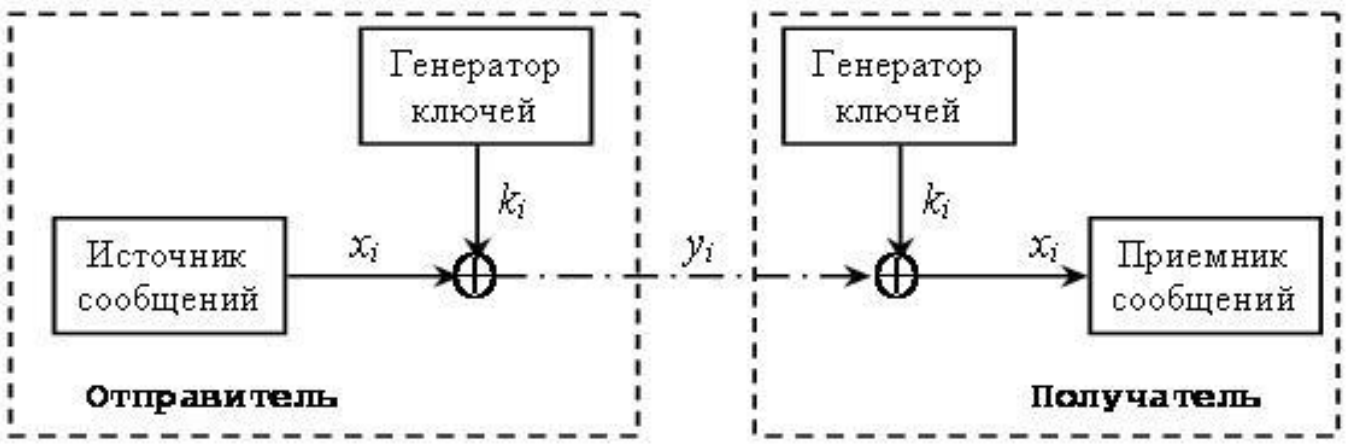
АЛГЕБРАИЧЕСКИЕ МЕТОДЫ КРИПТОАНАЛИЗА НЕКОТОРЫХ ПОТОЧНЫХ ШИФРОВ

Пилеко С.М.

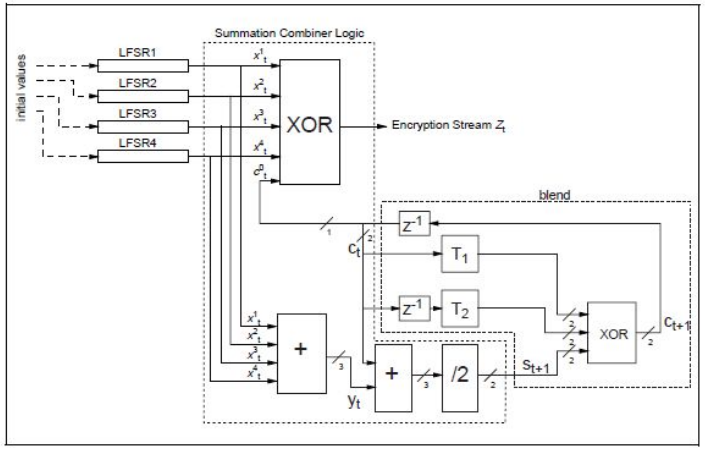
Кафедра алгебры, геометрии и анализа ШЕН ДВФУ

Научный руководитель – к.ф.-м.н., доцент С.Г. Чеканов

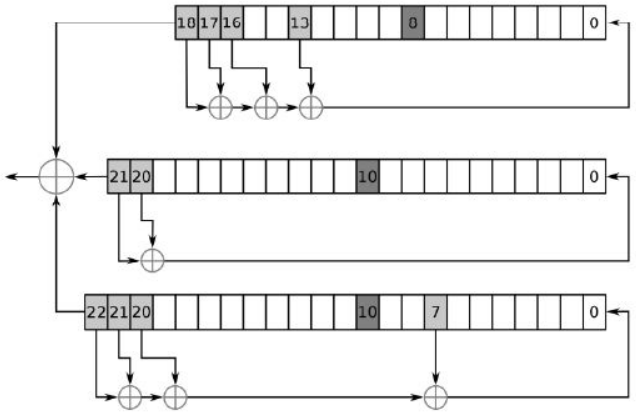
1. Схема поточного шифра



Blutooth



GSM (A5)



Преимущества:

- высокая скорость шифрования,
- отсутствует эффект размножения ошибок, то есть число искаженных элементов в расшифрованной последовательности равно числу искаженных элементов зашифрованной последовательности, пришедшей из канала связи.

