Московский государственный технический университет имени Н.Э. Баумана

О свойствах $\oplus_W$-марковских подстановок

Пудовкина М.

Алгоритм блочного шифрования $C_l(*, b)$

- $(X,*)$ – абелева группа;
- $\beta^b = b(\beta)$ для $b \in G \leq S(X)$.
- $W^b = \{\beta^b | \beta \in W\}$ для $W \subseteq X$.
- $C_l(*, b)$ – а.б.ш., раундовая функция $g: X^2 \to X$ задана

  $g: (x, k) \longmapsto (x * k)^b$, $g(x, k) = g_k(x) \quad \forall (x, k) \in X^2$,

  – $b \in S(X)$,

  – $f_k^{(l)} = g_{k_1} \dots g_{k_l}$ – функция зашифрования.
- XSL–а.б.ш., $b = sh$,

  – s – преобразование слоя перемешивания (s – боксы),
  h – преобразование линейного слоя.

Автоматная модель а.б.ш. $C_l(*, b)$

- Автомат $A = (K, X^2, g)$, g_k действует на биграммах.

$$(\alpha_1, \alpha_0)^{g_k} = \left(\alpha_1^{g_k}, \alpha_0^{g_k}\right), (\alpha_1, \alpha_0) \in X^2.$$

- Если раундовые ключи независимо и равновероятно выбираемы из X, то на множестве состояний X^2 – цепь Маркова $\xi^{(0)}, \xi^{(1)}, \dots, \xi^{(l)}$,

$p_{(\alpha_1,\alpha_0),(\beta_1,\beta_0)} = \mathrm{P}\left\{\left(\alpha_1^{g_k}, \alpha_0^{g_k}\right) = (\beta_1, \beta_0)\right\}$ – элемент матрицы вероятностей переходов.

(из теории вероятностных автоматов).

Укрупнения цепи Маркова

- $\theta^{(0)}, \theta^{(1)} \ldots, \theta^{(l)}$ – д.о. цепь Маркова с конечным множеством состояний Q и матрицей вероятностей переходов $q = \left(q_{i,j}\right)$.
- $\mathbf{U} = \{U_0, \ldots, U_{r-1}\}$ – разбиение Q;
- $\theta_{\mathbf{U}}^{(0)}$,…,$\theta_{\mathbf{U}}^{(l)}$ – последовательность дискретные с.в. на множестве $\{0, \ldots, r-1\}$:

  $\theta_{\mathbf{U}}^{(t)} = j \Leftrightarrow \theta^{(t)} \in U_j$ для $\forall j \in \{0, \ldots, r-1\}$, $t = 1, \ldots, l$.
- [КемС70]. Состояния цепи Маркова можно укрупнить посредством $\mathbf{U}$, если для $\forall$ распределения с.в. $\theta^{(0)}$ на Q п.с.в. $\theta_{\mathbf{U}}^{(0)}$,…, $\theta_{\mathbf{U}}^{(l)}$ – цепь Маркова, переходные вероятности которой не зависят от распр. с.в. $\theta^{(0)}$. Полученная цепь Маркова называется *укрупнённой*.

$*$- и $*_{\mathbf{W}}$- марковские алгоритмы блочного шифрования

- $\xi^{(0)}, \dots, \xi^{(l)}$ можно укрупнить $\mathbf{R} = \{R_\varepsilon | \varepsilon \in X\}$, где $(R_\varepsilon = \{(\alpha * \varepsilon, \alpha) | \alpha \in X\})$, если

$$p_{\theta,\varepsilon}(g|\alpha) = p_{\theta,\varepsilon}(g) \text{ для } \forall\, \theta, \varepsilon, \alpha \in X\,, \qquad (1)$$

$$p_{\theta,\varepsilon}(g) = |X|^{-1}|K|^{-1}|\{(\alpha, k) \in X \times K | (\theta * \alpha)^{g_k} = \varepsilon * \alpha^{g_k}\}|.$$

