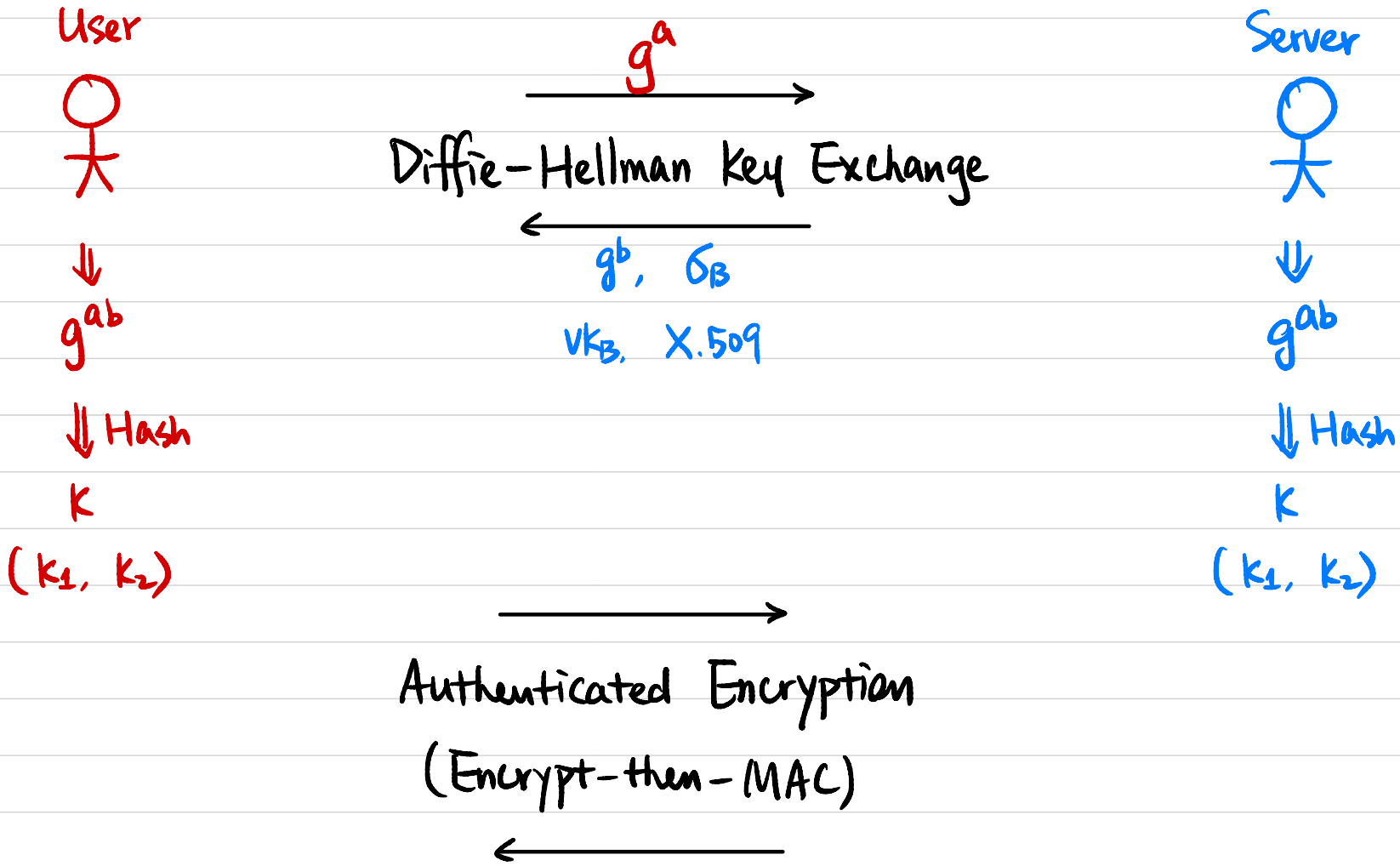
CSCI 1515 Applied Cryptography

This Lecture:

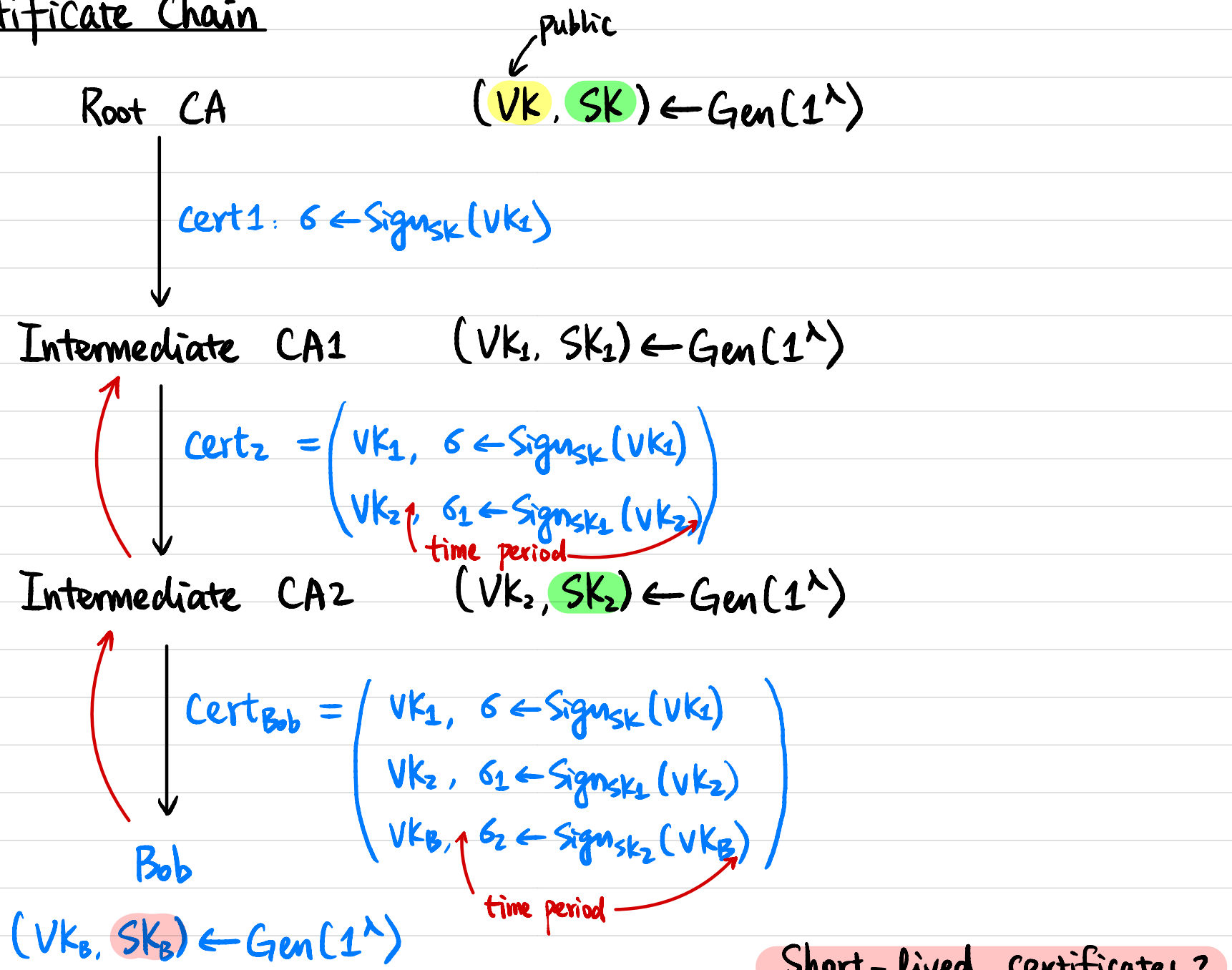
- Password-Based Authentication (Continued)
- Putting it Together: Secure Authentication
- Case Study: Group Chat