Недостатки:

- Ключ шифрования имеет длину равную длине открытого текста, что усложняет распределение ключей

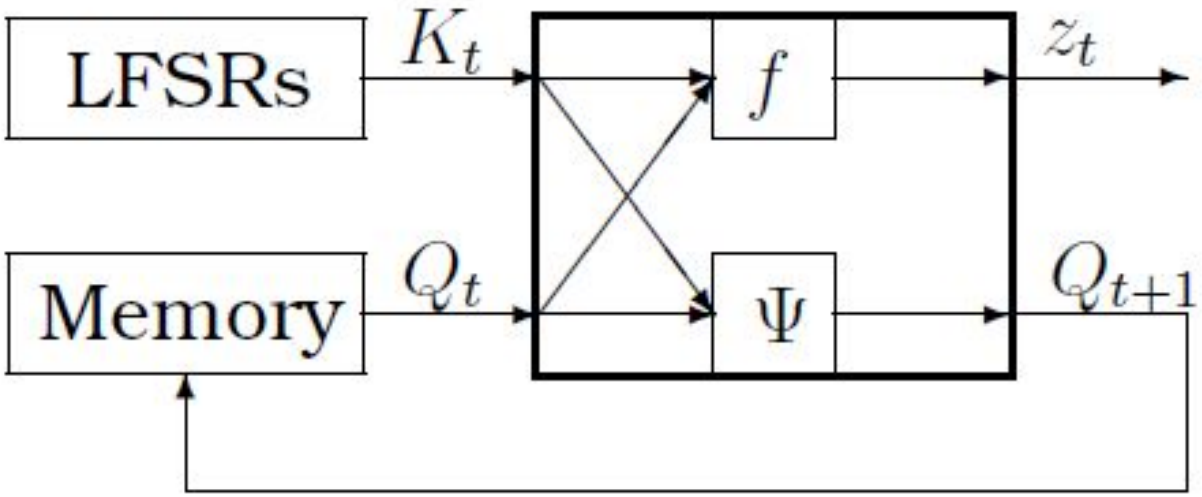
2. Оценка стойкости шифра

Определение. Назовем шифр Σ_B совершенным, если для любых $x \in X, y \in Y$
выполняется равенство

$$p(x/y) = p_X(x)$$

$\Sigma_B = (X, K, Y, E, D, P(X), P(K))$ - вероятностная модель
$P(K), P(X)$ - распределения вероятностей
$p_X(x) > 0, x \in X$ и $p_K(k) > 0, k \in K$
$P(Y) = \{p_y(y), y \in Y\}$
$p_y(y) = \sum_{(x,k)E_k(x)=y} p_X(x) \cdot p_k(k)$

3. Генераторы ключевых последовательностей



Определение. Пусть F конечное поле. Будем говорить, что (l, m) – генератор определяется следующими компонентами:

1) ЛРС размерности $n_1, \ldots, n_s$ и матрицами обратной связи $L_1, \ldots, L_s$;
2) внутреннее состояние $S \in F^m \times F^n$, и $n = n_1 + \ldots + n_s$;
3) матрица над F размерности $n \times n$, которая имеет вид

$$L = \begin{pmatrix} L_1 & 0 & 0 \\ 0 & \ddots & 0 \\ 0 & 0 & L_s \end{pmatrix};$$

4) матрица проектирования P над F размерности $n \times l$;
5) нелинейная функция обновления памяти $\gamma: F^m \times F^l \to F^m$;
6) функция выхода $f: F^m \times F^l \to F$.