- [LaiMM91] Блочные алгоритмы, для которых справедливо (1), называются $*$ -*марковскими алгоритмами блочного шифрования*.
- $\xi_{\mathbf{R}}^{(0)}, \dots, \xi_{\mathbf{R}}^{(l)}$ – укрупненная цепь Маркова $\xi^{(0)}, \dots, \xi^{(l)}$ разбиением $\mathbf{R} = \{R_\varepsilon | \varepsilon \in X\}$.
- Назовём l-раундовый итерационный $*$-марковский алгоритм с марковской п.с.в. $\xi_{\mathbf{R}}^{(0)}, \dots, \xi_{\mathbf{R}}^{(l)}$ $*_{\mathbf{W}}$-*марковским* для $\mathbf{W}$, если $\xi_{\boldsymbol{R}_{\mathbf{W}}}^{(0)}, \dots, \xi_{\boldsymbol{R}_{\mathbf{W}}}^{(l)}$ является цепью Маркова.
  - $\mathbf{W} = \{W_0, \dots, W_{r-1}\}$ – разбиение X,
  - $\mathbf{R}_{\mathbf{W}} = \{R_W | W \in \mathbf{W}\}$, $R_W = \bigcup_{\varepsilon \in W} R_\varepsilon$.

$*_{\mathbf{W}}$-марковские алгоритмы

- [ПогП17]. *Для l -раундового $*$ -марковского а.б.ш. состояния марковской п.с.в. $\xi_{\mathbf{R}}^{(0)},\ldots,\xi_{\mathbf{R}}^{(l)}$ допускают укрупнение посредством разбиения* $\mathbf{W} \Leftrightarrow p_{\theta,W_c}(g) = a_{j,c}$ *для* $\forall (j,c) \in \{0,\ldots,r-1\}^2,\ \forall \theta \in W_j$ *и некоторых* $a_{j,c}$, $0 \le a_{j,c} \le 1$.
  - $p_{\theta,W_c}(g) = \sum_{\delta \in W_c} p_{\theta,\delta}(g)$, $\theta \in X$.
- Для $*_{\mathbf{W}}$-марковского алгоритма матрица $\left(p_{W_i,W_j}(f^{(l)})\right)$ вероятностей переходов блоков разбиения $\mathbf{W}$ равна $\prod_{i=1}^{l} p_{\mathbf{W}}(g)$,
  - $p_{W_i,W_j}(g) = a_{i,j}\ \ i,j \in \{0,\ldots,r-1\}$,
  - $p_{\mathbf{W}}(g) = \left(p_{W_i,W_j}(g)\right)$ – матрица вероятностей переходов блоков разностей.

$$\begin{pmatrix} p_{W_0,W_0}(g) & \ldots & p_{W_0,W_{r-1}}(g) \\ \vdots & \ldots & \vdots \\ p_{W_{r-1},W_0}(g) & \ldots & p_{W_{r-1},W_{r-1}}(g) \end{pmatrix}.$$

- Обобщение метода усеченных разностей.

$*_{\mathbf{W}}$-марковские преобразования

- $b \in S(X)$, $\mathbf{W} = \{W_0, \dots, W_{r-1}\}$ – разбиение X, $|X| \geq r \geq 2$.
  - $\hat{p}_{\varepsilon,\delta}(b) = |X|^{-1}\left|\{\alpha \in X \middle| (\theta * \alpha)^b = \varepsilon * \alpha^b\}\right|$, $\varepsilon, \delta \in X$;
    - $\hat{p}(b) = \left(\hat{p}_{\varepsilon,\delta}(b)\right)$ – матрица вероятностей переходов разностей b;
  - $\hat{p}_{\varepsilon,W_c}(b) = \sum_{\delta \in W_c} \hat{p}_{\varepsilon,\delta}(b)$, $c = 0, \dots, r-1$.
- Назовём $b \in S(X)$ $*_{\mathbf{W}}$-*марковским* для $\mathbf{W}$, если
  $\hat{p}_{\varepsilon,W_c}(b) = a_{j,c}$ для $\forall (j,c) \in \{0, \dots, r-1\}^2$, $\varepsilon \in W_j$ и некоторых $a_{j,c}$, $0 \leq a_{j,c} \leq 1$.
- $\hat{p}_{\mathbf{W}}(b) = \left(\hat{p}_{W_i,W_j}(b)\right)$ – матрица вероятностей переходов блоков,
  - $\hat{p}_{W_i,W_j}(b) = a_{i,j}$, $i, j \in \{0, \dots, r-1\}$.
- Для $C_l(*, b)$ справедливо равенство $\hat{p}(b) = p(g)$.

