ОБ АЛГОРИТМИЧЕСКОЙ РЕАЛИЗАЦИИ *S*-БОКСОВ

конференция РусКрипто

Докладчик: д.ф.-м.н., проф. Фомичёв В.М.

Авторы: Фомичёв В.М., Задорожный Д.И., Коренева А.М., Лолич Д.М., Юзбашев А.В.

Актуальность и цель работы

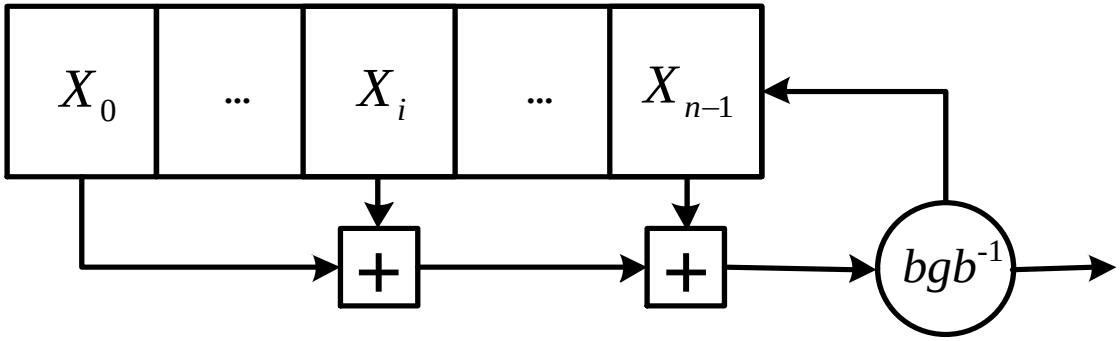
• **s-боксы** – важнейшие конструктивные элементы раундовых подстановок СБШ, удовлетворяющие ряду критериев [Menyachikhin A. CTCrypt Preproceedings, 2016] (DES: 6×4 (бит), ГОСТ 28147-89: 4×4, ГОСТ Р 34.12-2015 («Кузнечик»): 8×8).

• Обычно *s*-боксы заданы таблицами, и этот способ ресурсоемкий по размеру памяти и по времени обращения.

• Цель – разработка с помощью МАГ (модифицированного аддитивного генератора) альтернативного алгоритмического подхода к реализации *s*-боксов, существенно расширяющего возможности синтеза *s*-боксов больших размеров.

Конструкция МАГ

$X_0,\ldots,X_{n-1}$ – начальное состояние МАГ (числа кольца вычетов Z_{2^r}); $g{:}V_r\to V_r$ – модификация; b – биекция $Z_{2^r}\leftrightarrow V_r$, $b(X)=\bar{X}$. [Коренева А.М., Фомичёв В.М. Перемешивающие свойства модифицированных аддитивных генераторов, 2017].



Преобразование φ^g (множества состояний МАГ) – подстановка $\Leftrightarrow$ g – подстановка V_r:

$$\varphi^g(\bar{X}_0,\ldots,\bar{X}_{n-1})=(\bar{X}_1,\ldots,\bar{X}_{n-1},g(b((\sum_{k\in D}X_k)\bmod 2^r)))$$

где $D=\{d_0,\ldots,d_q\}\subseteq\{0,\ldots,n-1\}$ – множество точек съёма, $0<q$, $0=d_0<\ldots<d_q<n$.

МАГ генерирует знаки гаммы X_i по закону рекурсии, $i\geq 0$:

$$X_{i+n}=b^{-1}(g(b((\sum_{k\in D}X_{i+k})\bmod 2^r))). \qquad (1)$$

Свойства подстановок

При фиксации $z=(z_0,\ldots, z_{n-2})$ переменных $\bar{X}_0,\ldots,\bar{X}_{n-2}$ и любом $l\geq 1$ функция $\bar{X}_{n-1} \to \bar{X}_{n-1+l}$, реализуемая (1), есть преобразование $s^{(l)}(z,x)$ множества V_r; $x=\bar{X}_{n-1}$.

Теорема 1. Пусть $d_q=n-1$, g – подстановка, тогда $s^{(l)}(z,x)$ – подстановка при $l=1,\ldots,n-1-d_{q-1}$ и любой z.

Обозначим: Γ – перемеш. орграф подстановки φ^g с множ. вершин $V=\{1,\ldots,nr\}$; $H=\{n(r-1),\ldots,nr-1\}\subset V$ - номера переменных $x_{n(r-1)},\ldots,x_{nr-1}\in\bar{X}_{n-1}$;
H^2-expΓ – локальный экспонент Γ (min $\gamma\in N$: для $\forall i,j\in H$ из i в j есть путь длины t при $\forall t\geq\gamma$.
[Фомичёв В.М., Кяжин С.Н. Локальная примитивность матриц и графов, 2017]

Теорема 2. Пусть $n=3$, $r=8$, $D=\{0,2\}$, $\bar{X}_2=(x_0,\ldots,x_7)$, K – соверш-й s-бокс 4×4, $g(x_0,\ldots,x_7)=(K(x_0\oplus x_4,x_1\oplus x_5,x_2\oplus x_6,x_3\oplus x_7),K(x_0,x_1,x_2,x_3))$, тогда H^2-exp$\Gamma=2$.

