

密钥管理器

MLE密钥

$K_M$

$G$

$\oplus$

$H$

$t$

$C$

$|$

$C$

$t$

CAONT

存根

修剪包

明文

$M$

$M$

$c$

修剪包