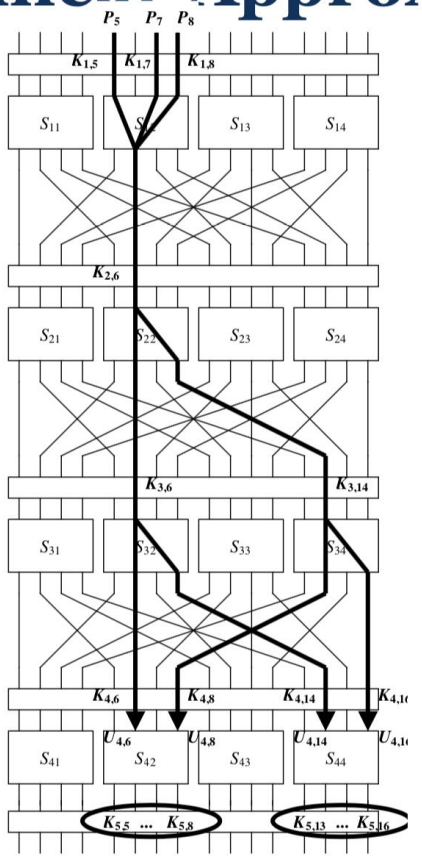
Answer why a final key mixing is required by a cipher

1901210488 时绍森

Linear Approximation of SPN



S_{12}: $X_1 \oplus X_3 \oplus X_4 = Y_2$ with probability 12/16 and bias +1/4
S_{22}: $X_2 = Y_2 \oplus Y_4$ with probability 4/16 and bias −1/4
S_{32}: $X_2 = Y_2 \oplus Y_4$ with probability 4/16 and bias −1/4
S_{34}: $X_2 = Y_2 \oplus Y_4$ with probability 4/16 and bias −1/4

用 **SPN** 举例，若没有最后一轮 **key mixing**，由于 **S** 盒是已知的，因此可以直接根据输出倒推至倒数第二轮加密后的状态，那么最后一轮 **S** 盒就没有意义了。