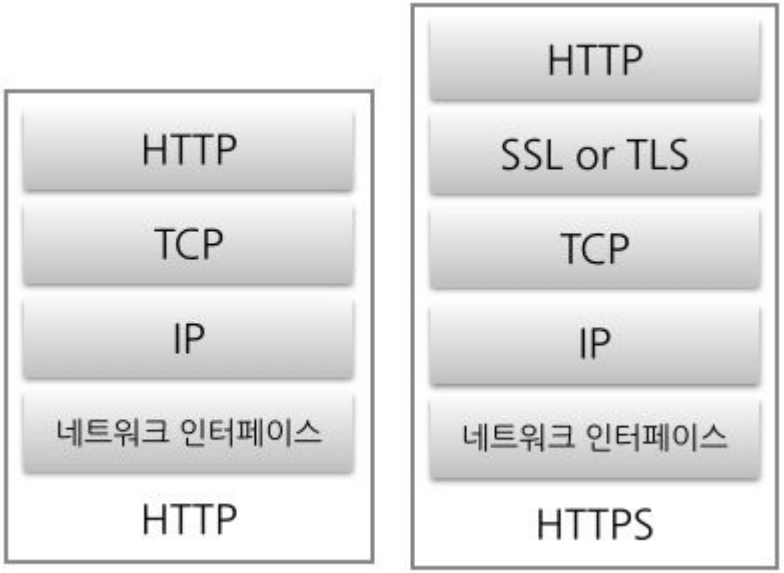
HTTPS

이해은**(Main)**, 최상희(Sub)

HTTPS(HyperText Transfer Protocol Secure)



Why HTTPS

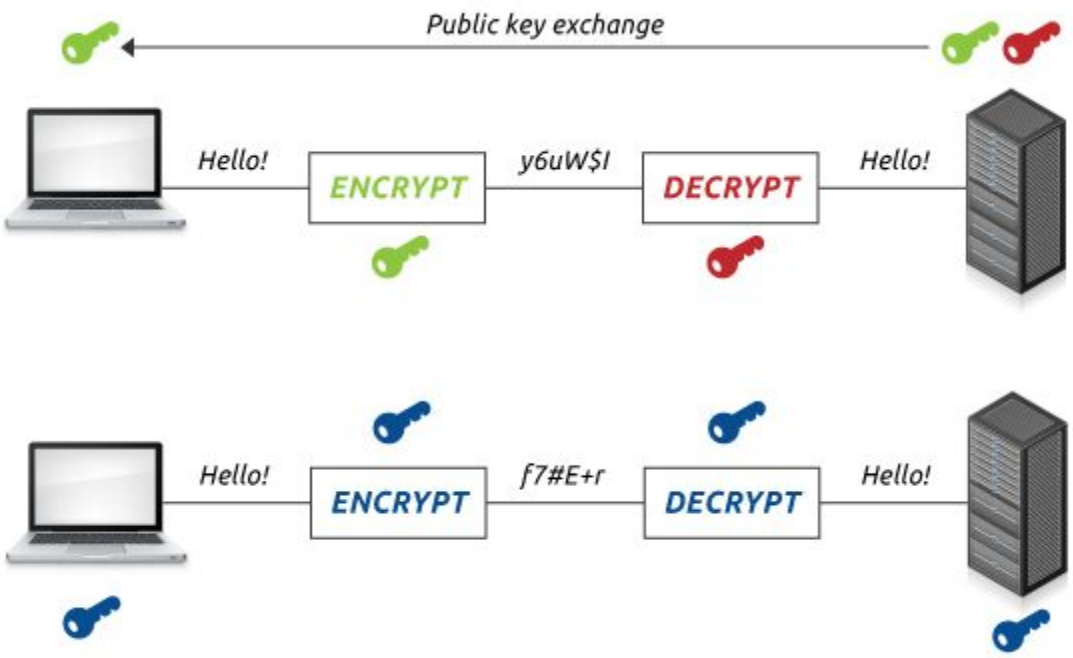
1. 웹 사이트의 무결성 보호

   서버와 사용자 사이의 통신을 침입자가 변조하지 못하도록 합니다.

2. 사용자의 개인정보 보호

   서버와 사용자 사이의 통신을 도청하지 못하도록 합니다.

SSL(Secure Socket Layer)

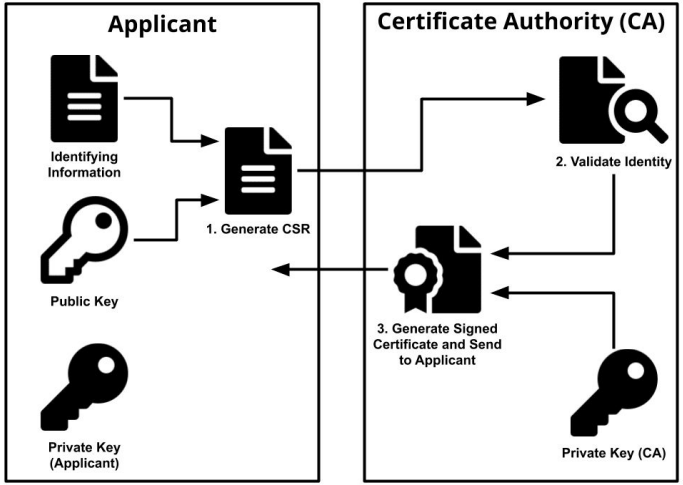


SSL 인증서

클라이언트와 서버간의 통신을 제3자가 보증해주는 전자화된 문서

역할

1. 클라이언트가 접속한 서버가 신뢰할 수 있는 서버임을 보장합니다.
2. SSL 통신에 사용할 공개키를 클라이언트에게 제공합니다.



SSL 인증서 구조

X.509 v3 인증서 구조

- Certificate
  - Version 인증서의 버전을 나타냄
  - Serial Number CA가 할당한 정수로 된 고유 번호
  - Signature 서명 알고리즘 식별자
  - Issuer 발행자
  - Validity 유효기간
    - Not Before 유효기간 시작 날짜
    - Not After 유효기간 끝나는 날짜
  - Subject 소유자
  - Subject Public Key Info 소유자 공개 키 정보
    - Public Key Algorithm 공개 키 알고리즘
    - Subject Public Key
  - Issuer Unique Identifier (Optional) 발행자 고유 식별자
  - Subject Unique Identifier (Optional) 소유자 고유 식별자
  - Extensions (Optional) 확장
    - ...
- Certificate Signature Algorithm
- Certificate Signature

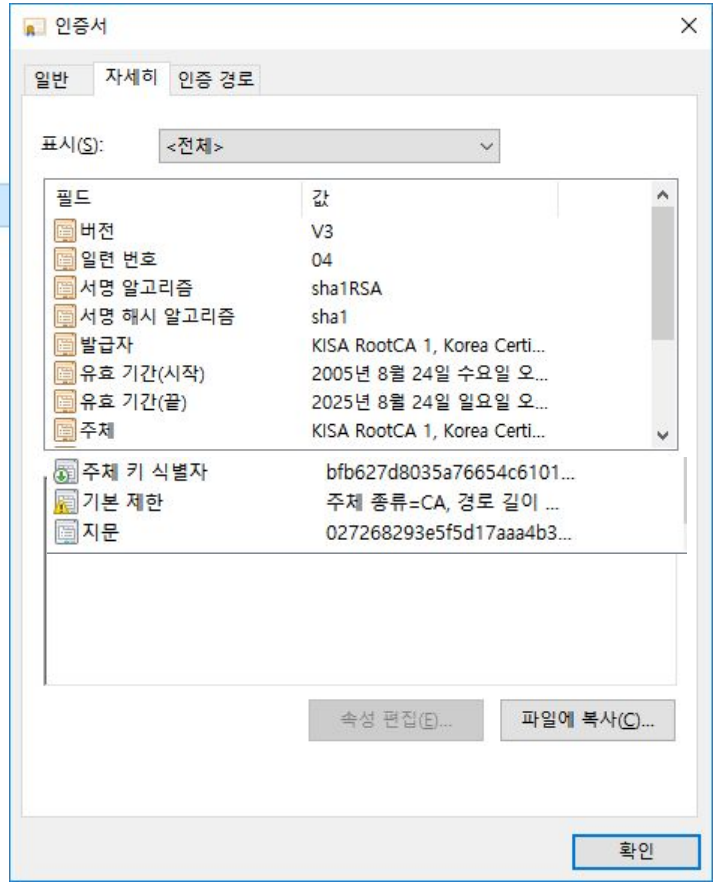
SSL 인증서 구조

C:\Users\사용자 이름\AppData\LocalLow\NPKI

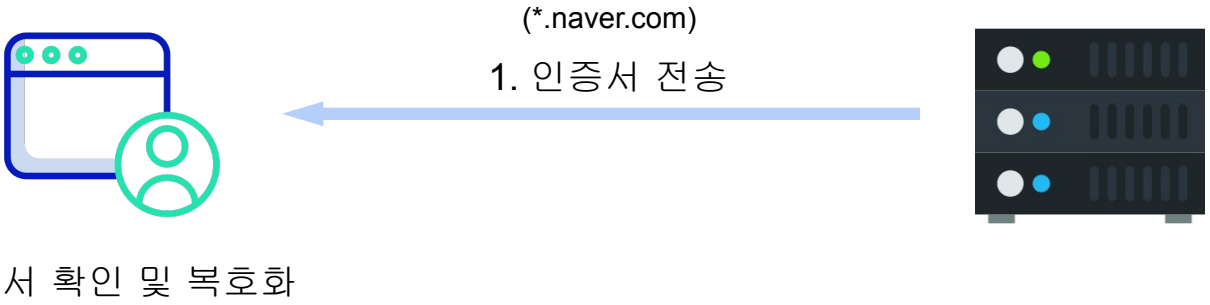
CrossCert	2018-11-16 오후...	파일 폴더
KICA	2018-11-16 오후...	파일 폴더
KISA	2018-11-16 오후...	파일 폴더
NCASign	2017-01-31 오후...	파일 폴더
SignKorea	2018-11-16 오후...	파일 폴더
TradeSign	2018-11-16 오후...	파일 폴더
yessign	2018-11-16 오후...	파일 폴더

SSL 인증서 구조

2587df3e181c92c06c2e9677d44a0095...	2016-11-08 오전...	보안 인증서
BFB627D8035A76654C6101415631E5...	2017-05-18 오후...	보안 인증서
c8d08ec749ae1f2042b24b7f13c97758...	2010-07-12 오후...	보안 인증서
FF8A46723358E8488822AA1768DA16...	2016-11-08 오전...	보안 인증서



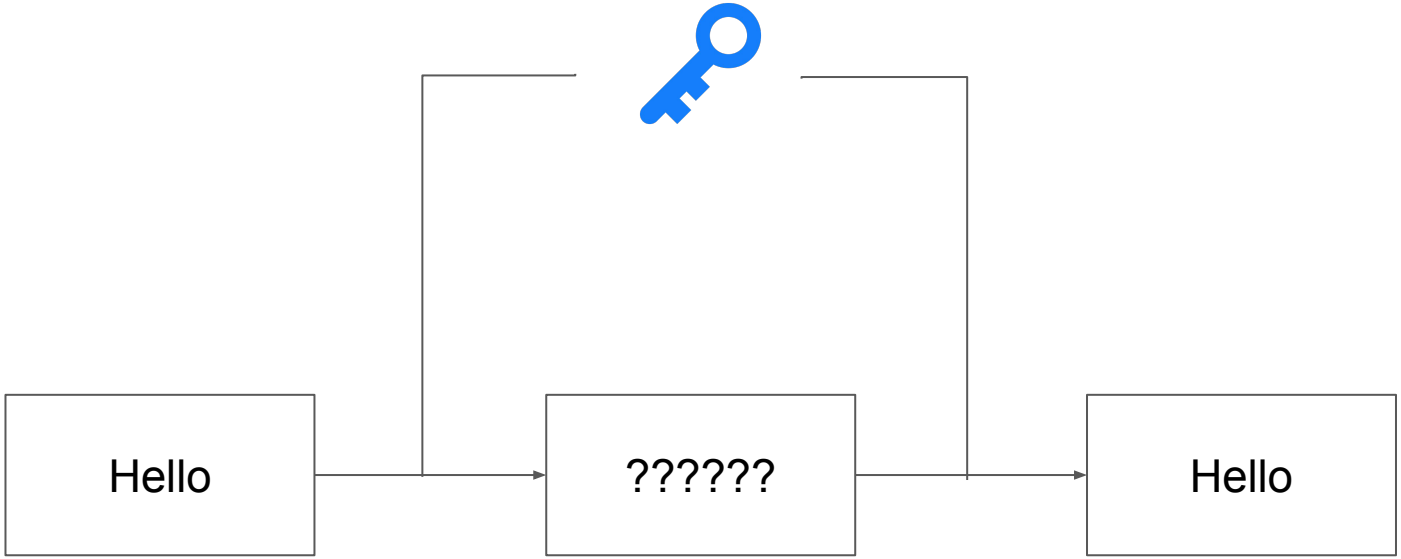
SSL 인증서 - 인증 과정



인증서를 복호화 할 수 있다는 것은 인증서가 CA의 비공개 키에 의해 암호화 되었다는 것을 의미하고

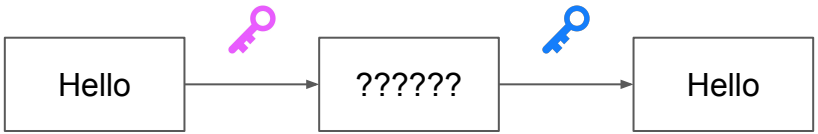
이는 곧 인증서가 신뢰할 수 있는 기관(서버)에서 제공한 인증서라는 것을 확인할 수 있음을 의미합니다.

