A fully post-quantum, hybrid, sender anonymous, and efficient initial handshake for the Signal protocol

Rune Fiedler[1]

[1]ETH Zurich
rune.fiedler@inf.ethz.ch

Rolfe Schmidt[2]

[2]Signal Messenger
rolfe@signal.org

Lea Thiemt[3]

[3]FAU Erlangen-Nürnberg
lea.thiemt@fau.de

and many co-authors

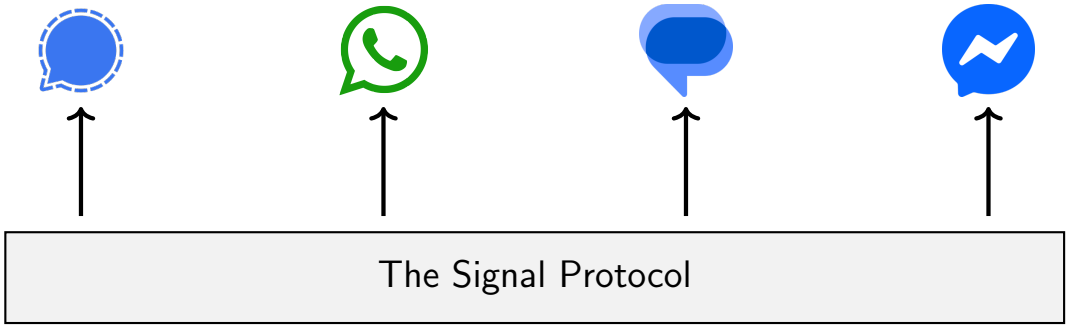
CAW 2026

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

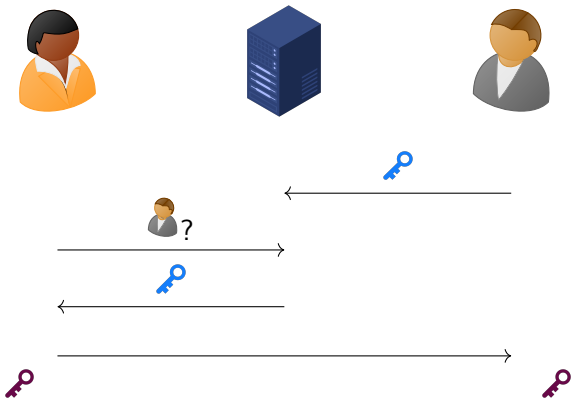
armasuisse Science and Technology
Cyber-Defence Campus

Background

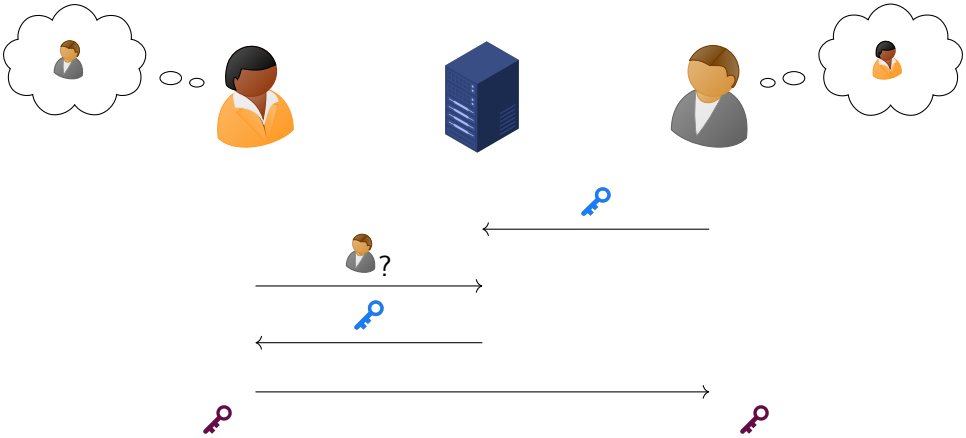
The Signal Protocol



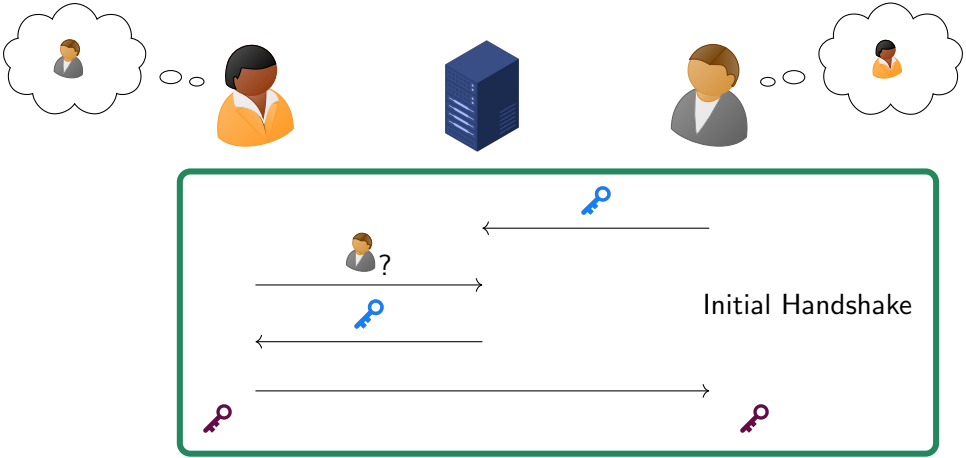
Signal: Asynchronous Authenticated Key Exchange



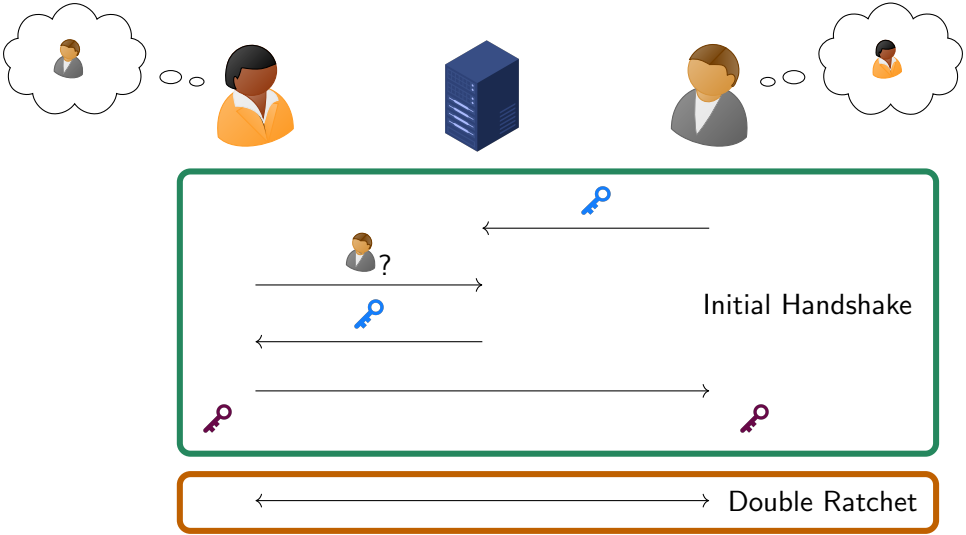
Signal: Asynchronous Authenticated Key Exchange



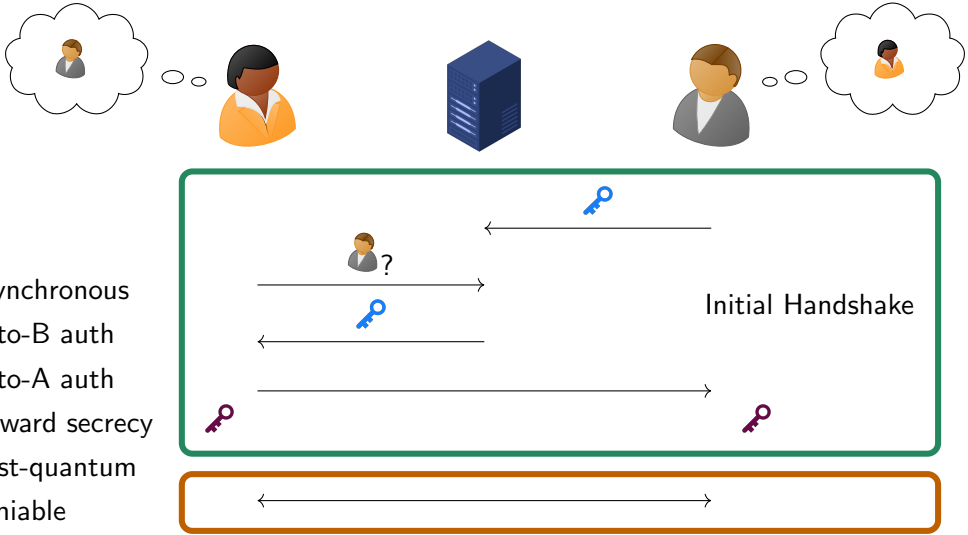
Signal: Asynchronous Authenticated Key Exchange



Signal: Asynchronous Authenticated Key Exchange



Signal: Asynchronous Authenticated Key Exchange



- asynchronous
- A-to-B auth
- B-to-A auth
- forward secrecy
- post-quantum
- deniable

Building Blocks

Diffie–Hellman (DH)

Building Blocks

Diffie–Hellman (DH)


(A, a) ——————— (B, b)

$B^a \leftarrow$ shared secret $\rightarrow A^b$

Building Blocks

Diffie–Hellman (DH)


(A, a) ——————— (B, b)

$B^a \leftarrow$ shared secret $\rightarrow A^b$

	classical	post-quantum
confidentiality	✓	✗
authentication	(✓)	✗

Building Blocks

Diffie–Hellman (DH)

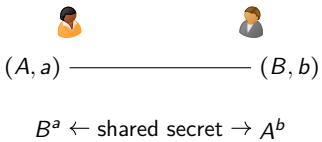
$B^a \leftarrow$ shared secret $\rightarrow A^b$

Key Encapsulation Mechanism (KEM)

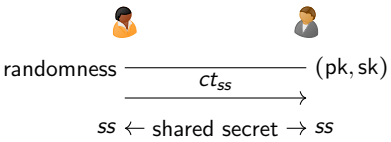
	classical	post-quantum
confidentiality	✓	✗
authentication	(✓)	✗

Building Blocks

Diffie–Hellman (DH)



Key Encapsulation Mechanism (KEM)



	classical	post-quantum
confidentiality	✓	✗
authentication	(✓)	✗

Building Blocks

Diffie–Hellman (DH)

$B^a \leftarrow$ shared secret $\rightarrow A^b$

	classical	post-quantum
confidentiality	✓	✗
authentication	(✓)	✗

Key Encapsulation Mechanism (KEM)

