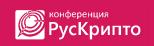




Ежегодная международная научно-практическая конференция «РусКрипто'2021»

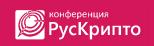
О кодировках неабелевых 2-групп наложения ключа с циклической подгруппой индекса 2

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



Перспектива: шифрсистемы с неабелевой операцией наложения ключа

- \mathbb{Z}_2^m или \mathbb{Z}_{2^m} во многих современных шифрсистемах как группы наложения ключа
- Возможно применение квантовых алгоритмов для нахождения «скрытых сдвигов»
 - lacktriangle полиномиальный алгоритм Саймона для \mathbb{Z}_2^m
 - lacktriangle алгоритма Куперберга трудоёмкостью $2^{O(m^{1/2})}$ для \mathbb{Z}_{2^m}



Перспектива: шифрсистемы с неабелевой операцией наложения ключа

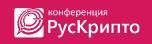
- \mathbb{Z}_2^m или \mathbb{Z}_{2^m} во многих современных шифрсистемах как группы наложения ключа
- Возможно применение квантовых алгоритмов для нахождения «скрытых сдвигов»
 - lacktriangle полиномиальный алгоритм Саймона для \mathbb{Z}_2^m
 - lacktriangle алгоритма Куперберга трудоёмкостью $2^{O(m^{1/2})}$ для \mathbb{Z}_{2^m}
 - ⇒актуально рассматривать в качестве групп наложения ключа неабелевы 2-группы



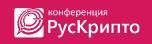
■ группа диэдра
$$D_{2^m}$$
, $m \geq 3$, $a^{2^{m-1}} = e$, $u^2 = e$, $ua = a^{-1}u$



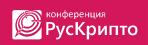
- **■** группа диэдра D_{2^m} , $m \ge 3$, $a^{2^{m-1}} = e$, $u^2 = e$, $ua = a^{-1}u$
- lacktriangle обобщенная группа кватернионов Q_{2^m} , $m \geq 3$, $a^{2^{m-1}} = e$, $u^2 = a^{2^{m-2}}$, $ua = a^{-1}u$



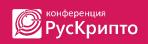
- **■** группа диэдра D_{2^m} , $m \geq 3$, $a^{2^{m-1}} = e$, $u^2 = e$, $ua = a^{-1}u$
- обобщенная группа кватернионов Q_{2^m} , $m \ge 3$, $a^{2^{m-1}} = e$, $u^2 = a^{2^{m-2}}$, $ua = a^{-1}u$
- модулярная максимально-циклическая группа M_{2^m} , $m \ge 4$, $a^{2^{m-1}} = e$, $u^2 = e$, $ua = a^{1+2^{m-2}}u$



- **■** группа диэдра D_{2^m} , $m \ge 3$, $a^{2^{m-1}} = e$, $u^2 = e$, $ua = a^{-1}u$
- обобщенная группа кватернионов Q_{2^m} , $m \ge 3$, $a^{2^{m-1}} = e$, $u^2 = a^{2^{m-2}}$, $ua = a^{-1}u$
- модулярная максимально-циклическая группа M_{2^m} , $m \ge 4$, $a^{2^{m-1}} = e$, $u^2 = e$, $ua = a^{1+2^{m-2}}u$
- полудиэдральная группа SD_{2^m} , $m \ge 4$, $a^{2^{m-1}} = e$, $u^2 = e$, $ua = a^{-1+2^{m-2}}u$



- H_m одна из четырёх групп D_{2^m} , Q_{2^m} , M_{2^m} , SD_{2^m} , $m \geq 4$.
- $u^{\varepsilon_1}a^{\varepsilon_2}$ запись элементов H_m , $\varepsilon_1 \in \{0,1\}$, $\varepsilon_2 \in \{0,\dots,2^{m-1}-1\}$,