대칭키 암호화

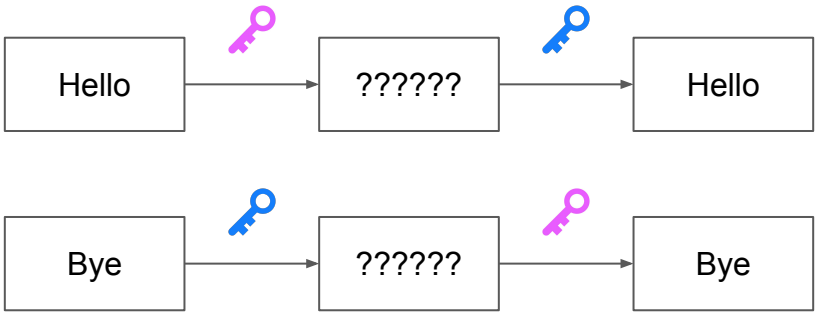


비대칭키 암호화

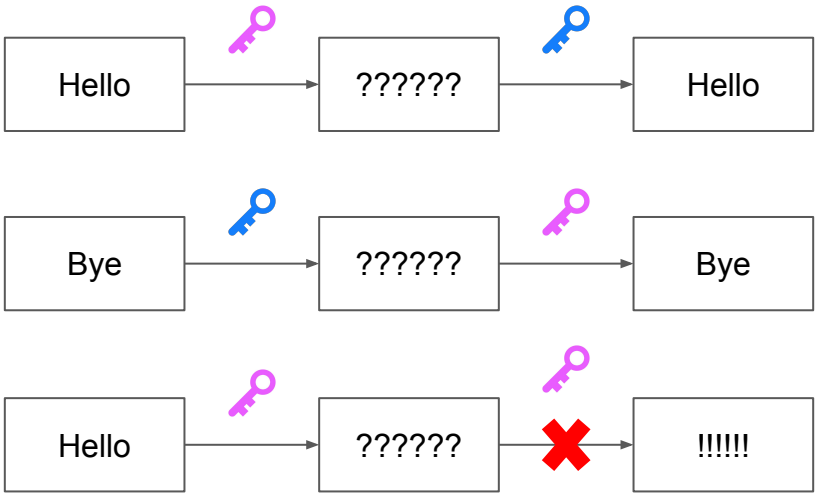
비대칭키 암호화



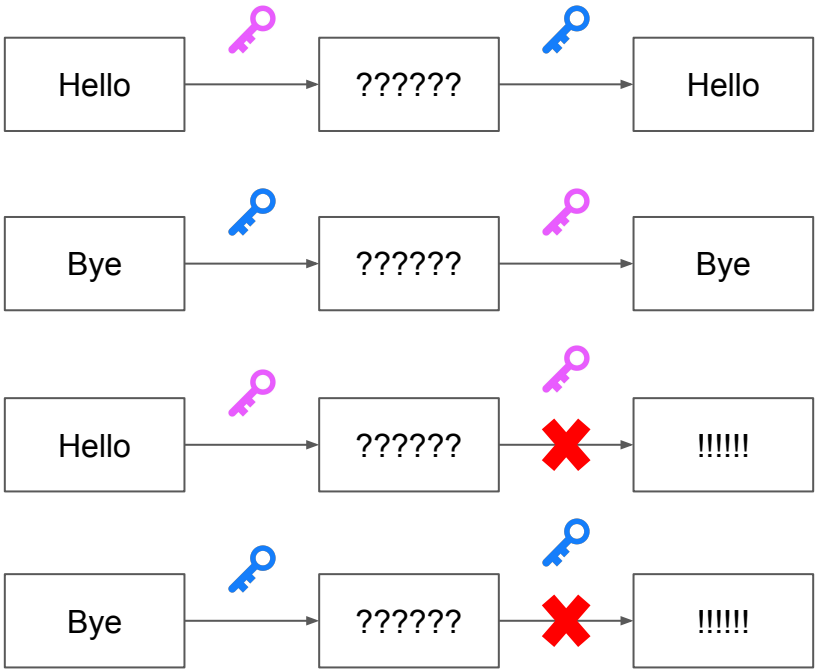
비대칭키 암호화



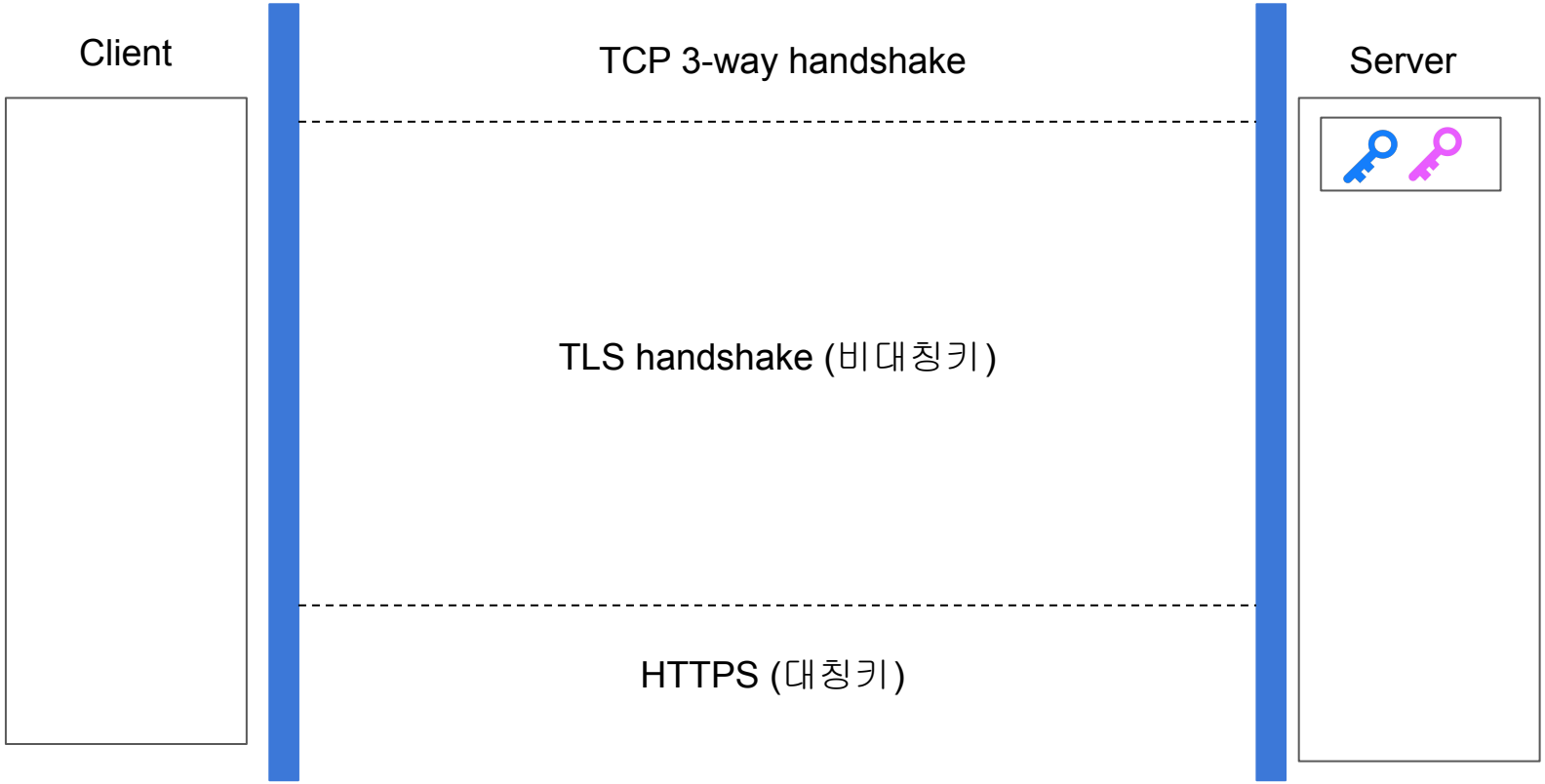
비대칭키 암호화



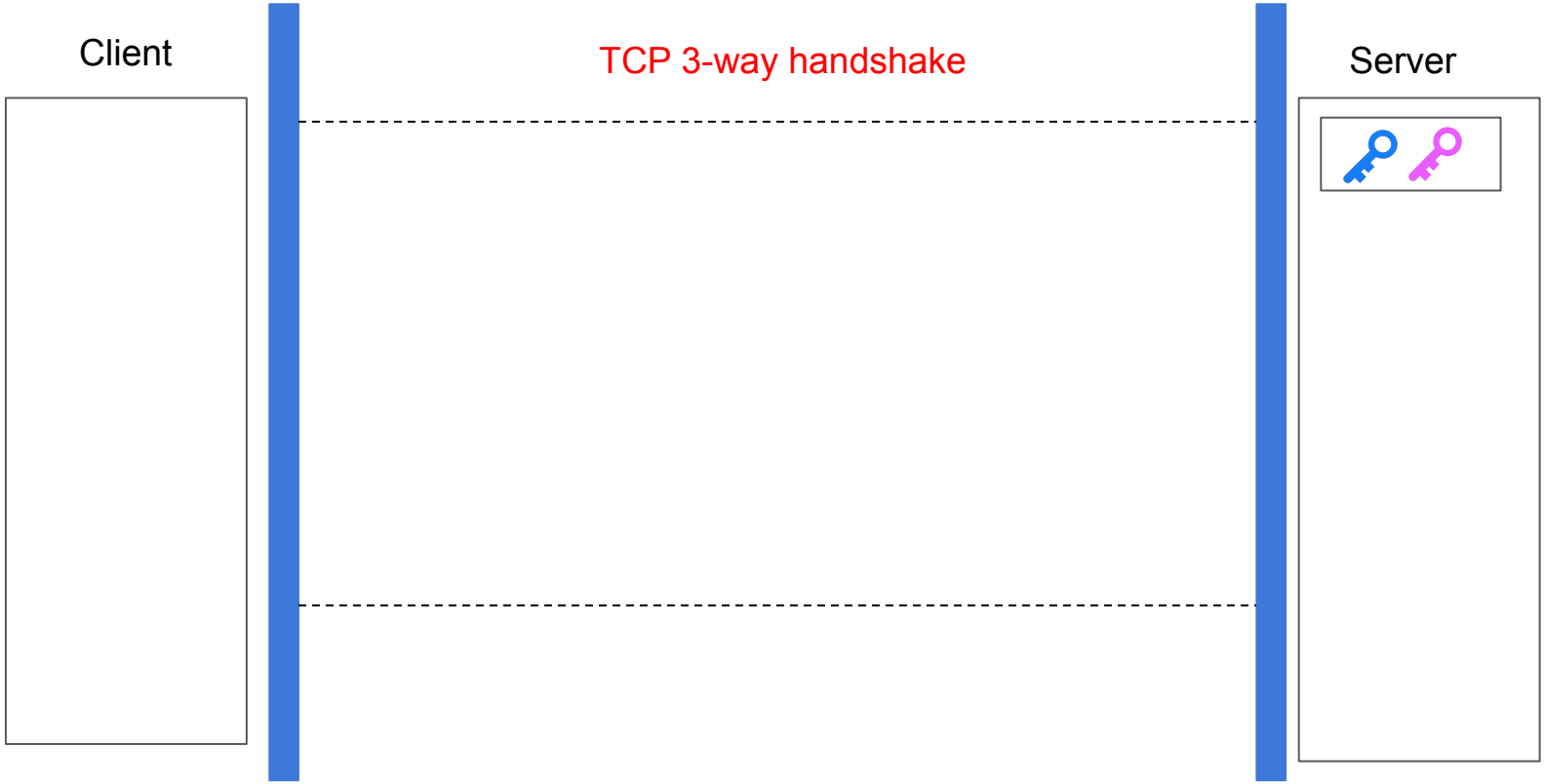
비대칭키 암호화



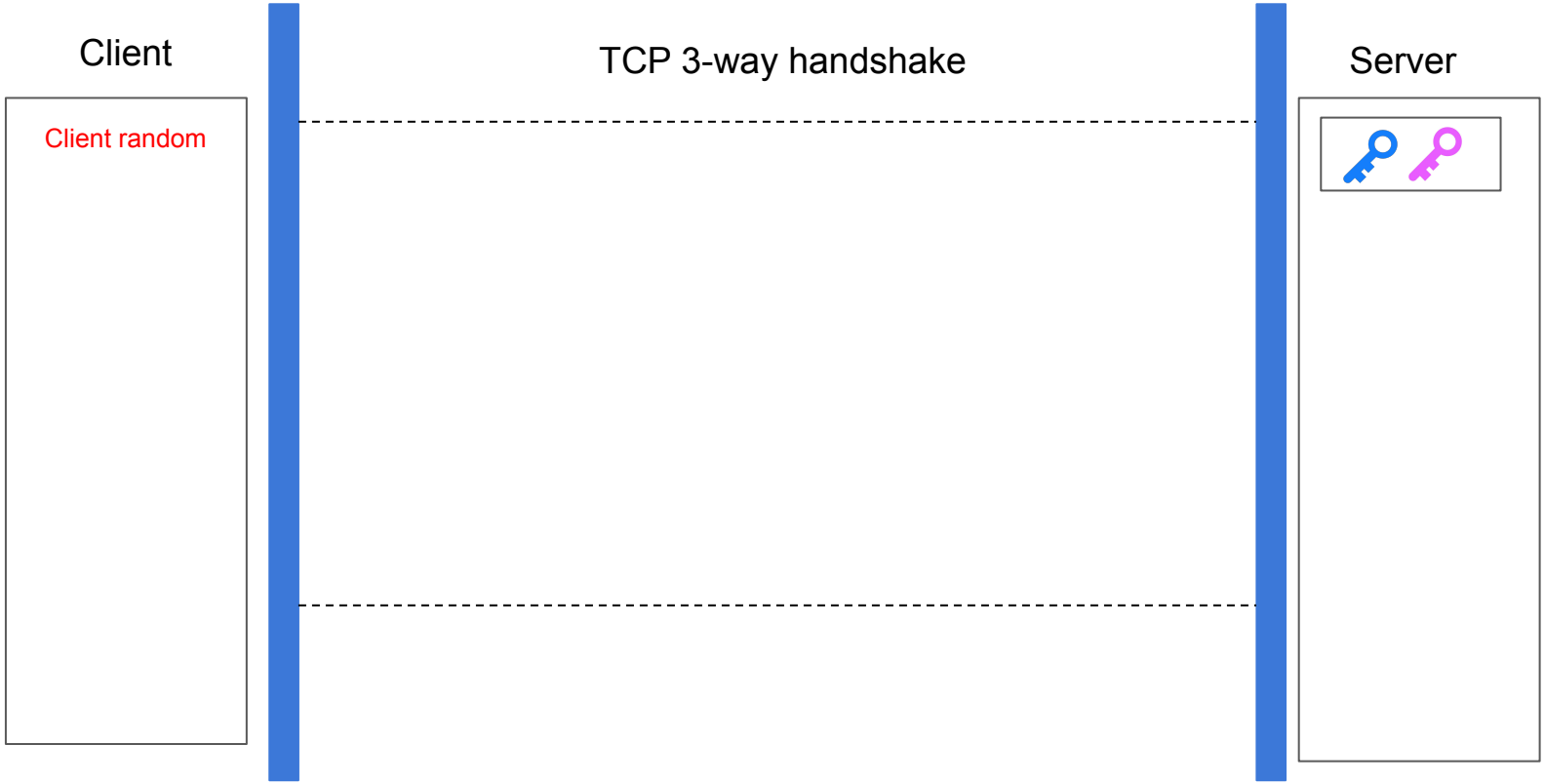
HTTPS 통신 과정


Client
TCP 3-way handshake
Server
TLS handshake (비대칭키)
HTTPS (대칭키)

