конференция РусКрипто'2013

Алгоритмы развертывания ключа XSL-шифрсистем, стойкие относительно линейного метода анализа

аспирант кафедры №42: Хоруженко Г.И.

Москва 2013

http://www.ruscrypto.ru/conference/

Шифрсистема A (1)

Длина блока открытого/шифртекста равен n, ключа шифрования - n', число раундов - r.

$$n, n', m, d, r \in \mathrm{N},\ n = md\,,$$

$$s = \ s_{d-1},...,s_0 \ \ \in S\ \ V_n\ \ , s_v = \ \ s_u^{m-1}, \ldots, s_u^{0}\ \ \in S\ \ V_m\ \ , s_u^{v} : V_m \to \{0,1\},$$

$$u \in \{0,...,d-1\}, v \in \{0,...,m-1\},$$

$$\sigma \in S\ \ \{0,\ldots,n-1\}\ \ ,\ h : V_n \to V_n,\ h\ \ \ \alpha_{n-1},\ldots,\alpha_0\ \ \ =\ \ \alpha_{\sigma\ \ n-1}, \ldots, \alpha_{\sigma\ \ n-1}\ \ \ .$$

Раундовая функция $g_{k^{(i)}} : V_n \to V_n$

$$\alpha^{\ \ i}\ \ = g_{k^{(i)}}\ \ \alpha^{\ \ i-1}\ \ \ = h\ \ s\ \ \alpha^{\ \ i-1} \oplus k^{\ \ i}\ \ \ \ ,$$

Алгоритм развертывания ключа (АРК)

$$k^{(i)} = \mathbf{a}_i k \oplus c_i,$$

где $\mathbf{a}_i$ - матрица $n' \times n$, c_i - константа, зависящая от номера раунда, $i \in \{1,\ldots,r\}$.

Шифрсистема A (2)

$\alpha_{n-1}^{(i-1)}$	$\alpha_{n-2}^{(i-1)}$	$\alpha_{n-3}^{(i-1)}$	$\alpha_{n-4}^{(i-1)}$	$\alpha_{n-5}^{(i-1)}$	…	$\alpha_{4}^{(i-1)}$	$\alpha_{3}^{(i-1)}$	$\alpha_{2}^{(i-1)}$	$\alpha_{1}^{(i-1)}$	$\alpha_{0}^{(i-1)}$

$$\oplus$$

$k_{n-1}^{(i)}$	$k_{n-2}^{(i)}$	$k_{n-3}^{(i)}$	$k_{n-4}^{(i)}$	$k_{n-5}^{(i)}$	…	$k_{4}^{(i)}$	$k_{3}^{(i)}$	$k_{2}^{(i)}$	$k_{1}^{(i)}$	$k_{0}^{(i)}$

s_{d-1}	s_{d-2}	…	s_1	s_0

h

$\alpha_{n-1}^{(i)}$	$\alpha_{n-2}^{(i)}$	$\alpha_{n-3}^{(i)}$	$\alpha_{n-4}^{(i)}$	$\alpha_{n-5}^{(i)}$	…	$\alpha_{4}^{(i)}$	$\alpha_{3}^{(i)}$	$\alpha_{2}^{(i)}$	$\alpha_{1}^{(i)}$	$\alpha_{0}^{(i)}$

Линейный метод анализа (1)

$A^{(0)}$ - множество номеров битов блока открытого текста;

$A^{r'_\omega}$ - множество номеров битов блока шифртекста;

C - множество номеров битов ключа шифрования;

δ - преобладание линейной характеристики,

$$\delta = P\left\{\left(\sum_{j\in A^{(0)}} \oplus \alpha_j^{0}\right) \oplus \left(\sum_{j\in A^{(r')}} \oplus \alpha_j^{r'}\right) = \left(\sum_{j\in C} \oplus k_j\right)\right\} - \frac{1}{2},$$

где $\alpha^{0} \in_U V_n, k \in_U V_n, \alpha^{r'} \in V_n$.