- ullet H_m одна из четырёх групп D_{2^m} , Q_{2^m} , M_{2^m} , SD_{2^m} , $m\geq 4$.
- $u^{\varepsilon_1}a^{\varepsilon_2}$ запись элементов H_m , $\varepsilon_1 \in \{0,1\}$, $\varepsilon_2 \in \{0,\dots,2^{m-1}-1\}$,
- φ_{rr} : $H_m \to S(H_m)$ правое регулярные подстановочные представление, $\forall i \in \{0, ..., 2^{m-1} 1\}, \forall x \in H_m$ $\varphi_{rr}(a^i)$: $x \mapsto xa^i$, $\varphi_{rr}(ua^i)$: $x \mapsto xua^i$,



- ullet H_m одна из четырёх групп D_{2^m} , Q_{2^m} , M_{2^m} , SD_{2^m} , $m\geq 4$.
- $u^{\varepsilon_1}a^{\varepsilon_2}$ запись элементов H_m , $\varepsilon_1 \in \{0,1\}$, $\varepsilon_2 \in \{0,\dots,2^{m-1}-1\}$,
- φ_{rr} : $H_m \to S(H_m)$ правое регулярные подстановочные представление, $\forall i \in \{0, \dots, 2^{m-1}-1\}, \forall x \in H_m$ $\varphi_{rr}(a^i)$: $x \mapsto xa^i$, $\varphi_{rr}(ua^i)$: $x \mapsto xua^i$,
- $\varphi_{lr} : H_m \to S(H_m)$ левое регулярные подстановочные представление, $\forall i \in \{0, ..., 2^{m-1}-1\}, \forall x \in H_m$

$$\varphi_{lr}(a^i): x \mapsto a^{-i}x, \ \varphi_{lr}(ua^i): x \mapsto (ua^i)^{-1}x.$$



$$\varphi_{lr} = \rho^{-1} \varphi_{rr} \rho, \ \rho : g \mapsto g^{-1}.$$



$$\varphi_{lr} = \rho^{-1} \varphi_{rr} \rho, \ \rho : g \mapsto g^{-1}.$$

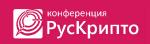
$$\varphi_{rr}(a) = (e, a, ..., a^{2^{m-1}-1})(u, ua, ..., ua^{2^{m-1}-1}),$$



$$\varphi_{lr} = \rho^{-1} \varphi_{rr} \rho, \ \rho : g \mapsto g^{-1}.$$

$$\varphi_{rr}(a) = (e, a, ..., a^{2^{m-1}-1})(u, ua, ..., ua^{2^{m-1}-1}),$$

•
$$\varphi_{rr}(u) = \prod_{j=0}^{2^{m-1}-1} (a^j, ua^{-j})$$
 при $H_m = D_{2^m}$,

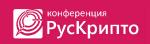


$$\varphi_{lr} = \rho^{-1} \varphi_{rr} \rho, \ \rho : g \mapsto g^{-1}.$$

$$\varphi_{rr}(a) = (e, a, ..., a^{2^{m-1}-1})(u, ua, ..., ua^{2^{m-1}-1}),$$

•
$$\varphi_{rr}(u) = \prod_{j=0}^{2^{m-1}-1} (a^j, ua^{-j})$$
 при $H_m = D_{2^m}$,

$$ullet$$
 $\phi_{rr}(u) = \prod_{j=0}^{2^{m-2}-1} (a^j, ua^{-j}, a^{j+2^{m-2}}, ua^{2^{m-2}-j})$ при $H_m = Q_{2^m}$,



