Функции в регистрах сдвига с обратной связью, используемые для порождения псевдослучайных последовательностей

Бонич Татьяна Андреевна

Новосибирский государственный университет

Интерес к генераторам

Многие криптографы интересовались свойствами функции обратной связи в регистре сдвига с нелинейными обратными связями[1].
В том числе, чтобы построить генератор псевдослучайной последовательности битов[2].
Существует множество поточных шифров, основанных на регистрах сдвига с линейной и нелинейной обратной связью. Один из них — Grain[3], разработанный в 2004 году. Другой — шифр A5/1[4], который является текущим стандартом GSM. Также можно упомянуть каскад Голлмана[5], генератор сжатия[6] и многие другие.

---

[1] Menezes A., van Oorschot P. C. and Vanstone S., Handbook of Applied Cryptography, 1996.

[2] Carlet C., Boolean functions for cryptography and error-correcting codes, 2010.

[3] Hell M., Johansson T., Meier W., A Stream Cipher for Constrained Environments, 2007.

[4] Canteaut A., A5/1, 2011.

[5] Gollmann D., Kaskadenschaltungen taktgesteuerter Schieberegister als Pseudozufallszahlengeneratoren, 1983.

[6] Coppersmith D., Krawczyk H., Mansour Y., The Shrinking Generator, 1994.

Примеры шифров

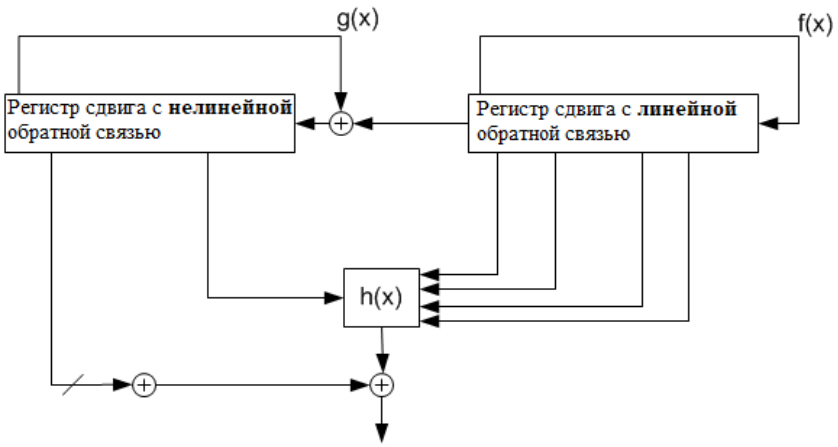

Рис.: Grain

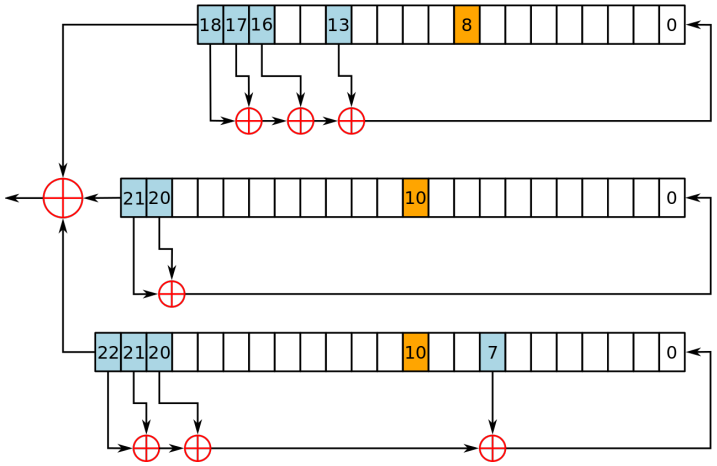

Рис.: A5/1

Регистры сдвига с обратной связью

Регистр сдвига с обратной связью состоит из двух частей: двоичного вектора

$$x = (x_1, \dots x_n)$$

длины n и определенной на нем **функции обратной связи**

$$f : (x_1, \dots, x_n) \to \{0,1\},$$

где f – булева функция от n переменных.
Сначала биты вектора x заполняются конкретными значениями. Каждое заполнение вектора называется **состоянием** регистра. Затем регистр начинает изменять свое состояние с помощью функции обратной связи. Если одно состояние регистра было - $(x_1, x_2, \dots, x_{n-1}, x_n)$, то следующее состояние будет - $(x_2, x_3, \dots, x_n, f(x_1, x_2, \dots, x_{n-1}, x_n))$.

Регистры сдвига с обратной связью

Если функция обратной связи является линейной, то регистр называют **регистром сдвига с линейной обратной связью (РСЛОС)**. Если функция обратной связи является нелинейной, то регистр называют **регистром сдвига с нелинейной обратной связью (РСНОС)**.
Заметим, что каждая булева функция от n переменных единственным образом представляется в виде **алгебраической нормальной формы (АНФ)**:

$$f(x_1, \ldots, x_n) = (\bigoplus_{k=1}^{n} \bigoplus_{i_1, \ldots, i_k} a_{i_1, \ldots, i_k} x_{i_1} \cdot \cdots \cdot x_{i_k}) \oplus a_0,$$

где при каждом k все индексы $i_1, \ldots, i_k$ различны и параметры $a_0, a_{i_1, \ldots, i_k}$ принимают значения 0 или 1.