One-Sided Secure Authentication

$(VK_B, SK_B) \leftarrow Gen(1^\lambda)$

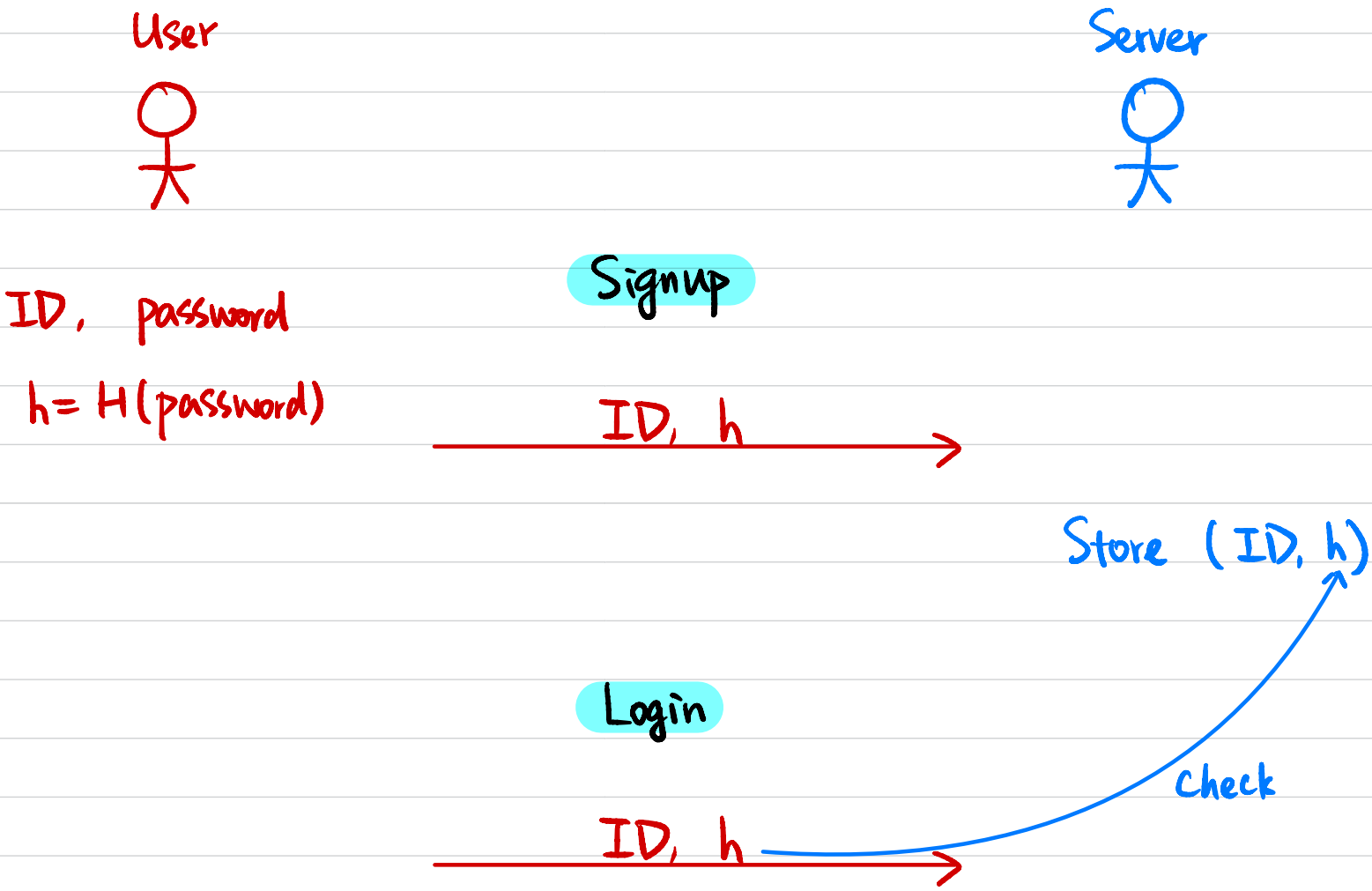


Certificate Chain



Short-lived certificates ?

Password-Based Authentication



Attacks ?

Online Dictionary Attack

ID, password

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

Signup

ID, h →

Store (ID, h)

Login

ID, h' →

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

Offline Dictionary Attack

ID, password

h = H(password)

Signup

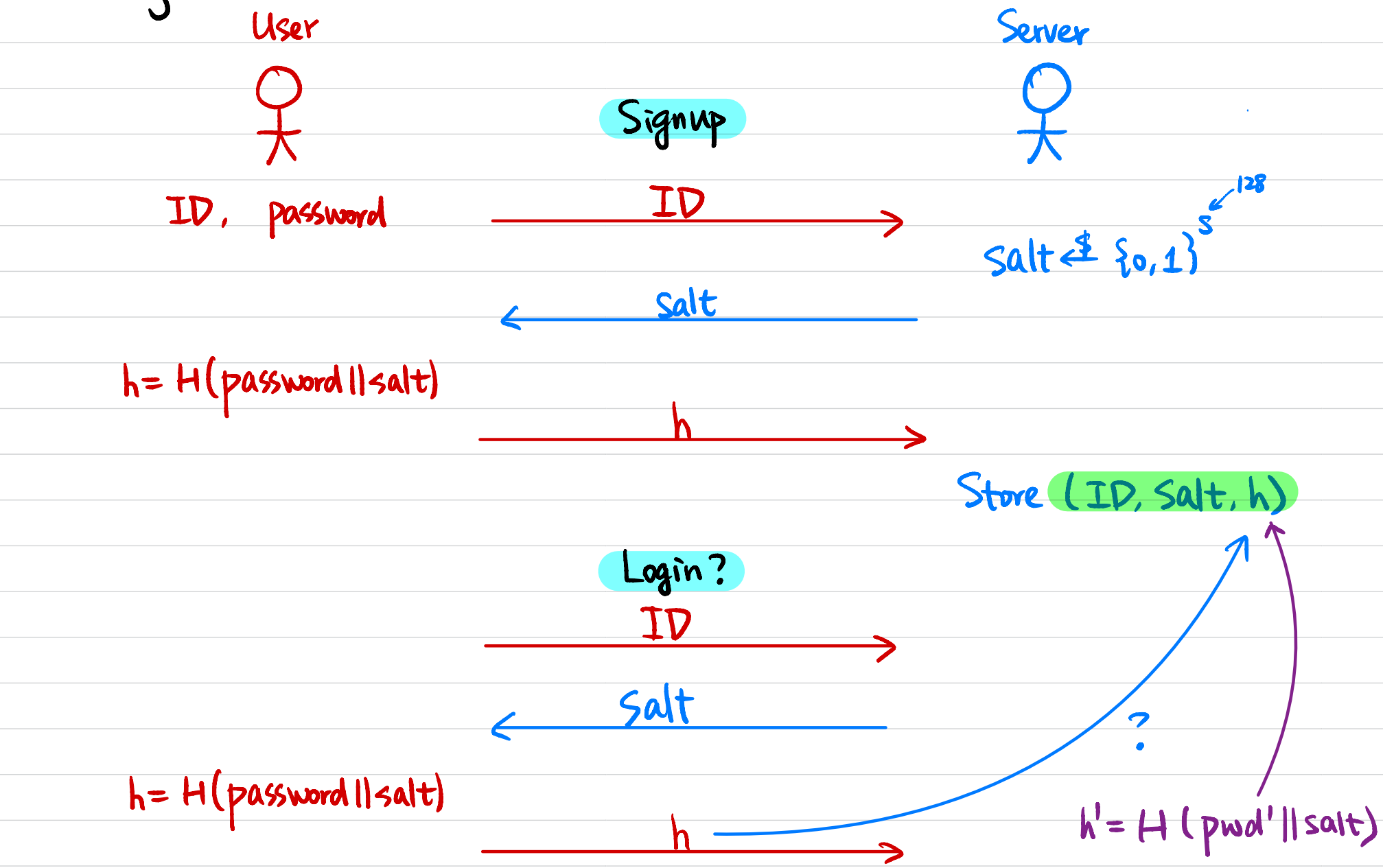
ID, h

Store (ID, h)

h' = H(pwd')

