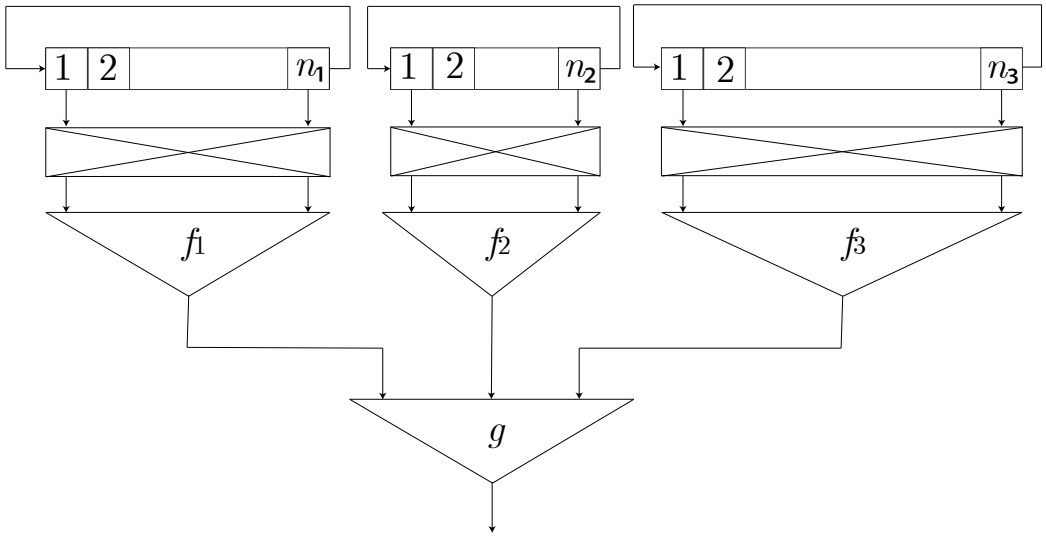
Исследование поточного алгоритма шифрования типа «Раскольников» Вариант №4.

Роман Астраханцев, СКБ-171

4 февраля 2022 г.

Описание алгоритма



Поточный алгоритм шифрования типа «Раскольников» состоит из:

1. трех РСЛОС $L_i, i \in \overline{1,3}$, над полем $\mathbb{F}_2$ с характеристическими многочленами $F_1(x), F_2(x), F_3(x)$ степени соответственно n_1, n_2, n_3.

2. трех коммутаторов (перестановок) $K_i, i \in \overline{1,3}, Ki \in S(l_i)$, на вход коммутатору K_i подаются значения РСЛОС L_i с индексами

$$1 = p1 < p2 < \cdots < p_{l_i-1} < p_{l_i} = n_i$$

3. трех функций усложнения выхода РСЛОС $f_i(x_1, x_2, \ldots, x_{l_i}), i \in \overline{1,3}$,

4. комбинирующей булевой функции $g(x,y,z)$, задаваемой формулой ($\wedge$ – «и», $\neg$ – отрицание, $\vee$ – «или», $\veebar$ – «исключающее или»):

$$g(x,y,z) = (\neg x \vee \neg y) \wedge (x \vee y \vee \neg z) \wedge (\neg y \vee z)$$

Ключом являются:

- начальное заполнение регистра L_1
- коммутатор K_2
- начальное заполнение регистра L_3

1 Исследование ключевого множества

Множетсво ключей K состоит из всезможожных троек вида (k_1, k_2, k_3), где

- k_1 - какое-то заполнение регистра L_1 длины n_1,
- k_2 - какая-то перестановка длины n_2,
- k_3 - какое-то заполнение регистра L_3 длины n_1.

Тогда общее число ключей будет равно

$$|K| = 2^{n_1} \cdot n_2! \cdot 2^{n_3}$$

Приведём пример параметров n_1, n_2, n_3, при котором $|K| > 2^{64}$. Пусть $n_1 = 25, n_2 = 10, n_3 = 25$, тогда

$$|K| = 2^{25} \cdot 10! \cdot 2^{25} > 2^{25} \cdot 2^{21} \cdot 2^{25} > 2^{71} > 2^{64}$$

2 Исследование узлов алгоритма

2.1 Узлы РСЛОС

Регистр сдвига с линейной обратной связью или *РСЛОС* — это блок, который генерирует двоичные псевдослучайные периодические последовательности, которые называются линейными рекуррентными последовательностями (ЛРП).

