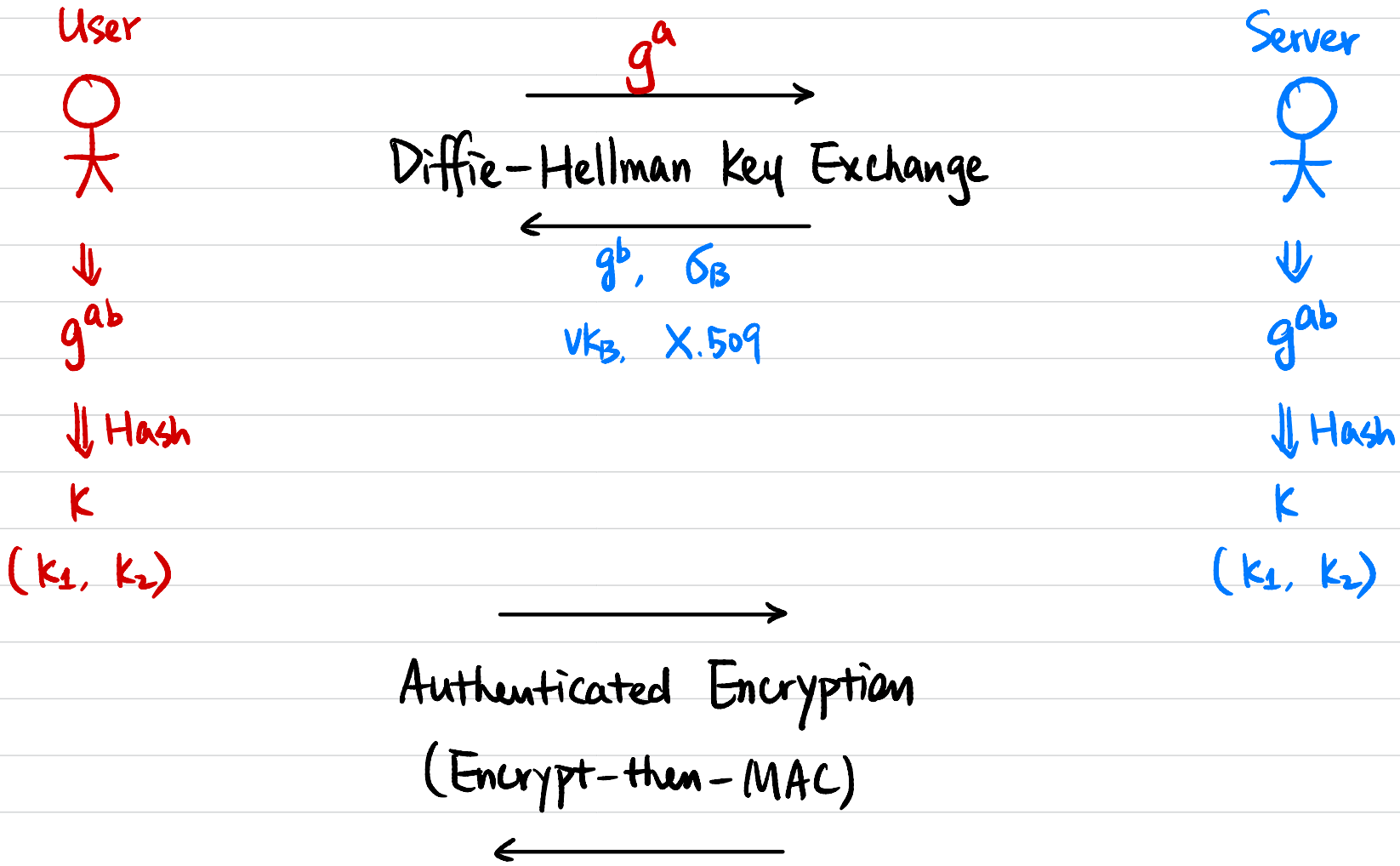
CSCI 1515 Applied Cryptography

This Lecture:

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

One-Sided Secure Authentication

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



Certificate Chain

Root CA — $(VK, SK) \leftarrow Gen(1^\lambda)$ (public: VK)

$\downarrow$ cert1: $\sigma \leftarrow Sign_{SK}(VK_1)$

Intermediate CA1 — $(VK_1, SK_1) \leftarrow Gen(1^\lambda)$

$\downarrow$ $cert_2 = \begin{pmatrix} VK_1, & \sigma \leftarrow Sign_{SK}(VK_1) \\ VK_2, & \sigma_1 \leftarrow Sign_{SK_1}(VK_2) \end{pmatrix}$

