Cryptography Engineering

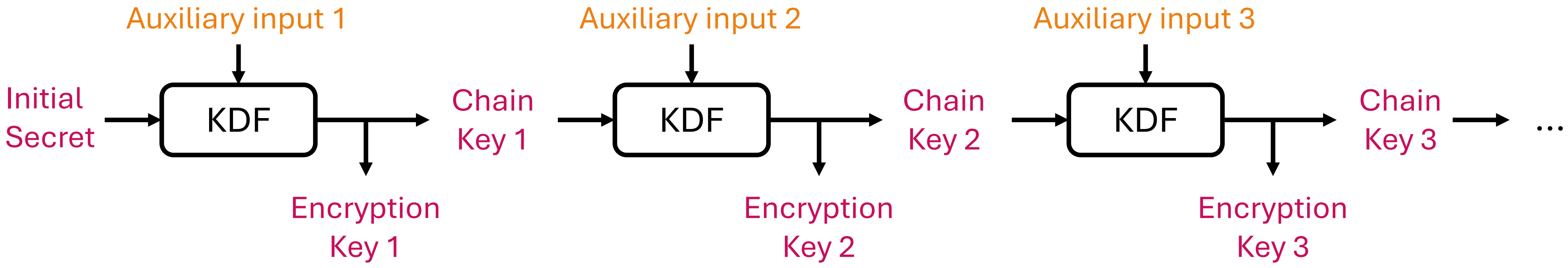
- Lecture 5 (Nov 18, 2024)

- Today's notes:
  - Key Ratcheting (Continue)
  - Forward/Backward Secrecy
  - Diffie-Hellman Ratcheting

- No homework

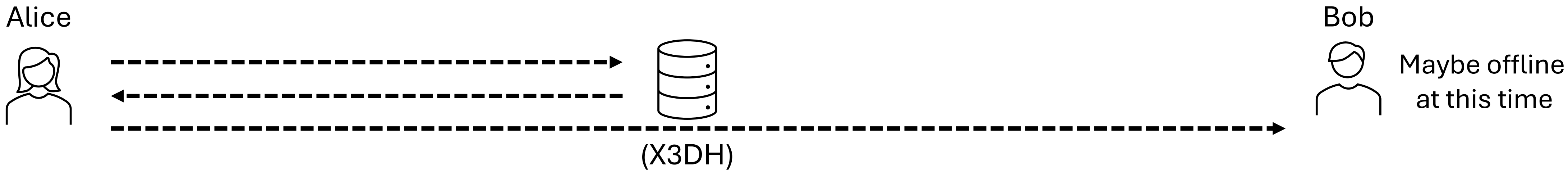
Symmetric-key Ratcheting

- KDF chain
  - KDF: Key derivation function



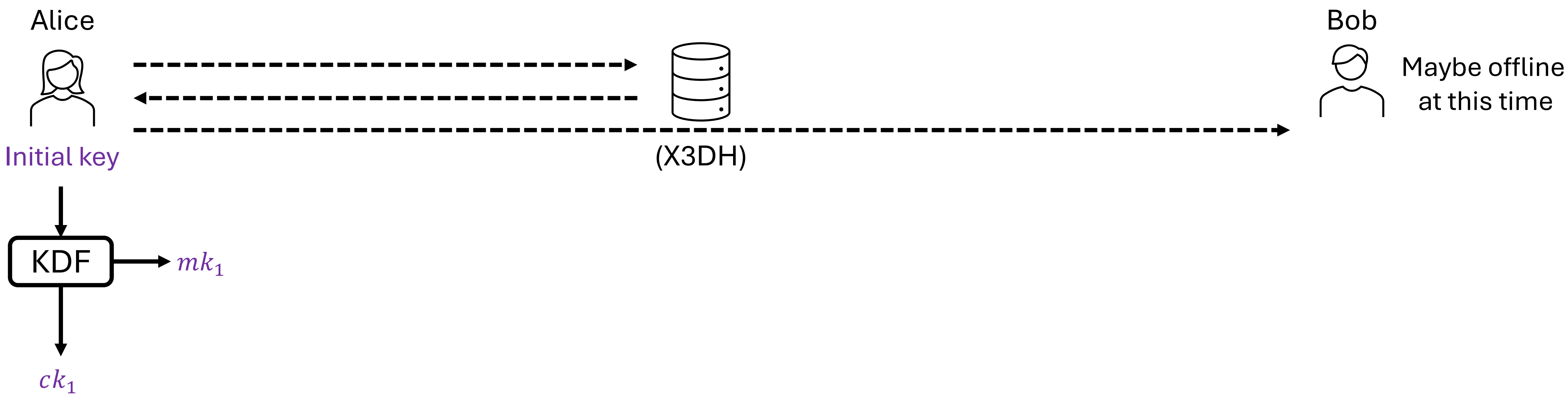
Symmetric-key Ratcheting

- A toy example of instant messaging using symmetric-key ratcheting



Symmetric-key Ratcheting

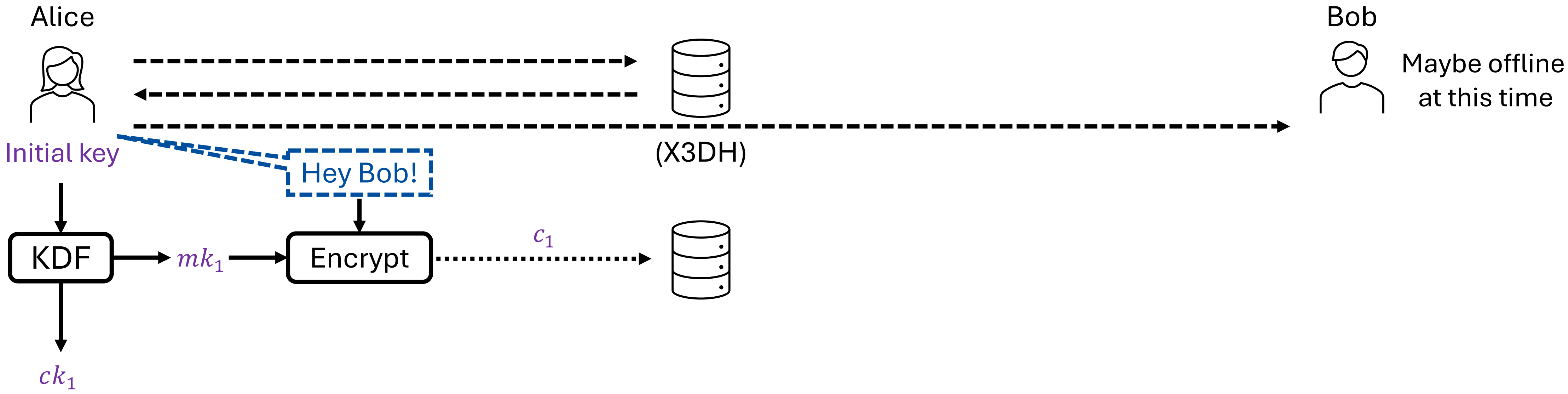
- A toy example of instant messaging using symmetric-key ratcheting



*We ignore the auxiliary input to KDF

Symmetric-key Ratcheting

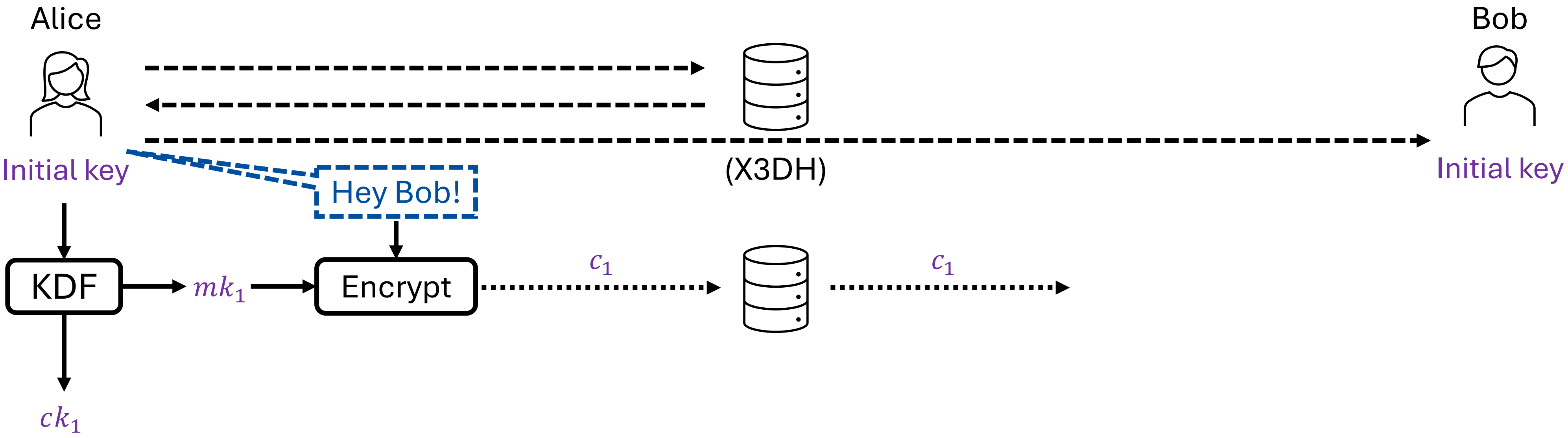
- A toy example of instant messaging using symmetric-key ratcheting



*We ignore the auxiliary input to KDF

Symmetric-key Ratcheting

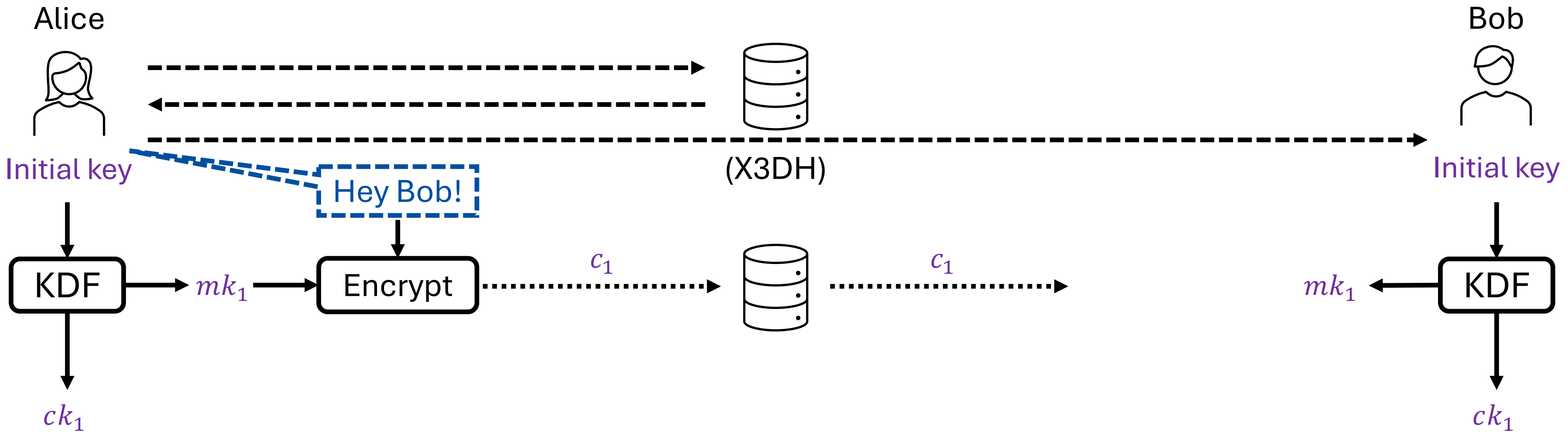
- A toy example of instant messaging using symmetric-key ratcheting



*We ignore the auxiliary input to KDF

Symmetric-key Ratcheting

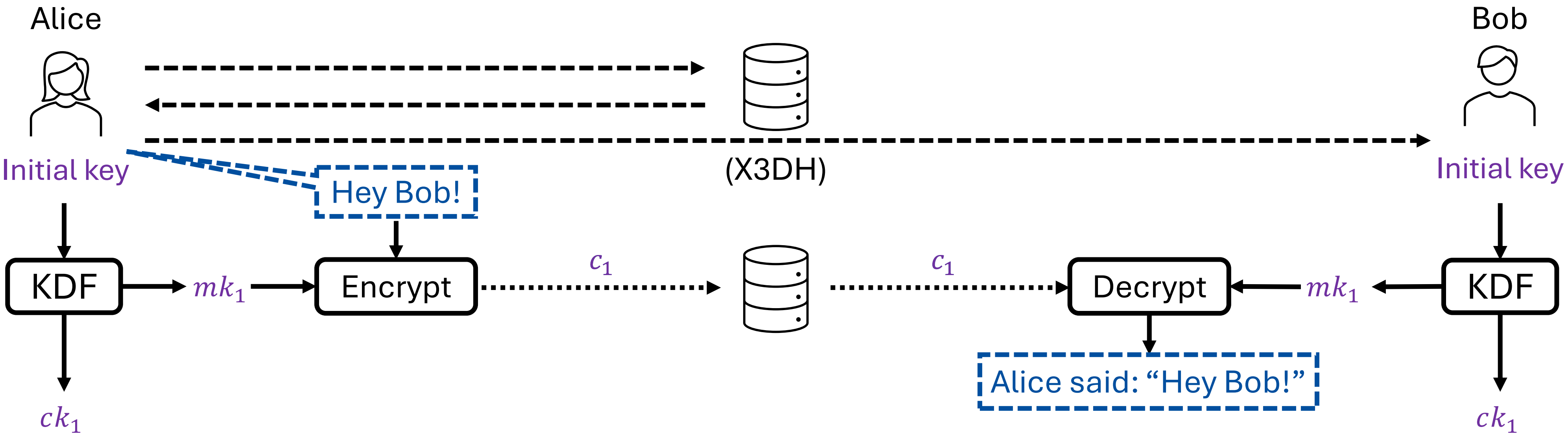
- A toy example of instant messaging using symmetric-key ratcheting



