CSCI 1515 Applied Cryptography

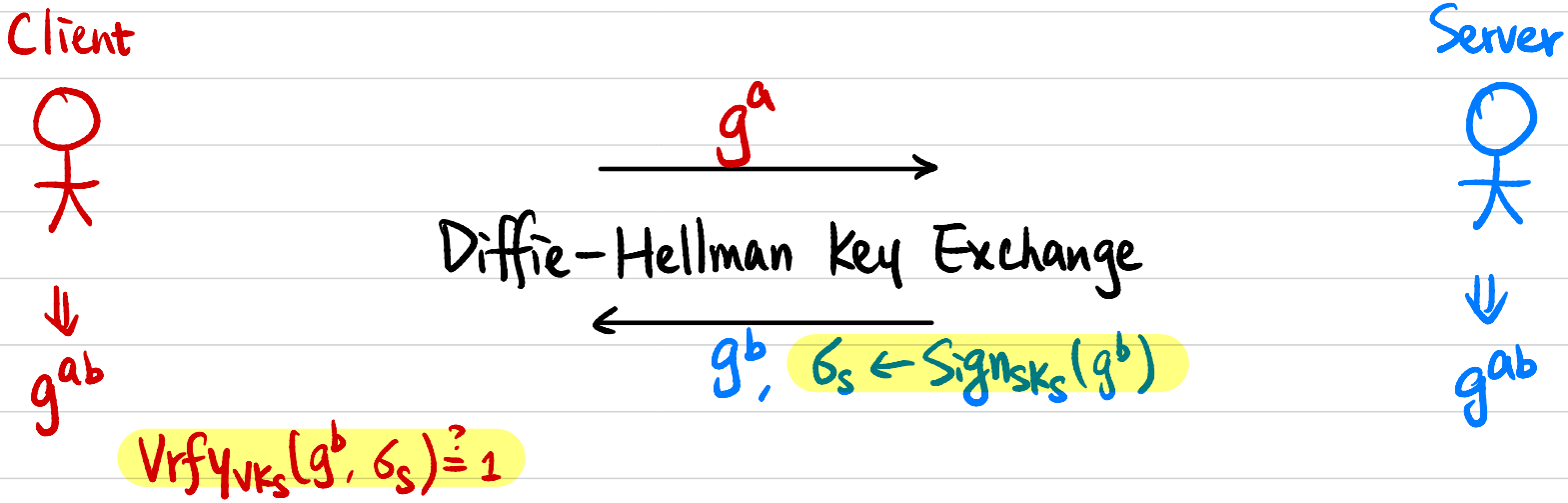
This Lecture:

- Public Key Infrastructure (continued)
- Password-Based Authentication
- Two-Factor Authentication (2FA)

One-Sided Secure Authentication

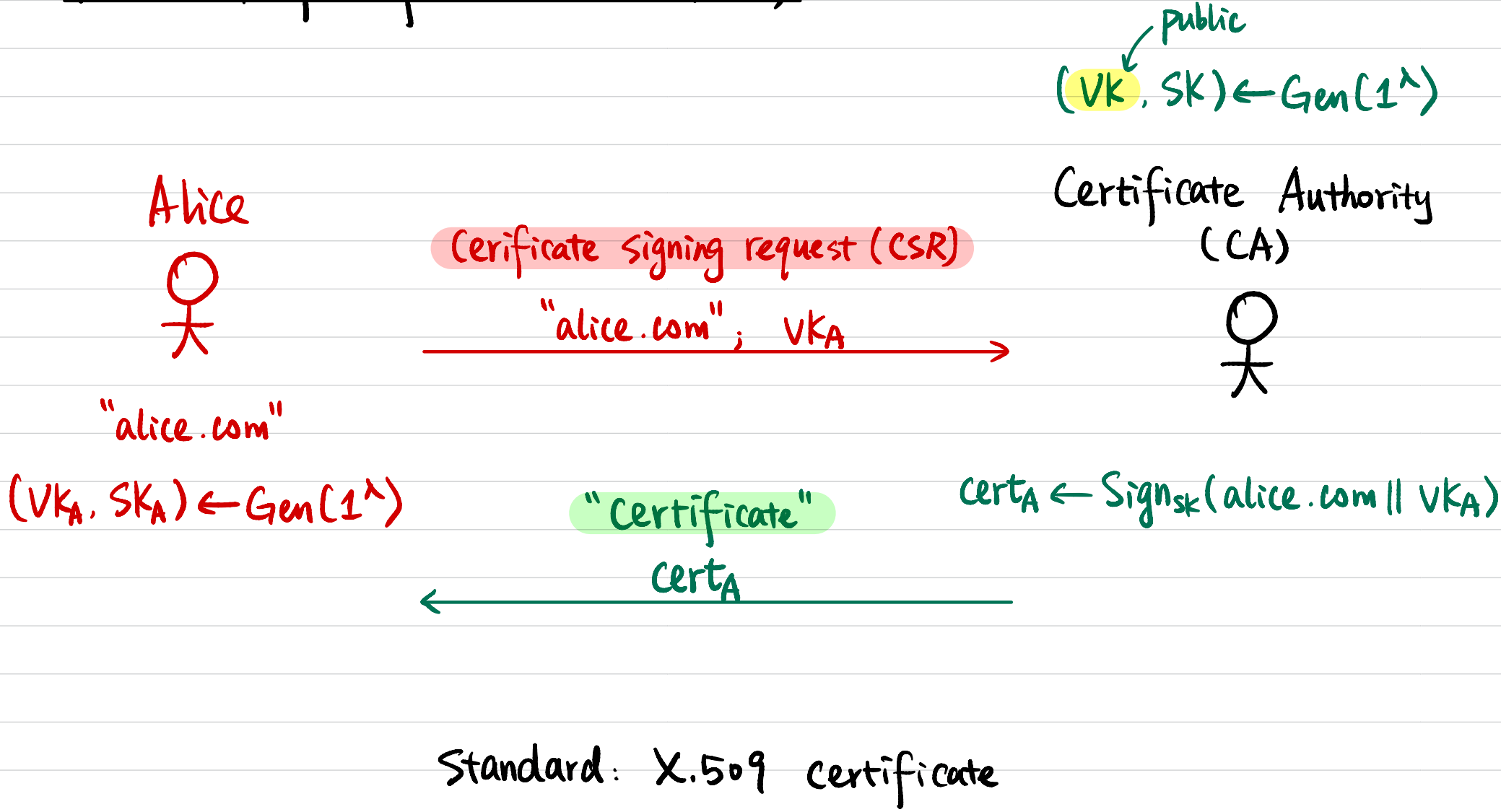
public — Where does it come from?

