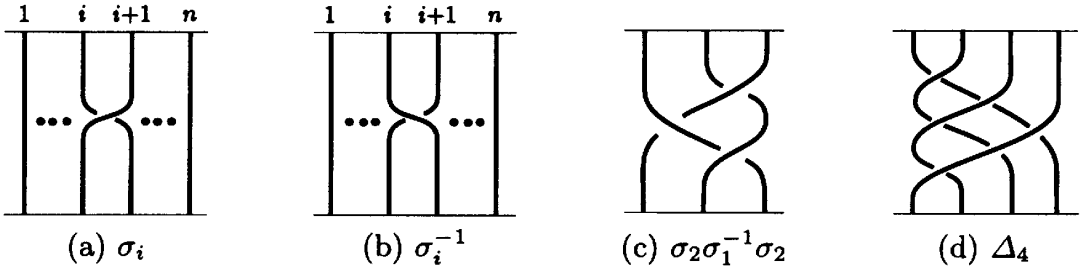
Жуков А.Е.

Нечисловые алгебраические системы и криптография с открытым ключом

(слайды обзорного доклада)

Группы кос

$$B_n = \left\langle \sigma_1,\ldots,\sigma_{n-1} \;\middle|\; \begin{array}{ll} \sigma_i\sigma_j\sigma_i = \sigma_j\sigma_i\sigma_j, & |i-j|=1 \\ \sigma_i\sigma_j = \sigma_j\sigma_i, & |i-j|\geq 2 \end{array} \right\rangle$$



(a) σ_i (b) σ_i^{-1} (c) $\sigma_2\sigma_1^{-1}\sigma_2$ (d) Δ_4

Fig. 1. An example of braids

$$\Delta_4 = \sigma_1\sigma_2\sigma_3\underline{\sigma_1\sigma_2\sigma_1} = \sigma_1\underline{\sigma_2\sigma_3\sigma_2}\sigma_1\sigma_2 = \underline{\sigma_1\sigma_3}\sigma_2\underline{\sigma_3\sigma_1}\sigma_2 =$$
$$= \sigma_3\underline{\sigma_1\sigma_2\sigma_1}\sigma_3\sigma_2 = \sigma_3\sigma_2\sigma_1\underline{\sigma_2\sigma_3\sigma_2} = \sigma_3\sigma_2\sigma_1\sigma_3\sigma_2\sigma_3$$

$$B_n \subset B_m, \quad m < n$$

$$B_{l+r} = \langle \sigma_1,\ldots,\sigma_{l+r-1} \rangle \supset B_l = \langle \sigma_1,\ldots,\sigma_{l-1} \rangle, B_r = \langle \sigma_l,\ldots,\sigma_{l+r-1} \rangle$$

Сопряженность : $x \sim y$

$$\Leftrightarrow \exists a : x^a = axa^{-1} = y$$

Проблема сопряженности.

1. *Дано*: $x, y \in B_n$

Определить: $x \sim y$?

Проблема поиска сопрягающего элемента.

2. *Дано*: $x, y \in B_n, \quad x \sim y$

Определить: $a \in B_n : axa^{-1} = y$

Обобщенная проблема поиска сопрягающего элемента.

3. *Дано*: $x, y \in B_n, \quad y = bxb^{-1}, \quad b \in B_m, \quad m < n, \quad b - неизвестен$

Определить: $a \in B_m : axa^{-1} = y$

Проблема сопряженной разрешимости.

4. *Дано*: $x, y \in B_n, \quad y = bxb^{-1}, \quad b \in B_m, \quad m < n$

Определить: $a_1, a_2 \in B_n : a_1 x a_2 = y$

Проблема извлечения корня.

