УДК 004.056.55
DOI 10.21685/2587-7704-2018-3-2-5

Open Access | RESEARCH ARTICLE

Способы построения генераторов псевдослучайных последовательностей

Д. В. Солдатенков
Пензенский государственный университет, Россия, 440026 г. Пенза, ул. Красная, 40

О. В. Липилин
Пензенский государственный университет, Россия, 440026 г. Пенза, ул. Красная, 40

Аннотация. В соответствии с образовательным стандартом при освоении компетенции ПК-7 студенты должны знать основные задачи и понятия криптографических методов защиты информации; основные криптографические методы защиты информации; требования к шифрам и основные характеристики шифров, а также получить навыки по использованию типовых криптографических преобразований. В связи с этим в данной работе изучаются способы построения генераторов псевдослучайных последовательностей на базе регистров сдвига с линейной обратной связью [1], в режиме счетчика, описанного в ГОСТ 34.13-2015 [2], а также рассматривается алгоритм Блюм-Блюм-Шуба [3], основанный на сложности факторизации больших чисел.

Ключевые слова: генераторы псевдослучайных последовательностей, поточные шифры, блочные шифры, криптостойкость, бент-функции, нелинейность функции, сбалансированные функции, корреляционный иммунитет.

Methods for designing pseudorandom sequence generators

D. V. Soldatenkov
Penza State University, 40 Krasnaya Street, 440026, Penza, Russia

O. V. Lipilin
Penza State University, 40 Krasnaya Street, 440026, Penza, Russia

Abstract. In accordance with the educational standard in mastering the PC-7 competence, students should know the main tasks and concepts of cryptographic methods for protecting information; basic cryptographic methods for protecting information; requirements for ciphers and basic characteristics of ciphers, as well as gain skills in using typical cryptographic transformations. In this regard, this paper presents methods for designing pseudorandom sequence generators based on linear feedback shift register [1] in the counter mode, described in GOST 34.13-2015 [2], and the Blum-Blum-Shub algorithm [3], based on the complexity of factoring large numbers.

Keywords: pseudorandom sequence generators, stream ciphers, block ciphers, cryptostrength, bent functions, nonlinear function, balanced function, correlation immunity.

1. Регистры сдвига с линейной обратной связью m

Регистры сдвига с линейной обратной связью широко применяются при построении поточных шифров, однако их нельзя напрямую использовать для шифрования, поскольку вырабатываемая последовательность является предсказуемой. Поэтому в криптографических приложениях используются методы усложнения последовательностей. Известны следующие методы усложнения [1]:

– фильтрующие генераторы;
– комбинирующие генераторы;
– композиция линейных регистров;
– схемы с динамическим изменением закона рекурсии;
– схемы с элементами памяти.

Далее рассмотрены фильтрующие генераторы, которые строятся на основе регистров сдвига с линейной обратной связью, к элементам вырабатываемой последовательности применяется некоторая функция *f*, называемая фильтрующей функцией. Структурная схема фильтрующего генератора приведена на рис. 1. Фильтрующая функция должна иметь высокую степень нелинейной и быть сбалансированной.

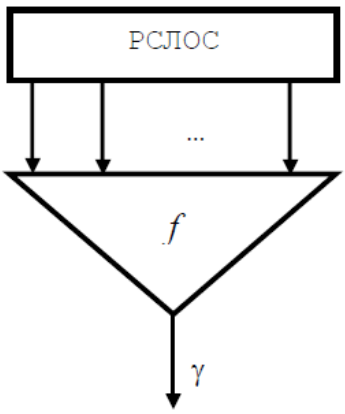

Рис. 1. Структурная схема фильтрующего генератора

При построении фильтрующих генераторов рассматриваются несколько вариантов выбора фильтрующих функций. Бент-функции, обладающие максимальной нелинейностью, не являются сбалансированными. На основе бент-функции можно построить сбалансированную функцию, однако ее применение в качестве фильтрующей функции также нежелательно. Оба вида функций не обладают корреляционным иммунитетом, что делает возможным реализацию корреляционной атаки на фильтрующий генератор псевдослучайной последовательности. В качестве фильтрующей функции необходимо использовать сбалансированную корреляционно-иммунную функцию [2].

Функция $f: F_2^n \to F^2$ называется корреляционно-иммунной порядка для $1 \le m < n$ и обладает порядком корреляционного иммунитета $cim(f) = m$, если при любом векторе a, $1 \le |a| \le m$, функция $f(x) + (a, x)$ является сбалансированной. Если f сбалансирована и $cim(f) = m$, тогда функция f называется устойчивой или m-эластичной.

Дальнейшее усиление корреляционно-иммунных свойств функций связано с требованиями корреляционной иммунности подфункций, полученных фиксациями части ее переменных.