*We ignore the auxiliary input to KDF

Symmetric-key Ratcheting

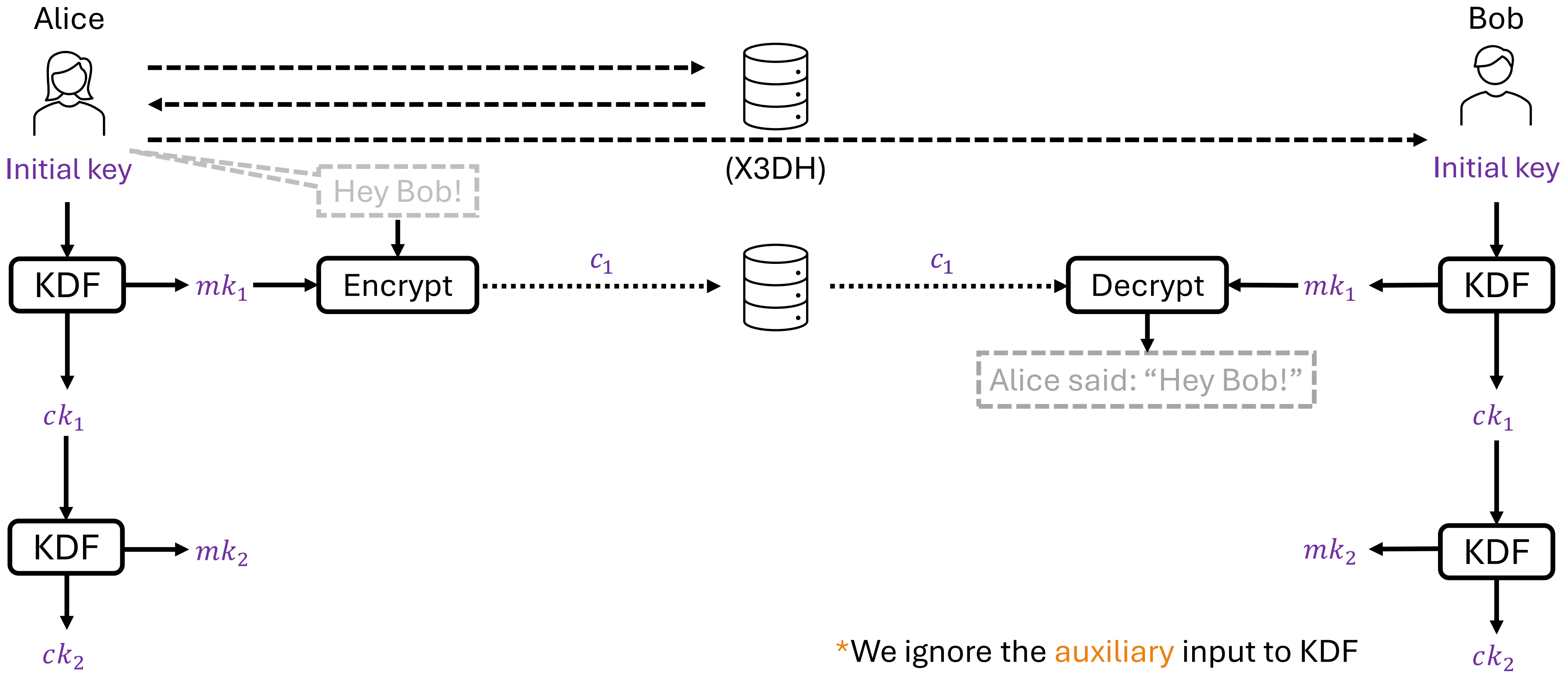
- A toy example of instant messaging using symmetric-key ratcheting



*We ignore the auxiliary input to KDF

Symmetric-key Ratcheting

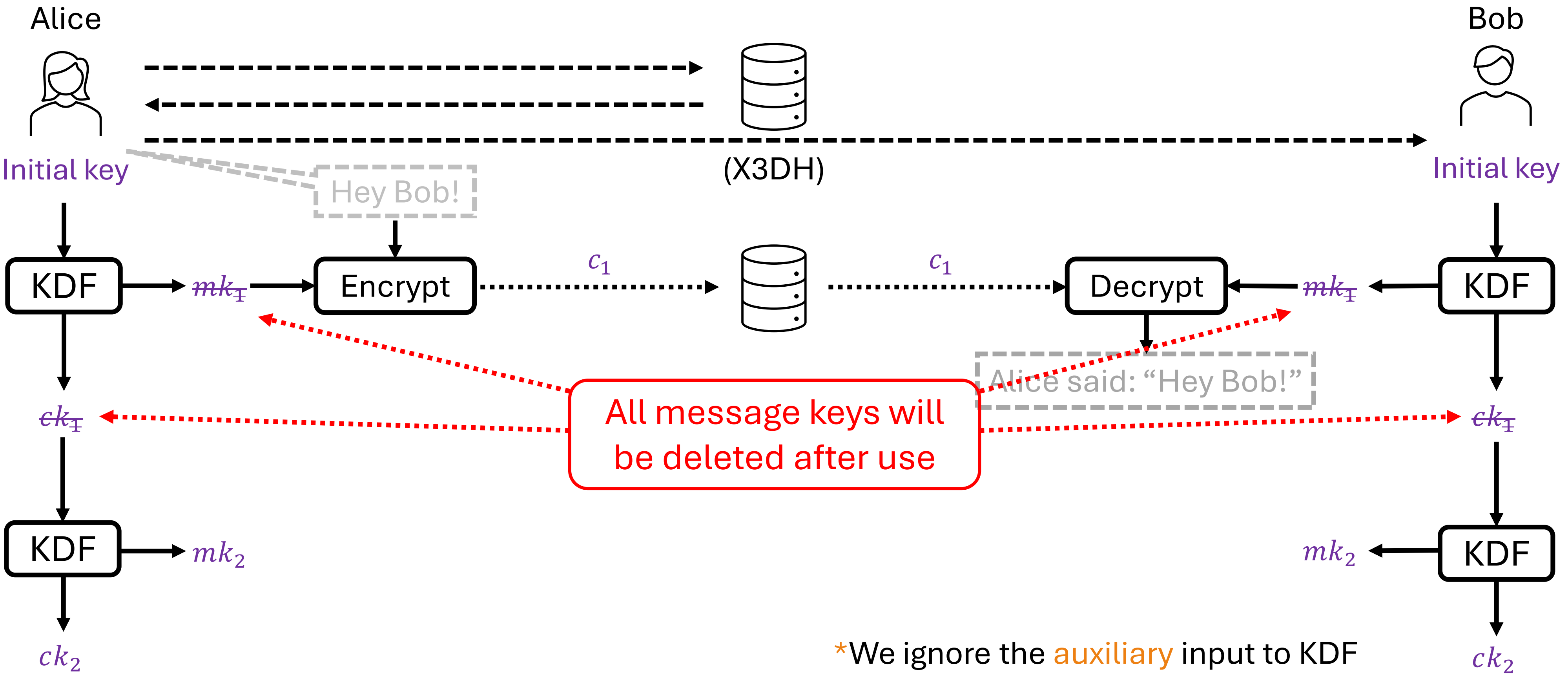
- A toy example of instant messaging using symmetric-key ratcheting



*We ignore the auxiliary input to KDF

Symmetric-key Ratcheting

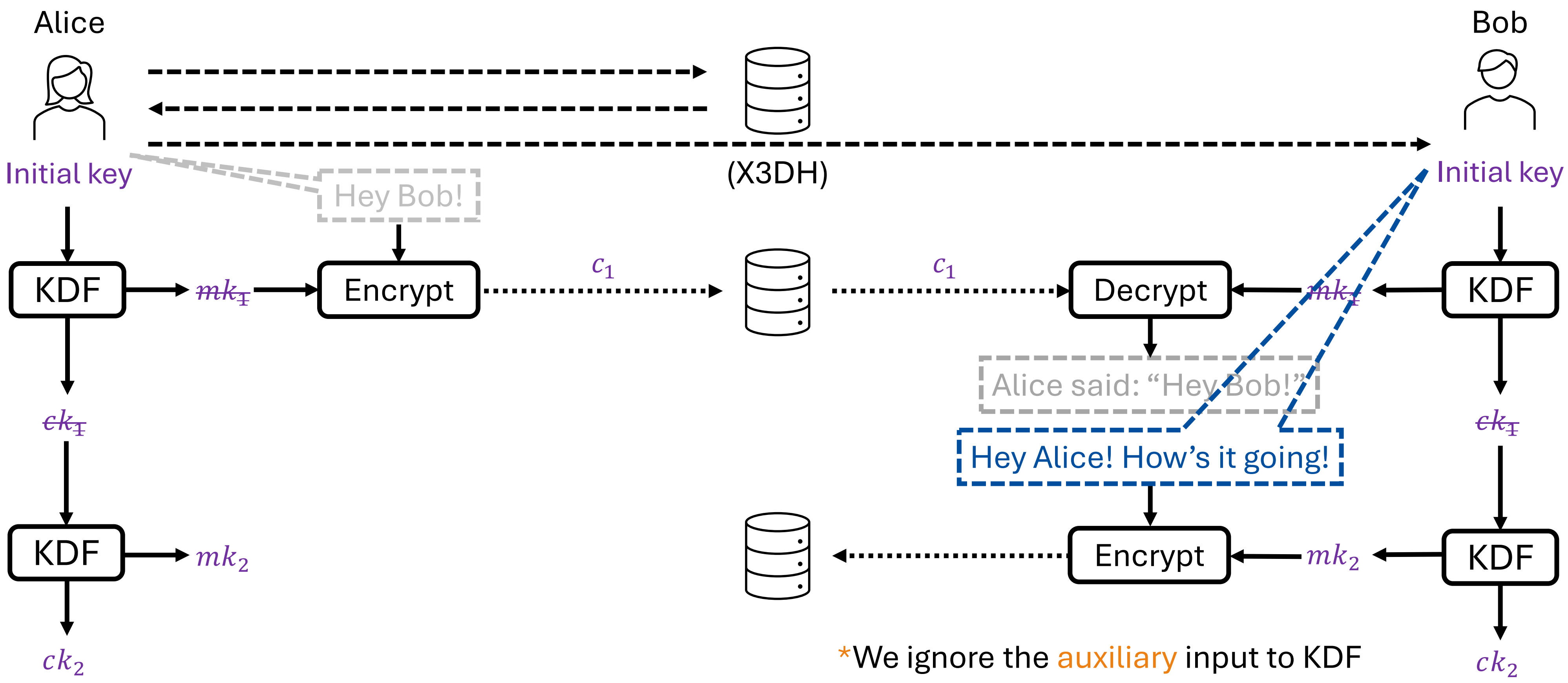
- A toy example of instant messaging using symmetric-key ratcheting



*We ignore the auxiliary input to KDF

Symmetric-key Ratcheting

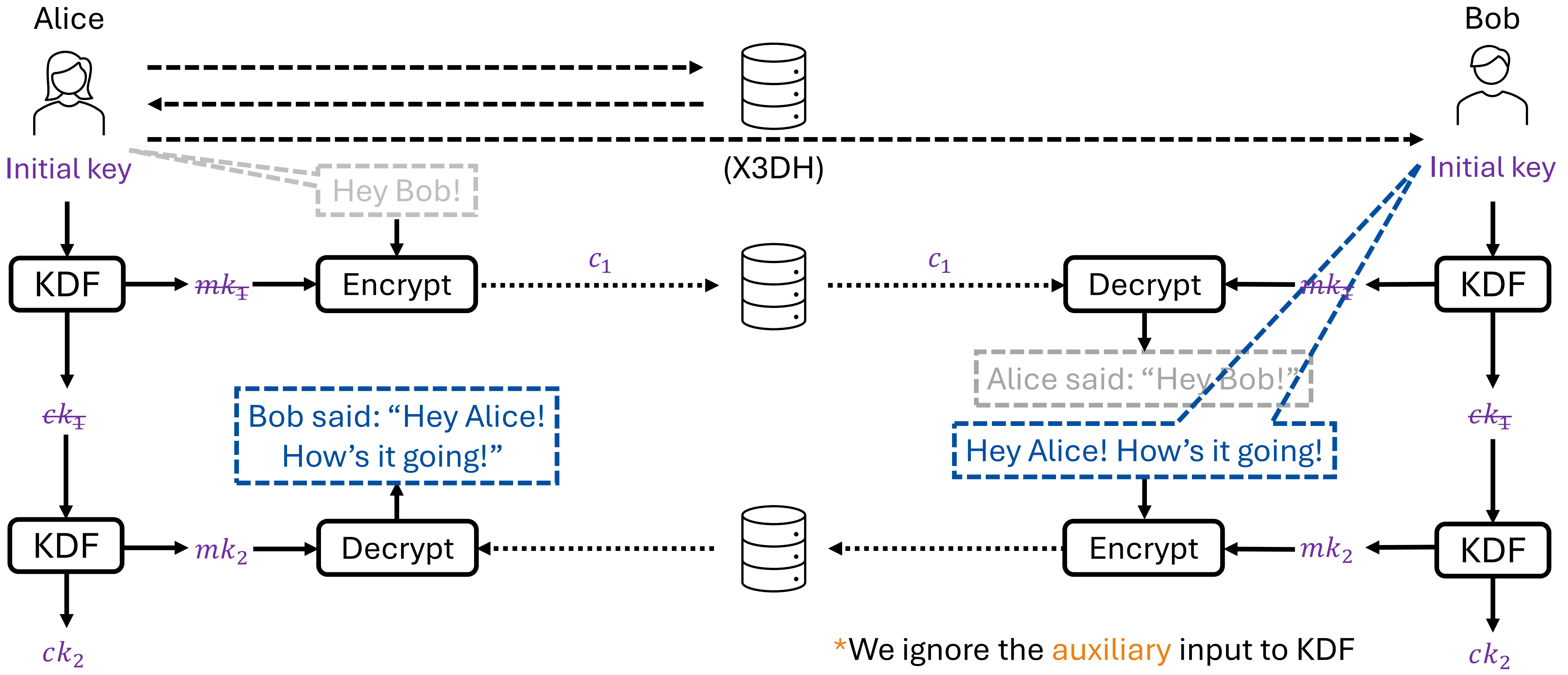
- A toy example of instant messaging using symmetric-key ratcheting



