γ_2

AES

$k \oplus M = \gamma_2$

CBT

$S_1 \oplus S_2 = S_0$

$C = (S_1 \oplus S_3) \oplus k$

$$\begin{cases} S_1 = H(S_0) \\ S_2 = H_2(S_0) \oplus S_1 \end{cases}$$

P — seed → V

AES $\Leftarrow$ Hash(seed) $\{0,1\}^{128}$

$\Downarrow$

$x_1, \cdots, x_n$

$k = C \oplus (S_1 \oplus S_3)$

FS

$M_2 k \oplus \gamma_i \cdot \Delta$