Широкое распространение в криптографических приложениях линейных регистров сдвига над конечными полями $\mathbb{F}_{2^n}$ и кольцами вычетов обусловлено целым рядом факторов. Среди них можно отметить:

- использование только простейших операций сложения и умножения, аппаратно реализованных практически на всех вычислительных средствах;
- высокое быстродействие создаваемых на их основе криптографических алгоритмов;
- большое количество теоретических исследований свойств линейных рекуррентных последовательностей (ЛРП), свидетельствующих об их удовлетворительных криптографических свойствах

В данном шифре в ключ входят только заполнения регистра сдвига, а вид характеристического многочлена, является параметром построения шифра. Значит, нужно подобрать такие функции обратной связи, чтобы для любого **ненулевого** заполнения ЛРП была максимального периода. В этом нам помогут следующие теормы и следствие из них.

Теорема 2.1. *Пусть u – ЛРП над полем $\mathbb{F}_q$ с реверсивным минимальным многочленом $F(x)$ степени m и $q^m > 2$. Тогда следующие утверждения эквивалентны:*

(1) u – ЛРП максимального периода;

(2) многочлен $F(x)$ неприводим над $\mathbb{F}_q$, и его корень α в минимальном поле разложения $\mathbb{F}_{q^m}$ над $\mathbb{F}_q$ есть примитивный элемент поля.

Теорема 2.2. *Неприводимый многочлен $F(x)$ примитивен в том и только в том случае, когда для любого простого числа p, делящего $q^m - 1$, многочлен $x^{\frac{q^m-1}{p}}$ не сравним с 1 по модулю многочлена $F(x)$.*

Следствие 2.3. *Если $F(x)$ – неприводимый многочлен над полем $\mathbb{F}_2$ степени m, и $2^m - 1$ – простое число, то $F(x)$ – примитивный многочлен.*

Исходя из утверждений выше, для того чтобы линейная рекуррентная последовательность порядка m над полем из q элементов имела максимальный период, необходимо и достаточно, чтобы ее минимальный многочлен был примитивным многочленом.

Более конкретно, над полем $\mathbb{F}_2$ необходимо реверсивный минимальный многочлен $F(x)$ на основе просых чисел Мерсенна. В этом случае для любого **ненулевого** заполнения ЛРП получается максимального периода.

Приведём конкретный пример многочленов $F_1(x), F_2(x), F_3(x)$ для заданных нашим алгоритмом РСЛОС L_1, L_2, L_3.

Пусть $n_1 = 31, n_2 = 13, n_3 = 19$ ($2^{31}-1, 2^{13}-1$ и $2^{19}-1$ — это известные числа Мерсенна).

Пример неприодимых многочленов соотвествующих степеней из $\mathbb{F}_2$[x].

$$\begin{aligned} F_1(x) =& x^{31} + x^{30} + x^{29} + x^{28} + x^{27} + x^{24} + x^{21} + x^{19} + \\ &+ x^{18} + x^{13} + x^{12} + x^{10} + x^4 + x^3 + 1 \end{aligned}$$

$$F_2(x) = x^{13} + x^{12} + x^{11} + x^8 + x^7 + x^6 + x^5 + x^4 + x^2 + x + 1$$

$$F_3(x) = x^{19} + x^{15} + x^{13} + x^{12} + x^{10} + x^9 + x^5 + x^4 + x^2 + x + 1$$

В этом случае любое **ненулевое** заполнение каждого РСЛОС L_1, L_2, L_3 даст нам максимальный период на каждом из регистрах. Кроме того, каждый регистр сдвига был выбран разной длинны для того, чтобы исключить случай совместного зацикливания двух ЛРП. Иными словами итоговый период совместной работы всех трёх регистров будет равна

$$N_{L_1L_2L_3} = \text{НОК}(2^{n_1}-1, 2^{n_2}-1, 2^{n_3}-1) = \text{НОК}(2^{31}-1, 2^{13}-1, 2^{19}-1) \approx 2^{63}$$

Это означает, что вектор начальных заполнений (u_1, u_2, u_3) регистров L_1, L_2, L_3 вернётся в сам в себя после $N_{L_1L_2L_3} \approx 2^{63}$ совместных тактов работы всех трёх регистров.

При этом мощность ключевого множества по-прежнему будет удовлетворять условию $|K| > 2^{64}$:

$$|K| = 2^{31} \cdot 13! \cdot 2^{19} > 2^{31} \cdot 2^{32} \cdot 2^{19} > 2^{82} > 2^{64}$$

2.2 Функций усложнения