5. *Дано*: $y \in B_n, \quad y = x^p, \quad x - неизвестен$

Определить: $z \in B_n : y = z^p$

Однонаправленная функция

$$f : B_l \times B_{l+r} \to B_{l+r} \times B_{l+r}$$

$$f(a,x) = (axa^{-1}, x)$$

Протокол выработки секретного ключа

$\boldsymbol{A}$: $a \in B_l$ $\quad y_1 = axa^{-1} \mapsto \boldsymbol{B}$

$\boldsymbol{B}$: $b \in B_r$ $\quad y_2 = bxb^{-1} \mapsto \boldsymbol{A}$

$\boldsymbol{A}$: $K = ay_2a^{-1} = abxb^{-1}a^{-1}$

$\boldsymbol{B}$: $K = by_1b^{-1} = baxa^{-1}b^{-1} = abxb^{-1}a^{-1}$

Криптосистема с открытым ключом

$$H : B_{l+r} \to \{0,1\}^k$$

$$x \in B_{l+r}, \quad a \in B_l$$

$$\begin{cases} \textbf{\textit{открытый}} \quad \textbf{\textit{ключ}}: \quad \left(x, y = axa^{-1}\right) \\ \textbf{\textit{секретный}} \quad \textbf{\textit{ключ}}: \quad a \end{cases}$$

Шифрование :

$m \in \{01\}^k, \quad b \in B_r.$

$(c,d): \quad d = bxb^{-1}, \quad c = m \oplus H(byb^{-1})$

Расшифрование :

$ada^{-1} = abxb^{-1}a^{-1} = baxa^{-1}b^{-1} = byb^{-1}$

$\Rightarrow m = c \oplus H(byb^{-1})$

***Диффи – Хеллман*:**

$$\boldsymbol{A}: \quad y_1 = x^a \mapsto \boldsymbol{B}$$

$$\boldsymbol{B}: \quad y_2 = x^b \mapsto \boldsymbol{A}$$

$$\boldsymbol{A}: \quad K = (y_2)^a = (x^b)^a = x^{ab}$$

$$\boldsymbol{B}: \quad K = (y_1)^b = (x^a)^b = x^{ab}$$

$$\forall a \in A, \quad \forall b \in B:$$

$$\{E_a(x), b\} \Rightarrow E_{ab}(x); \quad \{E_b(x), a\} \Rightarrow E_{ab}(x)$$

$$\{E_a(x), E_b(x)\} \Rightarrow E_{ab}(x)$$

$$\boldsymbol{ЭльГамаль}: \begin{cases} открытый \quad ключ: \left(g, g^a\right) \\ открытый \quad текст: \quad m \\ зашифрованное \quad сообщение: \\ \left(g^{ab} \cdot m, g^b\right) или \left(g^{ab} \oplus m, g^b\right) \end{cases}$$

$$\forall a \in A, \quad \forall b \in B:$$

$$\{E_a, b\} \Rightarrow E_{ab}^{-1}; \quad \{E_b, a\} \Rightarrow E_{ab}^{-1}$$

$$\{E_a, E_b\} \Rightarrow E_{ab}^{-1}$$

Полупрямое произведение групп G и H

$$\mathrm{Aut}G \supseteq \mathrm{Inn}G = \left\{ f_g \in \mathrm{Aut}G \,\middle|\, f_g(x) = gxg^{-1} \quad \forall x \in G \right\}$$

$$H \xrightarrow{\theta} \mathrm{Aut}G \qquad h \xrightarrow{\theta} f_h \qquad f_h(g) = (g)^h$$

$$G \times_\theta H = \left\{ (g,h) \,\middle|\, g \in G, h \in H \right\}$$

$$(g_1,h_1)(g_2,h_2) = \left(g_1 \cdot (g_2)^{h_1}, h_1 \cdot h_2 \right)$$

$$(g,h)^{-1} = \left((g^{-1})^{h^{-1}}, h^{-1} \right)$$

Пример: $\mathrm{Aut}\boldsymbol{Z}_3 \cong \boldsymbol{Z}_2 \Rightarrow$

f_0:	f_1:
$0 \to 0$	$0 \to 0$
$1 \to 1$	$1 \to 2$
$2 \to 2$	$2 \to 1$

$$\boldsymbol{Z}_3 \times_\theta \boldsymbol{Z}_2 - \textit{неабелева}:$$

$$\begin{cases} (2,0) \cdot (1,1) = (2 + f_0(1), 0 + 1) = (0,1) \\ (1,1) \cdot (2,0) = (1 + f_1(2), 1 + 0) = (2,1) \end{cases}$$

Проблема сопряженности :