$(vk_S, sk_S) \leftarrow Gen(1^\lambda)$



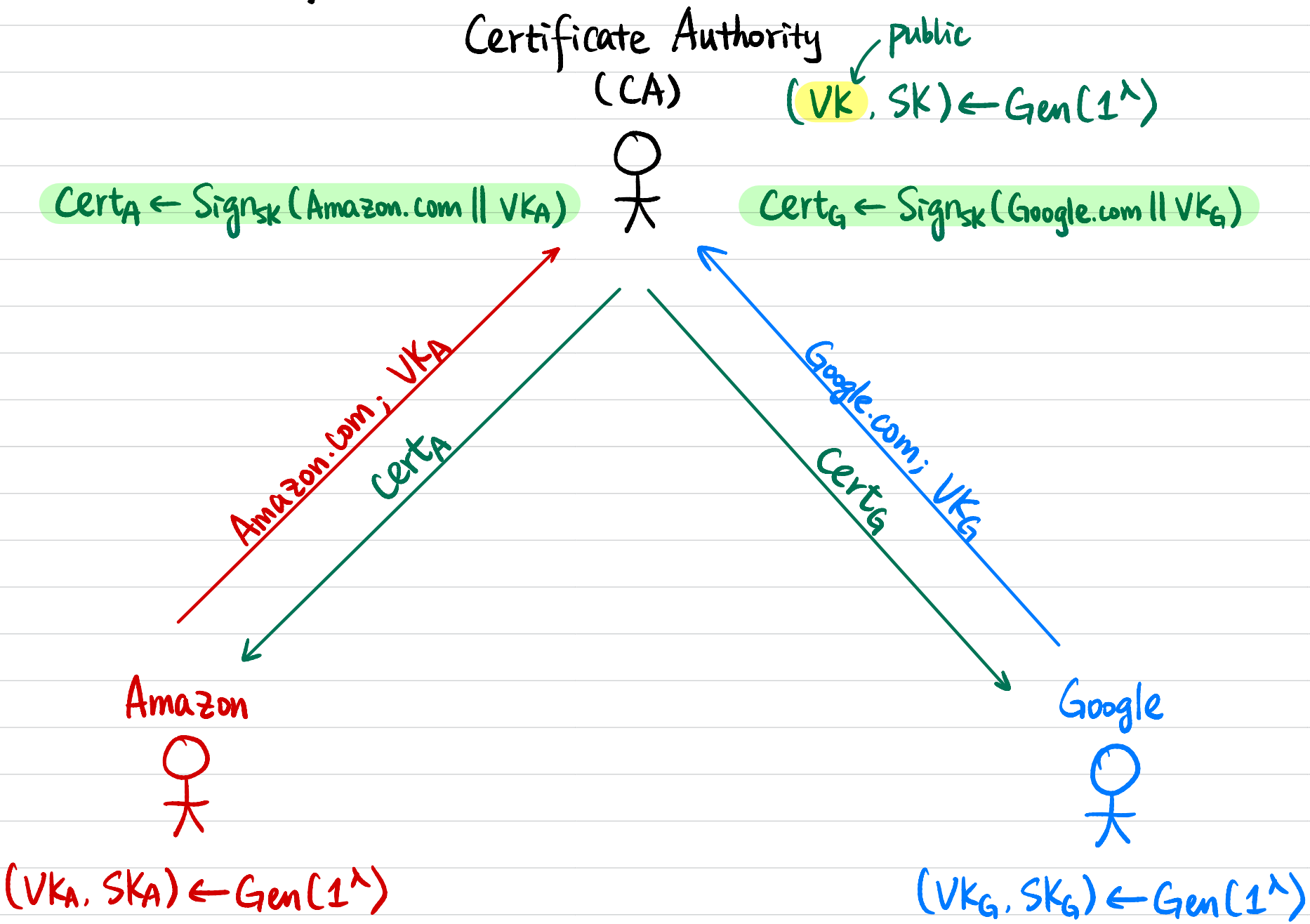
Can we prevent Man-in-the-Middle Attack?

