ПОСТРОЕНИЕ ФУНКЦИИ ГЕНЕРАЦИИ КРИПТОГРАФИЧЕСКИ СТОЙКИХ ПСЕВДОСЛУЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ НА БАЗЕ АЛГОРИТМА ШИФРОВАНИЯ «КУЗНЕЧИК»

Беляев С.С.[1], Будько М.Б.[2], Будько М.Ю.[3], Гирик А.В.[4], Грозов В.А.[5]

Цель статьи: *повысить криптостойкость ПСП, получаемых с помощью функции генерации на базе алгоритма шифрования «Кузнечик».*

Методы исследования: *методики построения генераторов псевдослучайных последовательностей с использованием стойкого криптоалгоритма в качестве функции генерации в соответствии с рекомендациями NIST SP 800-90; методы теории вероятностей и математической статистики (проверки статистических гипотез, критерий согласия Пирсона), методы оценки энтропии случайного процесса.*

Полученный результат: *предложен способ построения основного компонента генератора псевдослучайных последовательностей – функции генерации псевдослучайных последовательностей на основе криптоалгоритма «Кузнечик» (российский стандарт шифрования ГОСТ Р 34.12-2015) с помощью ряда модификаций исходного алгоритма. Особенности алгоритма позволяют использовать его в режиме, который объединяет достоинства известных режимов работы блочных шифров OFB и CTR. Разработаны и реализованы процедура формирования раундовых ключей, а также другие модификации алгоритма, повышающие его защищенность при сохранении его производительности. Оценка работы генератора выполнялась по статистическим свойствам выходных последовательностей (тесты NIST SP 800-22), критерию Пирсона χ^2, а также min-энтропии (тесты NIST 800-90B). По рассмотренным характеристикам предложенная функция генерации близка к эталонному варианту на базе ГОСТ 34.12-2015 «Кузнечик», но превосходит ее по уровню защищенности.*

Ключевые слова: *генератор случайных битов, псевдослучайные последовательности, ГОСТ Р 34.12-2015 «Кузнечик», SP-сеть, сеть Фейстеля, критерий Пирсона, min-энтропия, NIST 800-90, NIST SP 800-22.*

DOI:10.21681/2311-3456-2021-4-25-34

Введение

В настоящее время глобальное развитие цифровых технологий резко повышает требования к обеспечению информационной безопасности соответствующих коммуникационных процессов. При этом существенную опасность представляют атаки на каналы связи, нацеленные на получение несанкционированного доступа к передаваемым данным.

Криптографические методы являются основными при организации защиты данных. Их надежность во многом определяется качеством используемых криптографических примитивов, в том числе – генераторов случайных последовательностей (ГСП), среди которых выделяют генераторы истинно- и псевдослучайных последовательностей (соответственно ГСП и ГПСП) [1-4]. ГСП используют для выработки случайных битов измерения физических величин, имеющих случайную природу и поэтому фактически непредсказуемых. ГПСП строятся на основе детерминированных алгоритмов, однако при этом они должны обеспечивать как непредсказуемость генерируемых выходных значений, так и неотличимость их статистических свойств от свойств истинно случайных последовательностей.

В последние десятилетия в области построения ГСП происходит становление стандартизации. Один из вариантов соответствующих рекомендаций представлен в документах NIST (Национальный Институт Стандартов и Технологии США) Special Publication 800-90 A, B, C (Recommendation for Random Bit Generator (RBG) Constructions (DRAFT NIST Special Publication 800-90C), 2012; Recommendation for the Entropy Sources Used for

1 Беляев Сергей Степанович, ассистент факультета БИТ Университета ИТМО, Санкт-Петербург, Россия. E mail: ssbelyaev@itmo.ru, ORCID 0000-0001-6411-1154

2 Будько Марина Борисовна, кандидат технических наук, старший научный сотрудник факультета БИТ Университета ИТМО, Санкт-Петербург, Россия. E-mail: mbbudko@itmo.ru, ORCID 0000-0001-7054-5709

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

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

5 Грозов Владимир Андреевич, аспирант, Университет ИТМО, Санкт-Петербург, Россия. E mail: vagrozov@itmo.ru , ORCID 0000-0002-7998-8175

Random Bit Generation (DRAFT NIST Special Publication 800-90B); Recommendation for Random Number Generation Using Deterministic Random Bit Generators (Draft NIST Special Publication 800-90A). Их итоговая третья часть, NIST SP 800-90C, описывает структуру генераторов случайных битов, в которой объединяется применение механизмов детерминированных генераторов, описываемых в NIST 800-90A, и источников энтропии, определяемых в NIST 800-90B.

Функционирование ГСП, как правило, связано с ощутимыми техническими трудностями, нестабильностью используемого оборудования, низкой скоростью, а также значительными затратами времени и ресурсов. При этом возникает проблема поиска надежного и практически реализуемого источника энтропии. Долгое время приоритетными вариантами получения случайных данных считались процессы, относящиеся к оптике и квантовой физике [1,2,4]. Однако практическое массовое использование таких генераторов в настоящее время неосуществимо. В то же время на фоне бурного развития микроэлектроники и миниатюризации различных широко используемых датчиков возвращается интерес к неквантовым источникам случайности [6-10]. Использование доступных и дешевых источников энтропии делает возможным построение практически реализуемых ГСП, спроектированных на принципах, сформулированных в рекомендациях NIST.

ГПСП строятся на основе некоторого детерминированного алгоритма и не имеют названных недостатков ГСП. Однако они не могут гарантировать необходимую степень криптостойкости выходных последовательностей. Криптографически стойкие ГПСП обычно строятся на базе блочных или поточных криптоалгоритмов, разные типы которых имеют в этом отношении свои преимущества [2,4,5].

