Генерация систем

1) Генерируем матрицы $M_1, M_2 \in GL_n(\mathbb{F}_2)$ — две обратимые матрицы порядка n над полем $\mathbb{F}_2$.
$A := \mathbf{0}$;
while $\det(A) = 0$ do
for $i \in 1..n$ do
for $j \in 1..n$ do
$A[i,j] := random\{0,1\}$;
end for;
end for;
end while;

Генерируем случайные векторы v_1, v_2 над $\mathbb{F}_2$ размерности n.
Определяем аффинные преобразования $S : \mathbb{F}_2^n \to \mathbb{F}_2^n$ по правилу $S(x) = M_1x + v_1$ и $T : \mathbb{F}_2^n \to \mathbb{F}_2^n$ по правилу $T(x) = M_2x + v_2$. Здесь $x = (x_1, x_2, ..., x_n)$. Матрицы M_1, M_2 называются матрицами аффинных преобразований S и T.

Например, если $n = 2$, матрица преобразования равна $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, а вектор равен $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$, то преобразование имеет вид $\begin{pmatrix} y_1 \\ y_2 \end{pmatrix} = \begin{pmatrix} x_1 + x_2 + 1 \\ x_2 \end{pmatrix}$.
2) Составляем отображение $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$, которое определяется следующим образом

$$F(x_1, x_2, ..., x_n) = \begin{cases} x_1 \\ x_2 + g_2(x_1) \\ x_3 + g_3(x_1, x_2) \\ ... \\ x_n + g_n(x_1, x_2, ..., x_{n-1}) \end{cases},$$

где $g_i(x_1, ...x_{i-1})$, $i \in \overline{1,n}$ — случайные квадратичные полиномы, то есть функции вида $\sum\limits_{\substack{1 \le k,l \le i-1 \\ k \ne l}} a_{kl}x_kx_l + \sum\limits_{k=1}^{i-1} b_kx_k + c_i$, $i \in \overline{1,n}$.

B:=$\mathbf{0}$;
for $i \in 1..n-1$ do
for $j \in 1..\frac{i(i-1)}{2} + i + 1$ do
$B[i,j] := random\{0,1\}$;
end for;
end for;

$B \to b_i = (b_{i1}, b_{i2}, ..., b_{i\ \frac{i(i-1)}{2}+i+1}) \to g_i(x_1, ..., x_{i-1})$.

Таким образом, имеем три отображения:

$$S : \mathbb{F}_2^n \to \mathbb{F}_2^n, \begin{cases} s_1 = s_1(x_1, x_2, ..., x_n) \\ s_2 = s_2(x_1, x_2, ..., x_n) \\ ... \\ s_n = s_n(x_1, x_2, ..., x_n) \end{cases},$$

$$T : \mathbb{F}_2^n \to \mathbb{F}_2^n, \begin{cases} t_1 = t_1(x_1, x_2, ..., x_n) \\ t_2 = t_2(x_1, x_2, ..., x_n) \\ ... \\ t_n = t_n(x_1, x_2, ..., x_n) \end{cases},$$

$$F : \mathbb{F}_2^n \to \mathbb{F}_2^n, \begin{cases} y_1 = x_1 \\ y_2 = x_2 + g_2(x_1) \\ y_3 = x_3 + g_3(x_1, x_2) \\ ... \\ y_n = x_n + g_n(x_1, x_2, ..., x_{n-1}) \end{cases},$$

3) Вводим отображение $P := S \circ F \circ T : \mathbb{F}_2^n \to \mathbb{F}_2^n$. Запишем P в явном виде

$$F \circ T : \mathbb{F}_2^n \to \mathbb{F}_2^n, \begin{cases} y_1 = t_1(x_1, x_2, ..., x_n) \\ y_2 = t_2(x_1, x_2, ..., x_n) + g_2(t_1(x_1, x_2, ..., x_n)) \\ ... \\ y_n = t_n(x_1, x_2, ..., x_n) + g_n(t_1(x_1, x_2, ..., x_n), t_2(x_1, x_2, ..., x_n), ..., t_{n-1}(x_1, x_2, ..., x_n)) \end{cases}$$

$$P = S \circ F \circ T : \mathbb{F}_2^n \to \mathbb{F}_2^n, \begin{cases} s_1 = s_1(y_1, y_2, ..., y_n) \\ s_2 = s_2(y_1, y_2, ..., y_n) \\ ... \\ s_n = s_n(y_1, y_2, ..., y_n) \end{cases}$$

Возьмём произвольный вектор $u \in \mathbb{F}_2^n$ и вычислим $v := P(u)$ — шифротекст. Для нахождения исходного сообщения (если не знаем S и T) получим систему квадратичных уравнений $P(u) = v$.

Например, при $n = 3$, для отображений $S : \begin{cases} s_1 = x_1 \\ s_2 = x_1 + x_3 \\ s_3 = x_2 + x_3 \end{cases}, F : \begin{cases} y_1 = x_1 \\ y_2 = x_2 + x_1 + 1 \\ y_3 = x_3 + x_1 x_2 \end{cases}$

$T : \begin{cases} t_1 = x_1 + x_2 + x_3 + 1 \\ t_2 = x_1 + x_3 + 1 \\ t_3 = x_2 + x_3 \end{cases}$, получим следующее:

$$F \circ T : \mathbb{F}_2^3 \to \mathbb{F}_2^3, \begin{cases} y_1 = x_1 + x_2 + x_3 + 1 \\ y_2 = x_2 + 1 \\ y_3 = x_1 x_2 + x_2 x_3 + x_1 + 1 \end{cases}$$

$P = S \circ F \circ T : \mathbb{F}_2^3 \to \mathbb{F}_2^3, \begin{cases} s_1 = x_1 + x_2 + x_3 + 1 \\ s_2 = x_1x_2 + x_2x_3 + x_2 + x_3 \\ s_3 = x_1x_2 + x_2x_3 + x_1 + x_2 \end{cases}$

Возьмём сообщение $u = (1, 0, 1)$ и зашифруем его $P((1, 0, 1)) = (1, 1, 1)$. Значит, для восстановления сообщения нужно решать систему $\begin{cases} x_1 + x_2 + x_3 = 0 \\ x_1x_2 + x_2x_3 + x_2 + x_3 = 1 \\ x_1x_2 + x_2x_3 + x_1 + x_2 = 1 \end{cases}$