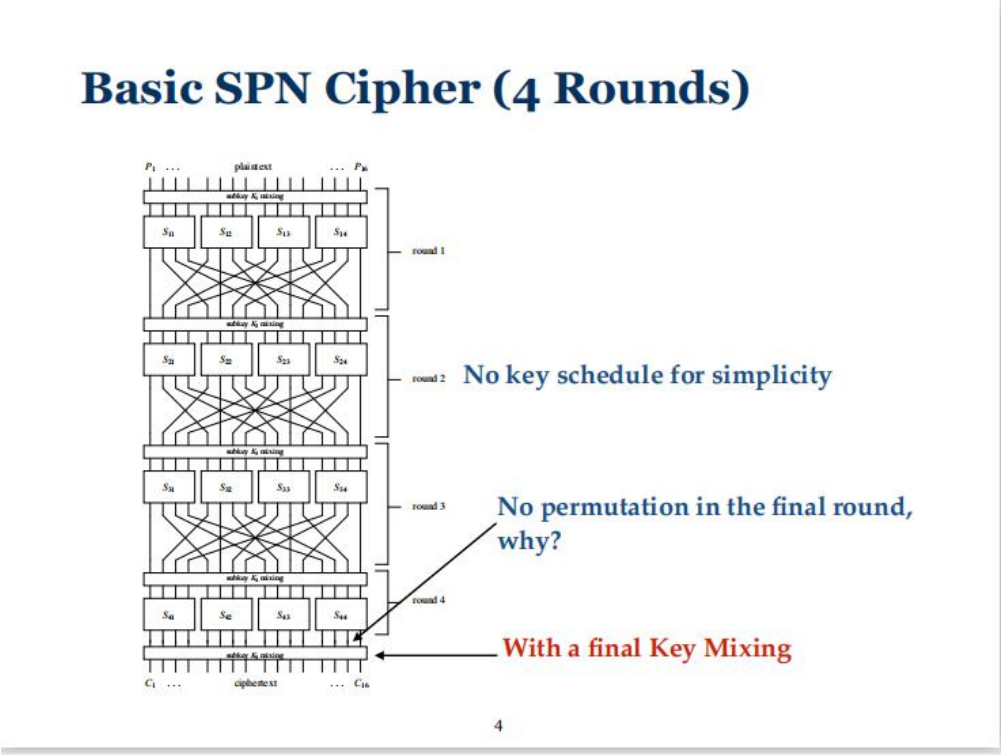
Why a final key mixing is required by a cipher?

一、SPN 结构密码的加密过程



二、问题分析

若没有最后一轮的轮密钥加，则可以直接获得倒数第二轮输出的密文C'，失去了最后一轮置换加密的意义，导致加密轮数不足而造成的密码安全性不足。

差分密码分析过程如下：通过最后一轮输出的密文C以及相应的$S-box$,可直接获得倒数第二轮输出的密文C'。差分分析将直接从C'开始进行，通过枚举倒数第二轮的密钥K_{R-1}来获得倒数第二轮输出的密文C''。通过检验选择的部分明文和获得的倒数第二轮输出密文组成的$(M，C'')$是否符合前$R-2$轮加密函数$F_{R-2}(\ )$的差分特性，以获得倒数第二轮的轮密钥K_{R-1}。再穷举第三轮的轮密钥检验在各轮密钥参与加密的情况下$(M，C''')$是否符合$F_{R-3}(\ )$的差分特性，由此获得

倒数第三轮的轮密钥。以此类推，逐渐获得所有的轮密钥。

线性密码分析过程与差分密码分析的过程基本相同，仅将验证明文密文对(M,C'')是否满足差分特征转换为验证(M,C'')是否满足加密函数的线性特征即可。