейных раундовых функций на статистические свойства результирующей последовательности.

Сравнение различных алгоритмов малоресурсной (легковесной) криптографии приводятся в статьях [13, 14].

Статья [15] посвящена исследованию легковесного ГПСП для применения в защите данных в области Интернета вещей и содержит сравнение алгоритмов генераторов по их аппаратной сложности.

Существенна также надежная проверка качества выбранного генератора, поэтому большой интерес представляют исследования, направленные на развитие и совершенствование техники тестирования генераторов ПСП [16, 17].

В статье [18] предложена улучшенная методика тестирования, включающая группировку тестов в соответствии с характером тестируемых свойств, а также выбор лучшего из однотипных тестов в группе на основе оценки, учитывающей такие параметры теста, как возможность обработки коротких ПСП и время обработки одной ПСП.

В работе [19] предложен комплексный подход к решению различных проблем создания и применения оценочных тестов. В работе отмечаются недостатки существующих методик оценки результатов тестирования и формулируются требования к системе оценки статистической безопасности ГПСЧ. Также предложена структура полнофункциональной системы оценки статистической безопасности ГПСЧ и криптоалгоритмов.

В настоящее время не существует общепринятого подхода к количественной оценке близости псевдослучайных последовательностей к истинно случайным, а также отсутствует единый критерий сравнения качества генераторов ПСП. С учетом многообразия существующих генераторов ПСП и важности их роли в защите данных актуальна проблема обоснованного оценивания качества генераторов.

В статье представлено исследование и сравнение статистических свойств генераторов ПСП, реализованных на основе стойких криптоалгоритмов. Во втором разделе обсуждается возможность использования и выбор алгоритмов шифрования в качестве криптостойких ГПСП, кратко описывается методика тестирования, а также процесс подготовки тестируемых данных. В третьем разделе предложен способ оценки близости ПСП к истинно случайной последовательности с помощью заданного уровня прохождения статистических тестов. Приведенные результаты тестирования генераторов демонстрируют влияние комбинаций ключевых последовательностей и размера выборки на качество выходных ПСП. В разделе 4 вводится критерий сравнения ГПСП, основанный на соотношении «качество – скорость», и приводятся результаты применения этого критерия к рассматриваемым генераторам. Раздел 5 содержит некоторые рекомендации, дополняющие оценивание ГПСП посредством введенного критерия.

Цель и методы

Целью работы является предложение способа сравнения эффективности генераторов псевдослучайных последовательностей на основе (выбранных) стойких криптоалгоритмов, используемых для защиты данных применительно к КФС.

Для достижения этой цели требуется решить следующие задачи:

Провести исследование качества выходных ПСП выбранных генераторов с помощью проверки их статистических свойств.

Предложить способ и критерий сравнения исследуемых ГПСП.

Сформулировать рекомендации по выбору ГПСП применительно к использованию в задачах защиты данных.

Использование алгоритмов поточного шифрования в качестве программных криптографически стойких генераторов является уже давно применяемым решением. Преимущество поточных генераторов заключается в высокой скорости работы при достаточной степени непредсказуемости выходных значений. Их криптостойкость, а также секретность ключевой последовательности, и определяют надежность шифра.

Алгоритмы блочных шифров можно использовать как генераторы ПСП за счет выбора соответствующих

режимов работы – режим обратной связи по выходу (Output Feedback mode, OFB) и режим счетчика (Counter mode, CTR). При их реализации блочные шифры работают в режиме поточного шифрования. Блочные алгоритмы основаны на преобразованиях подстановки и перестановки. Многораундовая структура алгоритма обеспечивает многократные повторы этих операций и приводит к рассеиванию и перемешиванию битов открытого текста. Это гарантирует высокую криптостойкость шифра и непредсказуемость выходных данных.

Для сравнения были выбраны алгоритмы на основе поточных шифров Salsa20 [20] и HC-256 [21], а также на основе блочного шифра AES в режимах шифрования OFB и CTR [22]. Эти алгоритмы обладают подтвержденной высокой криптостойкостью.

Криптостойкость алгоритма во многом определяется длиной его ключа, поэтому использовались шифры с длиной ключа 256 бит – максимальной стандартной длиной ключа. Это, в том числе, соответствует рекомендациям, содержащимся в предварительном докладе европейского консорциума квантовой криптографии исследователей в науке и промышленности (PQCRYPTO), относительно криптографических методов, устойчивых к атакам с помощью квантовых компьютеров [23].

Генерировались последовательности длиной $l=10^6$ бит. Тестирование проводилось при следующих значениях размера выборки: 100, 1000, 2000 и 4000 таких последовательностей.