Intermediate CA2 — $(VK_2, SK_2) \leftarrow Gen(1^\lambda)$

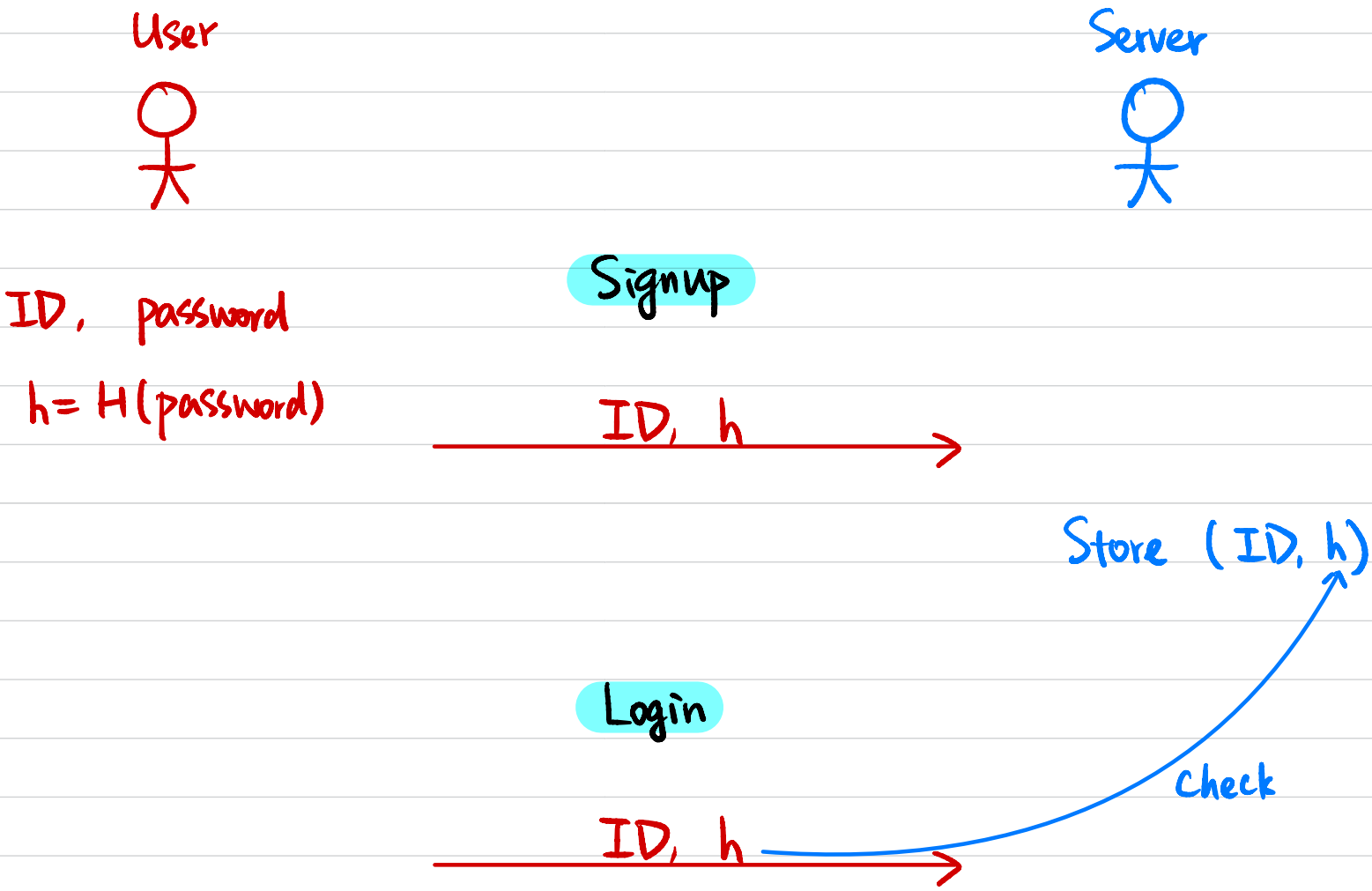
$\downarrow$ $cert_{Bob} = \begin{pmatrix} VK_1, & \sigma \leftarrow Sign_{SK}(VK_1) \\ VK_2, & \sigma_1 \leftarrow Sign_{SK_1}(VK_2) \\ VK_B, & \sigma_2 \leftarrow Sign_{SK_2}(VK_B) \end{pmatrix}$

Bob

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

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

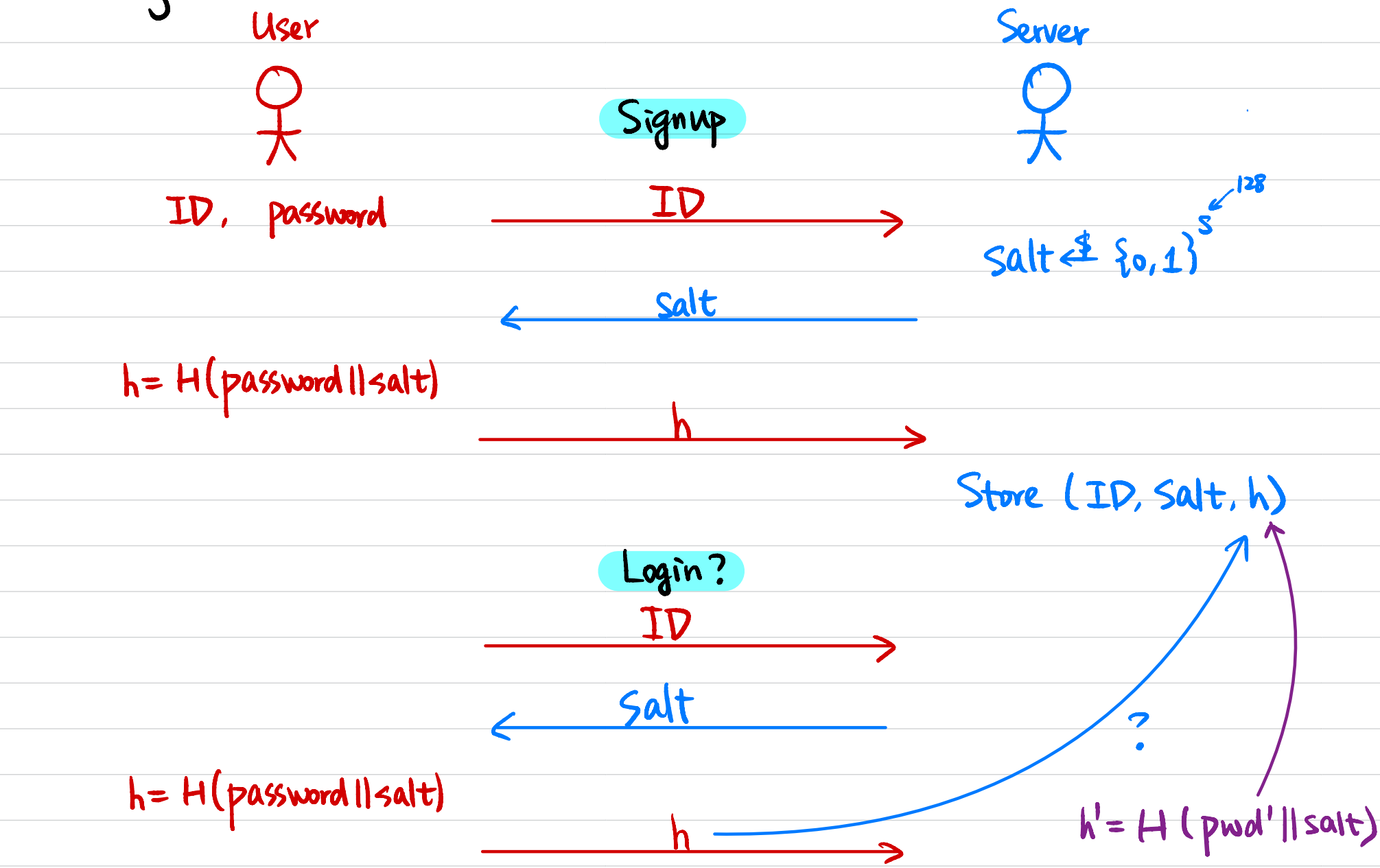
ID, h

Store (ID, h)

h' = H(pwd')