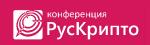
$$\varphi_{lr} = \rho^{-1} \varphi_{rr} \rho, \ \rho : g \mapsto g^{-1}.$$

$$\varphi_{rr}(a) = (e, a, ..., a^{2^{m-1}-1})(u, ua, ..., ua^{2^{m-1}-1}),$$

•
$$\varphi_{rr}(u) = \prod_{j=0}^{2^{m-1}-1} (a^j, ua^{-j})$$
 при $H_m = D_{2^m}$,

$$ullet$$
 $\phi_{rr}(u) = \prod_{j=0}^{2^{m-2}-1} (a^j, ua^{-j}, a^{j+2^{m-2}}, ua^{2^{m-2}-j})$ при $H_m = Q_{2^m}$,

$$ullet$$
 $\phi_{rr}(u) = \prod_{j=0}^{2^{m-1}-1} (a^j, ua^{2^{m-2}j-j})$ при $H_m = SD_{2^m}$,



$$\varphi_{lr} = \rho^{-1} \varphi_{rr} \rho, \ \rho : g \mapsto g^{-1}.$$

$$\varphi_{rr}(a) = (e, a, ..., a^{2^{m-1}-1})(u, ua, ..., ua^{2^{m-1}-1}),$$

•
$$\varphi_{rr}(u) = \prod_{j=0}^{2^{m-1}-1} (a^j, ua^{-j})$$
 при $H_m = D_{2^m}$,

$$ullet$$
 $\phi_{rr}(u) = \prod_{j=0}^{2^{m-2}-1} (a^j, ua^{-j}, a^{j+2^{m-2}}, ua^{2^{m-2}-j})$ при $H_m = Q_{2^m}$,

$$ullet$$
 $\phi_{rr}(u) = \prod_{j=0}^{2^{m-1}-1} (a^j, ua^{2^{m-2}j-j})$ при $H_m = SD_{2^m}$,

•
$$\varphi_{rr}(u) = \prod_{j=0}^{2^{m-2}-1} (a^{2j}, ua^{2j})(a^{2j+1}, ua^{2j+1+2^{m-2}})$$
 при $H_m = M_{2^m}$.

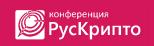


Системы импримитивности

Опр. Транзитивная группа подстановок $G \leq S(X)$ называется *импримитивной*, если существует сохраняемое G нетривиальное разбиение W множества X на равномощные блоки, т.е.

$$g(W) = W \ \forall g \in G.$$

- в противном случае примитивной.
- W— система импримитивности (нетривиальное разбиение X).



Системы импримитивности групп P_m , G_m • H_m близка к $\mathbb{Z}_{2^m}^+$ (в смысле строения систем импримитивности)

- H_m близка к $G_m = \langle V_m^+(2), \mathbb{Z}_{2^m}^+ \rangle$



Системы импримитивности групп P_m , G_m • H_m близка к $\mathbb{Z}_{2^m}^+$ (в смысле строения систем импримитивности)

- H_m близка к $G_m = \langle V_m^+(2), \mathbb{Z}_{2^m}^+ \rangle$
- P_m максимальная 2-подгруппа в $S(V_m(2))$, содержащая G_m
 - силовская 2-подгруппа $S(V_m(2))$
 - описывается операцией сплетения $P_m = P_2 \wr P_{m-1}$



Системы импримитивности групп P_m , G_m

- H_m близка к $\mathbb{Z}_{2^m}^+$ (в смысле строения систем импримитивности)
- H_m близка к $G_m = \langle V_m^+(2), \mathbb{Z}_{2^m}^+ \rangle$
- ullet P_m максимальная 2-подгруппа в $S(V_m(2))$, содержащая G_m
 - силовская 2-подгруппа $S(V_m(2))$
 - ullet описывается операцией сплетения $P_m=P_2\wr P_{m-1}$
- Справедливо включение $V_m^+(2)$, $\mathbb{Z}_{2^m}^+ \leq P_m$
- P_m , G_m импримитивны с r-й системой импримитивности

$$W^{(r,m)} = \left\{ W_0^{(r,m)}, \dots, W_{2^r - 1}^{(r,m)} \right\},$$

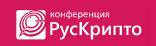
$$\left| W_j^{(r,m)} \right| = 2^{m-r},$$

$$W_j^{(r,m)} = \{ j \in \{0, \dots, 2^m - 1\} | j \equiv t \pmod{2^r} \},$$

$$t = 0, \dots, 2^r - 1, r = 0, \dots, m.$$



Кодировки группы H_m • $v: H_m \to \{0, \dots, 2^m-1\}$ – биективное отображение, осуществляющее кодировку элементов группы H_m числами $0, ..., 2^m-1$,