*We ignore the auxiliary input to KDF

Symmetric-key Ratcheting

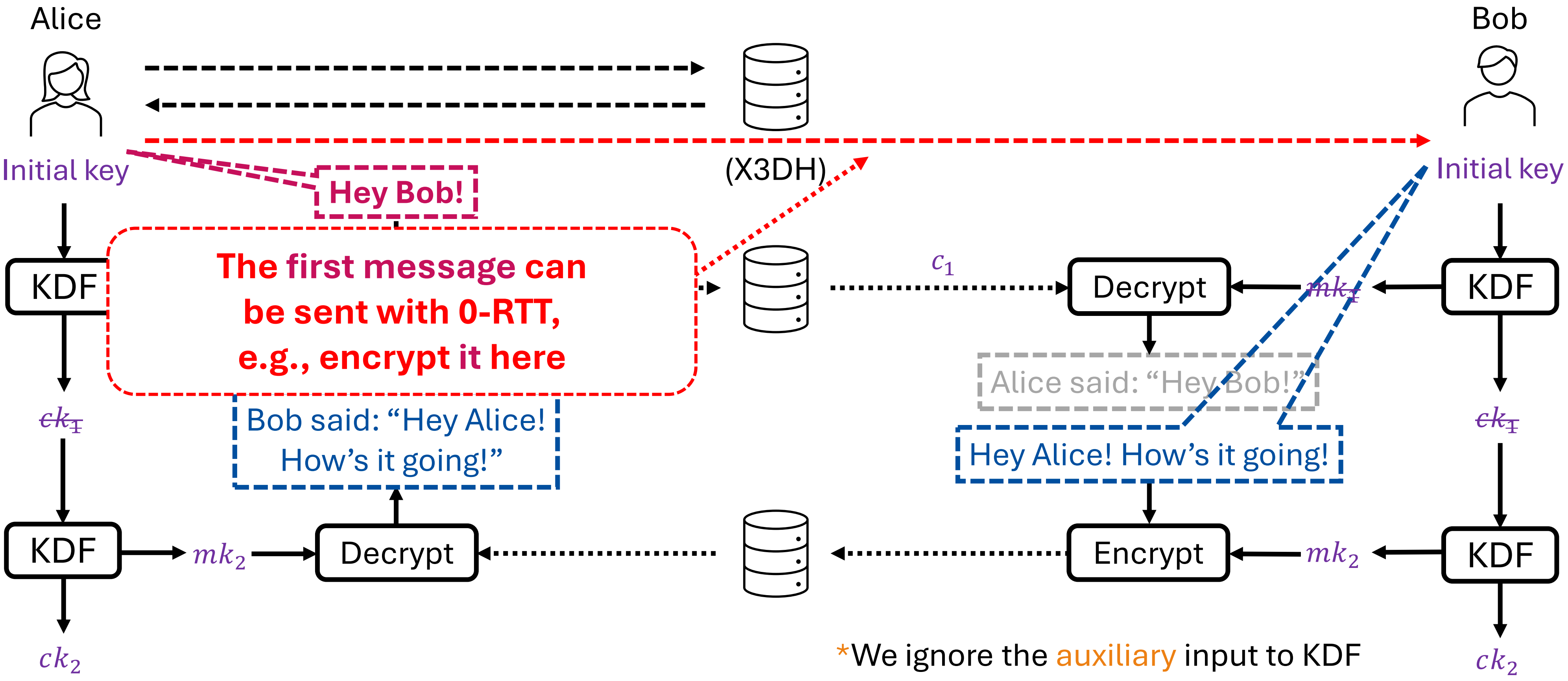
- A toy example of instant messaging using symmetric-key ratcheting



*We ignore the auxiliary input to KDF

Symmetric-key Ratcheting

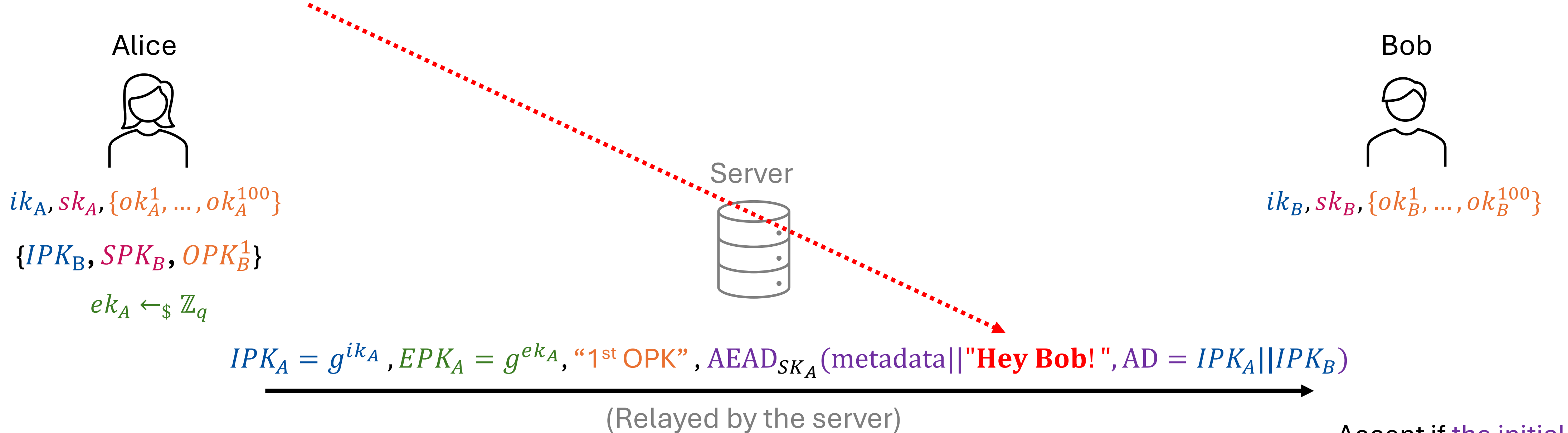
- A toy example of instant messaging using symmetric-key ratcheting



*We ignore the auxiliary input to KDF

Symmetric-key Ratcheting

- Make the first message 0-RTT (Zero Round Time Trip)...



Alice

$ik_A, sk_A, \{ok_A^1, \dots, ok_A^{100}\}$

$\{IPK_B, SPK_B, OPK_B^1\}$

$ek_A \leftarrow_{\$} \mathbb{Z}_q$

Server

Bob

$ik_B, sk_B, \{ok_B^1, \dots, ok_B^{100}\}$

$IPK_A = g^{ik_A}, EPK_A = g^{ek_A}$, "1st OPK", $\mathrm{AEAD}_{SK_A}(\mathrm{metadata}||\text{"Hey Bob! "}, \mathrm{AD} = IPK_A||IPK_B)$

(Relayed by the server)

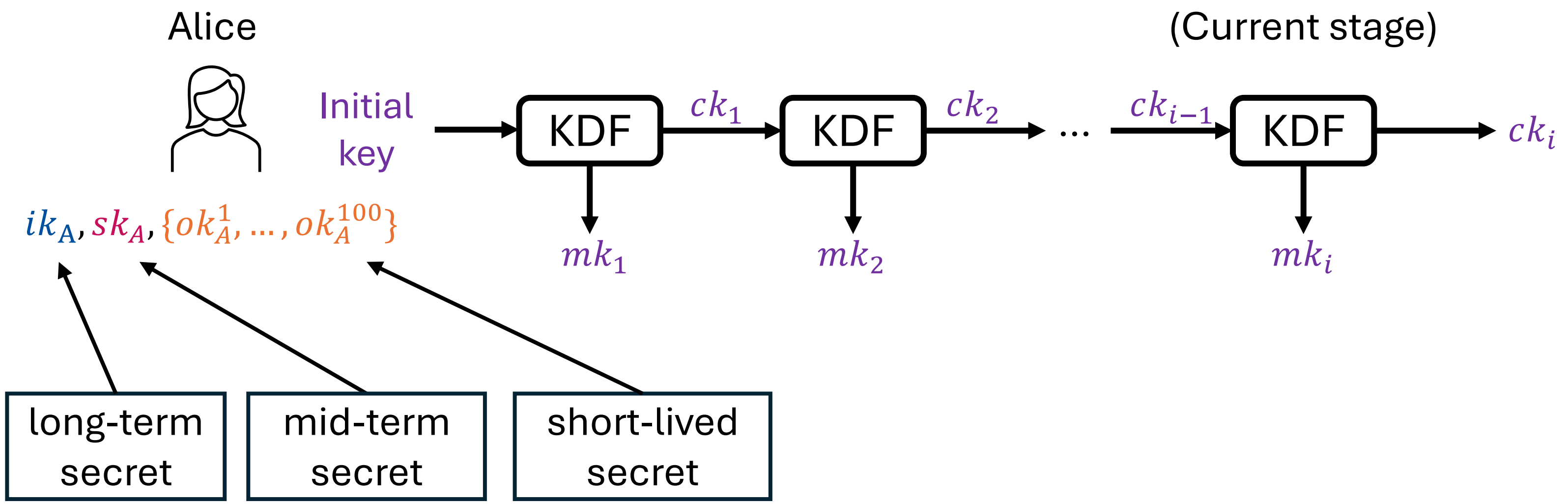
Accept if the initial ciphertext can be decrypted

SK_A = X3DH_Key_Alice($ik_A, ek_A, IPK_B, SPK_B, OPK_B^1$)

SK_B = X3DH_Key_Bob($IPK_A, EPK_A, ik_B, sk_B, ok_B^1$)

Forward Secrecy

- Long-term secret keys are compromised, but past communication remains secure...



Alice

(Current stage)

Initial key

KDF

ck_1

KDF

ck_2

…

ck_{i-1}

KDF

ck_i

mk_1

mk_2

mk_i

$ik_{\mathrm{A}}, sk_A, \{ok_A^1, \dots, ok_A^{100}\}$

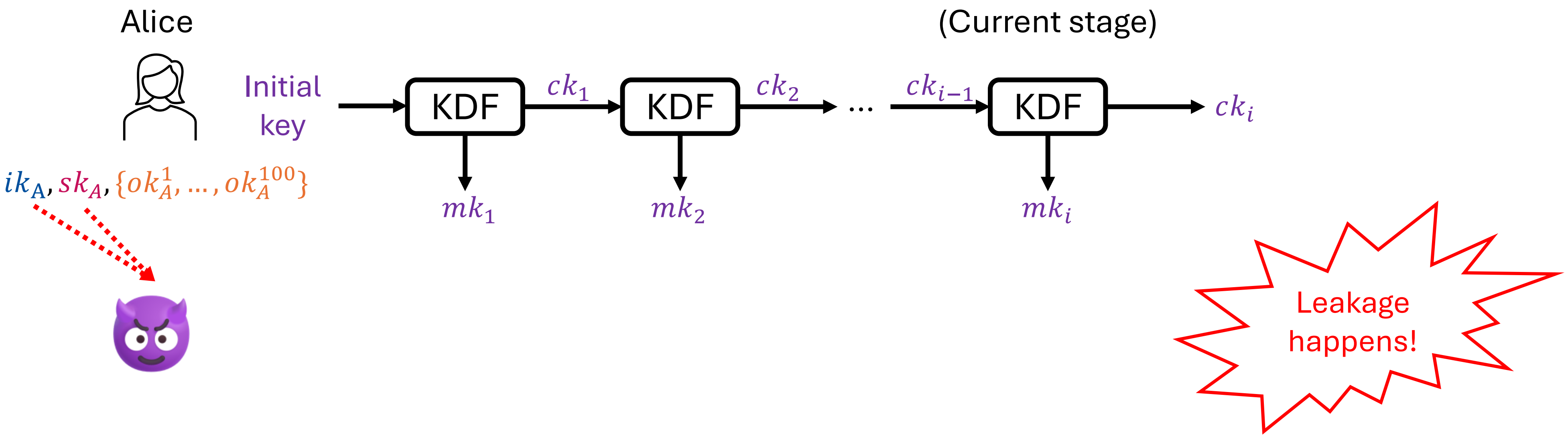
long-term secret

mid-term secret

short-lived secret

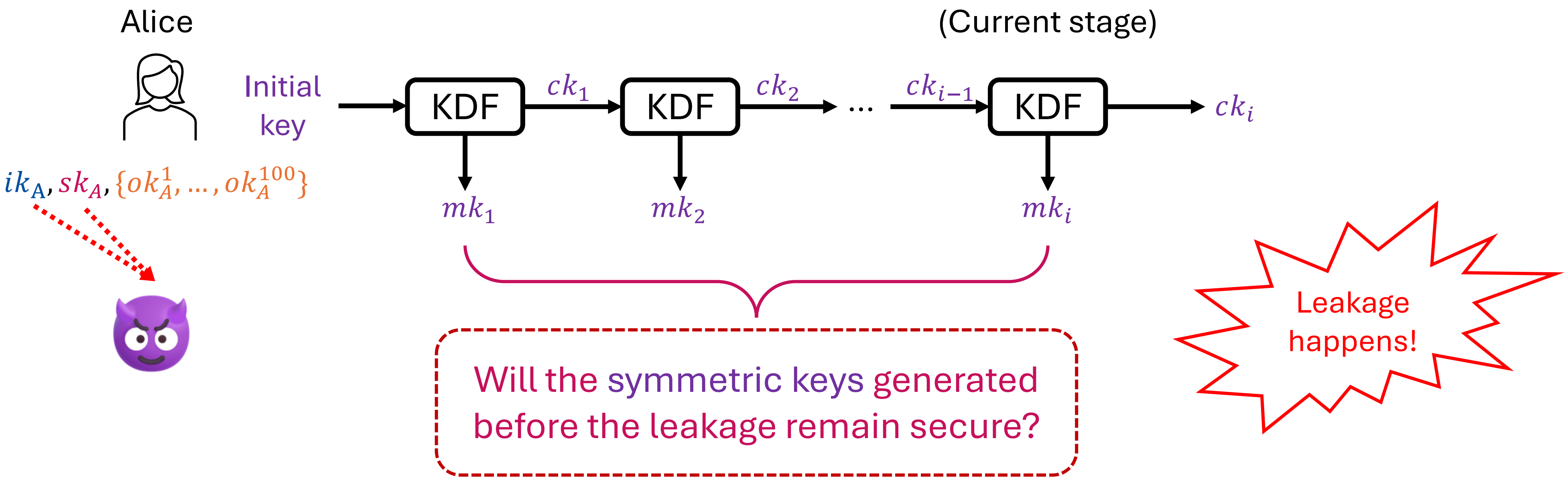
Forward Secrecy

- Long-term secret keys are compromised, but past communication remains secure...



Forward Secrecy

- Long-term secret keys are compromised, but past communication remains secure…



Will the symmetric keys generated before the leakage remain secure?

Forward Secrecy

- Recall: How the X3DH protocol computes a shared secret...

Alice

Leakage!