Алгоритмы блочных шифров можно использовать как ГПСП за счет выбора соответствующих режимов работы, а именно режима обратной связи по выходу (Output Feedback mode, OFB) и режима счетчика (Counter mode, CTR), в которых блочные шифры выполняют поточное шифрование. Блочные алгоритмы основаны на многократных преобразованиях подстановки и перестановки, что гарантирует высокую криптостойкость шифра и непредсказуемость выходных данных. Современные подходы к разработке криптостойких ГСП, например, сформулированные в Рекомендациях NIST, предполагают совместное использование непрерывного потока энтропии, полученной от естественных источников, и детерминированных генераторов.

Обычно при исследовании генераторов случайных последовательностей рассматриваются отдельные аспекты повышения их качества. Работа [5] представляет ГПСП с новым механизмом перестановок на базе сети Фейстеля с 16 ветвями, использующей блоки криптоалгоритма AES. В работе [11] решается задача получения достаточного количества энтропии от метастабильных процессов на защелках транзистора с помощью их моделирования цепями Маркова. Статья [12] посвящена разработке и оценке качества облегченных генераторов псевдослучайных чисел. В этой работе описаны принципы проектирования облегченных генераторов (LW, light-weight) и сформулированы требования к их качеству. В работе приведен пример преобразования классического генератора в LW-генератор путем модификации функции обратной связи. Предложены методы оценки качества псевдослучайных чисел, формируемых облегченным генератором. В работе [13] выполняется анализ классификации ГПСП и предлагается ее развитие. Обосновывается необходимость использовать наряду с традиционными сетями Фейстеля архитектуру «Квадрат» и «Куб», а также их гибридные варианты. В работе [14] изучается влияние нелинейных раундовых функций современных блочных криптоалгоритмов. Выполняется теоретическая оценка минимально необходимого числа раундов для полного рассеяния и перемешивания информации. В работе [15] предложено дополнить традиционную структуру ГПСП этапом улучшения статистических свойств выходной последовательности. В статье [16] выполняется уточнение оценки min-энтропии с применением условной вероятности. Работа [8] представляет собой характерный пример разработки генератора случайных последовательностей с использованием неквантовых источников энтропии – сенсоров дрона. Также появляются работы, использующие в качестве источников энтропии совершенно новые, ранее не использовавшиеся устройства: носимые датчики, измеряющие гальваническую реакцию кожи на проявления эмоций [9], или генераторы случайных последовательностей на основе биометрических данных человека [10].

Перспективным с точки зрения использования в качестве ГПСП представляется российский стандарт ГОСТ 34.12-2015 «Кузнечик». Исследованию вопросов надежности, криптостойкости и повышению быстродействия этого алгоритма шифрования посвящен ряд работ [17-21].

В большинстве публикаций последних лет, посвященных генераторам СП, генераторы каждого из двух типов исследуются по отдельности – либо ГСП, либо ГПСП. При таком подходе за пределами рассмотрения оказываются важные вопросы практического построения генератора, а именно выбора конкретных алгоритмов для отдельных блоков, реализации их взаимодействия, оценивания качества работы генератора в целом.

В работе представлено построение эффективного детерминированного генератора СП (генератора ПСП) на базе алгоритма российского стандарта шифрования ГОСТ Р 34.12-2015 «Кузнечик». Результаты работы такого генератора должны обладать высокой степенью криптостойкости, случайности, равномерности распределения.

В статье рассматриваются способы повышения эффективности функции генерации ПСП, построенной на базе российского стандарта шифрования ГОСТ Р 34.12-2015 «Кузнечик». Во втором разделе представлена общая структура детерминированного генератора, описание алгоритма «Кузнечик», а также его особенно-

сти. Третий раздел посвящен построению функции генерации на основе модификации указанного алгоритма. В четвертом разделе приводится методика оценки качества выходных последовательностей. Пятый раздел содержит результаты тестирования и оценки качества выходных битовых последовательностей.

Алгоритм построения генератора псевдослучайных последовательностей

В статье предлагается вариант построения генератора псевдослучайных последовательностей (ГПСП) на основе российского стандарта шифрования ГОСТ Р 34.12-2015 «Кузнечик» с учетом рекомендаций NIST 800-90A. Его структура представлена на рис. 1.

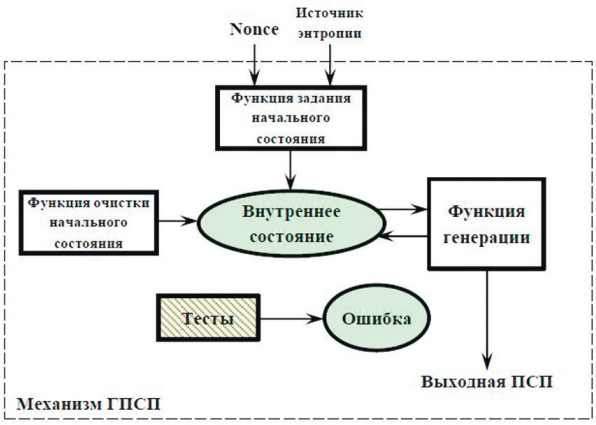


Рис. 1. Функциональная модель генератора псевдослучайных последовательностей

В качестве алгоритма, реализующего функцию генерации ПСП, используется алгоритм блочного шифрования ГОСТ Р 34.12-2015 «Кузнечик». Он является симметричным блочным шифром, обладающим высокой криптостойкостью, имеющим размер блока 128 битов и длину ключа 256 битов. Процесс работы алгоритма состоит из 10 раундов. Алгоритм использует сеть Фейстеля для генерации раундовых ключей и подстановочно-перестановочную (SP)-сеть для шифрования.

Отметим важные особенности указанного алгоритма.