$K = (a_0, a_1, b_0, b_1, b_2)$, $a_{t+2} = a_{t+1} + a_t$, $b_{t+3} = b_{t+2} + b_t$, $f(a, b) = a \cdot b + a + b$

Пусть $K = (0, 1, 0, 1, 0)$, тогда

$$\begin{cases} 0 = a_0 b_0 + a_0 + b_0 \\ 1 = a_1 b_1 + a_1 + b_1 \\ 0 = a_2 b_2 + a_2 + b_2 \\ 1 = a_3 b_3 + a_3 + b_3 \\ 1 = a_4 b_4 + a_4 + b_4 \\ 1 = a_5 b_5 + a_5 + b_5 \\ 1 = a_6 b_6 + a_6 + b_6 \\ 1 = a_7 b_7 + a_7 + b_7 \\ 1 = a_8 b_8 + a_8 + b_8 \\ 0 = a_9 b_9 + a_9 + b_9 \\ 1 = a_{10} b_{10} + a_{10} + b_{10} \end{cases}$$

t	0	1	2	3	4	5	6	7	8	9	10
a_t	0	1	1	0	1	1	0	1	1	0	1
b_t	0	1	0	0	1	1	1	0	1	0	0
z_t	0	1	0	1	1	1	1	1	1	0	1

$$
\begin{cases}
0 = a_0b_0 + a_0 + b_0 \\
1 = a_1b_1 + a_1 + b_1 \\
1 = a_0b_2 + a_1b_2 + a_0 + a_1 + b_2 \\
0 = a_0b_0 + a_0b_2 + a_0 + b_0 + b_2 \\
1 = a_1b_0 + a_1b_1 + a_1b_2 + a_1 + b_0 + b_1 + b_2 \\
1 = a_0b_0 + a_0b_1 + a_1b_0 + a_1b_1 + a_0 + a_1 + b_0 + b_1 \\
1 = a_0b_1 + a_0b_2 + a_0 + b_1 + b_2 \\
1 = a_1b_0 + a_1 + b_0 \\
1 = a_0b_1 + a_1b_1 + a_0 + a_1 + b_1 \\
0 = a_0b_2 + a_0 + b_2 \\
1 = a_1b_0 + a_1b_2 + a_1 + b_0 + b_2
\end{cases}
$$

4. r – функции, z - функции

Определение. Пусть $r \geq 1$. Функция $F: \mathbb{F}^{r \cdot l + r} \to \mathbb{F}$ называется r – функцией, если

$$F(X_1, \dots, X_r, y_1, \dots, y_r) = 0,$$

где $X_1, \dots, X_r$ – последовательности входных значений, $y_1, \dots, y_r$ – соответствующие выходы.

Для значений r последовательных элементов ключевого потока $z_t, \dots, z_{t+r-1}$ верно следующее уравнение.

$$F(K_t, \dots, K_{t+r-1}, z_t, \dots, z_{t+r-1}) = 0$$

Определение. Пусть $K_t \in \mathbb{F}^l$ - ключевая последовательность, t - счетчик, (z_t) - значения на выходе. Функция $F_Z: \mathbb{F}^{l \cdot r} \to \mathbb{F}$ для $Z \in \mathbb{F}^r$ называется z - функцией, где $z_t, \dots, z_{t+r-1}$ принимаем за Z, то F_Z равно нулю на соответствующих входах $K_t, \dots, K_{t+r-1}$. Для любого $t \geq 0$:

$$(z_t, \dots, z_{t+r-1}) = Z \Rightarrow F_Z(K_t, \dots, K_{t+r-1}) = 0$$

Алгоритм

Алгебраическая атака на (l, m) - генератор с помощью системы уравнений, составленной из z - функций.

