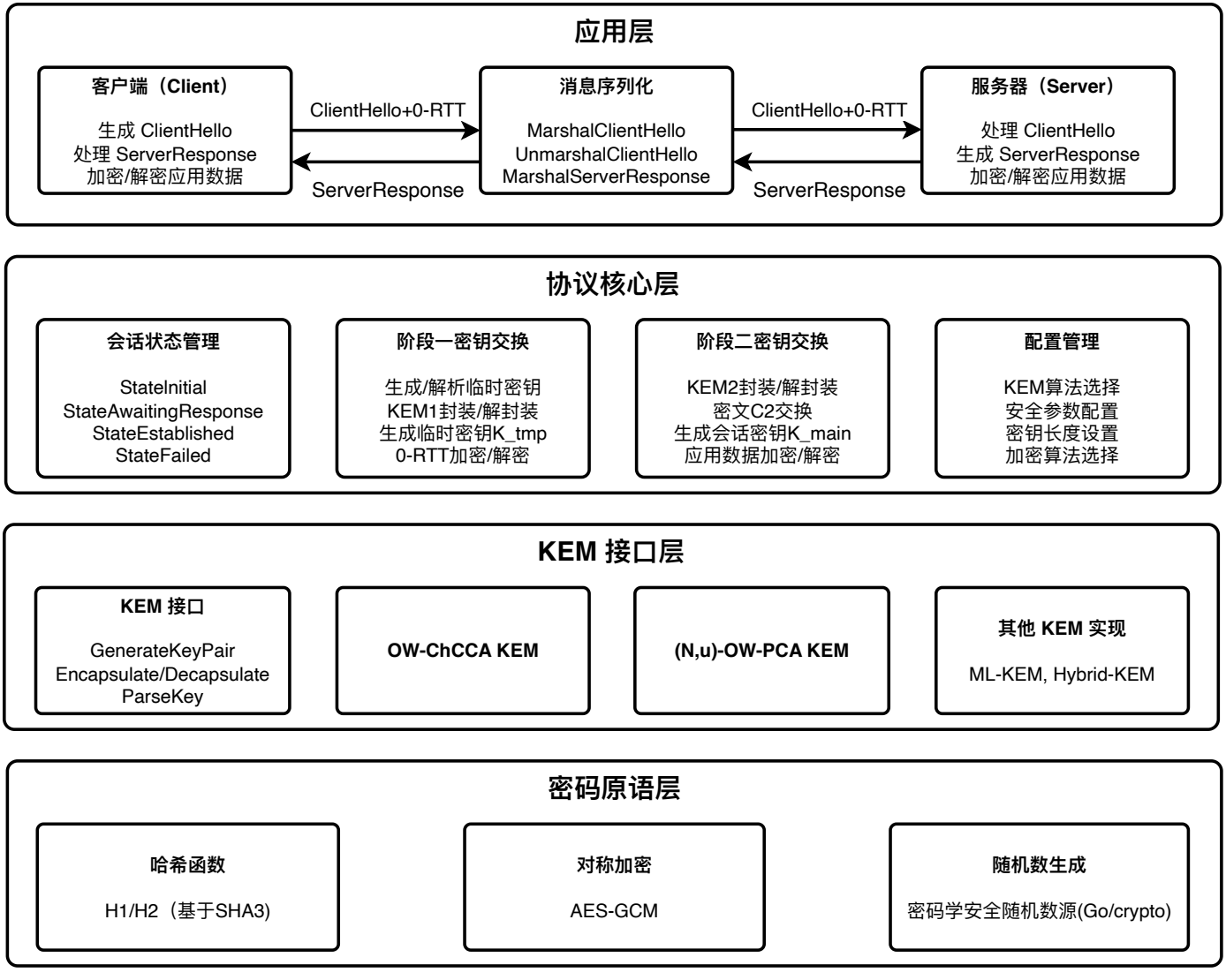
应用层
客户端（Client）
生成 ClientHello
处理 ServerResponse
加密/解密应用数据
ClientHello+0-RTT
ServerResponse
消息序列化
MarshalClientHello
UnmarshalClientHello
MarshalServerResponse
ClientHello+0-RTT
ServerResponse
服务器（Server）
处理 ClientHello
生成 ServerResponse
加密/解密应用数据
协议核心层
会话状态管理
StateInitial
StateAwaitingResponse
StateEstablished
StateFailed
阶段一密钥交换
生成/解析临时密钥
KEM1封装/解封装
生成临时密钥K_tmp
0-RTT加密/解密
阶段二密钥交换
KEM2封装/解封装
密文C2交换
生成会话密钥K_main
应用数据加密/解密
配置管理
KEM算法选择
安全参数配置
密钥长度设置
加密算法选择
KEM 接口层
KEM 接口
GenerateKeyPair
Encapsulate/Decapsulate
ParseKey
OW-ChCCA KEM
(N,u)-OW-PCA KEM
其他 KEM 实现
ML-KEM, Hybrid-KEM
密码原语层
哈希函数
H1/H2（基于SHA3)
对称加密
AES-GCM
随机数生成
密码学安全随机数源(Go/crypto)