Экспериментальные исследования

Объект исследования:

множества подстановок $S_i=\{s_i^{(2)}(z,x)\colon z\in V_{16}\}$, реализованные МАГ при n=3, r=8, D={0,2}, где g_i (см. теорему 2) построена с помощью s-бокса K_i размера 4×4, i=1,…,8. [Рекомендации по стандартизации ТК26 «Задание узлов замены … ГОСТ 28147-89», 2013]

Для K_i получен список S_i подстановок s вида $\{s_i^{(2)}(z,x)\colon z\in V_{16}\}$, i=1,…,8. Для всех подстановок $s\in S_i$ с координ. функциями $s_1,\ldots,s_8$ проверены свойства:

1) совершенность (существенная зависимость s_j от x_i, i,j=1,…,8);
2) нелинейность всех нетривиальных комбинаций $\alpha_1 s_1\oplus\ldots\oplus\alpha_8 s_8$;
3) близость максимальной разностной характеристики p_s к максимальной разностной характеристике случайной подстановки.

Результаты исследования

1. Свойства 1 и 2 выполнены для большинства подстановок (табл.1).

Таблица 1 – Количество подстановок (из 65536), не обладающих свойствами 1 и 2.

Свойство	Узел замены 4×4, использованный в МАГ							
	K_1	K_2	K_3	K_4	K_5	K_6	K_7	K_8
1	128	384	384	0	10	354	320	6
2	0	0	0	0	0	12	8	4

2. Для подстановки s со свойствами 1 и 2 $p_s=(10+2k)/256$, $k=0,1,\ldots,15$. В табл. 2 - число подстановок s, где $p_s=10/256$.

Таблица 2 – Количество подстановок s, для которых $p_s=10/256$.

Узел замен	K_1	K_2	K_3	K_4	K_5	K_6	K_7	K_8
Количество подстановок	44	24	68	100	24	48	84	48

Обратные подстановки s' (к каждой подстановке s из табл. 2) обладают свойствами 1 и 2 и их разностная характеристика $p_{s'}$ также равна 10/256.

Анализ построенных подстановок

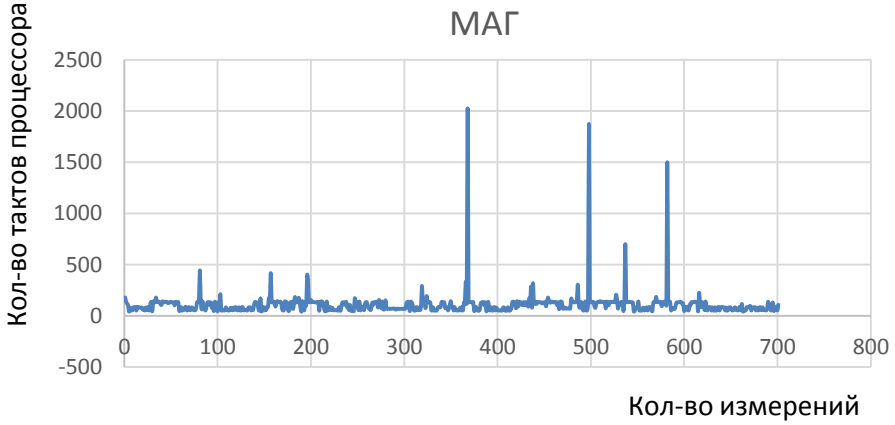
1) Лучшие значения p_s=10/256 близки к p_s=6/256 оптимальных s-боксов [Menyachikhin A.].
2) Среднее значение p_s не превышает среднего значения случайных подстановок степени 256.

Таблица 3 – Сравнение характеристик p_s для s-боксов известных алгоритмов.

«Skipjack»	«Кузнечик»	s-боксы работы [1]	s-боксы таблицы 2
12/256	8/256	6/256	10/256

Время реализации s-бокса в тактах (1 такт ≈ 1/3,5 нс, ЭВМ Intel Core i5-4690 @ 3.50 GHz, 4 cores):

Алгоритм «Кузнечик» (реализация А. Апрелева) ~ 100 тактов;
Алгоритм на основе МАГ ~ 100 тактов.



Выводы

Предложенный подход позволяет алгоритмически реализовать *s*-боксы 8×8 с использованием МАГ и *s*-боксов 4×4. Получено несколько десятков *s*-боксов 8×8 с рядом позитивных криптографических свойств.

Направления дальнейших исследований:

- другие характеристики *s*-боксов 8×8 на основе МАГ;
- синтез больших *s*-боксов (16×16, 32×32 и др.).

Спасибо за внимание!