23-round differential Distinguisher of probability 2^-61.5

■ : This key bit is guessed by the upper part of the attack
□ : This state bit can be computed by the upper part of the attack

■ : This key bit is guessed by the lower part of the attack
□ : This state bit can be computed by the lower part of the attack

0 : The difference on this bit is 0
1 : The difference on this bit is 1
? : The difference on this bit can be 0 or 1
? : The difference on this bit is considered 0 by probabilist propagation
■ : This bit takes all possible values
■ : The value of this bit is fix for a specific structure