Public Key Infrastructure (PKI)

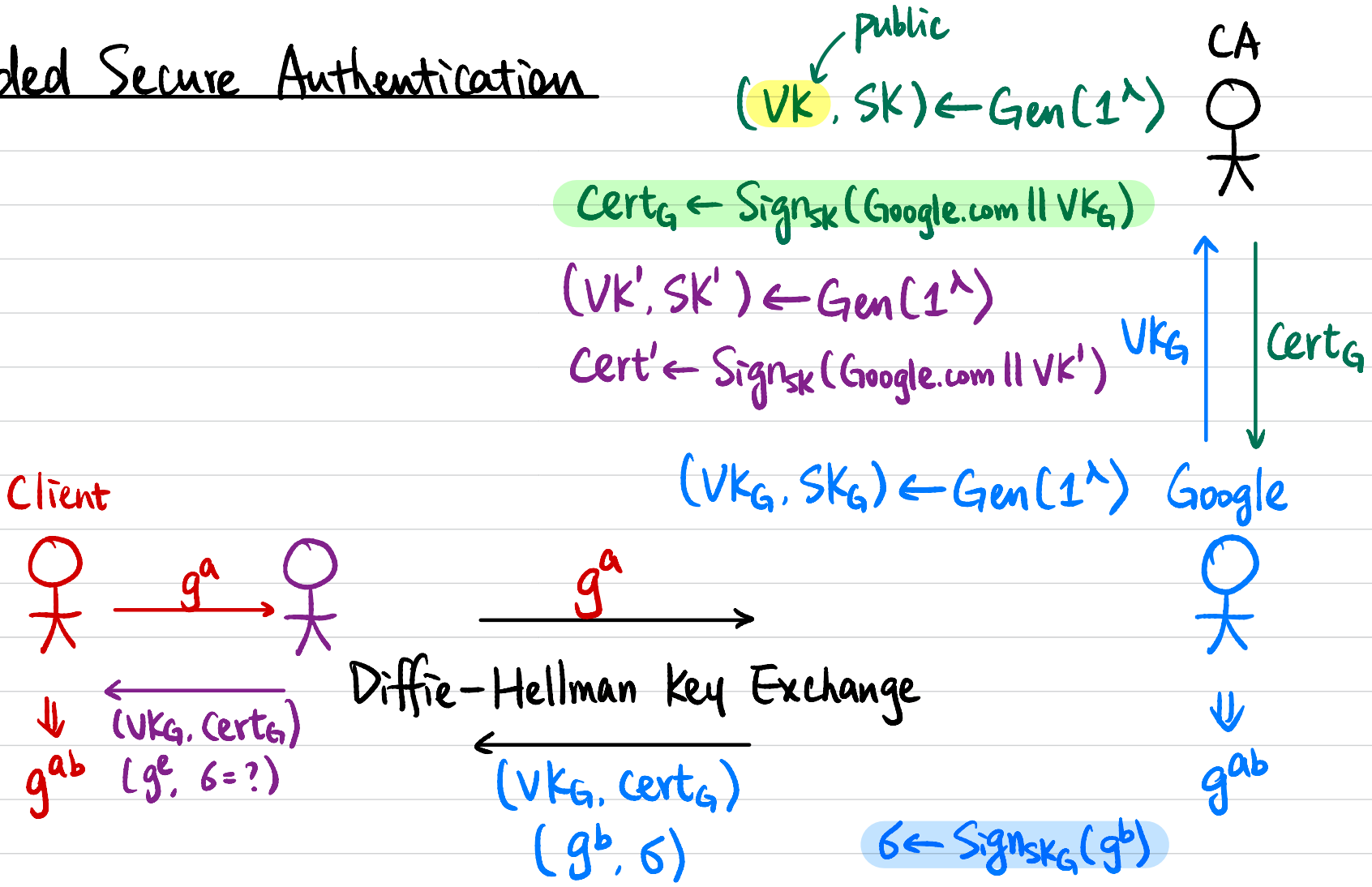


Standard: X.509 certificate

Public Key Infrastructure (PKI)