- Кодировки группы H_m v: $H_m \to \{0, ..., 2^m 1\}$ биективное отображение, осуществляющее кодировку элементов группы H_m числами $0, ..., 2^m - 1$,
- \tilde{v}_{φ} : $H_m \to S(\{0, ..., 2^m 1\})$ естественный изоморфизм, $\tilde{v}_{\varphi}(b)$: $v(\alpha) \mapsto v(b(\alpha))$ для $\forall (\alpha, b) \in H_m \times \varphi(H_m)$, где $\varphi \in \{\varphi_{rr}, \varphi_{lr}\}.$
- «удобные» для использования в криптографических приложениях

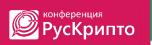


Импримитивность групп $\tilde{v}\varphi_{rr}(H_m)$, $\tilde{v}\varphi_{lr}(H_m)$

Пусть подстановка $g \in S(V_m(2))$ является произведением двух независимых циклов длины 2^{m-1} ,

$$g = \left(\alpha_0^{(1)}, \dots, \alpha_{2^{m-1}-1}^{(1)}\right) \left(\alpha_0^{(2)}, \dots, \alpha_{2^{m-1}-1}^{(2)}\right),$$

$$\Rightarrow U_{i,j}^{(t,m,g)} = \left\{\alpha_j^{(i)}, \alpha_{j+2^t}^{(i)}, \dots, \alpha_{j+2^{m-1}-2^t}^{(i)}\right\},$$



Импримитивность групп $\tilde{v}\varphi_{rr}(H_m)$, $\tilde{v}\varphi_{lr}(H_m)$

Пусть подстановка $g \in S(V_m(2))$ является произведением двух независимых циклов длины 2^{m-1} ,

$$g = \left(\alpha_{0}^{(1)}, \dots, \alpha_{2^{m-1}-1}^{(1)}\right) \left(\alpha_{0}^{(2)}, \dots, \alpha_{2^{m-1}-1}^{(2)}\right),$$

$$\Rightarrow U_{i,j}^{(t,m,g)} = \left\{\alpha_{j}^{(i)}, \alpha_{j+2^{t}}^{(i)}, \dots, \alpha_{j+2^{m-1}-2^{t}}^{(i)}\right\},$$

$$U^{(t+1,m,g)} = \left\{U_{1,0}^{(t,m,g)}, U_{2,0}^{(t,m,g)}, \dots, U_{1,2^{t}-1}^{(t,m,g)}, U_{2,2^{t}-1}^{(t,m,g)}\right\},$$

$$U_{j}^{(t,m,g)} = \left\{U_{1,c}^{(t,m,g)} \cup U_{2,j+c \bmod 2^{t}}^{(t,m,g)} \middle| c = 0, \dots, 2^{t} - 1\right\},$$

где $i \in \{1,2\}, j \in \{0, ..., 2^t - 1\}, t \in \{0, ..., m - 1\}.$

- $\bullet \left| U^{(t,m,g)} \right| = \left| U_j^{(t,m,g)} \right| = 2^t$
- разбиения $U_0^{(t,m,g)}$, ..., $U_{2^t-1}^{(t,m,g)}$ укрупнения разбиения $U^{(t+1,m,g)}$.



