XXII ВСЕРОССИЙСКАЯ ШКОЛА–КОЛЛОКВИУМ ПО СТОХАСТИЧЕСКИМ МЕТОДАМ

Д. С. Богданов, **В. О. Миронкин** (Лаборатории ТВП, НИУ ВШЭ, Москва). **О коллизиях отображений, построенных на основе случайной подстановки.**

Введение. В последнее время в научной литературе все чаще появляются работы, связанные с разработкой новых методов генерации псевдослучайных последовательностей, основанных на базе низкоресурсных технологий, в частности, на использовании алгоритмов блочного шифрования. Интерес к данной проблематике объясняется, как минимум, двумя факторами: необходимостью применения методов генерации псевдослучайных последовательностей в мобильных устройствах и современной тенденцией упрощения программной и аппаратной реализаций соответствующих методов.

Так, например, в работе [3] предложена модель генерации псевдослучайных последовательностей, использующая результаты зашифрования и расшифрования некоторой служебной информации, а в работе [6] исследован ряд вероятностно-статистических свойств этой модели, определяющих возможность прохождения генерируемых последовательностей через пакеты статистических тестов, подобных NIST [5]. На рис. 1 изображена блок-схема генерации псевдослучайной последовательности $\overline{y} = y_1, \ldots, y_l$, $l \in \mathbb{N}$, на основе модели [3] с использованием алгоритма блочного шифрования $E_k : V_N \to V_N$, где k — произвольный ключ шифрования [1].

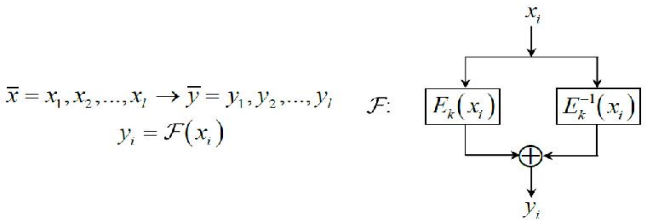

Рис. 1. Схема генерации элементов последовательности $\overline{y} = y_1, \ldots, y_l$

При этом в качестве служебной информации выступает некоторая последовательность $\overline{x} = x_1, \ldots, x_l$, где $x_i \in V_N$, $i = \overline{1,l}$, а каждый элемент y_i генерируемой последовательности $\overline{y}$ формируется по следующему закону:

$$y_i = \mathcal{F}(x_i) = E_k(x_i) \oplus E_k^{-1}(x_i), \quad i \in \overline{1,l},$$

где $\oplus$ — операция побитового сложения двоичных векторов (XOR), а $\mathcal{F}$ — интегральное преобразование.

Рассмотрим обобщение модели [6], где, помимо операции XOR, может быть использована операция $\boxplus$ — сложение в кольце $\mathbb{Z}_N$, $N = 2^n$, $n \in \mathbb{N}$.

1. Вероятность коллизии. Как было указано выше, модель [3] строится на основе блочного шифра, реализующего некоторое биективное отображение E_k, обладающее требуемыми вероятностно-статистическими и криптографическими качествами [1, 4]. Поэтому для описания свойств указанной модели в качестве отображения E_k (при случайном выборе ключа) будем рассматривать случайную равновероятную подстановку $\pi \in S_N$ и, соответственно, интегральное преобразование $\mathcal{F}'$:

$$\mathcal{F}'(x) = \pi(x) * \pi^{-1}(x), \tag{1}$$

где $* \in \{\oplus, \boxplus\}$.