One-Sided Secure Authentication



$Vrfy_{VK}(Google.com \| VK_G, Cert_G) \stackrel{?}{=} 1$

$Vrfy_{VK_G}(g^b, \sigma) \stackrel{?}{=} 1$

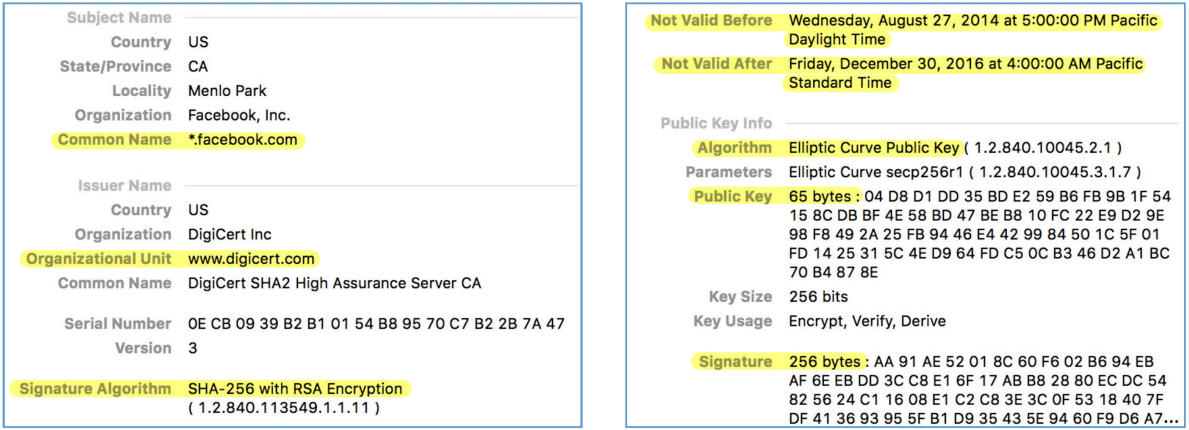
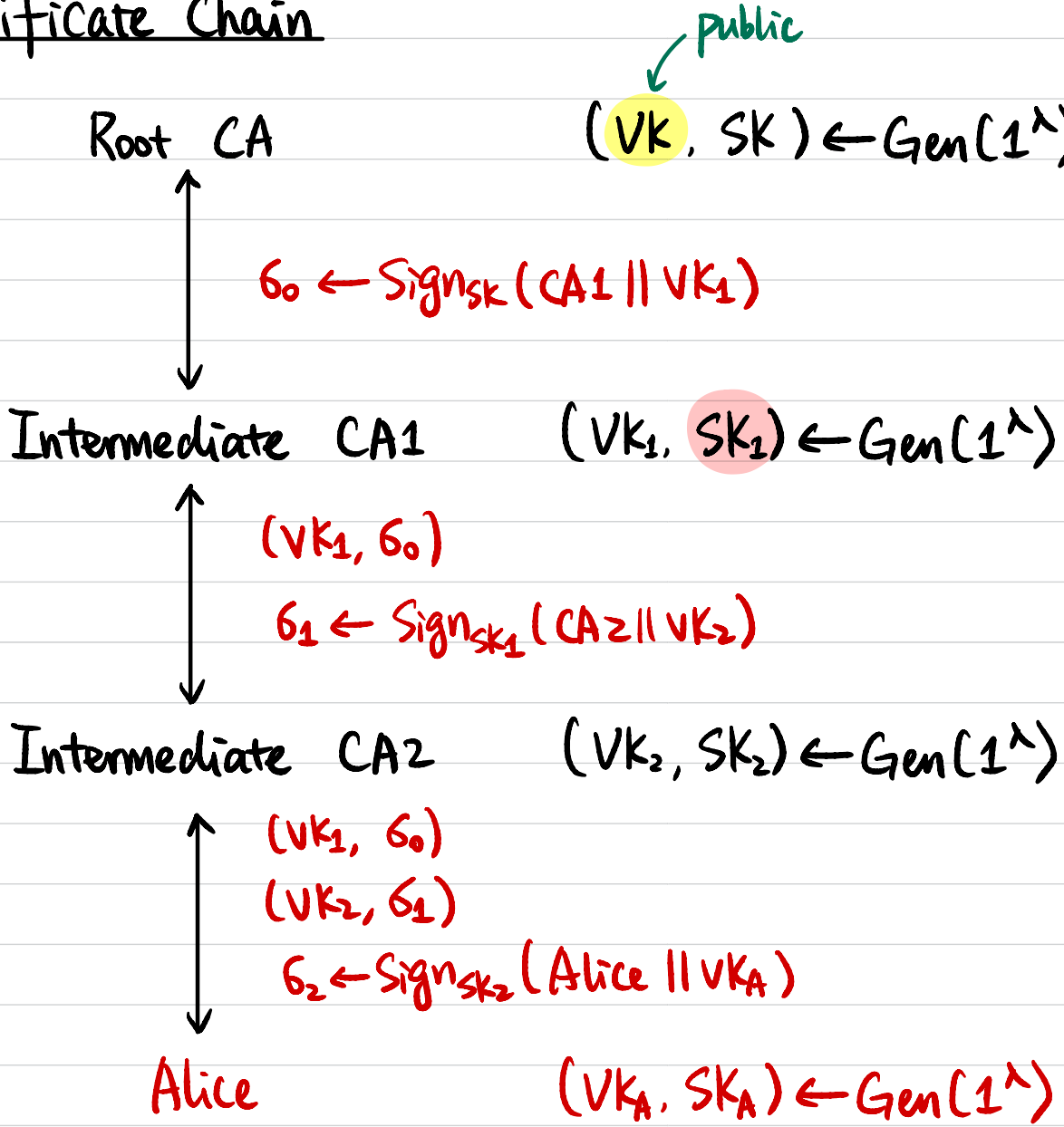