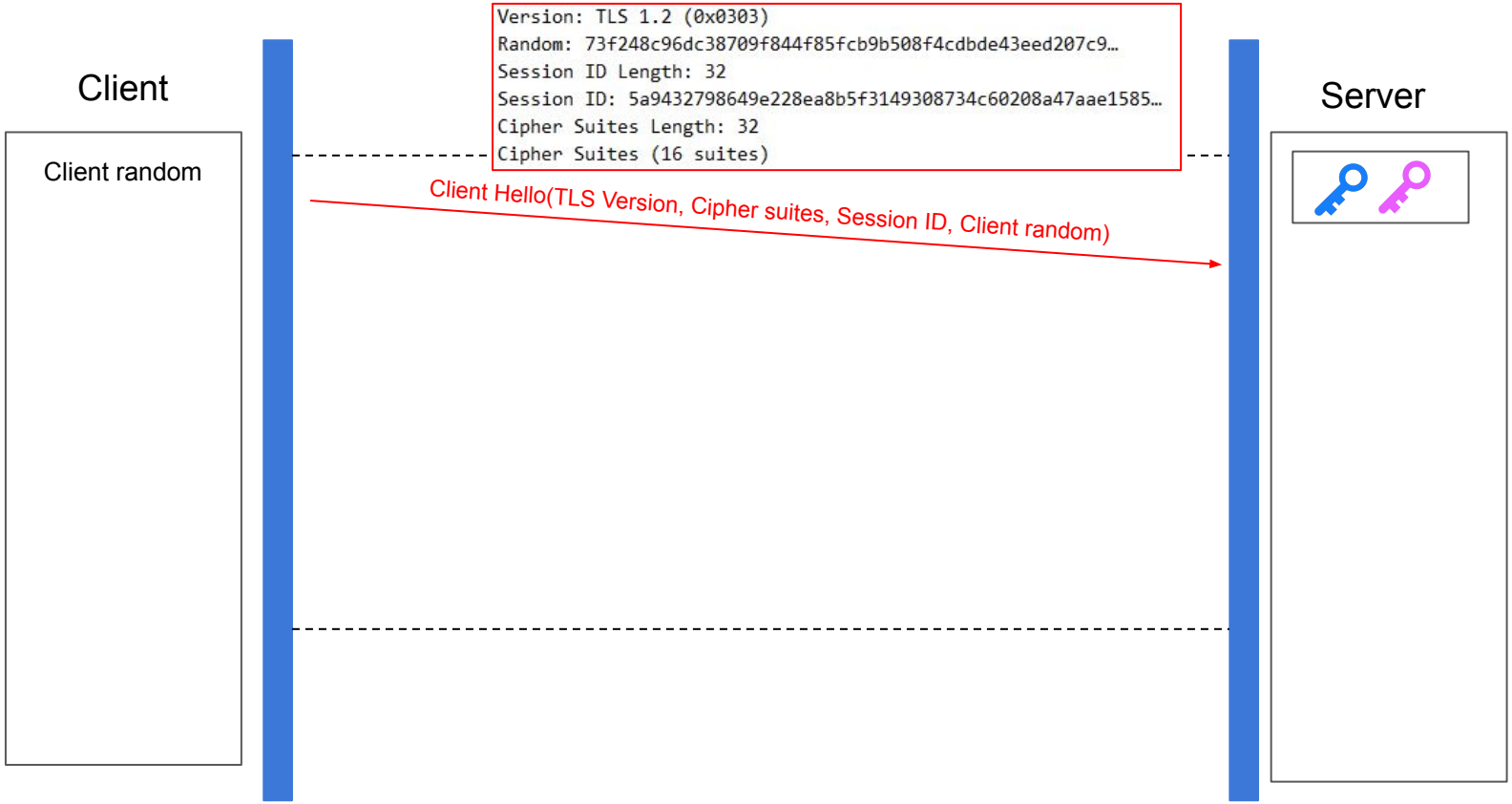
HTTPS 통신 과정



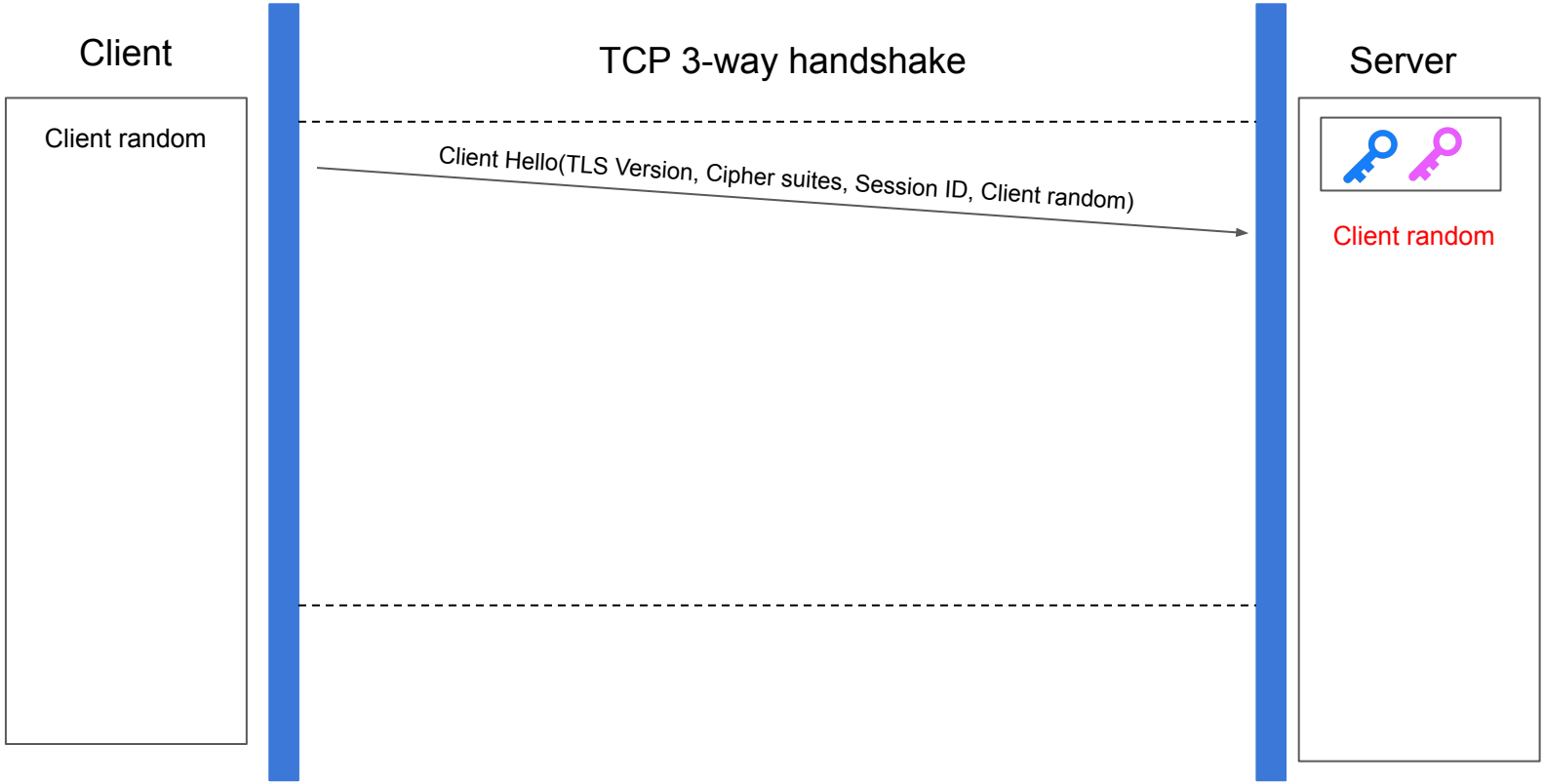
HTTPS 통신 과정



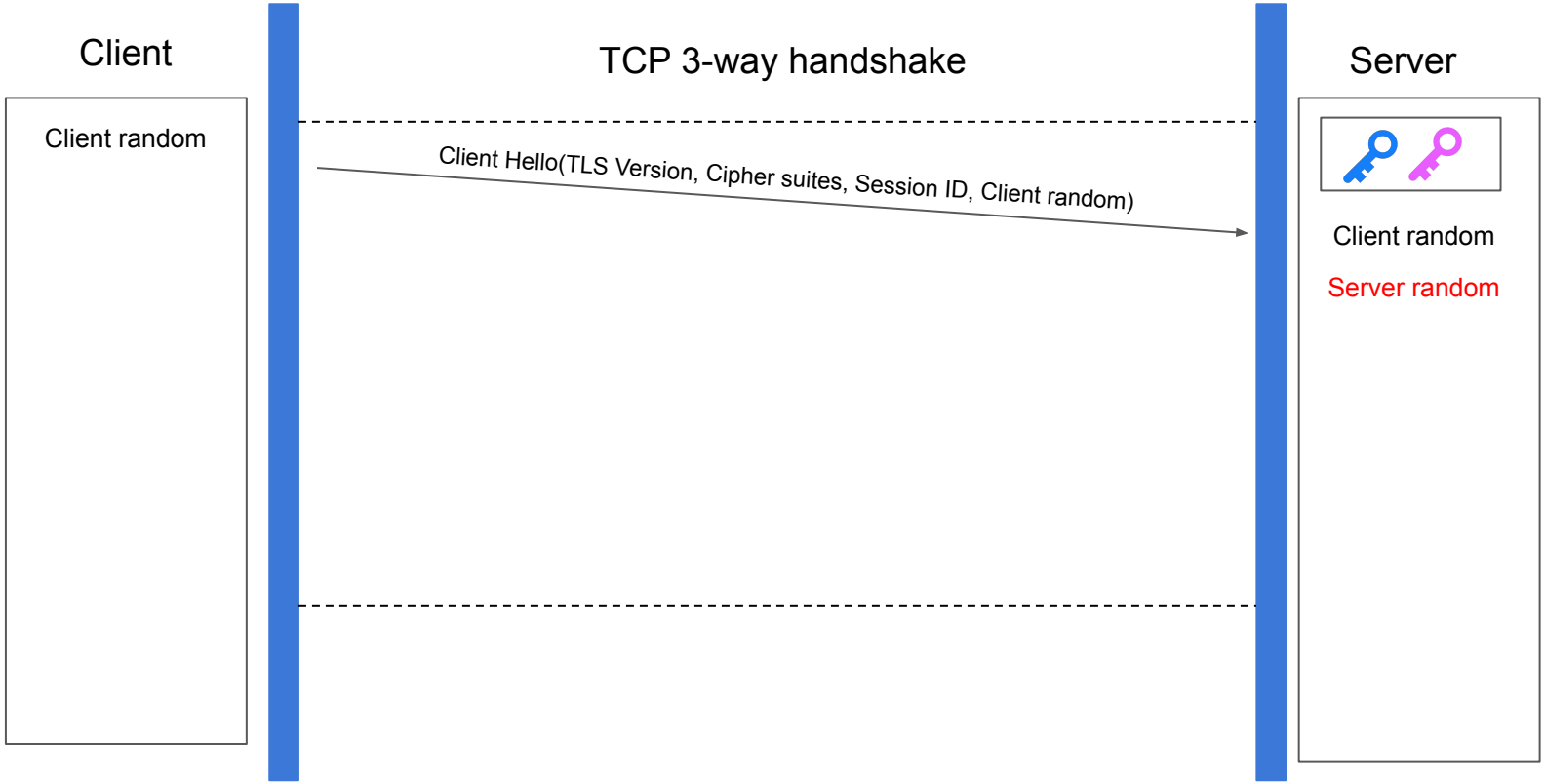
HTTPS 통신 과정


Client
Client random
Server
Version: TLS 1.2 (0x0303)
Random: 73f248c96dc38709f844f85fcb9b508f4cdbde43eed207c9…
Session ID Length: 32
Session ID: 5a9432798649e228ea8b5f3149308734c60208a47aae1585…
Cipher Suites Length: 32
Cipher Suites (16 suites)
Client Hello(TLS Version, Cipher suites, Session ID, Client random)