Рассмотрим вероятностное пространство $(\Omega, \mathcal{F}, \mathbf{P})$, где пространство элементарных исходов $\Omega = \{\pi \in S_N\}$ — множество всех $N!$ подстановок на множестве V_N, алгебра событий $\mathcal{F}$ — множество всех подмножеств Ω, а вероятностная мера $\mathbf{P}$ является равновероятной:

$$\mathbf{P}\{\pi\} = \frac{1}{N!} \quad \text{для любой} \quad \pi \in \Omega. \tag{2}$$

Определение. Будем говорить, что элементы $x_i \neq x_j : x_i, x_j \in V_N$ образуют *коллизию* при отображении $\mathcal{F}'$, если выполняется равенство

$$\pi(x_i) * \pi^{-1}(x_i) = \pi(x_j) * \pi^{-1}(x_j).$$

Для произвольной подстановки $\pi \in \Omega$ и произвольных элементов $x_i, x_j \in V_N$ положим

$$p_\pi^{(*)}(x_i, x_j) = \mathbf{P}\left\{\pi(x_i) * \pi^{-1}(x_i) = \pi(x_j) * \pi^{-1}(x_j)\right\}.$$

Замечание. Значение вероятности $p_\pi^{(*)}(x_i, x_j)$ появления коллизии при отображении $\mathcal{F}'$ позволяет оценивать количество и длину серий одинаковых элементов в генерируемых последовательностях $\overline{y}$ (характеристики, используемые в NIST).

Оценим вероятность коллизий $p_\pi^{(*)}(x_i, x_j)$, возникающих при генерации элементов выходной последовательности в случаях использования операций XOR и сложения в кольце $\mathbb{Z}_N$.

Теорема 1. *Пусть случайная подстановка $\pi : V_N \to V_N$, $N = 2^n$, $n \geqslant 3$, имеет распределение (2) на Ω, и пусть операция $*$ из (1) совпадает с операцией $\boxplus$. Тогда для произвольных $x_i, x_j \in V_N$:*

$$p_\pi^{(\boxplus)}(x_i, x_j) = \begin{cases} \dfrac{2N^3 - 12N^2 - 14N + 167}{2N(N-1)(N-2)(N-3)}, & \text{если} \quad x_i - x_j = {}^N\!/_4,\ {}^{3N}\!/_4,\ 3k,\ N-6k, \\ & \quad k \text{ — нечетное}, \\ & \quad 3k,\ N-3k \notin \{{}^N\!/_4, {}^{3N}\!/_4, {}^N\!/_2\}, \\ \dfrac{2N^3 - 20N^2 + 20N + 35}{2N(N-1)(N-2)(N-3)}, & \text{если} \quad x_i - x_j = 6k,\ N-6k, \\ & \quad 6k,\ N-6k \notin \{{}^N\!/_4, {}^{3N}\!/_4, {}^N\!/_2\}, \\ \dfrac{N^3 - 7N^2 + 9N + 23}{N(N-1)(N-2)(N-3)}, & \text{если} \quad x_i - x_j = 2z,\ z \notin \{3k, N-3k, {}^N\!/_2\}, \\ \dfrac{N^3 - 7N^2 + 8N + 26}{N(N-1)(N-2)(N-3)}, & \text{если} \quad x_i - x_j = z,\ z \text{ — нечетное}, \\ & \quad z \notin \{3k, N-3k, {}^N\!/_2\}, \\ \dfrac{4N^3 - 19N^2 + 16N + 8}{4N(N-1)(N-2)(N-3)} & \text{если} \quad x_i - x_j = {}^N\!/_2. \end{cases}$$

Следствие 1. *Пусть случайная подстановка $\pi : V_N \to V_N$, $N = 2^n$, имеет распределение (2) на Ω, и пусть операция $*$ из (1) совпадает с операцией $\boxplus$. Тогда для произвольных $x_i, x_j \in V_N$ при $n \to \infty$ справедлива асимптотика $p_\pi^{(\boxplus)}(x_i, x_j) \to {}^1\!/_N$.*

Для случая использования в соотношении (1) операции XOR [6] справедлив следующий результат.