Импримитивность группы $\tilde{v}\varphi_{rr}(H_m)$ Теорема. Пусть $m \geq 4$, $g = \tilde{v}\varphi_{rr}(a)$. $\tilde{v}\varphi_{rr}(H_m) \leq P_m \Leftrightarrow$ выполняется одно

Теорема. Пусть $m \ge 4$, $g = \tilde{v}\varphi_{rr}(a)$. $\tilde{v}\varphi_{rr}(H_m) \le P_m \Leftrightarrow$ выполняется одно из условий:

- $U^{(t,m,g)} = W^{(t,m)}$ для $\forall t \in \{1, ..., m\};$
- $U_{p \bmod 2^t}^{(t,m,g)} = W^{(t,m)}$ для $\forall t \in \{0, ..., m-1\}$ и некоторого $p \in \Delta_{rr}(H_m)$,

где

- ullet $\Delta_{rr}(H_m) = \{0, ..., 2^{m-1} 1\}$, если $H_m = D_{2^m}$,
- $\Delta_{rr}(H_m) = \{0, 2^{m-2}\}$, если $H_m = M_{2^m}$,
- $\Delta_{rr}(H_m)=\emptyset$, если $H_m\in\{Q_{2^m},SD_{2^m}\}$.



Импримитивность группы $\tilde{v}\varphi_{lr}(H_m)$

Теорема. Пусть $m \ge 4$, $g = \tilde{v}\varphi_{lr}(a)$. $\tilde{v}\varphi_{lr}(H_m) \le P_m \Leftrightarrow$ выполняется одно из условий:

- $U^{(t,m,g)} = W^{(t,m)}$ для $\forall t \in \{1, ..., m\};$
- $U_{p \bmod 2^t}^{(t,m,g)} = W^{(t,m)}$ для $\forall t \in \{0, ..., m-1\}$ и некоторого $p \in \Delta_{lr}(H_m)$,

где

- $\Delta_{lr}(H_m) = \{0, 2^{m-2}\}$, если $H_m \in \{D_{2^m}, M_{2^m}, SD_{2^m}\}$
- $\Delta_{lr}(H_m)=\emptyset$, если $H_m=Q_{2^m}$.



Импримитивность группы $\tilde{v} \varphi_{lr}(H_m)$

Теорема. Пусть $m \ge 4$, $g = \tilde{v}\varphi_{lr}(a)$. $\tilde{v}\varphi_{lr}(H_m) \le P_m \Leftrightarrow \delta$ выполняется одно из условий:

- $U^{(t,m,g)} = W^{(t,m)}$ для $\forall t \in \{1, ..., m\};$
- $U_{p \bmod 2^t}^{(t,m,g)} = W^{(t,m)}$ для $\forall t \in \{0, ..., m-1\}$ и некоторого $p \in \Delta_{lr}(H_m)$,

где

- $\Delta_{lr}(H_m) = \{0, 2^{m-2}\}$, если $H_m \in \{D_{2^m}, M_{2^m}, SD_{2^m}\}$
- $\Delta_{lr}(H_m)=\emptyset$, если $H_m=Q_{2^m}$.
- ullet $\Delta_{rr}(H_m) = \{0, ..., 2^{m-1} 1\}$, если $H_m = D_{2^m}$,
- ullet $\Delta_{rr}(H_m) = \{0, 2^{m-2}\}$, если $H_m = M_{2^m}$,
- $\Delta_{rr}(H_m) = \emptyset$, если $H_m \in \{Q_{2^m}, SD_{2^m}\}$.



Импримитивность группы $\tilde{v}\varphi_{lr}(H_m)$

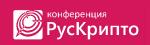
Теорема. Пусть $m \ge 4$, $g = \tilde{v}\varphi_{lr}(a)$. $\tilde{v}\varphi_{lr}(H_m) \le P_m \Leftrightarrow$ выполняется одно из условий:

- $U^{(t,m,g)} = W^{(t,m)}$ для $\forall t \in \{1, ..., m\};$
- $U_{p \bmod 2^t}^{(t,m,g)} = W^{(t,m)}$ для $\forall t \in \{0, ..., m-1\}$ и некоторого $p \in \Delta_{lr}(H_m)$,

где

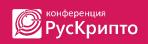
- $\Delta_{lr}(H_m) = \{0, 2^{m-2}\}$, если $H_m \in \{D_{2^m}, M_{2^m}, SD_{2^m}\}$
- $\Delta_{lr}(H_m)=\emptyset$, если $H_m=Q_{2^m}$.