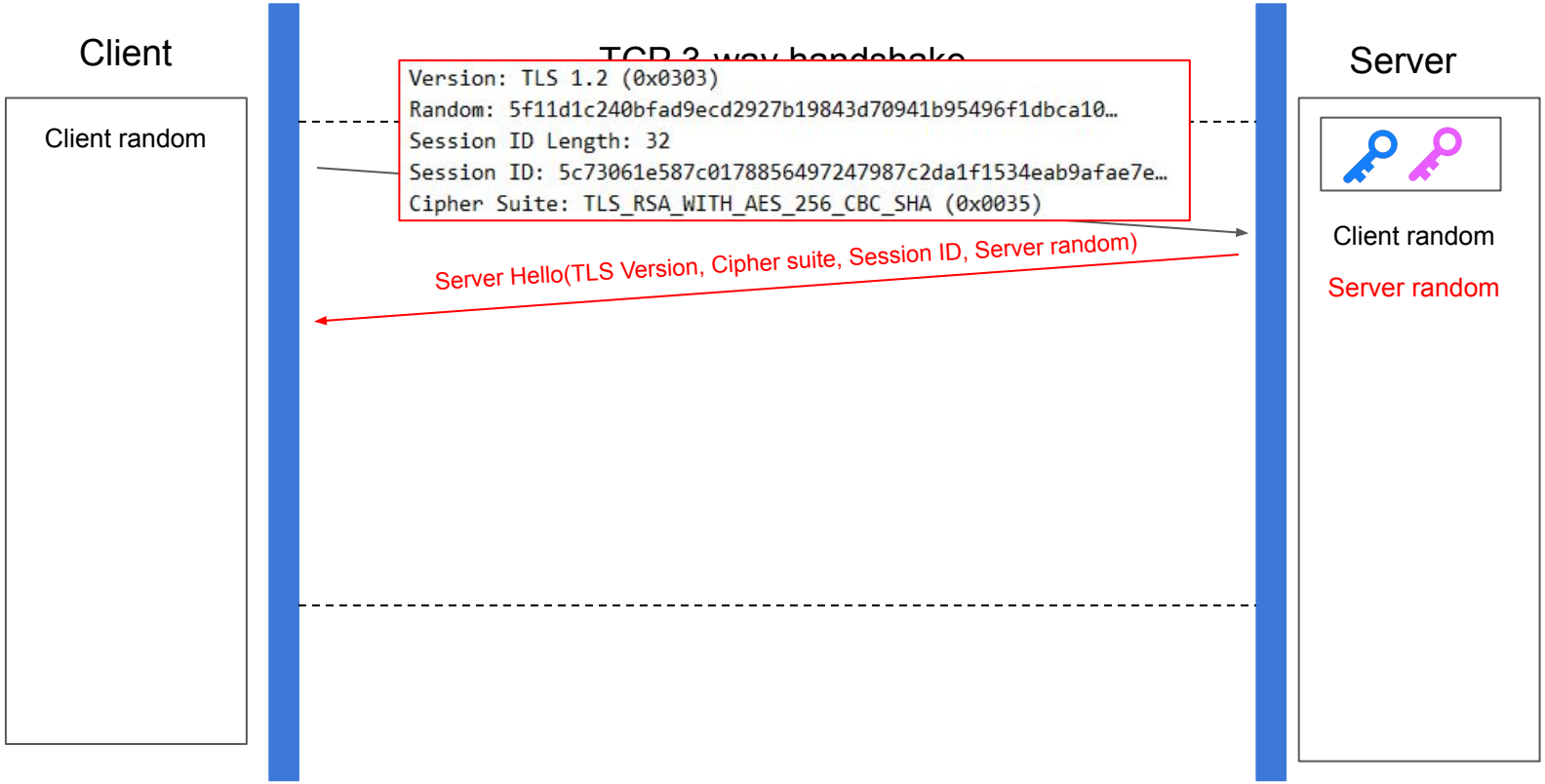
HTTPS 통신 과정


Client
TCP 3-way handshake
Server
Client random
Client Hello(TLS Version, Cipher suites, Session ID, Client random)
Client random

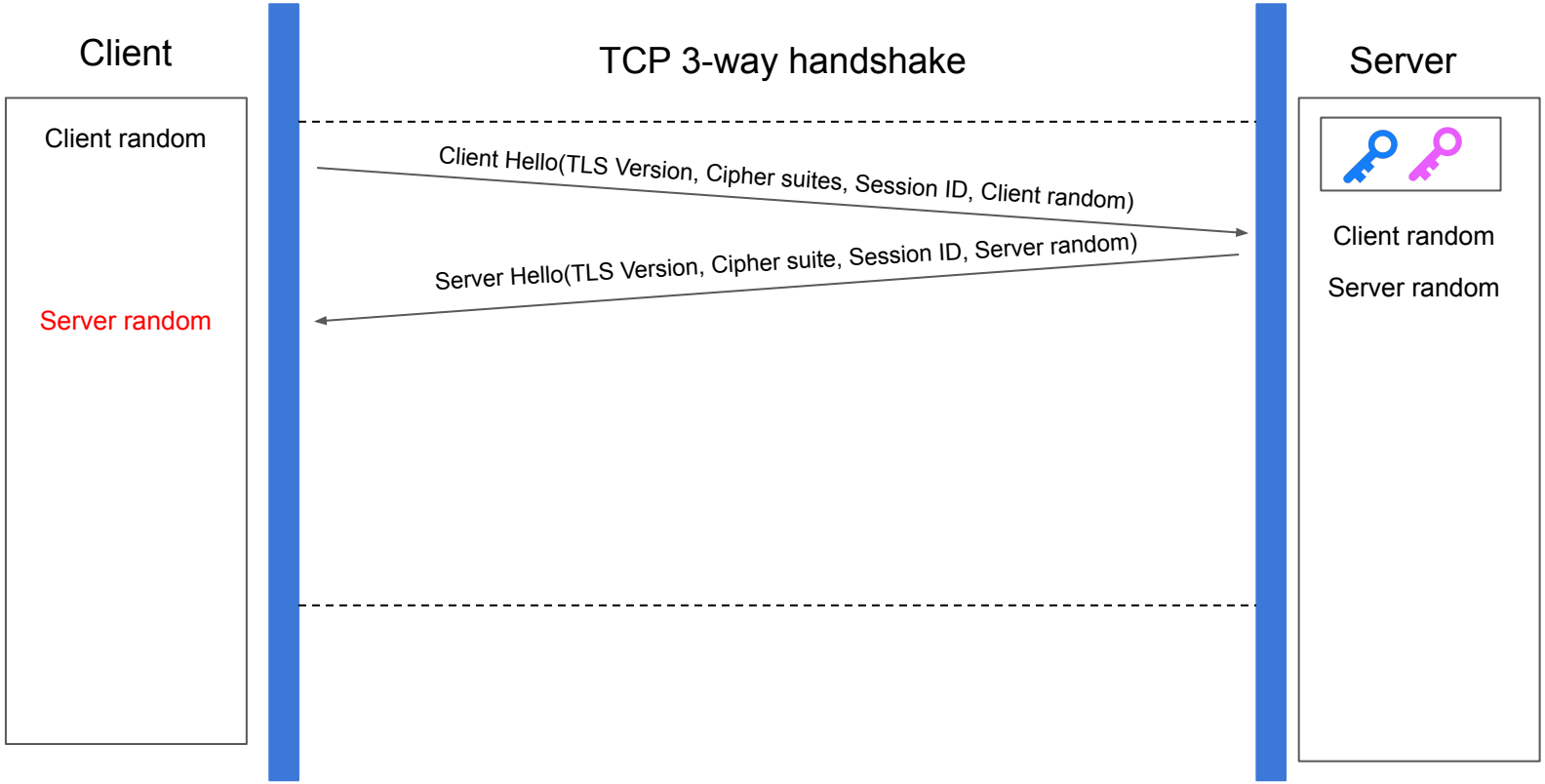
HTTPS 통신 과정


Client
TCP 3-way handshake
Server
Client random
Client Hello(TLS Version, Cipher suites, Session ID, Client random)
Client random
Server random

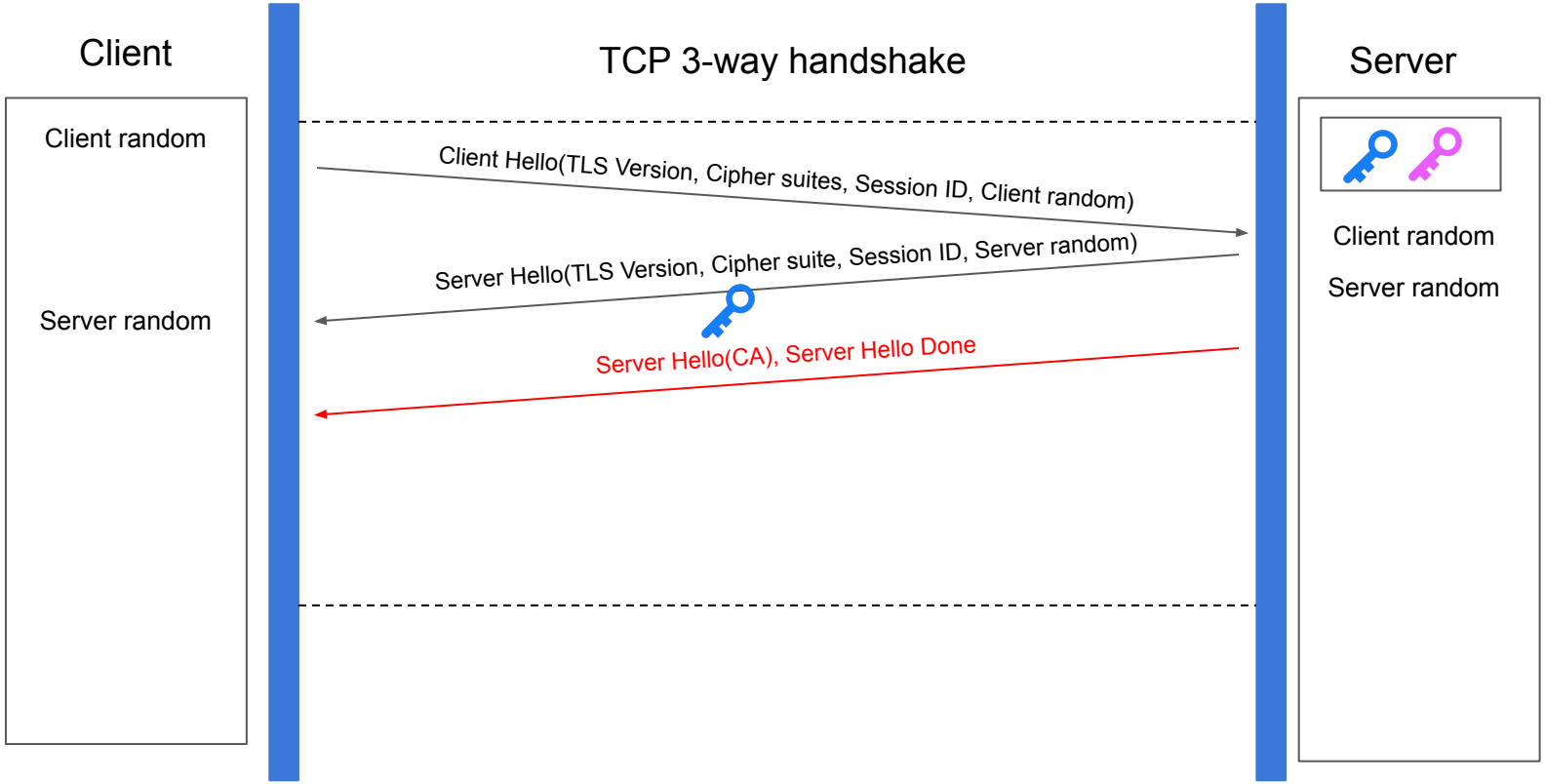
HTTPS 통신 과정


Client
Client random
TCP 3-way handshake
Version: TLS 1.2 (0x0303)
Random: 5f11d1c240bfad9ecd2927b19843d70941b95496f1dbca10…
Session ID Length: 32
Session ID: 5c73061e587c0178856497247987c2da1f1534eab9afae7e…
Cipher Suite: TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)
Server Hello(TLS Version, Cipher suite, Session ID, Server random)
Server
Client random
Server random

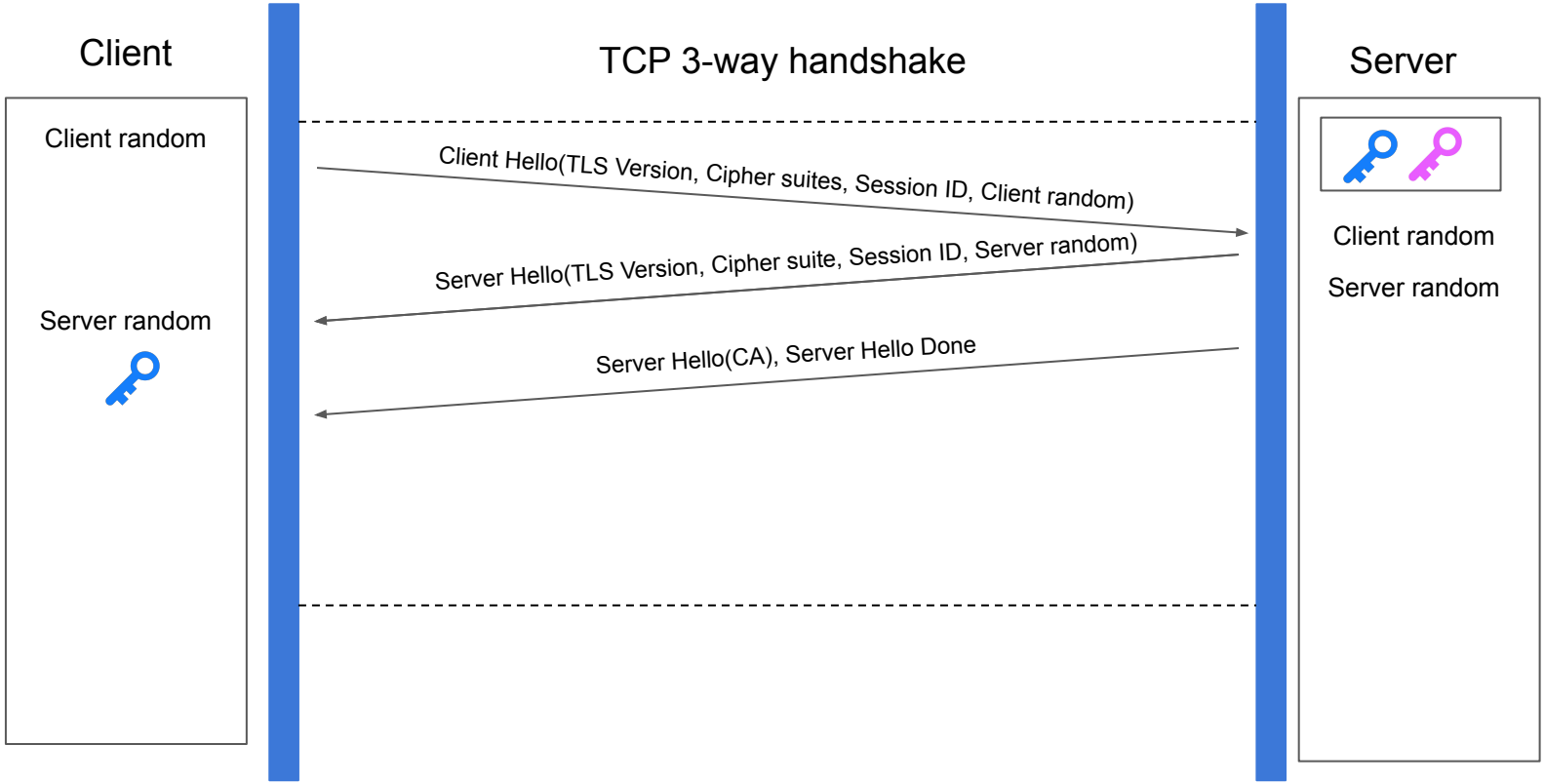
HTTPS 통신 과정


Client
TCP 3-way handshake
Server
Client random
Client Hello(TLS Version, Cipher suites, Session ID, Client random)
Client random
Server random
Server Hello(TLS Version, Cipher suite, Session ID, Server random)
Server random

