$$x^8 + x^4 + x^3 + x^2 + 1$$



$$E_{l,k}^{(K_k)}$$

$$V_l \mapsto V_l$$

$$D_{l,k}^{(K_k)}$$

0 mod

 $mea_{l,k}$ 

$$\prod_{i=c}^{n} \tau^{(i)}$$

$$V_d \mapsto V_d$$

$$K \in V_k$$

 $i_i \in \{0, 1, 2, 3, ..., 35\}$ 

 $\mod 2$ O  $\mod 2 \neq 0$ 

$$(s_{a,d,h})$$

$$(s_{a,d,h}) \in V_8$$

$$a = \overline{0, r - 1}$$

$$d = \overline{0, s - 1}$$

$$B_1, B_2, B_4, \ldots, B_{l/8}$$

 $\mod 64 \neq 0$ 

$$E_{l,k}^{(K_k)} = \prod_{i=0}^{\sqrt{n}-1} \prod_{t=0}^{\sqrt{n}-1} (\kappa_l^{(K_z)} \odot \chi_l^{(\frac{t}{2})} \odot \pi_l \odot \Gamma_l \odot \Omega_l \odot \vartheta_l) ||(\kappa_l^{(K_z)} \odot (\vartheta_l | \Omega_l | \Gamma_l | \chi_l^{(\frac{t+1}{2})} | \kappa_l^{(K_z)}) \Psi^{(K_z)}),$$

$$(s_{a,d,h})$$

$$(s_{a,d,h}) \in GF(2^8)$$

 $b \in \{0, 1, 2, 3\}$ 

$$\chi_l^{(\frac{t+1}{2})}$$

$$h = \frac{t+1}{2}$$

$$\chi_l^{(\frac{t}{2})}$$

$$h = \frac{t}{2}$$

$$\kappa_l^{(K_z)}$$

$$K_l^{(K_z)}, z = i \times 6 + t$$

$$\chi_l^{((t+1)/2)}$$

$$\chi_l^{(t/2)}$$

$$r = 4, s = 4, h = \overline{0,3}$$

r = 8, s = 8, h = 1

$$S = (s_{a,d,h})$$

$$r_h \in \{0, 1, 2, 3\}$$

$$\zeta_r = \frac{r \times l}{512}$$

$$(S_{a,d,h}) = \begin{vmatrix} x_{00} & x_{01} & x_{02} & x_{03} \\ x_{10} & x_{11} & x_{12} & x_{13} \\ x_{20} & x_{21} & x_{22} & x_{23} \\ x_{30} & x_{31} & x_{32} & x_{33} \end{vmatrix} \Rightarrow \begin{vmatrix} x_{00} & x_{01} & x_{02} & x_{03} \\ x_{13} & x_{10} & x_{11} & x_{12} \\ x_{22} & x_{23} & x_{20} & x_{21} \\ x_{31} & x_{32} & x_{33} & x_{30} \end{vmatrix}$$

$$s_{a,d,h} \in V_8$$

$$\beta_r \mod 4(s_{a,d,h})$$

$$\beta_b: V_8 \mapsto V_8, b \in \{0, 1, 2, 3\}$$

 $s_{a.a.}$ 

$$\beta_0(0x33) = 0xf7$$

$$s_h \in \{0, 1, 2, 3\}$$

$$\zeta_s = \frac{s \times l}{512}$$

$$(S_{a,d,h}) = \begin{vmatrix} x_{00} & x_{01} & x_{02} & x_{03} \\ x_{10} & x_{11} & x_{12} & x_{13} \\ x_{20} & x_{21} & x_{22} & x_{23} \\ x_{30} & x_{31} & x_{32} & x_{33} \end{vmatrix} \Rightarrow \begin{vmatrix} x_{00} & x_{31} & x_{22} & x_{13} \\ x_{10} & x_{01} & x_{32} & x_{23} \\ x_{20} & x_{11} & x_{02} & x_{33} \\ x_{30} & x_{21} & x_{12} & x_{03} \end{vmatrix}$$

r = 8, s = 8; h = 1

$$\eta(x) = x^8 + x^4 + x^3 + x^2 + 1$$

$$T = (t_{a,d})$$

$$(t_{a,d}) = (q \ggg a) \otimes S_d$$

$$S = (s_{a,d,h}), r = 8, s = 8, h = 1$$

 $h \in \{0, 1, 2, 3\}$ 

$$S = (s_{a,d,h}), r = 4, s = 4, h = \overline{0,3}$$

$$(S_{a,d,h}) = \begin{vmatrix} x_{00} & x_{01} & x_{02} & x_{03} \\ x_{10} & x_{11} & x_{12} & x_{13} \\ x_{20} & x_{21} & x_{22} & x_{23} \\ x_{30} & x_{31} & x_{32} & x_{33} \end{vmatrix} \Rightarrow \begin{vmatrix} x_{03} & x_{13} & x_{23} & x_{33} \\ x_{02} & x_{12} & x_{22} & x_{32} \\ x_{01} & x_{11} & x_{21} & x_{31} \\ x_{00} & x_{10} & x_{20} & x_{30} \end{vmatrix}$$