Шифр, основанный на SP-сети, получает на вход блок длиной 128 битов и ключи. После этого он совершает несколько раундов, состоящих из стадий подстановки S (нелинейного преобразования S) и перестановки P (линейного преобразования L). Таким образом, в «Кузнечик» каждый раунд включает в себя линейное и нелинейное преобразование, а также операцию наложения так называемого итерационного ключа при помощи операции XOR. Как уже отмечалось, генерация раундовых ключей выполняется при помощи сети Фейстеля. В алгоритме «Кузнечик» раунд шифрования SP-сетью и итерация сети Фейстеля при формировании раундовых ключей построены на использовании общего блока преобразований Ek. Схема этого блока приведена на рис. 2. Такое построение обеспечивает относительную простоту алгоритма.

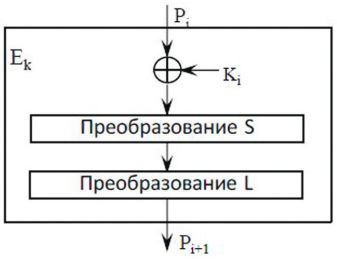


Рис. 2. Схема общего блока преобразования алгоритма «Кузнечик»

Собственно шифрование состоит из 9 раундов, в каждом из которых выполняется описанный выше блок преобразований. После них выполняется последний, 10-й раунд, состоящий только из наложения последнего (10-го) итерационного ключа. Схема преобразований одного раунда шифрования Ek иначе может быть записана в виде формулы $P_{i+1} = E_k(P_i, K_i)$, где P_i – входной 128 битный блок, P_{i+1} – выходной 128 битный блок, K_i – раундовый ключ. Тогда один цикл шифрования можно представить в виде схемы, представленной на рис. 3.

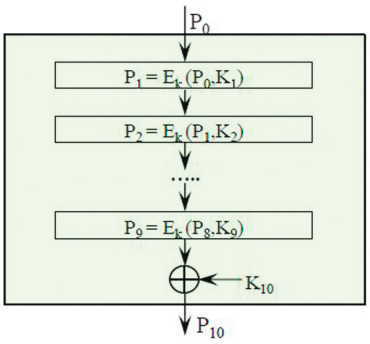


Рис 3. Один цикл шифрования в алгоритме «Кузнечик»

Раундовые ключи формируются путем преобразований на основе мастер-ключа K длиной 256 битов. Перед началом шифрования он разбивается на 2 половины, которые составят первую пару раундовых ключей – K_1^0 и K_2^0. Для генерации каждой следующей пары применяются 8 итераций сети Фейстеля (F). Схема работы сети Фейстеля представлена на рис. 4, где Ek – блок преобразований, (K_1^0, K_2^0) – раундовые ключи, подающиеся на вход схемы, (K_1^1, K_2^1) – новая пара ключей (результат генерации). Верхний индекс является текущим номером пары раундовых ключей. В каждой итерации используется такой же блок преобразования Ek, как и в SP-сети.

Важной особенностью алгоритма «Кузнечик» является использование дополнительной ключевой информации в виде набора констант C_i, которые являются результатом линейного преобразования L, применяемого к значению номера итерации. Подробнее о них будет говориться в следующем подразделе.

DOI:10.21681/2311-3456-2021-4-25-34

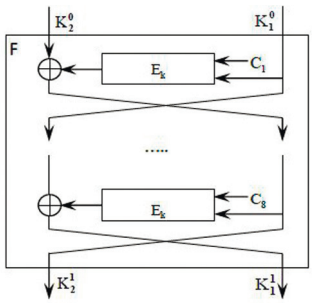


Рис. 4. Схема сети Фейстеля (F) для вычисления очередной пары раундовых ключей в алгоритме «Кузнечик»

Особый интерес представляет алгоритм линейного преобразования L. Оно применяется к 128 битной последовательности вида $a = a_{15} \| \ldots \| a_i \| \ldots \| a_0, i = 0,\ldots,15$, где a_i – 8-битная строка, || – символ конкатенации. Преобразование выполняется путем вычисления новых значений последовательности по формуле:

$$\gamma(a_{15},\ldots,a_0) = \delta^{-1}\left[D_0 * \delta(a_{15}) \oplus D_1 * \delta(a_{14}) \oplus \ldots \oplus D_{15} * \delta(a_0)\right] \quad (1)$$

где δ – биективное отображение двоичной строки в элемент поля Галуа, δ^{-1} – отображение, обратное к δ, D=(148, 32, 133, 16, 194, 192, 1, 251, 1, 192, 194, 16, 133, 32, 148, 1) – коэффициенты, определенные алгоритмом «Кузнечик», ⊕, * – операции сложения и умножения в поле Галуа GF(2^8). Операция * в (1) выполняются в конечном поле Галуа над неприводимым многочленом $x^8 + x^7 + x^6 + x + 1$.

В результате первого шага преобразования получается 8-битная строка $\gamma(a_{15},\ldots,a_0)$. С ее помощью формируется новая 128 битная последовательность вида $G(a) = \gamma(a_{15},\ldots,a_0) \| a_{15} \| \ldots \| a_1$.

Такие операции выполняются еще 15 раз до полного обновления исходной последовательности a.

Выражение (1) содержит многократное выполнение трудоемких операций умножения в поле Галуа. В целях повышения быстродействия предлагается заранее вычислить одномерные массивы $B_i = D_i * \delta(a_{15-i}), i = 0,\ldots,15$, в каждом из которых содержатся 256 однобайтовых элементов. В этом случае выражение (1) записывается в виде

$$\gamma(a_{15},\ldots,a_0) = \delta^{-1}\left(B_0(a_{15}) \oplus B_1(a_{14}) \oplus \ldots \oplus B_{15}(a_0)\right) \quad (2)$$

При такой организации вычислений умножение в поле Галуа заменяется выбором элементов из массивов и операций XOR между этими элементами. Это существенно повышает скорость работы алгоритма. Аналогичный подход рассматривался в [15].

Подход к построению ГПСП

Любой детерминированный генератор случайных последовательностей формирует поток битов. Следовательно, естественным для него является режим поточного шифрования. Рекомендации NIST 800-90A предполагают использование режима поточного шифрования CTR. Однако для внесения дополнительной неопределенности в процесс генерации ПСП целесообразно использовать режим OFB. В режиме OFB для получения очередного блока псевдослучайной последовательности на вход алгоритма подается ее предыдущий блок, к которому применяется операция наложения очередного раундового ключа.