$SK_A = \text{X3DH\_Key\_Alice}(\boxed{ik_A,} ek_A, IPK_B, SPK_B, OPK_B)$

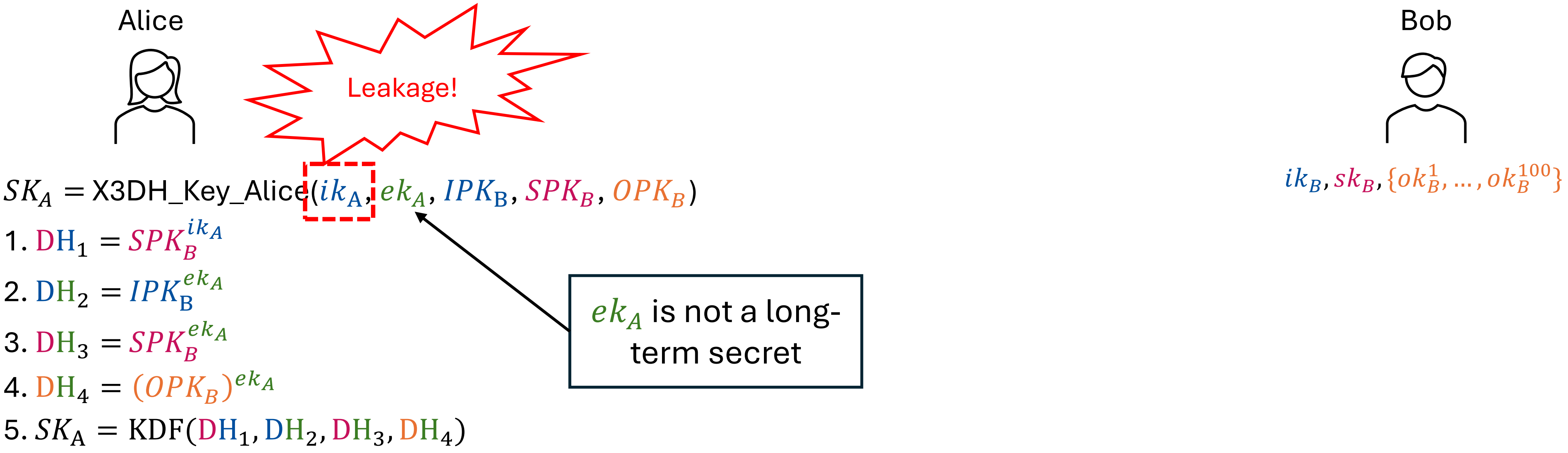
1. $\mathrm{DH}_1 = SPK_B^{ik_A}$
2. $\mathrm{DH}_2 = IPK_B^{ek_A}$
3. $\mathrm{DH}_3 = SPK_B^{ek_A}$
4. $\mathrm{DH}_4 = (OPK_B)^{ek_A}$
5. $SK_A = \mathrm{KDF}(\mathrm{DH}_1, \mathrm{DH}_2, \mathrm{DH}_3, \mathrm{DH}_4)$

Bob

$ik_B, sk_B, \{ok_B^1, \dots, ok_B^{100}\}$

Forward Secrecy

- Recall: How the X3DH protocol computes a shared secret…



Alice

Leakage!

Bob

$ik_B, sk_B, \{ok_B^1, \dots, ok_B^{100}\}$

$SK_A = \text{X3DH\_Key\_Alice}(\boxed{ik_A,} ek_A, IPK_B, SPK_B, OPK_B)$

1. $DH_1 = SPK_B^{ik_A}$
2. $DH_2 = IPK_B^{ek_A}$
3. $DH_3 = SPK_B^{ek_A}$
4. $DH_4 = (OPK_B)^{ek_A}$
5. $SK_A = \text{KDF}(DH_1, DH_2, DH_3, DH_4)$

ek_A is not a long-term secret

Forward Secrecy

- Recall: How the X3DH protocol computes a shared secret...

Alice

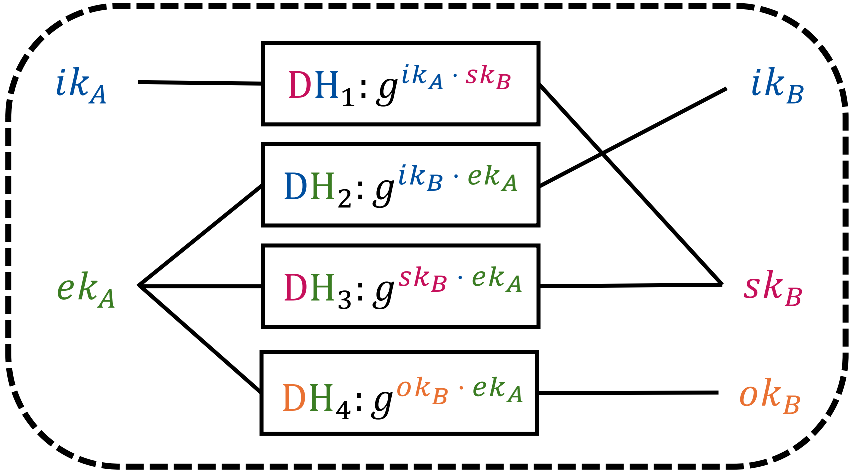
Leakage!

$SK_A = \text{X3DH\_Key\_Alice}(\boxed{ik_A,} ek_A, IPK_B, SPK_B, OPK_B)$

1. $DH_1 = SPK_B^{ik_A}$
2. $DH_2 = IPK_B^{ek_A}$
3. $DH_3 = SPK_B^{ek_A}$
4. $DH_4 = (OPK_B)^{ek_A}$
5. $SK_A = \text{KDF}(DH_1, DH_2, DH_3, DH_4)$

Bob

$ik_B, sk_B, \{ok_B^1, \ldots, ok_B^{100}\}$



ik_A
ek_A
$DH_1: g^{ik_A \cdot sk_B}$
$DH_2: g^{ik_B \cdot ek_A}$
$DH_3: g^{sk_B \cdot ek_A}$
$DH_4: g^{ok_B \cdot ek_A}$
ik_B
sk_B
ok_B

Forward Secrecy

- Recall: How the X3DH protocol computes a shared secret…

Alice

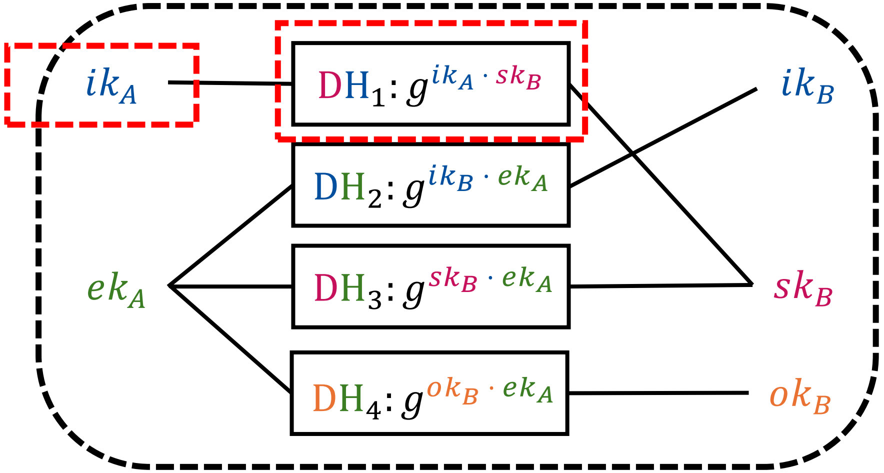
Leakage!

Bob

$ik_B, sk_B, \{ok_B^1, \ldots, ok_B^{100}\}$

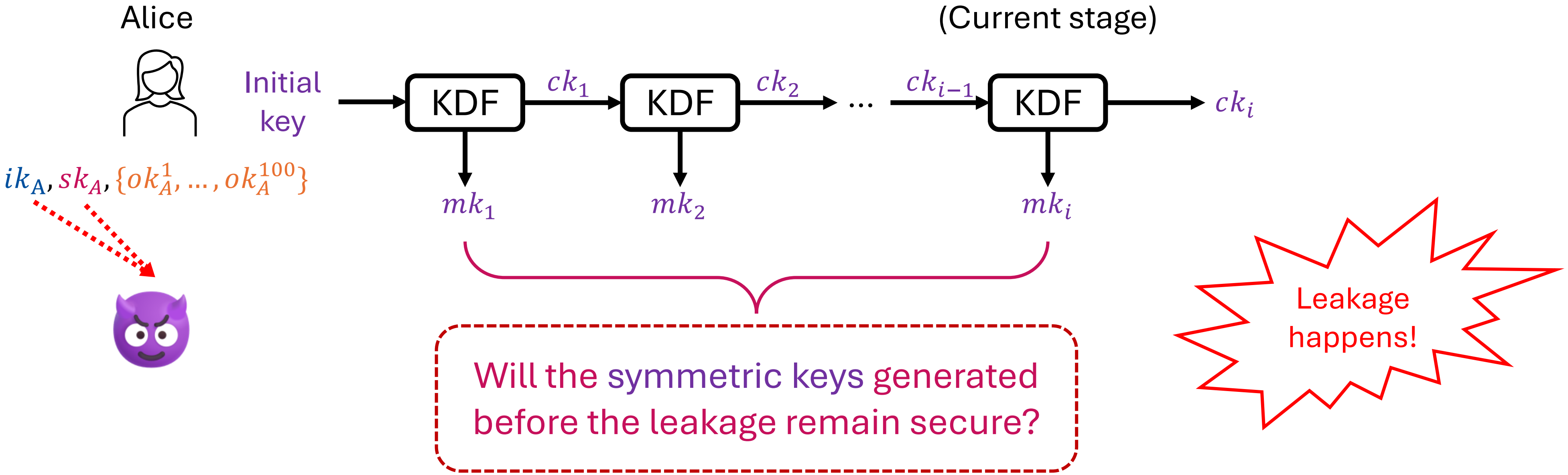
SK_A = X3DH_Key_Alice($ik_A, ek_A, IPK_B, SPK_B, OPK_B$)

1. $DH_1 = SPK_B^{ik_A}$
2. $DH_2 = IPK_B^{ek_A}$
3. $DH_3 = SPK_B^{ek_A}$
4. $DH_4 = (OPK_B)^{ek_A}$
5. $SK_A = \mathrm{KDF}(DH_1, DH_2, DH_3, DH_4)$


ik_A
$DH_1: g^{ik_A \cdot sk_B}$
$DH_2: g^{ik_B \cdot ek_A}$
$DH_3: g^{sk_B \cdot ek_A}$
$DH_4: g^{ok_B \cdot ek_A}$
ek_A
ik_B
sk_B
ok_B

Forward Secrecy

- Long-term secret keys are compromised, but past communication remains secure…

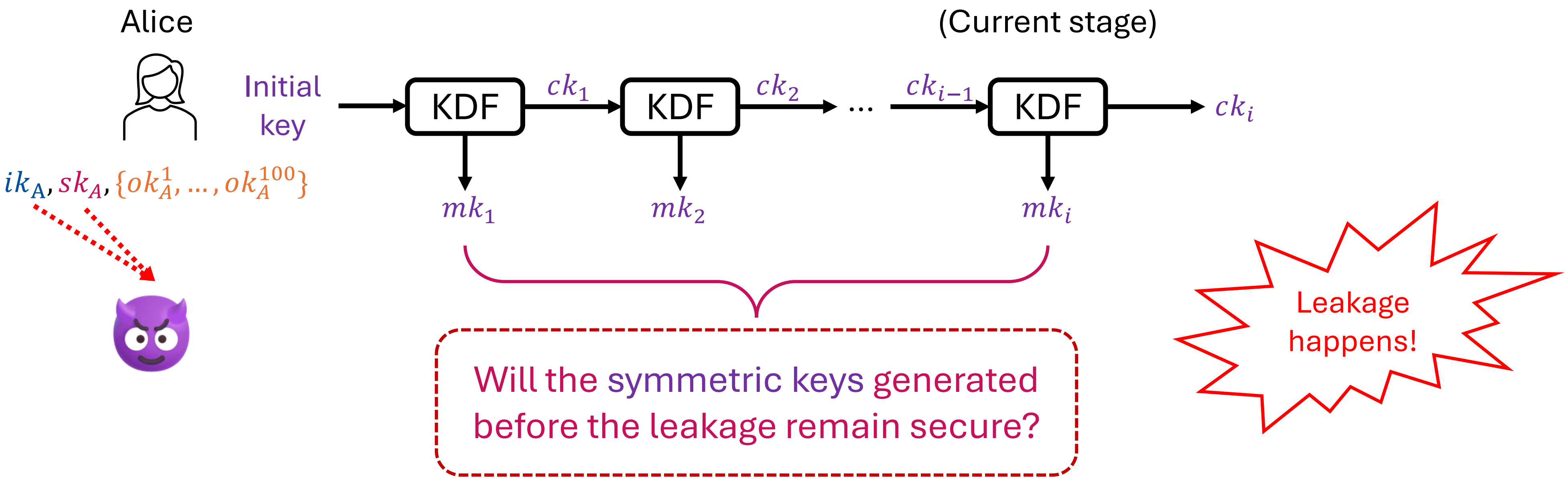


Will the symmetric keys generated before the leakage remain secure?

Initial_key (of X3DH)$= \mathrm{KDF}(\mathrm{DH}_1, \mathrm{DH}_2, \mathrm{DH}_3, \mathrm{DH}_4)$

Forward Secrecy

- Long-term secret keys are compromised, but past communication remains secure...



Will the symmetric keys generated before the leakage remain secure?

Leakage happens!

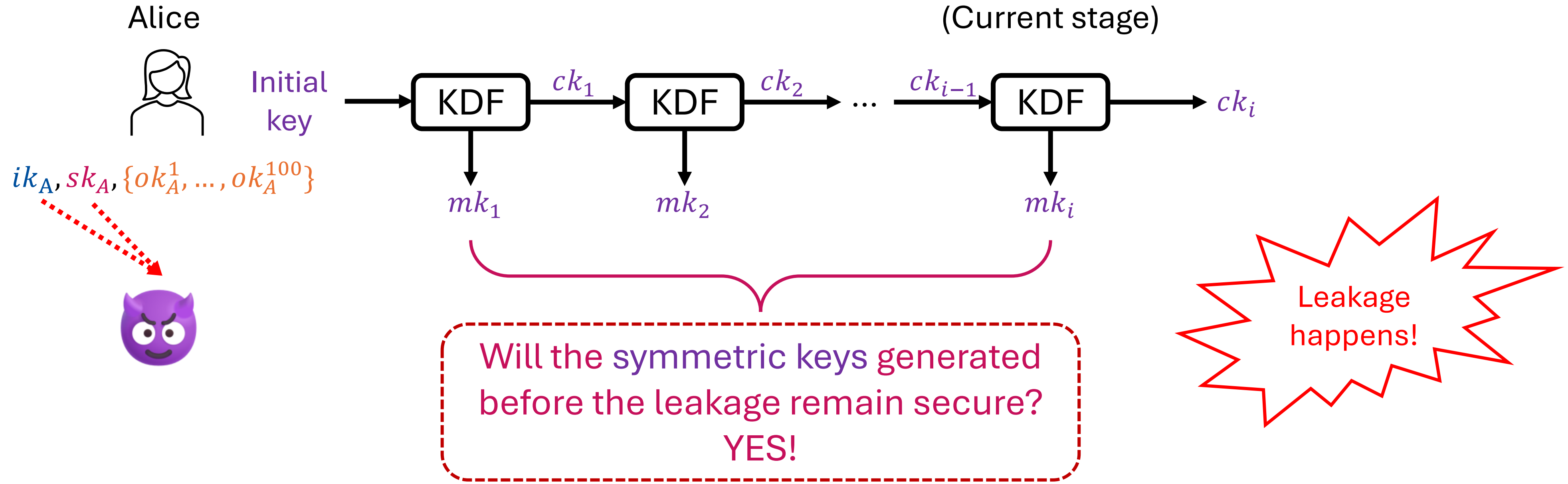
Initial_key (of X3DH)= $\mathrm{KDF}(\boxed{\mathrm{DH}_1} \mathrm{DH}_2, \mathrm{DH}_3, \mathrm{DH}_4)$

DH_1 is not secure

But DH_2,3,4 remain secret

Forward Secrecy

- Long-term secret keys are compromised, but past communication remains secure...



