Ежегодная международная научно-практическая конференция
«РусКрипто’2020»

О групповых свойствах TH-обобщения алгоритма Фейстеля

Пудовкина Марина
профессор, МГТУ им. Н.Э. Баумана

Операция сплетения групп подстановок

Опр 1. Пусть $G \leq S(X), H \leq S(X)$, $G^J = \{g | g: J \to G\}$.

Множество $\{(g,h)|(g,h) \in G^J \times H\}$ относительно операции

$$(g_1,h_1)(g_2,h_2) = (g, h_1h_2),$$

где

- $(g_1,h_1)(g_2,h_2) \in G^J \times H$,
- $g \in G^J$ задано $g(j) = g_1(j)g_2(j^{h_1})$ для $\forall j \in J$,

является группой, которая называется *сплетением* группы G группой H

- обозначается $G \wr H$.

Операция экспоненцирования групп подстановок

- $B^U = \{f | U \to B\}$

Опр 2. *Экспоненцированием группы G группой H* называется группа подстановок степени $|X|^{|J|}$ множества $X^J = \{\varphi | \varphi: J \to X\}$ абстрактно изоморфная сплетению $G \wr H$ и задаваемая действием на множестве X^J:

$$(g,h): \varphi(j) \longmapsto \varphi\left(j^{h^{-1}}\right)^{g\left(j^{h^{-1}}\right)} \text{ для } \forall j \in J,$$

где $(g,h) \in G \wr H$, $\varphi \in X^J$

- обозначение $G \uparrow H$

Операция экспоненцирования групп подстановок

- Группа $G \uparrow H$ имеет нормальный делитель

$$N = \{(g, 1) | g \in G^J\} \cong \underbrace{G \times \cdots \times G}_{|J|}$$

причем $G \uparrow H/N \cong H$.

- Известна

Теорема. *Группа $G \uparrow H$ примитивна тогда и только тогда, когда группа G примитивна и нерегулярна, а группа H транзитивна.*

- В терминах подгрупп группы экспоненцирования в классификационной теореме О'Нана-Скотта описывается ряд классов примитивных групп.

Аддитивная абелева группа

- Пусть $(X, +)$ – конечная абелева группа,
- 0 – её нулевой элемент, $0_m = (\underbrace{0, \dots, 0}_{m})$.
- $(X, +)$ может являться аддитивной группой поля $GF(p)$ или кольца $\mathbb{Z}_p$, $p \geq 2$.

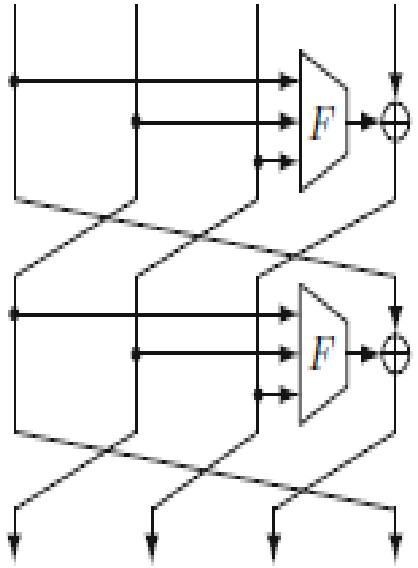
Неавтономные регистры сдвига (SH-обобщения)

Опр. Неавтономный регистр сдвига (НРС) реализует преобразование множества X^m с частичными функциями переходов $g_{h,k}: X^m \to X^m$,

$$g_{h,k}: (\alpha_1, \dots, \alpha_m) \longmapsto (\alpha_2, \dots, \alpha_m, \alpha_1 + h(\alpha_1, \dots, \alpha_m) + k),$$

где $k \in X, h: X^{m-1} \to X$.

- совпадает с обобщенным SH (source-heavy) алгоритмом Фейстеля
- RC2, SPEED
- алгоритмы блочного шифрования на основе SHA-1, SHA-2



Неавтономные регистры сдвига (SH-обобщения)

Опр. Неавтономный регистр сдвига (НРС) реализует преобразование множества X^m с частичными функциями переходов $g_{h,k}: X^m \to X^m$,

$$g_{h,k}: (\alpha_1, \dots, \alpha_m) \longmapsto (\alpha_2, \dots, \alpha_m, \alpha_1 + h(\alpha_1, \dots, \alpha_m) + k),$$

где $k \in X, h: X^{m-1} \to X$.

Опр. Группа $G^{(m)}(h) = \langle g_{h,k} | k \in X \rangle$, порождённая всеми частичными функциями, называется *группой неавтономного регистра сдвига*.

