

Lab4

Лабораторная работа №4

Найти начальные состояния регистров, зная выходную последовательность, функцию и линейные рекуррентные соотношения комбинирующего генератора двоичной псевдослучайной последовательности.

- Так как я видимо не смог нормально распаковать выходную последовательность, все вычисления были проведены на собственных случайно сгенерированных начальных состояниях.

Пусть задано m линейных рекуррентных последовательностей по модулю 2 сложности n и булева функция $F : GF(2)^m \rightarrow GF(2)$. Выходом такой последовательности на такте t будет $F(x_1, x_2, x_3, \dots, x_m)$, где x_1, x_2, \dots, x_m - выходы рекуррент на такте t .

Необходимо восстановить начальные состояния системы линейных рекуррентных последовательностей.

Для упрощения будем считать, что выходы каждой из рекуррент равновероятные. Булева функция из условия так же является равновероятной.

Рассмотрим некоторое начальное состояние $r = (r_1, r_2, r_3, \dots, r_n)$ для первой рекурренты.

Рассмотрим две подфункции $f_0 = F(0, x_2, x_3, \dots, x_m)$, $f_1 = F(1, x_2, x_3, \dots, x_m)$

$$P(F = 1 | x_1 = 1) = \frac{|f_1|}{2^{m-1}}$$

$$P(x_1 = 1 | F = 1) = \frac{P(F=1|x_1=1)*P(x_1=1)}{P(F=1)} = \frac{\frac{|f_1|}{2^{m-1}} * \frac{1}{2}}{\frac{1}{2}} = P(F = 1 | x_1 = 1)$$

Аналогично

$$P(x_1 = 0 | F = 1) = P(F = 1 | x_1 = 0) = \frac{|f_0|}{2^{m-1}}$$

А также верно и $F(x_1 = 1 | F = 0) = \frac{|f_0|}{2^{m-1}}$ (это уже следует из равновероятности F).

Таким образом, основываясь только на выводе и свойствах функции F мы можем оценить является ли данное состояние верным для первой рекурренты. Однако это будет работать, только если значения $|f_0|$ и $|f_1|$ отличаются значительно.

Оценить это можно двумя способами.

С одной стороны мы можем посчитать коэффициенты Фурье для векторов $(0, 0, \dots, 0)$ и $(1, 0, 0 \dots 0)$

Для первого вектора: $\tilde{f}(0, 0, \dots, 0) = |F| = |f_0| + |f_1|$

Для второго: $\tilde{f}(1, 0, \dots, 0) = \sum_{V_n} f(\vec{x}) * (-1)^{x_1} = |f_0| - |f_1|$

И если вторая разность достаточно велика то можно оценивать вероятности:

Перебираем все возможные состояния r для рекурренты. Для этого можно воспользоваться двумя оптимизациями:

- Во-первых, так как рекуррента ЛИНЕЙНАЯ мы можем расписать ее как сумму m рекуррент(базисов). То есть мы можем просто хранить m последовательностей(нужной нам длины) с начальными состояниями $(1, 0, \dots, 0), (0, 1, 0, \dots, 0), \dots, (0, 0, \dots, 0, 1)$ и для каждого состояния r складывать нужные нам части базиса.
- Во-вторых, вместо прямого перебора можно использовать перебор с помощью кода Грея(состояния в последовательности отличаются на 1 бит): для перехода из одного состояния в другое необходимо добавить по модулю 2 нужный нам элемент базиса. Какой это будет элемент определяется следующей последовательностью: $\vec{x}_1 = (1), x_n = \vec{x}_{n-1} || n || \vec{x}_{n-1}$. (Еще в начале нужно добавить 0 но это не критично).

Исходя из равенства $P(x_1 = 1 | F = 1) = \frac{|f_1|}{2^{m-1}}$ мы можем посчитать эту вероятность приближенно исходя из данного нам выхода функции F и текущего состояния. То есть мы считаем количество 1 в развернутой последовательности при условии, что в выходе F стоит 1, назовем это количество fs_1 . Аналогично для $|f_0|$ и $F = 0$, а это fs_0 .

Оценивать состояние можно двумя способами:

- Можно просто посчитать $|fs_1 - fs_0|$ и искать самое большое(при большой $||f_0| - |f_1||$ оно будет большим)
- Можно посчитать вероятности $P_0 = \frac{|f_0|}{2^{m-1}}, P'_0 = \frac{fs_0}{s_0}, P_1 = \frac{|f_1|}{2^{m-1}}, P'_1 = \frac{fs_1}{s_1}$. Где s_0 - количество 0 в выходе, s_1 - количество 1 в выходе. Далее будем искать минимум функции $g = (P_0 - P'_0)^2 + (P_1 - P'_1)^2$ среди всех состояний. Данный подход удобен и в общем случае для глубины 2, которую мы будем рассматривать позже.