Линейная характеристика ω шифрсистемы А для r'_ω раундов

$$\omega = A^{(0)}, A^{(r'_\omega)}, C, \delta .$$

Линейный метод анализа (2)

$$f_k^{\,i,j} = \prod_{b=i}^{j} g_{k^{(b)}},$$

$$\varepsilon_b = \Big(0,\ldots,0,\underset{b}{1},0,\ldots,0 \Big) \in V_{n'}, b \in \{0,\ldots,n'-1\},$$

$$B_w\left(f_k^{\,i,j} \right) =$$

$$= \left\{ b \in \{0,\ldots,n-1\} \mid \exists \gamma^0 \in V_n, \gamma^1 = f_k^{\,i,j}\left(\gamma^0\right), \gamma'^1 = f_{k\oplus\varepsilon_b}^{\,i,j}\left(\gamma^0\right), \gamma_w^1 \neq \gamma_w'^1 \right\} -$$

- множество бит ключа шифрования, от которых существенно зависит w-й выходной бит функции $f_k^{\,i,j}$.

Линейный метод анализа (3)

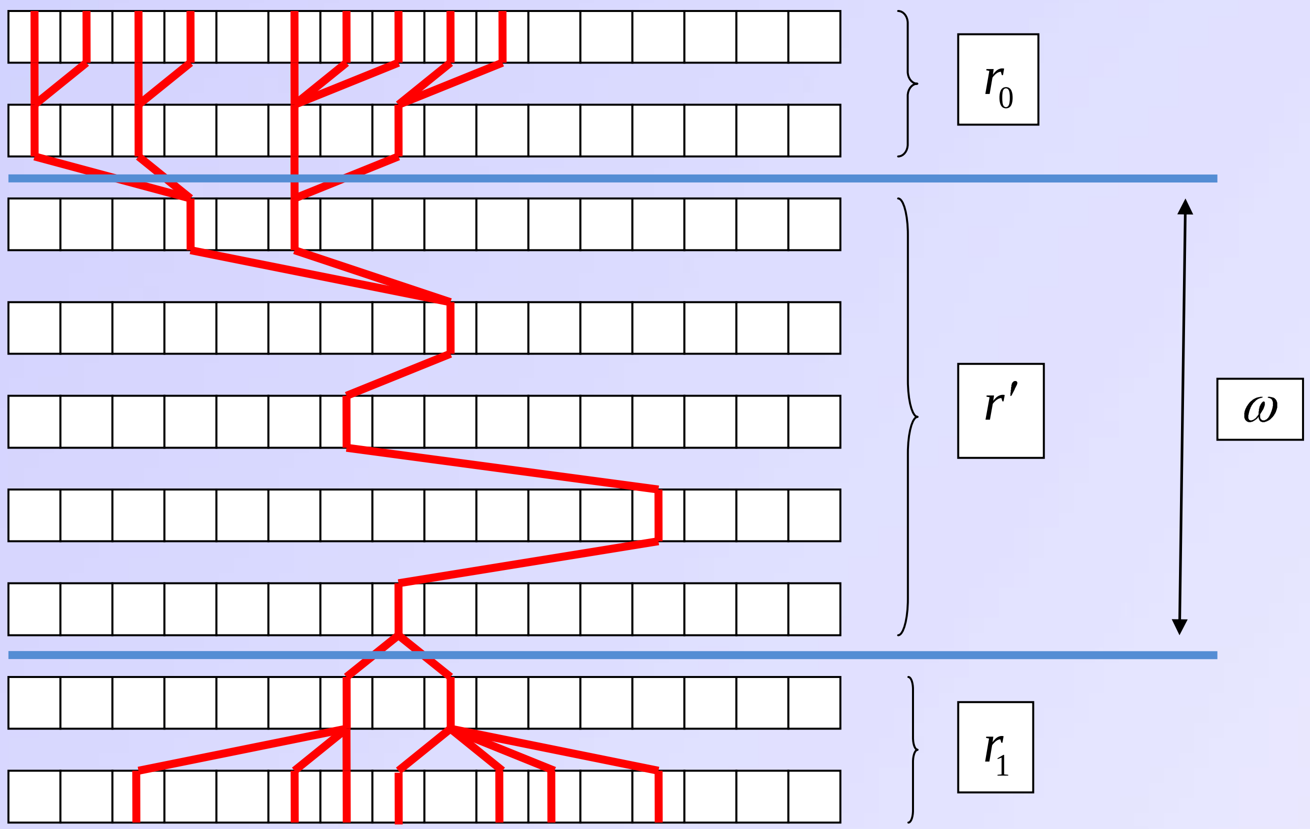
$$f'^{\,i,j}_{(k^{(i)},\ldots,k^{j})} = \prod_{b=i}^{j} g_{k^{(b)}},$$

