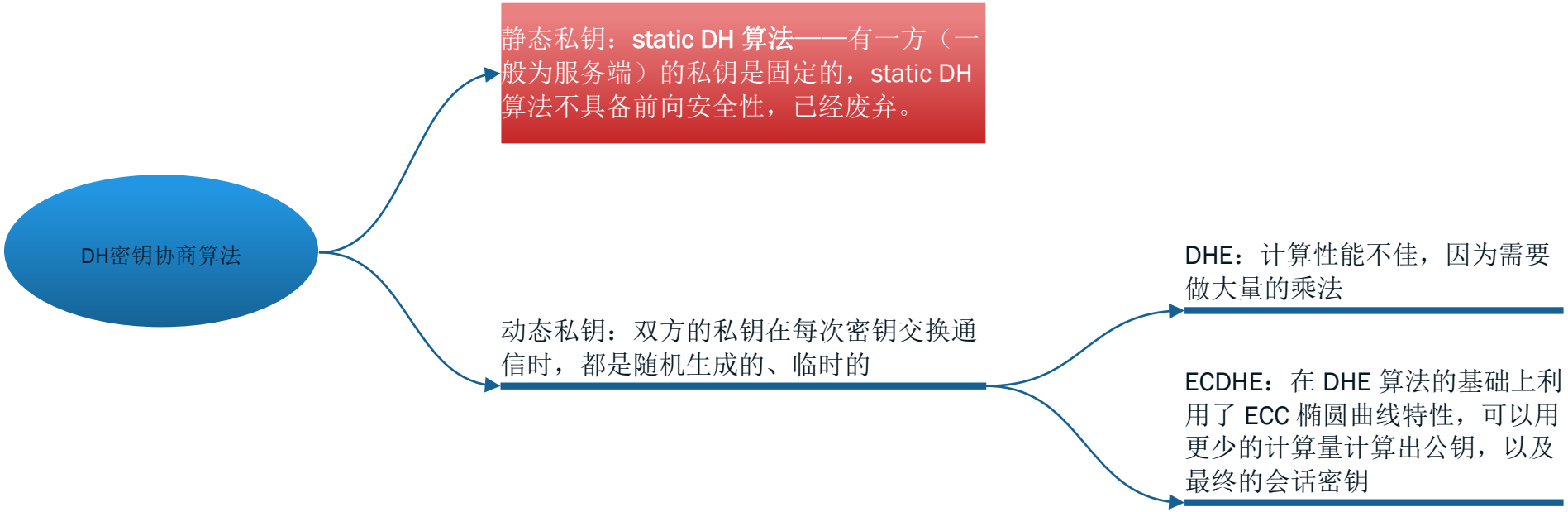
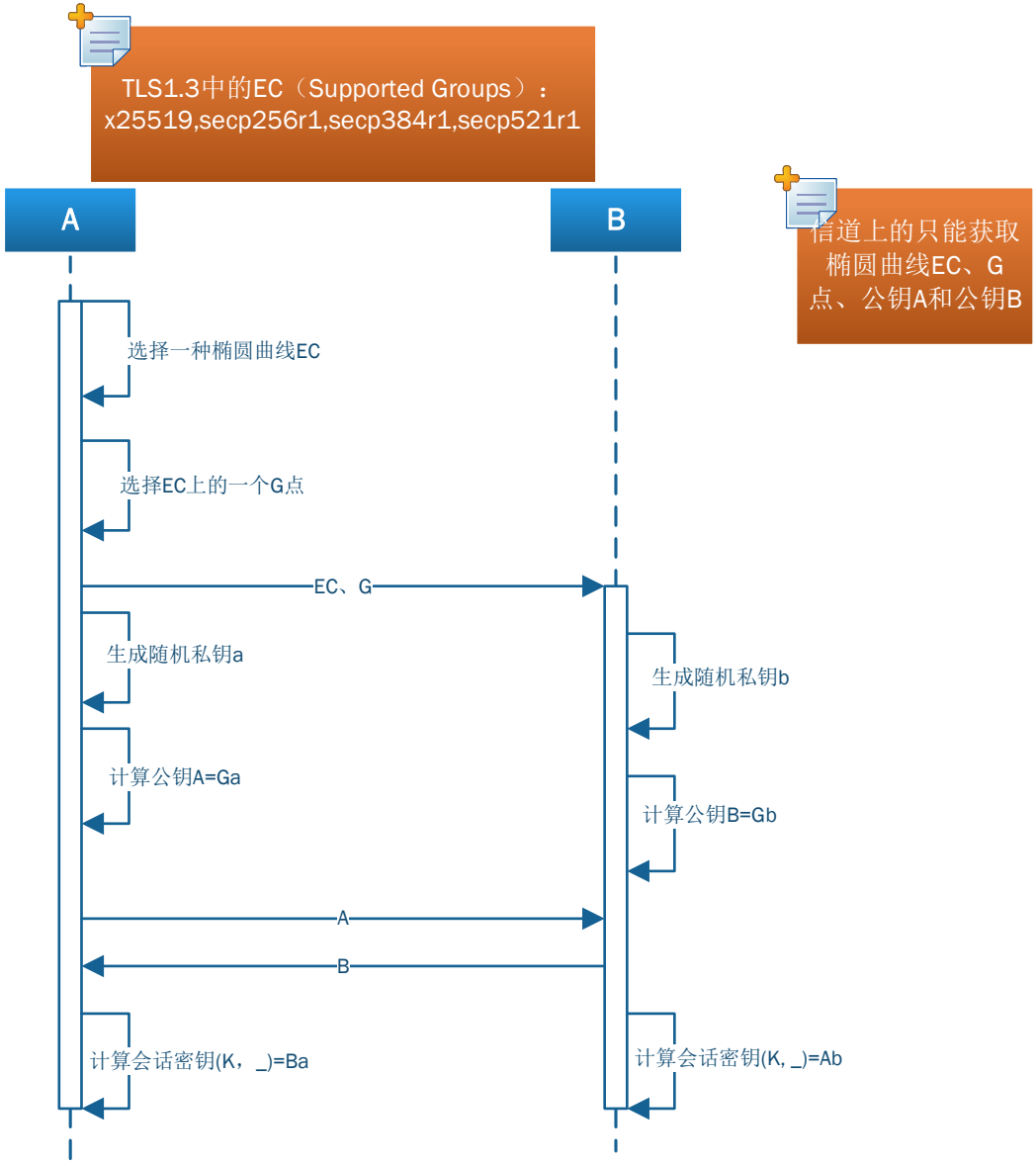