Достаточные условия на s-боксы и линейное преобразование h, при которых XSL-алгоритм $\bigoplus_{\mathbf{W}}$-марковский

Утверждение 1. *Пусть* $d, m \in \mathbb{N}, d > 1, n = d \cdot m,$

$$s = (s_{d-1}, \dots, s_0) \in S(V_m)^d, h \in GL_n(2),$$

и частичная раундовая функция $g_k \in S(V_n)$ *задана условием*

$$g_k : \alpha \mapsto (\alpha \oplus k)^{sh} \text{ для } \forall\ (\alpha, k) \in V_n^2.$$

Пусть также $\mathbf{W}^{(j)}$ *– такое разбиение пространства* V_m *на* $r^{(j)}$ *блоков, что* s*-бокс* s_j *является* $\bigoplus_{\mathbf{W}^{(j)}}$*-марковским для* $j = 0, \dots, d-1$. *Тогда, если* h *сохраняет разбиение*

$$\bar{\mathbf{W}}_d = \mathbf{W}^{(d-1)} \times \dots \times \mathbf{W}^{(0)},$$

то $\bigoplus$*-марковский алгоритм блочного шифрования с раундовой функцией* g *также является* $\bigoplus_{\bar{\mathbf{W}}_d}$*-марковским.*

Аффинная эквивалентность и $\bigoplus_{\mathbf{W}}$-марковость

- V_n – n-мерное пространство над полем $GF(2)$.
- Подстановки $s, s' \in S(V_n)$ называются *аффинно-эквивалентными*, если $\exists$ такие $h^{(1)}, h^{(2)} \in AGL_n(2)$, что $s' = h^{(1)} s h^{(2)}$.
- $h = (h_0, \delta) \in AGL_n(2)$ задано $h\colon \alpha \mapsto \alpha^{h_0} \oplus \delta$.
- $G_{\mathbf{W}} = \{g \in G | \mathbf{W}^g = \mathbf{W}\}$ – для разбиения $\mathbf{W}$ пространства V_n и $G \leq S(V_n)$.
- **Утверждение 2**. *Пусть* $\mathbf{W}$ – *нетривиальное разбиение пространства* V_n, s – *произвольная* $\bigoplus_{\mathbf{W}}$-*марковская подстановка из* $S(V_n)$. *Тогда* $s' = asb$ – $\bigoplus_{\mathbf{W}^{b_0}}$-*марковская подстановка для разбиения* $\mathbf{W}^{b_0}$ *пространства* V_n *и* $\forall$ *таких аффинных преобразований* $a = (a_0, \delta)$, $b = (b_0, \delta')$ *из* $AGL_n(2)$, *что* $a_0 b_0 \in GL_{\mathbf{W}}(2)$.