$$B'_w\left(f'^{\,i,j}_{(k^{(i)},\ldots,k^{j})}\right) = \{\, b, z \in \{0,\ldots,n-1\}\times\{i,\ldots,j\} \mid$$

$$\exists\gamma^0 \in V_n, \gamma^1 = f'^{\,i,j}_{(k^{(i)},\ldots,k^{j})}\ \gamma^0,\ \gamma'^1 = f'^{\,i,j}_{(k^{(i)},\ldots,k^{z}\oplus\varepsilon_b,\ldots,k^{j})}\ \gamma^0,\ \gamma_w^1 \neq \gamma'^1_w \,\} -$$

- множество бит раундовых ключей, от которых существенно зависит w-й выходной бит функции $f'^{\,i,j}_{(k^{(i)},\ldots,k^{j})}$.

Линейный метод анализа (4)



$$r = r_0 + r'_\omega + r_1$$

Линейный метод анализа (5)

Мощность множества опробуемых ключей $\tilde{K}_\omega$ определяется из соотношения

$$\log_2 |\tilde{K}_\omega| = \left| \left(\bigcup_{i \in A^0} B_i \quad f_k^{1,r_0} \quad \right) \cup \left(\bigcup_{j \in A^{r'}} B_j \left(\quad f_k^{r-r_1,r} \quad {}^{-1} \right) \right) \right|.$$

Трудоемкость атаки есть

$$T_\omega = \frac{1}{\delta^2} \left| \tilde{K}_\omega \right| + \frac{|K|}{\left| \tilde{K}_\omega \right|}$$

операций шифрования. Трудоемкость атаки минимальна при $\left| \tilde{K}_\omega \right| = \delta \sqrt{|K|}$.

Пусть задано значение T_0, и Ω - множество линейных характеристик шифрсистемы А.

Определение 1. Шифрсистема А является стойкой относительно линейного метода анализа, если справедливо соотношение

$$\min_{\omega \in \Omega, \tilde{K}_\omega} T_\omega > T_0.$$

Построение линейных характеристик (1)

$l_{i,j,\beta}$ - линейный аналог j-й координатной функции $s_i^{\ j}$ подстановки s-бокса s_i, $i \in \{0,\ldots,d-1\}$, $j \in \{0,\ldots,m-1\}$ вида

$$\beta_{m-1}x_{m-1} \oplus \beta_{m-2}x_{m-2} \oplus \ldots \oplus \beta_0 x_0,$$

где $\beta \in V_m$.

