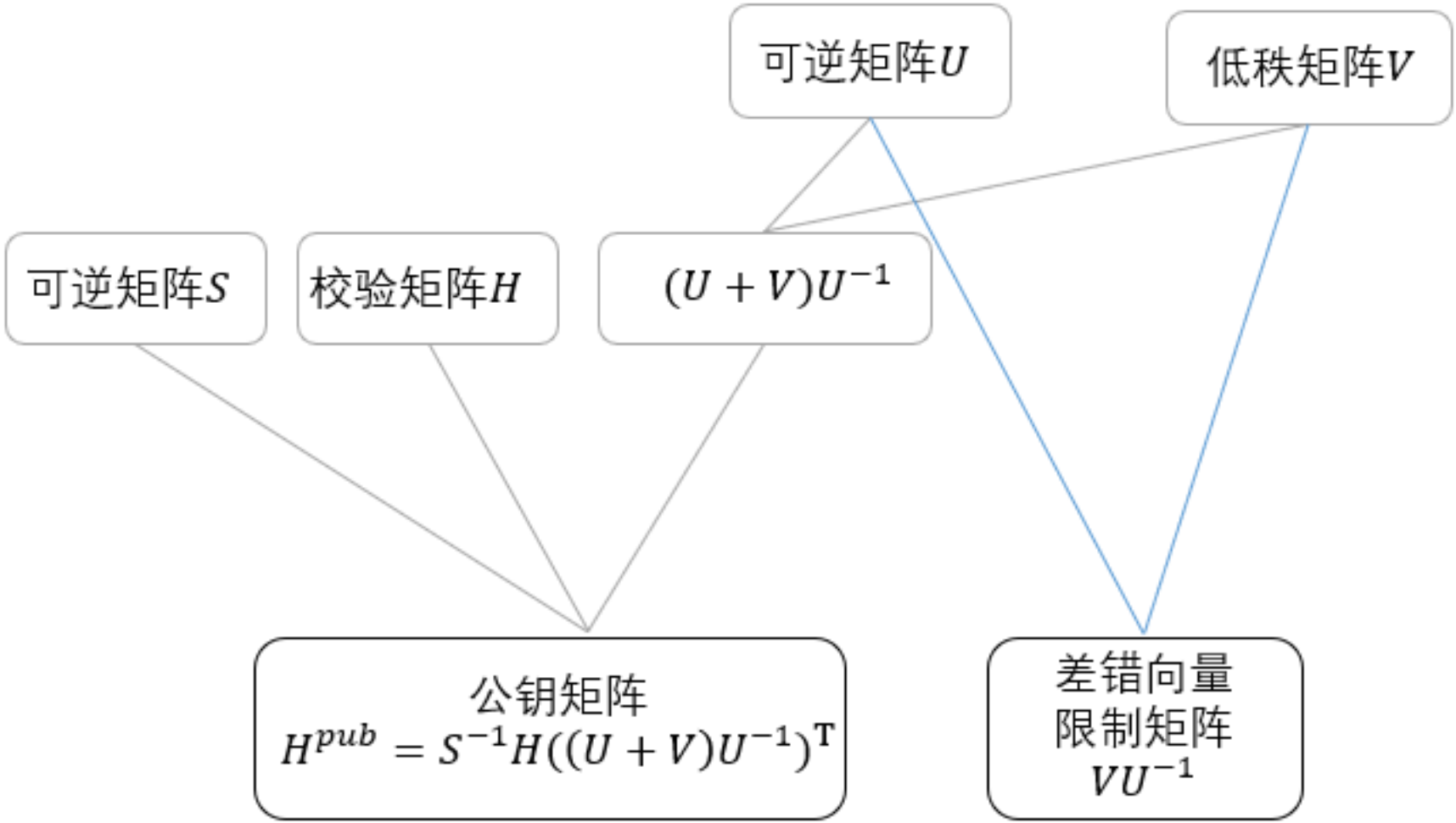
可逆矩阵U
低秩矩阵V
可逆矩阵S
校验矩阵H
$(U+V)U^{-1}$
公钥矩阵
$H^{pub}=S^{-1}H((U+V)U^{-1})^{\mathrm{T}}$
差错向量
限制矩阵
VU^{-1}