Неавтономные регистры сдвига (SH-обобщения)

- Пусть $v_\beta^{(i,m)}: X^m \to X^m,\ \beta \in X, i \in \{1, \dots, m\}$,

$$v_\beta^{(i,m)}: (\alpha_1, \dots, \alpha_m) \longmapsto (\alpha_1, \dots, \alpha_{i-1}, \alpha_i + \beta, \alpha_{i+1}, \dots \alpha_m)$$

- $J(h) = \{j_1, \dots, j_{q(h)}\}$ – множество номеров всех существенных переменных $x_{j_1}, \dots, x_{j_{q(h)}}$ функции $h(x_1, \dots, x_{m-1})$,
  - $J(h) \subset \{1, \dots, m-1\}$,
  - $q(h) = |J(h)|$,
  - $d = d(h) = \text{НОД}\{j_1, \dots, j_{q(h)}, m\}$.

Неавтономные регистры сдвига (SH-обобщения)

- Пусть $d > 1$.
- Положим $l = l(h) = m/d$,
- Функцию $h^{(d)}: X^{l-1} \longrightarrow X$ зададим условием

$$h^{(d)}(\beta_1, \dots, \beta_{l-1}) = h(\gamma_1, \dots, \gamma_{m-1})$$

для $\forall(\beta_1, \dots, \beta_{l-1}) \in X^{l-1}$, где

- $\gamma_j = \beta_i$, если $j/d = i$, $i \in \{1,2, \dots, l-1\}$,
- $\gamma_j = 0$, если $j/d \notin \{1,2, \dots, l-1\}$,

Неавтономные регистры сдвига (SH-обобщения)

- Множество функций $\Phi = \{\varphi \mid \varphi: \{1, \dots, d\} \to X^l\}$.
- Для каждого $\alpha = (\alpha_1, \dots, \alpha_m) \in X^m$ положим $\psi: \alpha \to \varphi_\alpha$, где

$$\varphi_\alpha: i \longmapsto (\alpha_i, \alpha_{i+d}, \dots, \alpha_{i+(l-1)d}).$$

- ψ есть биекция между множествами Φ и X^m.

Основной результат 1 (SH-обобщение)

Теорема 1. *Пусть* $m \geq 3, d > 1, l \geq 1, m = ld$. *Тогда*:

- $\psi^{-1} G^{(m)}(h)\psi \leq G^{(l)}(h^{(d)}) \uparrow \langle (d, d-1, \dots, 1) \rangle$,

группа $G^{(m)}(h)$ *подобна подгруппе экспоненцирования групп* $G^{(l)}(h^{(d)})$ *и* $\langle (d, d-1, \dots, 1) \rangle$;

- *группа*

$$Q = \left\langle g_{h,0}^{-j} v_{\beta}^{(m,m)} g_{h,0}^{j}, g_{h,0}^{d} \,\middle|\, j \in \{0, \dots, d-1\}, \beta \in X \right\rangle$$

индуцирует на множествах

$$\Omega_i = \left\{ (\delta_i, \delta_{i+d}, \dots, \delta_{i+(l-1)d}) \middle| (\delta_i, \delta_{i+d}, \dots, \delta_{i+(l-1)d}) \in X^l \right\}$$

группы Q_i *подобные* $G^{(l)}(h^{(d)})$, $i = 1, \dots, d$;

Основной результат 1 (SH-обобщение)

Теорема 1. *Пусть* $m \geq 3, d > 1, l \geq 1, m = ld$. *Тогда*:

- $Q \triangleleft G^{(m)}(h)$ *и* $G^{(m)}(h)/Q \cong \langle (d, d-1, \dots, 1) \rangle$;
- *если* M – *минимальный нормальный делитель группы* $G^{(l)}(h^{(d)})$, *содержащий элемент* $v_\beta^{(l,l)}$ *для каждого* $\beta \in X$, *то*

$$\left|G^{(m)}(h)\right| = d|M|^d\left|G^{(l)}(h^{(d)})/M\right|;$$

- *группа* $G^{(m)}(h)$ *примитивна, если примитивна и нерегулярна группа* M.

Неавтономные регистры сдвига (ТН-обобщения)

- Пусть $J = \{j_1, \dots, j_q\} \subseteq \{1, \dots, m-1\}$, $q = |J|$,
  - $1 \le j_1 < \cdots < j_q \le m-1$
- Для $\forall j_i \in J$ отображение $h_i: X^2 \to X$ задано условием

$$h_i: (\alpha, k_i) \longmapsto \hat{h}_i(\alpha) + k_i \text{ для } \forall (\alpha, k_i) \in X^2,$$

где $\hat{h}_i: X \to X$, $i = 1, \dots, q$.

Положим

- $d = \text{НОД}\{j_1, \dots, j_q, m\}$, $l = m/d$,
- $h = (h_1, \dots, h_q)$.