$ss \leftarrow$ shared secret $\rightarrow ss$

	classical	post-quantum
confidentiality	✓	✓
authentication	(✓)	(✓)

Building Blocks

Diffie–Hellman (DH)

$B^a \leftarrow$ shared secret $\rightarrow A^b$

	classical	post-quantum
confidentiality	✓	✗
authentication	(✓)	✗

Key Encapsulation Mechanism (KEM)

$ss \leftarrow$ shared secret $\rightarrow ss$

session key $\leftarrow$ KDF(secrets)

	classical	post-quantum
confidentiality	✓	✓
authentication	(✓)	(✓)

Building Blocks

Diffie–Hellman (DH)

(A, a) —— (B, b)

$B^a \leftarrow$ shared secret $\rightarrow A^b$

Key Encapsulation Mechanism (KEM)

randomness —— $(\mathsf{pk}, \mathsf{sk})$

$\xrightarrow{ct_{ss}}$

$ss \leftarrow$ shared secret $\rightarrow ss$

session key $\leftarrow \mathsf{KDF}(\text{secrets})$

	classical	post-quantum
confidentiality	✓	✗
authentication	(✓)	✗

	classical	post-quantum
confidentiality	✓	✓
authentication	(✓)	(✓)

Signature

$(\mathsf{vk}, \mathsf{sk})$

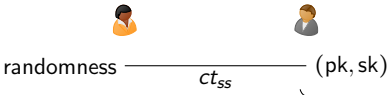
Building Blocks

Diffie–Hellman (DH)

$B^a \leftarrow$ shared secret $\rightarrow A^b$

	classical	post-quantum
confidentiality	✓	✗
authentication	(✓)	✗

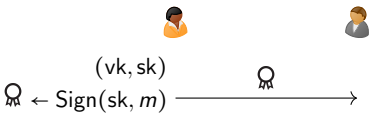
Key Encapsulation Mechanism (KEM)



session key $\leftarrow \mathsf{KDF}(\text{secrets})$

	classical	post-quantum
confidentiality	✓	✓
authentication	(✓)	(✓)

Signature



Building Blocks

Diffie–Hellman (DH)

$B^a \leftarrow$ shared secret $\rightarrow A^b$

	classical	post-quantum
confidentiality	✓	✗
authentication	(✓)	✗

Key Encapsulation Mechanism (KEM)

$ss \leftarrow$ shared secret $\rightarrow ss$

session key $\leftarrow$ KDF(secrets)

	classical	post-quantum
confidentiality	✓	✓
authentication	(✓)	(✓)

Signature

	classical	post-quantum
authentication	✓	✓
deniability	✗	✗

Building Blocks

Diffie–Hellman (DH)

$B^a \leftarrow$ shared secret $\rightarrow A^b$

Key Encapsulation Mechanism (KEM)

$ss \leftarrow$ shared secret $\rightarrow ss$

session key $\leftarrow$ KDF(secrets)

	classical	post-quantum
confidentiality	✓	✗
authentication	(✓)	✗

	classical	post-quantum
confidentiality	✓	✓
authentication	(✓)	(✓)

Signature

	classical	post-quantum
authentication	✓	✓
deniability	✗	✗

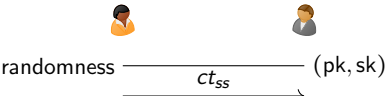
Ring Signature

Building Blocks

Diffie–Hellman (DH)

$B^a \leftarrow$ shared secret $\rightarrow A^b$

Key Encapsulation Mechanism (KEM)



session key $\leftarrow \mathsf{KDF}(\text{secrets})$

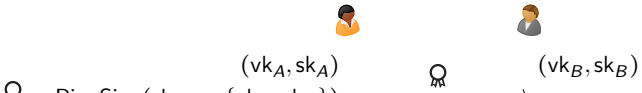
	classical	post-quantum
confidentiality	✓	✗
authentication	(✓)	✗

	classical	post-quantum
confidentiality	✓	✓
authentication	(✓)	(✓)

Signature

	classical	post-quantum
authentication	✓	✓
deniability	✗	✗

Ring Signature



Building Blocks

Diffie–Hellman (DH)

$B^a \leftarrow$ shared secret $\rightarrow A^b$

	classical	post-quantum
confidentiality	✓	✗
authentication	(✓)	✗

Key Encapsulation Mechanism (KEM)

$ss \leftarrow$ shared secret $\rightarrow ss$

session key $\leftarrow$ KDF(secrets)

	classical	post-quantum
confidentiality	✓	✓
authentication	(✓)	(✓)

Signature

	classical	post-quantum
authentication	✓	✓
deniability	✗	✗

Ring Signature

Building Blocks

Diffie–Hellman (DH)

$B^a \leftarrow$ shared secret $\rightarrow A^b$

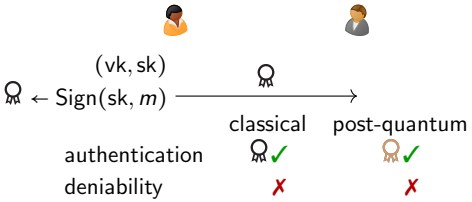
	classical	post-quantum
confidentiality	✓	✗
authentication	(✓)	✗

Key Encapsulation Mechanism (KEM)

session key $\leftarrow$ KDF(secrets)

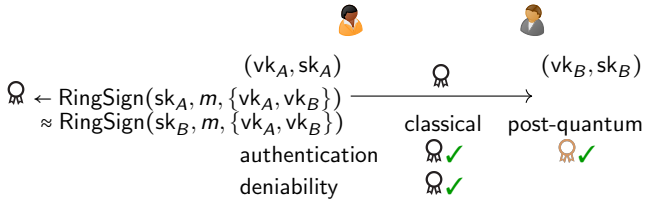
	classical	post-quantum
confidentiality	✓	✓
authentication	(✓)	(✓)

Signature



	classical	post-quantum
authentication	✓	✓
deniability	✗	✗

Ring Signature



	classical	post-quantum
authentication	✓	✓
deniability	✓	

The initial handshake so far: X3DH

long-term (A, a)

ephemeral (X, x)

(B, b) long-term

(S, s) semi-static

(Y, y) ephemeral

The initial handshake so far: X3DH

long-term (A, a)

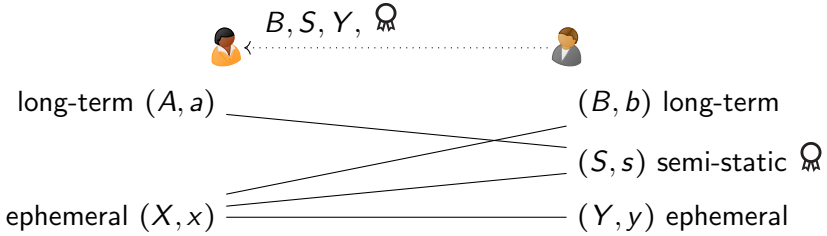
ephemeral (X, x)