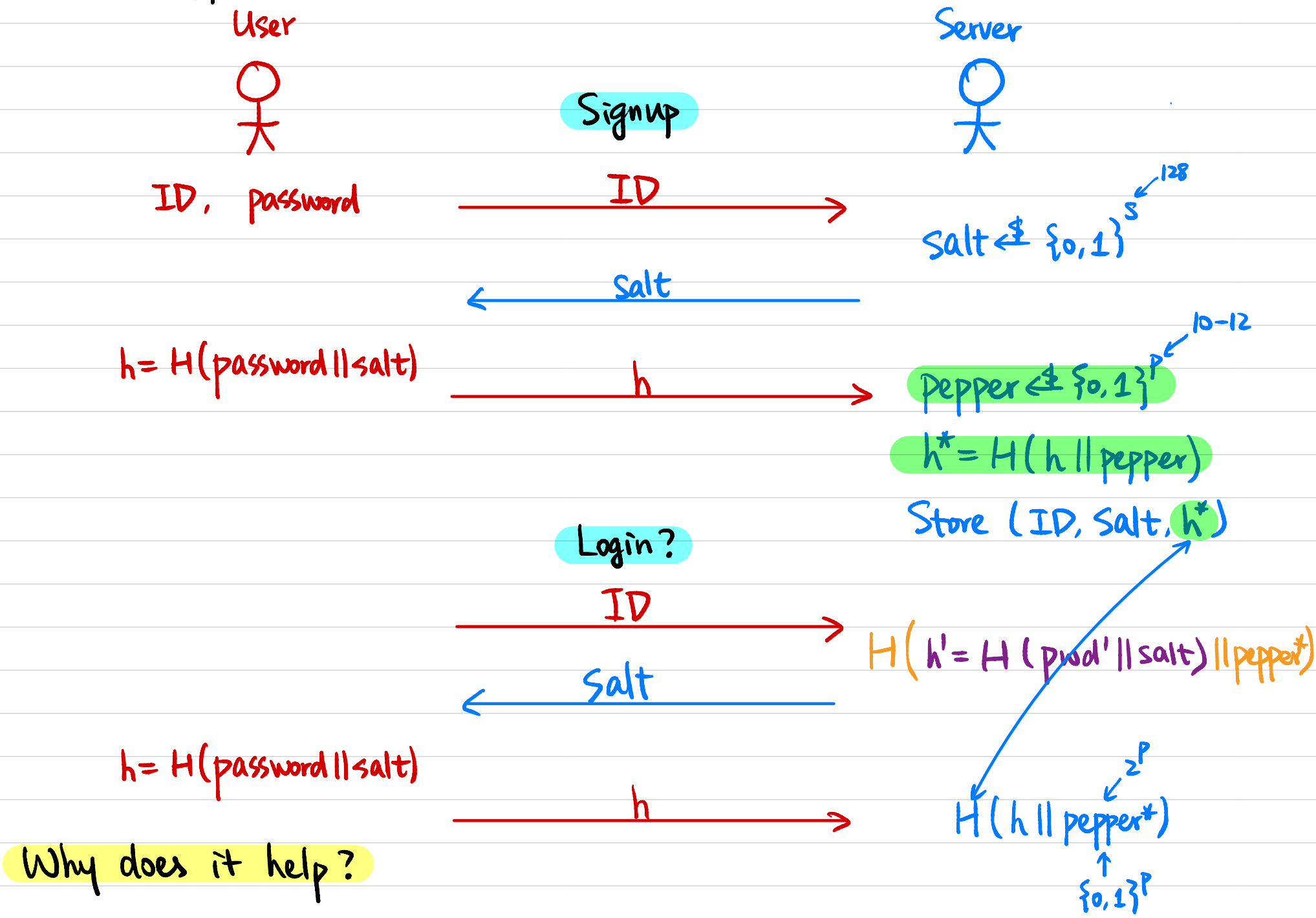
(preprocessing)

Salting



Why does it help?

Salt & Pepper


User
Server
Signup
ID, password
ID
Salt ← $ {0,1}^s
128
Salt
h = H(password || salt)
h
10-12
pepper ← $ {0,1}^p
h* = H(h || pepper)
Store (ID, Salt, h*)
Login?
ID
H(h' = H(pwd' || salt) || pepper*)
Salt
h = H(password || salt)
h
2^p
H(h || pepper*)
{0,1}^p
Why does it help?

