Московский государственный технический университет имени Н.Э. Баумана

О подстановочных гомоморфизмах *-марковских алгоритмов блочного шифрования с неабелевой группой наложения ключа

М.А. Пудовкина

Алгоритм блочного шифрования $C_l(*, b\ )$

- $(X,*)$ – группа.
- $C_l(*, b\ )$ – а.б.ш., раундовая функция $g: X^2 \to X$ задана

$$g: (x,k) \longmapsto b(x * k\ ),$$

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

– $b \in S(X)$,

Алгоритм блочного шифрования $C_l(*, b)$

- $(X,*)$ – группа.
- $C_l(*, b)$ – а.б.ш., раундовая функция $g: X^2 \to X$ задана

$$g: (x, k) \longmapsto b(x * k),$$

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

  - $b \in S(X)$,
  - XSL– а.б.ш., $b = sh$,
    - s – преобразование слоя перемешивания (s – боксы),
    - h – преобразование линейного слоя.

$*$-марковские алгоритмы блочного шифрования

- $\theta^{(0)}, \theta^{(1)} \ldots, \theta^{(l)}$ – 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.
- $\theta_{\mathbf{U}}^{(0)}, \ldots, \theta_{\mathbf{U}}^{(l)}$ – последовательность дискретные с.в. на множестве $\{0, \ldots, r-1\}$:
  $\theta_{\mathbf{U}}^{(t)} = j \Leftrightarrow \theta^{(t)} \in U_j$ для $\forall j \in \{0, \ldots, r-1\}$, $t = 1, \ldots, l$.

$*$-марковские алгоритмы блочного шифрования

- $\theta^{(0)}, \theta^{(1)} \ldots, \theta^{(l)}$ – 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.
- $\theta_{\mathbf{U}}^{(0)}, \ldots, \theta_{\mathbf{U}}^{(l)}$ – 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. $\theta_{\mathbf{U}}^{(0)}, \ldots, \theta_{\mathbf{U}}^{(l)}$ – цепь Маркова, переходные вероятности которой не зависят от распр. с.в. $\theta^{(0)}$. Полученная цепь Маркова называется *укрупнённой*.

Алгоритм блочного шифрования $C_l(*, b)$

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

$$g: (x, k) \longmapsto b(x * k),$$

$$(x_1, x_2) \longmapsto (b(x_1 * k), b(x_2 * k)) \ \forall (x_1, x_2, k) \in X^3.$$

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

(из теории вероятностных автоматов),

$$p_{(\alpha_1,\alpha_0),(\beta_1,\beta_0)} = \mathrm{P}\{(g_k(\alpha_1), g_k(\alpha_0)) = (\beta_1, \beta_0)\} -$$

элемент матрицы вероятностей переходов.

Алгоритм блочного шифрования $C_l(*, b)$

- Если раундовые ключи независимо и равновероятно выбираемы из X, то на множестве состояний X^2 – цепь Маркова $\xi^{(0)}, \xi^{(1)}, \dots, \xi^{(l)}$.
- $\xi^{(0)}, \dots, \xi^{(l)}$ можно укрупнить разбиением $\mathbf{R} = \{R_\varepsilon | \varepsilon \in X\}$

$(R_\varepsilon = \{(\alpha * \varepsilon, \alpha) | \alpha \in X\})$, если

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

$$p_{\theta,\varepsilon}(g) =$$

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

Алгоритм блочного шифрования $C_l(*, b)$

- Если раундовые ключи независимо и равновероятно выбираемы из X, то на множестве состояний X^2 – цепь Маркова $\xi^{(0)}, \xi^{(1)}, \dots, \xi^{(l)}$.
- $\xi^{(0)}, \dots, \xi^{(l)}$ можно укрупнить разбиением $\mathbf{R} = \{R_\varepsilon | \varepsilon \in X\}$ $(R_\varepsilon = \{(\alpha * \varepsilon, \alpha) | \alpha \in X\})$, если

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

$$p_{\theta,\varepsilon}(g) =$$

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

- **Определение** [LaiMM91] Блочные алгоритмы, для которых справедливо (1), называются $*$-*марковскими алгоритмами блочного шифрования*.