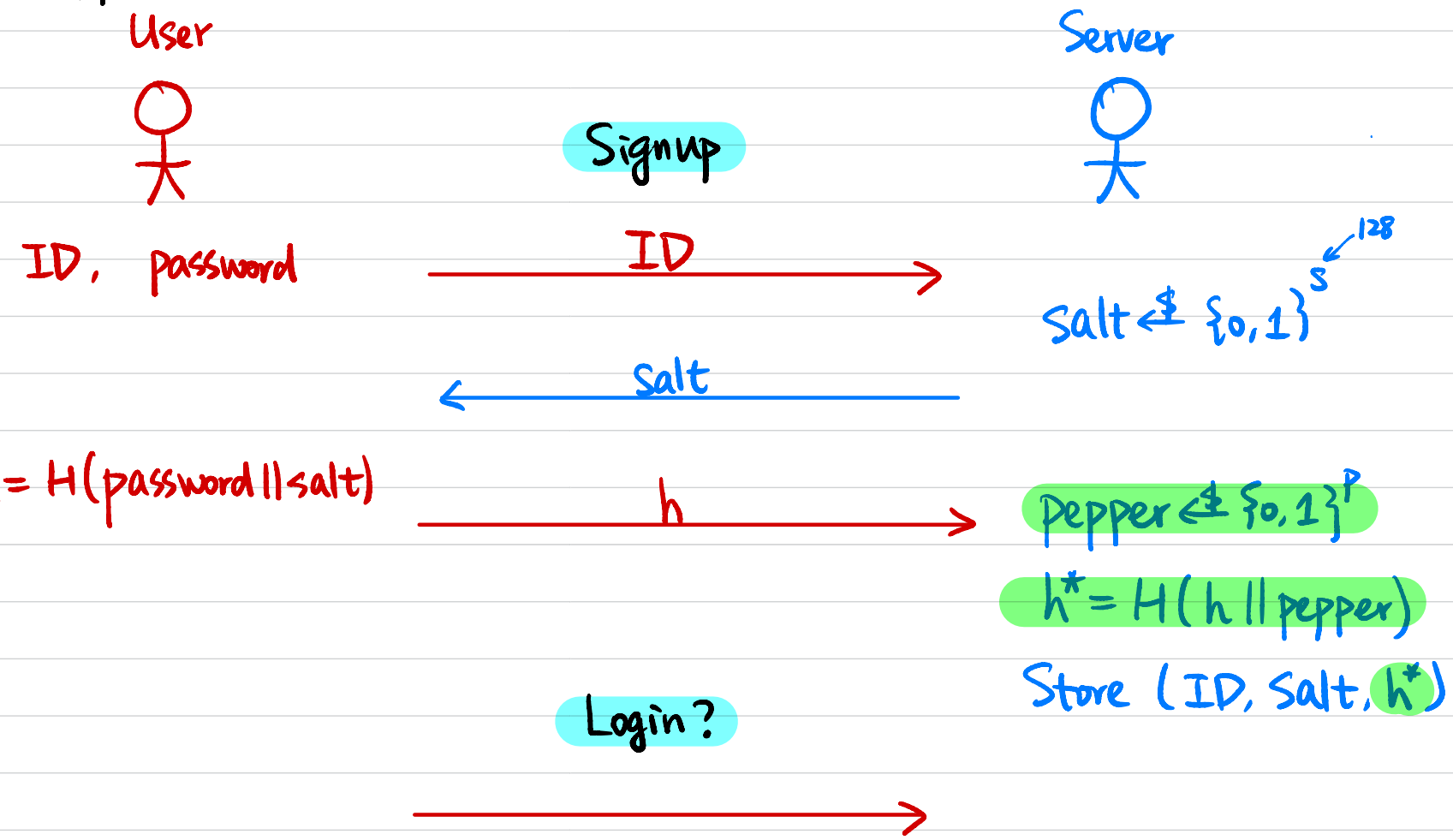
(preprocessing)

Salting



Why does it help?

Salt & Pepper



Why does it help?