Связь между $\oplus_{\mathbf{W}}$-марковостью подстановки и группой автоморфизмов её орграфа

- $V_n^{\times} = V_n \backslash \{\vec{0}_n\}$.
- $\bar{\Gamma}(b) = (V_n^{\times}, Y)$ – (взвешенный) орграф (с петлями) подстановки $b \in S(V_n)$, множество дуг Y задаётся $(2^n - 1) \times (2^n - 1)$-матрицей смежности $\mathbf{q}(b) = (q_{i,j}(b))$, где
  - $q_{i,j}(b) = 1$, если $\hat{p}_{i,j}(b) \neq 0$,
  - $q_{i,j}(b) = 0$, если $\hat{p}_{i,j}(b) = 0$,

  при этом дуга (i, j) имеет вес $\hat{p}_{i,j}(b)$, если $\hat{p}_{i,j}(b) \neq 0$.
- $\bar{\Gamma}(b)$ – (взвешенный с петлями) граф для инволюции b.
- **Теорема 3.** *Пусть b – произвольная подстановка на V_n. Тогда для $\forall$ элемента*

$$g = \left(\alpha_1^{(1)}, \dots, \alpha_{d_1}^{(1)}\right) \cdot \dots \cdot \left(\alpha_1^{(r)}, \dots, \alpha_{d_r}^{(r)}\right) \in \mathrm{Aut}\bar{\Gamma}(b)$$

подстановка b является $\oplus_{\mathbf{W}^{(g)}}$-марковской для разбиения $\mathbf{W}^{(g)} = \{W_0, \dots, W_r\}$, где

$$W_0 = \{\vec{0}_n\},\ W_j = \left\{\alpha_1^{(j)}, \dots, \alpha_{d_j}^{(j)}\right\} \text{ для } j = 1, \dots, r.$$

Разностно d-равномерные преобразования

- [Nyb93]. Для числа $d \in \mathbb{N}$ преобразование $b: V_n \to V_n$ называется *разностно d-равномерным* (differentially d-uniform), если

$$\max\left\{\hat{p}_{\varepsilon,\delta}(b)\middle|(\varepsilon,\delta) \in (V_n^{\times})^2\right\} = 2^{-n}d.$$

Разностно 2-равномерное преобразование также называется APN-*преобразованием*.

- Пусть $s \in S(V_n)$, s – произвольная APN-подстановка,
  $s' = asb,\ a = (a_0, \delta), b = (b_0, \delta') \in AGL_n(2), a_0^{-1} = b_0.$
- Тогда $a_0 g a_0^{-1} \in \mathrm{Aut}\bar{\Gamma}(s')$ для $\forall\ g \in \mathrm{Aut}\bar{\Gamma}(s)$.
- Если орграфы $\bar{\Gamma}(s)$, $\bar{\Gamma}(s')$ изоморфны, то $a_0 \in \mathrm{Aut}\bar{\Gamma}(s)$.
- Если $g = \left(\alpha_1^{(1)}, \dots, \alpha_{d_1}^{(1)}\right) \dots \left(\alpha_1^{(r)}, \dots, \alpha_{d_r}^{(r)}\right)$, то s – $\bigoplus_{\mathbf{W}^{(g)}}$-марковская, s' – $\bigoplus_{\mathbf{W}'^{(g)}}$-марковская, где

$$\mathbf{W}^{(g)} = \{W_0, \dots, W_r\}, \mathbf{W}'^{(g)} = \{W'_0, \dots, W'_r\}, W_j^{b_0} = W'_j.$$

$$W_0 = W'_0 = \{\vec{0}_n\}, W_j = \left\{\alpha_1^{(j)}, \dots, \alpha_{d_j}^{(j)}\right\}.$$

Пример для APN-подстановки

- $m = 3$, $GF(2^3) = GF(2)[x]/(x^3 \oplus x \oplus 1)$,

$$s: \alpha \mapsto \alpha^{-1}, \text{ если } \alpha \neq \vec{0}_3, \quad s: \vec{0}_3 \mapsto \vec{0}_3.$$