(B, b) long-term

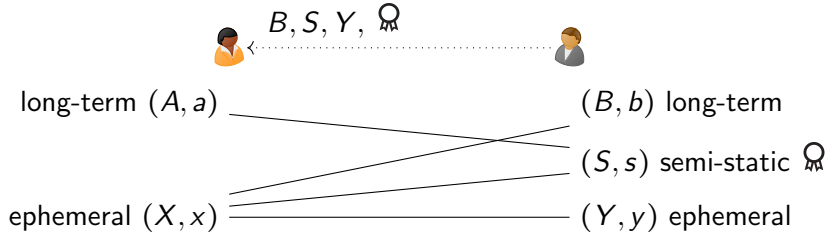
(S, s) semi-static

(Y, y) ephemeral

The initial handshake so far: X3DH

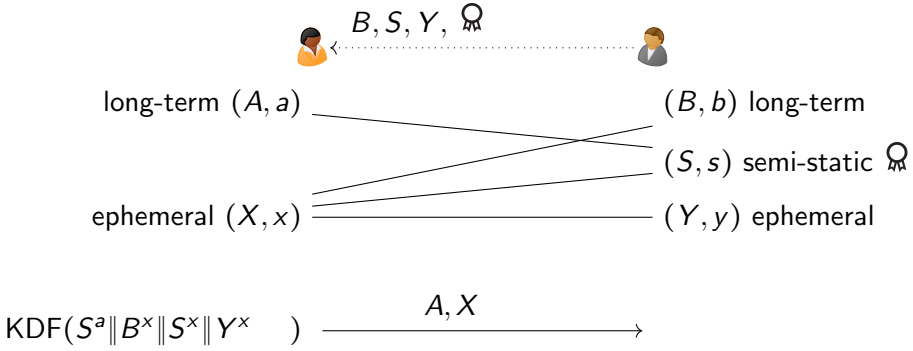


The initial handshake so far: X3DH

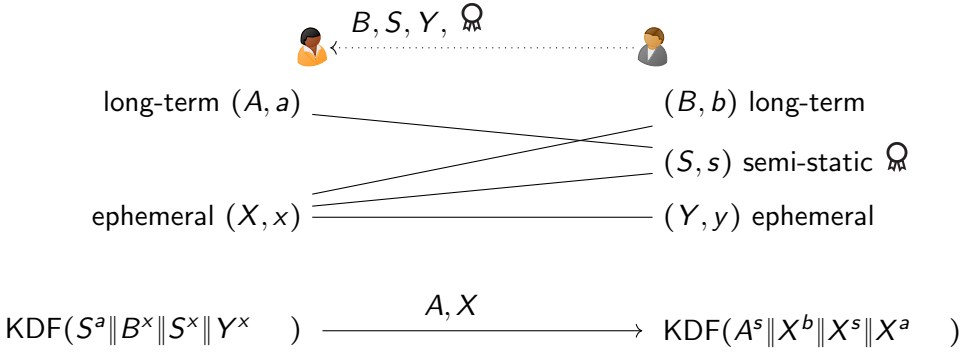


$\mathrm{KDF}(S^a \| B^x \| S^x \| Y^x \quad)$

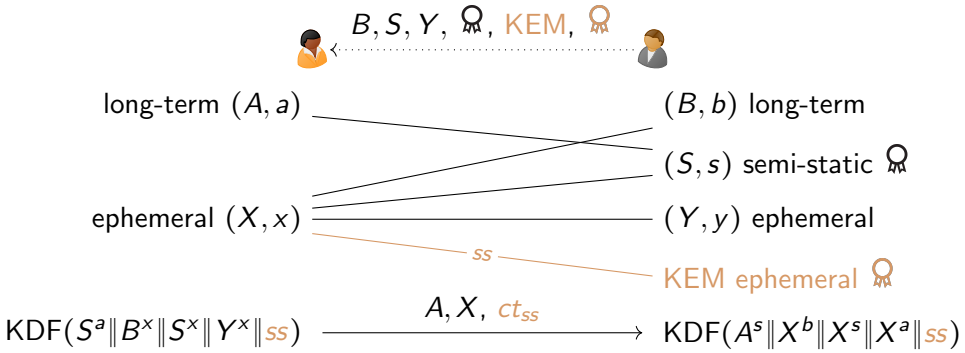
The initial handshake so far: X3DH



The initial handshake so far: X3DH

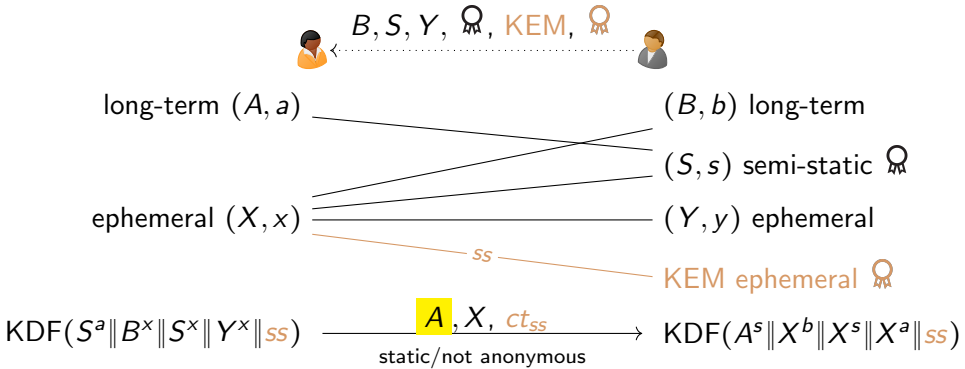


The initial handshake so far: X3DH and PQXDH



Anonymity of the Handshake

Anonymity of handshake?



Sealed Sender: Hiding A's identity

long-term (A, a)

(B, b) long-term

$$m = (A, X, ct_{ss}) \longrightarrow$$

Sealed Sender: Hiding A's identity

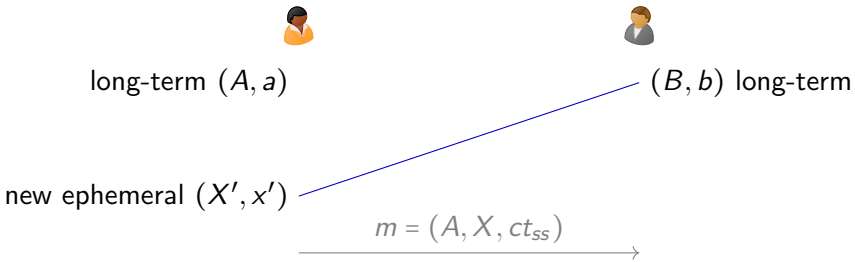
long-term (A, a)

(B, b) long-term

new ephemeral (X', x')

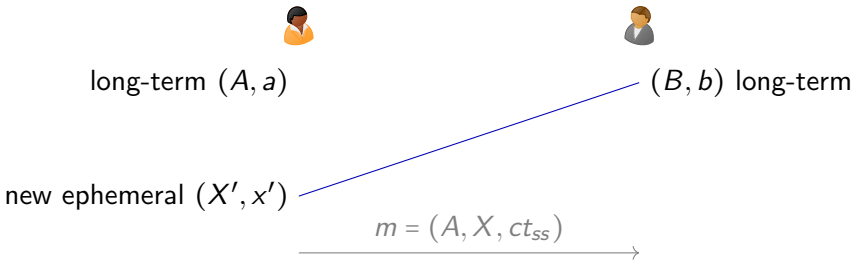
$m = (A, X, ct_{ss})$

Sealed Sender: Hiding A's identity



$CK \| k_A \leftarrow \mathsf{KDF}(\mathrm{eph.\&long})$

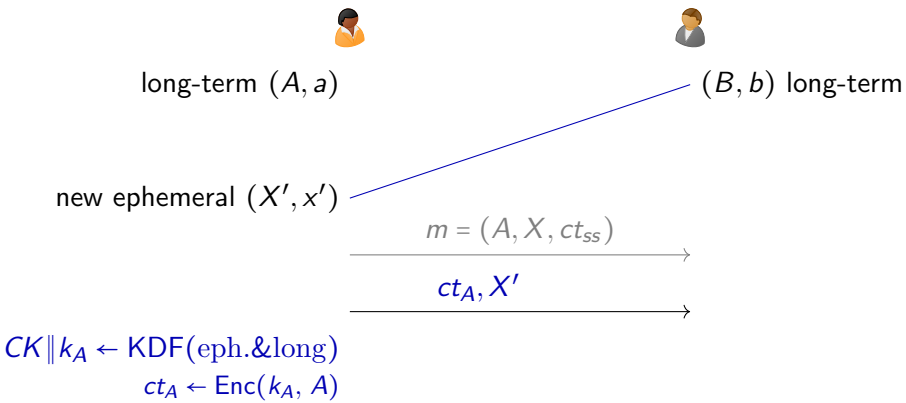
Sealed Sender: Hiding A's identity



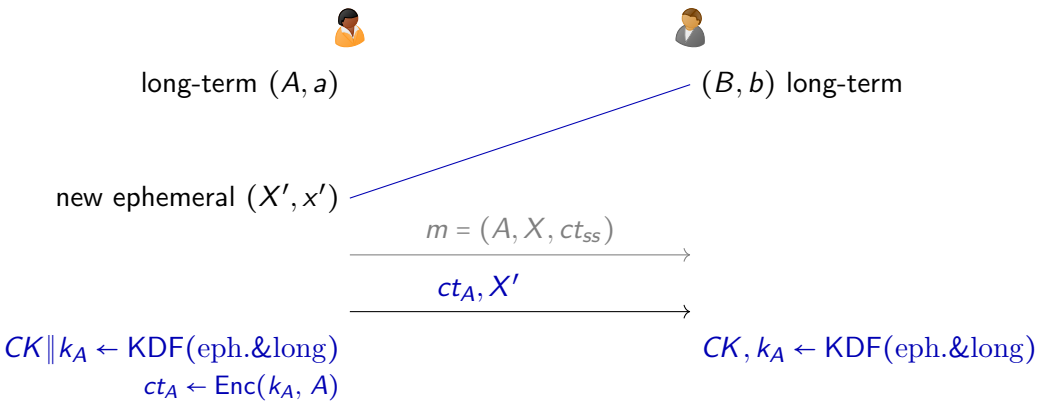
$CK \| k_A \leftarrow \mathsf{KDF}(\mathrm{eph.\&long})$