Отрицания \Rightarrow условия примитивности группы $\tilde{v}\varphi_p(H_m) \leq P_m$ при $p \in \{lr, rr\}$.



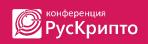
Свойства «естественных» кодировок Утверждение. Пусть
$$s: H_m \to H_m, \ v_c: H_m \to \{0, \dots, 2^m-1\}, c \in \{1,2,3\},$$
 $v_1: x \mapsto \begin{cases} 2i, & \text{если } x = a^i, \\ 2i+1, & \text{если } x = ua^i, \end{cases}$

•
$$i \in \{0, \dots, 2^{m-1} - 1\}$$



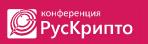
Утверждение. Пусть
$$s: H_m \to H_m, \ v_c: H_m \to \{0, \dots, 2^m-1\}, c \in \{1,2,3\},$$
 $v_1: x \mapsto \begin{cases} 2i, & \text{если } x = a^i, \\ 2i+1, & \text{если } x = ua^i, \\ v_2: x \mapsto \begin{cases} i, & \text{если } x = a^i, \\ 2^{m-1}+i, & \text{если } x = ua^i, \end{cases}$

•
$$i \in \{0, \dots, 2^{m-1} - 1\}$$



Утверждение. Пусть
$$s: H_m \to H_m, \ v_c: H_m \to \{0, \dots, 2^m-1\}, c \in \{1,2,3\},$$
 $v_1: x \mapsto \begin{cases} 2i, & \text{если } x = a^i, \\ 2i+1, & \text{если } x = ua^i, \\ v_2: x \mapsto \begin{cases} i, & \text{если } x = ua^i, \\ 2^{m-1}+i, & \text{если } x = ua^i, \\ v_3: x \mapsto \begin{cases} i, & \text{если } x = ua^i, \\ 2^m-i-1, & \text{если } x = ua^i, \end{cases}$

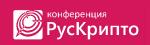
•
$$i \in \{0, \dots, 2^{m-1} - 1\}$$



Утверждение. Пусть
$$s: H_m \to H_m, \ v_c: H_m \to \{0, \dots, 2^m-1\}, c \in \{1,2,3\},$$
 $v_1: x \mapsto \begin{cases} 2i, & \text{если } x = a^i, \\ 2i+1, & \text{если } x = ua^i, \\ v_2: x \mapsto \begin{cases} i, & \text{если } x = ua^i, \\ 2^{m-1}+i, & \text{если } x = ua^i, \\ v_3: x \mapsto \begin{cases} i, & \text{если } x = ua^i, \\ 2^m-i-1, & \text{если } x = ua^i, \end{cases}$

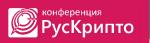
•
$$i \in \{0, ..., 2^{m-1} - 1\}$$

$$s: \alpha \mapsto \alpha^{-1} \quad \forall \alpha \in H_m.$$



I. Тогда для $\varphi_{rr}(H_m)$ справедливы включения:

$$ilde{v}_1 arphi_{rr}(H_m) \leq P_m,$$
 $\langle ilde{v}_1(s), ilde{v}_1 arphi_{rr}(H_m) \rangle \leq P_m$ для $\forall H_m \in \{D_{2^m}, Q_{2^m}, M_{2^m}, SD_{2^m}\},$ $\langle ilde{v}_1(s), ilde{v}_1 arphi_{rr}(H_m) \rangle \leq P_m$ для $\forall H_m \in \{D_{2^m}, Q_{2^m}, M_{2^m}, SD_{2^m}\},$ $ilde{v}_2 arphi_{rr}(H_m) \leq P_m$ для $H_m \in \{D_{2^m}, M_{2^m}\}.$