Figure 13.4: An example X.509 certificate

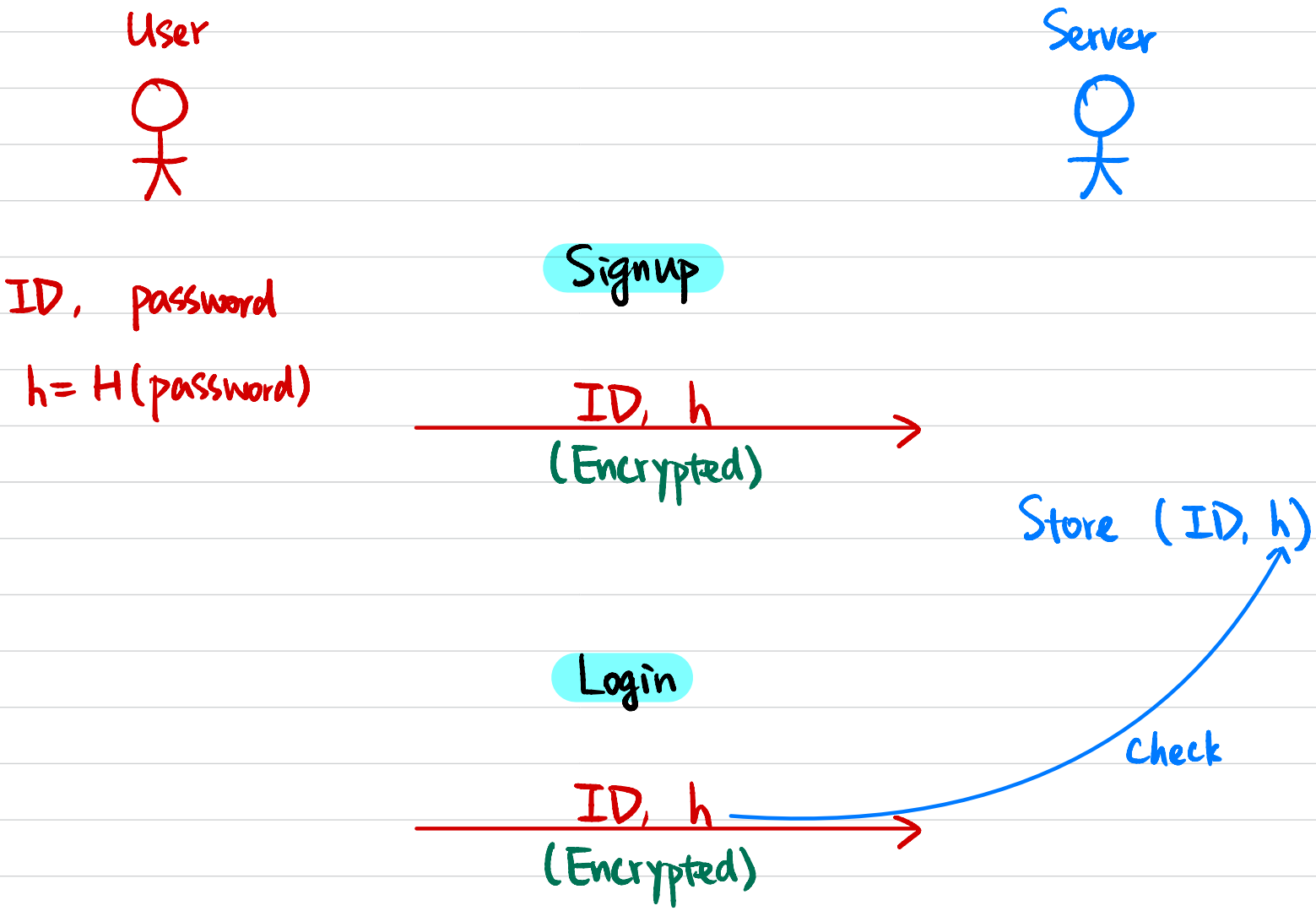
Certificate Chain



Certificate Revocation

- Short-lived certificates
- Certificate revocation lists (CRLs)

Password-Based Authentication



Password Security ?

Online Dictionary Attack

ID, password

$h = H(\text{password})$

Signup

ID, h

(Encrypted)

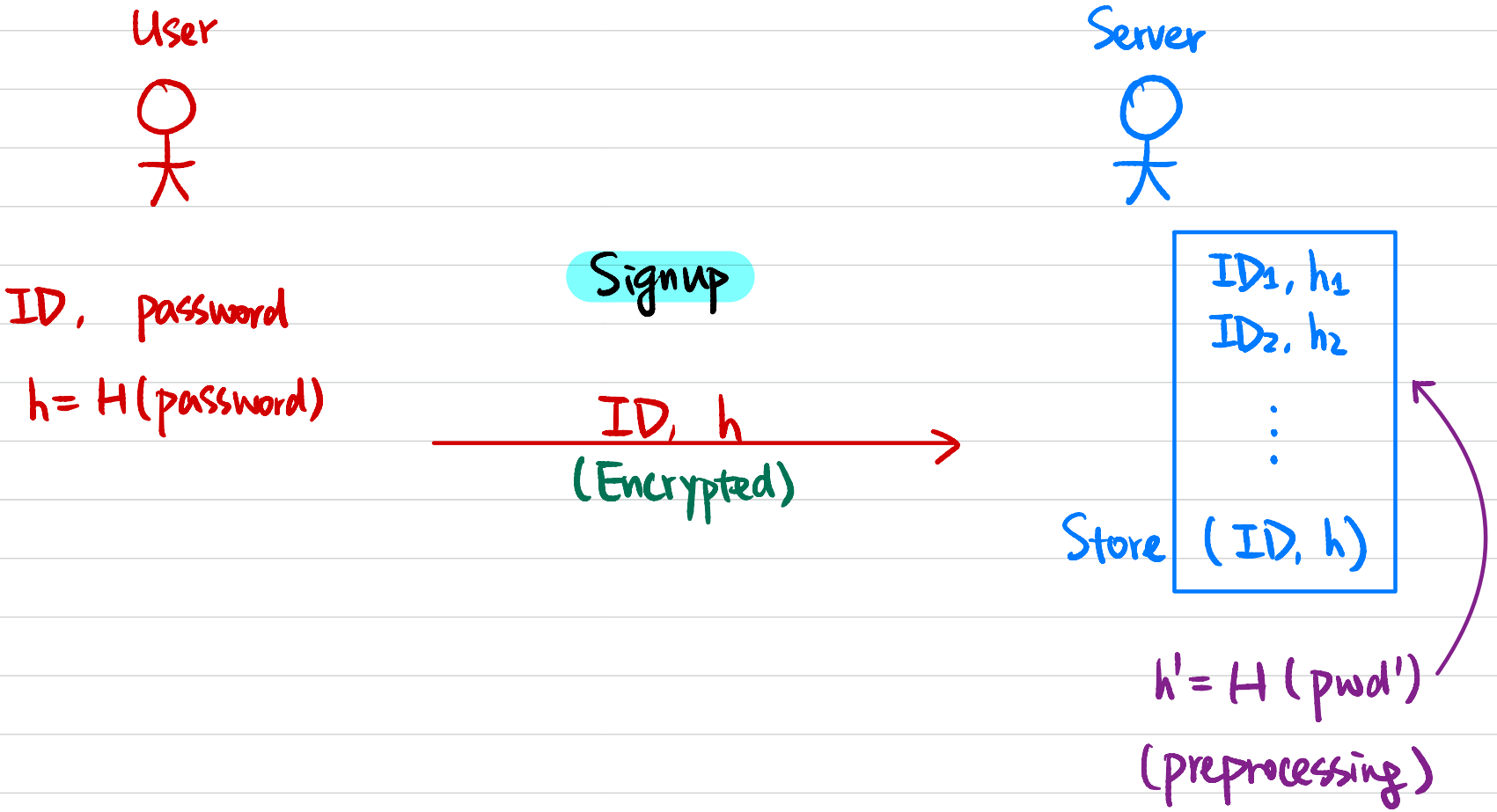
Store (ID, h)