Для исследования генераторов был выбран пакет статистических тестов NIST STS. На сегодняшний день он является основным инструментом проверки случайности ПСП. NIST STS специально разрабатывался для задач криптологии. Пакет разработан с использованием современных достижений, накопленных в области статистического тестирования ГСП. Все тесты созданы для исследования битовых последовательностей. Тесты можно считать в достаточной степени независимыми [24]. Пакет NIST STS считается наиболее приемлемым с точки зрения строгости оценки свойств ГПСП, эффективным по затратам машинного времени и доступным для использования на различных платформах [17]. Использовалась версия NIST STS-2.1.2. В ее состав входят 15 тестов (или 188 – с учетом подтестов).

Обычно для удобства восприятия результатов тестирования вычисленная с помощью эталонного распределения вероятностей тестовая статистика преобразуется в так называемое значение p-*value*. Это значение трактуется как вероятность того, что при заданном уровне значимости a идеальный ГСП может произвести ПСП, менее случайную, чем исследуемая. Такое событие тем менее вероятно, чем меньше значение p-*value*. Выполнение условия p-*value*>=a означает успешное прохождение теста.

Выводы о прохождении теста для всей выборки делаются по результатам проверки двух следующих условий:

Попадание вычисляемой пакетом тестов NIST величины Pr – доли последовательностей, сгенерированных с помощью ГПСП, прошедших тест (определяется как отношение количества прошедших тест последовательностей к общему количеству протестированных) – в доверительный интервал

$$\left[(1-\alpha)-3\sqrt{\frac{\alpha(1-\alpha)}{m}},\ (1-\alpha)+3\sqrt{\frac{\alpha(1-\alpha)}{m}}\right], \qquad (1)$$

где m – размер выборки.

Равномерность распределения вероятностей p-value на отрезке [0,1]. Для проверки равномерности пакетом NIST вычисляется величина статистики для k=10 интервалов [0,0.1), [0.1,0.2), ..., [0.9,1):

$$\chi^2 = \frac{\sum_{i=1}^{k}\left(v_i - m/k\right)^2}{m/k}, \qquad (2)$$

где v_i – рассчитанное для каждого интервала количество принадлежащих ему значений p-value. В соответствии с критерием c^2 выполняется проверка того, насколько реальное распределение значений p-*value* близко к теоретическому (равномерному) распределению. Если число прошедших тест последовательностей велико, распределение этой статистики должно приближаться к распределению χ^2 с числом степеней свободы (k-1).

С целью изучения влияния характера ключей на качество выходных ПСП рассматривались ключевые последовательности совершенно различной степени случайности. Рассматривались следующие виды ключей:

Ключи, имеющие явные закономерности (например, состоящие из повторяющихся групп битов).

Ключи, полученные с помощью *rand*() – функции генерации случайных чисел из стандартной библиотеки языка C.

Ключи, полученные с помощью хэш-функции алгоритма Salsa20 из ключей 1-го набора.

Ключи, полученные с помощью той же хэш-функции из ключей 2-го набора.

Для получения статистически значимых результатов тестирования использовались 40 ключей, т.е. по 10 ключей каждого вида. Для всех генераторов использовались одинаковые наборы ключей.

Результаты

Для проверки статистических свойств последовательностей, получаемых с помощью разных генераторов ПСП, пакетом статистических тестов NIST STS было протестировано в общей сложности более 100000 последовательностей при уровнях значимости α=0.01 и α=0.001 и разных размерах выборки m. Проведение такого количества испытаний повышает надежность выводов о качестве исследуемого генератора. Последовательности были протестированы всеми 188 тестами пакета. Тестирование проводилось в два этапа.

На первом этапе проверка статистических свойств последовательностей проводилась при величине выборки m=100. Результаты тестирования показали, что не было однозначно забраковано ни одной последовательности, т.е. для всех последовательностей было выполнено хотя бы одно из приведенных во II разделе

условий. Незначительное количество последовательностей было забраковано по отдельным из 188 тестов при уровне значимости α=0.01. При этом количество забракованных последовательностей существенно снижается при изменении уровня значимости до α=0.001.

На втором этапе проводилось уточнение результатов первого этапа. Для этого размер выборки был увеличен до m=1000. Результаты тестирования показали значительное снижение числа забракованных последовательностей при уровне значимости α=0.01 по отдельным тестам по сравнению с размером выборки *m*=100 и отсутствие не пройденных тестов при уровне значимости α=0.001.

Кроме того, не было выявлено закономерностей по не пройденным тестам. Характер распределения отрицательных результатов по тестам является случайным. Это дает возможность интерпретировать их как статистические аномалии.

Таким образом, все используемые генераторы производят качественные ПСП.

Результаты тестирования показывают, что влияние типа ключа на статистические свойства ПСП практически отсутствует.

Основной задачей исследования является поиск подхода к численному сравнению качества ГПСП.

Для оценки качества генераторов ПСП использовались результаты их тестирования при уровне значимости α=0.01. Это означает допустимость того, что только одна последовательность из 100 будет отклонена. Выполнение условия p-*value*≥0.01 будет означать, что последовательность будет считаться случайной с уровнем доверия Lα=99%.