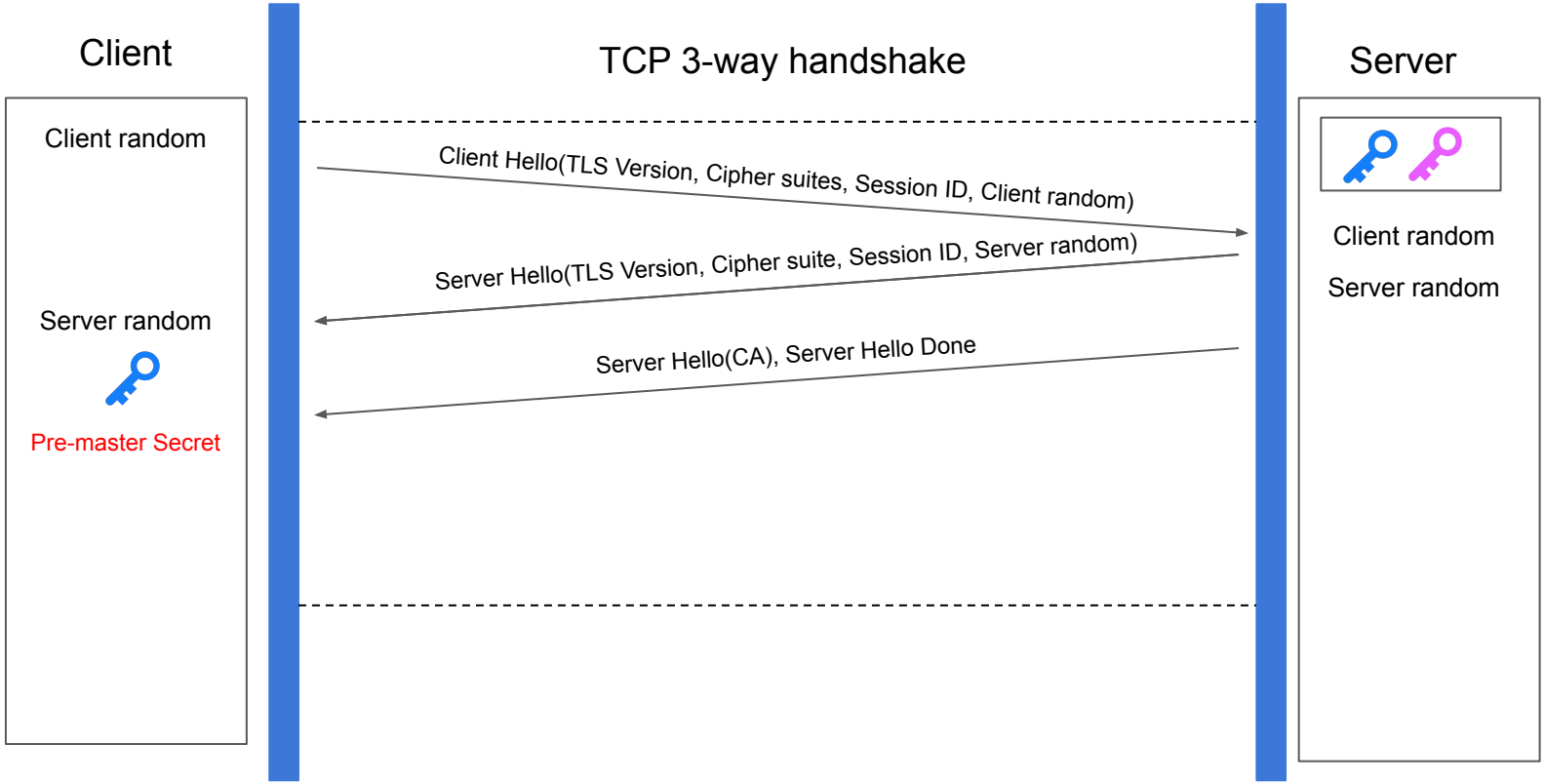
HTTPS 통신 과정


Client
TCP 3-way handshake
Server
Client random
Server random
Client Hello(TLS Version, Cipher suites, Session ID, Client random)
Server Hello(TLS Version, Cipher suite, Session ID, Server random)
Server Hello(CA), Server Hello Done
Client random
Server random

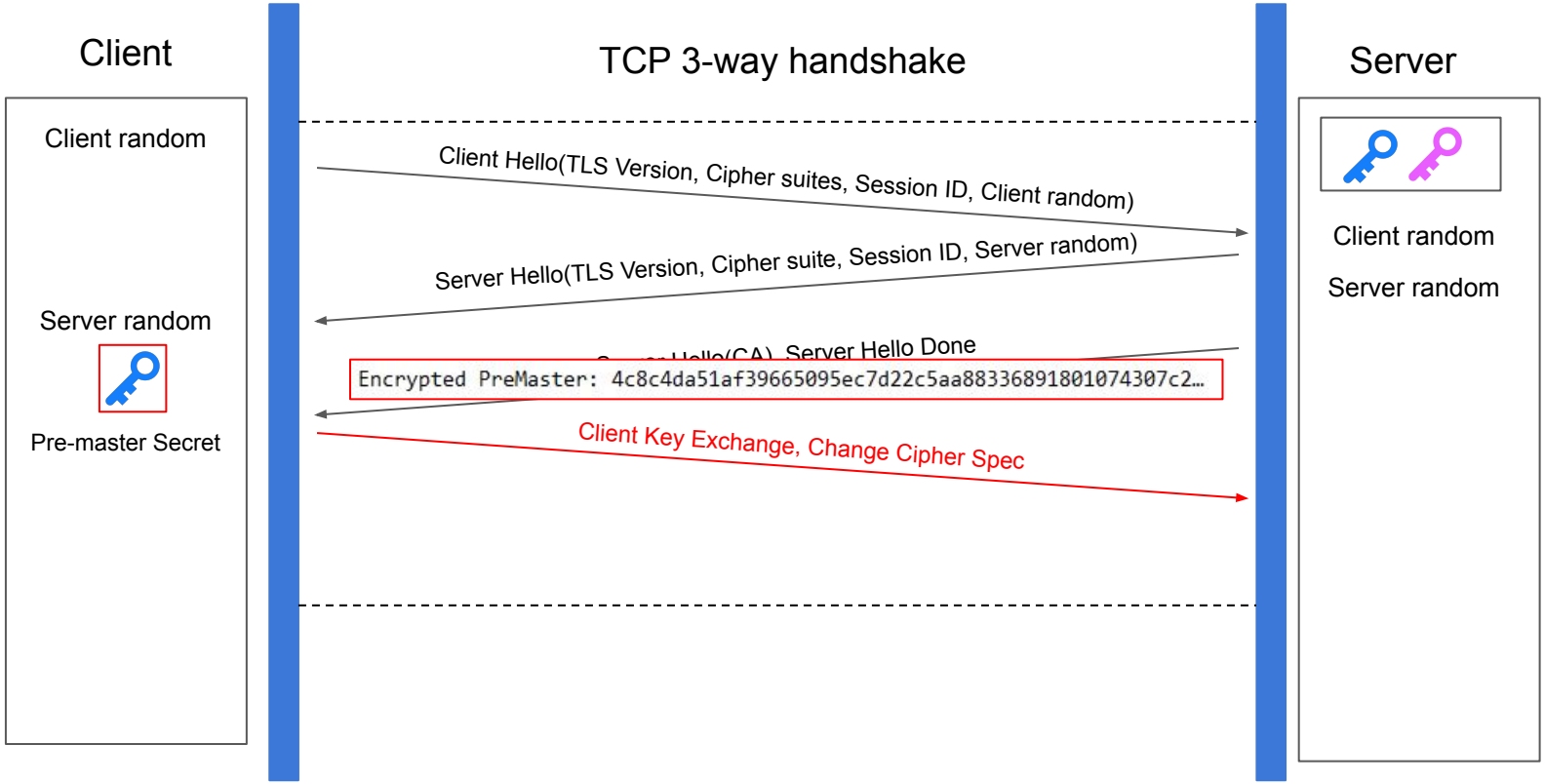
HTTPS 통신 과정


Client
TCP 3-way handshake
Server
Client random
Client Hello(TLS Version, Cipher suites, Session ID, Client random)
Client random
Server random
Server Hello(TLS Version, Cipher suite, Session ID, Server random)
Server random
Server Hello(CA), Server Hello Done

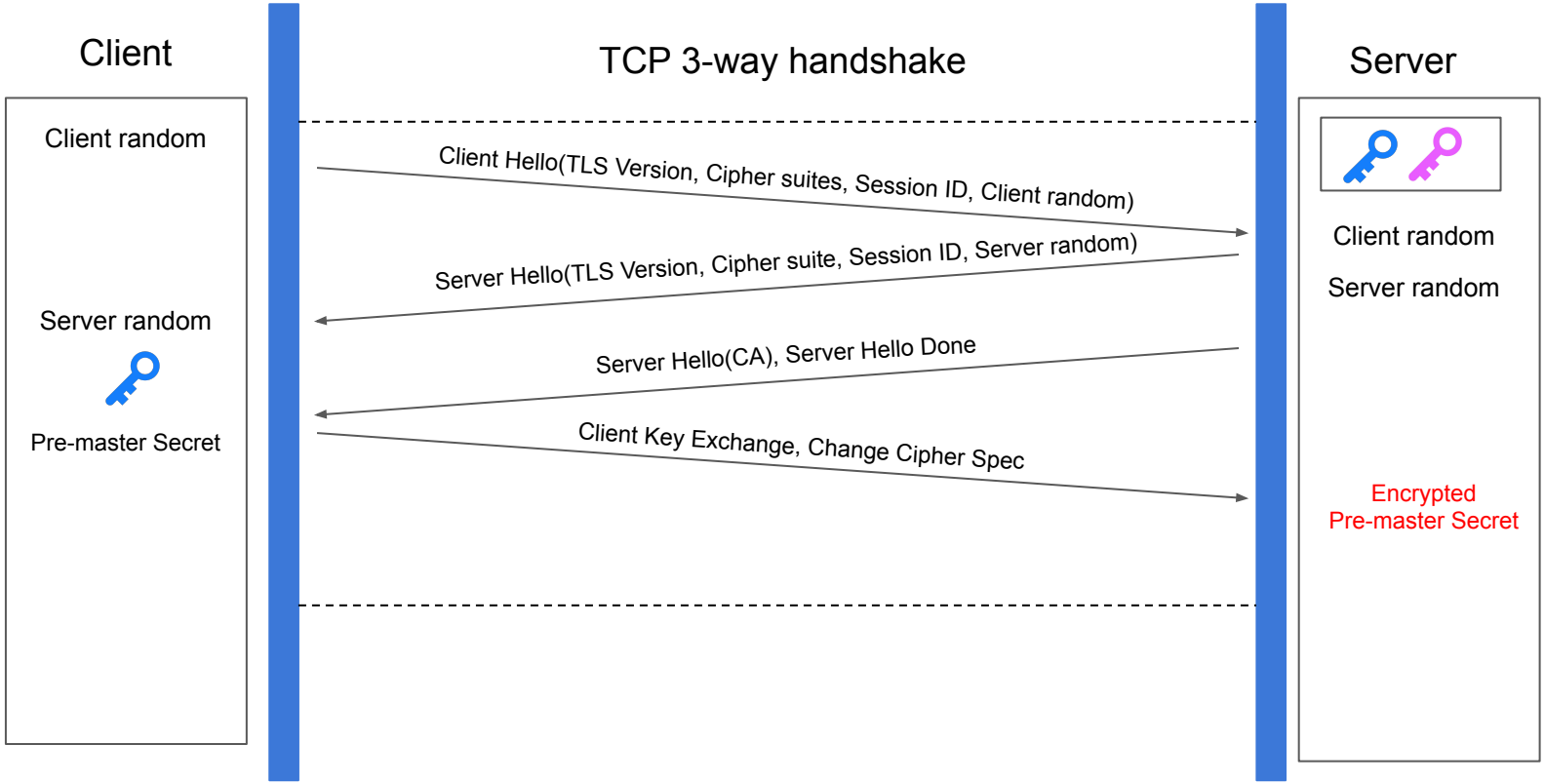
HTTPS 통신 과정


Client
TCP 3-way handshake
Server
Client random
Client Hello(TLS Version, Cipher suites, Session ID, Client random)
Client random
Server random
Server Hello(TLS Version, Cipher suite, Session ID, Server random)
Server random
Server Hello(CA), Server Hello Done
Pre-master Secret