$*_{\mathbf{W}}$-марковские алгоритмы

- $\xi_{\mathbf{R}}^{(0)},\ldots,\xi_{\mathbf{R}}^{(l)}$ – укрупненная цепь Маркова $\xi^{(0)},\ldots,\xi^{(l)}$ разбиением $\mathbf{R}=\{R_\varepsilon|\varepsilon\in X\}$.
- **Определение**. Назовём l-раундовый итерационный $*$-марковский алгоритм с марковской п.с.в. $\xi_{\mathbf{R}}^{(0)},\ldots,\xi_{\mathbf{R}}^{(l)}$ $*_{\mathbf{W}}$-*марковским* для $\mathbf{W}$, если $\xi_{\boldsymbol{R}_{\mathbf{W}}}^{(0)},\ldots,\xi_{\boldsymbol{R}_{\mathbf{W}}}^{(l)}$ является цепью Маркова.
  - $\mathbf{W}=\{W_0,\ldots,W_{r-1}\}$ – разбиение X,
  - $\mathbf{R_W}=\{R_W|W\in\mathbf{W}\}$, $R_W=\bigcup_{\varepsilon\in W}R_\varepsilon$.

$*_{\mathbf{W}}$-марковские алгоритмы

- $\xi_{\mathbf{R}}^{(0)},\ldots,\xi_{\mathbf{R}}^{(l)}$ – укрупненная цепь Маркова $\xi^{(0)},\ldots,\xi^{(l)}$ разбиением $\mathbf{R}=\{R_\varepsilon|\varepsilon\in X\}$.
- Назовём l -раундовый итерационный $*$ -марковский алгоритм с марковской п.с.в. $\xi_{\mathbf{R}}^{(0)},\ldots,\xi_{\mathbf{R}}^{(l)}$ $*_{\mathbf{W}}$-*марковским* для $\mathbf{W}$, если $\xi_{\boldsymbol{R}_{\mathbf{W}}}^{(0)},\ldots,\xi_{\boldsymbol{R}_{\mathbf{W}}}^{(l)}$ является цепью Маркова.
  - $\mathbf{W}=\{W_0,\ldots,W_{r-1}\}$ – разбиение X,
  - $\mathbf{R}_{\mathbf{W}}=\{R_W|W\in\mathbf{W}\}$, $R_W=\bigcup_{\varepsilon\in W}R_\varepsilon$.
- [ПогП17]. *Для l -раундового $*$ -марковского а.б.ш. марковская 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* $a_{j,c}$, $0\le a_{j,c}\le 1$.
  - $p_{\theta,W_c}(g)=\sum_{\delta\in W_c}p_{\theta,\delta}(g)$, $\theta\in X$.

$*_{\mathbf{W}}$-марковские алгоритмы

– $\mathbf{W} = \{W_0, \dots, W_{r-1}\}$ – разбиение X,

- Для $*_{\mathbf{W}}$-марковского алгоритма матрица $\left(p_{W_i,W_j}(f^{(l)})\right)$ вероятностей переходов блоков разбиения $\mathbf{W}$ равна $\prod_{i=1}^{l} p_{\mathbf{W}}(g)$,
  - $p_{W_i,W_j}(g) = a_{i,j} \;\; i,j \in \{0, \dots, r-1\}$,
  - $p_{\mathbf{W}}(g) = \left(p_{W_i,W_j}(g)\right)$ – матрица вероятностей переходов блоков разностей.
- Обобщение метода усеченных разностей.

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

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

- $b \in S(X)$, $\mathbf{W} = \{W_0, \dots, W_{r-1}\}$ – разбиение X, $|X| \geq r \geq 2$.
  - $\hat{p}_{\varepsilon,\delta}(b) = |X|^{-1}|\{\alpha \in X | b(\theta * \alpha) = \varepsilon * b(\alpha)\}|$, $\varepsilon, \delta \in X$;
    - $\hat{p}(b) = \left(\hat{p}_{\varepsilon,\delta}(b)\right)$ – матрица вероятностей переходов разностей b;
  - $\hat{p}_{\varepsilon,W_c}(b) = \sum_{\delta \in W_c} \hat{p}_{\varepsilon,\delta}(b)$, $c = 0, \dots, r-1$.

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

- $b \in S(X)$, $\mathbf{W} = \{W_0, \dots, W_{r-1}\}$ – разбиение X, $|X| \geq r \geq 2$.
  - $\hat{p}_{\varepsilon,\delta}(b) = |X|^{-1}|\{\alpha \in X | b(\theta * \alpha) = \varepsilon * b(\alpha)\}|$, $\varepsilon, \delta \in X$;
    - $\hat{p}(b) = \left(\hat{p}_{\varepsilon,\delta}(b)\right)$ – матрица вероятностей переходов разностей b;
  - $\hat{p}_{\varepsilon,W_c}(b) = \sum_{\delta \in W_c} \hat{p}_{\varepsilon,\delta}(b)$, $c = 0, \dots, r-1$.
- **Определение.** 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,
  - $\hat{p}_{W_i,W_j}(b) = a_{i,j}$, $i, j \in \{0, \dots, r-1\}$.

