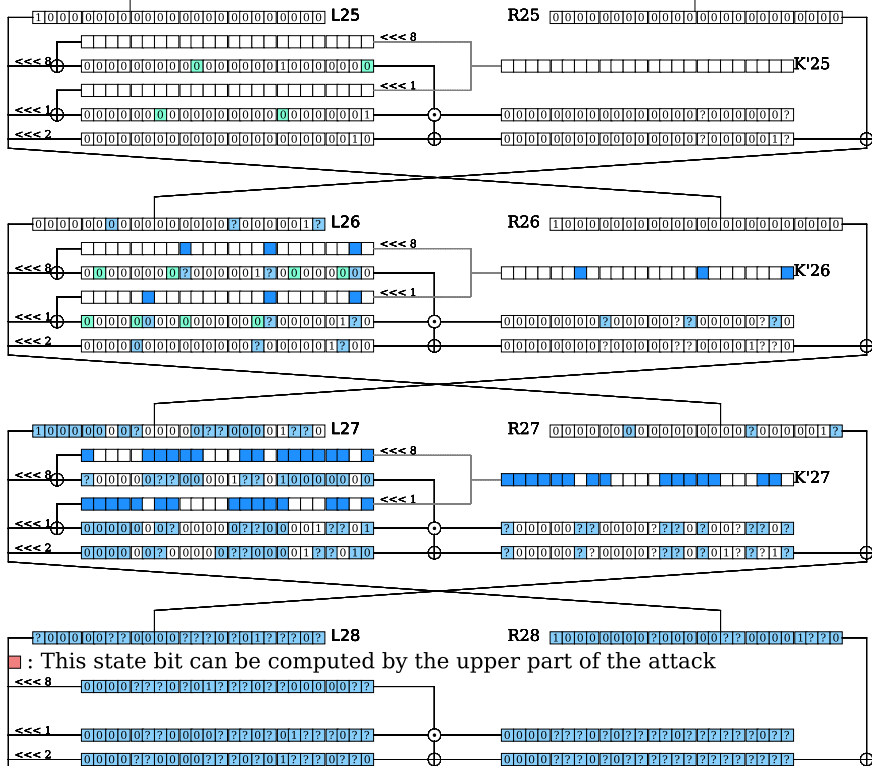


17-rounds differential distinguisher



■: This key bit is guessed by the upper part of the attack

■: This state bit is guessed by the upper part of the attack, it is used to sieve the candidates during the match

■: 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

■: This state bit is guessed by the lower part of the attack, it is used to sieve the candidates during the match

■: The difference on this bit is 0

■: 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

■: The difference on this bit can be computed by the upper and lower part of the attack

■: The value of this bit is fix