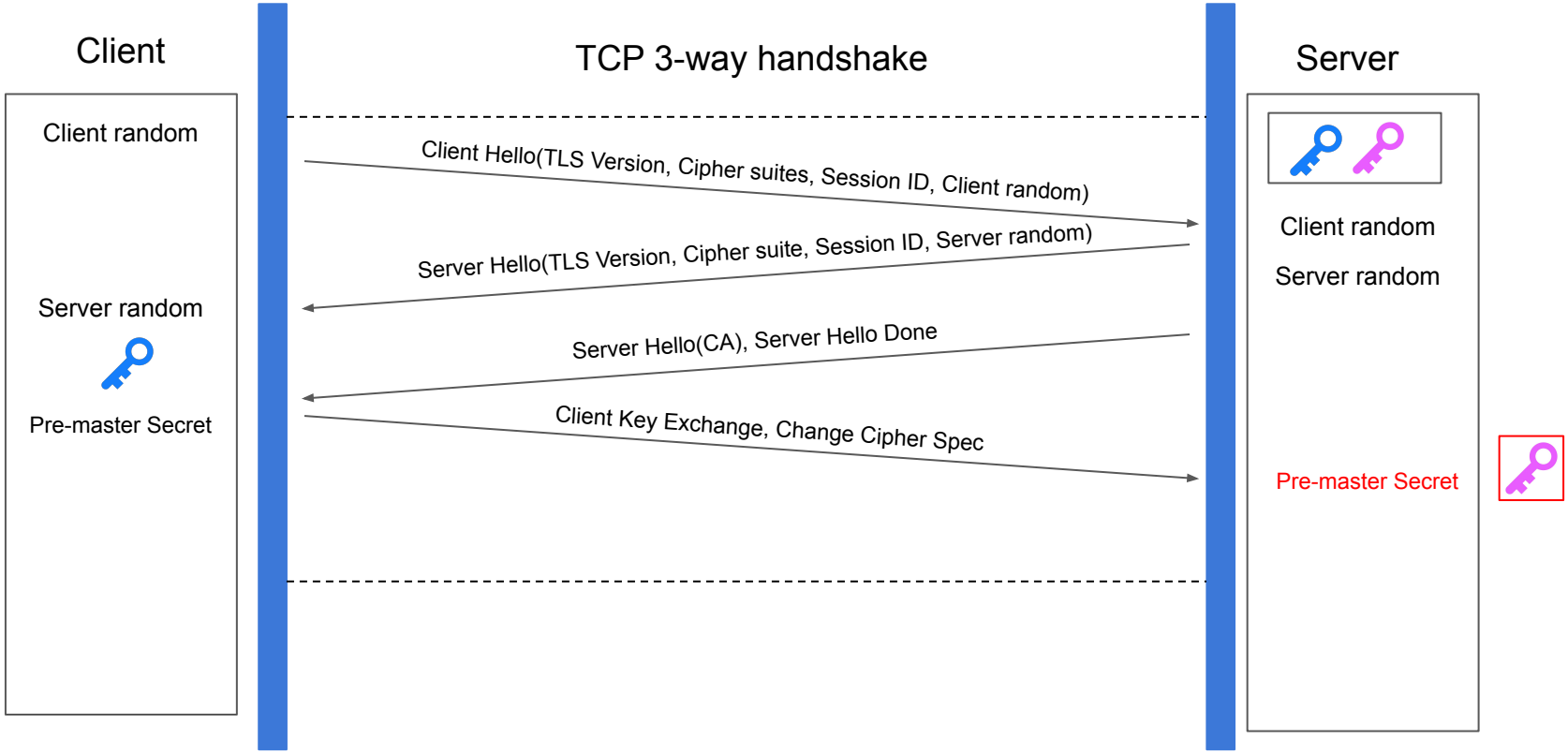
HTTPS 통신 과정


Client
TCP 3-way handshake
Server
Client random
Client Hello(TLS Version, Cipher suites, Session ID, Client random)
Server Hello(TLS Version, Cipher suite, Session ID, Server random)
Client random
Server random
Server random
Server Hello Done
Encrypted PreMaster: 4c8c4da51af39665095ec7d22c5aa8833689180107 4307c2…
Pre-master Secret
Client Key Exchange, Change Cipher Spec

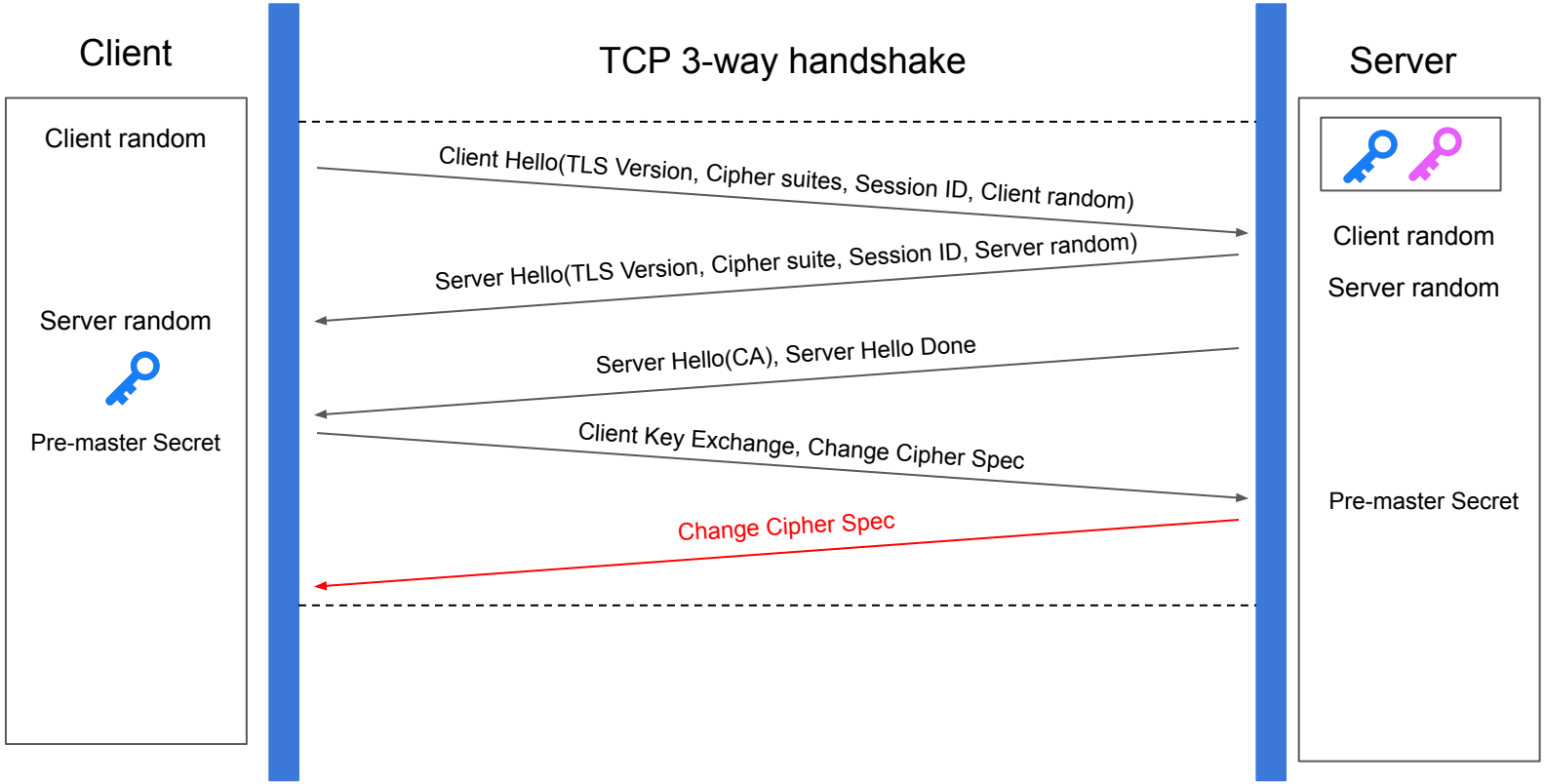
HTTPS 통신 과정


Client
TCP 3-way handshake
Server
Client random
Client Hello(TLS Version, Cipher suites, Session ID, Client random)
Client random
Server random
Server Hello(TLS Version, Cipher suite, Session ID, Server random)
Server random
Server Hello(CA), Server Hello Done
Pre-master Secret
Client Key Exchange, Change Cipher Spec
Encrypted
Pre-master Secret

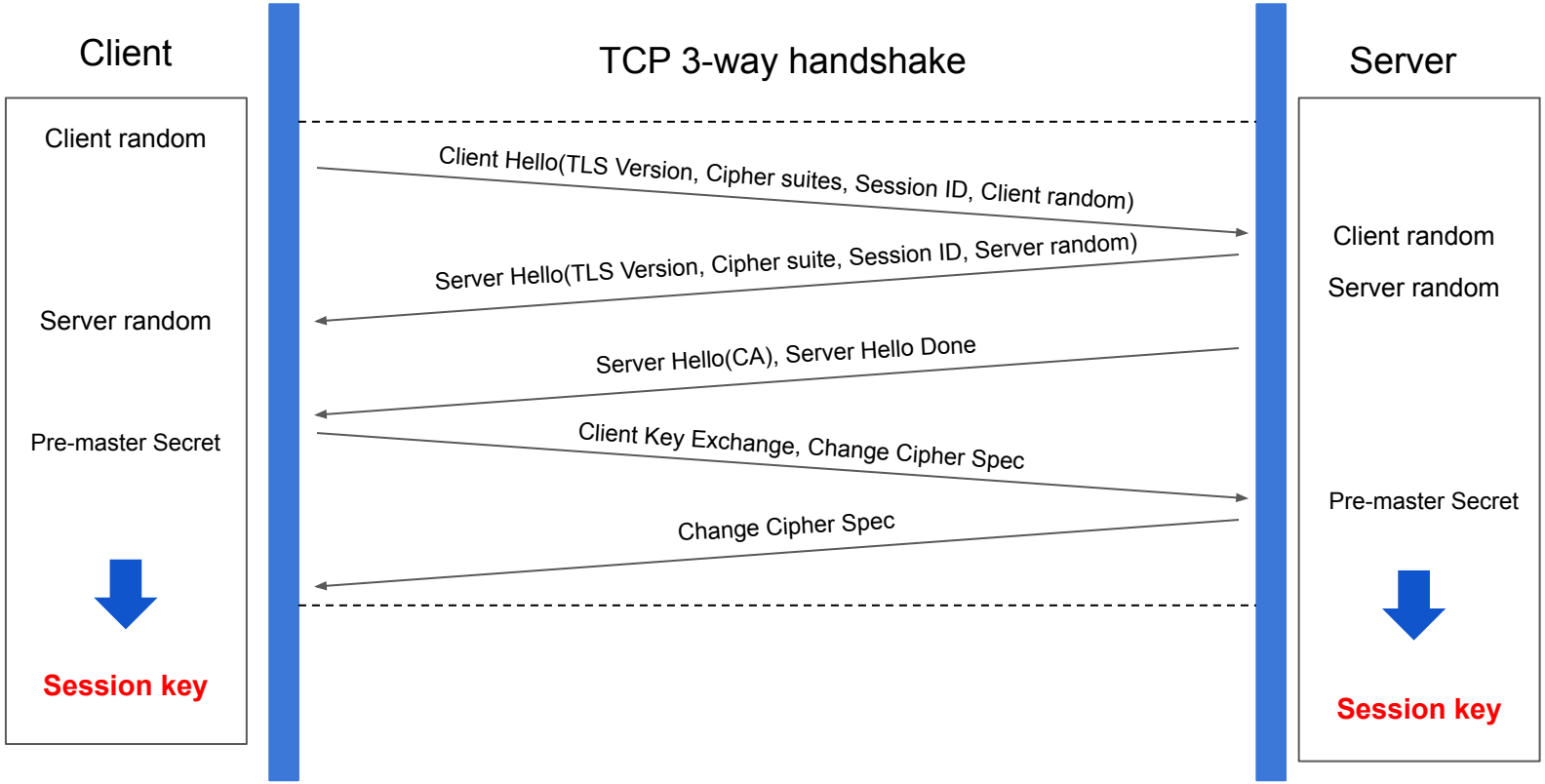
HTTPS 통신 과정


Client
TCP 3-way handshake
Server
Client random
Server random
Pre-master Secret
Client Hello(TLS Version, Cipher suites, Session ID, Client random)
Server Hello(TLS Version, Cipher suite, Session ID, Server random)
Server Hello(CA), Server Hello Done
Client Key Exchange, Change Cipher Spec
Client random
Server random
Pre-master Secret