Будем считать, что выборка состоит из практически случайных последовательностей, если не менее 99% входящих в нее последовательностей во всех тестах признаны случайными (как прошедшие тест с уровнем доверия Lα). Генератор, выходные последовательности которого удовлетворяют этому условию, будем считать эталонным. Для оценки степени случайности тестируемых псевдослучайных последовательностей будем использовать величину Nt – количество тестов, признавших тестируемую псевдослучайную последовательность случайной с заданным уровнем доверия L_α=99%..

$$N_t = \sum_{i=1}^{M} n_t^i, \quad (3)$$

где M – общее количество тестов; величины n^i_t определяются следующим образом:

$$n_t^i = \begin{cases} 1, \text{ если } Pr \geq 0.99 \\ 0, \text{ если } Pr < 0.99 \end{cases} \quad (4)$$

Величина *Pr* описана в предыдущем разделе.

Значение ключа служит единственным источником энтропии для генерируемых последовательностей, поскольку алгоритм генерации является детерминированным. Для изучения влияния величины энтропии на статистические свойства получаемых ПСП их генерация выполнялась в трех вариантах. С помощью различных комбинаций ключевых последовательностей были получены разные выборки ПСП (1 ключ, 10 ключей, 40 ключей), для которых определялась величина N_t.

Вариант с 1 ключом: для каждого из 40 рассмотренных ключей формировалась выборка из m последовательностей длиной $l=10^6$ бит.

Вариант с 10 ключами: в качестве ключа генератора использовались поочередно наборы из всех 10 ключей каждой группы. Каждая десятая часть выборки генерировалась при своем значении ключа. Из полученных 10 частей путем конкатенации на выходе формировалась очередная выборка из m последовательностей длиной l бит каждая.

Вариант с 40 ключами: использовался набор из всех 40 рассмотренных ключей. Каждая сороковая часть выборки генерировалась при очередном значении ключа. С помощью конкатенации из полученных 40 частей формировалась выборка из m последовательностей длиной l бит.

Результаты обработки полученных значений N_t для разных комбинаций ключей в зависимости от размера выборки m приведены на рисунках 1-3.

На рисунке 1 показан характер изменения параметра Nt для варианта с 1 ключом. Генерация ПСП осуществлялась для каждого ключа при значениях размера выборки m 100, 1000, 2000 и 4000 последовательностей. По результатам тестирования значения параметра N_t усреднялись по ключам. Характер кривых показывает, что при таком формировании ПСП статистические свойства псевдослучайных последовательностей при увеличении выборки ухудшаются. Это связано с тем, что единственным источником энтропии для детерминированного КСГПСП является ключ, который обладает определенным количеством энтропии, величина которой в процессе генерации ПСП не изменяется. Это приводит к тому, что чем больше длина ПСП (т.е. чем больше выборка *m*) тем на большее количество бит генератор «растягивает» имеющуюся энтропию. Вследствие этого статистические характеристики тестируемых последовательностей ухудшились.

Анализ результатов показывает, что увеличение количества ключей вызывает заметные изменения в характере кривых (рис.2, рис.3). Это можно объяснить только вводом дополнительной энтропии в процессе работы генераторов через увеличение количества ключей. Для идеальных истинно случайных последовательностей значение параметра должно быть постоянным и равняться полному количеству тестов, т.е. 188 (вне зависимости от размера выборки).

Критерий оценки генераторов по соотношению «качество – скорость»

Предлагается использовать как численный критерий качества генераторов безразмерную величину

$$q = RN_TV, \quad (5)$$

где N_t, – введенное выше значение, характеризующее статистические свойства генератора, V – скорость

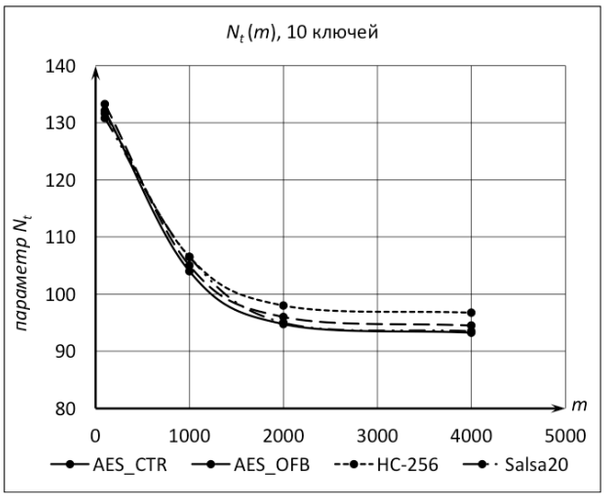

Рис.1. Зависимость параметра N_t от размера выборки (1 ключ)