$ct_A \leftarrow \mathsf{Enc}(k_A, A)$

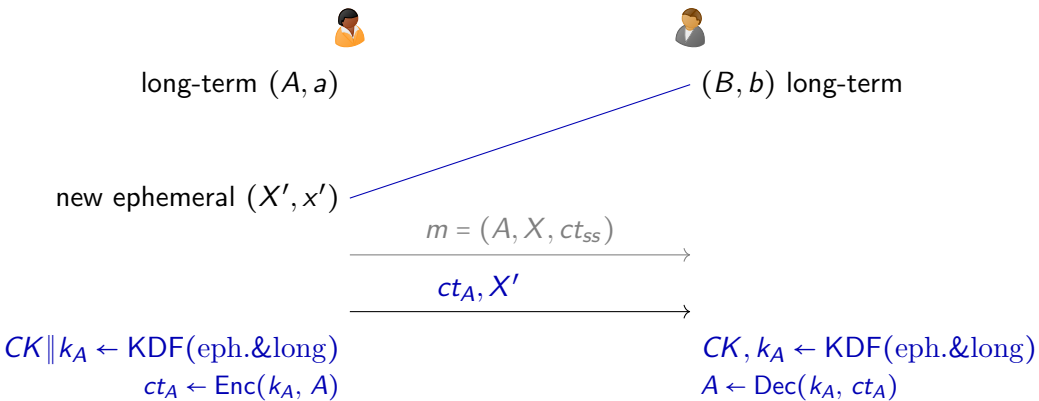
Sealed Sender: Hiding A's identity



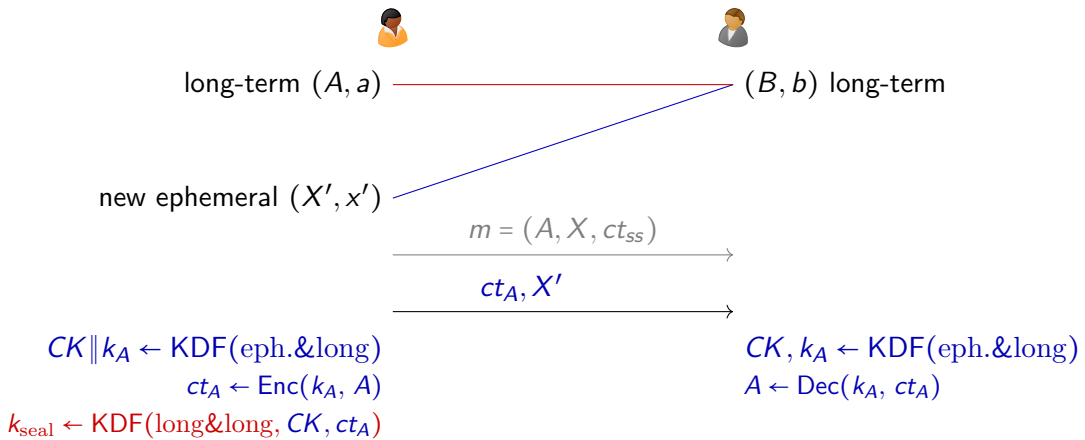
Sealed Sender: Hiding A's identity



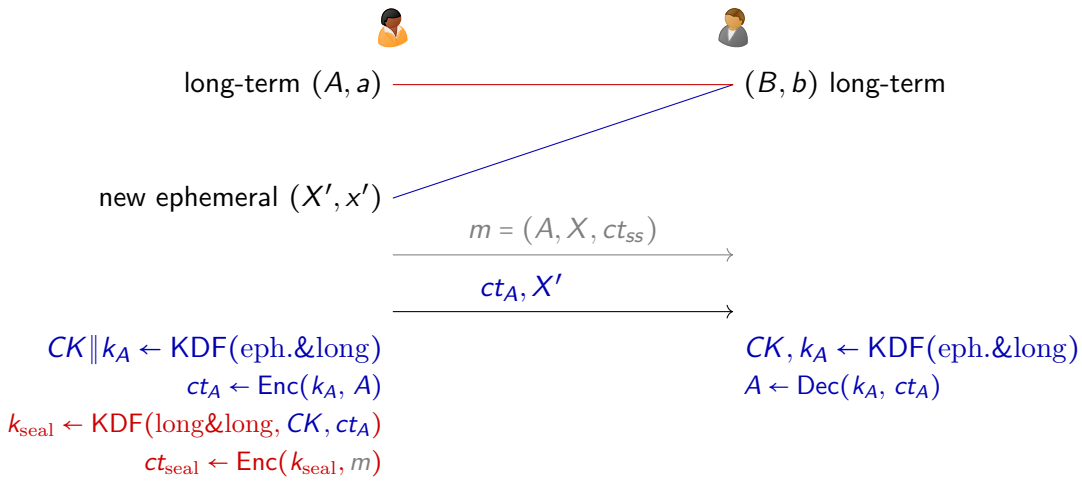
Sealed Sender: Hiding A's identity



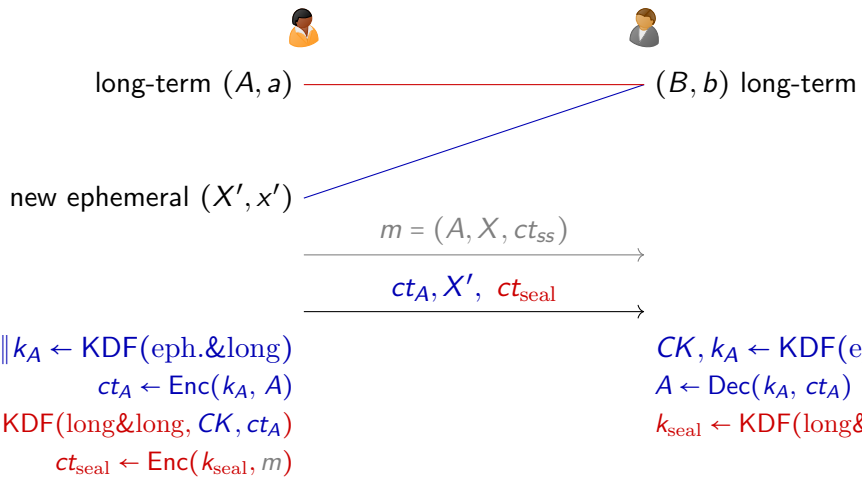
Sealed Sender: Hiding A's identity



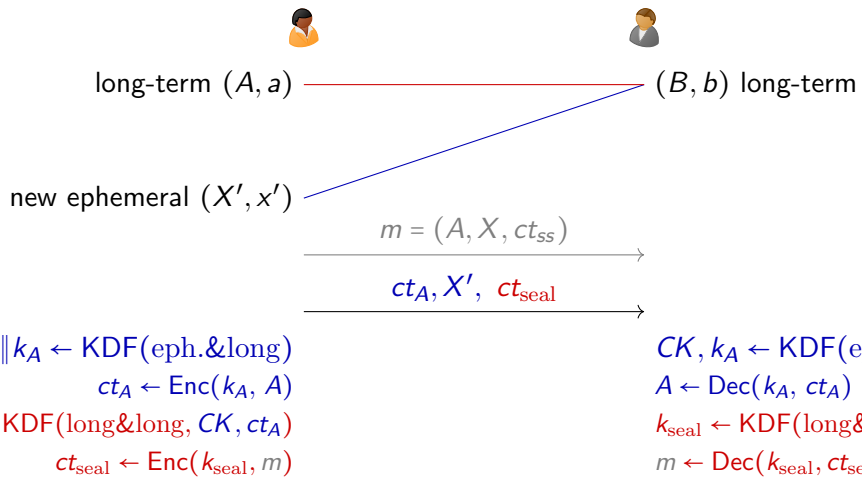
Sealed Sender: Hiding A's identity



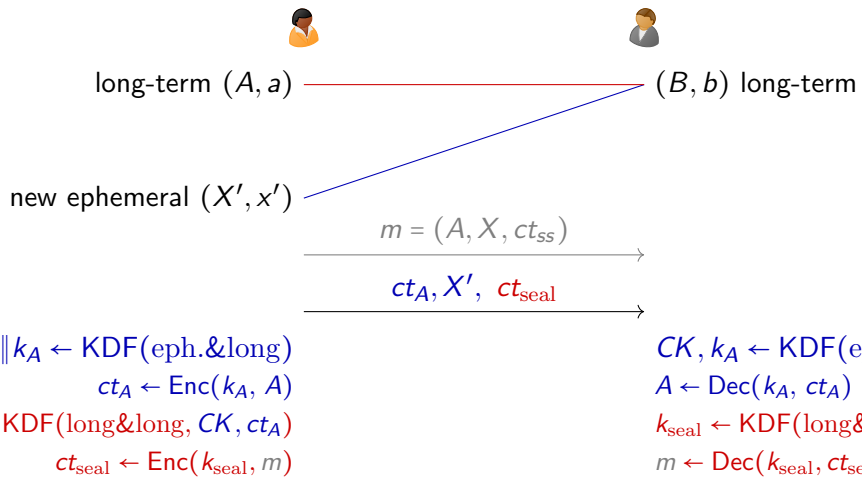
Sealed Sender: Hiding A's identity



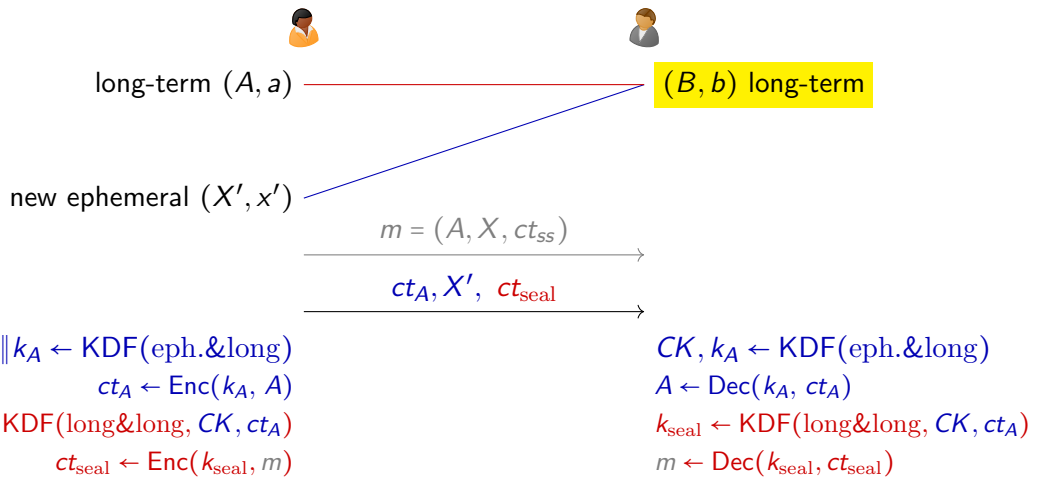
Sealed Sender: Hiding A's identity



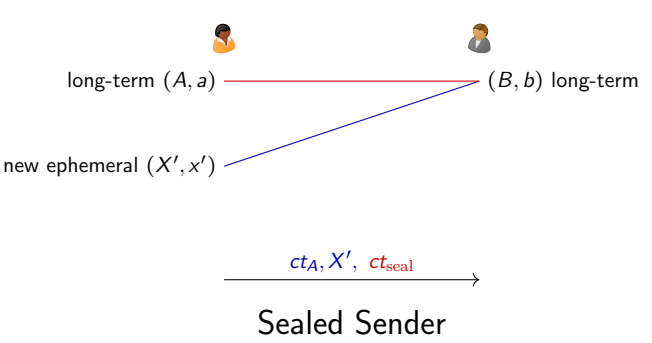
Sealed Sender Problems: Not PQ secure

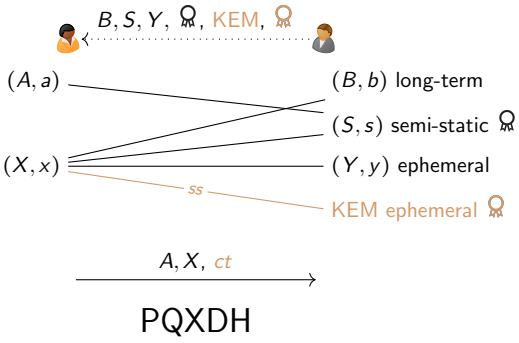


Sealed Sender Problems: Not PQ secure & no compromise anonymity

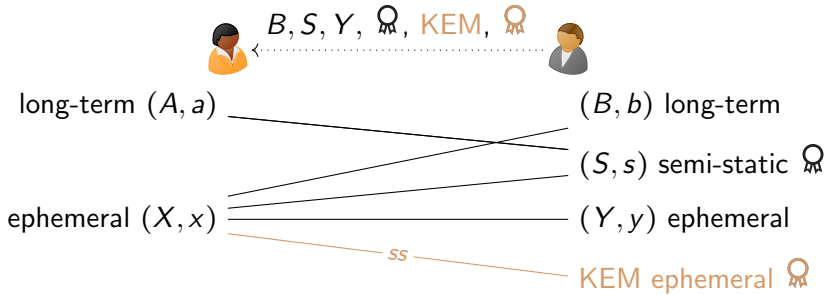


More Sealed Sender Problems: Redundancy in combinations

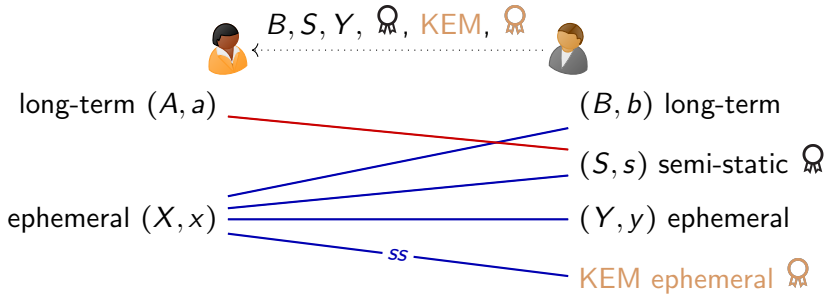




Sender anonymous PQXDH handshake



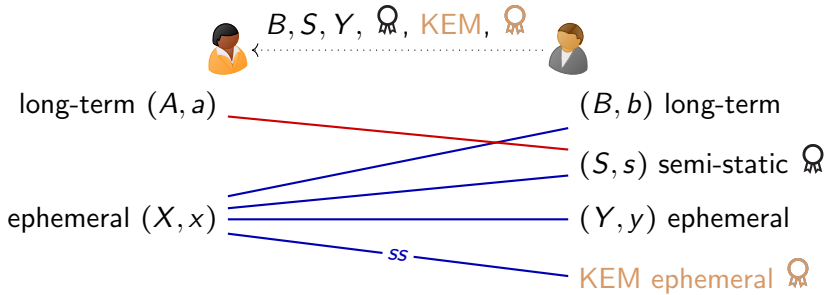
Sender anonymous PQXDH handshake



Phase 1: ephemeral-only → no A

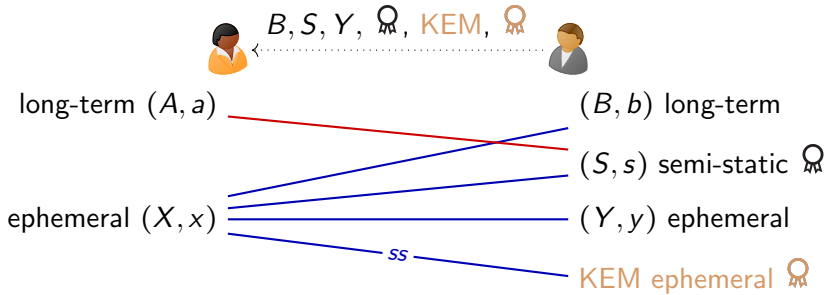
Phase 2: S^a is the *only* DH touching A