Всё вышеперечисленное выполнено в функции `GetInitialState(cfs, ftable, stream, n, m, c_ind, L)`

Однако при анализе BF1 можно увидеть, что нужные нам коэффициенты Фурье:

$$\tilde{f}(1, 0, 0, 0, 0, 0) = 0$$

$$\tilde{f}(0, 1, 0, 0, 0, 0) = 8$$

$$\tilde{f}(0, 0, 1, 0, 0, 0) = 6$$

$$\tilde{f}(0, 0, 0, 1, 0, 0) = 2$$

$$\tilde{f}(0, 0, 0, 0, 1, 0) = 2$$

$$\tilde{f}(0, 0, 0, 0, 0, 1) = 0$$

Судя по коэффициентам, таким способом возможно восстановить только 2 и 3 состояния(что успешно получается).

Дальше придется анализировать уже состояния с условием наличия известных состояний.

Пусть у нас известна полностью последовательность для состояния 1, тогда для состояния 2 введем дополнительные подфункции:

$$f_{00} = F(0, 0, x_3, \dots, x_m)$$

$$f_{01} = F(0, 1, x_3, \dots, x_m)$$

$$f_{10} = F(1, 0, x_3, \dots, x_m)$$

$$f_{11} = F(1, 1, x_3, \dots, x_m)$$

Тогда

$$P(F = 1 | x_1 = a, x_2 = b) = \frac{|f_{ab}|}{2^{m-2}}$$

И, следовательно:

$$P(x_2 = 1 | F = 1, x_1 = 1) = \frac{P(F=1, x_1=1, x_2=1)}{P(F=1, x_1=1)} = \frac{|f_{11}|}{|f_1|}$$

И аналогично

$$P(x_2 = 1 | F = 1, x_1 = 0) = \frac{|f_{01}|}{|f_0|}$$

$$P(x_2 = 0 | F = 1, x_1 = 1) = \frac{|f_{10}|}{|f_1|}$$

$$P(x_2 = 0 | F = 1, x_1 = 0) = \frac{|f_{00}|}{|f_0|}$$

f_{ab} можно найти так же с помощью коэффициентов Фурье:

$$\tilde{f}(0, 0, \dots, 0) = |f_{00}| + |f_{01}| + |f_{10}| + |f_{11}|$$

$$\tilde{f}(1, 0, \dots, 0) = |f_{00}| + |f_{01}| - |f_{10}| - |f_{11}|$$

$$\tilde{f}(0, 1, \dots, 0) = |f_{00}| - |f_{01}| + |f_{10}| - |f_{11}|$$

$$\tilde{f}(1, 1, \dots, 0) = |f_{00}| - |f_{01}| - |f_{10}| + |f_{11}|$$

Таким образом, как и в первом случае мы можем с помощью выходной последовательности и данного состояния оценить эти параметры с помощью функции

$$g = \left(\frac{fs_0}{s_0} - \frac{|f_{01}|}{|f_0|} \right)^2 + \left(\frac{fs_1}{s_1} - \frac{|f_{00}|}{|f_0|} \right)^2 + \left(\frac{fs_2}{s_2} - \frac{|f_{11}|}{|f_1|} \right)^2 + \left(\frac{fs_3}{s_3} - \frac{|f_{10}|}{|f_1|} \right)^2$$

В данном случае критерием достаточной величины будет $A = |f_{00}| - |f_{01}| - |f_{10}| + |f_{11}|$

Выводы получились следующими:

Для состояния 2:

$$\tilde{f}(0, 1, 0, 1, 0, 0) = -10$$

Следовательно можно найти 4 состояние.

Для состояния 4:

$$\tilde{f}(1, 0, 0, 1, 0, 0) = -6$$

Получилось найти состояние 1

Для состояния 3:

$$\tilde{f}(0, 0, 1, 0, 1, 0) = -4$$

Получилось найти состояние 5

Для состояния 5:

$$\tilde{f}(0, 0, 0, 0, 1, 1) = -6$$

Получилось найти состояние 6

Восстановление состояний производилось с помощью функции `GetDoubleState(cfs_a, cfs_b, ftable, stream, n, m, a, b, state_a, L)`

Таким образом мы восстановили все состояния.