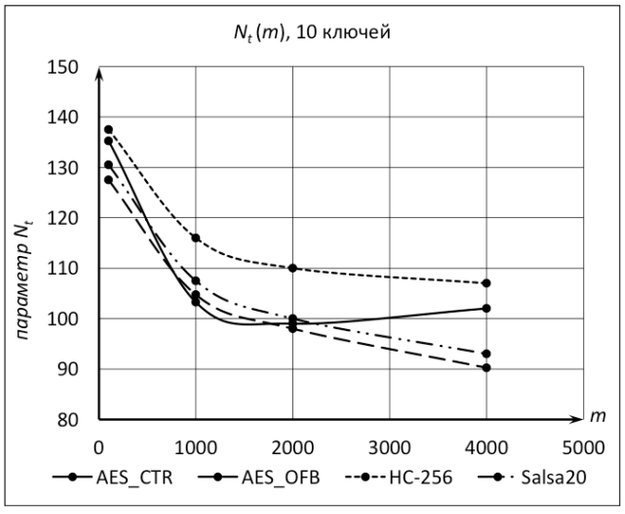

Рис.2. Зависимость параметра N_t от размера выборки (10 ключей)

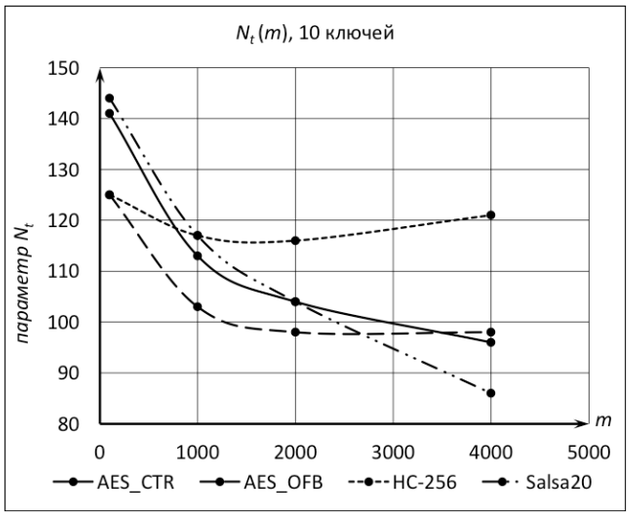

Рис.3. Зависимость параметра N_t от размера выборки (40 ключей)

работы генератора (байт/сек), R – коэффициент перехода к безразмерным значениям.

Поскольку скорость работы алгоритма V зависит от используемого процессора, удобнее перейти от скорости к производительности генератора p, выраженной в циклах на байт, с помощью соотношения

$$V = \frac{F_{CPU}}{p}, \qquad (6)$$

где F_{CPU} – тактовая частота процессора (Гц).

Производительность генераторов зависит от разных факторов: от вида платформы, на которой предполагается использовать генератор, от аппаратной поддержки операций, используемых в алгоритмах, от средств распараллеливания вычислительных процессов алгоритмов. На рисунке 4 приведены значения производительности алгоритмов (в циклах на байт) использовавшихся в работе генераторов в один поток для процессора Intel Core 2 Duo @ 2137МГц. Выбранная размерность позволяет сравнивать производительности независимо от процессора.

Лучшей производительностью среди выбранных ГПСП в указанных условиях обладает генератор HC-256 (рис.4).

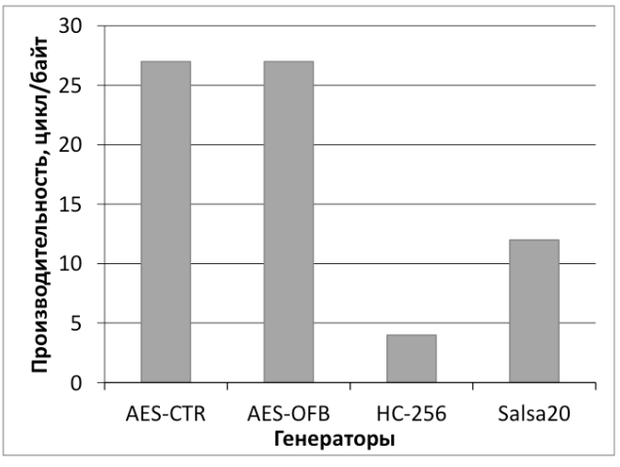

Рис.4. Производительность рассмотренных генераторов (p, цикл/байт), процессор Intel Core 2 Duo @2137МГц

При расчете критерия целесообразно перейти к относительным (нормированным) значениям, выполняя деление скорости V на V_{MAX} – лучшую (т.е. максимальную) скорость среди сравниваемых генераторов. Нормирование производительности генератора выполняется делением производительности p на P_{MIN} – лучшую (соответственно, минимальную) производительность в циклах на байт сравниваемых генераторов, а величины N_t – на общее количество тестов M. Величина $N_t^{норм}$ фактически показывает степень отклонения статистических свойств тестируемого генератора от генератора, принятого в качестве эталонного.