Input: (l, m) - генератор, секретные значения $S_0 = (Q_0, K)$, некоторая часть элементов ключевого потока

Output:Секретный ключ K

1: Зафиксируем $r \geq 1$ и найдем $i(Z)$ z - функции для каждого $Z \in \mathbb{F}^r$

2: Инициализируем пустую систему уравнений

3: При каждом запуске программы для известных элементов ключевого потока $(z_t, ..., z_{t+r-1}) = Z_t^r$ добавим в систему следующие уравнения:

$F_{Z_t^r}^{(1)}(K_t, ..., K_{t+r-1}) = 0$

$\dots$

$F_{Z_t^r}^{(i(Z_t^r))}(K_t, ..., K_{t+r-1}) = 0$

4: Востановим K, решив полученную систему уравнений

5: **return** K

5. Пример построения системы уравнений с помощью z-функций

$$\begin{cases} 0 = a_0 \\ 0 = b_0 \\ 1 = a_1b_1 + a_1 + b_1 \\ 0 = a_2 \\ 0 = b_2 \\ 1 = a_3b_3 + a_3 + b_3 \\ 1 = a_4b_4 + a_4 + b_4 \\ 1 = a_5b_5 + a_5 + b_5 \\ 1 = a_6b_6 + a_6 + b_6 \\ 1 = a_7b_7 + a_7 + b_7 \\ 1 = a_8b_8 + a_8 + b_8 \\ 0 = a_9 \\ 0 = b_9 \\ 1 = a_{10}b_{10} + a_{10} + b_{10} \end{cases} \qquad \begin{cases} 0 = a_0 \\ 0 = b_0 \\ 1 = a_1b_1 + a_1 + b_1 \\ 1 = a_0b_2 + a_1b_2 + a_0 + a_1 + b_2 \\ 0 = a_0 \\ 0 = b_0 + b_2 \\ 1 = a_1b_0 + a_1b_1 + a_1b_2 + a_1 + b_0 + b_1 + b_2 \\ 1 = a_0b_0 + a_0b_1 + a_1b_0 + a_1b_1 + a_0 + a_1 + b_0 + b_1 \\ 1 = a_0b_1 + a_0b_2 + a_0 + b_1 + b_2 \\ 1 = a_1b_0 + a_1 + b_0 \\ 1 = a_0b_1 + a_1b_1 + a_0 + a_1 + b_1 \\ 0 = a_0 \\ 0 = b_2 \\ 1 = a_1b_0 + a_1b_2 + a_1 + b_0 + b_2 \end{cases}$$

6. Методы решения нелинейных систем уравнений

6.1 Алгоритм Бухбергера

Определение. Базис $f_1, ..., f_m$ идеала $I = (f_1, ..., f_m)$ называется базисом Гребнера этого идеала, если всякий многочлен $h \in I$ редуцируется к нулю при помощи $f_1, ..., f_m$.

Определение. Набор многочленов $f_1, ..., f_m$ - базис Гребнера в $I = (f_1, ..., f_m)$, если для любого $h \in I$ одночлен h_C делится на один из одночленов $f_{1C}, f_{2C}, ..., f_{mC}$.

6.2 Линеаризация

Алгоритм

Решение систем уравнений методом линеаризации

Input: Система уравнений $f_1(X) = 0, ..., f_N(X) = 0$ с $f_i(X) \in \mathbb{F}_q[X]$.

Output: все корни

1: Пусть $\varepsilon \subset \{0, ..., q-1\}^n$ - множество всех встречающихся показателей степени, т.е. $f_i(X) = \Sigma_{E \in \varepsilon} c_E^{(i)} X^E$ для всех f_i.

2: Выбрать произвольный порядок в ε.

3: Создать пустую матрицу M размера $N|\varepsilon|$. Строки индексируются функциями f_i, а столбцы - показателями $E \in \varepsilon$.

4: Для всех f_i и $E \in \varepsilon$ запись в строке f_i и столбце E устанавливается на $C_E^{(i)}$.

5: Вычислить с исключением Гаусса базис ядра матрицы M, т. е. максимальный набор линейно независимых векторов $V \in \mathbb{F}_q^{|\varepsilon|}$ таких, что $M \cdot V = \vec{0}$.

6: Получим из векторов ядра все корни.

7: **return** K

7. Список литературы

1. Armknecht F. Algebraic attacks on combiners with memory./ Armknecht F, Krause M. - Mannheim, 2006. - 175 p.
2. Алферов А.П. Основы криптографии: учеб. пособие 2-е изд., испр. и доп. / Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В. - М. Гелиос АРВ, 2002. - 480 с.