Sender anonymous PQXDH handshake



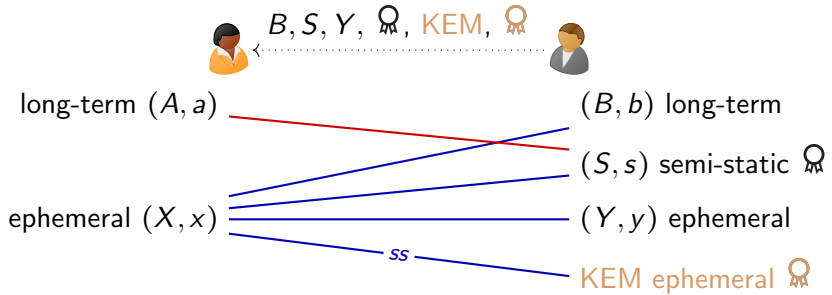
$CK \| K_{\text{seal}} \leftarrow \text{KDF}(B^x \| S^x \| Y^x \| ss \| X \| ct_{ss})$

Sender anonymous PQXDH handshake



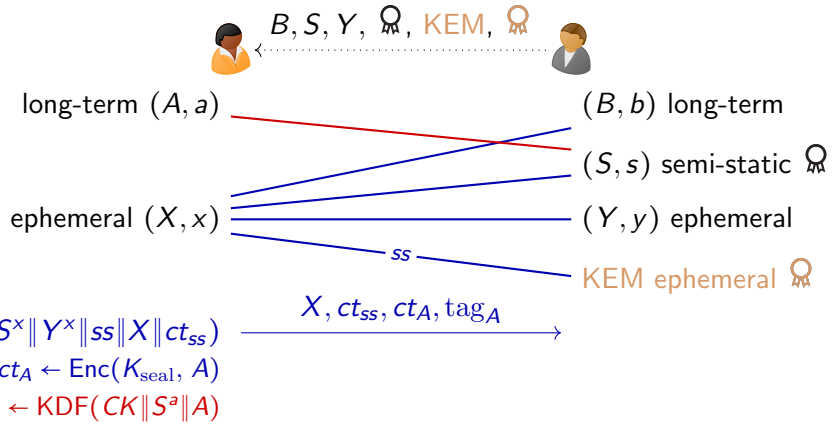
$$CK \| K_{\text{seal}} \leftarrow \text{KDF}(B^x \| S^x \| Y^x \| ss \| X \| ct_{ss})$$
$$ct_A \leftarrow \text{Enc}(K_{\text{seal}}, A)$$

Sender anonymous PQXDH handshake

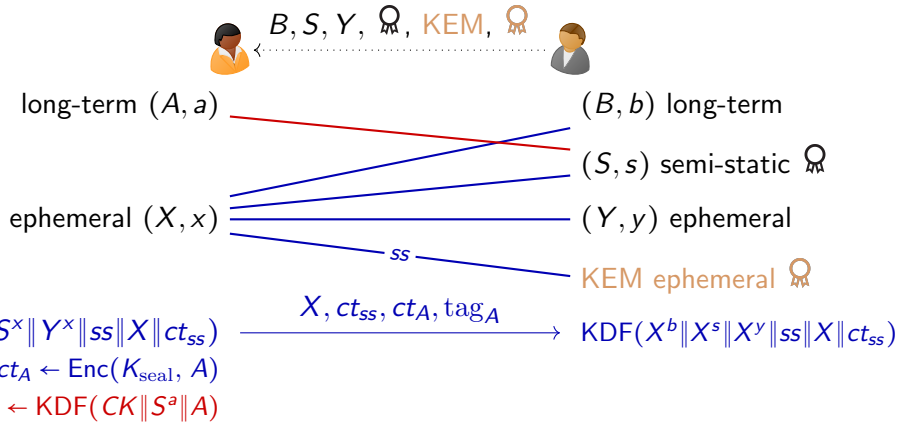


$$CK \| K_{\text{seal}} \leftarrow \text{KDF}(B^x \| S^x \| Y^x \| ss \| X \| ct_{ss})$$
$$ct_A \leftarrow \text{Enc}(K_{\text{seal}}, A)$$
$$k \| \text{tag}_A \leftarrow \text{KDF}(CK \| S^a \| A)$$

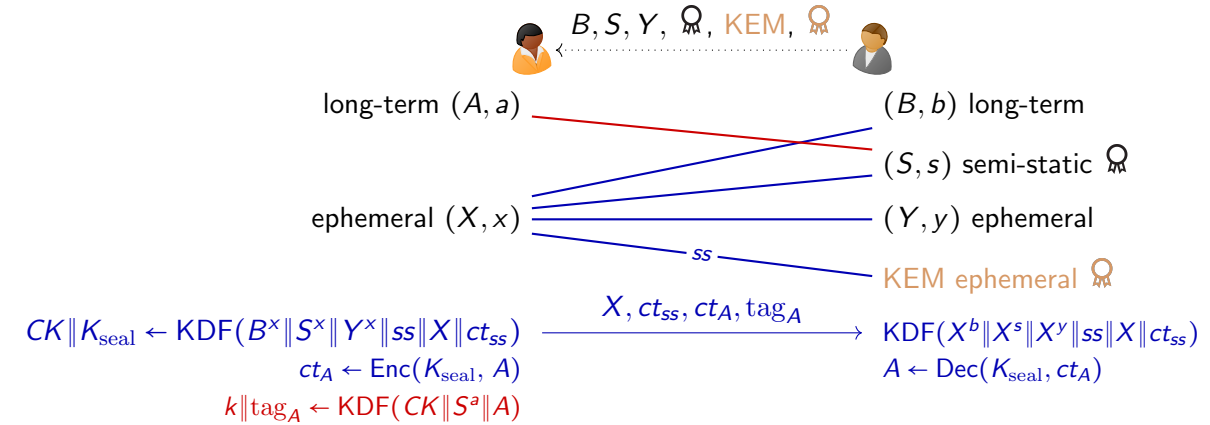
Sender anonymous PQXDH handshake



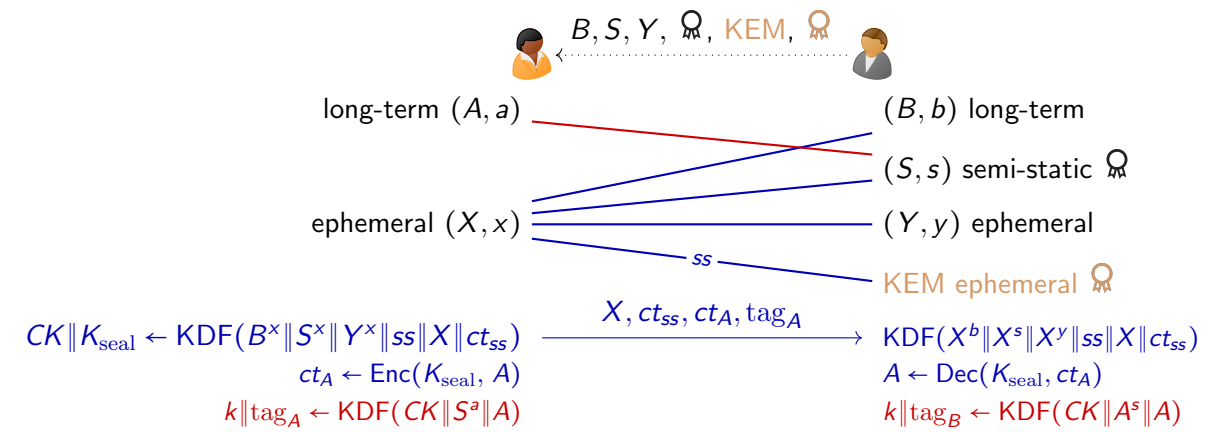
Sender anonymous PQXDH handshake



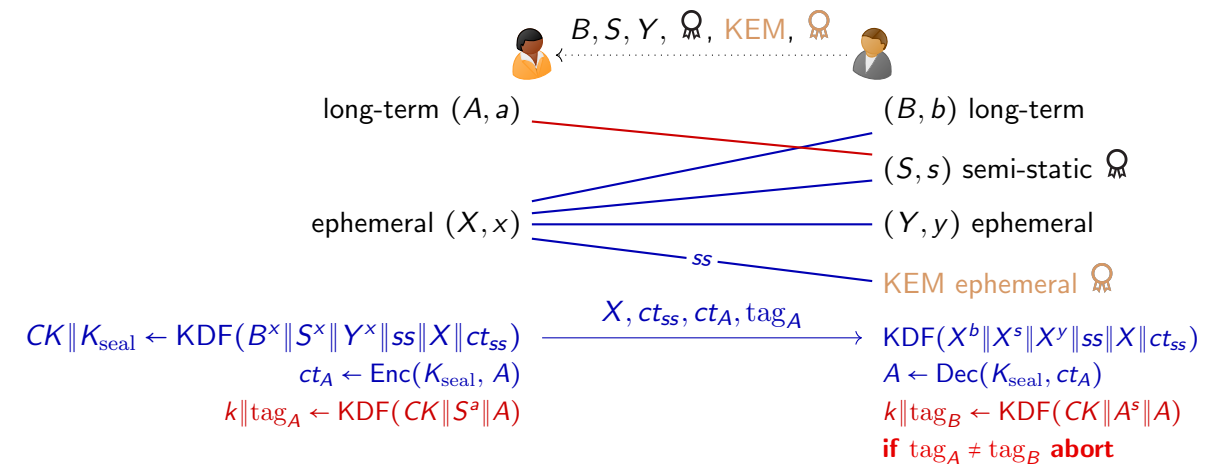
Sender anonymous PQXDH handshake



Sender anonymous PQXDH handshake



Sender anonymous PQXDH handshake



Sender anonymous PQXDH handshake

This is
Sealed PQXDH

long-term (A, a)

ephemeral (X, x)