$*_W$-марковские преобразования

- Для $C_l(*, b\ )$ справедливо равенство $\hat{p}(b) = p(g)$.
- $(X,*)$ – группа наложения ключа:
  - $\sigma_k \in S(X),\ \sigma_k : x \mapsto x * k\ \ \forall\ k \in X$;
  - $\rho: X \to S(X)$ – правое регулярное представление $(X,*)$;
  - $X^* = \langle \sigma_k | k \in X \rangle,\quad \rho(X) = X^*,\ \ \rho(k) = \sigma_k\ \forall\ k \in X$;
  - $g_k = \sigma_k b\ \ \forall\ k \in X$.

Свойства группы $G = \langle b, X^* \rangle$

- $Q \subseteq S(X)$ *сохраняет разбиение* $\mathbf{W}$ множества X, если $q(W) \in \mathbf{W}$ для $\forall (W, q) \in \mathbf{W} \times Q$.

- **Утверждение 1**. *Пусть* $\exists$ *разбиение* $\mathbf{W} = \{W_0, \dots, W_{r-1}\}$ *множества* X, *сохраняемое* $\{g_k | k \in X\}$, $e \in W_0$, $r \geq 2$. *Тогда:*
  - *группа* $G = \langle b, X^* \rangle$ *импримитивна с системой импримитивности* $\mathbf{W}$, *а* $w = |W_0| = \cdots = |W_{r-1}|$ *для некоторого* $w \in \mathbb{N}$, $1 < w < |X|$;

Свойства группы $G = \langle b, X^* \rangle$

- $Q \subseteq S(X)$ *сохраняет разбиение* $\mathbf{W}$ множества X, если $q(W) \in \mathbf{W}$ для $\forall (W, q) \in \mathbf{W} \times Q$.

- **Утверждение 1**. *Пусть* $\exists$ *разбиение* $\mathbf{W} = \{W_0, \dots, W_{r-1}\}$ *множества* X, *сохраняемое* $\{g_k | k \in X\}$, $e \in W_0$, $r \geq 2$. *Тогда:*
  - *группа* $G = \langle b, X^* \rangle$ *импримитивна с системой импримитивности* $\mathbf{W}$, *а* $w = |W_0| = \dots = |W_{r-1}|$ *для некоторого* $w \in \mathbb{N}$, $1 < w < |X|$;
  - $(W_0, *) \leq (X, *)$, *а* W_j – j*-й правый смежный класс* $(X, *)$ *по* $(W_0, *)$, $j = 0, \dots, r-1$;

Свойства группы $G = \langle b, X^* \rangle$

- $Q \subseteq S(X)$ *сохраняет разбиение* $\mathbf{W}$ множества X, если $q(W) \in \mathbf{W}$ для $\forall (W, q) \in \mathbf{W} \times Q$.

- **Утверждение 1**. *Пусть* $\exists$ *разбиение* $\mathbf{W} = \{W_0, \dots, W_{r-1}\}$ *множества* X, *сохраняемое* $\{g_k | k \in X\}$, $e \in W_0$, $r \geq 2$. *Тогда:*
  - *группа* $G = \langle b, X^* \rangle$ *импримитивна с системой импримитивности* $\mathbf{W}$, *а* $w = |W_0| = \dots = |W_{r-1}|$ *для некоторого* $w \in \mathbb{N}$, $1 < w < |X|$;
  - $(W_0,*) \leq (X,*)$, *а* W_j – j-*й правый смежный класс* $(X,*)$ *по* $(W_0,*)$, $j = 0, \dots, r-1$;
  - *если группа* $G = \langle b, X^* \rangle$ *не имеет точных подстановочных представлений степени* d, *где* $d \mid |X|$, $d < |X|$, *а среди всех разбиений сохраняемых* G *блоки разбиения* $\mathbf{W}$ *имеют минимальную мощность, то* $(W_0,*)$ – *нормальная подгруппа группы* $(X,*)$.