Определим функцию $u_t : V_m \to E \times \; 0,1 \;, t \in \; 0,...,n-1$

$$u_t \;\; \beta \;\; = \;\; U, \delta \;\; ,$$

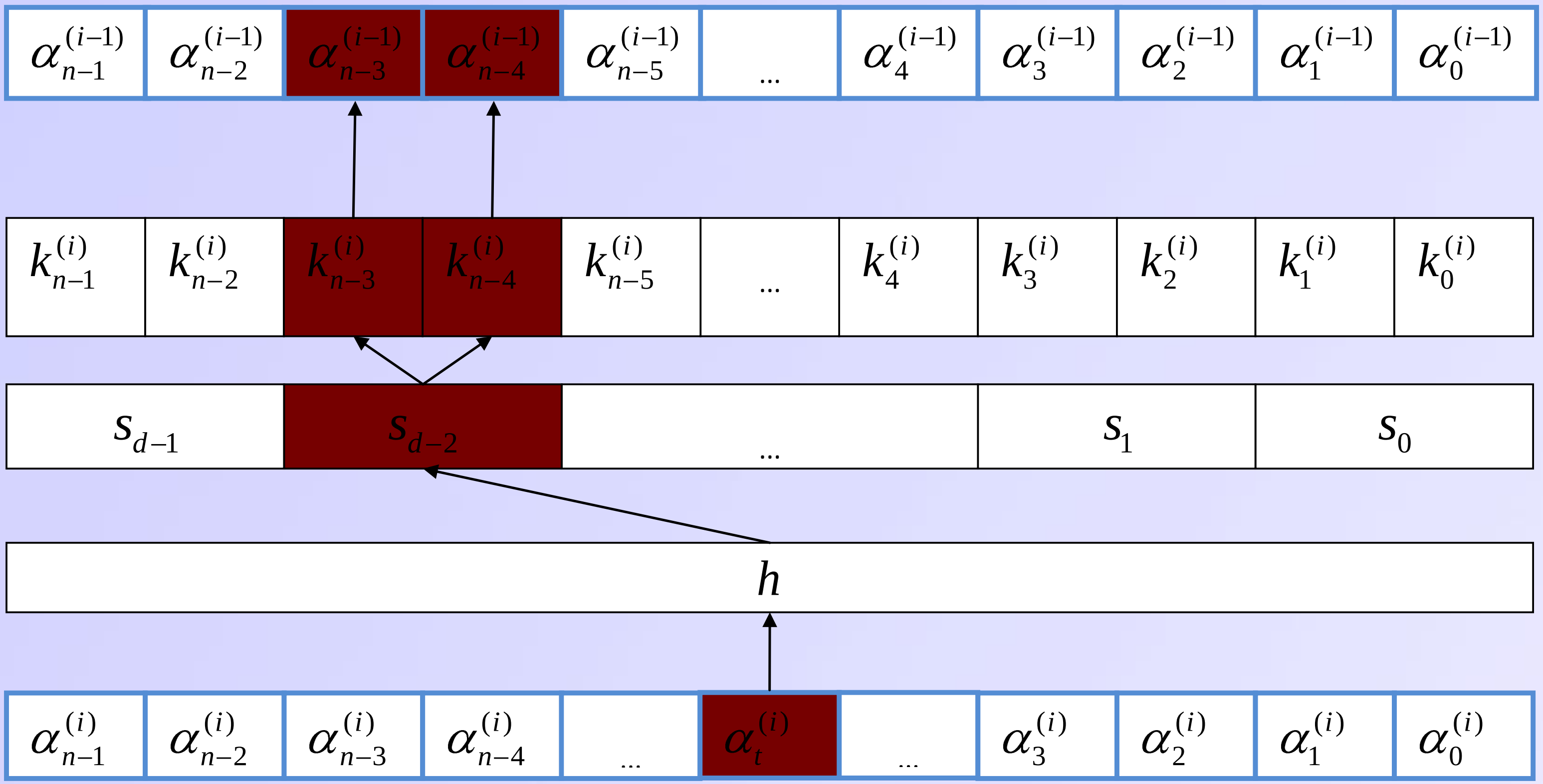
$$i = \left\lfloor \frac{\sigma^{-1} \;\; t}{m} \right\rfloor, j = \sigma^{-1} \;\; t \;\; (\bmod m)$$

$$U = \;\; w \in \{im,\ldots,(i+1)m-1\} \,|\, \beta_{w-im} = 1$$

$$\delta = \left| \frac{\| l_{i,j,\beta} \oplus s_i^{\ j} \;\; \|}{2^m} - \frac{1}{2} \right|,$$