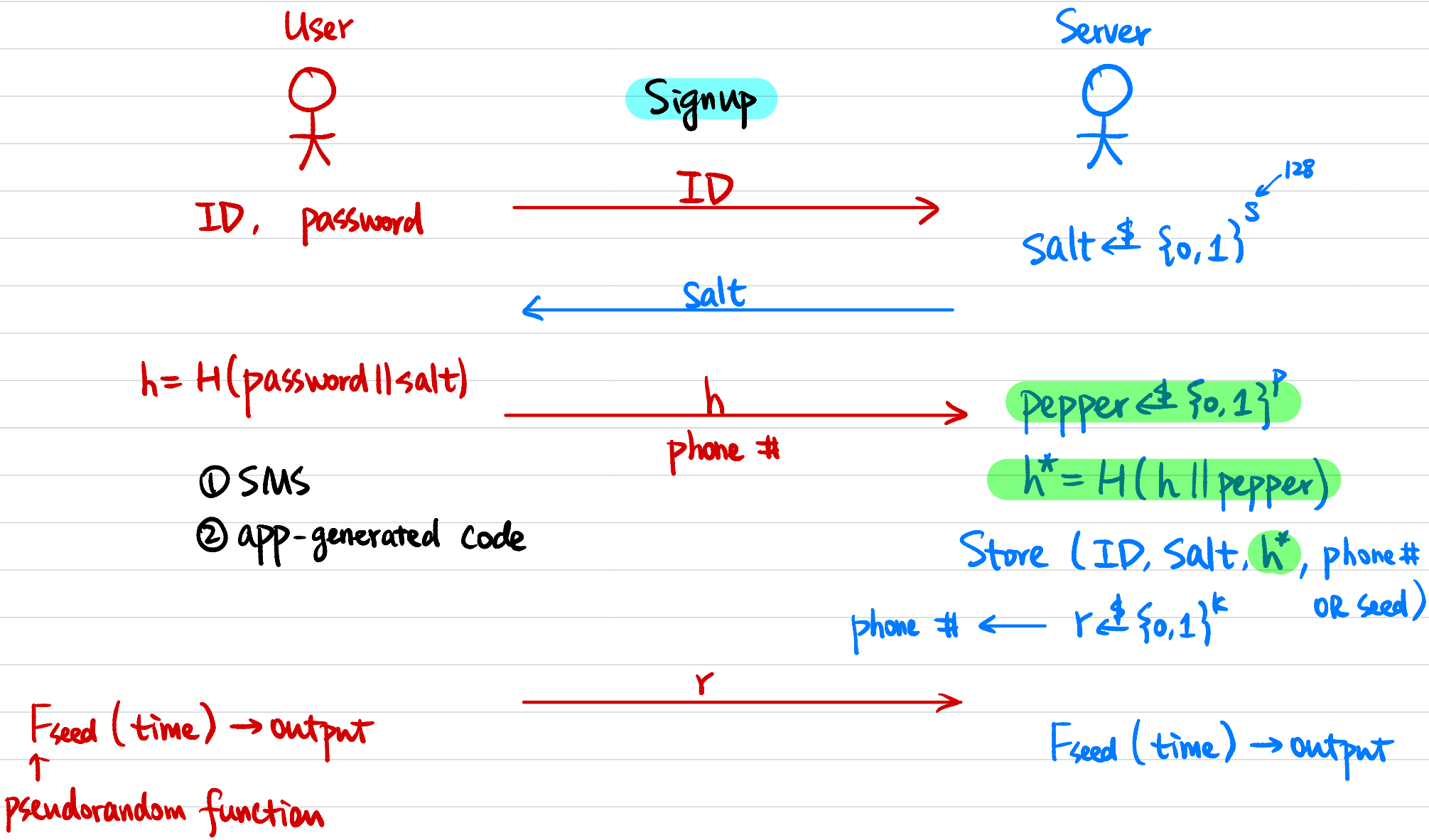
Slow Hash Functions

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

Application-Specific Integrated Circuit (ASIC) → blockchain mining

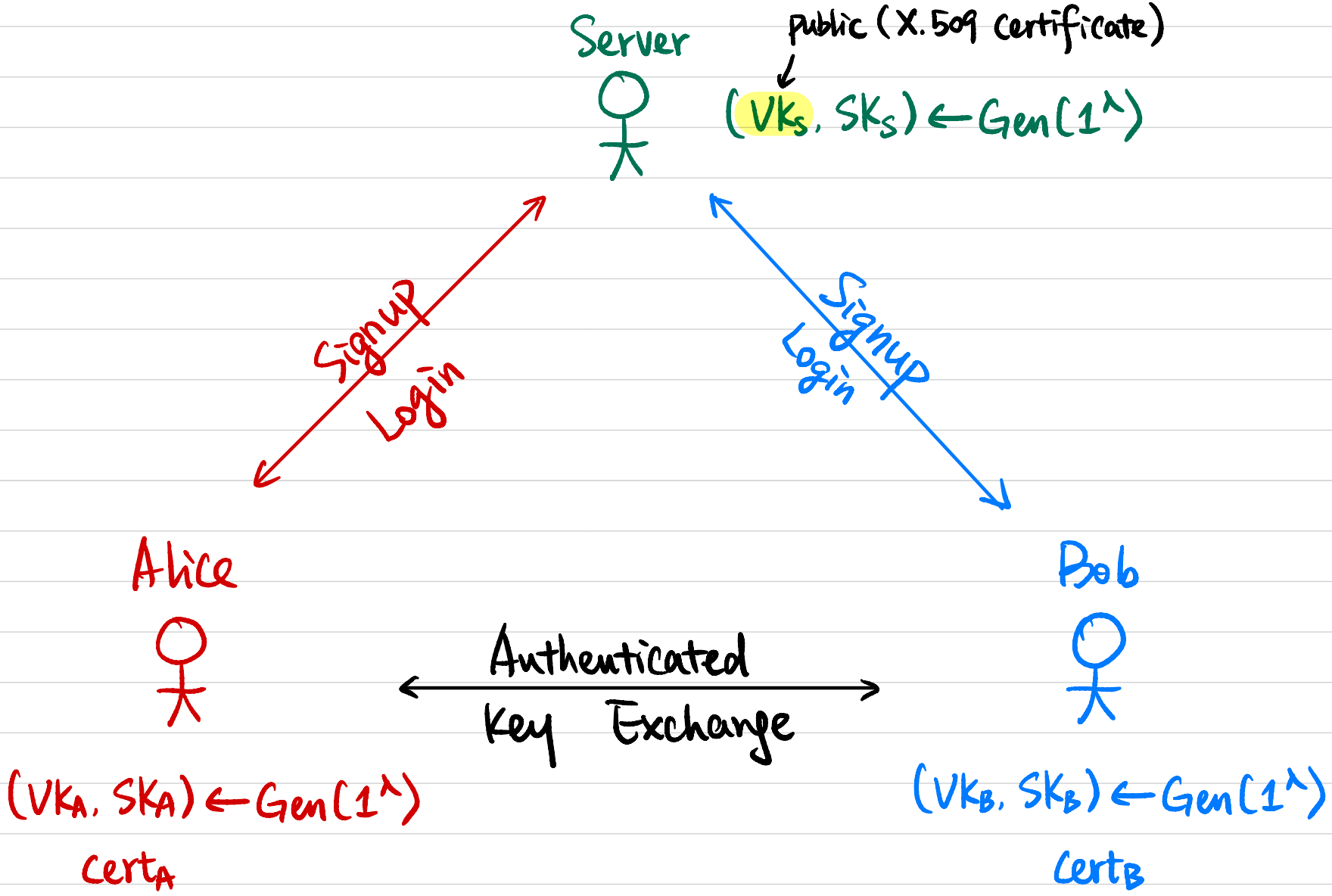
- Memory-hard hash functions
  - ↳ Scrypt