- $\mathbf{W} = \{W_0, \dots, W_{r-1}\}$ – разбиение множества X, $e \in W_0$.
  - $(W_0,*) \leq (X,*)$;
  - W_j – j-й правый смежный класс $(X,*)$ по $(W_0,*)$, $j = 0, \dots, r-1$.
- $\varphi_{\mathbf{W}}: X \to \{0, \dots, r-1\}$: $\varphi_{\mathbf{W}}: \alpha \longmapsto i \Leftrightarrow \alpha \in W_i$
- Бинарная операция $\circ$ на $\{0, \dots, r-1\}$, $(W_0,*) \trianglelefteq (X,*)$,

$$W_i * W_j = W_{i \circ j}, \forall i, j \in \{0, \dots, r-1\}. \qquad (1)$$

- Если b сохраняет $\mathbf{W}$, то $\bar{b} \in S(\{0, \dots, r-1\})$,

$$\bar{b}\,(\varphi_{\mathbf{W}}(\alpha)) = \varphi_{\mathbf{W}}(b(\alpha)) \qquad \forall \alpha \in X. \qquad (2)$$

- $\mathbf{W} = \{W_0, \dots, W_{r-1}\}$ – разбиение множества X, $e \in W_0$.
  - $(W_0,*) \leq (X,*)$;
  - W_j – j-й правый смежный класс $(X,*)$ по $(W_0,*)$, $j = 0, \dots, r-1$.
- $\varphi_{\mathbf{W}}: X \to \{0, \dots, r-1\}$: $\varphi_{\mathbf{W}}: \alpha \longmapsto i \Leftrightarrow \alpha \in W_i$
- Бинарная операция $\circ$ на $\{0, \dots, r-1\}$, $(W_0,*) \trianglelefteq (X,*)$,

$$W_i * W_j = W_{i \circ j}, \forall i,j \in \{0, \dots, r-1\}. \qquad (1)$$

- Если b сохраняет $\mathbf{W}$, то $\bar{b} \in S(\{0, \dots, r-1\})$,

$$\bar{b}\,(\varphi_{\mathbf{W}}(\alpha)) = \varphi_{\mathbf{W}}(b(\alpha)) \qquad \forall \alpha \in X. \qquad (2)$$

- $(Y,\diamond)$ – группа, $s \in S(Y)$, $|Y| < |X|$.
- **Определение**. Сюръективное отображение $\theta: X \longrightarrow Y$,

$$\theta\big(b(x * k)\big) = s(\theta(x) \diamond \theta(k)) \qquad \forall (x,k) \in X^2,$$

называется *гомоморфизмом алгоритма* $C_l(*, b)$ в алгоритм $C_l(\diamond, s)$.

- $\mathbf{W} = \{W_0, \dots, W_{r-1}\}$

$$\varphi_{\mathbf{W}}: X \to \{0, \dots, r-1\}: \ \varphi_{\mathbf{W}}: \alpha \to i \Leftrightarrow \alpha \in W_i,$$

- Бинарная операция $\circ$ на $\{0, \dots, r-1\}$, $(W_0,*) \trianglelefteq (X,*)$,

$$W_i * W_j = W_{i \circ j}, \forall i, j \in \{0, \dots, r-1\}. \quad (1)$$

- Если b сохраняет $\mathbf{W}$, то $\bar{b} \in S(\{0, \dots, r-1\})$,

$$\bar{b}\,(\varphi_{\mathbf{W}}(\alpha)) = \varphi_{\mathbf{W}}(b(\alpha)) \ \ \forall \alpha \in X. \quad (2)$$

- **Теорема 2**. *Пусть* $l \in \mathbb{N}$, $\mathbf{W} = \{W_0, \dots, W_{r-1}\}$ *– нетривиальное разбиение* X, $e \in W_0$, $(W_0,*) \trianglelefteq (X,*)$. *Тогда следующие условия эквивалентны:*

1. $\{g_k | k \in X\}$ *сохраняет разбиение* $\mathbf{W}$.
2. *В* $C_l(\circ, \bar{b})$ *корректно определены бинарная операция* $\circ$ *и подстановка* $\bar{b}$, *заданные соответственно условиями* (1) *и* (2), *а* $\varphi_{\mathbf{W}}$ *– гомоморфизм* $C_l(*, b)$ *в* $C_l(\circ, \bar{b})$.
3. $C_l(*, b)$ *является* $*_{\mathbf{W}}$*-марковским, если* $\mathbf{W}$ *– множество смежных классов группы* $(X,*)$ *по её нормальной подгруппе* $(W_0,*)$.