- Матрица $\mathbf{q}(s)$ симметрическая,

$\mathrm{Aut}\bar{\Gamma}(s) =$

$= \{e, (4,6)(5,7), (2,4)(3,5), (2,6)(3,7), (2,4,6)(3,5,7), (2,6,4)(3,7,5)\}$

- Полным перебором по всем $a_0, b_0 \in GL_3(2)$ получено, что для $\forall\ a = (a_0, \delta),\ b = (b_0, \delta') \in AGL_3(2)$, преобразование $s' = asb$ удовлетворяет следующим свойствам:
  - $|\mathrm{Aut}\bar{\Gamma}(s')| \in \{2,3,4,6\}$;
  - s' – $\oplus_{\mathbf{W}'}$ -марковская для некоторого такого нетривиального разбиения $\mathbf{W}'$, что $\exists$:
    - 2 блока мощности 2, 4 блока мощности 1;
    - 2 блока мощности 3, 2 блока мощности 1;
    - 3 блока мощности 2, 2 блока мощности 1.

$b - \bigoplus_{\mathbf{W}}$-марковская подстановка, $\mathrm{Aut}\bar{\Gamma}(b) = \{e\}$

Утверждение 4. *Пусть* $b \in S(V_n)$ *и* $\exists$ *такое* $W \subseteq V_n^{\times}$, *что* $\hat{p}_{\theta,W}(b) = \hat{p}_{\theta',W}(b)$ *для* $\forall\ (\theta, \theta') \in W^2 \cup (V_n^{\times} \backslash W)^2$. *Тогда подстановка* b *является* $\bigoplus_{\mathbf{W}}$*-марковской для разбиения* $\mathbf{W} = \left\{\{\vec{0}_n\}, W, V_n^{\times} \backslash W\right\}$.

Кроме того, если (взвешенный) подграф $\bar{\Gamma}_W(b)$ *орграфа* $\bar{\Gamma}(b)$ *с множеством вершин* $W \subseteq V_n^{\times}$ *таков, что* $\mathrm{Aut}\bar{\Gamma}_W(b) \neq \{e\}$, *тогда для*

$$\forall g = \left(\alpha_1^{(1)}, \ldots, \alpha_{d_1}^{(1)}\right) \ldots \left(\alpha_1^{(r)}, \ldots, \alpha_{d_r}^{(r)}\right) \in \mathrm{Aut}\bar{\Gamma}_W(b)$$

подстановка b *также является* $\bigoplus_{\mathbf{W}(g)}$*-марковской для разбиения*

$$\mathbf{W}^{(g)} = \left\{\{\vec{0}_n\}, W_1^{(g)}, \ldots, W_r^{(g)}, V_n^{\times} \backslash W\right\},$$

где

$$W_j^{(g)} = \left\{\alpha_1^{(j)}, \ldots, \alpha_{d_j}^{(j)}\right\} \text{ для } j = 1, \ldots, r, \quad W = \cup_{j=1}^{r} W_j^{(g)}.$$

Пример для разностно 4-равномерной подстановки

- $m = 4$, $GF(2^4) = GF(2)[x]/(x^4 \oplus x \oplus 1)$,
- $s: \alpha \mapsto \begin{pmatrix} 1\,1\,1\,0 \\ 1\,1\,0\,1 \\ 1\,0\,1\,1 \\ 0\,1\,1\,1 \end{pmatrix} \alpha^{-1}$, если $\alpha \neq \vec{0}_4$, $\quad s: \vec{0}_4 \mapsto \vec{0}_4$.
- $\mathrm{Aut}\bar{\Gamma}(s) = \{e\}$.
- Непосредственной проверкой для подмножества $W = \{1,6,7\}$ показывается, что:
  - $\hat{p}_{\theta,W}(b) = \hat{p}_{\theta',W}(b)$ для $\forall\ (\theta, \theta') \in W^2 \cup (V_n^{\times} \backslash W)^2$;
  - $(1,6,7) \in \mathrm{Aut}\bar{\Gamma}_W(s)$.
- s – $\oplus_{\mathbf{W}}$-марковская подстановка для разбиения $\mathbf{W} = \left\{\{\vec{0}_n\}, W, V_n^{\times} \backslash W\right\}$.

Спасибо за внимание!