

 $D_0$ 

begd

 $R_0$ 

R: receiver context X: invalid, D: data

S: shuffle, S<sup>-1</sup>: inverse shuffle