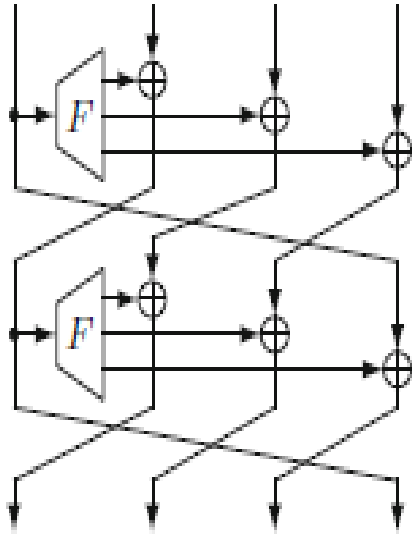
Неавтономные регистры сдвига (TH-обобщения)

- Частичная раундовая функция $g_{J,h,k}: X^m \to X^m$, обобщенного TH-алгоритма Фейстеля, задана для $\forall k = (k_1, \dots, k_q) \in X^q$ условием

$$g_{J,h,k}: (\alpha_1, \dots, \alpha_m) \longmapsto$$

$$\longmapsto \left(\alpha_2, \dots, \alpha_{j_1}, \alpha_{j_1+1} + h_1(\alpha_1, k_1), \alpha_{j_1+2}, \dots, \alpha_{j_q},\right.$$

$$\left.\alpha_{j_q+1} + h_q(\alpha_1, k_q), \alpha_{j_q+2}, \dots, \alpha_m, \alpha_1\right)$$



- MARS , BEAR, LION

Неавтономные регистры сдвига (ТН-обобщения)

- Частичная раундовая функция $g_{J,h,k}: X^m \to X^m$, обобщенного ТН-алгоритма Фейстеля, задана для $\forall k = (k_1, \dots, k_q) \in X^q$ условием

$$g_{J,h,k}: (\alpha_1, \dots, \alpha_m) \longmapsto$$
$$\longmapsto (\alpha_2, \dots, \alpha_{j_1}, \alpha_{j_1+1} + h_1(\alpha_1, k_1), \alpha_{j_1+2}, \dots, \alpha_{j_q},$$
$$\alpha_{j_q+1} + h_q(\alpha_1, k_q), \alpha_{j_q+2}, \dots, \alpha_m, \alpha_1)$$

- $G^{(m)}(J,h) = \langle g_{J,h,k} | k \in X^q \rangle$ – группа неавтономного регистра сдвига.

Основной результат 2 (ТН-обобщение)

Теорема 2. *Пусть* $m \geq 4, J = \{j_1, \dots, j_q\}, 2 \leq j_1 < \dots < j_q \leq m,$ $d > 1, J^{(d)} = \{j_1/d, \dots, j_q/d\}, l = m/d > 1.$

Тогда:

- $\psi^{-1} G^{(m)}(J, h)\psi \leq G^{(l)}(J^{(d)}, h) \uparrow \langle (d, d-1, \dots, 1) \rangle,$

группа $G^{(m)}(J, h)$ *подобна подгруппе экспоненцирования групп* $G^{(l)}(J^{(d)}, h)$ *и* $\langle (d, d-1, \dots, 1) \rangle$;

Основной результат 2 (ТН-обобщение)

Теорема 2. *Пусть* $m \geq 4, J = \{j_1, \dots, j_q\}, 2 \leq j_1 < \dots < j_q \leq m,$ $d > 1, J^{(d)} = \{j_1/d, \dots, j_q/d\}, l = m/d > 1.$

- *группа*

$$Q = \left\langle g_{J,h,0_q}^{-i} v_{\beta_1}^{(j_1,m)} \dots v_{\beta_q}^{(j_q,m)} g_{J,h,0_q}^{i}, g_{J,h,0_q}^{d} \,\middle|\, i \in \{0, \dots, d-1\}, \beta_1, .., \beta_q \in X \right\rangle$$

индуцирует на множествах

$$\Omega_i = \left\{ (\delta_i, \delta_{i+d}, \dots, \delta_{i+(l-1)d}) \middle| (\delta_i, \delta_{i+d}, \dots, \delta_{i+(l-1)d}) \in X^l \right\}$$

группы Q_i *подобные* $G^{(l)}(J^{(d)}, h), i = 1, \dots, d;$

Основной результат 2 (ТН-обобщение)

Теорема 2. *Пусть* $m \geq 4, J = \{j_1, \dots, j_q\}, 2 \leq j_1 < \cdots < j_q \leq m,$ $d > 1, J^{(d)} = \{j_1/d, \dots, j_q/d\}, l = m/d > 1.$

Тогда:

- *если* M *– минимальный нормальный делитель группы* $G^{(l)}(J^{(d)}, h)$, *содержащий элемент* $v_\beta^{(t,l)}$ *для каждых* $t \in J^{(d)}$, $\beta \in X$, *то*

$$\left|G^{(m)}(J,h)\right| = d|M|^d\left|G^{(l)}(J^{(d)},h)/M\right|;$$

- *группа* $G^{(m)}(J,h)$ *примитивна, если примитивна и нерегулярна группа* M.

Экспоненцирование и неавтономные регистры сдвига (SH, TH-обобщения)

Благодарю за внимание!!!