Достаточным условием корреляционной иммунности порядка m функций f является сбалансированность любой ее подфункции, полученной фиксацией произвольными константами любых m переменных. Другими словами, при случайном равновероятном выборе $x \in F_2^n$ и любых фиксированных $a_1, \ldots, a_m \in F_2^m$ выполняется равенство

$$P\left\{ f(x) = 1 | x_{j_1} = a_1, \ldots, x_{j_m} = a_m \right\} = \frac{1}{2},$$

где $j_1, \ldots, j_m \in \{1, \ldots, n\}, 1 \le j_1 < \ldots < j_m \le n$.

Использование таких функций в качестве функций выхода в комбинирующих или фильтрующих генераторах позволяет обеспечить стойкость к некоторым методам корреляционного криптоанализа [3].

2. Режим гаммирования

Параметром режима гаммирования по ГОСТ 34.13-2015 [4] является целочисленная величина s, $0 < s \le n$, где n – параметр алгоритма блочного шифрования, называемый длиной блока. При использовании режима гаммирования не требуется применение процедуры дополнения сообщения.

Для зашифрования и расшифрования каждого отдельного открытого текста на одном ключе используется значение уникальной синхропосылки $IV \in V_{n/2}$.

Зашифрование в режиме гаммирования заключается в покомпонентном сложении открытого текста с гаммой шифра, которая вырабатывается блоками длины s путем зашифрования последовательности значений счетчика $CTR_i \in V_n, i = 1,2,\ldots,n$, базовым алгоритмом блочного шифрования с последующим усечением. Начальным значением счетчика является $CTR_i = I_n(IV) = IV \| 0^{\frac{n}{2}}$. Последующие значения счетчика вырабатываются с помощью функции $Add : V_n \to V_n$ следующим образом:

$$CTR_{i+1} = Add(CTR_i) = Vec_n(Int_n(CTR_i) \boxplus_n 1).$$

3. Алгоритм Блюм-Блюм-Шуба

Алгоритм Блюм-Блюм-Шуба [5] основан на сложности решения задачи факторизации больших чисел. Алгоритм генерирует последовательность псевдослучайных бит и состоит из следующих шагов:

а) сгенерировать два больших простых числа p и q, таких, что $p = q = 3 mod 4$, это гарантирует, что каждый квадратичный вычет имеет один квадратный корень, который также является квадратичным вычетом, и наибольший общий делитель $НОД(\varphi(p-1), \varphi(q-1))$ должен быть мал, что способствует увеличению длины цикла;

б) вычислить $M = p \cdot q$;

в) взять большое число x_0, взаимно простое с M;

г) на каждом шаге генерации последовательности вычисляется число $x_{i+1} = x_i^2 \mod M$;

д) в качестве результата берется либо бит четности, либо один или несколько наименее значимых бит x_i.

На сегодняшний день этот алгоритм является, пожалуй, наиболее надежным ГПСЧ. Для вскрытия начального состояния или угадывания следующего элемента псевдослучайной последовательности атакующий должен знать числа p и q [6].

У генератора, основанного на алгоритме Блюм-Блюм-Шуба, есть недостаток – это крайне низкая скорость. С целью увеличения производительности на каждом шаге генерации можно возвращать вместо одного $log(log M)$ бит, что позволит увеличить скорость, не снижая криптостойкости.

Библиографический список

1. Основы криптографии : учеб. пособие / А. П. Алферов, А. Ю. Зубов, А. С. Кузьмин, А. В. Черемушкин. – Москва : Гелиос АРВ, 2005. – 480 с.
2. Андерсон, О. Р. Поточные шифры. Результаты зарубежной открытой криптологии / О. Р. Андерсон. – Москва, 1997. – 389 с.
3. Лось, А. Б. Криптографические методы защиты информации : учебник для академического бакалавриата / А. Б. Лось, А. Ю. Нестеренко, М. И. Рожков. – 2-е изд., испр. – Москва : Юрайт, 2018.
4. ГОСТ Р 34.13-2015. Информационная технология. Криптографическая защита информации. Режимы работы блочных шифров. – Москва : Стандартинформ, 2015.
5. Алгоритм Блюм-Блюм-Шуба. – URL: https://ru.wikipedia.org/wiki/%D0%90%D0%BB%D0%B3%D0%BE%D1%80%D0%B8%D1%82%D0%BC_%D0%91%D0%BB%D1%8E%D0%BC_%E2%80%94_%D0%91%D0%BB%D1%8E%D0%BC%D0%B0_%E2%80%94_%D0%A8%D1%83%D0%B1%D0%B0 (дата обращения: 06.10.2018).
6. В поисках криптостойкого ГПСЧ. – URL: https://habr.com/post/196442/ (дата обращения: 06.10.2018).

Солдатенков, Д. В.
Способы построения генераторов псевдослучайных последовательностей / Д. В. Солдатенков, О. В. Липилин // Инжиниринг и технологии. – 2018. – Vol. 3(2). – DOI 10.21685/2587-7704-2018-3-2-5.