Two-Factor Authentication (2FA)

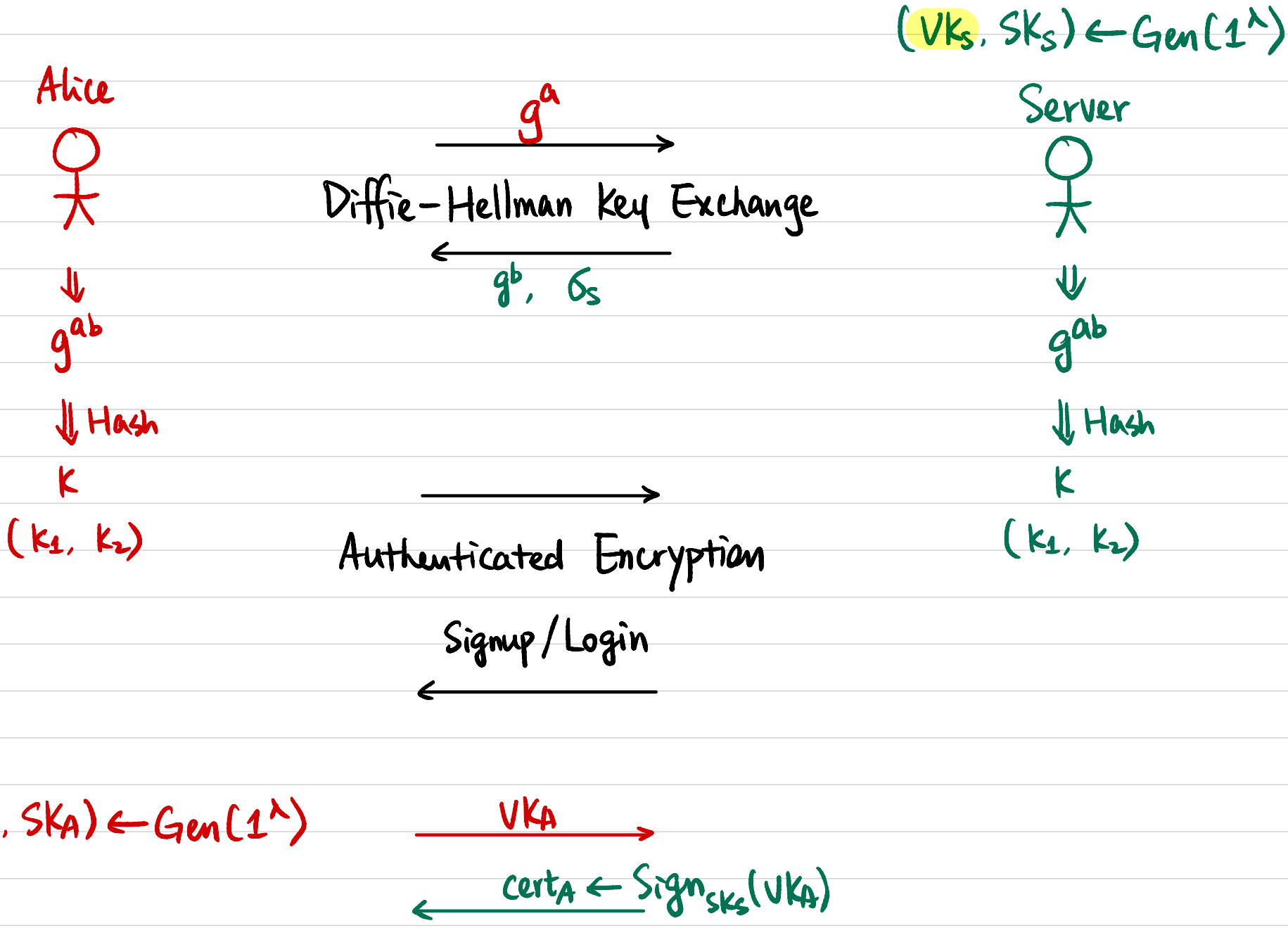


How would you design it ?