(B, b) long-term

(S, s) semi-static

(Y, y) ephemeral

ss

KEM ephemeral

$X, ct_{ss}, ct_A, \mathrm{tag}_A$

$CK \| K_{\mathrm{seal}} \leftarrow \mathrm{KDF}(B^x \| S^x \| Y^x \| ss \| X \| ct_{ss})$

$ct_A \leftarrow \mathrm{Enc}(K_{\mathrm{seal}}, A)$

$k \| \mathrm{tag}_A \leftarrow \mathrm{KDF}(CK \| S^a \| A)$

$\mathrm{KDF}(X^b \| X^s \| X^y \| ss \| X \| ct_{ss})$

$A \leftarrow \mathrm{Dec}(K_{\mathrm{seal}}, ct_A)$

$k \| \mathrm{tag}_B \leftarrow \mathrm{KDF}(CK \| A^s \| A)$

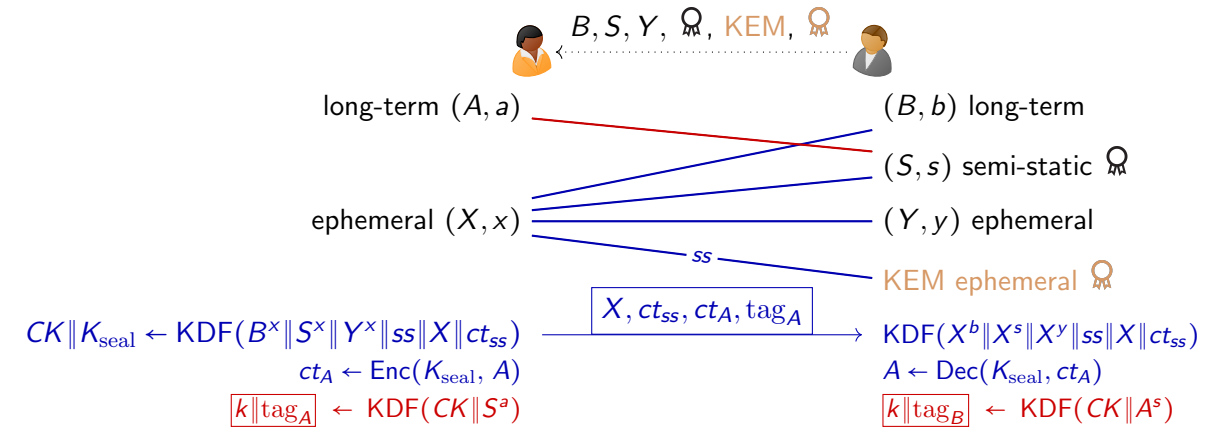
if $\mathrm{tag}_A \neq \mathrm{tag}_B$ **abort**

Better Guarantees, Less Cost

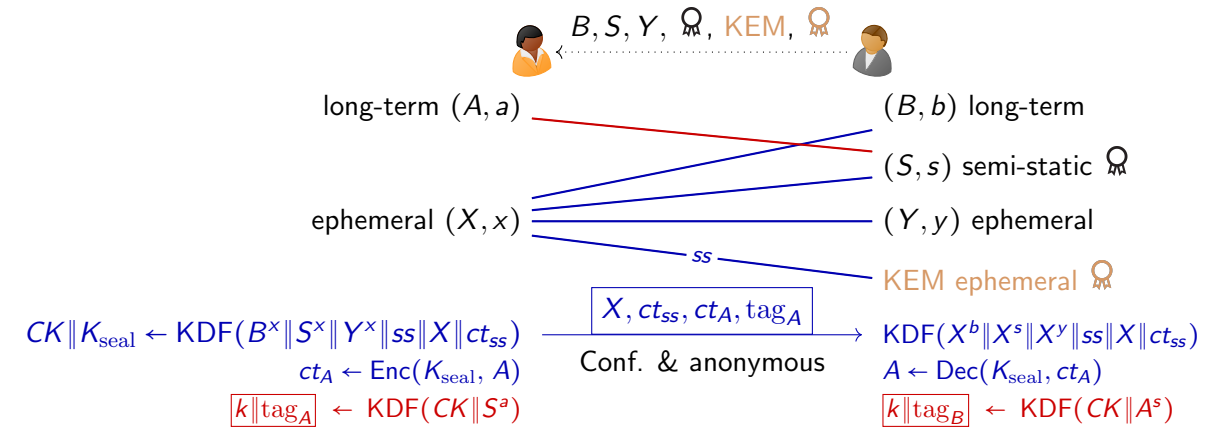
Scheme	Anonymity (post-quantum)	Forward Anonymity (post-quantum)	Compute	Communication
PQXDH	✗✗	✗✗	100%	100%
X3DH + Sealed Sender	✗	✗✗	119%	32%
PQXDH + Sealed Sender	✗	✗✗	140%	121%
Sealed PQXDH	✓	✓	101%	116%

- SPQXDH gets classical and PQ anonymity, forward anonymity, at the cost of one KDF call compared to PQXDH.
- Allows elimination of Sealed Sender, reducing cost and complexity over today's deployment.
- **We are building it.**

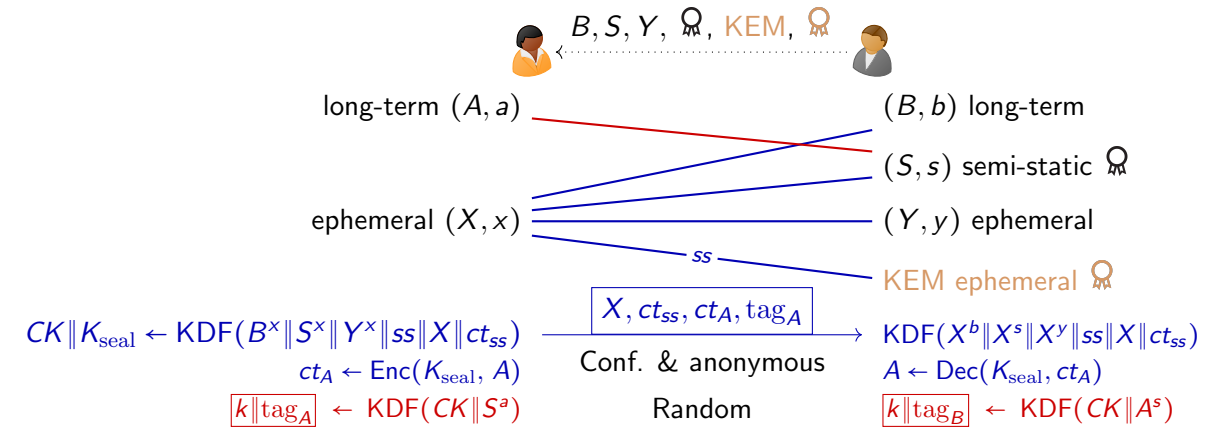
A note on security proofs: Sender anonymous key exchange & modularity



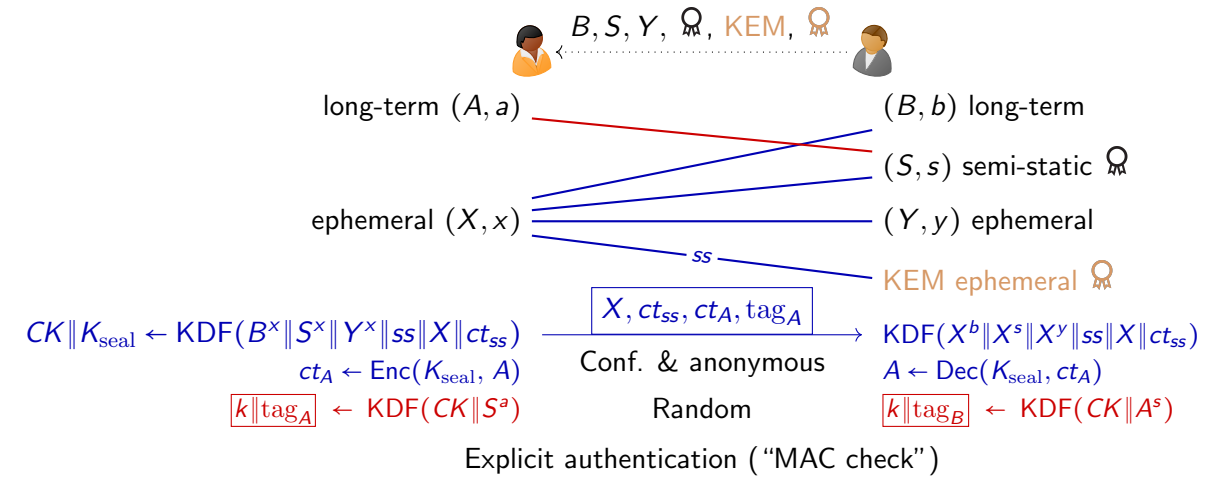
A note on security proofs: Sender anonymous key exchange & modularity



A note on security proofs: Sender anonymous key exchange & modularity

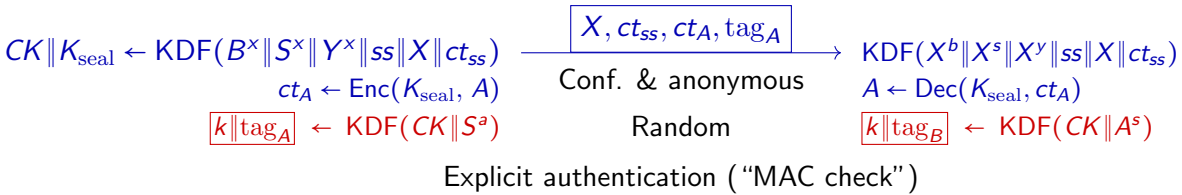


A note on security proofs: Sender anonymous key exchange & modularity



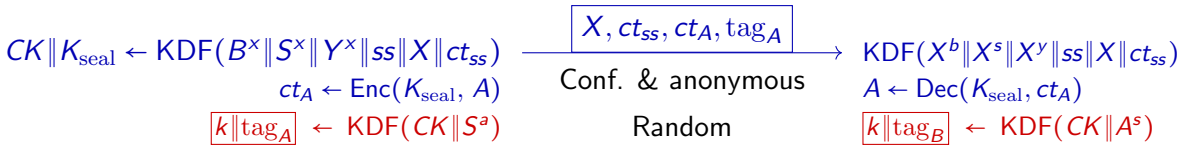
A note on security proofs: Sender anonymous key exchange & modularity