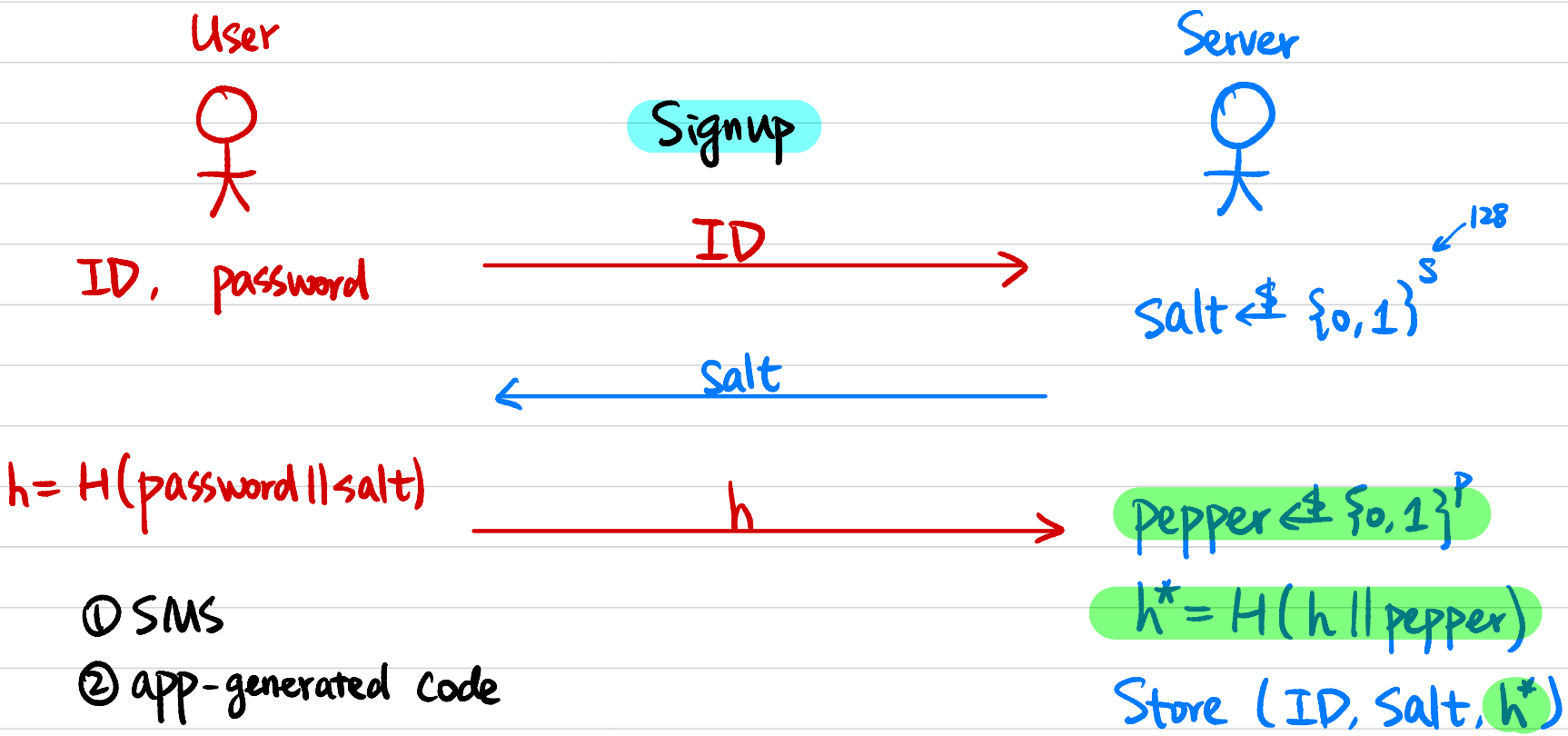
Slow Hash Functions

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

Application-Specific Integrated Circuit (ASIC) → blockchain mining

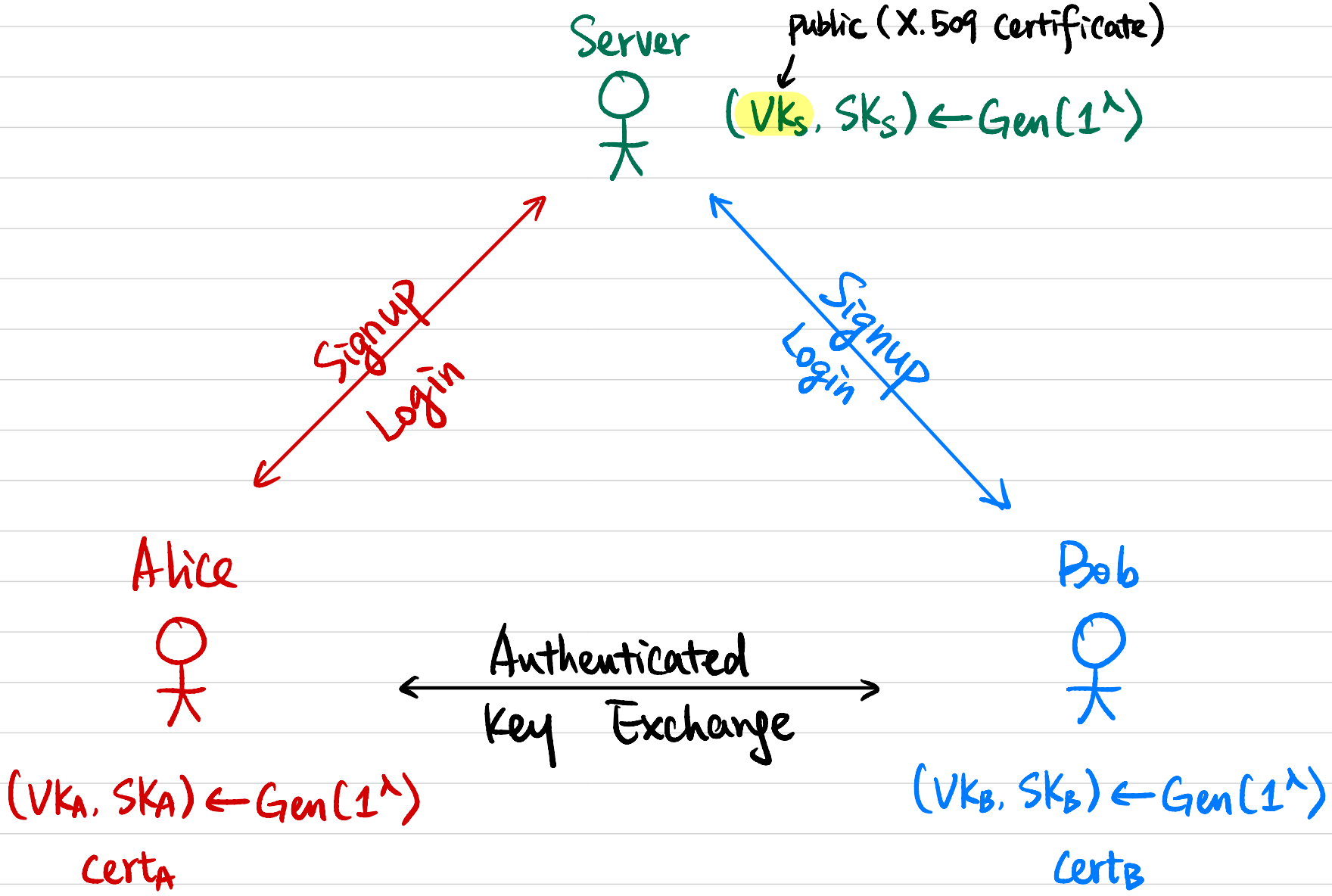
- Memory-hard hash functions
  - ↳ Scrypt