Putting it Together: Secure Authentication



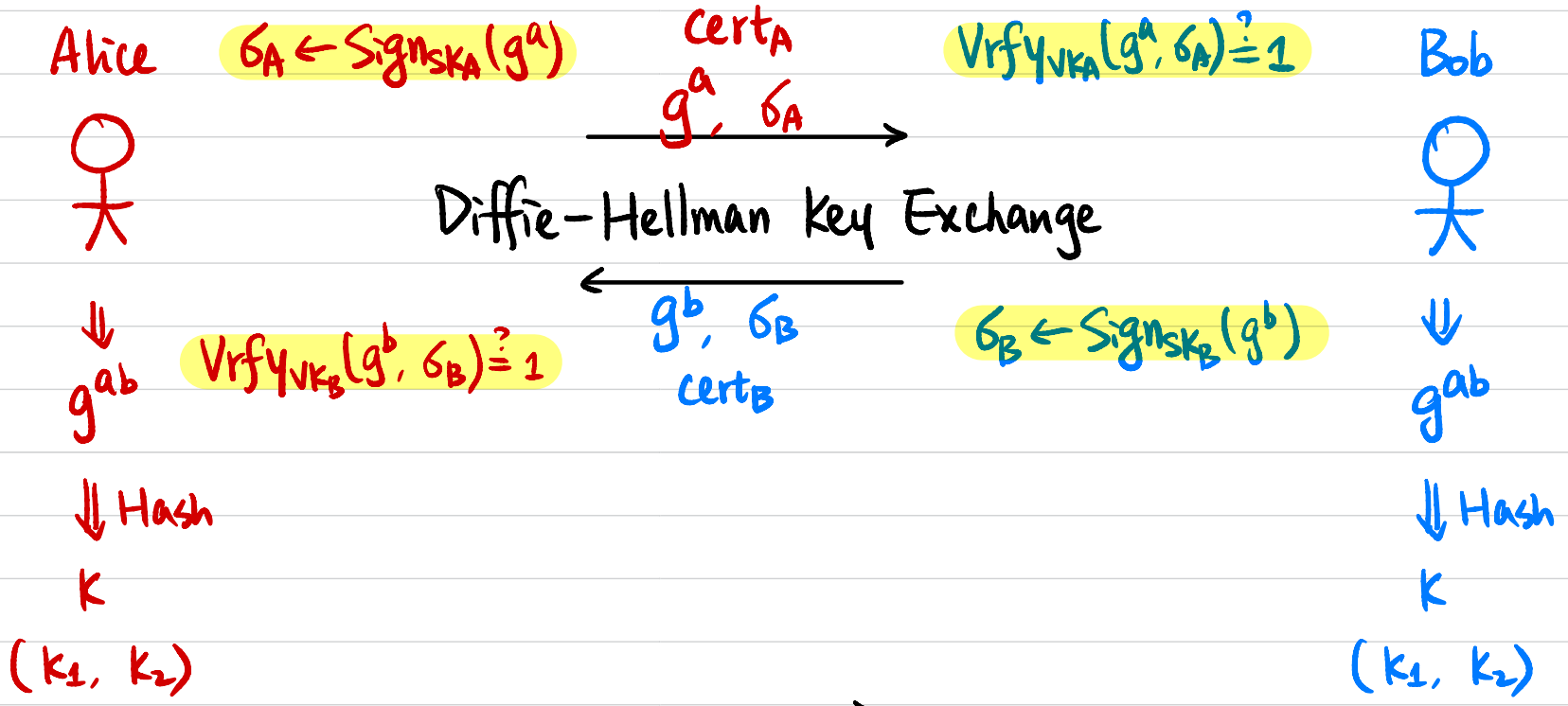
One-Sided Secure Authentication



Two-Sided Authenticated Key Exchange

$(VK_A, SK_A) \leftarrow Gen(1^\lambda)$; $cert_A$

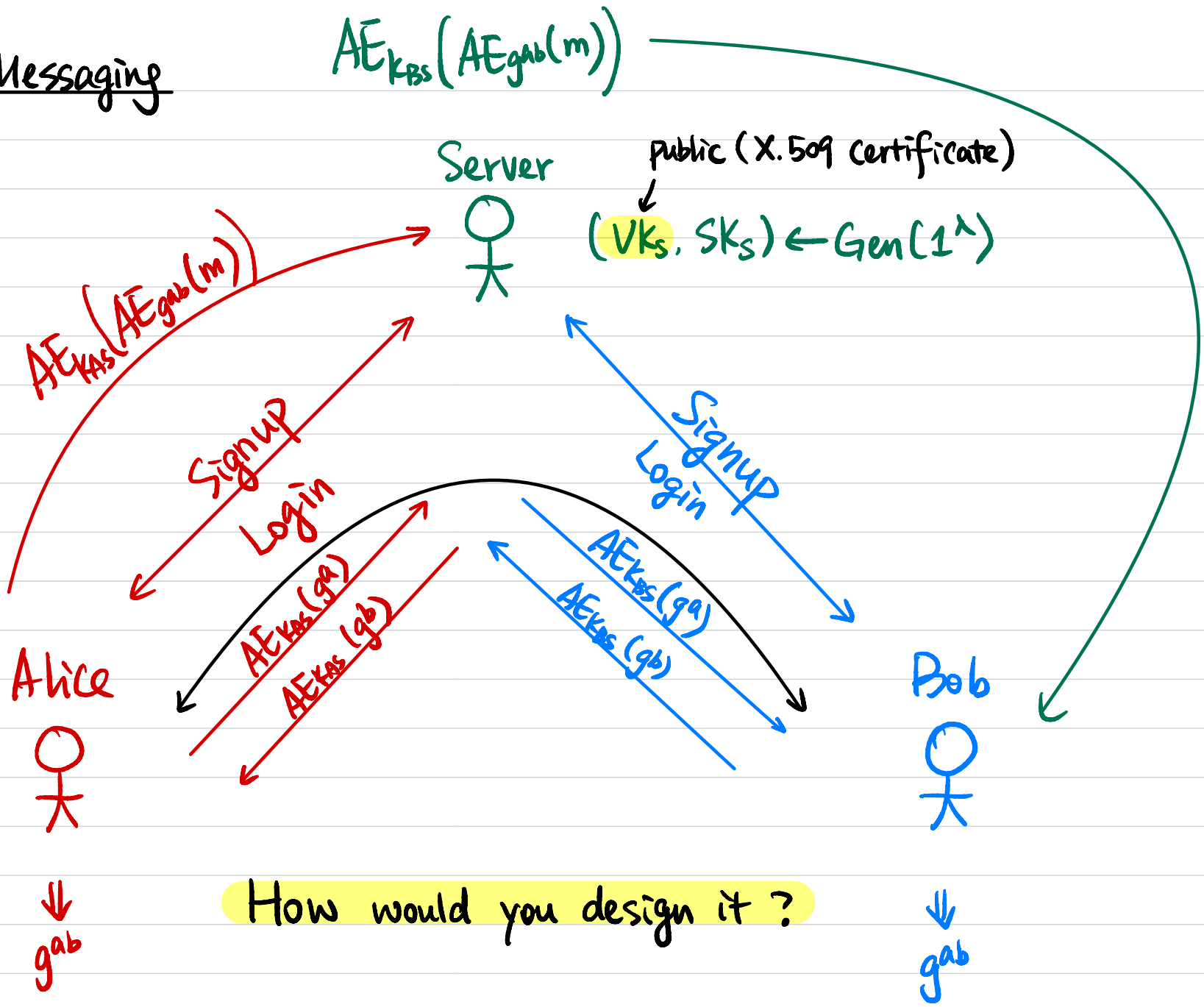
$(VK_B, SK_B) \leftarrow Gen(1^\lambda)$; $cert_B$