С учетом вышесказанного, коэффициент перехода к безразмерным значениям R записывается следующим образом:

$$R = \frac{p_{\min}}{M F_{CPU}}. \quad (7)$$

Таким образом, окончательно критерий «качество – скорость» записывается в следующем виде:

$$q = N_t^{норм} V^{норм} = \frac{N_t^{норм}}{p^{норм}}. \quad (8)$$

Диапазон возможных значений критерия q представляет собой отрезок [0,1].

Ниже представлены значения критерия q в зависимости от размера выборки (рис.5).

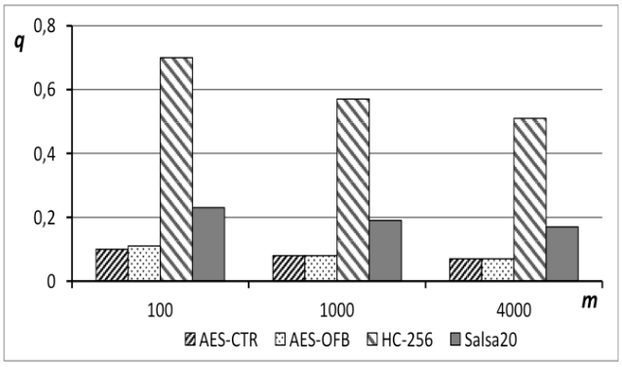

Рис.5. Оценка генераторов по соотношению «качество – скорость» (1 ключ) на платформе Intel

Для других комбинаций ключей соотношение между значениями q для разных генераторов остается аналогичным.

Обобщая полученные результаты, расположим рассмотренные генераторы в порядке убывания значения критерия «качество-скорость»: HC-256, Salsa20, AES-CTR, AES-OFB.

Все приведенные результаты показывают явное преимущество генератора HC-256 по указанному критерию.

Рекомендации по выбору ГПСЧ

Необходимо отметить, что чисто количественные оценки качества генераторов не охватывают всех факторов, которые необходимо учитывать при выборе генератора для конкретных задач.

В зависимости от особенностей организации и функционирования конкретной КФС приоритетными могут оказываться разные аспекты реализации и применения генератора. Далее приведены рекомендации для обоснованного выбора ГПСП в соответствии с особенностями работы в условиях конкретной КФС на примере рассмотренных в статье генераторов.

Если определяющей характеристикой генератора является скорость работы (приложения, для которых время реакции является критичным), выбор следует производить среди поточных алгоритмов. Например, если используется 32-битная платформа с полным набором аппаратных команд, такие алгоритмы могут обеспечить наиболее высокую скорость генерации ПСП. Среди рассмотренных генераторов следует отдать предпочтение HC-256, имеющему наилучшее соотношение качества и скорости.

Если наиболее существенна криптостойкость, следует учитывать фактическую изученность стойкости алгоритмов и выбирать те, для которых неизвестны факты успешных атак (все рассмотренные генераторы).

Если наиболее существенным является требование переносимости и возможность использования вычислительных устройств малой мощности (например, 8- или 16-битных процессоров с ограниченной вычислительной мощностью и ограничениями на потребление энергии), то предпочтительно выбирать генератор на основе блочных шифров, разработанных с кросс-платформенной совместимостью. Алгоритм AES отвечает этим требованиям в силу своей байт-ориентированной структуры.

Для ускорения работы за счет организации параллельных вычислений следует применять генераторы, ориентированные на распараллеливание (среди рассмотренных это Salsa20 и AES в режиме счетчика).

Выводы

Криптостойкие генераторы псевдослучайных последовательностей являются необходимой составной частью систем защиты информации, во многом определяя их надежность. Повышение уровня защиты информации является актуальной задачей, в том числе, для киберфизических систем, многие из которых работают в режиме постоянного обмена данными.

Оценку эффективности и сравнения генераторов ПСП предложено выполнять на основе такого критерия, как соотношение «качество – скорость». С помощью этого критерия было выполнено сравнение исследуемых КСГПСП.

Повышение защищенности данных в киберфизических системах требует тщательного подхода к выбору ГПСП. Существование большого количества алгоритмов генерации ПСП делает актуальным обоснованное сравнение генераторов.

Для проверки предложенного критерия было проведено тестирование выходных ПСП выбранных генераторов ПСП на основе стойких криптоалгоритмов с помощью пакета статистических тестов NIST STS. Для получения статистически значимых результатов тестирование проводилось с различными размерами выборки, уровнями значимости и большим количеством ключей разных типов.

Проведенные исследования показали возможность применения генераторов на основе стойких криптоалгоритмов, т.к. все рассмотренные генераторы показали высокое качество производимых ПСП.

Анализ результатов тестирования проводился на основе выбранного параметра – количества тестов, признавших тестируемую псевдослучайную последовательность истинно случайной как прошедшую тест с уровнем доверия 99%.