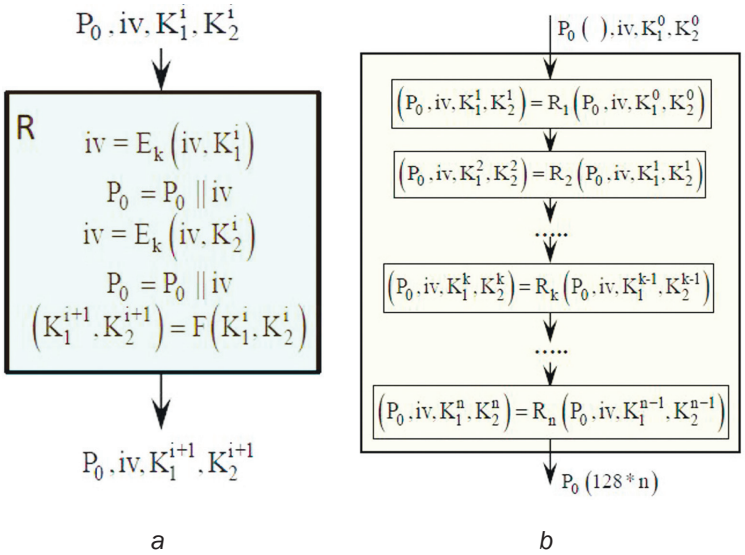
Возможности алгоритма «Кузнечик» позволяют вносить уникальные значения счетчика в раундовые ключи путем использования дополнительных констант Ci. Такой вариант работы алгоритма соответствует режиму CTR. При этом формирование выходной последовательности предлагается организовать в режиме OFB. Таким образом, фактически объединяются возможности режимов OFB и CTR.

Работа криптоалгоритма «Кузнечик» в качестве генератора псевдослучайных последовательностей дает возможность иначе организовать процесс формирования внутренней ключевой информации, а также сократить ее жизненный цикл. Обычное применение алгоритма «Кузнечик» в целях шифрования требует обязательного хранения данных о раундовых ключах и его начальном состоянии для выполнения процедуры блочного шифрования. При использовании алгоритма в качестве ГСП особенности работы сети Фейстеля позволяют обеспечить непрерывную выработку раундовых ключей и отказаться от хранения их полного набора.

Схема генерации 256 битов псевдослучайной последовательности в режиме поточного шифрования представлена на рис. 5-a, где P_0 – результирующая последовательность, в которую добавляются путем конкатенации новые сгенерированные блоки, iv – начальный вектор инициализации, который затем используется как выходной блок очередного раунда работы генератора.

Работа генератора в режиме поточного шифрования для одного запроса на генерацию схематично показана на рис. 5-b. Она заключается в последовательной генерации 128-битных блоков псевдослучайной последовательности. В качестве начального вектора инициализации (iv) берется 128-битный блок, который предварительно заполняется случайными битами, полученными от источника энтропии. В дальнейшем на его место записывается текущий сгенерированный блок результирующей последовательности, уничтожая его прежнее содержимое (в соответствии с режимом OFB). Также на вход ГПСП поступает мастер-ключ $K = K_1 \| K_2$, который при инициализации запроса рассматривается как первая пара раундовых ключей – K_1^0 и K_2^0.

Предлагается следующая модификация исходного алгоритма. При вычислении каждой следующей пары раундовых ключей их значения записываются снова в K_1 и K_2, заменяя предшествующие значения. Таким образом, одновременно в памяти в этом случае хранятся только 2 значения ключей для следующего раунда



a *b*

Рис. 5. a. Схема генерации 256 битов ПСП в режиме поточного шифрования. b. Цикл работы генератора для одного запроса в режиме поточного шифрования

генерации псевдослучайной (выходной) последовательности (рис. 4) вместо предусмотренных 10. Это делает механизм генерации раундовых ключей, а, следовательно, и механизм работы всего генератора более защищенным.

Также в алгоритм вносятся следующие дополнительные изменения. Наличие в алгоритме «Кузнечик» констант Ci позволяет вносить в его работу дополнительную неопределенность. Для этого предлагается организовать два параллельно работающих счетчика – счетчик запросов на генерацию новой псевдослучайной последовательности и счетчик итераций сети Фейстеля. Их текущие значения размещаются внутри констант C_i (рис. 6).

Такая организация работы счетчиков исключает возможность повторений значения константы C_i. При необходимости в состав 128 битов константы C_i может быть записано уникальное значение nonce (“number used once” – “число, используемое только один раз”). Это дает возможность вносить дополнительную неопределенность в процесс формирования раундовых ключей.

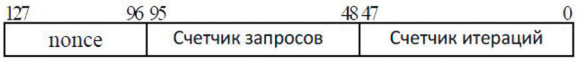


Рис. 6. Структура константы C_i

Следует отметить, что предложенная организация работы с раундовыми ключами приводит к тому, что при генерации каждого нового блока выходной последовательности используется уникальный набор раундовых ключей. Таким образом, повышается непредсказуемость результата генерации.

Использование сети Фейстеля для вычисления раундовых ключей позволяет использовать модифицированный алгоритм с любым другим числом раундов в одном цикле шифрования (8, 14, 20 раундов и т.д. вместо 10 при необходимости). Такое варьирование числа раундов позволяет по мере надобности либо повышать секретность выходных данных, либо увеличивать скорость их получения.

Методика контроля качества выходных последовательностей

Для генераторов псевдослучайных последовательностей, используемых в задачах криптографической защиты данных, необходима надежная проверка близости свойств выходных последовательностей к свойствам истинно случайных. В качестве оценки меры такой близости обычно выступает наличие равномерного распределения, большого периода, равной частоты появления одинаковых подстрок, статистических свойств и непредсказуемости выходных значений.