I. Тогда для $\varphi_{rr}(H_m)$ справедливы включения:

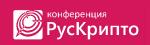
$$ilde{v}_{1} arphi_{rr}(H_{m}) \leq P_{m},$$
 $\langle ilde{v}_{1}(s), ilde{v}_{1} arphi_{rr}(H_{m}) \rangle \leq P_{m} \ \partial$ ля $\forall H_{m} \in \{D_{2}^{m}, Q_{2}^{m}, M_{2}^{m}, SD_{2}^{m}\},$
 $\langle ilde{v}_{1}(s), ilde{v}_{1} arphi_{rr}(H_{m}) \rangle \leq P_{m} \ \partial$ ля $\forall H_{m} \in \{D_{2}^{m}, Q_{2}^{m}, M_{2}^{m}, SD_{2}^{m}\},$
 $ilde{v}_{2} arphi_{rr}(H_{m}) \leq P_{m} \ \partial$ ля $H_{m} \in \{D_{2}^{m}, M_{2}^{m}\}.$

II. Тогда для $\varphi_{lr}(H_m)$ справедливы включения:

$$ilde{v}_1 arphi_{lr}(H_m) \leq P_m,$$
 $\langle ilde{v}_1(s), ilde{v}_1 arphi_{lr}(H_m) \rangle \leq P_m$ для $\forall H_m \in \{D_{2^m}, Q_{2^m}, M_{2^m}, SD_{2^m}\},$ $ilde{v}_2 arphi_{lr}(H_m) \leq P_m$ для $H_m = M_{2^m},$ $ilde{v}_3 arphi_{lr}(H_m) \leq P_m$ для $H_m \in \{D_{2^m}, SD_{2^m}\}.$



- I. Тогда для $\varphi_{rr}(H_m)$:
- группа $\tilde{v}_2 \varphi_{rr}(H_m)$ примитивна для $H_m \in \{Q_{2^m}, SD_{2^m}\};$
- группы $\langle \tilde{v}_2(s), \tilde{v}_2 \varphi_{rr}(H_m) \rangle, \tilde{v}_3 \varphi_{rr}(H_m), \langle \tilde{v}_3(s), \tilde{v}_3 \varphi_{rr}(H_m) \rangle$ примитивны для $\forall H_m \in \{D_{2^m}, Q_{2^m}, M_{2^m}, SD_{2^m}\}.$



- I. Тогда для $\varphi_{rr}(H_m)$:
- группа $\tilde{v}_2 \varphi_{rr}(H_m)$ примитивна для $H_m \in \{Q_{2^m}, SD_{2^m}\};$
- группы $\langle \tilde{v}_2(s), \tilde{v}_2 \varphi_{rr}(H_m) \rangle, \tilde{v}_3 \varphi_{rr}(H_m), \langle \tilde{v}_3(s), \tilde{v}_3 \varphi_{rr}(H_m) \rangle$ примитивны для $\forall H_m \in \{D_{2^m}, Q_{2^m}, M_{2^m}, SD_{2^m}\}.$
- II. Тогда для $\varphi_{lr}(H_m)$:
- группа $\tilde{v}_2 \varphi_{lr}(H_m)$ примитивна для $\forall H_m \in \{D_{2^m}, Q_{2^m}, SD_{2^m}\};$
- группы $\langle \tilde{v}_2(s), \tilde{v}_2 \varphi_{lr}(H_m) \rangle$, $\langle \tilde{v}_3(s), \tilde{v}_3 \varphi_{lr}(H_m) \rangle$ примитивны для $\forall H_m \in \{D_{2^m}, Q_{2^m}, M_{2^m}, SD_{2^m}\};$
- группа $\tilde{v}_3 \varphi_{lr}(H_m)$ примитивна для $H_m \in \{M_{2^m}, Q_{2^m}\}$.





Спасибо за внимание!