В статье показано, что введенный критерий «качество – скорость» дает возможность выявить различия статистических свойств рассмотренных генераторов ПСП.

Рецензент: *Бегаев Алексей Николаевич, кандидат технических наук, Генеральный директор АО «Эшелон-СЗ», Санкт-Петербург, Россия. E-mail: a.begaev@nwechelon.ru*

Литература

1 Dong P., Han Y., Guo X., Xie F. A systematic review of studies on cyber physical system security // International Journal of Security and Its Applications. 2015. Vol. 9. No. 1. Pp. 155-164. DOI: 10.14257/ijsia.2015.9.1.17.
2 Jing Q., Vasilakos A., Wan J., Lu J., Qiu D. Security of the Internet of Things: perspectives and challenges. Wireless Networks. 2014. Vol. 20(8). Pp. 2481-2501. DOI: 10.1007/s11276-014-0761-7.
3 AlDozari F. Security and privacy challenges in Cyber-Physical Systems // Journal of Information Security. 2017. Vol. 8. No. 4. Pp. 285–295. DOI: 10.4236/jis.2017.84019.
4 Humayed A., Lin J., Li F., and Luo B. Cyber-Physical Systems Security – A Survey // arXiv:1701.04525v1. 2017.
5 Zhang, H., Shu, Y.C., Cheng, P. and Chen, J.M. Privacy and Performance Trade-Off in Cyber-Physical Systems. IEEE Network, 2016. V. 30. Iss. 2. P. 62–66. DOI: 10.1109/MNET.2016.7437026.
6 Vegh L., Miclea L. Enhancing security in cyber-physical systems through cryptographic and steganographic techniques // In Proc. of IEEE International Conference on Automation, Quality and Testing, Robotics (AQTR). 2014. DOI: 10.1109/AQTR.2014.6857845.
7 Avdonin I., Budko M., Budko M., Grozov V., Guirik A. A method of creating perfectly secure data transmission channel between unmanned aerial vehicle and ground control station based on one-time pads. In Proc. of 9th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT). 2017. Pp. 410-413. DOI: 10.1109/ICUMT.2017.8255167.
8 Иванов М.А., Скитев А.А., Стариковский А.В. Классификация генераторов псевдослучайных чисел, ориентированных на решение задач защиты информации // REDS: телекоммуникационные устройства и системы. 2017. Т. 7. № 4. С. 484-487.
9 Аникин И.В., Альнаджар Х.Х. Оценка качества работы генератора псевдослучайных чисел, основанного на нечеткой логике, с помощью метода Монте-Карло // Информация и безопасность. 2017. Т. 20. № 3 (4). С. 444-447.
10 Аникин И.В., Альнаджар Х.Х. Сравнительный анализ и оценка качества генератора псевдослучайных чисел, основанного на нечеткой логике // Информационные системы и технологии. 2017. № 2 (100). С. 5-11.
11 Chugunkov I.V., Novikova O.Y., Perevozchikov V.A., Troitskiy S.S. The development and researching of lightweight pseudorandom number generators. Proc. of the 2016 IEEE North West Russia Section young researchers in electrical and electronic engineering conference, EICONRUSNW 2016. Pp. 185-189. DOI: 10.1109/EIConRusNW.2016.7448150.
12 Chugunkov I.V., Bitkina M.A., Rumyantseva I.S. The entropy assessment of modern stochastic algorithms. Proc. IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus). 2017. DOI: 10.1109/EIConRus.2017.7910568.
13 Жуков А.Е. Легковесная криптография. Часть 1 // Вопросы кибербезопасности. 2015. № 1 (9). С. 26–43.
14 Жуков А.Е. Легковесная криптография. Часть 2 // Вопросы кибербезопасности. 2015. № 2 (10). С. 2–10.
15 Orue A., Hernandez-Encinas L., Martin A., Vitini F.M. A Lightweight Pseudorandom Number Generator for Securing the Internet of Things.IEEE Access. Vol. 5. P. 27800–27806. DOI: 10.1109/ACCESS.2017.2774105.
16 Doganaksoy A., Sulak F., Uguz M., Seker O., Akcengiz Z. Mutual correlation of NIST statistical randomness tests and comparison of their sensitivities on transformed sequences // Turkish Journal of Electrical Engineering and Computer Sciences. 2017. No. 1. Pp. 655–665. DOI: 10.3906/elk-1503-214.
17 Sys M., Riha Z., Matyas V. On the interpretation of results from the NIST Statistical Test Suite // Romanian Journal of information science and technology. – 2015. Vol. 18. No. 1. Pp. 18–32.
18 Мордашов А.С. Статистическое тестирование российского стандарта функции хэширования ГОСТ 34.11-2012 («СТРИБОГ») // Вопросы кибербезопасности. 2015. № 3 (11). С. 56–59.
19 Прокофьев А.О., Чугунков И.В., Матрюхина Е.А., Гриднева Е.А. Вопросы построения программных систем оценки качества стохастических алгоритмов // Современные информационные технологии и ИТ-образование. 2016. Т. 12. № 3–1. С. 169–178.
20 Bernstein D.J. Salsa20/8 and Salsa20/12 [Электронный ресурс]. – Режим доступа: http://cr.yp.to/snuffle/812.pdf.
21 Wu H. Stream Cipher HC-256 [Электронный ресурс]. – Режим доступа: http://www.ecrypt.eu.org/stream/p3ciphers/hc/hc256_p3.pdf.
22 AES [Электронный ресурс]. – Режим доступа: https://csrc.nist.gov/csrc/media/publications/fips/197/final/documents/fips-197.pdf.
23 Augot D., Batina L., Bernstein D.J., et al. Initial recommendations of long-term secure post-quantum systems. 2015 [Электронный ресурс]. – Режим доступа: https:\\pqcrypto.eu.org/docs/initial-recommendations.pdf.
24 Sulak F., Uguz M., Kocak O., Doganaksoy A. On the independence of statistical randomness tests included in the NIST testsuite // Turkish Journal of Electrical Engineering and Computer Sciences. 2017. No. 25. Pp. 3673–3683. DOI: 10.3906/elk-1605-212.