Will the symmetric keys generated before the leakage remain secure? YES!

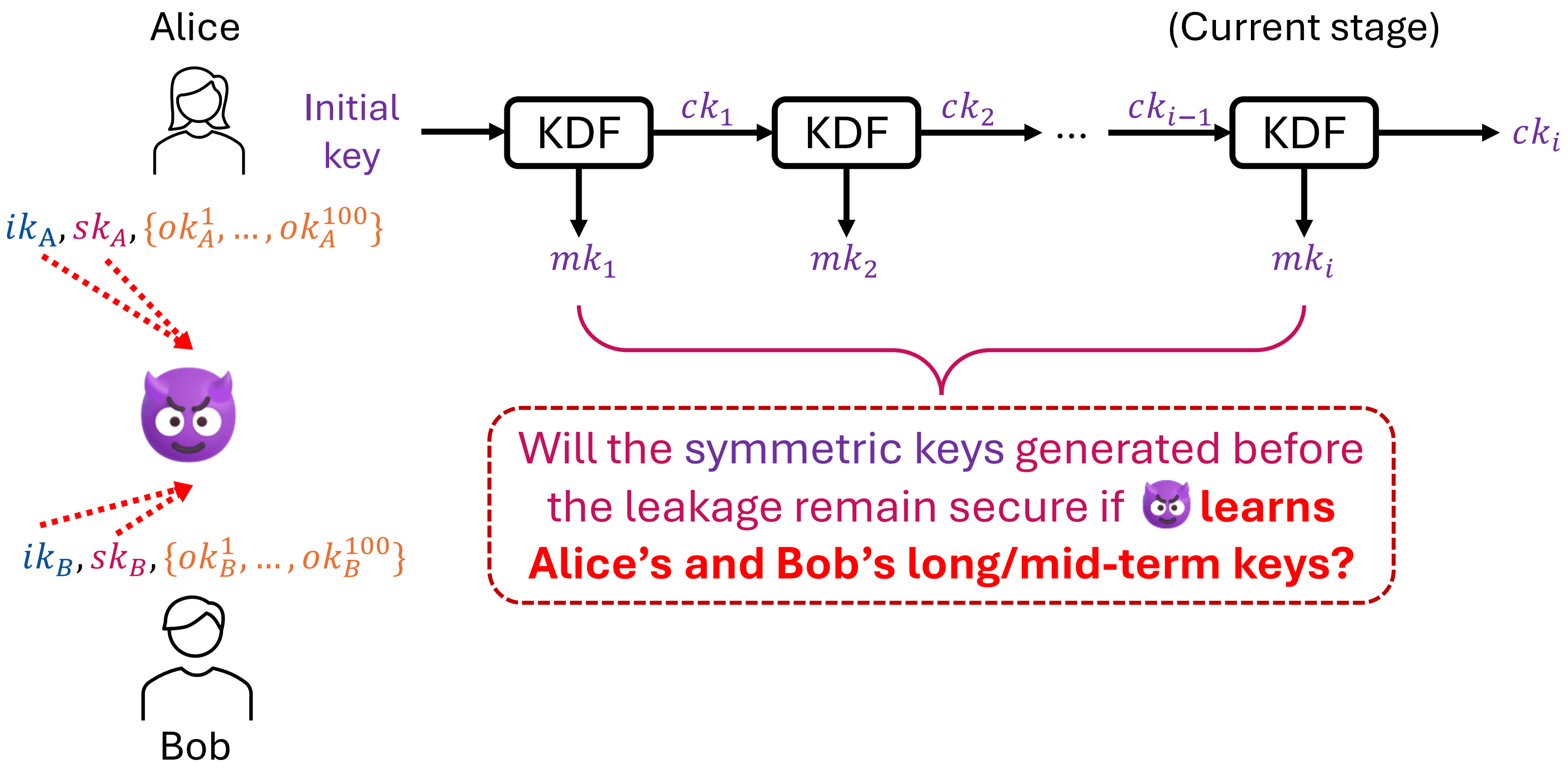
Initial_key (of X3DH)= $\mathrm{KDF}(\boxed{\mathrm{DH}_1}, \mathrm{DH}_2, \mathrm{DH}_3, \mathrm{DH}_4)$

DH_1 is not secure

But DH_2,3,4 remain secret

Forward Secrecy

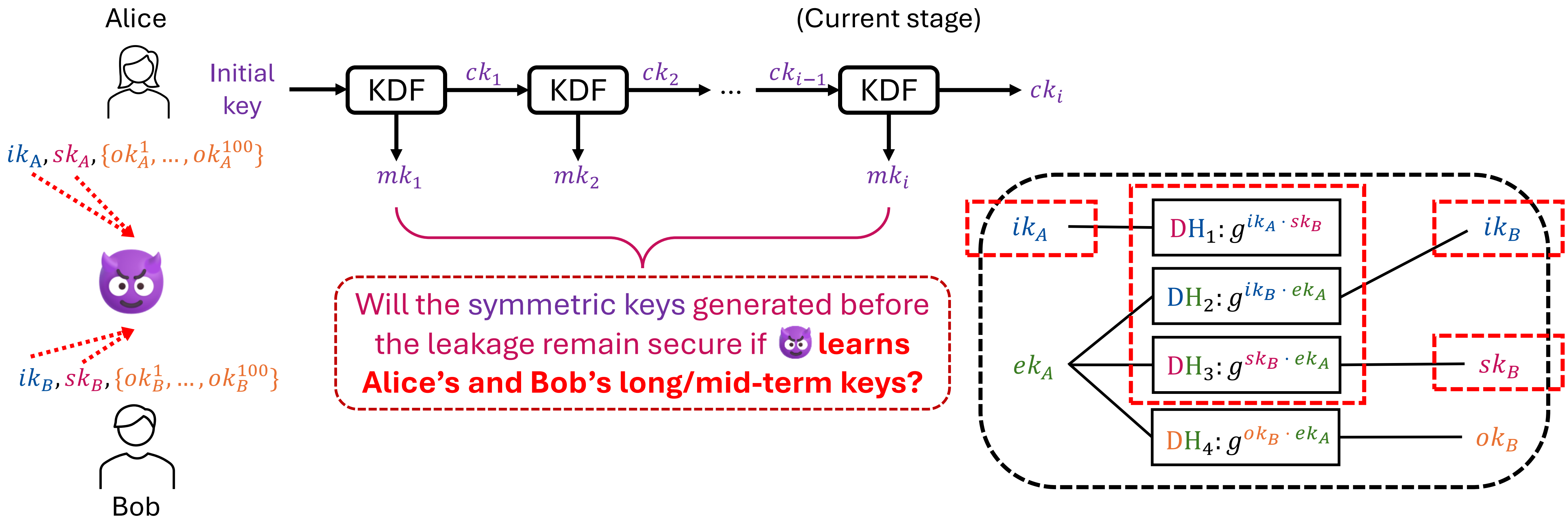
- Long-term secret keys are compromised, but past communication remains secure…



Will the symmetric keys generated before the leakage remain secure if 😈 **learns Alice's and Bob's long/mid-term keys?**

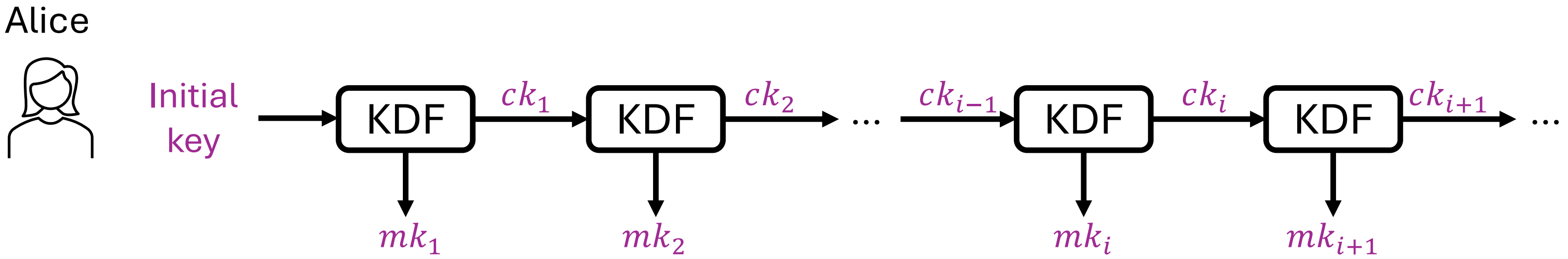
Forward Secrecy

- Long-term secret keys are compromised, but past communication remains secure…

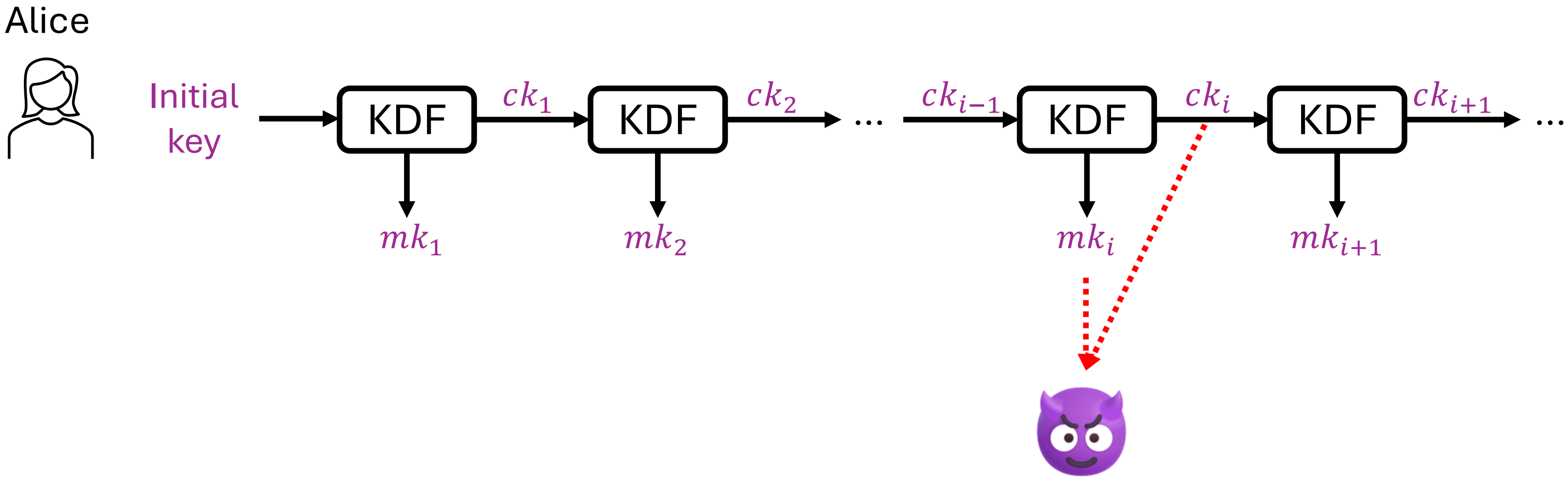

Alice
Initial key
KDF
ck_1
KDF
ck_2
…
ck_{i-1}
(Current stage)
KDF
ck_i
mk_1
mk_2
mk_i
$ik_A, sk_A, \{ok_A^1, \dots, ok_A^{100}\}$
$ik_B, sk_B, \{ok_B^1, \dots, ok_B^{100}\}$
Bob
ik_A
$\mathrm{DH}_1: g^{ik_A \cdot sk_B}$
$\mathrm{DH}_2: g^{ik_B \cdot ek_A}$
$\mathrm{DH}_3: g^{sk_B \cdot ek_A}$
$\mathrm{DH}_4: g^{ok_B \cdot ek_A}$
ek_A
ik_B
sk_B
ok_B

Will the symmetric keys generated before the leakage remain secure if 😈 **learns Alice's and Bob's long/mid-term keys?**

