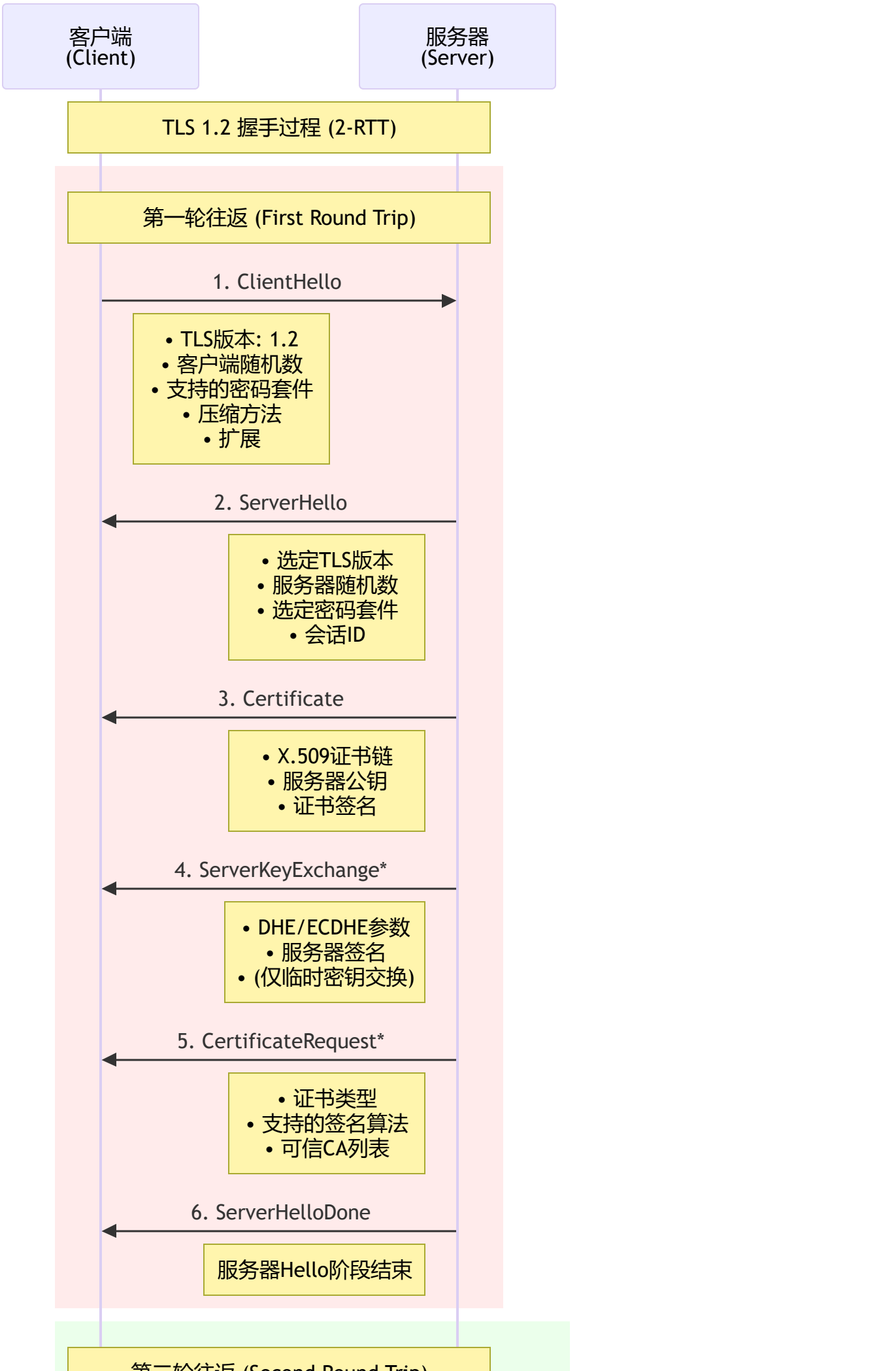
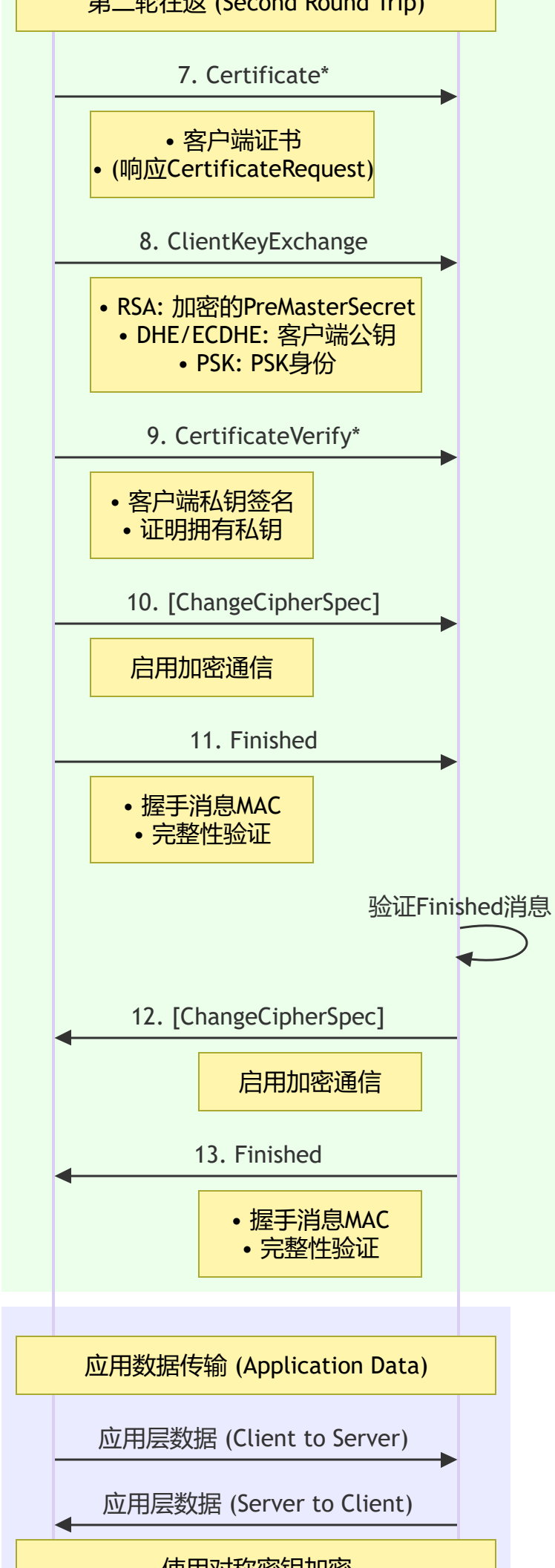
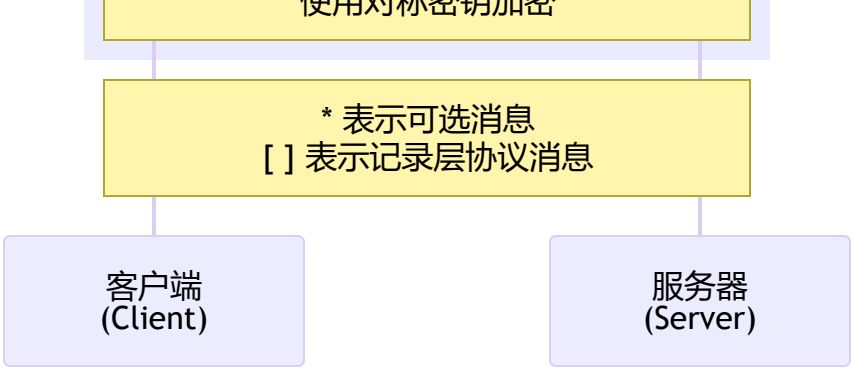