Authenticated Encryption

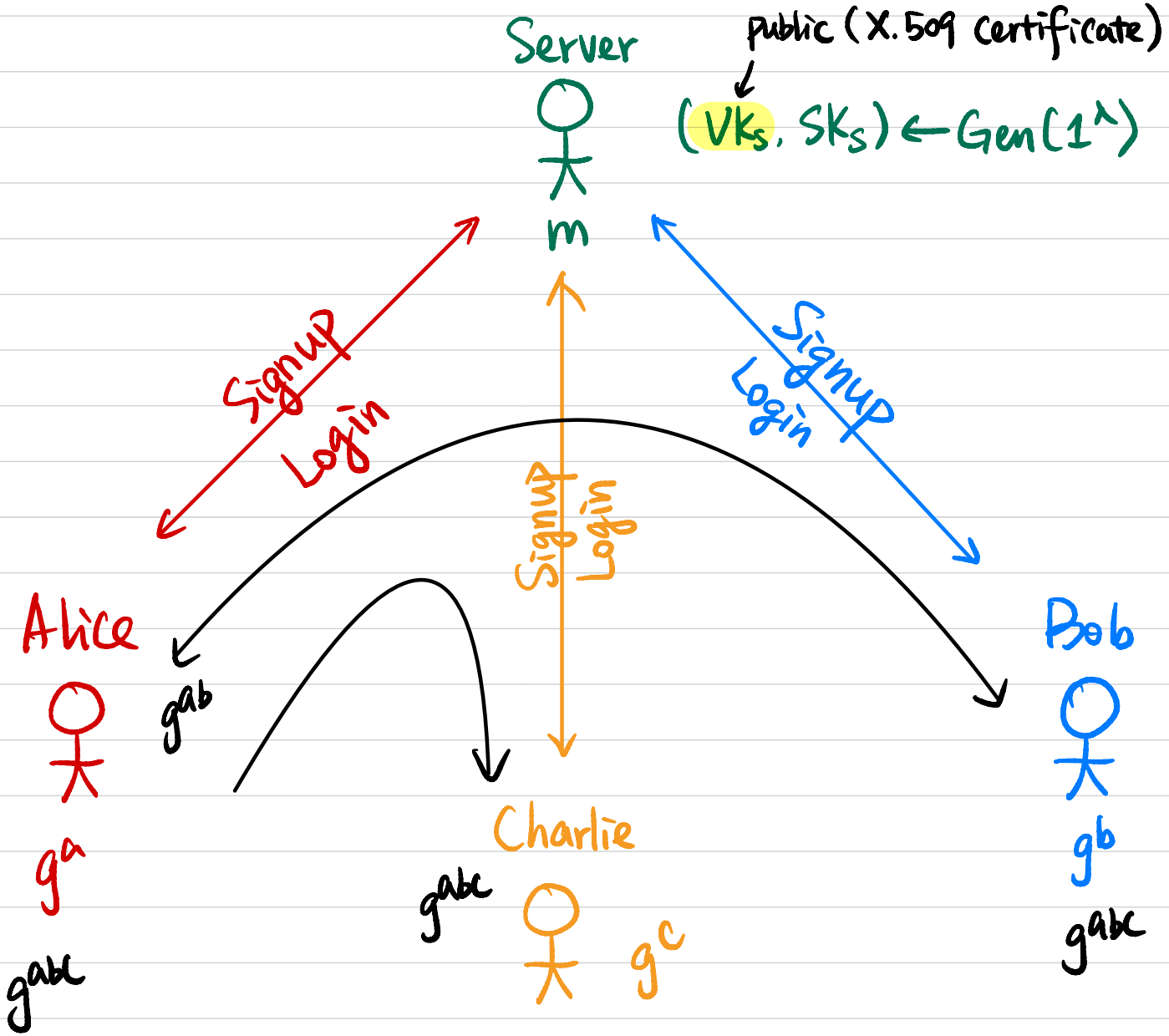
(Encrypt-then-MAC)

Secure Messaging



How would you design it ?

Group Chat ?



How would you design it ?