ВЕРОЯТНОСТНЫЕ СВОЙСТВА САМОСЖИМАЮЩЕГОСЯ ГЕНЕРАТОРА

Храмова Е.В., БГУ, Минск

1. Описание самосжимающегося генератора.

В работе [1] был предложен самосжимающийся генератор. В дальнейшем будем рассматривать самосжимающийся генератор, который использует линейный регистр сдвига ($LFSR_A$) длины $|A|$. Выходная последовательность z самосжимающегося генератора определятся на основе выходной последовательности $LFSR_A$ $a=(a_1,a_2,\ldots)$ следующим образом:

1) последовательность a разбивается на группы из двух элементов:

$$a=(a_1,a_2,\ldots)=((a_1,a_2),(a_3,a_4),\ldots);$$

2) вычисляются элементы выходной последовательности z:

$$z_{j(i)}=\begin{cases}a_{2i}, \text{ если } a_{2i-1}=1,\\ \text{не вычисляется, если } a_{2i-1}=0,\end{cases}$$

где $i=1,2,\ldots,$

$$j(i)=\begin{cases}j(i-1)+1, \text{если } a_{2i-1}=1,\\ j(i-1), \text{если } a_{2i-1}=0,\end{cases} \qquad j(0)=0.$$

2. Вероятностные свойства самосжимающегося генератора.

Из работы [1] известно, что выходную последовательность самосжимающегося генератора можно рассматривать как выходную последовательность некоторого сжимающегося генератора. Поэтому для исследования вероятностных свойств самосжимающегося генератора будем использовать подход, предложенный в [2] для изучения вероятностных свойств сжимающегося генератора.

Найдем оценку отклонения момента k-ого порядка суммы n значений выходной последовательности самосжимающегося генератора от момента k-ого порядка суммы n значений бинарной равномерно распределенной случайной последовательности.

Теорема 1. *Пусть z – последовательность, порождаемая самосжимающимся генератором. И пусть $n|A|\le 2^{|A|}$, $Z=\sum_{i=1}^{n} z_i$ и $Y=\sum_{i=1}^{n} y_i$, где y_i – незави-*

симые случайные величины Бернулли со следующим распределением вероятностей: $P\{y_i=1\}=\frac{1}{2}$; $P\{y_i=0\}=\frac{1}{2}$. *Если* $Z<\frac{n^2}{2^{|A|}}$, *то справедливы следующие оценки:*

$$|D\{Z\}-D\{Y\}|\le\frac{n^3+n^2}{2^{|A|}},\ |E\{Z^k\}-E\{Y_i^k\}|\le\frac{n^k}{2^{|A|}}. \quad (1)$$

Доказательство. Выходную последовательность $z=(z_1,z_2,\ldots)$ самосжимающегося генератора можно получить с помощью следующего сжимающегося генератора. В качестве управляющей последовательности s' сжимающегося генератора возьмем элементы выходной последовательности $LFSR_A$ с нечетными номерами: $s'=(a_1,a_3,\ldots)=(s'_1,s'_2,\ldots)$, а в качестве управляемой последовательности сжимающегося генератора возьмем элементы выходной последовательности $LFSR_A$ с четными номерами: $a'=(a_2,a_4,\ldots)=(a'_1,a'_2,\ldots)$. Тогда элементы выходной последовательности самосжимающегося генератора можно записать в следующем виде: $z_j=a'_{i_j(s')}$, $j=\overline{1,n}$, где $i_j(s')$ – номер j-ой "1" в управляющей последовательности s'. Поэтому сумма n значений выходной последовательности представима в виде: $Z=\sum_{j=1}^{n}z_j=\sum_{j=1}^{n}a'_{i_j(s')}$. Т.к. $n|A|\le 2^{|A|}$, то $i_j(s')\le 2^{|A|}-1$. Тогда, применяя результаты работы [2] для последовательности a', получим справедливость оценок (1). ■

Аналогично [2] будем рассматривать шаблон $template_B(a)$ такой, что для $\forall B\in\{0,1,*\}^n$, $B=(B(1),\ldots,B(n))$:

$$template_B(a)=\begin{cases}1, & \text{если } a_i=B(i),\ \forall B(i)\neq *,\\ 0, & \text{иначе,}\end{cases}\qquad \text{где } a=(a_1,\ldots,a_n).$$

Для математического ожидания шаблона $E\{template_B(Z)\}$ справедлива следующая оценка.

Теорема 2. *Пусть* z *– последовательность, порождаемая самосжимающимся генератором. И пусть* $Z_n=(z_1,\ldots,z_n)$ *и* $Y_n=(y_1,\ldots,y_n)$, *где* y_i *– незави-*

симые случайные величины Бернулли со следующим распределением вероятностей: $P\{y_i=1\}=\frac{1}{2}$, $P\{y_i=0\}=\frac{1}{2}$. *Тогда для* $\forall$ *шаблона* $B\in\{0,1,*\}^n$

$$|E\{template_B(Z_n)\}-E\{template_B(Y_n)\}|=O\left(\frac{n}{2^{|A|}}\right). \qquad (2)$$