Login

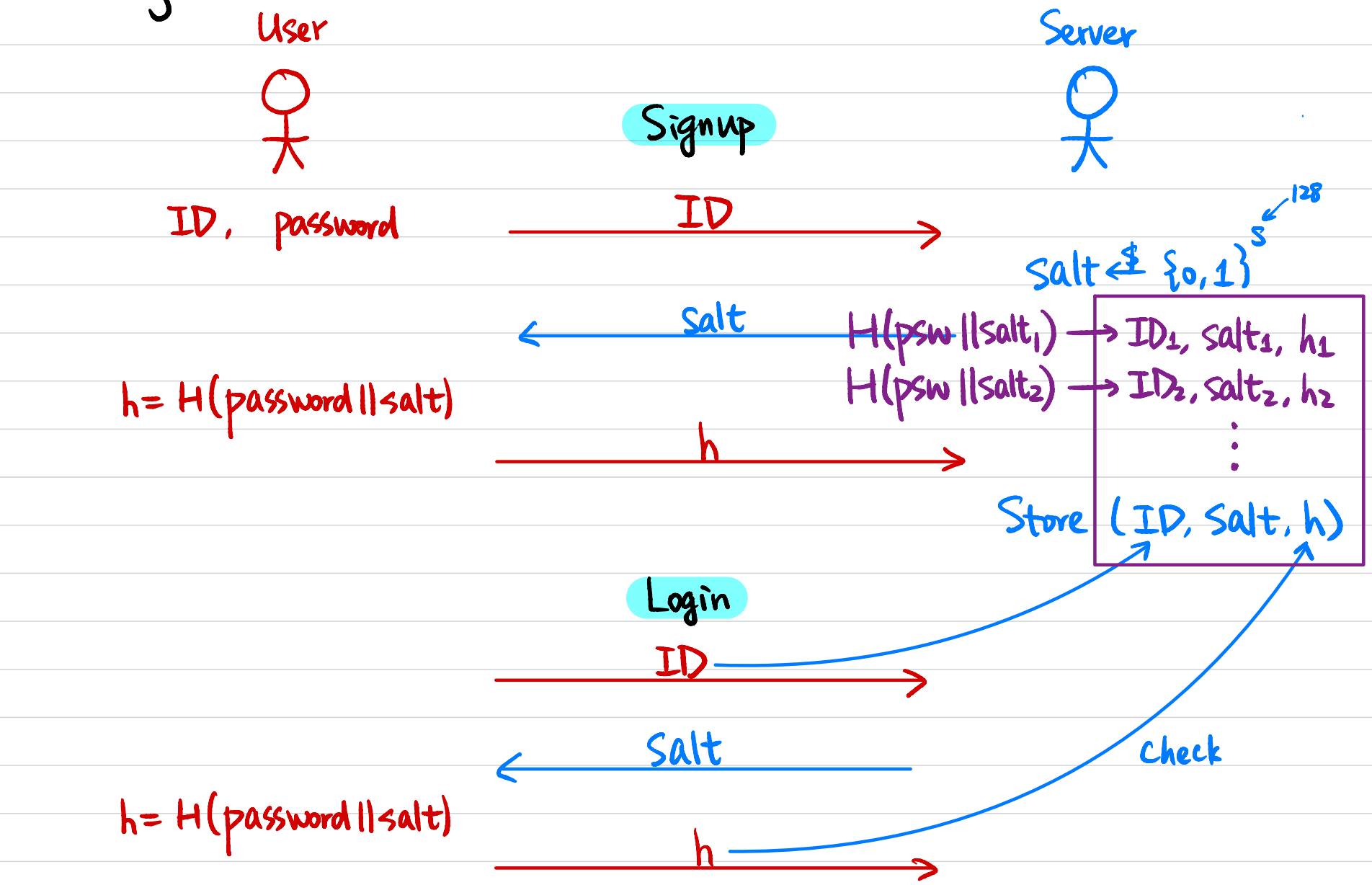
ID, $h' = H(\text{pwd}')$

(Encrypted)