Оценка качества выходных псевдослучайных последовательностей осуществлялась по их трем характеристикам: статистика критерия Пирсона χ2, min-энтропия и истинность проверяемой статистической гипотезы.

Контроль равномерности распределения проводится с помощью проверки того, насколько распределение выходной битовой последовательности близко к теоретическому (равномерному) распределению выполняется в соответствии с критерием χ2 (Пирсона). Для такой оценки вычисляется величина статистики

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

где m – общее число значений, v_i – рассчитанное для каждого интервала количество принадлежащих ему значений, k – количество интервалов. С помощью теста χ^2 проверяется, насколько количество значений v_i близко к теоретической величине m/k.

Поскольку в шифре ГОСТ Р 34.12-15 «Кузнечик» информация обрабатывается побайтово, расчет критерия

Пирсона проводится на 28 интервалах. Вычисленное значение χ^2 должно быть меньше значения Ккрит, которое для такого количества интервалов приблизительно равно 300.

Min-энтропия [1,2] (порядок энтропии $\alpha \to \infty$) является предельным случаем энтропии Реньи. Она вычисляется по формуле:

$$H = \min_{1 \le i \le k} \left(-\log_2 p_i\right) = -\log_2 \left(\max_{1 \le i \le k} p_i\right)$$

Min-энтропия используется как мера непредсказуемости значений случайных последовательностей. Min-энтропия исходной СП определяет предельное количество случайных битов, которое можно из нее извлечь. Имея строку из n битов «сырой» СП min-энтропией k, из нее можно извлечь самое большее k случайных битов, близких к равномерно распределенным.

Оценка количества энтропии проводилась по значению min-энтропии/бит. Расчет значения min-энтропии выполнялся с помощью набора тестов, описанных в NIST 800-90B.

Существуют различные методики тестирования генераторов псевдослучайных последовательностей, но, так или иначе, все они базируются на проверке некоторых гипотез относительно свойств ПСП, производимых генераторами. В качестве статистической гипотезы использовалось предположение, что тестируемая ПСП истинно случайная. Истинность или ложность такого предположения подтверждается или отклоняется с помощью методов математической статистики. Проверка статистических свойств полученных псевдослучайных последовательностей осуществлялась с помощь тестов NIST STS 800-22. Для получения статистически значимых результатов тестирование проводилось с различ-

Таблица 1

Характеристики выходных псевдослучайных последовательностей модифицированного алгоритма ГОСТ Р 34.12-15

Длина ПСП, биты	**2^{24}**	**2^{26}**	**2^{28}**	**2^{30}**
Критерий Пирсона	202-274	237-275	228-300	219-311
Min-энтропия	0.89-0.92	0.89-0.925	0.895-0.925	0.89-0.925
SP800-22, α=0.01	0.88%	0.46%	0.18%	0.025%
SP800-22, α=0.001	0.13%	0.11%	0.08%	0.00%

Таблица 2

Характеристики выходных псевдослучайных последовательностей эталонного алгоритма ГОСТ Р 34.12-15

Длина ПСП, биты	**2^{24}**	**2^{26}**	**2^{28}**	**2^{30}**
Критерий Пирсона	229-275	223-292	218-315	218-293
Min-энтропия	0.885-0.925	0.9-0.925	0.885-0.925	0.885-0.915
SP800-22, α=0.01	0.85%	0.51%	0.13%	0.038%
SP800-22, α=0.001	0.22%	0.13%	0.05%	0.00%

Таблица 3

Характеристики выходных псевдослучайных последовательностей модифицированного алгоритма ГОСТ Р 34.12-15 в зависимости от числа раундов

Количество раундов	**6**	**10**	**14**	**18**
Критерий Пирсона	215-277	211-315	220-285	208-304
Min-энтропия	0.885-0.925	0.88-0.925	0.88-0.95	0.89-0.92
SP800-22, α=0.01	0.49%	0.51%	0.46%	0.44%
SP800-22, α=0.001	0.15%	0.13%	0.12%	0.13%

ными размерами выборки, уровнями значимости (α) и большим количеством ключей разных типов.

Численный эксперимент

Оценка качества выходных псевдослучайных последовательностей модифицированного алгоритма ГОСТ Р 34.12-15 «Кузнечик» осуществлялась по 3 характеристикам, перечисленным выше. Для этого с помощью описанной функции генерации генерировались последовательности длиной l по 217, 219, 221 и 223 128-битных блоков. Количество последовательностей составляло 4000. Для тестов NIST STS SP800-22 генерировались последовательности размером 100× l и 1000× l. Результаты численного эксперимента приведены в табл. 1. Для пунктов 1 и 2 приведены диапазоны соответствующих значений. Строки 3-4 содержат доли последовательностей, для которых прохождение тестов не было полностью успешным, для двух уровней значимости.

Для сравнения те же самые исследования были повторены для генератора на базе алгоритма исходного шифра ГОСТ Р 34.12-15 «Кузнечик», примененного в качестве CTR-ГПСП в соответствии с рекомендациями NIST SP800-90A для тех же самых длин последовательностей. Результаты прохождения тестов приведены в табл. 2.

Результаты тестирования показали малое количество не пройденных тестов при выборке m=100 по отношению к общему количеству тестируемых последовательностей и не выявили каких-либо закономерностей не прохождения отдельных тестов.

Сравнение соответствующих характеристик для каждой длины последовательности показывает сопоставимость полученных результатов для двух генераторов, что говорит о работоспособности предложенной схемы функции генерации псевдослучайных последовательностей. Отдельные отклонения, имеющие место при расчете критерия Пирсона и в результатах прохождения тестов NIST STS встречаются в ничтожно малом количестве. Их анализ не выявил каких-либо закономерностей не прохождения отдельных тестов. Это дает основание предположить, что выявленные отклонения носят случайный характер и могут быть интерпретированы как статистические аномалии.

