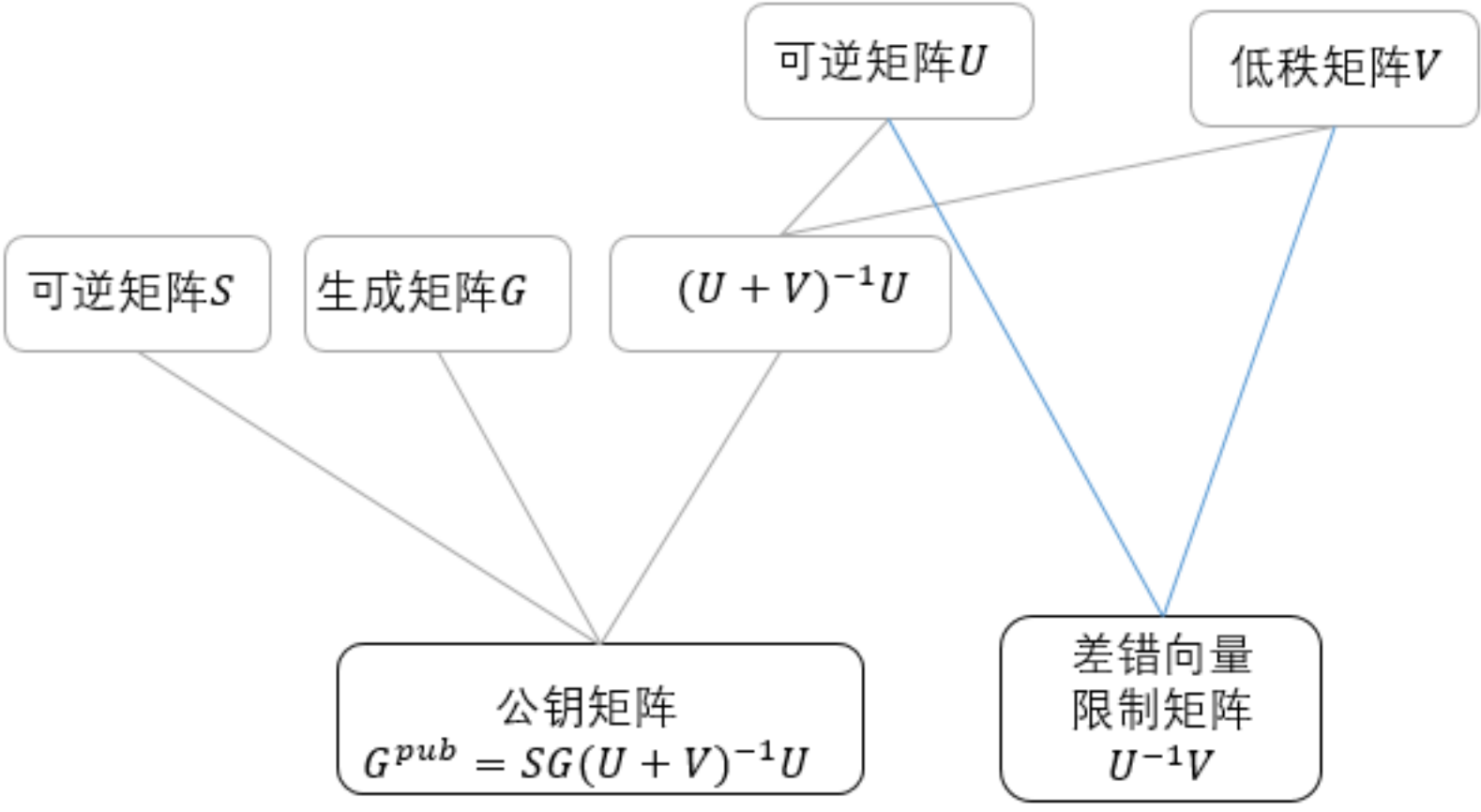
可逆矩阵U
低秩矩阵V
可逆矩阵S
生成矩阵G
$(U+V)^{-1}U$
公钥矩阵
$G^{pub}=SG(U+V)^{-1}U$
差错向量
限制矩阵
$U^{-1}V$