 УДК 004.421.5

METHOD FOR ASSESSING THE QUALITY OF CRYPTOSECURE PSEUDORANDOM SEQUENCE GENERATORS

Budko M.[1], Budko M.[2], Guirik A.[3], Grozov V.[4]

Purpose: *Developing a statistical testing procedure for pseudo-random sequence generators (PRSG) to increase the efficiency and reliability of cryptographic data protection systems.*

Research methods: *Statistical testing methods for pseudo-random sequence generators based on robust cryptoalgorithms and a method for comparative analysis of numerical experiment findings.*

Results: *A quality assessment procedure for pseudo-random sequence generators was developed. A brief overview of existing approaches to pseudo-random sequence generators quality assessment is given. Generators with proven high cryptographic strength were selected for further research. The generators were used to conduct a numerical experiment to identify how their parameters affect the properties of output sequences. Statistical properties were studied using NIST STS (statistical test suite). A method is proposed for estimating the proximity of generated pseudo-random sequences to truly random ones using a preset level of passing statistical tests. The "quality - speed" criterion is proposed based on this parameter to compare pseudo-random sequence generators. It is shown that this criterion may help reveal differences in pseudo-random sequence generators statistical properties. The developed method allows the data security level to be raised by choosing the best generation algorithm for pseudo-random sequences.*

Keywords: *cryptographic algorithm, NIST STS test package, bit sequence, pseudorandom sequence, statistical tests, data protection, PRS generation algorithm*

References

1 Dong P., Han Y., Guo X., Xie F. A systematic review of studies on cyber physical system security. International Journal of Security and Its Applications. 2015. Vol. 9. No. 1. Pp. 155–164. DOI: 10.14257/ijsia.2015.9.1.17.

2 Jing Q., Vasilakos A., Wan J., Lu J., Qiu D. Security of the Internet of Things: perspectives and challenges. Wireless Networks. 2014. Vol. 20(8). Pp. 2481–2501. DOI: 10.1007/s11276-014-0761-7.

3 AlDozari F. Security and privacy challenges in Cyber-Physical Systems // Journal of Information Security. 2017. Vol. 8. No. 4. Pp. 285–295. DOI: 10.4236/jis.2017.84019.

4 Humayed A., Lin J., Li F., and Luo B. Cyber-Physical Systems Security – A Survey // arXiv:1701.04525v1. 2017.

5 Zhang, H., Shu, Y.C., Cheng, P. and Chen, J.M. Privacy and Performance Trade-Off in Cyber-Physical Systems. IEEE Network, 2016. V. 30. Iss. 2. P. 62–66. DOI: 10.1109/MNET.2016.7437026.

6 Vegh L., Miclea L. Enhancing security in cyber-physical systems through cryptographic and steganographic techniques // In Proc. of IEEE International Conference on Automation, Quality and Testing, Robotics (AQTR). 2014. DOI: 10.1109/AQTR.2014.6857845.

7 Avdonin I., Budko M., Budko M., Grozov V., Guirik A. A method of creating perfectly secure data transmission channel between unmanned aerial vehicle and ground control station based on one-time pads. In Proc. of 9th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT). 2017. Pp. 410–413. DOI: 10.1109/ICUMT.2017.8255167.

8 Ivanov M.A., Skitev A.A., Starikovskij A.V. Klassifikaciya generatorov psevdosluchajnyh chisel, orientirovannyh na reshenie zadach zashchity informacii // REDS: telekommunikacionnye ustrojstva i sistemy [REDS: telecommunication devices and systems]. 2017. T. 7. № 4. Pp. 484–487.