Теорема 2. *Пусть случайная подстановка $\pi : V_N \to V_N$, $N = 2^n$, $n \in \mathbb{N}$, имеет распределение (2) на Ω, и пусть операция $*$ из (1) совпадает с операцией $\oplus$. Тогда для произвольных $x_i, x_j \in V_N$ справедливо равенство*

$$p_\pi^{(\oplus)}(x_i, x_j) = \frac{N^2 - N - 4}{N(N-1)(N-3)}.$$

Следствие 2. *Пусть случайная подстановка* $\pi : V_N \to V_N$, $N = 2^n$, $n \in \mathbb{N}$, *имеет распределение* (2) *на* Ω, *и пусть операция* $*$ *из* (1) *совпадает с операцией* $\oplus$. *Тогда для произвольных* $x_i, x_j \in V_N$ *при* $n \to \infty$ *справедлива асимптотика* $p_\pi^{(\oplus)}(x_i, x_j) \to 1/N$.

Следует отметить, что предложенная в [3] модель описывает способ реализации случайного равновероятного отображения $f : V_N \to V_N$ [2] на основе алгоритма блочного шифрования. Однако для случайного равновероятного отображения f должно выполняться равенство $\mathbf{P}\{f(x_i) = f(x_j)\} = 1/N$. В свою очередь, результаты теорем 1 и 2 показывают, что для построенного отображения $\mathcal{F}'$ в общем случае это равенство не выполняется.

На рис. 2 изображен график поведения квадратичного отклонения величин $p_\pi^{(\oplus)}(x_i, x_j)$ и $1/N$ с ростом параметра N.

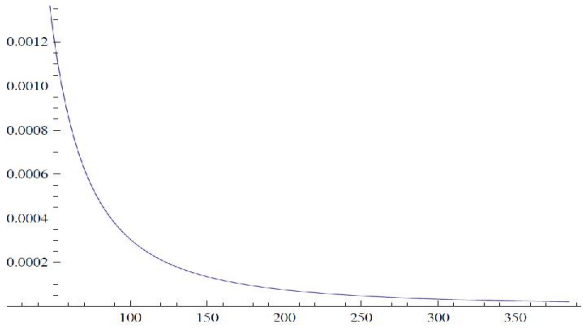

Рис. 2. Квадратичное отклонение величин $p_\pi^{(\oplus)}(x_i, x_j)$

Заключение. Ненулевые значения отклонений вероятности $p_\pi^{(*)}(x_i, x_j)$ от величины $1/N$, описанные в теоремах 1 и 2, позволяют получить ряд интегральных характеристик модели [3], например таких, как математическое ожидание числа одинаковых элементов в генерируемой последовательности $\overline{y}$, отличающиеся от тех же характеристик, соответствующих случайному равновероятному отображению. В связи с чем становятся актуальными задачи построения статистических критериев, позволяющих отличить последовательности, генерируемые с помощью модели [3], от псевдослучайных последовательностей.

СПИСОК ЛИТЕРАТУРЫ

1. *Алферов А. П.*, *Зубов А. Ю.*, *Кузьмин А. С.*, *Черемушкин А. В.* Основы криптографии. М.: Гелиос АРВ, 2002.
2. *Колчин В. Ф.* Случайные отображения. М.: Наука, 1984.
3. *Лавриков И. В.*, *Рудской В. И.* О возможных подходах к построению механизмов выработки производных ключей и механизмов выработки псевдослучайных последовательностей. В сб.: XVIII научно-практическая конференция «РусКрипто'2016». (22 – 25 марта 2016 г., Смирновское–Дулепово.) РусКрипто, 2016.
4. *Шнайер Б.* Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке СИ. М.: Триумф, 2002, 816 с.
5. NIST. A statistical test suite for random and pseudorandom number generators for cryptographic application. Special publication 2010, 800–22.
6. *Urivskiy A.*, *Rybkin A.*, *Borodin M.* On some properties of PRNGs based on block ciphers in counter mode. — Electron. Notes Discrete Math., 2017, v. 57 p. 211–218.