$$K_z \in V_l$$

 $z \in \{0, 1, 2, ..., 35\}$ 

$$D_{l,k}^{(K_k)} = \prod_{i=\sqrt{n}-1}^{0} \prod_{t=\sqrt{n}-1}^{0} (\hat{\vartheta}_l \odot \hat{\Omega}_l \odot \hat{\Gamma}_l \odot \hat{\pi}_l \odot \chi_l^{(\frac{\hat{\iota}}{2})} \odot \kappa_l^{(K_z)}) ||(\hat{\vartheta}_l |\hat{\Omega}_l |\hat{\Gamma}_l | \hat{\pi}_l | \chi_l^{(\frac{\hat{\iota}+1}{2})} |\kappa_l^{(K_z)}) \Psi^{(K_z)} \odot \kappa_l^{(K_z)}),$$

$$\chi_l^{(\frac{\hat{t}+1}{2})}$$

$$\chi_l^{(\hat{\frac{t}{2}})}$$

$$h = \frac{h}{2}$$

$$\chi_l^{((t+1)/2)}$$

$$\chi_l^{(\hat{t}/2)}$$

$$r = 4, s = 4, h = \overline{0,3},$$

$(S_{a,d,h}) =$	$ x_{00} $	$x_{01}$	$x_{02}$	$x_{03}$	$\Rightarrow$	$x_{00}$	$x_{01}$	$x_{02}$	$x_{03}$
	$x_{10}$	$x_{11}$	$x_{12}$	$x_{13}$		$x_{11}$	$x_{12}$	$x_{13}$	$x_{10}$
	$ x_{20} $	$x_{21}$	$x_{22}$	$x_{23}$		$x_{22}$	$x_{23}$	$x_{20}$	$x_{21}$
	$ x_{30} $	$x_{31}$	$x_{32}$	$x_{33}$		$ x_{33} $	$x_{30}$	$x_{31}$	$x_{32}$

$$-\beta_r \mod 4(s_{a,d,h})$$

$$-\beta_b: V_8 \mapsto V_8, b \in \{0, 1, 2, 3\}$$

$$-\beta_0(0xf7) = 0x33$$

$$(S_{a,d,h}) = \begin{vmatrix} x_{00} & x_{01} & x_{02} & x_{03} \\ x_{10} & x_{11} & x_{12} & x_{13} \\ x_{20} & x_{21} & x_{22} & x_{23} \\ x_{30} & x_{31} & x_{32} & x_{33} \end{vmatrix} \Rightarrow \begin{vmatrix} x_{00} & x_{11} & x_{22} & x_{33} \\ x_{10} & x_{21} & x_{32} & x_{03} \\ x_{20} & x_{31} & x_{02} & x_{13} \\ x_{30} & x_{01} & x_{12} & x_{23} \end{vmatrix}$$

$$\hat{T} = (\hat{t}_{a,d})$$

$$(\hat{t}_{a,d}) = (\hat{q} \lll a) \otimes S_d$$

$$\chi_l^{(\hat{h})}$$

$(S_{a,d,h}) =$	$ x_{00} $	$x_{01}$	$x_{02}$	$x_{03}$	$\Rightarrow$	$ x_{30} $	$x_{20}$	$x_{10}$	$x_{00}$
	$x_{10}$	$x_{11}$	$x_{12}$	$x_{13}$		$x_{31}$	$x_{21}$	$x_{11}$	$x_{01}$
	$ x_{20} $	$x_{21}$	$x_{22}$	$x_{23}$		$ x_{32} $	$x_{22}$	$x_{12}$	$x_{02}$
	$ x_{30} $	$x_{31}$	$x_{32}$	$x_{33}$		$ x_{33} $	$x_{23}$	$x_{13}$	$x_{03}$

 $K_z, z \in \{0, 1, 2, ..., 35\}$ 

$$\alpha = K_k$$

$$\alpha = K_{-z}$$

$$G^{(K_k)} = \kappa_k^{(\alpha)} \odot \mathcal{F}_k \odot \Gamma_k \odot \Omega_k^{(rh)} \odot \kappa_k^{(\alpha)},$$

$$\kappa_k^{(K_z)}$$

$$\kappa_k^{(\hat{K}_z)}$$

$$\Omega_k^{(rh)}$$

$$rh = \{1, 0, 3, 2, 3, 0, 1, 2\}$$

$$(k_{a,d,h})$$

$$(k_{a,d,h}) \in GF(2^8)$$

$$h=2\mapsto h=3$$

$$h=3\mapsto h=2$$

 $K_{F}$ ıTr(

$$Rt_{\sqrt{n}} \in R_{\frac{n}{2}}$$

$$t \in \{0, 1, 2, ..., \frac{n}{2} - 1\}$$

$$\Psi^{(K_z)} = \prod_{i=0}^{\sqrt{n}-1} \prod_{t=0}^{\frac{n}{2}} \prod_{z=0}^{\sqrt{n}-2} Rt_{(\iota_{K_{(i+t)}}^{(z)})} \doteq Rt_{(\iota_{K_{(i+t)}}^{(z+1)})},$$

$$\iota_{K_{(i+t)}}^{(-z)}$$

$$-y \in K_{[-z]}$$

$$K_z \in K_{z=i+t}$$

$$-\beta_0 =$$

$$-\beta_3 =$$