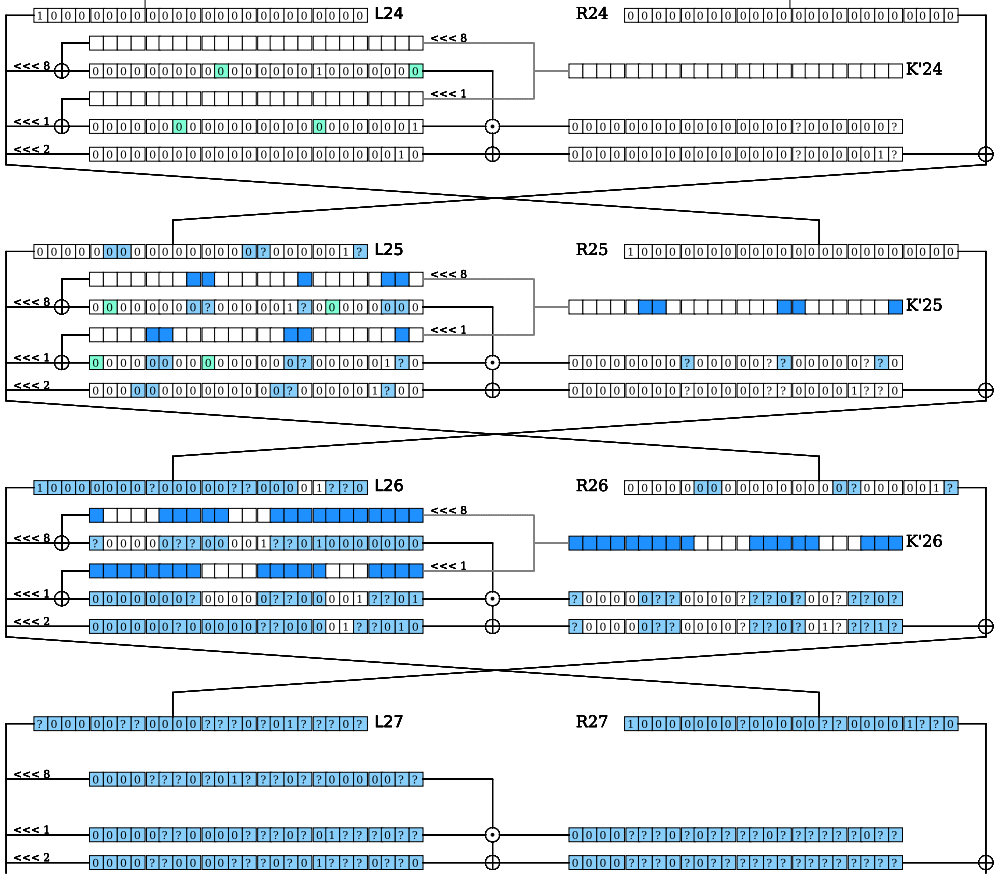


17-rounds differential distinguisher



- Red: This key bit is guessed by the upper part of the attack
- Red: This state bit can be computed by the upper part of the attack
- Yellow: This state bit is guessed by the upper part of the attack, it is used to sieve the candidates during the match
- Blue: This key bit is guessed by the lower part of the attack
- Blue: This state bit can be computed by the lower part of the attack
- Green: This state bit is guessed by the lower part of the attack, it is used to sieve the candidates during the match
- 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
- P: The difference on this bit is considered 0 by probabilist propagation
- Green: The difference on this bit can be computed by the upper and lower part of the attack
- Grey: The value of this bit is fix