Offline Dictionary Attack

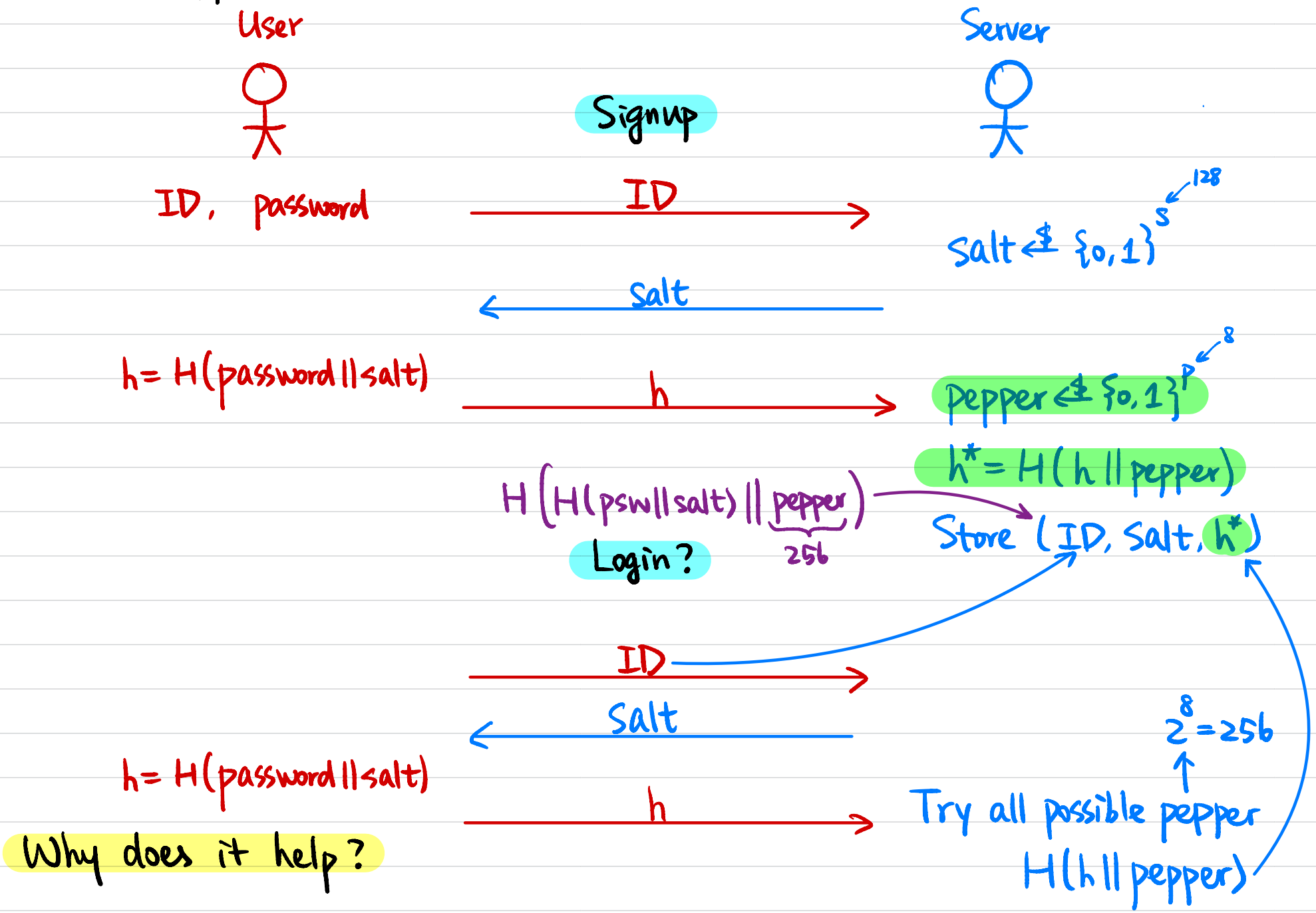


Salting



Why does it help?

Salt & Pepper


User
Server
Signup
ID, password
ID
Salt ← $ {0,1}^s
128
Salt
h = H(password || salt)
h
pepper ← $ {0,1}^p
8
h* = H(h || pepper)
H(H(psw||salt) || pepper)
256
Login?
Store (ID, Salt, h*)
ID
Salt
h = H(password || salt)
h
2^8 = 256
Try all possible pepper
H(h || pepper)
Why does it help?