Two-Factor Authentication (2FA)

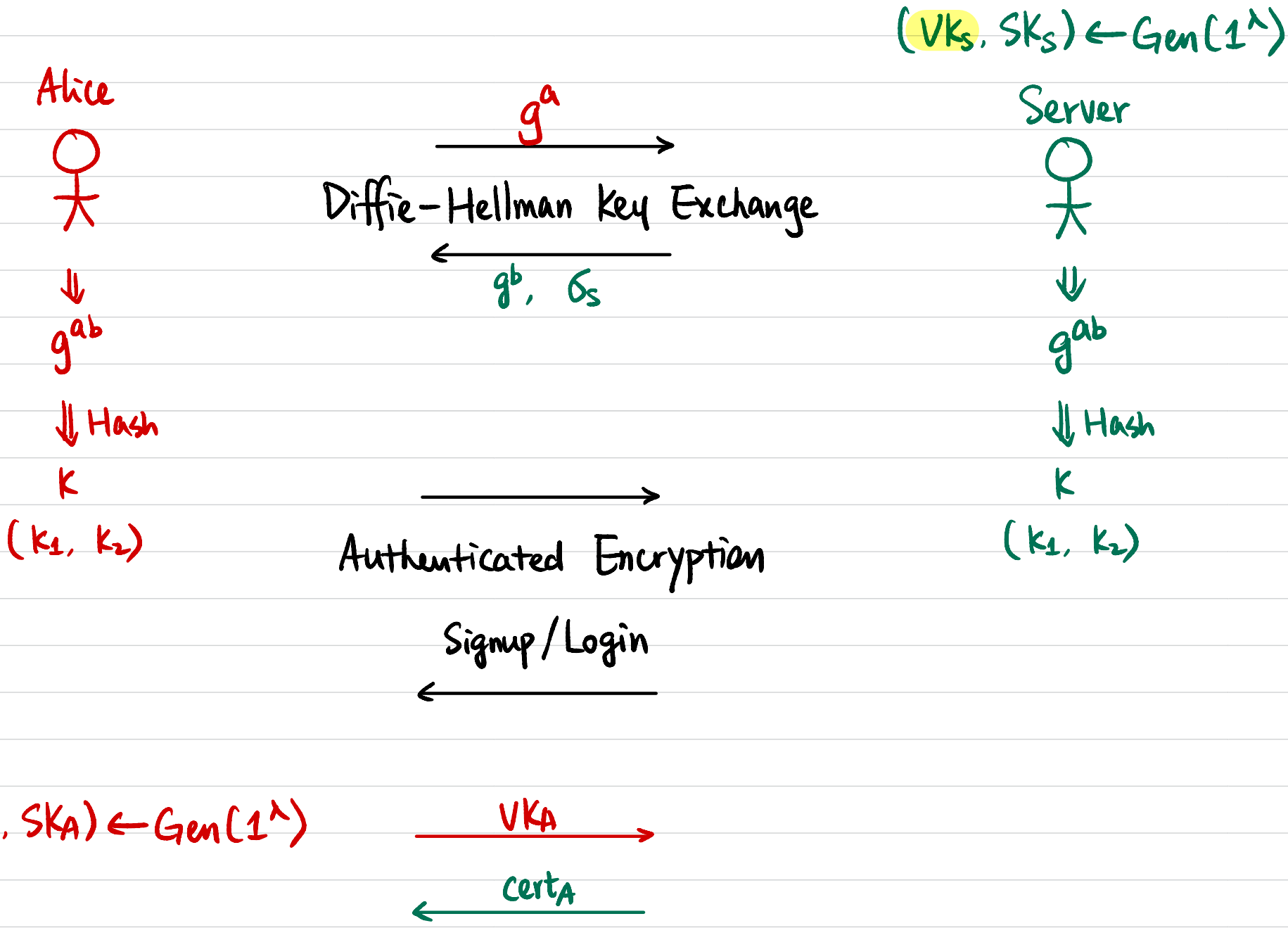


How would you design it ?