- Top-level: Model full protocol as sender anonymous key exchange



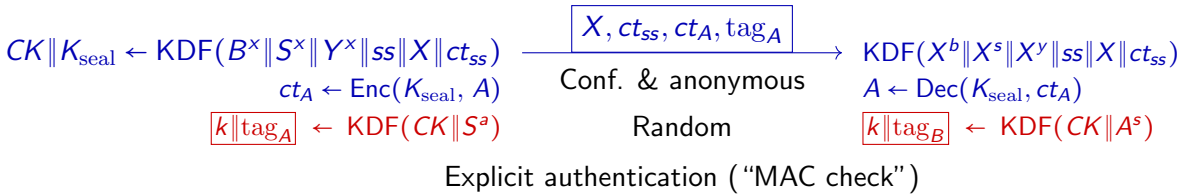
A note on security proofs: Sender anonymous key exchange & modularity

- Top-level: Model full protocol as sender anonymous key exchange
- Low-level: Model functional blocks (blue/red) as multi-key split KEM



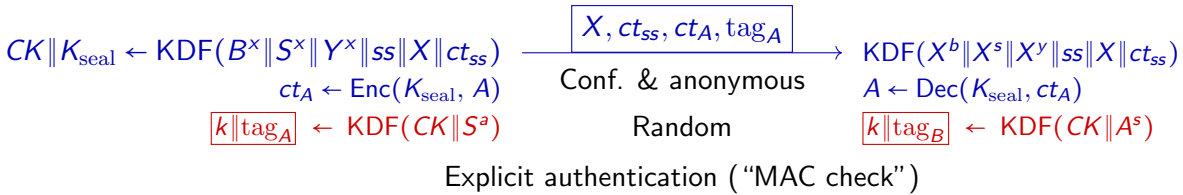
A note on security proofs: Sender anonymous key exchange & modularity

- Top-level: Model full protocol as sender anonymous key exchange
- Low-level: Model functional blocks (blue/red) as multi-key split KEM
  - Security: Ciphertext anonymous & key random & implicit authentication



A note on security proofs: Sender anonymous key exchange & modularity

- Top-level: Model full protocol as sender anonymous key exchange
- Low-level: Model functional blocks (blue/red) as multi-key split KEM
  - Security: Ciphertext anonymous & key random & implicit authentication
  - As long as one input key is uncorrupted



Post-quantum confidentiality + authentication

Status quo of post-quantum security of the handshake

		post-quantum				
Scheme	confidentiality	FS	mutual auth	Anonymity	FA	Deniability
X3DH	✗	✗	✗	✗✗	✗✗	✓
PQXDH	(✓)	(✓)	✗	✗✗	✗✗	✓

Towards a Post-Quantum Handshake [HKW25]

Goal: X3DH properties, but **post-quantum**.
Challenge: no PQ non-interactive key exchange.

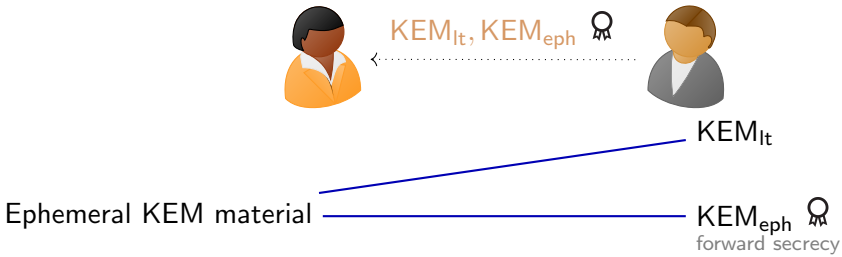
Towards a Post-Quantum Handshake [HKW25]

$\mathsf{KEM}_{\mathsf{lt}}$
receiver auth
long-term secrecy

Ephemeral KEM material

(1) $(ct_1, ss_1) \leftarrow \mathsf{Encaps}(\mathsf{KEM}_{\mathsf{lt}})$

Towards a Post-Quantum Handshake [HKW25]



(1) $(ct_1, ss_1) \leftarrow \text{Encaps}(KEM_{lt})$

(2) $(ct_2, ss_2) \leftarrow \text{Encaps}(KEM_{eph})$

Towards a Post-Quantum Handshake [HKW25]

No sender identity (or auth) involved!

$\mathsf{KEM}_{\mathsf{lt}}$

Ephemeral KEM material

$\mathsf{KEM}_{\mathsf{eph}}$

(1) $(ct_1, ss_1) \leftarrow \mathsf{Encaps}(\mathsf{KEM}_{\mathsf{lt}})$

(2) $(ct_2, ss_2) \leftarrow \mathsf{Encaps}(\mathsf{KEM}_{\mathsf{eph}})$

$K? \leftarrow \mathsf{KDF}(ss_1 \| ss_2 \| \mathrm{context})$

Towards a Post-Quantum Handshake [HKW25]

signing key

$\Rightarrow$ sender auth, but not deniable

Ephemeral KEM material

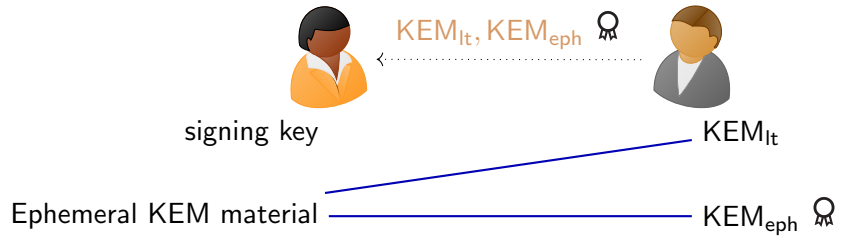
$\mathsf{KEM}_{\mathsf{lt}}$

$\mathsf{KEM}_{\mathsf{eph}}$

(1) $(ct_1, ss_1) \leftarrow \mathsf{Encaps}(\mathsf{KEM}_{\mathsf{lt}})$

(2) $(ct_2, ss_2) \leftarrow \mathsf{Encaps}(\mathsf{KEM}_{\mathsf{eph}})$

Towards a Post-Quantum Handshake [HKW25]



(1) $(ct_1, ss_1) \leftarrow \mathsf{Encaps}(\mathsf{KEM}_{\mathsf{lt}})$

(2) $(ct_2, ss_2) \leftarrow \mathsf{Encaps}(\mathsf{KEM}_{\mathsf{eph}})$

(3) $\sigma \leftarrow \mathsf{Sign}(sk_A, ctx)$

$K \| K_{\mathrm{seal}} \leftarrow \mathsf{KDF}(ss_1 \| ss_2 \| \sigma \| \mathrm{context})$

$ct_A \leftarrow \mathsf{Enc}(K_{\mathrm{seal}}, (VK_A, \sigma))$

Towards a Post-Quantum Handshake [HKW25]

$\mathsf{KEM}_{\mathsf{lt}}, \mathsf{KEM}_{\mathsf{eph}}$

signing key

$\mathsf{KEM}_{\mathsf{lt}}$

Ephemeral KEM material

$\mathsf{KEM}_{\mathsf{eph}}$

ct_1, ct_2, ct_A

(1) $(ct_1, ss_1) \leftarrow \mathsf{Encaps}(\mathsf{KEM}_{\mathsf{lt}})$

(2) $(ct_2, ss_2) \leftarrow \mathsf{Encaps}(\mathsf{KEM}_{\mathsf{eph}})$

(3) $\sigma \leftarrow \mathsf{Sign}(sk_A, ctx)$

$K \| K_{\mathrm{seal}} \leftarrow \mathsf{KDF}(ss_1 \| ss_2 \| \sigma \| \mathrm{context})$

$ct_A \leftarrow \mathsf{Enc}(K_{\mathrm{seal}}, (VK_A, \sigma))$

(1) $ss_1 \leftarrow \mathsf{Decaps}(\mathsf{KEM}_{\mathsf{lt}}, ct_1)$

(2) $ss_2 \leftarrow \mathsf{Decaps}(\mathsf{KEM}_{\mathsf{eph}}, ct_2)$

$K \| K_{\mathrm{seal}} \leftarrow \mathsf{KDF}(ss_1 \| ss_2 \| \sigma \| \mathrm{context}$

$(VK_A, \sigma) \leftarrow \mathit{Dec}(K_{\mathrm{seal}}, ct_A)$

Verify σ, return K

Towards a Post-Quantum Handshake [HKW25]

SignXKEM
complete, but
missing deniability

$\mathsf{KEM}_{\mathsf{lt}}, \mathsf{KEM}_{\mathsf{eph}}$

signing key

$\mathsf{KEM}_{\mathsf{lt}}$

Ephemeral KEM material

$\mathsf{KEM}_{\mathsf{eph}}$

ct_1, ct_2, ct_A

(1) $(ct_1, ss_1) \leftarrow \mathsf{Encaps}(\mathsf{KEM}_{\mathsf{lt}})$

(2) $(ct_2, ss_2) \leftarrow \mathsf{Encaps}(\mathsf{KEM}_{\mathsf{eph}})$

(3) $\sigma \leftarrow \mathsf{Sign}(sk_A, ctx)$

$K \| K_{\mathrm{seal}} \leftarrow \mathsf{KDF}(ss_1 \| ss_2 \| \sigma \| \mathrm{context})$

$ct_A \leftarrow \mathsf{Enc}(K_{\mathrm{seal}}, (VK_A, \sigma))$

(1) $ss_1 \leftarrow \mathsf{Decaps}(\mathsf{KEM}_{\mathsf{lt}}, ct_1)$

(2) $ss_2 \leftarrow \mathsf{Decaps}(\mathsf{KEM}_{\mathsf{eph}}, ct_2)$

$K \| K_{\mathrm{seal}} \leftarrow \mathsf{KDF}(ss_1 \| ss_2 \| \sigma \| \mathrm{context}$

$(VK_A, \sigma) \leftarrow \mathit{Dec}(K_{\mathrm{seal}}, ct_A)$

Verify σ, return K

From SignXKEM to RingXKEM [HKW25, KNTW25]

signing key — lt-KEM

Ephemeral KEM material — signed prekey

$ct_1, ct_2, \mathrm{Enc}(\sigma)$

(1) $(ct_1, ss_1) \leftarrow$ Encaps(lt-KEM)

(2) $(ct_2, ss_2) \leftarrow$ Encaps(signed prekey)

(3) ~~$\sigma \leftarrow \mathrm{Sign}(sk_A, ctx)$~~

σ proves Alice initiated

$K \| K_{\mathrm{seal}} \leftarrow \mathrm{KDF}(ss_1 \| ss_2 \| \sigma \| \mathrm{context})$