В табл. 3 приведены результаты исследования предложенной функции генерации ПСП (модифицированного алгоритма) при разных количествах используемых раундов при шифровании. Исследования были проведены для 6, 10, 14, 18 раундов шифрования. Длина генерируемых последовательностей $l=2^{19}$ 128-битных блоков – такая же, как и рекомендованная для шифра AES.

Результаты исследования продемонстрировали близость исследуемых характеристик псевдослучайных последовательностей при использовании разного количества раундов в одном цикле генерации 128-битного блока выходной последовательности, что говорит о возможности гибкого построения процесса генерации в зависимости от того, что является приоритетом – секретность или скорость.

Выводы

Изложенный в статье подход к построению механизма ГПСП использует особенности выбранного криптоалгоритма ГОСТ Р 34.12-2015 «Кузнечик», которые позволяют повысить эффективность генерации псевдослучайных последовательностей за счет ряда модификаций. Наличие в алгоритме сети Фейстеля дает возможность организовать формирование раундовых ключей таким образом, чтобы в памяти одновременно хранились только два из них вместо предусмотренных десяти. В результате время существования ключей в памяти сокращается, что приводит к повышению криптостойкости генератора. Сеть Фейстеля также позволяет гибко настраивать число раундов в зависимости от конкретных потребностей. Такое варьирование числа раундов позволяет по мере надобности либо повышать секретность выходных данных, либо увеличивать скорость их получения. Предложено включить в состав 128-битных констант C_i двух параллельных счетчиков (счетчика запросов и счетчика итераций сети Фейстеля) для обеспечения уникальности раундовых ключей. Связанное с этим некоторое снижение скорости работы алгоритма может быть компенсировано путем замены трудоемких операций умножения в поле Галуа на выбор значений из заранее вычисленных таблиц подстановки. Предложенная организация работы функции генерации псевдослучайных последовательностей позволяет использовать алгоритм блочного шифрования «Кузнечик» в особом режиме поточного шифрования, объединяющем преимущества режимов OFB и CTR.

Проведенная оценка работы ГПСП по трем характеристикам выходных последовательностей, а именно – статистика критерия Пирсона χ^2 min-энтропия, а также истинность статистической гипотезы о случайном характере последовательностей, показала, что исследуемые характеристики выходных последовательностей предложенного генератора и эталонного варианта генератора на основе ГОСТ Р 34.12-2015 «Кузнечик» (CTR-ГПСП) близки между собой. При этом предложенный генератор обладает более высоким уровнем непредсказуемости выходных блоков генерируемых последовательностей.

Литература

1. Herrero-Collantes M., Garcia-Escartin J.C. Quantum random number generators // Review of Modern Physics. 2016. Vol. 89 (1). P. 1–54.
2. Fischer V., Haddad P. Random number generators for cryptography // Circuits and Systems for Security and Privacy. CRC Press. 2016. P. 245–286.
3. 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.

DOI:10.21681/2311-3456-2021-4-25-34

4. Johnston D. Random number generators – principles and practices. A guide for engineers and programmers. DeG Press, 2018. 436 p.
5. Wassenberg J., Obryk R., Alakuijala J., Mogenet E. Randen-fast backtracking-resistant random generator with AES+ Feistel+ Reverie // arXiv preprint arXiv:1810.02227, 2018.
6. Смагин А.А., Клочков А.Е., Григорьев А.Ю. Исследование возможности использования датчиков мобильных устройств для генерации случайных последовательностей. // Автоматизация процессов управления. 2017. № 3. С. 103–109.
7. Song P., Zeng Y., Liu Z., Ma J., Liu H. True Random Number Generation Using Process Scheduling of Android Systems. In Proc. of International Conference on Networking and Network Applications (Xi'an, China, October 12-15, 2018). NaNA'2018. P. 304–309. DOI: 10.1109/NANA.2018.8648763.
8. Cho S.-M., Hong E., Seo S.-H. Random number generator using sensor for drones // Computer Science. IEEE Access. 2020. Vol. 8. P. 30343–30354. DOI:10.1109/ACCESS.2020.2972958.
9. Camara C., Martin H., Peris-Lopez P., Aldalaien M. Design and analysis of a true random number generator based on gsr signals for body sensor networks // Sensors. 2019. Vol. 19. P. 2033.
10. Гончаренко Ю.Ю., Нестеренко В.Р. Использование случайных биометрических образов для генерации криптостойких последовательностей с применением генеративносостязательных нейронных сетей // Научный результат. Информационные технологии. Т. 4. № 2. 2019. С. 69–74. DOI: 10.18413/2518-1092-2019-4-2-0-8.
11. Parker R.J. Entropy justification for metastability based NRB generator // IEEE 2nd International Verification and Security Workshop (IVSW), 2017. DOI: 10.1109/IVSW.2017.8031540.
12. Chugunkov I.V., Novikova O.Y., Perevozchikov V.A., Troitskiy S.S. The development and researching of lightweight pseudorandom number generators. In Proc. of IEEE NORTH WEST RUSSIA Section Young Researchers in Electrical and Electronic Engineering Conf. (St. Petersburg, Russia, February 2-3, 2016). EICONRUSNW'2016. P. 185-189. DOI: 10.1109/EIConRusNW.2016.7448150.
13. Chugunkov I.V., Ivanov M.A., Gridneva E.A., Shestakova N.Y. Classification of pseudo-random number generators applied to information security. In Proc. of IEEE NORTH WEST RUSSIA Section Young Researchers in Electrical and Electronic Engineering Conf. (St. Petersburg, Russia, February 2-3, 2017). EICONRUSNW-2017. P. 370–373. DOI: 10.1109/EIConRus.2017.7910569.
14. Chugunkov I.V., Bitkina M.A., Rumyantseva I.S., F.A. Trofimov. The entropy assessment of modern stochastic algorithms. In Proc. of IEEE NORTH WEST RUSSIA Section Young Researchers in Electrical and Electronic Engineering Conf. (St. Petersburg, Russia, February 2-3, 2017). EICONRUSNW-2017. P. 366–369. DOI: 10.1109/EIConRus.2017.7910568.
15. Chugunkov Ilya V., Gulyaev Vadim A., Baranova Elena A., Chugunkov Vladimir I. Method for Improving the Statistical Properties of Pseudo-random Number Generators. In Proc. of IEEE NORTH WEST RUSSIA Section Young Researchers in Electrical and Electronic Engineering Conf. (St. Petersburg, Russia, January 28, 2019). EICONRUSNW-2017. P. 206–209. DOI: 10.1109/EIConRus.2019.8656699.
16. Zhu S., Ma Y., Jing J. Analysis and improvement of entropy estimators in NIST SP 800-90B for non-IID entropy sources // IACR Trans. Symmetric Cryptol. 2017. Vol. 2017 (3). P. 151–168. DOI:10.13154/tosc.v2017.i3.151-168.
17. Ishchukova E.A., Babenko L.K., Anikeev M.V. Fast implementation and cryptanalysis of GOST R 34.12-2015 block ciphers. In Proc. of 9th Int. Conf. on Security of Information and Networks. (New Jersey, USA, July 20-22, 2016). SIN'2016. P. 104–111. DOI:10.1145/2947626.2947657.
18. Babenko L.K., E.A. Ishchukova. New results in a research of GOST R 34.12-2015. In Proc. of IEEE 11th Int. Conf. on Application of Information and Communication Technologies. (Moscow, Russia, September 20-22, 2017). AICT'2017. P. 8686920. DOI: 10.1109/ICAICT.2017.8686920.
19. Burov D.A., Pogorelov B.A. The influence of linear mapping reducibility on the choice of round constants // Mat. Vopr. Kriptogr. 2017. Vol. 8 (2). P. 51–64. DOI: https://doi.org/10.4213/mvk223.
20. Удальцов В.А. Исследование влияния сокращения количества раундов криптографических преобразований на устойчивость к статистическим атакам и производительность алгоритма шифрования «Кузнечик» // Сб. материалов V Междунар. научно-практич. конф. Актуальные направления научных исследований: перспективы развития. 2018. С. 183–185. DOI 10.21661/r-471085.21.
21. Дорохин С.В., Качков С.С., Сидоренко А.А. Реализация блочного шифра «Кузнечик» с использованием векторных инструкций // Труды МФТИ. 2018. Т. 10. № 4. С. 45–53.