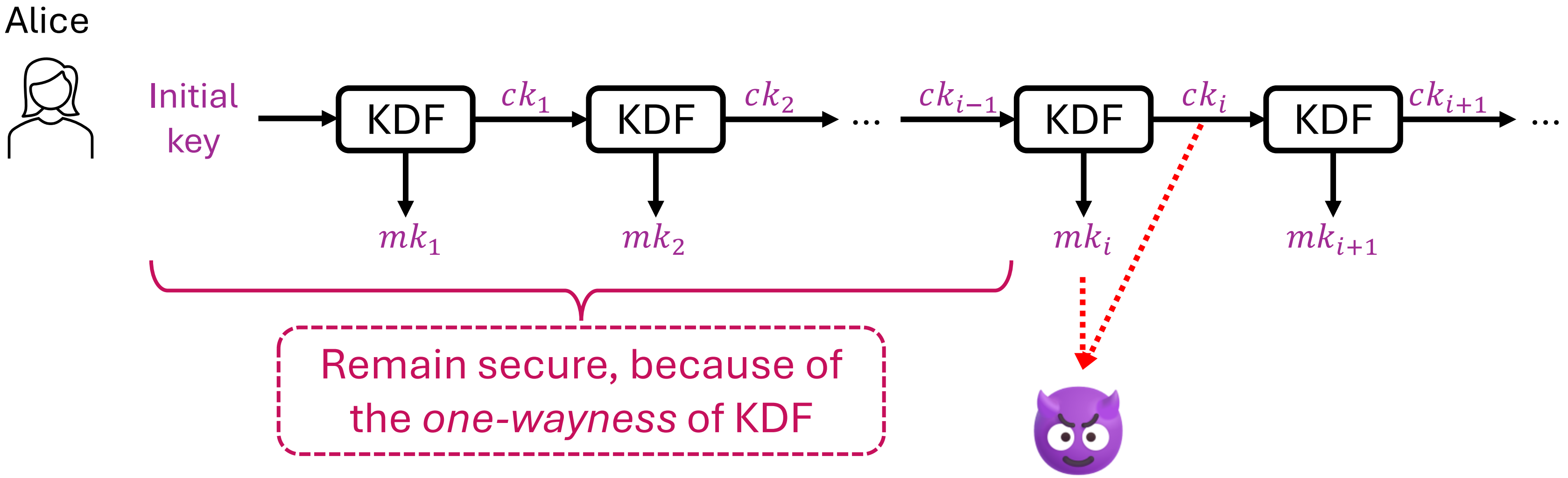
Backward Secrecy



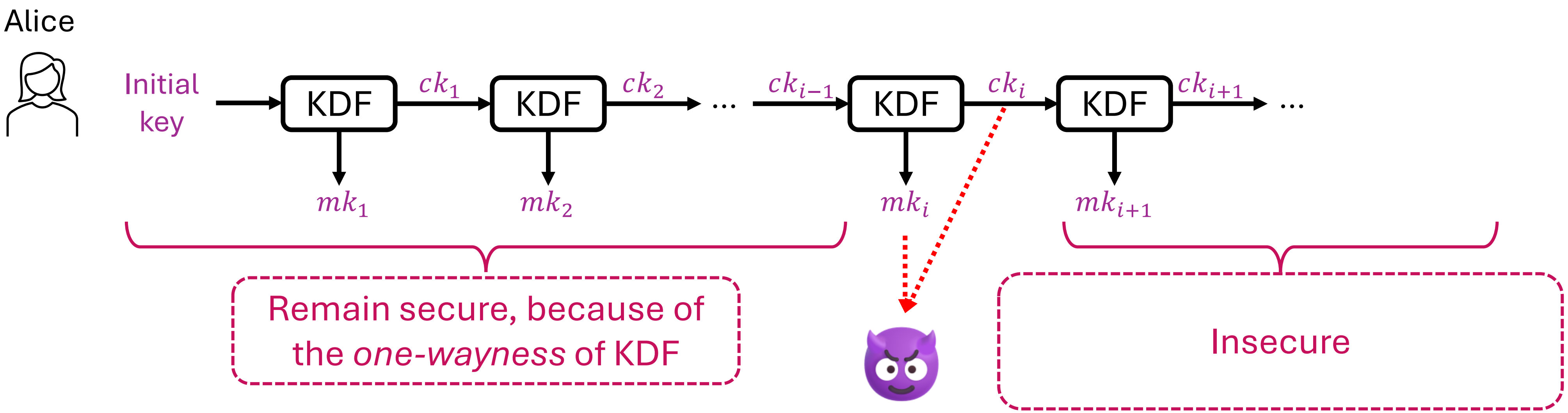
Backward Secrecy



Backward Secrecy

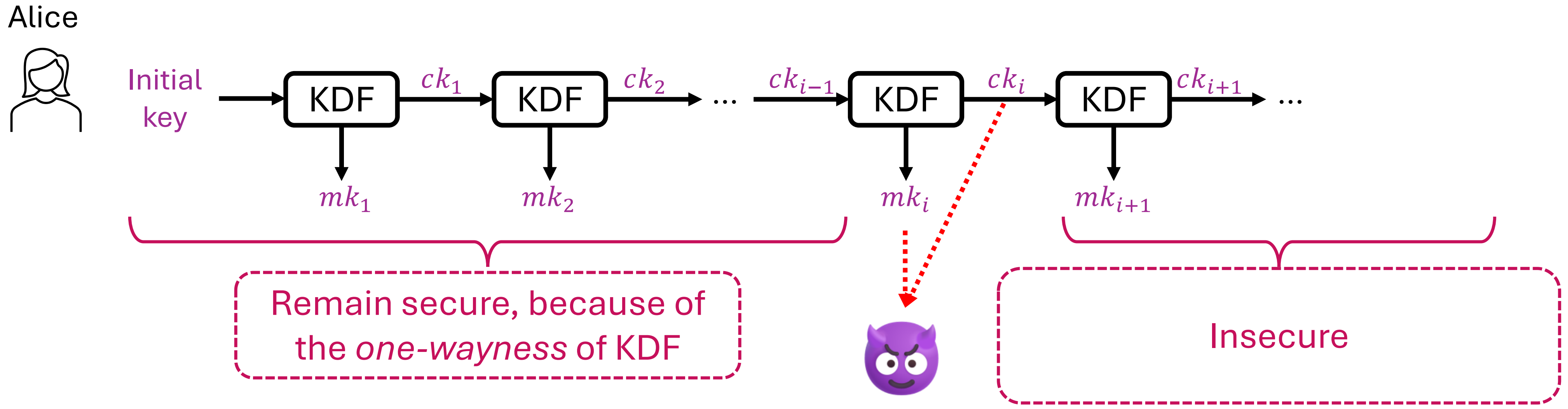


Backward Secrecy



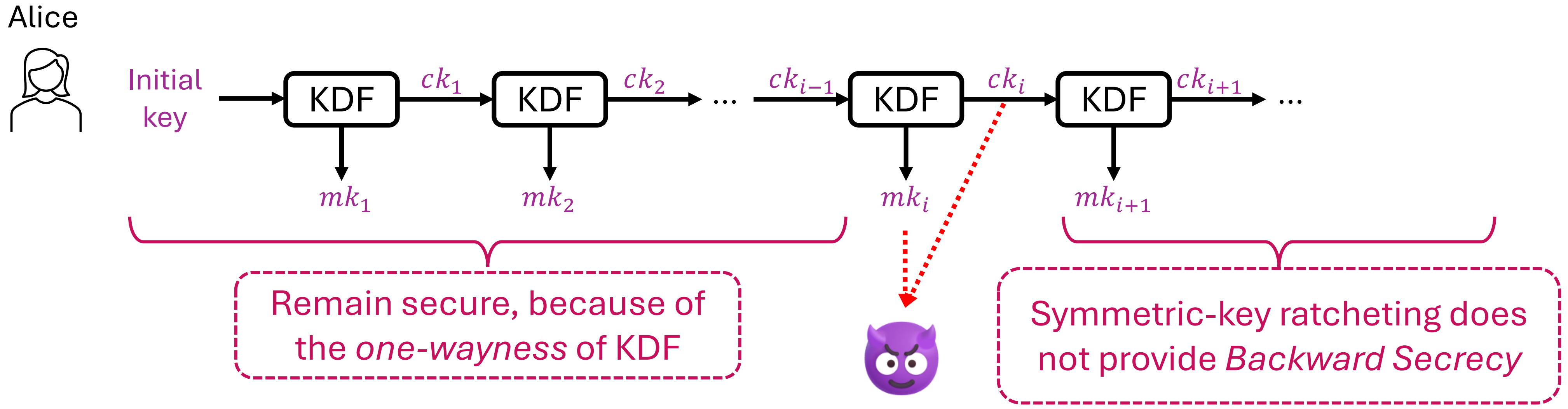
Backward Secrecy

- Future communication remains secure even if a current session key is compromised



Backward Secrecy

- Future communication remains secure even if a current session key is compromised



Remain secure, because of the *one-wayness* of KDF

Symmetric-key ratcheting does not provide *Backward Secrecy*

Diffie-Hellman Ratcheting

- X3DH + Symmetric-key Ratcheting
  - X3DH provides *Forward Secrecy*
  - Current session key compromises does not lead to the compromise of previous session keys
    - (by the one-wayness of KDF in Symmetric-key Ratcheting)
  - No Backward Secrecy

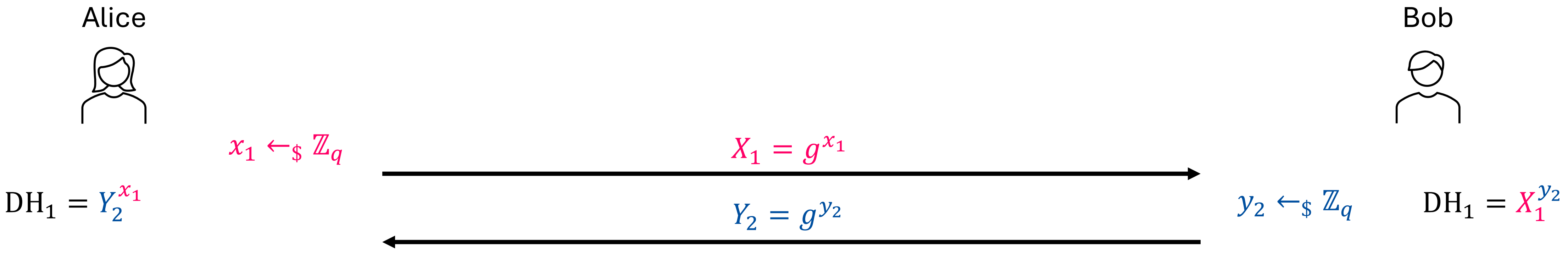
Diffie-Hellman Ratcheting

- X3DH + Symmetric-key Ratcheting
  - X3DH provides *Forward Secrecy*
  - Current session key compromises does not lead to the compromise of previous session keys
    - (by the one-wayness of KDF in Symmetric-key Ratcheting)
  - No Backward Secrecy

- Solution: Diffie-Hellman Ratcheting

Diffie-Hellman Ratcheting

- A toy example: Running DHKE continuously with *rotating ephemeral keys*…



Alice

Bob

$x_1 \leftarrow_{\$} \mathbb{Z}_q$

$X_1 = g^{x_1}$

$Y_2 = g^{y_2}$

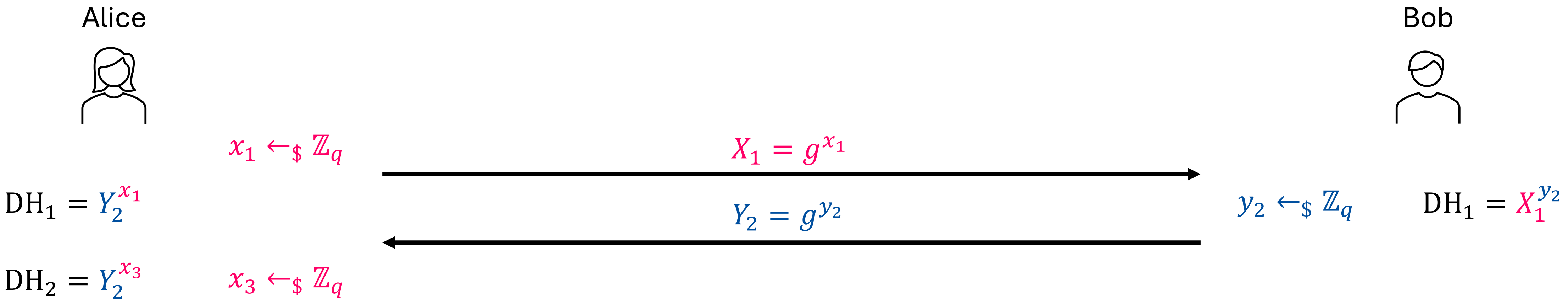
$y_2 \leftarrow_{\$} \mathbb{Z}_q$

$\mathrm{DH}_1 = Y_2^{x_1}$

$\mathrm{DH}_1 = X_1^{y_2}$

Diffie-Hellman Ratcheting

- A toy example: Running DHKE continuously with *rotating ephemeral keys*…



Alice

Bob

$x_1 \leftarrow_{\$} \mathbb{Z}_q$

$X_1 = g^{x_1}$

$\mathrm{DH}_1 = Y_2^{x_1}$

$y_2 \leftarrow_{\$} \mathbb{Z}_q$

$\mathrm{DH}_1 = X_1^{y_2}$

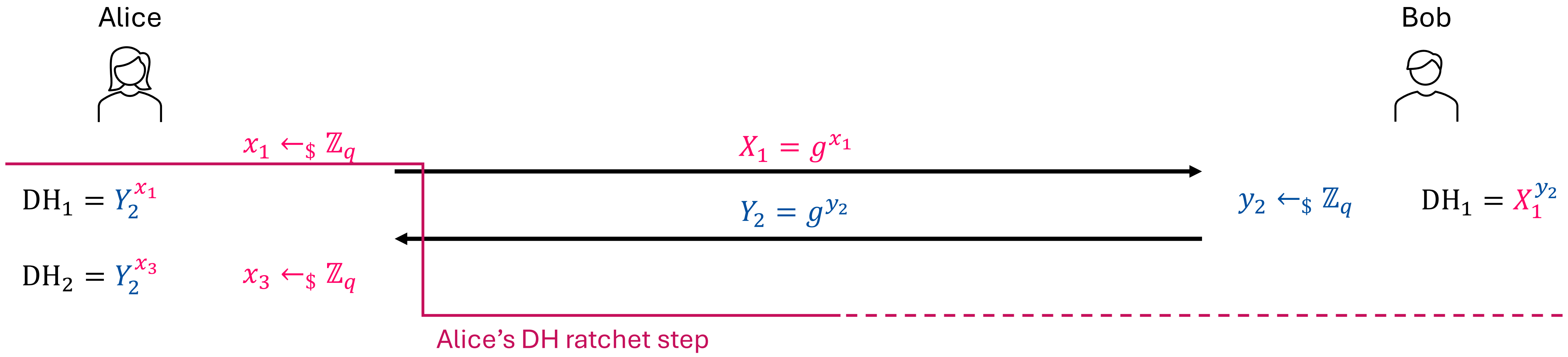
$Y_2 = g^{y_2}$

$\mathrm{DH}_2 = Y_2^{x_3}$

$x_3 \leftarrow_{\$} \mathbb{Z}_q$

Diffie-Hellman Ratcheting

- A toy example: Running DHKE continuously with *rotating ephemeral keys*…



Alice

Bob

$x_1 \leftarrow_\$ \mathbb{Z}_q$

$X_1 = g^{x_1}$

$\mathrm{DH}_1 = Y_2^{x_1}$

$Y_2 = g^{y_2}$

$y_2 \leftarrow_\$ \mathbb{Z}_q$

$\mathrm{DH}_1 = X_1^{y_2}$

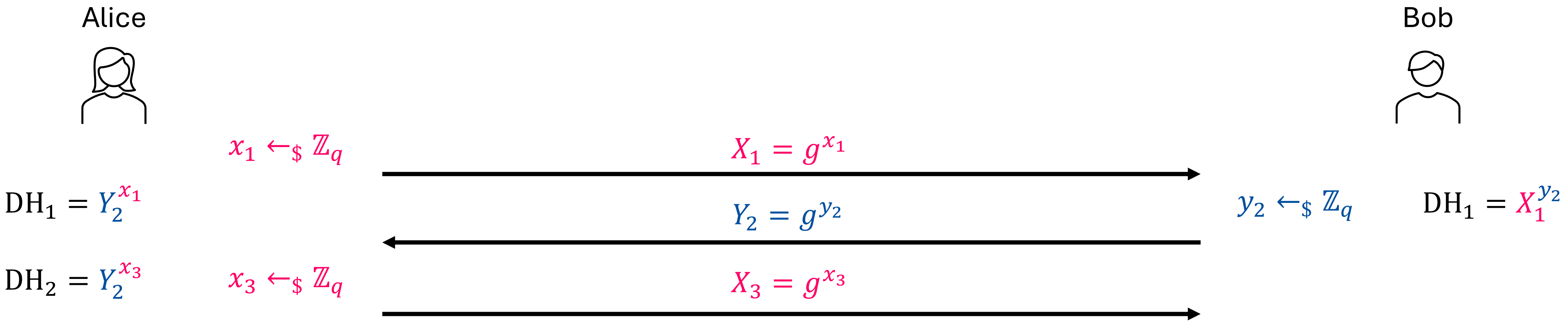
$\mathrm{DH}_2 = Y_2^{x_3}$

$x_3 \leftarrow_\$ \mathbb{Z}_q$

Alice's DH ratchet step

Diffie-Hellman Ratcheting

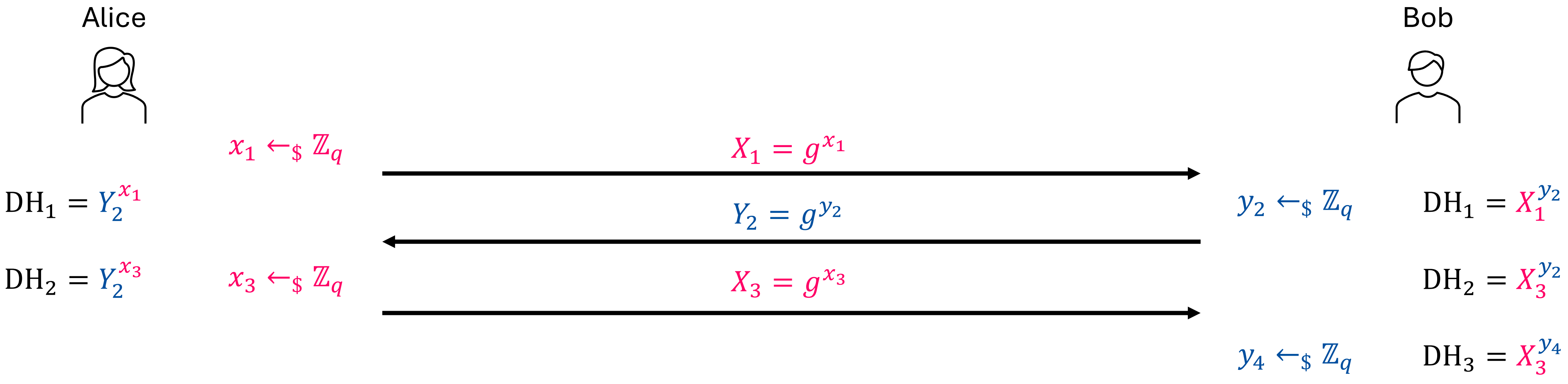
- A toy example: Running DHKE continuously with *rotating ephemeral keys*…