Putting it Together: Secure Authentication



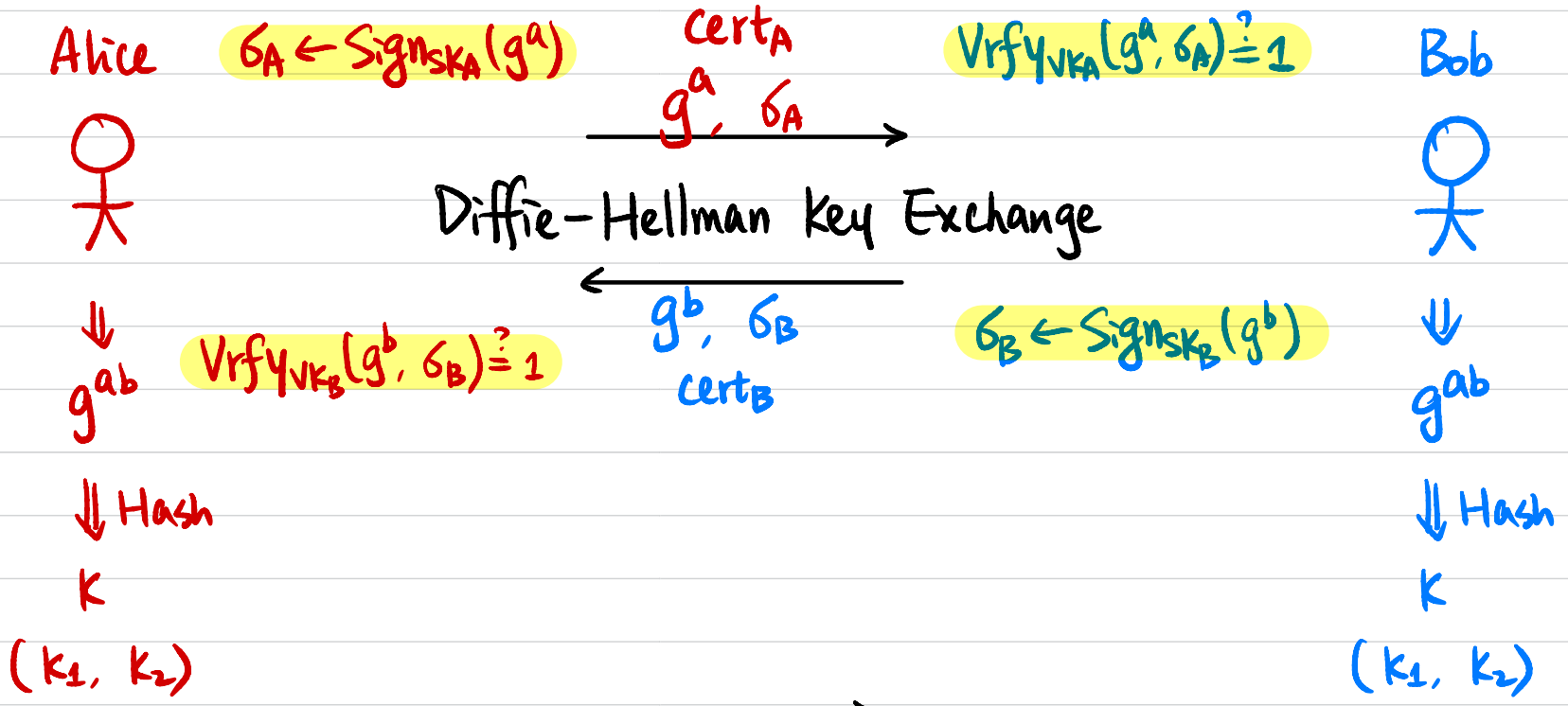
One-Sided Secure Authentication



Two-Sided Authenticated Key Exchange

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

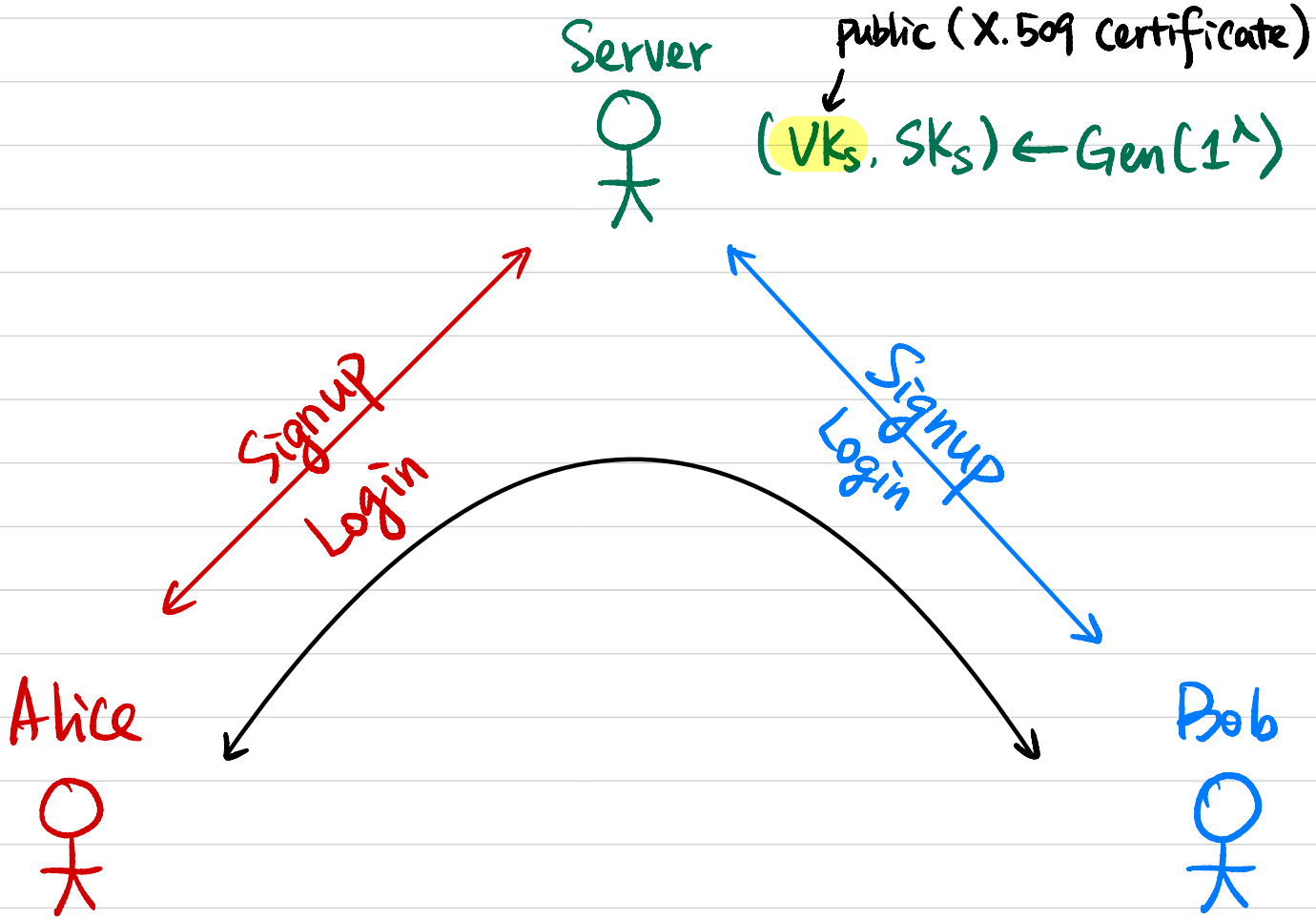
$(VK_B, SK_B) \leftarrow Gen(1^\lambda)$; $cert_B$