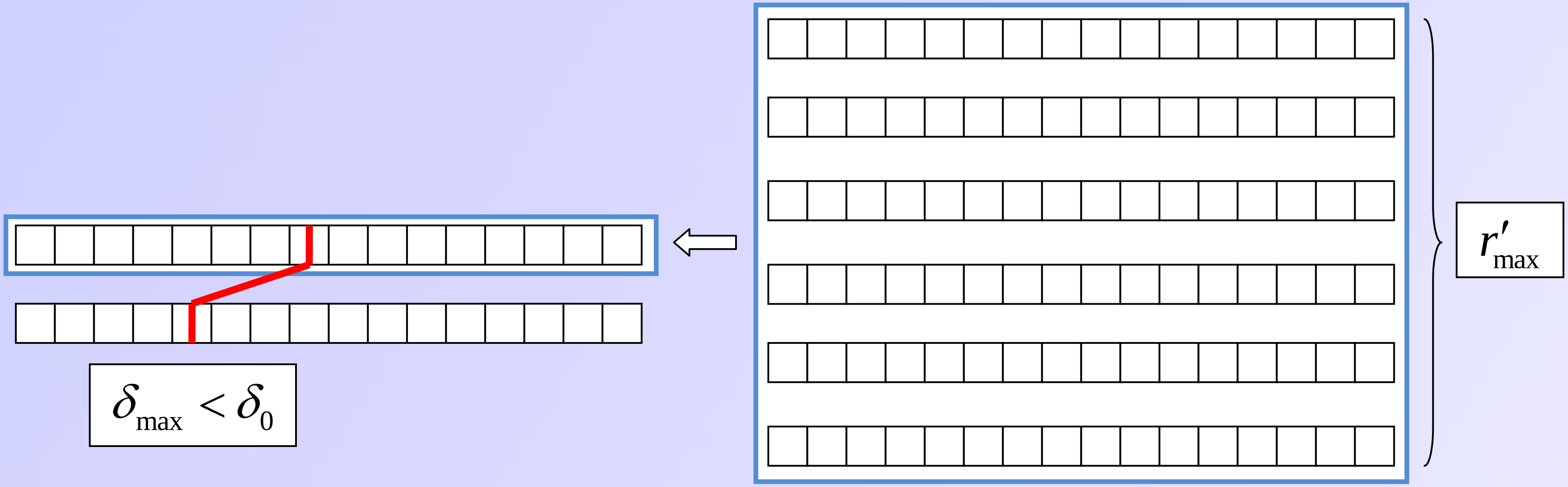
Трудоемкость построения таблицы значений функции u_t для всех t есть $T_u = 2^m n$.

Построение линейных характеристик (2)



$$U = \{n-3, n-4\}.$$

Построение линейных характеристик (3)