DEVELOPMENT OF A PSEUDO-RANDOM SEQUENCE GENERATION FUNCTION BASED ON THE "KUZNECHIK" CRYPTOGRAPHIC ALGORITHM

Belyaev S.[6], Budko M.[7], Budko M.[8] , Guirik A.[9], Grozov V.[10]

Purpose: *increasing the cryptographic strength level of the pseudo-random sequence generation function based on the «Kuznechik» encryption algorithm.*

Research methods: methods for constructing pseudo-random sequence generators using a strong cryptographic algorithm as a generation function in accordance with the recommendations of NIST SP 800-90. Methods of probability theory and mathematical statistics (statistical hypothesis testing, Pearson's criterion), methods for estimating the entropy of a random process.

Results: *a method for development of the main component of the deterministic generator – the function for generating pseudo-random sequences based on the «Kuznechik» encryption algorithm (Russian encryption standard GOST R 34.12-2015) due to a number of the original algorithm modifications is proposed. Features of the algorithm allow to use it in a mode that combines the advantages of the well-known encryption modes of block ciphers (OFB and CTR encryption modes). A procedure for generating round keys and other modifications of the algorithm that increase its security while maintaining its performance have been developed and implemented. The generator operation was evaluated on the basis of the statistical properties of the output sequences (NIST SP 800-22 tests), Pearson's χ2 criterion, and min-entropy (NIST 800-90B tests). According to the characteristics mentioned above, the proposed generation function is comparable with the reference version based on GOST 34.12-2015 «Kuznechik», but exceeds it in terms of security.*

Keywords: *random bit generator, pseudo-random sequences, GOST R 34.12-2015 «Kuznechik», SP-network, Feistel network, Pearson's criterion, min-entropy, NIST 800-90, NIST SP 800-22.*

References

1. Herrero-Collantes M., Garcia-Escartin J.C. Quantum random number generators // Review of Modern Physics. 2016. Vol. 89 (1). P. 1-54.
2. Fischer V., Haddad P. Random number generators for cryptography // Circuits and Systems for Security and Privacy. CRC Press. 2016. P. 245-286.
3. Ivanov M.A., Skitev A.A., Starikovskij A.V. Klassifikaciya generatorov psevdosluchajnyh chisel, orientirovannyh na reshenie zadach zashchity informacii // REDS: Telekommunikacionnye ustrojstva i sistemy [Telecommunications devices and systems], 2017, № 7 (4). S. 484-487.
4. Johnston D. Random number generators – principles and practices. A guide for engineers and programmers. DeG Press, 2018. 436 p.
5. Wassenberg J., Obryk R., Alakuijala J., Mogenet E. Randen-fast backtracking-resistant random generator with AES+ Feistel+ Reverie // arXiv preprint arXiv:1810.02227, 2018.
6. Smagin A.A., Klochkov A.E., Grigor'ev A.Yu. Issledovanie vozmozhnosti ispol'zovaniya datchikov mobil'nyh ustrojstv dlya generacii sluchajnyh posledovatel'nostej // Avtomatizaciya processov upravleniya [Automation of control processes], 2017. № 3. S. 103-109.
7. Song P., Zeng Y., Liu Z., Ma J., Liu H. True Random Number Generation Using Process Scheduling of Android Systems. In Proc. of International Conference on Networking and Network Applications (Xi'an, China, October 12-15, 2018). NaNA'2018. P. 304-309. DOI: 10.1109/NANA.2018.8648763.
8. Cho S.-M., Hong E., Seo S.-H. Random number generator using sensor for drones // Computer Science. IEEE Access. 2020. Vol. 8. P. 30343-30354. DOI:10.1109/ACCESS.2020.2972958.
9. Camara C., Martin H., Peris-Lopez P., Aldalaien M. Design and analysis of a true random number generator based on GSR signals for body sensor networks // Sensors. 2019. Vol. 19. P. 2033.
10. Goncharenko J.J. Nesterenko V.R. Ispol'zovanie sluchajnyh biometricheskih obrazov dlya generacii kriptostojkih posledovatel'nostej s primeneniem generativnosostyazatel'nyh nejronnyh setej // Nauchnyj rezul'tat. Informacionnye tekhnologii. T. 4. № 2. 2019. S. 69-74. DOI: 10.18413/2518-1092-2019-4-2-0-8.