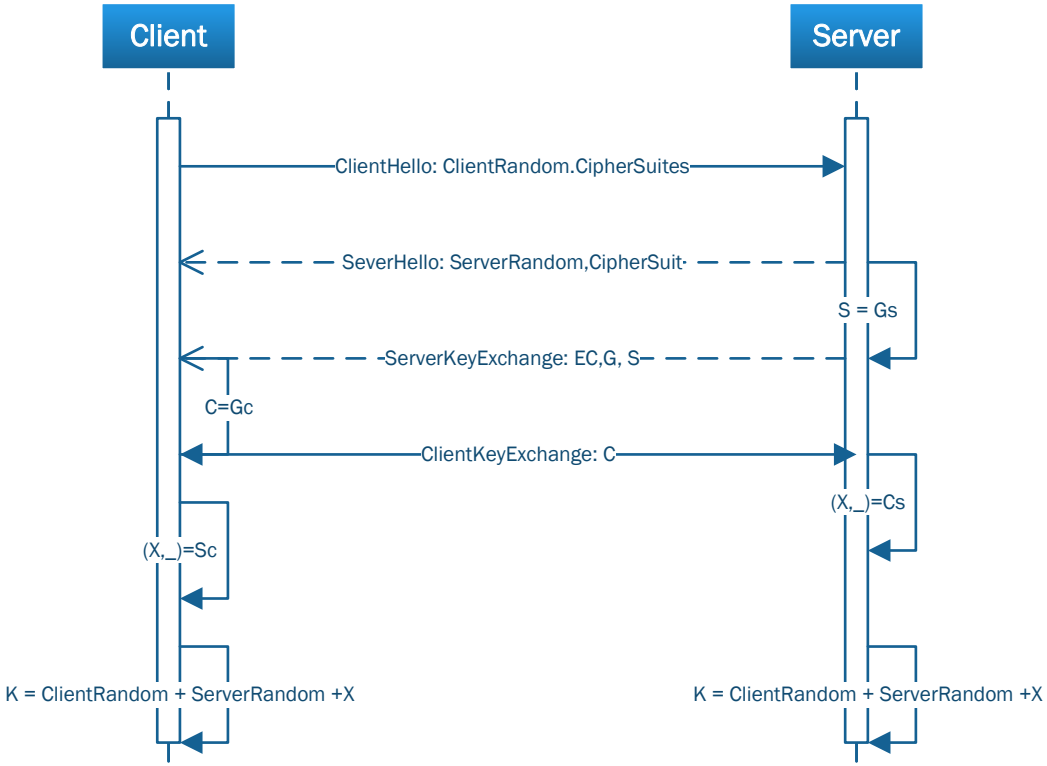
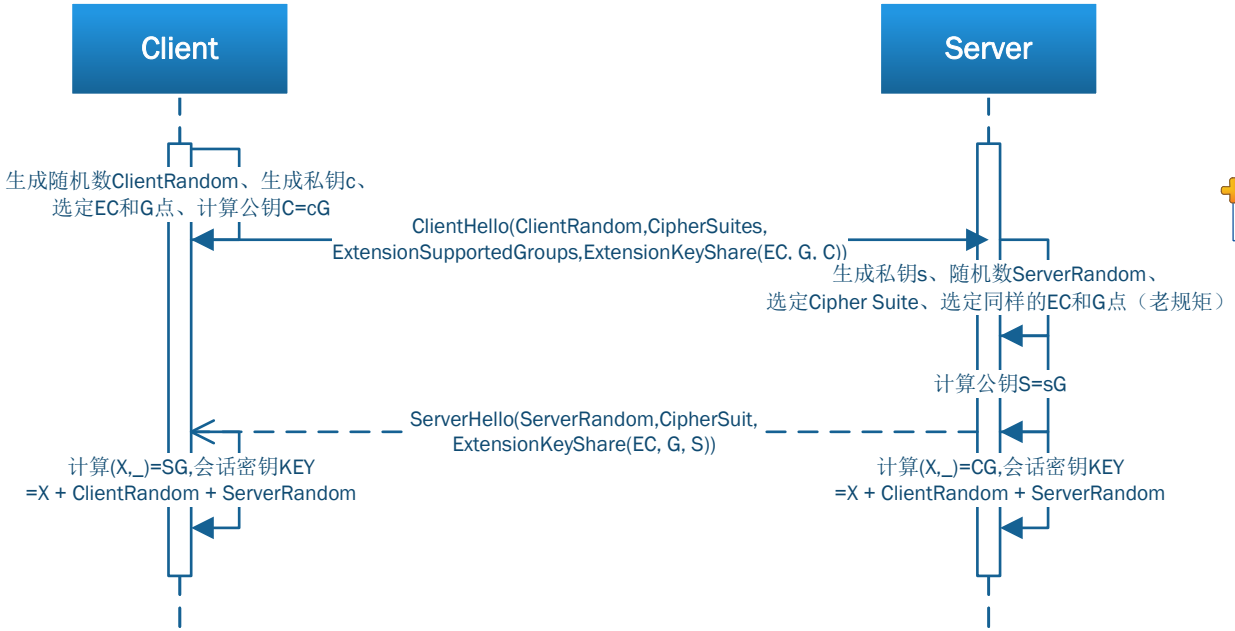

