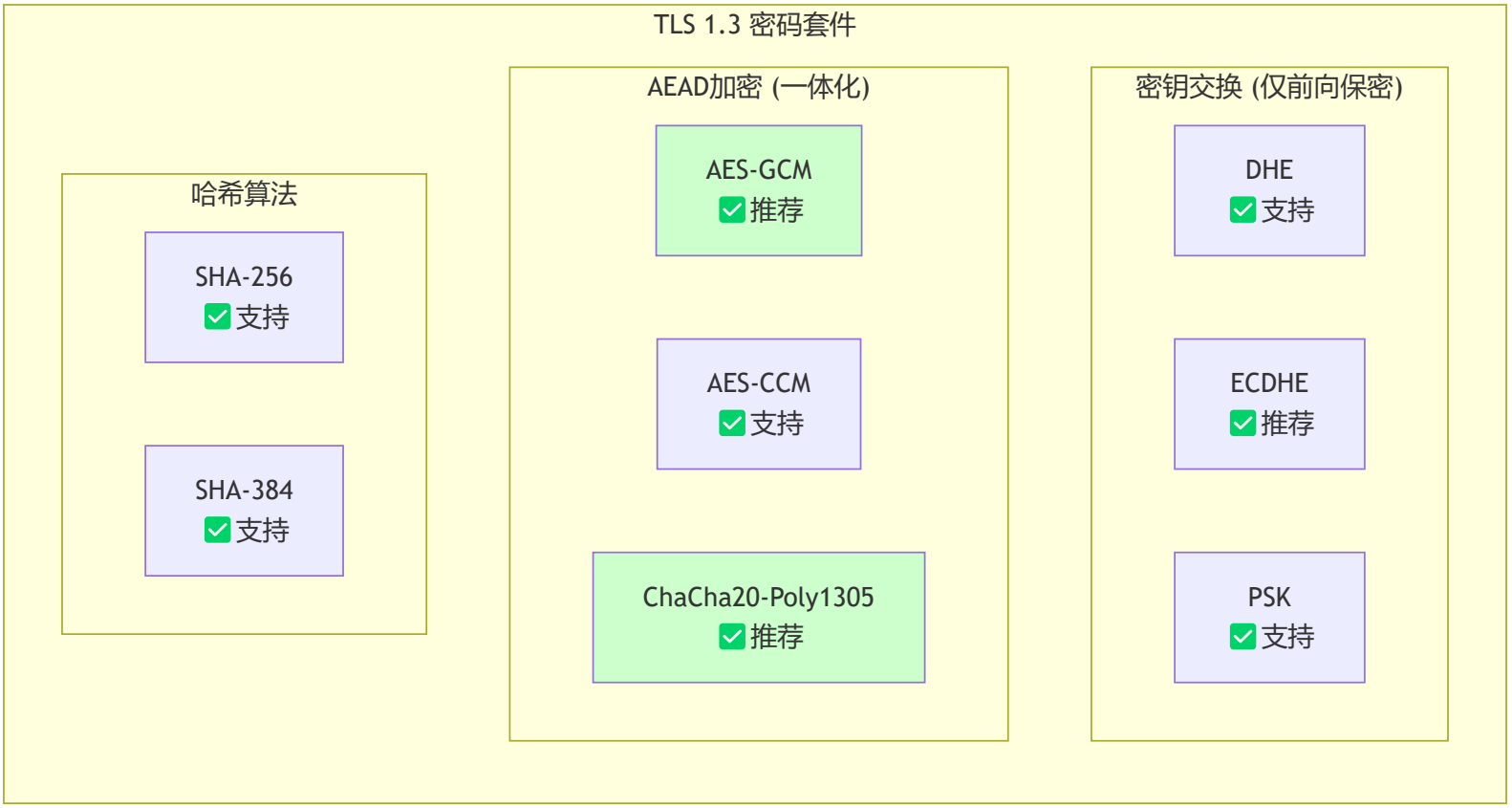
TLS 1.3 密码套件
哈希算法
SHA-256
✅支持
SHA-384
✅支持
AEAD加密 (一体化)
AES-GCM
✅推荐
AES-CCM
✅支持
ChaCha20-Poly1305
✅推荐
密钥交换 (仅前向保密)
DHE
✅支持
ECDHE
✅推荐
PSK
✅支持


TLS 1.2 密码套件
消息认证
SHA-1
❌不推荐
SHA-256
✅推荐
SHA-384
✅推荐
对称加密
AES-CBC
⚠️存在风险
AES-GCM
✅推荐
RC4
❌已禁用
ChaCha20
✅推荐
密钥交换
RSA
❌不推荐
DHE
✅推荐
ECDHE
✅推荐
PSK
✅特殊场景