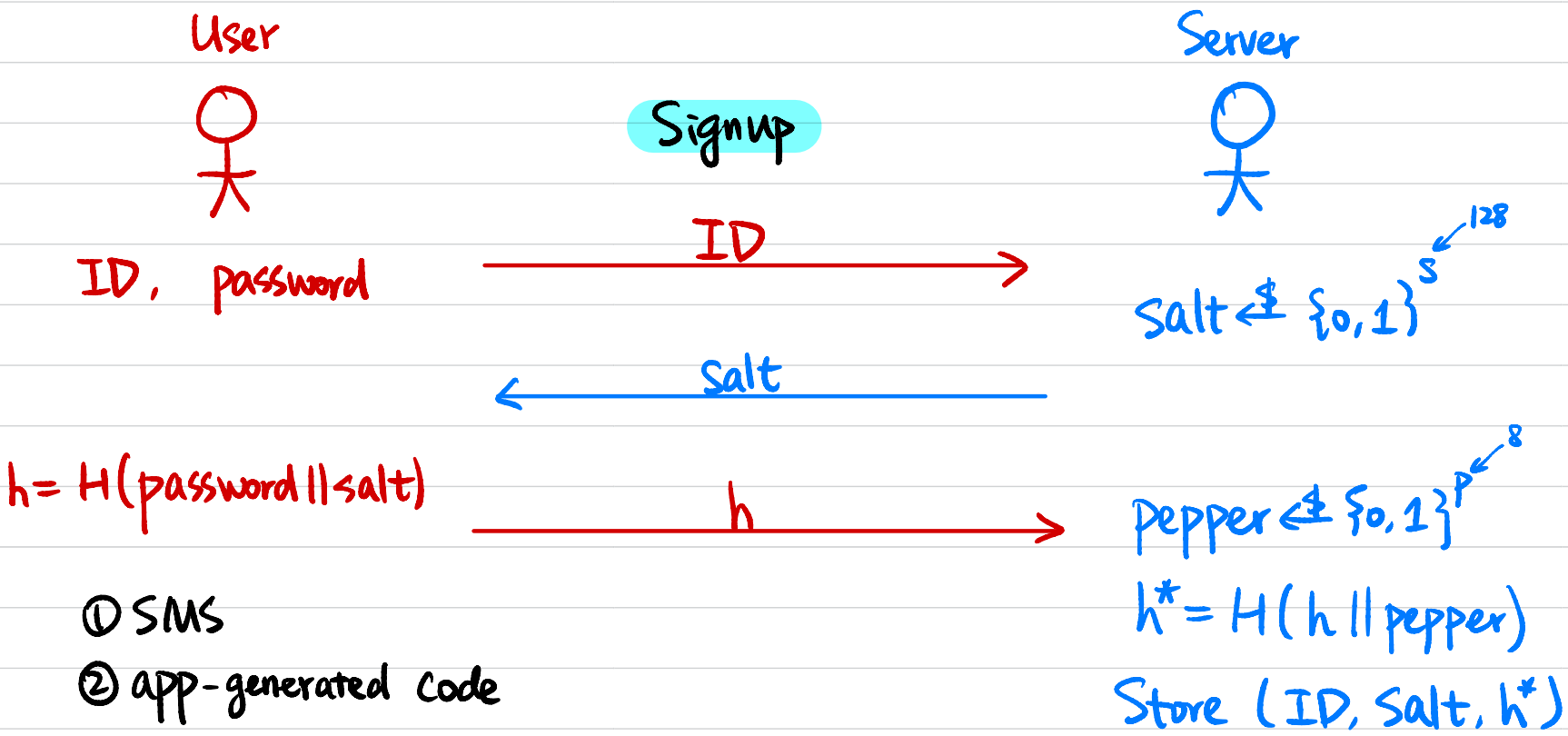
Slow Hash Functions

- Computation-heavy hash function
  - ↳ Compose SHA256 in a certain way.

Application-Specific Integrated Circuit (ASIC) → blockchain mining

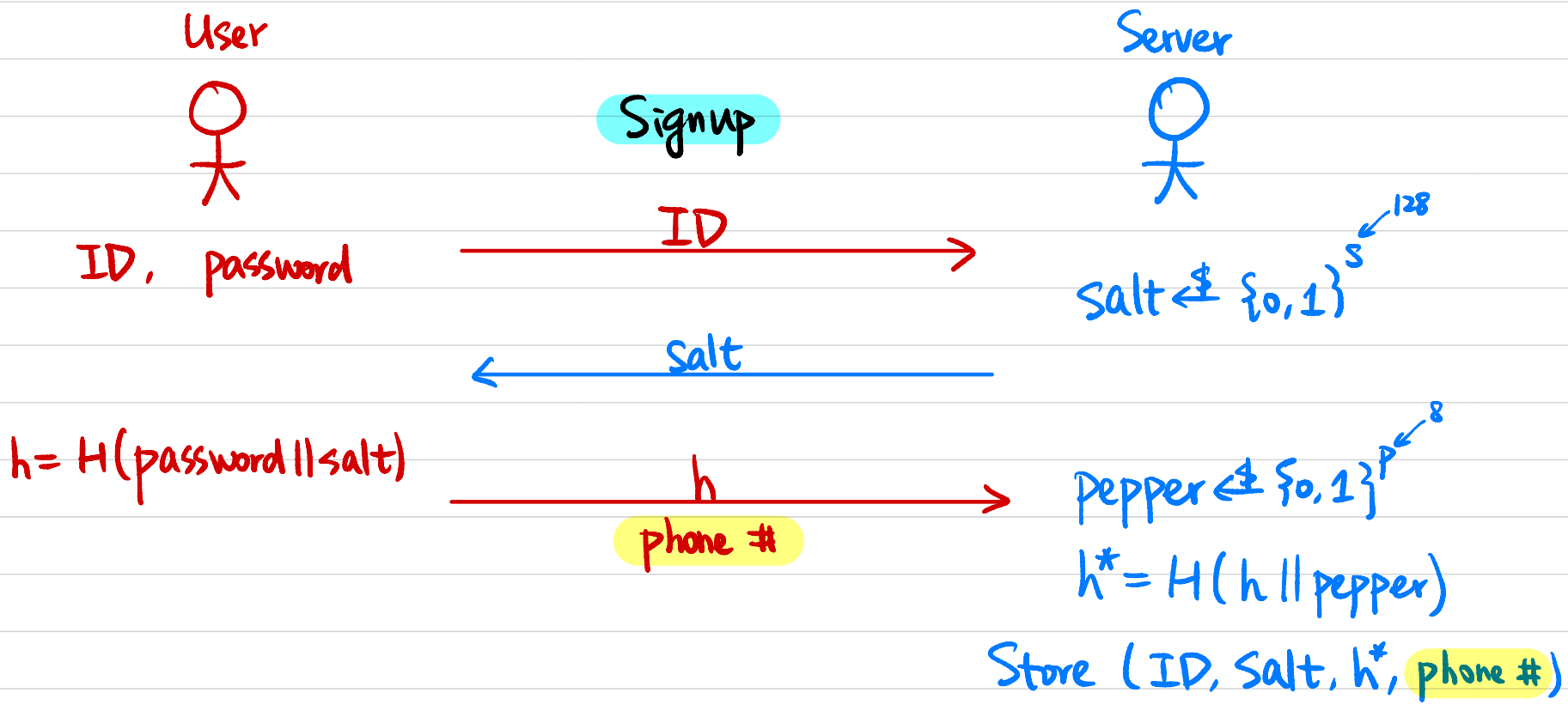
- Memory-hard hash functions
  - ↳ Scrypt

Two-Factor Authentication (2FA)



How would you design it ?

Two-Factor Authentication (2FA) ① SMS



Two-Factor Authentication (2FA) ② app-generated code