DH密钥协商算法
静态私钥：static DH 算法——有一方（一般为服务端）的私钥是固定的，static DH 算法不具备前向安全性，已经废弃。
动态私钥：双方的私钥在每次密钥交换通信时，都是随机生成的、临时的
DHE：计算性能不佳，因为需要做大量的乘法
ECDHE：在 DHE 算法的基础上利用了 ECC 椭圆曲线特性，可以用更少的计算量计算出公钥，以及最终的会话密钥


TLS1.3中的EC（Supported Groups）：
x25519,secp256r1,secp384r1,secp521r1
A
B
信道上的只能获取
椭圆曲线EC、G
点、公钥A和公钥B
选择一种椭圆曲线EC
选择EC上的一个G点
EC、G
生成随机私钥a
生成随机私钥b
计算公钥A=Ga
计算公钥B=Gb
A
B
计算会话密钥(K，_)=Ba
计算会话密钥(K, _)=Ab

Protocol	Length	Info
TLSv1.2	571	Client Hello
TLSv1.2	1474	Server Hello
TLSv1.2	1021	Certificate, Server Key Exchange, Server Hello Done
TLSv1.2	180	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
TLSv1.2	105	Change Cipher Spec, Encrypted Handshake Message



```
TLSv1.3    336 Client Hello
TLSv1.3   1443 Server Hello, Change Cipher Spec, Encrypted Extensions, Certificate, Certificate Verify, Finished
TLSv1.3    132 Change Cipher Spec, Finished
```



对比TLS1.2，减少了一次RTT（由2次减少为1次）

根据rfc8446：Clients can offer as many KeyShareEntry values as the number of supported groups it is offering, each representing a single set of key exchange parameters.（更多信息查看的Section 4.2.8）（下面的pcap截图：1比4的关系）

```
Extension: supported_groups (len=10)
    Type: supported_groups (10)
    Length: 10
    Supported Groups List Length: 8
  Supported Groups (4 groups)
      Supported Group: x25519 (0x001d)
      Supported Group: secp256r1 (0x0017)
      Supported Group: secp384r1 (0x0018)
      Supported Group: secp521r1 (0x0019)
```

```
Extension: key_share (len=38)
    Type: key_share (51)
    Length: 38
  Key Share extension
      Client Key Share Length: 36
    Key Share Entry: Group: x25519, Key Exchange length: 32
        Group: x25519 (29)
        Key Exchange Length: 32
        Key Exchange: 6f581c36e18173318208928de2693b27fd89e40
```