Гомоморфизмы алгоритма $C_l(*, b)$ 1

- $\mathrm{IG}_{\mathbf{W}}$ – максимальная подгруппа группы $S(X)$, сохраняющая $\mathbf{W}$.
  - $\mathbf{W} = \{W_0, \dots, W_{r-1}\}$ – разбиение X,
  - $|W_0| = \cdots |W_{r-1}| = w, \ \ 1 < r < |X|$.
- $\sigma_k : x \mapsto x * k \ \ \forall\, k \in X, \sigma_k \in S(X)$.
- $X^* = \langle \sigma_k | k \in X \rangle$.
- Из импримитивности группы $G = \langle b, X^* \rangle$ следуют включения:
  - $b \in \mathrm{IG}_{\mathbf{W}}, \ \langle g_k | k \in X \rangle \leq \mathrm{IG}_{\mathbf{W}}$,
  - $\left\langle g_{k^{(1)}} \dots g_{k^{(l)}} \middle| \left(k^{(1)}, \dots, k^{(l)}\right) \in X^l \right\rangle \leq \mathrm{IG}_{\mathbf{W}}$.

Гомоморфизмы алгоритма $C_l(*, \boldsymbol{b})$ 1

– $\mathbf{W} = \{W_0, \dots, W_{r-1}\}$ – разбиение X,

– $|W_0| = \cdots |W_{r-1}| = w, \ \ 1 < r < |X|.$

- **Определение.** *Подстановочный гомоморфизм* $\tilde{\varphi}_{\mathbf{W}}$ – естественный гомоморфизм импримитивной группы G в $S(\{0, \dots, r-1\})$, который однозначно задаётся отображением $\varphi_{\mathbf{W}}: X \to \{0, \dots, r-1\}$, удовлетворяющим условию

$$\bar{b}\,(\varphi_{\mathbf{W}}(\alpha)) = \varphi_{\mathbf{W}}(b(\alpha)) \ \ \forall \alpha \in X.$$

Гомоморфизмы алгоритма $C_l(*, \boldsymbol{b})$ 1

– $\mathbf{W} = \{W_0, \dots, W_{r-1}\}$ – разбиение X,

– $|W_0| = \cdots |W_{r-1}| = w, \ \ 1 < r < |X|$.

- **Определение.** *Подстановочный гомоморфизм* $\tilde{\varphi}_{\mathbf{W}}$ – естественный гомоморфизм импримитивной группы G в группу $S(\{0, \dots, r-1\})$, который однозначно задаётся отображением $\varphi_{\mathbf{W}}: X \to \{0, \dots, r-1\}$, удовлетворяющим условию

$$\bar{b}\,(\varphi_{\mathbf{W}}(\alpha)) = \varphi_{\mathbf{W}}(b(\alpha)) \ \ \forall \alpha \in X.$$

- Из наличия подстановочного гомоморфизма $\tilde{\varphi}_{\mathbf{W}}$ группы G не следует существование гомоморфизма θ алгоритма $C_l(*, b)$.
- Если $(W_0,*) \trianglelefteq (X,*)$, то $\theta = \varphi_{\mathbf{W}}$ и $C_l(*, b) - *_{\mathbf{W}}$-марковский (теорема 2).

Гомоморфизмы алгоритма $C_l(*, b)$ 2

- $(X,*)$ – группа Гамильтона (неабелева группа, содержащая только нормальные подгруппы).
  - группа Гамильтона представима как прямое произведение группы кватернионов Q_8, абелевой группы, каждый элемент которой конечного нечётного порядка, и абелевой группы показателя два.
- $(W_0,*)$ – произвольная подгруппа группы Гамильтона $(X,*)$.

Гомоморфизмы алгоритма $C_l(*, b\ )$ 2

- $(X,*)$ – группа Гамильтона (неабелева группа, содержащая только нормальные подгруппы).
  - группа Гамильтона представима как прямое произведение группы кватернионов Q_8, абелевой группы, каждый элемент которой конечного нечётного порядка, и абелевой группы показателя два.
- $(W_0,*)$ – произвольная подгруппа группы Гамильтона $(X,*)$.
- $\mathbf{W} = \{W_0, \dots, W_{r-1}\}$ – разбиение, состоящее из всех правых смежных классов группы $(X,*)$ по подгруппе $(W_0,*)$.
- Из теоремы 2 следует, если $b \in \mathrm{IG}_{\mathbf{W}}$, то:
  - $\varphi_{\mathbf{W}}$ – гомоморфизм $C_l(*, b\ )$ в $C_l(\circ, \bar{b}\ )$ и $\theta = \varphi_{\mathbf{W}}$;
  - $C_l(*, b\ )$ – $*_{\mathbf{W}}$-марковский.

Спасибо за внимание!