Alice
Bob
$x_1 \leftarrow_{\$} \mathbb{Z}_q$
$X_1 = g^{x_1}$
$\mathrm{DH}_1 = Y_2^{x_1}$
$Y_2 = g^{y_2}$
$y_2 \leftarrow_{\$} \mathbb{Z}_q$
$\mathrm{DH}_1 = X_1^{y_2}$
$\mathrm{DH}_2 = Y_2^{x_3}$
$x_3 \leftarrow_{\$} \mathbb{Z}_q$
$X_3 = g^{x_3}$

Diffie-Hellman Ratcheting

- A toy example: Running DHKE continuously with *rotating ephemeral keys*…



Alice

Bob

$x_1 \leftarrow_\$ \mathbb{Z}_q$ $\qquad X_1 = g^{x_1}$ →

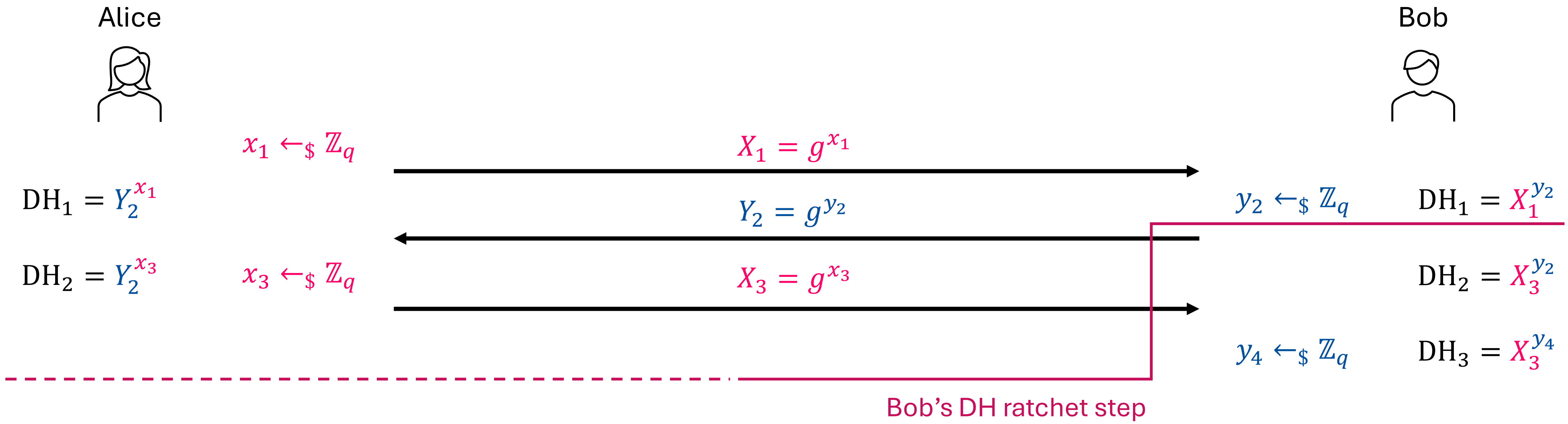
$\mathrm{DH}_1 = Y_2^{x_1}$ $\qquad$ ← $Y_2 = g^{y_2}$ $\qquad y_2 \leftarrow_\$ \mathbb{Z}_q$ $\qquad \mathrm{DH}_1 = X_1^{y_2}$

$\mathrm{DH}_2 = Y_2^{x_3}$ $\qquad x_3 \leftarrow_\$ \mathbb{Z}_q$ $\qquad X_3 = g^{x_3}$ → $\qquad \mathrm{DH}_2 = X_3^{y_2}$

$y_4 \leftarrow_\$ \mathbb{Z}_q$ $\qquad \mathrm{DH}_3 = X_3^{y_4}$

Diffie-Hellman Ratcheting

- A toy example: Running DHKE continuously with *rotating ephemeral keys*…



Alice

Bob

$x_1 \leftarrow_{\$} \mathbb{Z}_q$

$X_1 = g^{x_1}$

$y_2 \leftarrow_{\$} \mathbb{Z}_q$ $\quad \mathrm{DH}_1 = X_1^{y_2}$

$\mathrm{DH}_1 = Y_2^{x_1}$

$Y_2 = g^{y_2}$

$\mathrm{DH}_2 = Y_2^{x_3}$ $\quad x_3 \leftarrow_{\$} \mathbb{Z}_q$

$X_3 = g^{x_3}$

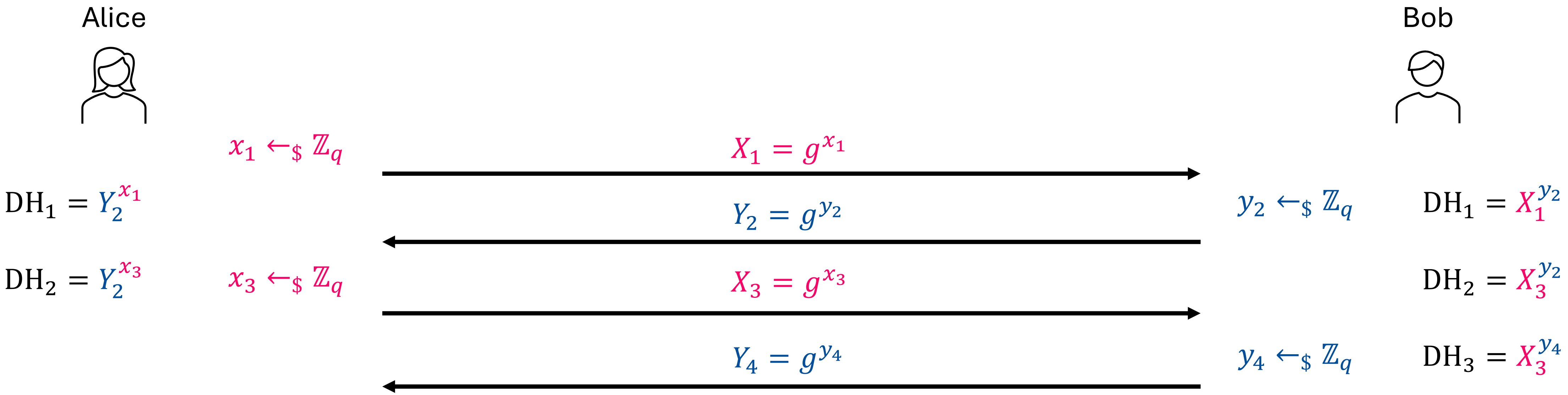
$\mathrm{DH}_2 = X_3^{y_2}$

$y_4 \leftarrow_{\$} \mathbb{Z}_q$ $\quad \mathrm{DH}_3 = X_3^{y_4}$

Bob’s DH ratchet step

Diffie-Hellman Ratcheting

- A toy example: Running DHKE continuously with *rotating ephemeral keys*…



Alice

Bob

$x_1 \leftarrow_{\$} \mathbb{Z}_q$ $\quad X_1 = g^{x_1}$ →

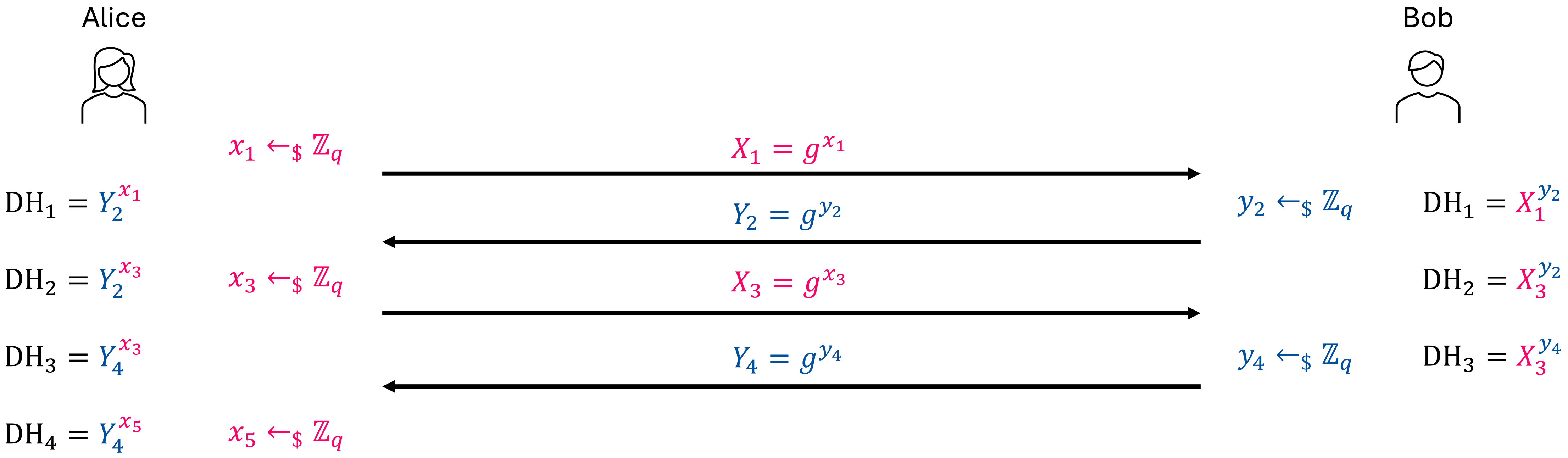
$\mathrm{DH}_1 = Y_2^{x_1}$ $\quad$ ← $Y_2 = g^{y_2}$ $\quad y_2 \leftarrow_{\$} \mathbb{Z}_q$ $\quad \mathrm{DH}_1 = X_1^{y_2}$

$\mathrm{DH}_2 = Y_2^{x_3}$ $\quad x_3 \leftarrow_{\$} \mathbb{Z}_q$ $\quad X_3 = g^{x_3}$ → $\quad \mathrm{DH}_2 = X_3^{y_2}$

← $Y_4 = g^{y_4}$ $\quad y_4 \leftarrow_{\$} \mathbb{Z}_q$ $\quad \mathrm{DH}_3 = X_3^{y_4}$

Diffie-Hellman Ratcheting

- A toy example: Running DHKE continuously with *rotating ephemeral keys*…



Alice

Bob

$x_1 \leftarrow_{\$} \mathbb{Z}_q$ $\quad X_1 = g^{x_1} \longrightarrow$

$\mathrm{DH}_1 = Y_2^{x_1}$ $\quad \longleftarrow Y_2 = g^{y_2}$ $\quad y_2 \leftarrow_{\$} \mathbb{Z}_q$ $\quad \mathrm{DH}_1 = X_1^{y_2}$

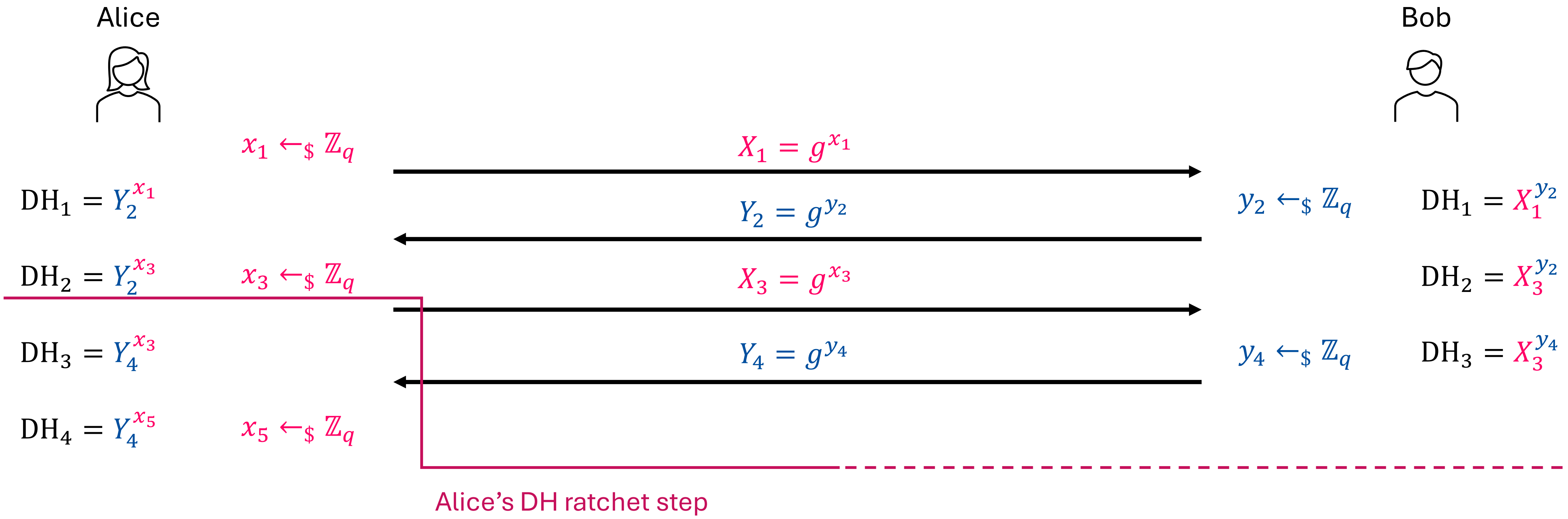
$\mathrm{DH}_2 = Y_2^{x_3}$ $\quad x_3 \leftarrow_{\$} \mathbb{Z}_q$ $\quad X_3 = g^{x_3} \longrightarrow$ $\quad \mathrm{DH}_2 = X_3^{y_2}$

