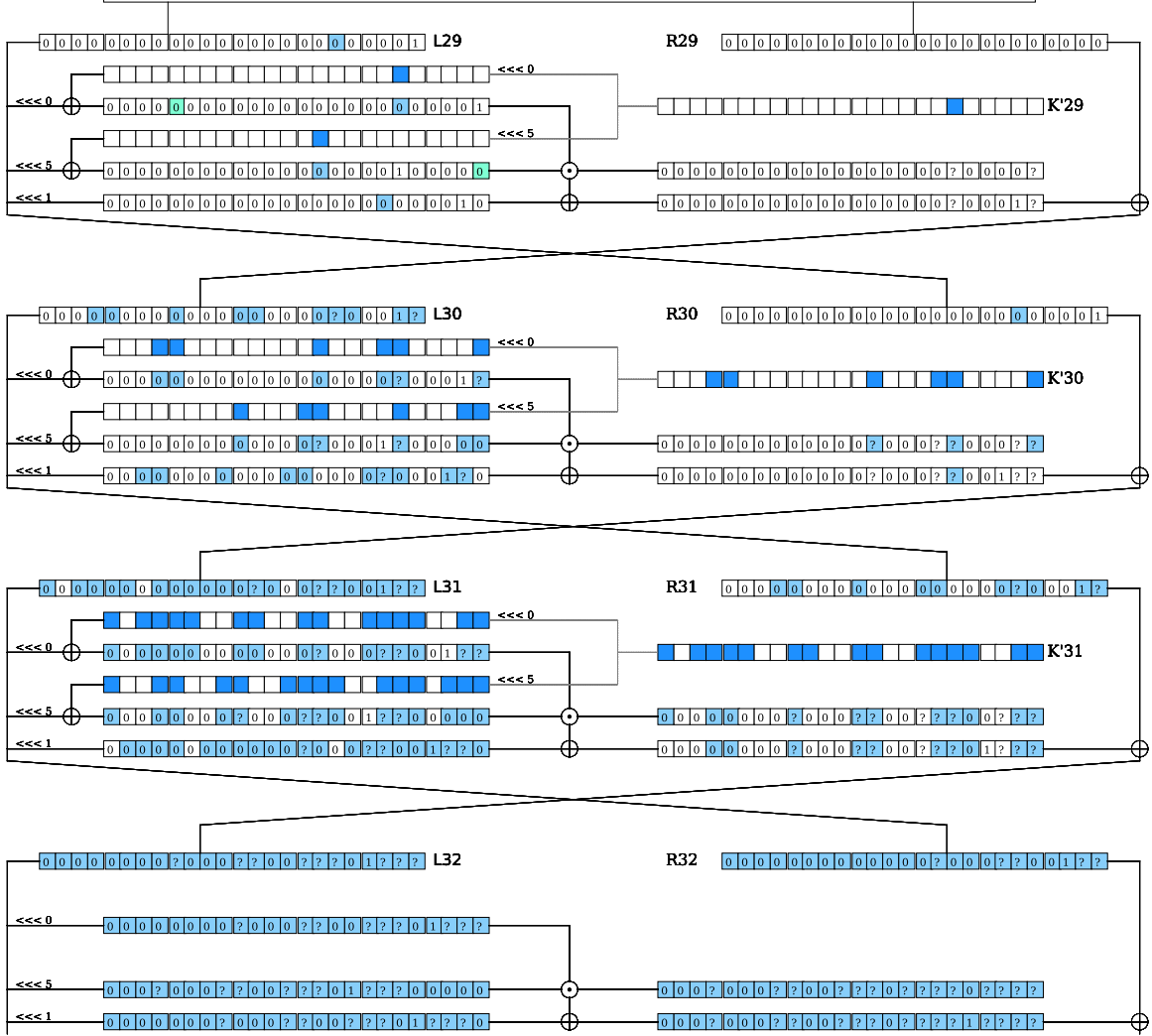


## 23-rounds differential distinguisher



- Red square: This key bit is guessed by the upper part of the attack
- Red square: This state bit can be computed by the upper part of the attack
- Yellow square: This state bit is guessed by the upper part of the attack, it is used to sieve the candidates during the match
- Blue square: This key bit is guessed by the lower part of the attack
- Blue square: This state bit can be computed by the lower part of the attack
- Green square: 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

- : The difference on this bit can be computed by the upper and lower part of the attack
- : The value of this bit is fix