6 Sergey Belyaev, Assistant, ITMO University, Saint-Petersburg, Russia. E-mail: ssbelyaev@itmo.ru, ORCID 0000-0001-6411-1154

7 Marina Budko, Ph. D., Asociate professor, ITMO University, Saint-Petersburg, Russia. E-mail: mbbudko@corp.ifmo.ru, ORCID 0000-0001-7054-5709

8 Mikhail Budko, Ph. D., Asociate professor, ITMO University, Saint-Petersburg, Russia. E-mail: mbudko@corp.ifmo.ru, OCRID 0000-0002-1444-277X

9 Alexei Guirik, Ph. D., Asociate professor, ITMO University, Saint-Petersburg, Russia. E-mail: avg@corp.ifmo.ru, ORCID 0000-0002-4021-7605

10 Vladimir Grozov, postgraduate student, ITMO University, Saint-Petersburg, Russia. E-mail: vagrozov@corp.ifmo.ru, ORCID 0000-0002-7998-8175

11. Parker R.J. Entropy justification for metastability based NRB generator // IEEE 2nd International Verification and Security Workshop (IVSW), 2017. DOI: 10.1109/IVSW.2017.8031540.
12. Chugunkov I.V., Novikova O.Y., Perevozchikov V.A., Troitskiy S.S. The development and researching of lightweight pseudorandom number generators. In Proc. of IEEE NORTH WEST RUSSIA Section Young Researchers in Electrical and Electronic Engineering Conf. (St. Petersburg, Russia, February 2-3, 2016). EICONRUSNW'2016. P. 185-189. DOI: 10.1109/EIConRusNW.2016.7448150.
13. Chugunkov I.V., Ivanov M.A., Gridneva E.A., Shestakova N.Y. Classification of pseudo-random number generators applied to information security. In Proc. of IEEE NORTH WEST RUSSIA Section Young Researchers in Electrical and Electronic Engineering Conf. (St. Petersburg, Russia, February 2-3, 2017). EICONRUSNW-2017. P. 370-373. DOI: 10.1109/EIConRus.2017.7910569.
14. Chugunkov I.V., Bitkina M.A., Rumyantseva I.S., F.A. Trofimov. The entropy assessment of modern stochastic algorithms. In Proc. of IEEE NORTH WEST RUSSIA Section Young Researchers in Electrical and Electronic Engineering Conf. (St. Petersburg, Russia, February 2-3, 2017). EICONRUSNW-2017. P. 366-369. DOI: 10.1109/EIConRus.2017.7910568.
15. Chugunkov Ilya V., Gulyaev Vadim A., Baranova Elena A., Chugunkov Vladimir I. Method for Improving the Statistical Properties of Pseudo-random Number Generators. In Proc. of IEEE NORTH WEST RUSSIA Section Young Researchers in Electrical and Electronic Engineering Conf. (St. Petersburg, Russia, January 28, 2019). EICONRUSNW-2017. P. 206-209. DOI: 10.1109/EIConRus.2019.8656699.
16. Zhu S., Ma Y., Jing J. Analysis and improvement of entropy estimators in NIST SP 800-90B for non-IID entropy sources // IACR Trans. Symmetric Cryptol. 2017. Vol. 2017 (3). P. 151-168. DOI:10.13154/tosc.v2017.i3.151-168.
17. Ishchukova E.A., Babenko L.K., Anikeev M.V. Fast implementation and cryptanalysis of GOST R 34.12-2015 block ciphers. In Proc. of 9th Int. Conf. on Security of Information and Networks. (New Jersey, USA, July 20-22, 2016). SIN'2016. P. 104-111. DOI:10.1145/2947626.2947657.
18. Babenko L.K., E.A. Ishchukova. New results in a research of GOST R 34.12-2015. In Proc. of IEEE 11th Int. Conf. on Application of Information and Communication Technologies. (Moscow, Russia, September 20-22, 2017). AICT'2017. P. 8686920. DOI: 10.1109/ICAICT.2017.8686920.
19. Burov D.A., Pogorelov B.A. The influence of linear mapping reducibility on the choice of round constants // Mat. Vopr. Kriptogr. 2017. Vol. 8 (2). P. 51-64. DOI: https://doi.org/10.4213/mvk223.
20. Udaltsov V.A. Issledovanie vliyaniya sokrashcheniya kolichestva raundov kriptograficheskih preobrazovanij na ustojchivost' k statisticheskim atakam i proizvoditel'nost' algoritma shifrovaniya «Kuznechik» // Sb. materialov V Mezhdunar. nauchno-praktich. konf. Aktual'nye napravleniya nauchnyh issledovanij: perspektivy razvitiya. 2018. S. 183-185. DOI 10.21661/r-471085.
21. Dorokhin S.V., Kachkov S.S., Sidorenko A.A. Realizaciya blochnogo shifra «Kuznechik» s ispol'zovaniem vektornyh instrukcij // Trudy MFTI. 2018. T. 10. № 4. S. 45-53.