$\mathrm{DH}_3 = Y_4^{x_3}$ $\quad \longleftarrow Y_4 = g^{y_4}$ $\quad y_4 \leftarrow_{\$} \mathbb{Z}_q$ $\quad \mathrm{DH}_3 = X_3^{y_4}$

$\mathrm{DH}_4 = Y_4^{x_5}$ $\quad x_5 \leftarrow_{\$} \mathbb{Z}_q$

Diffie-Hellman Ratcheting

- A toy example: Running DHKE continuously with *rotating ephemeral keys*…



Alice

Bob

$x_1 \leftarrow_\$ \mathbb{Z}_q$ $\quad X_1 = g^{x_1}$

$\mathrm{DH}_1 = Y_2^{x_1}$ $\quad Y_2 = g^{y_2}$ $\quad y_2 \leftarrow_\$ \mathbb{Z}_q$ $\quad \mathrm{DH}_1 = X_1^{y_2}$

$\mathrm{DH}_2 = Y_2^{x_3}$ $\quad x_3 \leftarrow_\$ \mathbb{Z}_q$ $\quad X_3 = g^{x_3}$ $\quad \mathrm{DH}_2 = X_3^{y_2}$

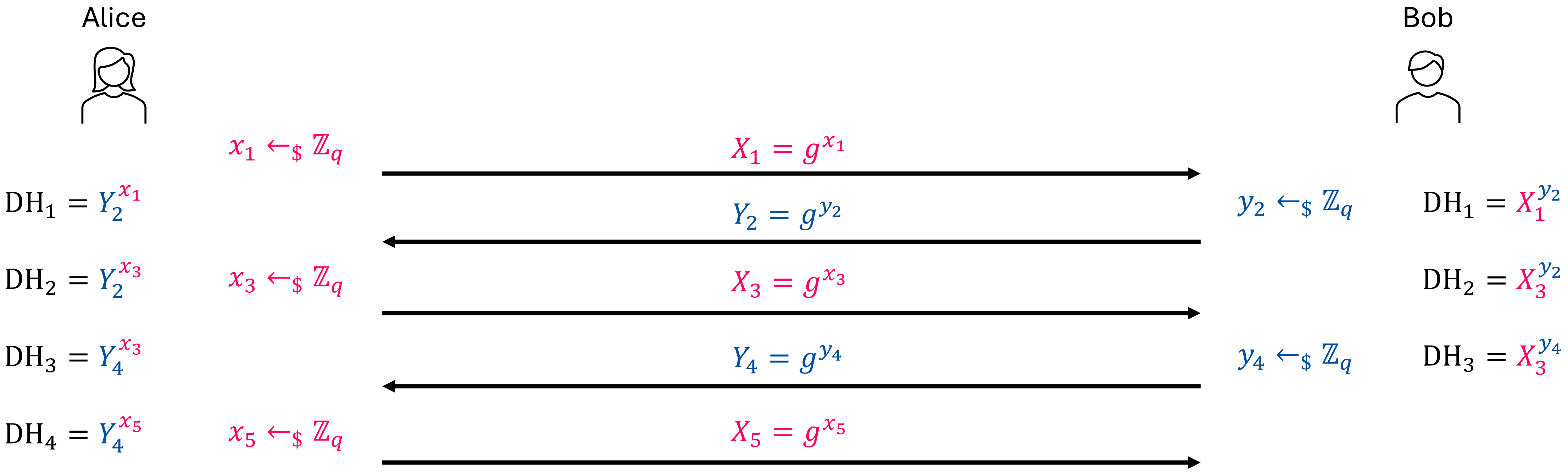
$\mathrm{DH}_3 = Y_4^{x_3}$ $\quad Y_4 = g^{y_4}$ $\quad y_4 \leftarrow_\$ \mathbb{Z}_q$ $\quad \mathrm{DH}_3 = X_3^{y_4}$

$\mathrm{DH}_4 = Y_4^{x_5}$ $\quad x_5 \leftarrow_\$ \mathbb{Z}_q$

Alice’s DH ratchet step

Diffie-Hellman Ratcheting

- A toy example: Running DHKE continuously with *rotating ephemeral keys*…



Alice

Bob

$x_1 \leftarrow_{\$} \mathbb{Z}_q$ $\quad X_1 = g^{x_1}$

$\mathrm{DH}_1 = Y_2^{x_1}$ $\quad Y_2 = g^{y_2}$ $\quad y_2 \leftarrow_{\$} \mathbb{Z}_q$ $\quad \mathrm{DH}_1 = X_1^{y_2}$

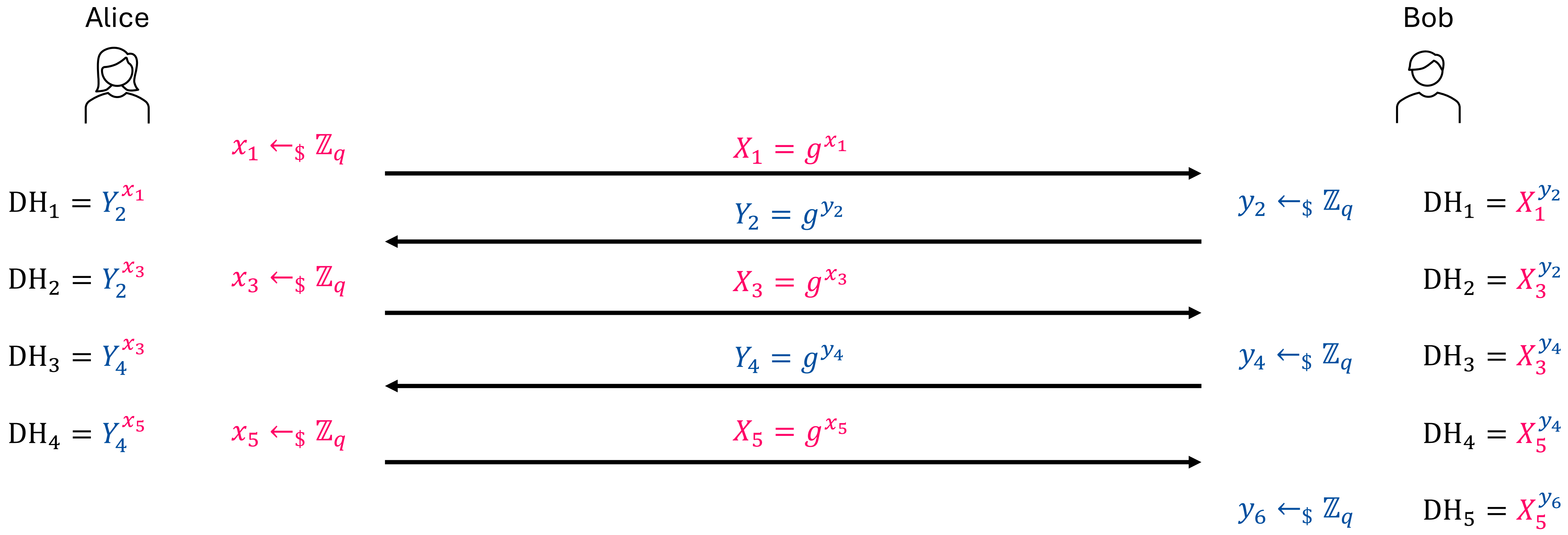
$\mathrm{DH}_2 = Y_2^{x_3}$ $\quad x_3 \leftarrow_{\$} \mathbb{Z}_q$ $\quad X_3 = g^{x_3}$ $\quad \mathrm{DH}_2 = X_3^{y_2}$

$\mathrm{DH}_3 = Y_4^{x_3}$ $\quad Y_4 = g^{y_4}$ $\quad y_4 \leftarrow_{\$} \mathbb{Z}_q$ $\quad \mathrm{DH}_3 = X_3^{y_4}$

$\mathrm{DH}_4 = Y_4^{x_5}$ $\quad x_5 \leftarrow_{\$} \mathbb{Z}_q$ $\quad X_5 = g^{x_5}$

Diffie-Hellman Ratcheting

- A toy example: Running DHKE continuously with *rotating ephemeral keys*...



Alice

Bob

$x_1 \leftarrow_\$ \mathbb{Z}_q$ $\quad X_1 = g^{x_1} \longrightarrow$

$\mathrm{DH}_1 = Y_2^{x_1}$ $\quad \longleftarrow Y_2 = g^{y_2}$ $\quad y_2 \leftarrow_\$ \mathbb{Z}_q$ $\quad \mathrm{DH}_1 = X_1^{y_2}$

$\mathrm{DH}_2 = Y_2^{x_3}$ $\quad x_3 \leftarrow_\$ \mathbb{Z}_q$ $\quad X_3 = g^{x_3} \longrightarrow$ $\quad \mathrm{DH}_2 = X_3^{y_2}$

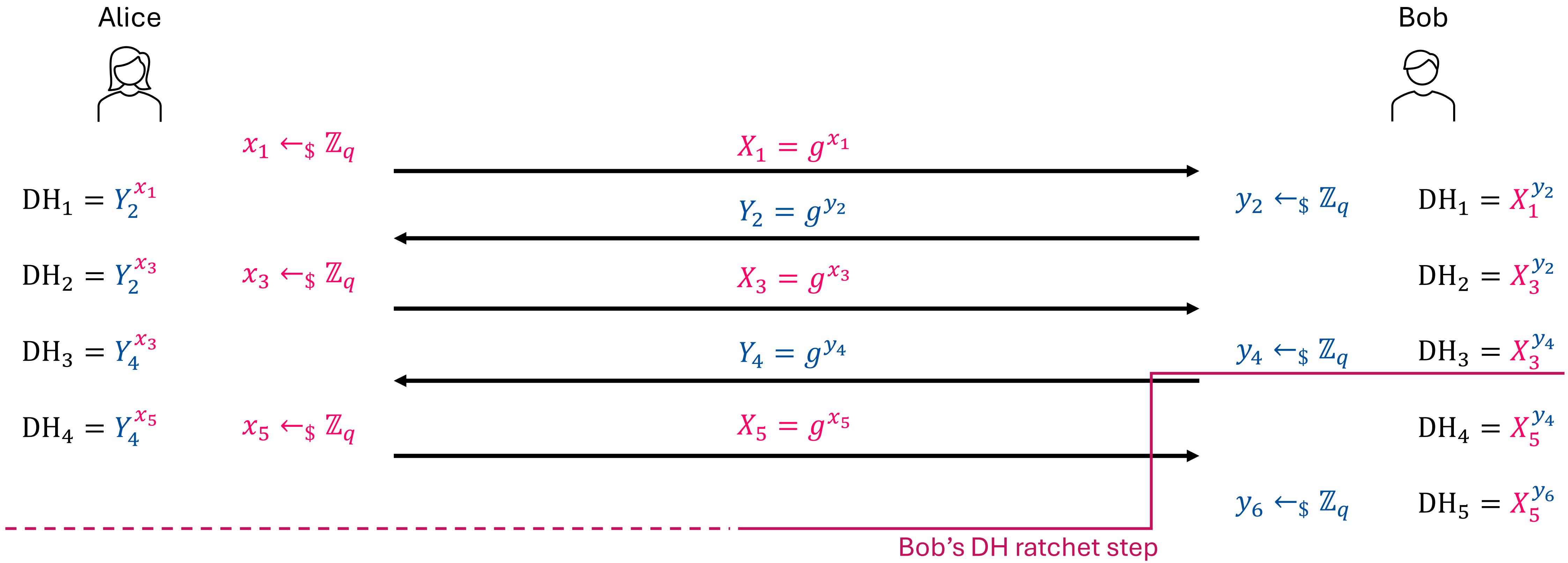
$\mathrm{DH}_3 = Y_4^{x_3}$ $\quad \longleftarrow Y_4 = g^{y_4}$ $\quad y_4 \leftarrow_\$ \mathbb{Z}_q$ $\quad \mathrm{DH}_3 = X_3^{y_4}$

$\mathrm{DH}_4 = Y_4^{x_5}$ $\quad x_5 \leftarrow_\$ \mathbb{Z}_q$ $\quad X_5 = g^{x_5} \longrightarrow$ $\quad \mathrm{DH}_4 = X_5^{y_4}$

$y_6 \leftarrow_\$ \mathbb{Z}_q$ $\quad \mathrm{DH}_5 = X_5^{y_6}$

Diffie-Hellman Ratcheting

- A toy example: Running DHKE continuously with *rotating ephemeral keys*…



Alice

Bob

$x_1 \leftarrow_{\$} \mathbb{Z}_q$ $\quad X_1 = g^{x_1} \rightarrow$

$\mathrm{DH}_1 = Y_2^{x_1}$ $\quad \leftarrow Y_2 = g^{y_2}$ $\quad y_2 \leftarrow_{\$} \mathbb{Z}_q$ $\quad \mathrm{DH}_1 = X_1^{y_2}$

$\mathrm{DH}_2 = Y_2^{x_3}$ $\quad x_3 \leftarrow_{\$} \mathbb{Z}_q$ $\quad X_3 = g^{x_3} \rightarrow$ $\quad \mathrm{DH}_2 = X_3^{y_2}$

$\mathrm{DH}_3 = Y_4^{x_3}$ $\quad \leftarrow Y_4 = g^{y_4}$ $\quad y_4 \leftarrow_{\$} \mathbb{Z}_q$ $\quad \mathrm{DH}_3 = X_3^{y_4}$

$\mathrm{DH}_4 = Y_4^{x_5}$ $\quad x_5 \leftarrow_{\$} \mathbb{Z}_q$ $\quad X_5 = g^{x_5} \rightarrow$ $\quad \mathrm{DH}_4 = X_5^{y_4}$

$y_6 \leftarrow_{\$} \mathbb{Z}_q$ $\quad \mathrm{DH}_5 = X_5^{y_6}$

Bob’s DH ratchet step

Double Ratcheting

- The main idea: Combine Symmetric-key Ratcheting and Diffie-Hellman Ratcheting
  - DH Ratcheting generates fresh shared DH secrets continuously via rotating new ephemeral keys…
  - These fresh DH secrets feed into Symmetric-key Ratcheting to add new secret information…

- More details will be explained in the next lecture

Coding Tasks

- Implement the Diffie-Hellman Ratcheting algorithm (can be without sockets).

Homework

No Homework

...but the **deadline** for homework in Lectures 1 and 2 is

22.11.2024 at 23:59 (this Friday evening)

Further Reading

- Old news -- *WhatsApp's Signal Protocol integration is now complete: https://signal.org/blog/whatsapp-complete/*
- Technical Documentations of Signal: https://signal.org/docs/
- Cohn-Gordon et al’s security analysis of Signal: https://eprint.iacr.org/2016/1013