客户端
(Client)
服务器
(Server)
TLS 1.2 握手过程 (2-RTT)
第一轮往返 (First Round Trip)
1. ClientHello
• TLS版本: 1.2
• 客户端随机数
• 支持的密码套件
• 压缩方法
• 扩展
2. ServerHello
• 选定TLS版本
• 服务器随机数
• 选定密码套件
• 会话ID
3. Certificate
• X.509证书链
• 服务器公钥
• 证书签名
4. ServerKeyExchange*
• DHE/ECDHE参数
• 服务器签名
• (仅临时密钥交换)
5. CertificateRequest*
• 证书类型
• 支持的签名算法
• 可信CA列表
6. ServerHelloDone
服务器Hello阶段结束


第二轮往返 (Second Round Trip)
7. Certificate*
• 客户端证书
• (响应CertificateRequest)
8. ClientKeyExchange
• RSA: 加密的PreMasterSecret
• DHE/ECDHE: 客户端公钥
• PSK: PSK身份
9. CertificateVerify*
• 客户端私钥签名
• 证明拥有私钥
10. [ChangeCipherSpec]
启用加密通信
11. Finished
• 握手消息MAC
• 完整性验证
验证Finished消息
12. [ChangeCipherSpec]
启用加密通信
13. Finished
• 握手消息MAC
• 完整性验证
应用数据传输 (Application Data)
应用层数据 (Client to Server)
应用层数据 (Server to Client)


使用对称密钥加密
* 表示可选消息
[ ] 表示记录层协议消息
客户端
(Client)
服务器
(Server)