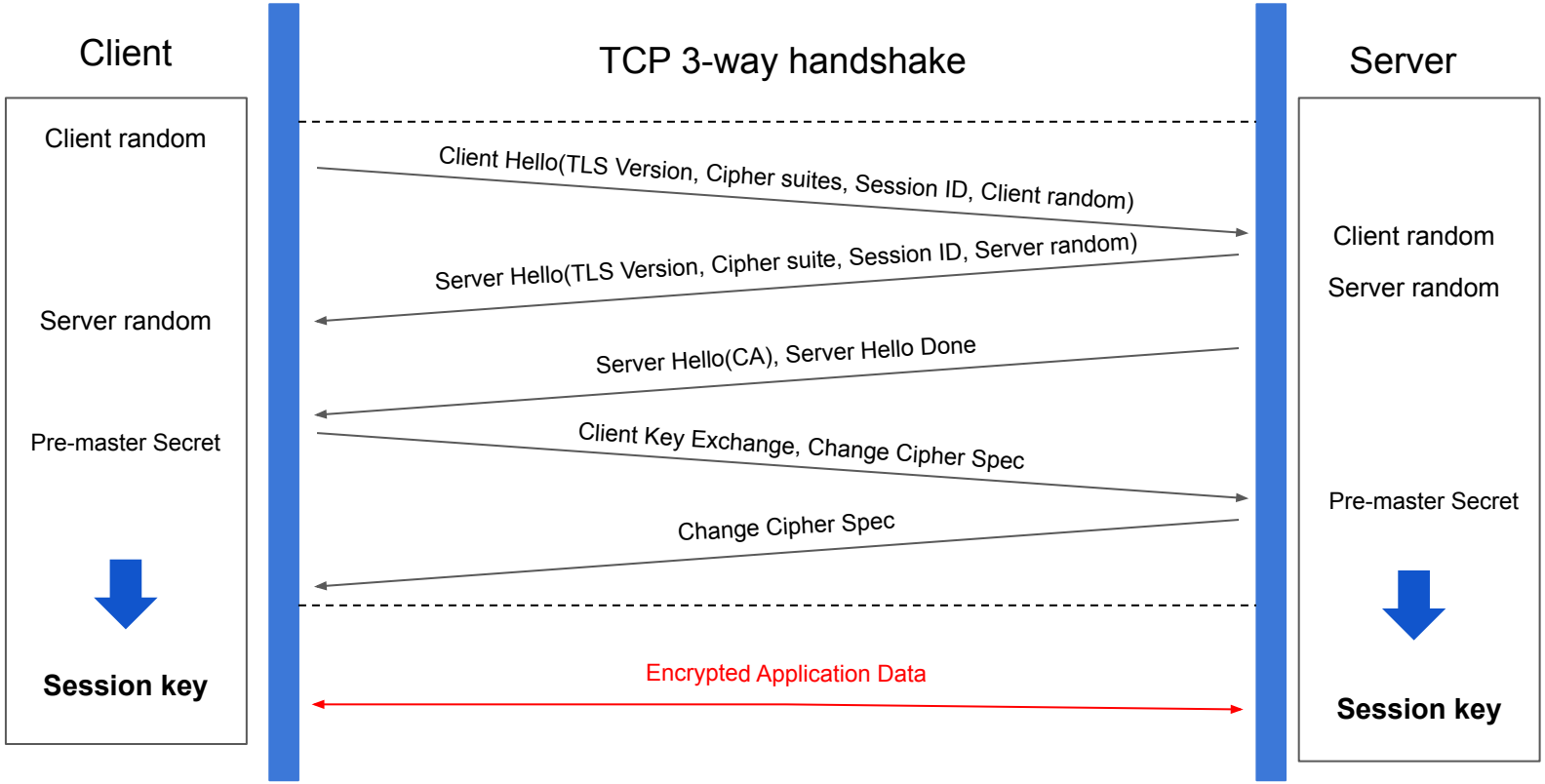
HTTPS 통신 과정


Client
TCP 3-way handshake
Server
Client random
Client Hello(TLS Version, Cipher suites, Session ID, Client random)
Client random
Server random
Server Hello(TLS Version, Cipher suite, Session ID, Server random)
Server random
Server Hello(CA), Server Hello Done
Pre-master Secret
Client Key Exchange, Change Cipher Spec
Pre-master Secret
Change Cipher Spec

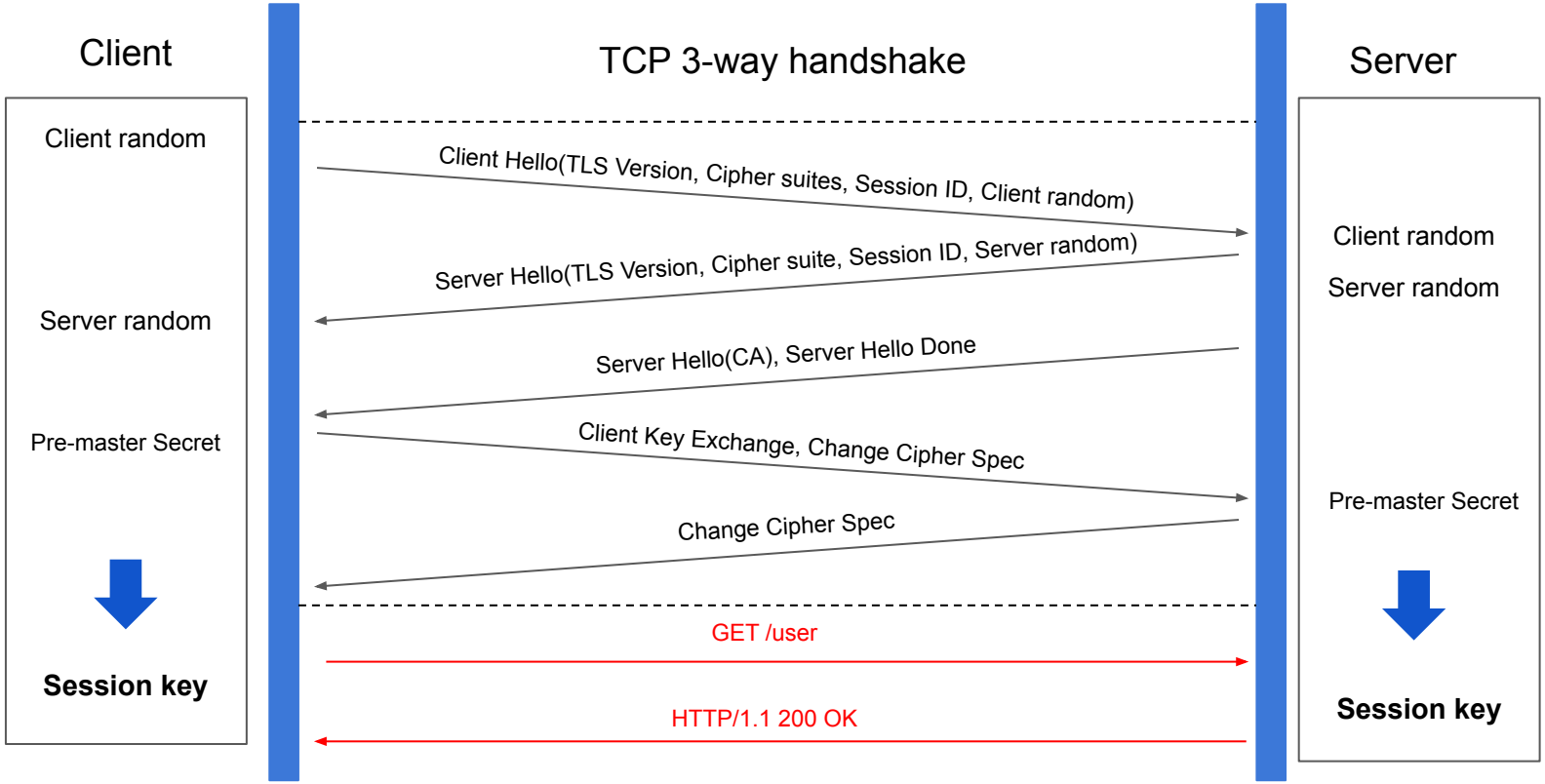
HTTPS 통신 과정


Client
TCP 3-way handshake
Server
Client random
Client Hello(TLS Version, Cipher suites, Session ID, Client random)
Client random
Server random
Server Hello(TLS Version, Cipher suite, Session ID, Server random)
Server random
Server Hello(CA), Server Hello Done
Pre-master Secret
Client Key Exchange, Change Cipher Spec
Pre-master Secret
Change Cipher Spec
Session key
Session key

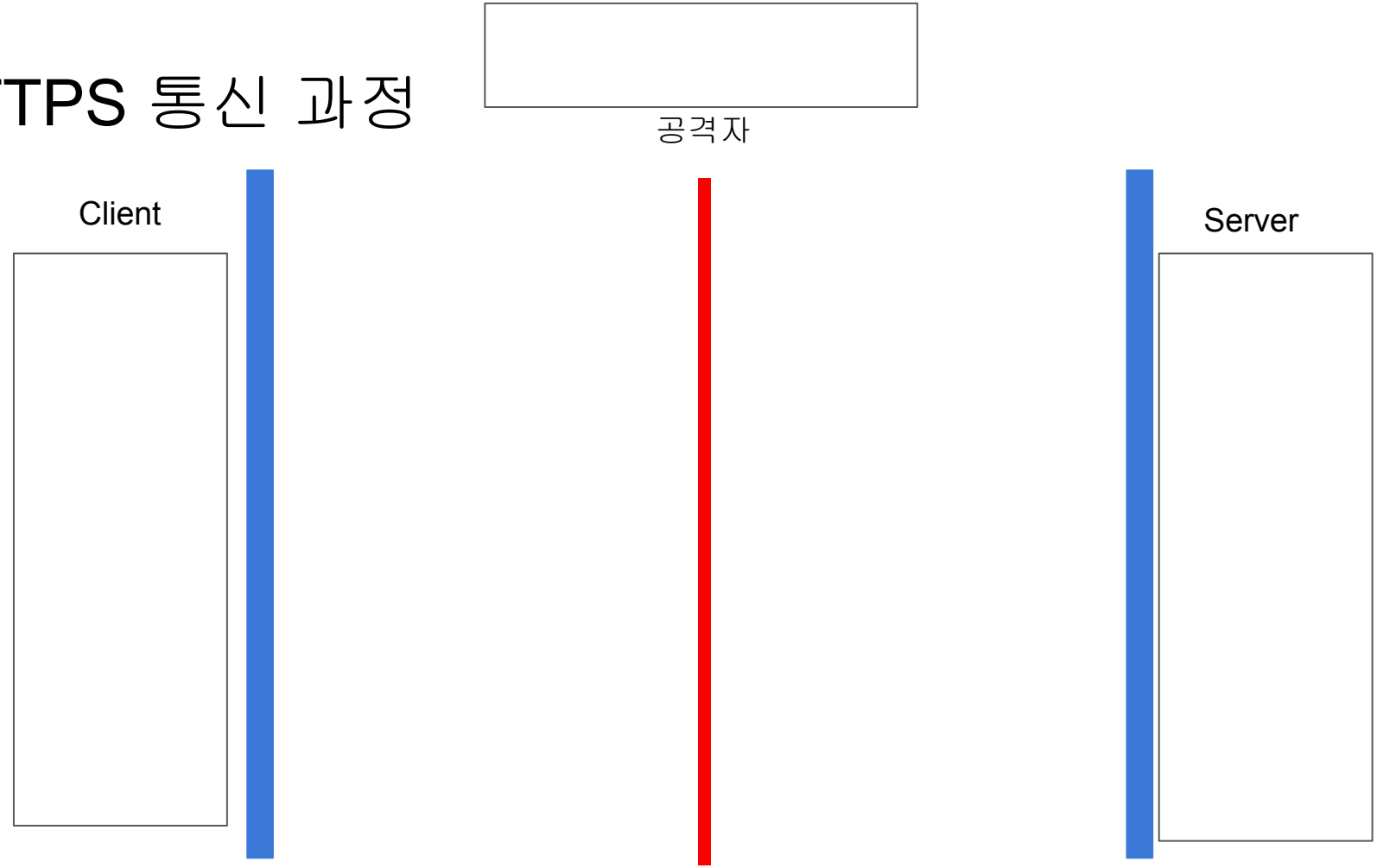
HTTPS 통신 과정


Client
TCP 3-way handshake
Server
Client random
Client Hello(TLS Version, Cipher suites, Session ID, Client random)
Client random
Server random
Server Hello(TLS Version, Cipher suite, Session ID, Server random)
Server random
Server Hello(CA), Server Hello Done
Pre-master Secret
Client Key Exchange, Change Cipher Spec
Pre-master Secret
Change Cipher Spec
Session key
Encrypted Application Data
Session key

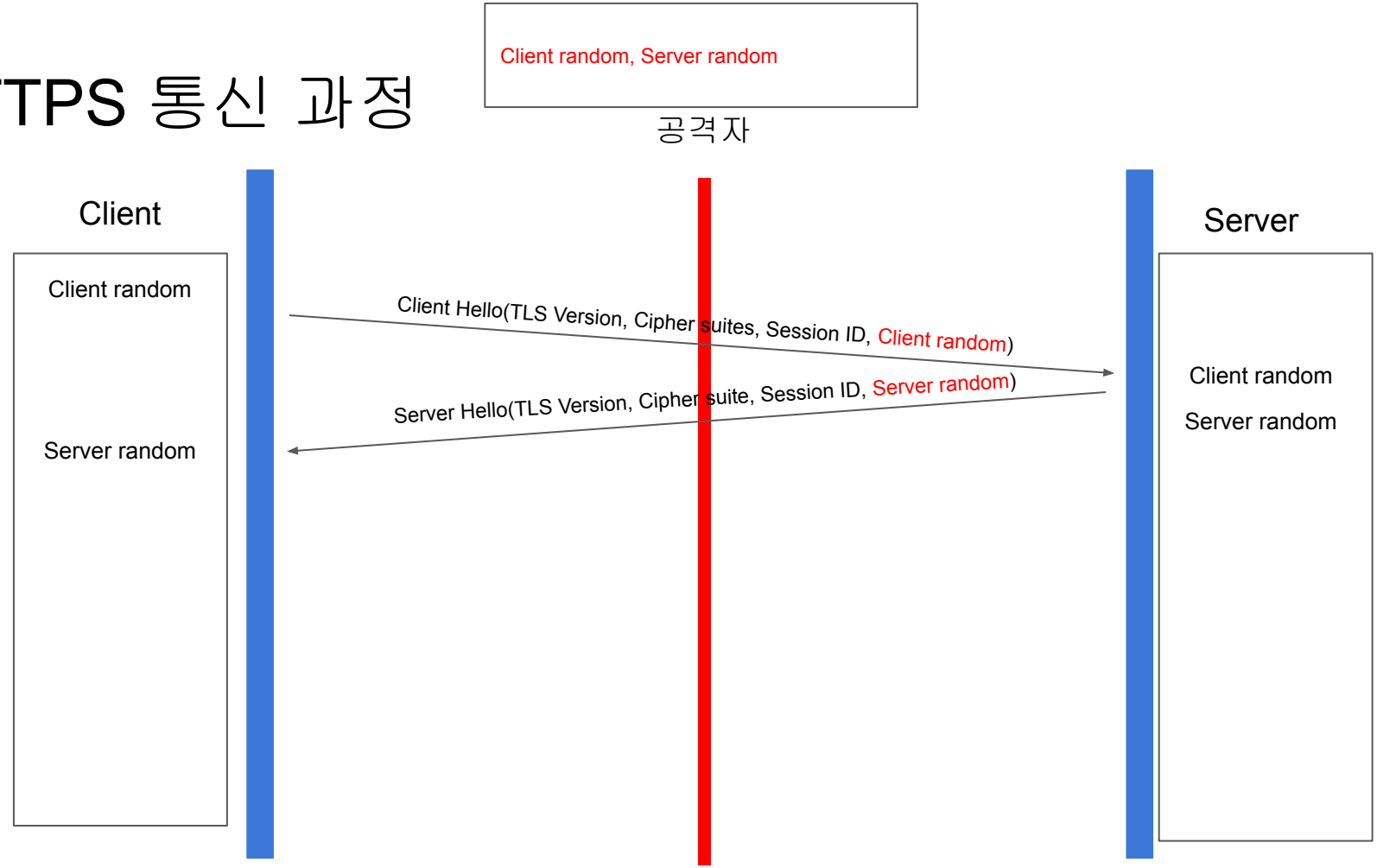
HTTPS 통신 과정


Client
TCP 3-way handshake
Server
Client random
Client Hello(TLS Version, Cipher suites, Session ID, Client random)
Client random
Server random
Server Hello(TLS Version, Cipher suite, Session ID, Server random)
Server random
Server Hello(CA), Server Hello Done
Pre-master Secret
Client Key Exchange, Change Cipher Spec
Pre-master Secret
Change Cipher Spec
GET /user
Session key
HTTP/1.1 200 OK
Session key

