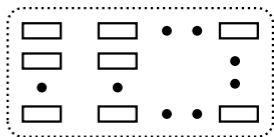
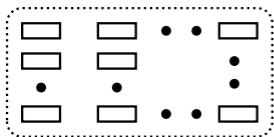


X Y  \oplus R \downarrow \mathcal{P} Blake2b
round \mathcal{P} \dots \mathcal{P} \downarrow Q \downarrow \mathcal{P} \mathcal{P} \dots \mathcal{P} Z \oplus \downarrow 