9 Anikin I.V., Al'nadzhar H.H. Ocenka kachestva raboty generatora psevdosluchajnyh chisel, osnovannogo na nechetkoj logike, s pomoshch'yu metoda Monte-Karlo // Informaciya i bezopasnost' [Information and security]. 2017. Vol. 20. No. 3 (4). Pp. 444–447.

10 Anikin I.V., Al'nadzhar H.H. Sravnitel'nyj analiz i ocenka kachestva generatora psevdosluchajnyh chisel, osnovannogo na nechetkoj logike // Informacionnye sistemy i tekhnologii [Information systems and technologies]. 2017. No. 2 (100). Pp. 5–11.

11 Chugunkov I.V., Novikova O.Y., Perevozchikov V.A., Troitskiy S.S. The development and researching of lightweight pseudorandom

1 Marina Budko, Ph.D., Associate Professor for ISCT faculty, ITMO University, Saint-Petersburg, Russia. E-mail: mbbudko@corp.ifmo.ru, ORCID 0000-0001-7054-5709

2 Mikhail Budko, Ph.D., Associate Professor for ISCT faculty, ITMO University, Saint-Petersburg, Russia. E-mail: mbudko@corp.ifmo.ru, OCRID 0000-0002-1444-277X

3 Alexei Guirik, Ph.D., Associate Professor for ISCT faculty, ITMO University, Saint-Petersburg, Russia. E-mail: avg@corp.ifmo.ru, ORCID 0000-0002-4021-7605

4 Vladimir Grozov, Postgraduate Student at ISCT faculty, ITMO University, Saint-Petersburg, Russia. E-mail: vagrozov@corp.ifmo.ru, ORCID 0000-0002-7998-8175

number generators. Proc. of the 2016 IEEE North West Russia Section young researchers in electrical and electronic engineering conference, EICONRUSNW 2016. Pp. 185–189. DOI: 10.1109/EIConRusNW.2016.7448150.
12 Chugunkov I.V., Bitkina M.A., Rumyantseva I.S. The entropy assessment of modern stochastic algorithms. Proc. IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus). 2017. DOI: 10.1109/EIConRus.2017.7910568.
13 Zhukov A.E. Legkovesnaya kriptografiya. Chast' 1 // Voprosy kiberbezopasnosti [Cybersecurity issues]. 2015. No. 1 (9). Pp. 26–43.
14 Zhukov A.E. Legkovesnaya kriptografiya. Chast' 2 // Voprosy kiberbezopasnosti [Cybersecurity issues]. 2015. No. 2 (10). Pp. 2–10.
15 Orue A., Hernandez-Encinas L., Martin A., Vitini F.M. A Lightweight Pseudorandom Number Generator for Securing the Internet of Things.IEEE Access. Vol. 5. Pp. 27800–27806. DOI: 10.1109/ACCESS.2017.2774105.
16 Doganaksoy A., Sulak F., Uguz M., Seker O., Akcengiz Z. Mutual correlation of NIST statistical randomness tests and comparison of their sensitivities on transformed sequences // Turkish Journal of Electrical Engineering and Computer Sciences. 2017. No. 1. Pp. 655–665. DOI: doi:10.3906/elk-1503-214.
17 Sys M., Riha Z., Matyas V. On the interpretation of results from the NIST Statistical Test Suite // Romanian Journal of information science and technology. – 2015. Vol. 18. No. 1. Pp. 18–32.
18 Mordashov A.S. Statisticheskoe testirovanie rossijskogo standarta funkcii heshirovaniya GOST 34.11-2012 («STRIBOG») // Voprosy kiberbezopasnosti [Cybersecurity issues]. 2015. No. 3 (11). Pp. 56–59.
19 Prokof'ev A.O., Chugunkov I.V., Matryuhina E.A., Gridneva E.A. Voprosy postroeniya programmnyh sistem ocenki kachestva stohasticheskih algoritmov // Sovremennye informacionnye tekhnologii i IT-obrazovanie [Modern information technologies and IT-education]. 2016. Vol. 12. No. 3–1. Pp. 169–178.
20 Bernstein D.J. Salsa20/8 and Salsa20/12. URL: http://cr.yp.to/snuffle/812.pdf.
21 Wu H. Stream Cipher HC-256 URL: http://www.ecrypt.eu.org/stream/p3ciphers/hc/hc256_p3.pdf.
22 AES. URL: https://csrc.nist.gov/csrc/media/publications/fips/197/final/documents/fips-197.pdf.
23 Augot D., Batina L., Bernstein D.J., et al. Initial recommendations of long-term secure post-quantum systems. 2015. URL: https://pqcrypto.eu.org/docs/initial-recommendations.pdf.
24 Sulak F., Uguz M., Kocak O., Doganaksoy A. On the independence of statistical randomness tests included in the NIST testsuite // Turkish Journal of Electrical Engineering and Computer Sciences. 2017. No. 25. Pp. 3673–3683. DOI: 10.3906/elk-1605-212.