Authenticated Encryption

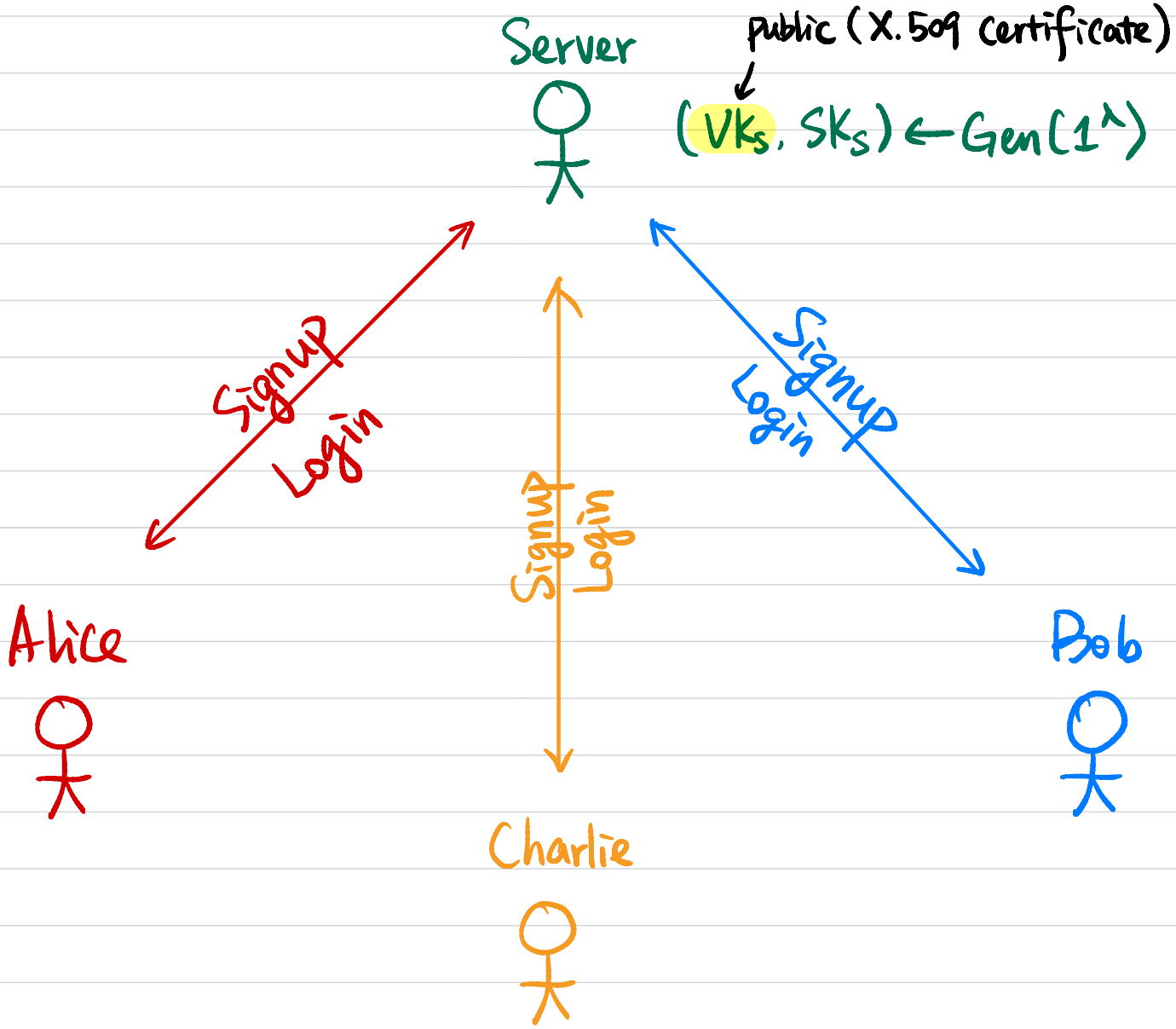
(Encrypt-then-MAC)

Secure Messaging



How would you design it ?

Group Chat ?



How would you design it ?

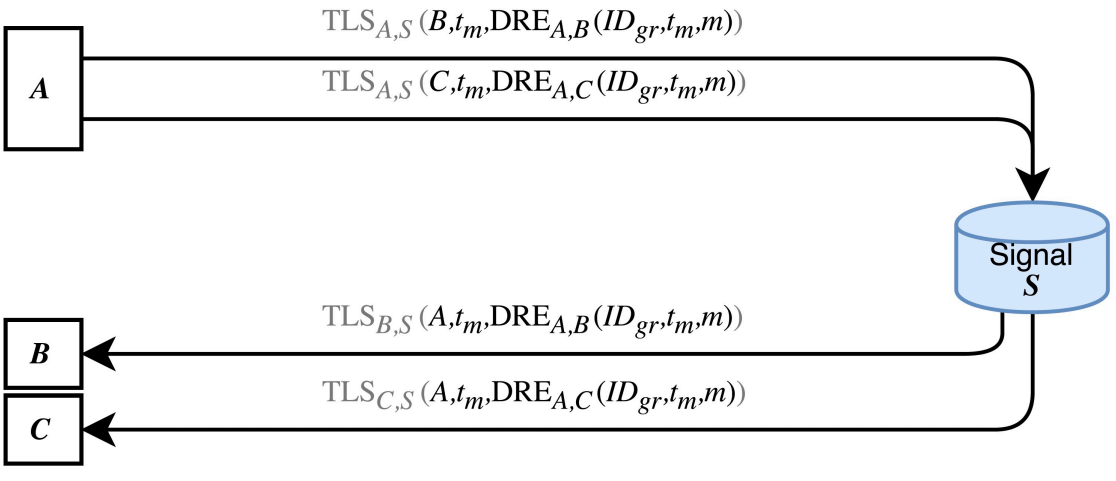


Figure 3. Schematic depiction of Signal's traffic, generated for a message m from sender A to receivers B and C in group gr with $\mathcal{G}_{gr} = \{A, B, C\}$. Transport layer protection is not in the analysis scope (gray).