для $x \sim y$ *найти* $u \in G$: $uxu^{-1} = y$

***Специальная проблема сопряженности*:**

для данного $\mathrm{Inn}g$ *найти* $g' \in G$:

$\mathrm{Inn}g' = \mathrm{Inn}g$

Криптосистема для неабелевой группы со сложной проблемой сопряженности

$$G = \langle \gamma_i \rangle, \quad g \in G$$

$$\begin{cases} \text{отрытый ключ}: & \{\varepsilon_i = g\gamma_i g^{-1}\} \\ \text{секретный ключ}: & g \quad (\text{или} \quad \mathrm{Inn}g) \end{cases}$$

$$\begin{cases} \text{шифрование}: & c = \mathrm{Inn}g(m) = gmg^{-1} = m^g \\ \text{расшифрование}: & m = \mathrm{Inn}^{-1}g(c) = g^{-1}cg = c^{g^{-1}} \end{cases}$$

Новая криптосистема

Неабелева группа $G = \langle \gamma_i \rangle \subset Z(G), \quad g \in G$

$$\mathrm{Inng} \Leftrightarrow \{ \mathrm{Inng}(\gamma_i) \} = \{ \gamma_i^g \} = \{ \varepsilon_i \}$$

$$\begin{cases} \textit{отрытый ключ}: \ (\mathrm{Inng}, \ \mathrm{Inng}^a) \\ \textit{секретный ключ}: \ \textit{число} \ a \end{cases}$$

Шифрование:

1) *Выразить о.т.* $m \in G$ *через* $\{\gamma_i\}$
2) *Выбрать число* b *и вычислить*
3) $\mathrm{Inn}(g^a)^b \Leftrightarrow \{\mathrm{Inng}^{ab}(\gamma_i)\}$

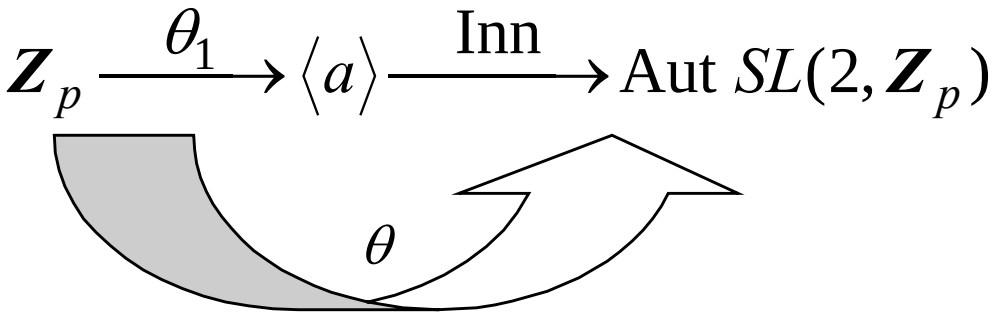
   Вычислить ш.т. $c = \mathrm{Inng}^{ab}(m)$
4) *Вычислить* $\varphi = \mathrm{Inng}^b \Leftrightarrow \{\mathrm{Inng}^b(\gamma_i)\}$
5) *Послать сообщение* (c, φ)

Расшифрование:

1) *Выразить ш.т.* $c \in G$ *через* $\{\gamma_i\}$
2) *Вычислить* $\varphi^{-a} = \mathrm{Inng}^{-ab}$
3) *О.т.* $m = \varphi^{-a}(c)$

Выбор группы G:

$$\alpha \in SL(2,p), \quad \alpha = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad o(\alpha) = p$$



$$G = SL(2, \boldsymbol{Z}_p) \times_\theta \boldsymbol{Z}_p$$

$$(x,y)\cdot(a,b)\cdot(x,y)^{-1} = \left(x\cdot(a)^y \cdot (x^{-1})^b, b\right)$$

$$SL(2, \boldsymbol{Z}_p) = \langle T, S \rangle, \quad T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

$$\forall m \in SL(2, \mathrm{Z}_p), \quad m_{12} \neq 0 \quad \Rightarrow$$

$$\Rightarrow m = T^{j_1} S T^{j_2} S T^{j_3}$$

$$G = \langle (T,0), (S,0), (E,1) \rangle$$