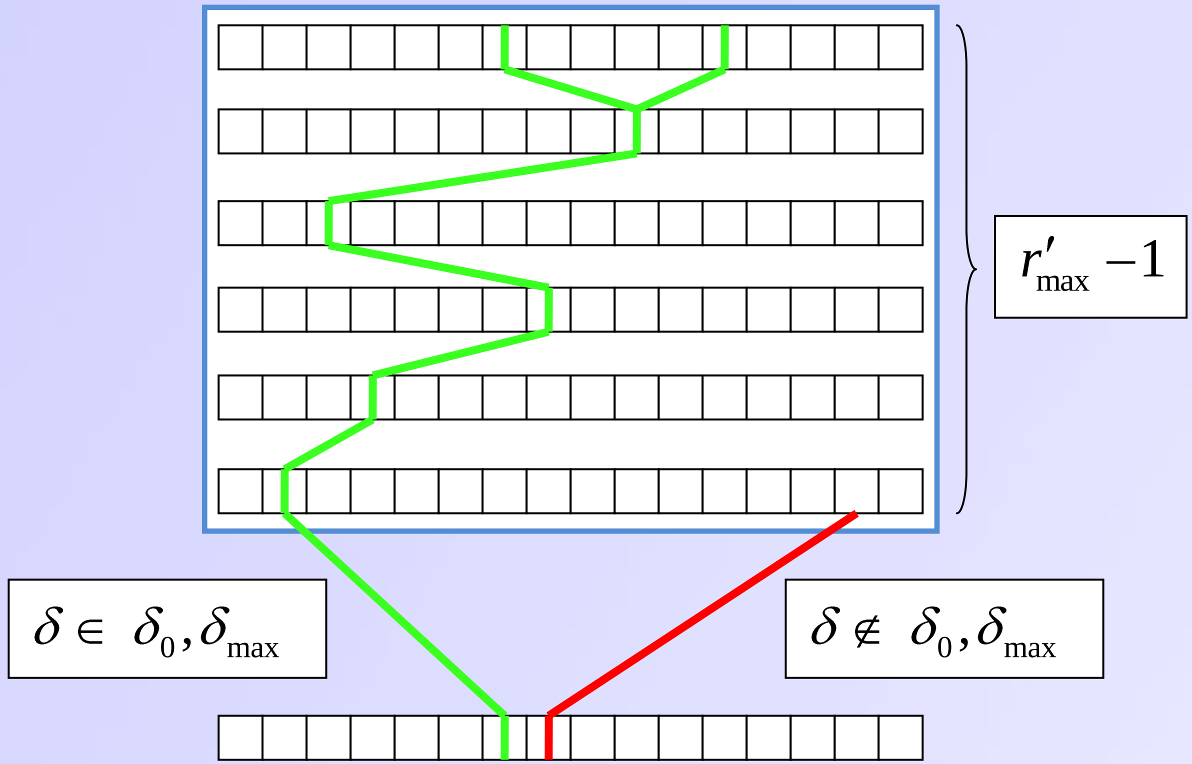


Алгоритм 1 итеративно строит линейную характеристику на наибольшее возможное число раундов. Длина линейной характеристики ограничена, поскольку

$$\delta > \delta_0, \delta_0 = 2^{-\frac{n}{2}}.$$

Трудоемкость алгоритма 1 ограничена сверху величиной $T_{\max}^{(1)} = 2^m nr$.

Построение линейных характеристик (4)



Алгоритм 2 итеративно, в обратном порядке, строит линейные характеристики, преобладания которых находятся в диапазоне δ_0, δ_{max} .

Построение АРК

Пусть $\tilde{r}$ - числа раундов, $\tilde{r} \in \mathrm{N}, \tilde{r} \ge \max\limits_{\omega \in \Omega} r'_{\omega}$,

$$O_{\omega} = \left(\bigcup_{i \in A^{0}} B'_{i} \left(f'^{\,1, r_0}_{k^{(1)}, \ldots, k^{(r_0)}} \right) \right) \cup \left(\bigcup_{j \in A^{r'}} B'_{j} \left(\left(f'^{\,r - r_1, r}_{k^{(r-r_1)}, \ldots, k^{(r)}} \right)^{-1} \right) \right),$$

$$n'_0 = \left| \bigcup_{\omega \in \Omega} O_{\omega} \right|.$$

Утверждение 1. Для шифрсистемы А с числом раундов $\tilde{r}$ и длиной ключа n'_0 существует такой АРК, что выполнено соотношение

$$\min_{\omega \in \Omega, \tilde{K}_{\omega}} \left| \frac{\left|\tilde{K}_{\omega}\right|}{\delta^2} + \frac{|K|}{\left|\tilde{K}_{\omega}\right|} \right| \ge T_0.$$

Вычислительный эксперимент (1)

- Выполнен для шифрсистемы SmallPresent, представленной в работе G. Leander в 2010

Вычислительный эксперимент (2)

Таблица 1. s-бокса $s = s_0,\ldots,s_0$, $s_0 = 4,10,9,2,13,8,0,14,6,11,1,12,7,15,5,3$.

Длина блока n	Минимальное число раундов r	Преобладание линейной характеристики	Длина ключа
12	6	2^{-6}	12
16	6	2^{-7}	16
20	7	2^{-9}	20
24	7	2^{-10}	24
28	7	2^{-13}	28
32	8	2^{-16}	32
36	9	2^{-17}	36
40	9	2^{-19}	40
44	9	2^{-22}	44
48	10	2^{-23}	48
52	10	2^{-24}	52
56	11	2^{-26}	56
60	11	2^{-30}	60
64	11	2^{-31}	64

Спасибо за внимание!