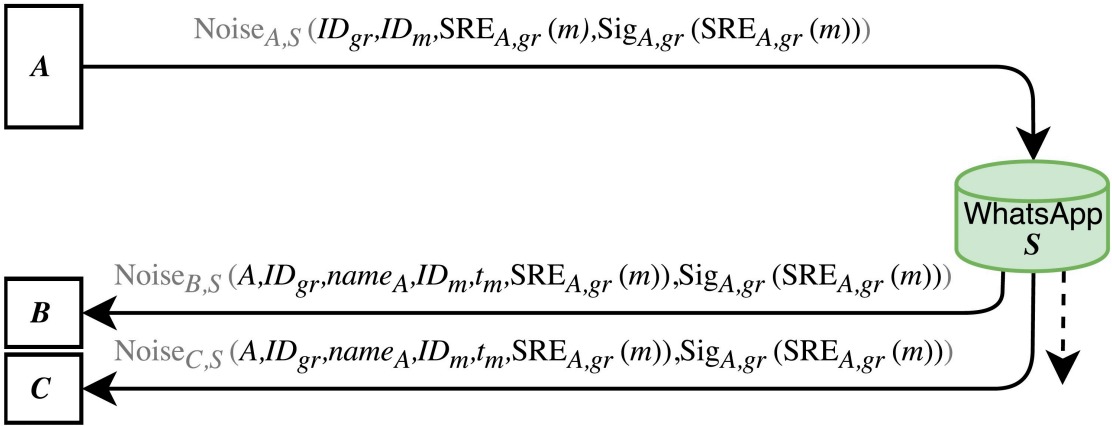
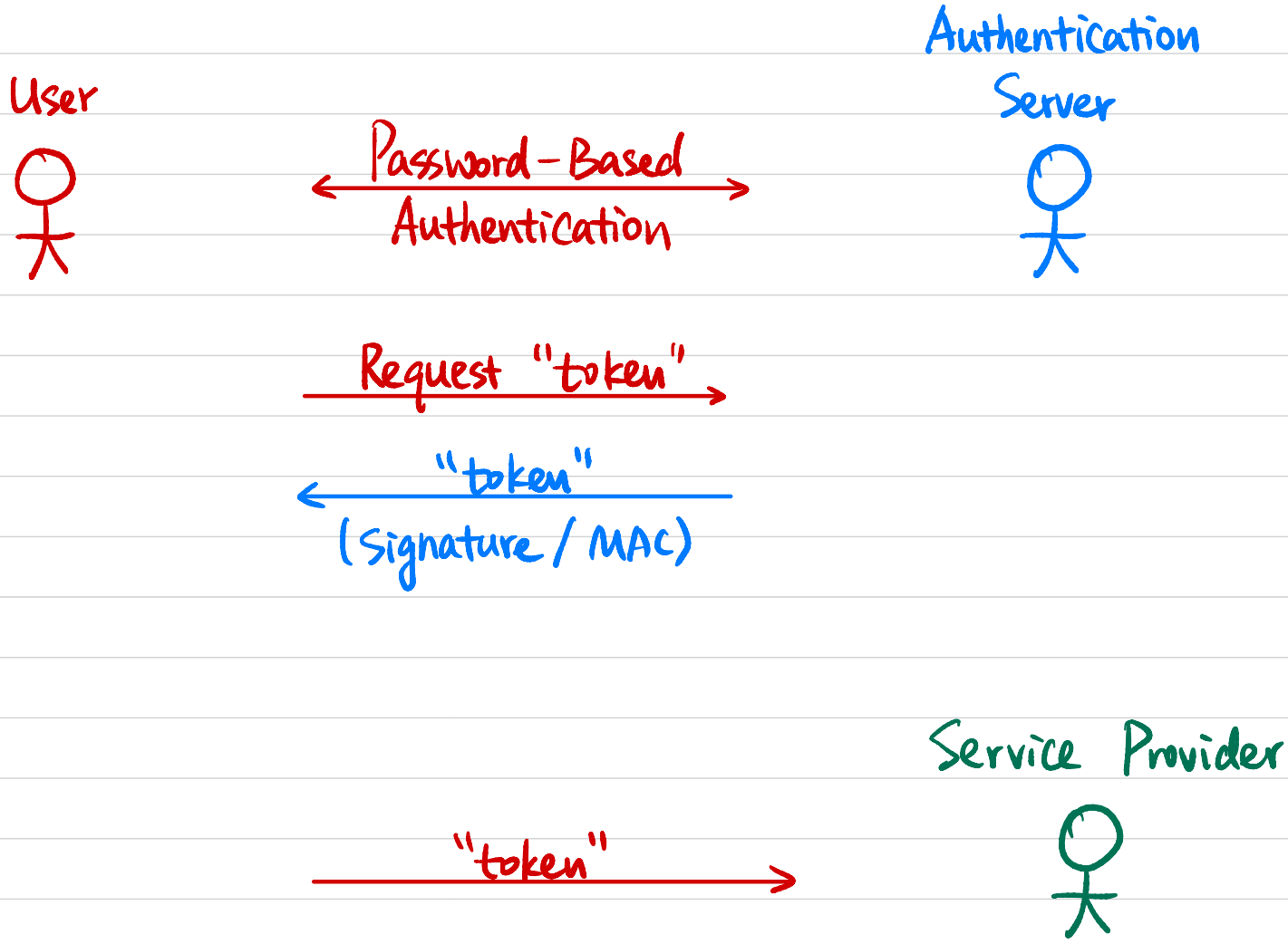


Figure 5. Schematic depiction of traffic, generated for a message m from sender A to receivers B, C in group gr with $\mathcal{G}_{gr} = \{A, B, C\}$ in WhatsApp.

Single Sign-On (SSO) Authentication



- OAuth / OpenID: Sign-in with Google / Apple / ···
- Kerberos: enterprises