Регистры сдвига с линейной обратной связью

Также РСЛОС можно задать с помощью **многочлена обратной связи**. Это такой многочлен степени n, определяющий биты, которые надо суммировать. Если

$$f(x_1, \ldots, x_n) = a_1 x_1 \oplus a_2 x_2 \oplus \cdots \oplus a_n x_n,$$

то многочлен обратной связи определяется так:

$$p(x) = a_1 x^n + a_2 x^{n-1} + \cdots + a_n x + 1.$$

Если $p(x)$ примитивный многочлен, то период последовательности, которая будет порождаться регистром сдвига, максимален. Примитивный многочлен делает возможным переход во все состояния, кроме нулевого.

Фильтрующий генератор

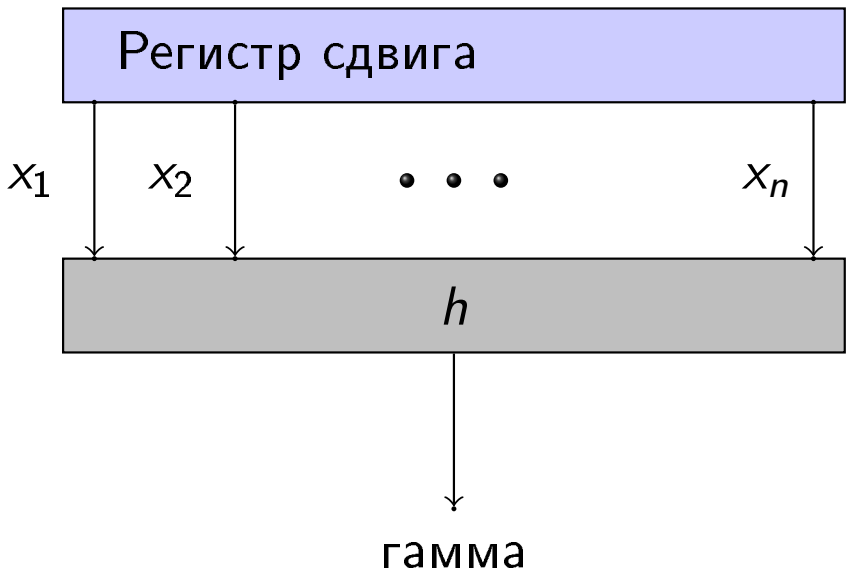

Рис.: Фильтрующий генератор.

Такие функции h, которые приводят к псевдослучайным последовательностям, чей период меньше заданного ℓ, будем называть **неподходящими**. А функции, что приводят к псевдослучайным последовательностям с периодом не меньше заданного ℓ, будем называть **подходящими**.

Примеры генераторов

Таблица: Пример неподходящей функции

0001	**1**
0010	**0**
0100	**0**
1001	1
0011	0
0110	0
1101	1
1010	0
0101	0
1011	1
0111	0
1111	0
1110	1
1100	0
1000	0

Таблица: Пример подходящей функции

0001	1
0010	0
0100	1
1001	1
0011	0
0110	1
1101	1
1010	0
0101	1
1011	0
0111	1
1111	1
1110	0
1100	0
1000	1

Анализ гаммы

Теорема 1

Пусть $2^n - 1 = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_s^{\alpha_s}$, *где* p_i *— различные простые целые числа,* $\alpha_i \in \mathbb{N}$, $s \in \mathbb{N}$ *и* ℓ *— делитель* $2^n - 1$ *такой, что* $\ell = q_1^{\omega_1} q_2^{\omega_2} \dots q_k^{\omega_k}$, *где* $\omega_i \in \mathbb{N}$, $k \leq s \in \mathbb{N}$. *Тогда количество подходящих булевых функций от n переменных для фильтрующего генератора, основанного на РСЛОС, равно*

$$2^{2^n} - 2 \sum_{\beta \in \mathbb{F}_2^k, \beta \neq 0} ((-1)^{\beta_1 + \dots + \beta_k + 1} 2^{q_1^{\omega_1 - \beta_1} \dots q_k^{\omega_k - \beta_k}}), \text{ где } \beta = (\beta_1, \dots, \beta_k).$$

Следствие 1

Количество булевых функций от n переменных, которые приводят к псевдослучайным последовательностям с периодом равным ℓ, *для фильтрующего генератора, основанного на РСЛОС, равно*

$$2^{\ell+1} - 2 \sum_{\beta \in \mathbb{F}_2^k, \beta \neq 0} ((-1)^{\beta_1 + \dots + \beta_k + 1} 2^{q_1^{\omega_1 - \beta_1} \dots q_k^{\omega_k - \beta_k}}), \text{ где } \beta = (\beta_1, \dots, \beta_k).$$

Анализ гаммы

Теорема 2

Пусть $n \in \mathbb{N}$ *и* ℓ *— делитель* 2^n *такой, что* $\ell \in \mathbb{N}$, $\ell = 2^t$, *где* $t \leq n \in \mathbb{N}$. *Тогда количество подходящих булевых функций от* n *переменных для фильтрующей модели генератора, основанного на РСНОС, равно* $2^{2^n} - 2^{2^{t-1}}$.

Следствие 2

Количество булевых функций от n *переменных, которые приводят к псевдослучайным последовательностям с периодом равным* ℓ, *для фильтрующего генератора, основанного на РСНОС, равно* $2^{2^t} - 2^{2^{t-1}}$.