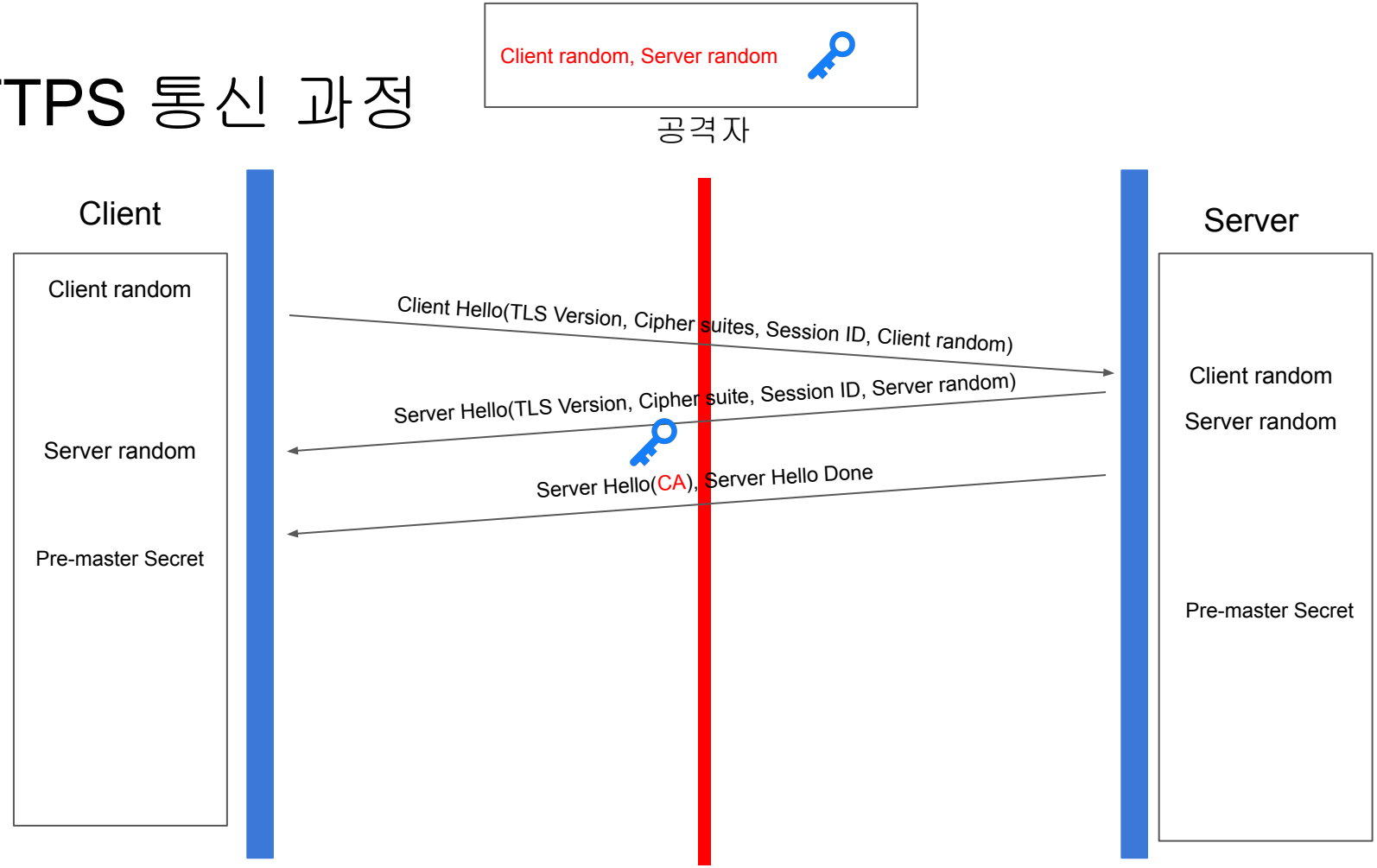
HTTPS 통신 과정



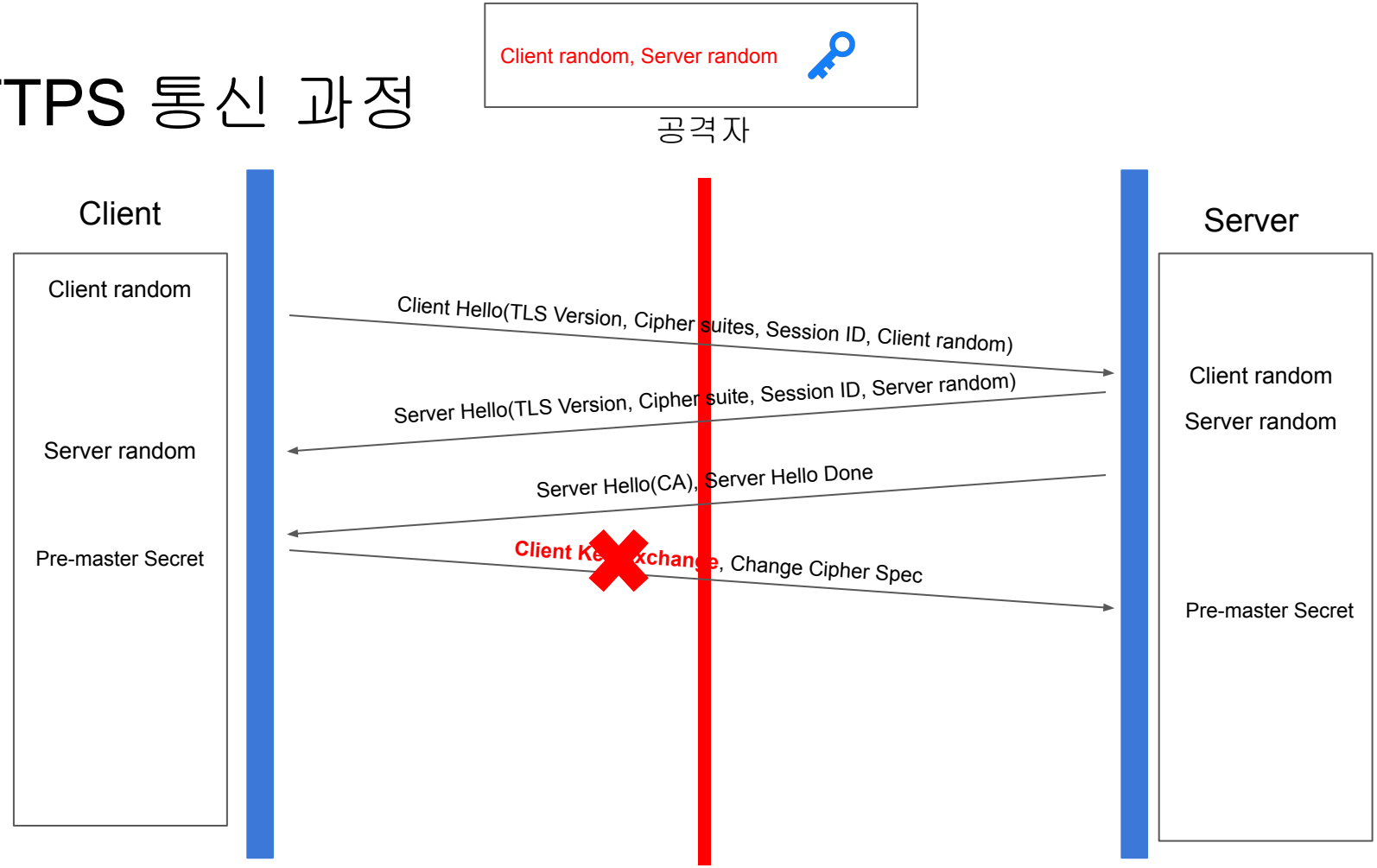
HTTPS 통신 과정


Client random, Server random
공격자
Client
Client random
Server random
Client Hello(TLS Version, Cipher suites, Session ID, Client random)
Server Hello(TLS Version, Cipher suite, Session ID, Server random)
Server
Client random
Server random

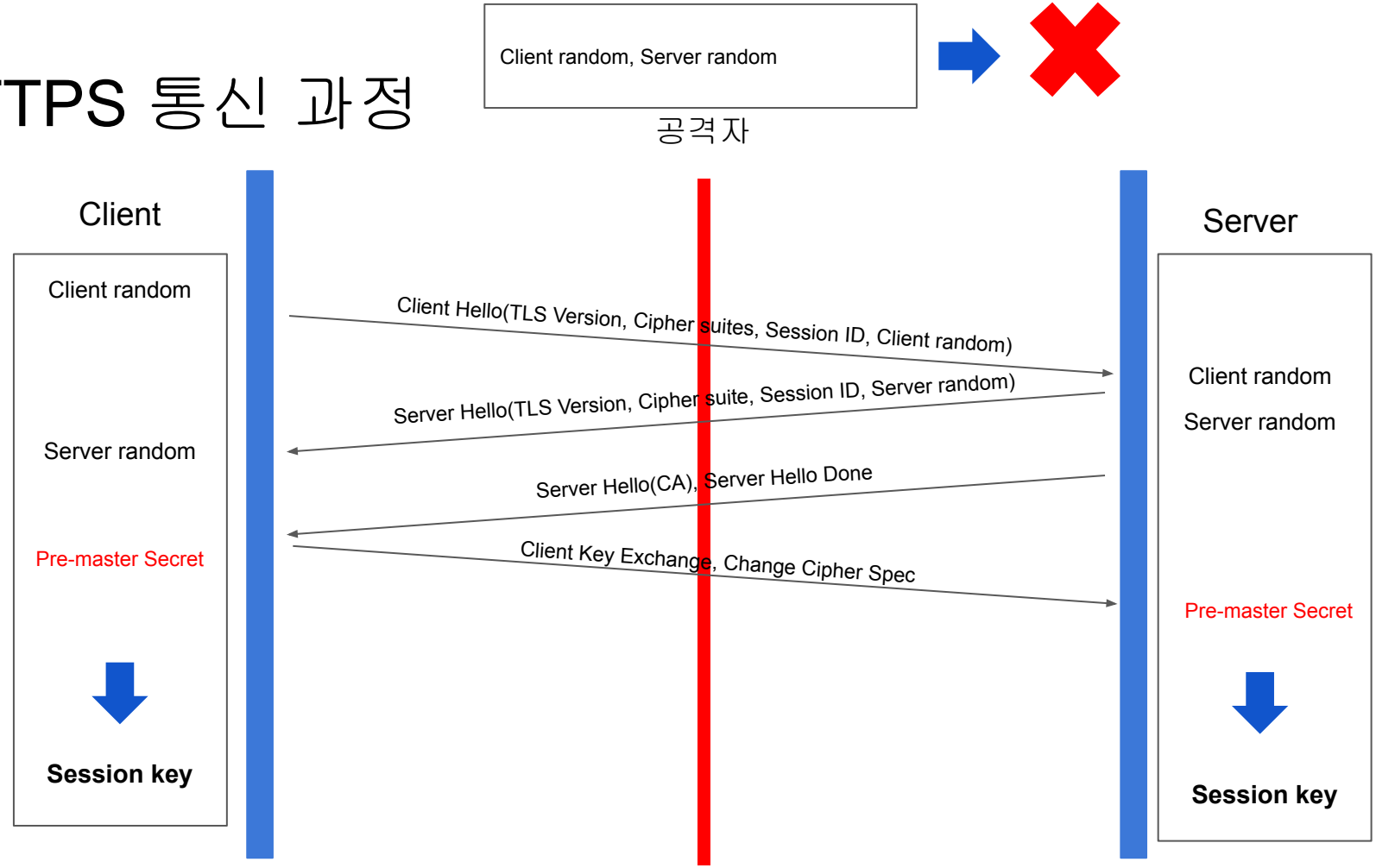
HTTPS 통신 과정


Client random, Server random
공격자
Client
Client random
Server random
Pre-master Secret
Client Hello(TLS Version, Cipher suites, Session ID, Client random)
Server Hello(TLS Version, Cipher suite, Session ID, Server random)
Server Hello(CA), Server Hello Done
Server
Client random
Server random
Pre-master Secret

HTTPS 통신 과정


Client random, Server random
공격자
Client
Client random
Server random
Pre-master Secret
Client Hello(TLS Version, Cipher suites, Session ID, Client random)
Server Hello(TLS Version, Cipher suite, Session ID, Server random)
Server Hello(CA), Server Hello Done
Client Key Exchange, Change Cipher Spec
Server
Client random
Server random
Pre-master Secret

HTTPS 통신 과정


Client random, Server random
공격자
Client
Client random
Server random
Pre-master Secret
Session key
Client Hello(TLS Version, Cipher suites, Session ID, Client random)
Server Hello(TLS Version, Cipher suite, Session ID, Server random)
Server Hello(CA), Server Hello Done
Client Key Exchange, Change Cipher Spec
Server
Client random
Server random
Pre-master Secret
Session key

꼿

Thanks