Доказательство. Аналогично теореме 1 элементы выходной последовательности $z=(z_1,z_2,\ldots)$ самосжимающегося генератора можно записать в следующем виде: $z_j=a'_{i_j(s')}$, где $a'=(a_2,a_4,\ldots)=(a'_1,a'_2,\ldots)$ – управляемая последовательность; $i_j(s')$ – номер j-ой "1" в управляющей последовательности $s'=(a_1,a_3,\ldots)=(s'_1,s'_2,\ldots)$, $j=\overline{1,n}$. Определим $Z_n=(z_1,\ldots,z_n)=(a'_{i_1(s')},\ldots,a'_{i_n(s')})$, $A'_{i_n(s')}=(a'_1,\ldots,a'_{i_n(s')})$. Используя последовательность s', на основе шаблона B длины n создадим шаблон $B_{s'}$ длины $i_n(s')$ следующим образом. Если $s'_i=0$, то $B_{s'}(i)=*$, если $s'_i=1$, то $B_{s'}(i)=B(i)$. Тогда $template_B(Z_n)=template_{B_{s'}}(A'_{i_n(s')})$. Для доказательства теоремы оценим следующую сумму:

$$\sum_{s'}P\{s'\}\,|\,E\{template_{B_{s'}}(A'_{i_n(s')})\}-E\{template_B(Y_n)\}|.$$

Используя результаты работы [2], получим:

$$\sum_{s'}P\{s'\}\,|\,E\{template_{B_{s'}}(A'_{i_n(s')})\}-E\{template_B(Y_n)\}|\le\sum_{s'}P\{s'\}\cdot\frac{i_n(s')}{2^{|A|}}=\frac{E\{i_n(s')\}}{2^{|A|}}. \qquad (3)$$

Справедливость оценки (2) следует из (3) и следующего соотношения из [2]:

$$E\{i_n(s')\}=O(n).$$ ■

С помощью теоремы 2 получим следующие свойства выходной последовательности самосжимающегося генератора.

Следствие 1. *Пусть* z *– последовательность, порождаемая самосжимающимся генератором. Тогда корреляция между элементами последовательности* z_t *и* z_{t+l+1} *определяется следующим соотношением:*

$$corr(z_t,z_{t+l+1})=O\left(\frac{l}{2^{|A|}}\right),\ t+l+1\le 2^{|A|}-1.$$

Доказательство. Для доказательства следствия будем использовать шаб-

лон B длины $l+2$ следующего вида: $\sigma_1 \underbrace{*\ldots*}_{l} \sigma_2$, где $\sigma_1, \sigma_2 \in \{0,1\}$. И пусть $Z_{l+2} = (z_t, \ldots, z_{t+l+1})$ и $Y_{l+2} = (y_1, \ldots, y_{l+2})$, где y_i – независимые случайные величины Бернулли со следующим распределением вероятностей: $P\{y_i = 1\} = \frac{1}{2}$, $P\{y_i = 0\} = \frac{1}{2}$. Используя теорему 2, получим:

$$|E\{template_B(Z_{l+2})\} - E\{template_B(Y_{l+2})\}| =$$

$$= |P\{z_t = \sigma_1, z_{t+l+1} = \sigma_2\} - P\{y_1 = \sigma_1, y_{l+2} = \sigma_2\}| = |P\{z_t = \sigma_1, z_{t+l+1} = \sigma_2\} - \frac{1}{4}| = O\left(\frac{l}{2^{|A|}}\right).$$

Запишем формулу корреляции между z_t и z_{t+l+1} следующим образом:

$$corr(z_t, z_{t+l+1}) = 2P\{z_t = z_{t+l+1}\} - 1 =$$

$$= 2(P\{z_t = 0, z_{t+l+1} = 0\} + P\{z_t = 1, z_{t+l+1} = 1\}) - 1 = 2\left(\frac{1}{4} + \frac{1}{4} + O\left(\frac{l}{2^{|A|}}\right)\right) - 1 = O\left(\frac{l}{2^{|A|}}\right). \blacksquare$$

Следствие 2. *Пусть P – произвольная бинарная k-грамма. И пусть Z_k – k последовательных бит последовательности z, порождаемой самосжимающимся генератором. Тогда* $|P\{Z_k = P\} - 2^{-k}| = O\left(\frac{k}{2^{|A|}}\right)$.

Доказательство. Пусть $Y_k = (y_1, \ldots, y_k)$, где y_i – независимые случайные величины Бернулли со следующим распределением вероятностей: $P\{y_i = 1\} = \frac{1}{2}$, $P\{y_i = 0\} = \frac{1}{2}$. Так как произвольную бинарную k-грамму P можно рассматривать как шаблон $B = (\sigma_1, \ldots, \sigma_k)$ размера k, где $\sigma_i \in \{0,1\}$, из теоремы 2, получим: $|E\{template_B(Z_k)\} - E\{template_B(Y_k)\}| = |P\{Z_k = P\} - \frac{1}{2^k}| = O\left(\frac{k}{2^{|A|}}\right)$. $\blacksquare$

Литература. 1. Meier W., Staffelbach O. The Self-Shrinking Generator // Eurocrypt'94. Proceedings. Springer-Verlag. 1998. P. 205-214. **2.** Coppersmith D., Krawchuk Y., Mansour Y. The shrinking generator // Advanced in Cryptology: Proceedings of Crypto 93, LNCS 773. 1994. P. 22-39.

ВОССТАНОВЛЕНИЕ ФУНКЦИОНАЛЬНОЙ ЗАВИСИМОСТИ В ЗАДАЧАХ ТЕПЛОПЕРЕНОСА

Чехменок С.Л., Иванов С.Н., БГУ, Минск

Для методологии теории тепло- и массопереноса характерно то, что она сочетает методы расчета температурных и массовых полей с помощью дифференциальных уравнений переноса и экспериментальные методы определения характеристик тепло- и массопереноса. В настоящее время для решения задач в