$ct_A \leftarrow \mathrm{Enc}(K_{\mathrm{seal}}, (VK_A, \sigma))$

(1) $ss_1 \leftarrow$ Decaps(lt-KEM, ct_1)

(2) $ss_2 \leftarrow$ Decaps(signed prekey, ct_2)

$K \| K_{\mathrm{seal}} \leftarrow \mathrm{KDF}(ss_1 \| ss_2 \| \sigma \| \mathrm{context})$

$(VK_A, \sigma) \leftarrow Dec(K_{\mathrm{seal}}, ct_A)$

Verify σ, return K

From SignXKEM to RingXKEM [HKW25, KNTW25]

signing key — lt-KEM

Ephemeral KEM material — signed prekey

$ct_1, ct_2, \mathsf{Enc}(\sigma)$

(1) $(ct_1, ss_1) \leftarrow \mathsf{Encaps}(\text{lt-KEM})$

(2) $(ct_2, ss_2) \leftarrow \mathsf{Encaps}(\text{signed prekey})$

(3) $\sigma \leftarrow \mathsf{RingSign}(sk_A, \{VK_A, VK_B\})$

either party could have signed

$K \| K_{\text{seal}} \leftarrow \mathsf{KDF}(ss_1 \| ss_2 \| \sigma \| \text{context})$

$ct_A \leftarrow \mathsf{Enc}(K_{\text{seal}}, (VK_A, \sigma))$

(1) $ss_1 \leftarrow \mathsf{Decaps}(\text{lt-KEM}, ct_1)$

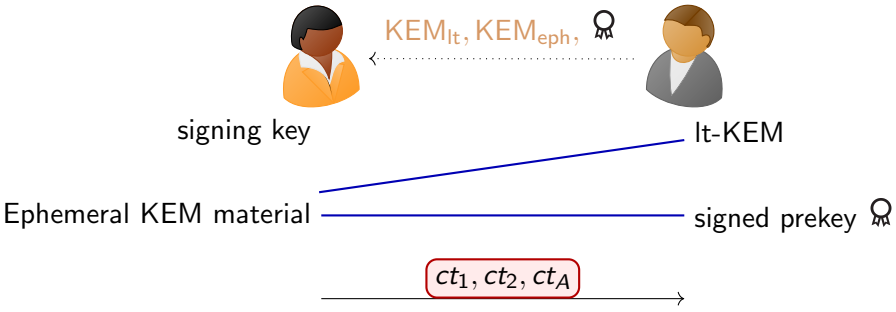
(2) $ss_2 \leftarrow \mathsf{Decaps}(\text{signed prekey}, ct_2)$

$K \| K_{\text{seal}} \leftarrow \mathsf{KDF}(ss_1 \| ss_2 \| \sigma \| \text{context})$

$(VK_A, \sigma) \leftarrow \mathit{Dec}(K_{\text{seal}}, ct_A)$

Verify σ, return K

From SignXKEM to RingXKEM [HKW25, KNTW25]



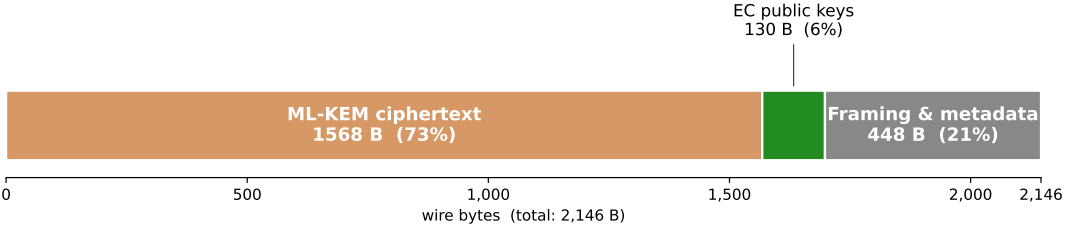
RingXKEM: Summary

	post-quantum					
Scheme	confidentiality	FS	mutual auth	Anonymity	FA	Deniability
X3DH	✗	✗	✗	✗✗	✗✗	✓
PQXDH	(✓)	(✓)	✗	✗✗	✗✗	✓
Sealed PQXDH	(✓)	(✓)	✗	✓	✓	✓
SignXKEM	✓	✓	✓	✓	✓	✗
RingXKEM	✓	✓	✓	✓	✓	✓

But at what cost?!?

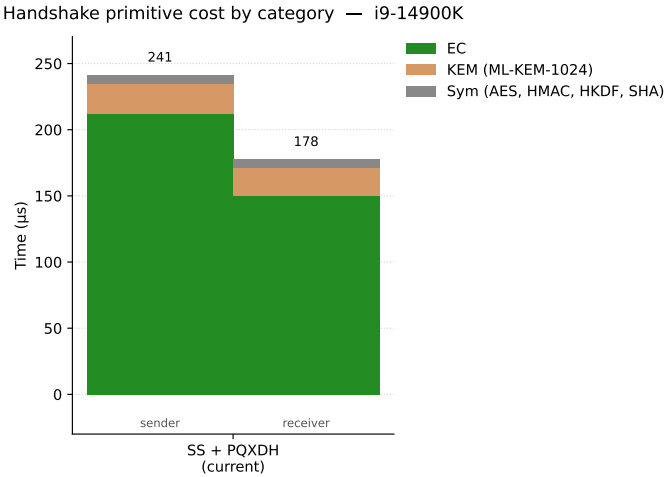
Today: Sealed Sender + PQXDH

A mix of three primitive families: **EC**, **lattice** (ML-KEM-1024), **symmetric** (AES, HMAC, SHA).



ML-KEM is ≈**73%** of what goes on the wire.

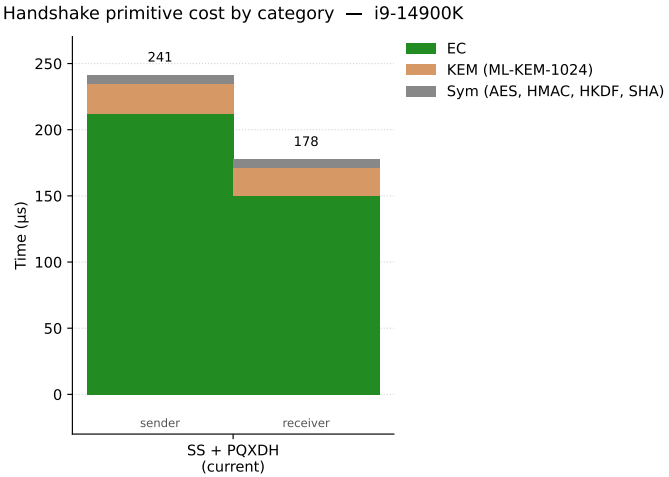
But compute tells a different story



- **EC dominates.**
  88% of sender cost, **85%** of receiver.

i9-14900K, Rust nightly, `--quick` criterion. xEd25519 verify counted as EC.

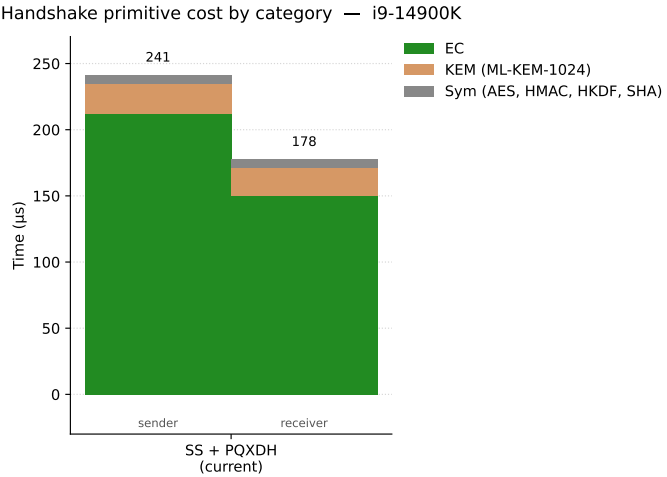
But compute tells a different story



- **EC dominates.**
  88% of sender cost, **85%** of receiver.
- **ML-KEM is fast.**
  Encap $\approx 22\,\mu s$ — *cheaper than a single* X25519 DH ($25\,\mu s$).

i9-14900K, Rust nightly, `--quick` criterion. xEd25519 verify counted as EC.

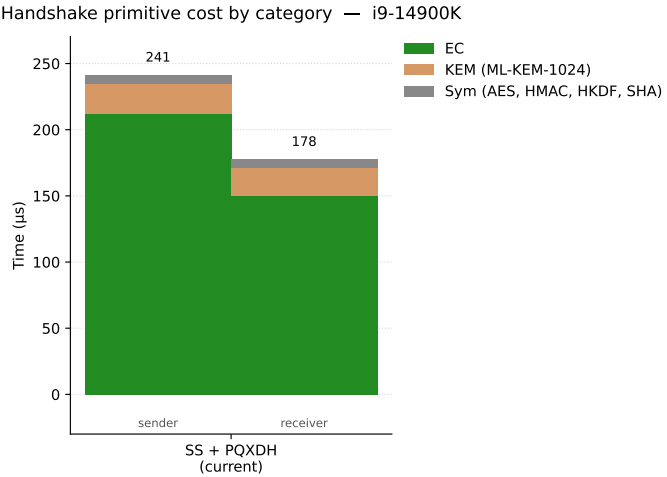
But compute tells a different story



- **EC dominates.**
  88% of sender cost, **85%** of receiver.
- **ML-KEM is fast.**
  Encap $\approx 22\,\mu s$ — *cheaper than a single* X25519 DH ($25\,\mu s$).
- **We do 12 DHs per session.**
  Each one already pricier than the whole ML-KEM operation.

i9-14900K, Rust nightly, `--quick` criterion. xEd25519 verify counted as EC.

But compute tells a different story



- **EC dominates.**
  88% of sender cost, **85%** of receiver.
- **ML-KEM is fast.**
  Encap $\approx 22\,\mu s$ — *cheaper than a single* X25519 DH ($25\,\mu s$).
- **We do 12 DHs per session.**
  Each one already pricier than the whole ML-KEM operation.
- **Can we do better?**

i9-14900K, Rust nightly, `--quick` criterion. xEd25519 verify counted as EC.

Improving the classical handshake: XHMQV

long-term (A, a)

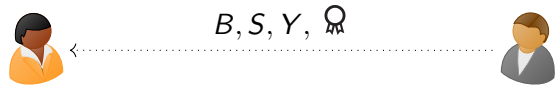
ephemeral (X, x)

(B, b) long-term

(S, s) semi-static

(Y, y) ephemeral

Improving the classical handshake: XHMQV



long-term (A, a)

(B, b) long-term

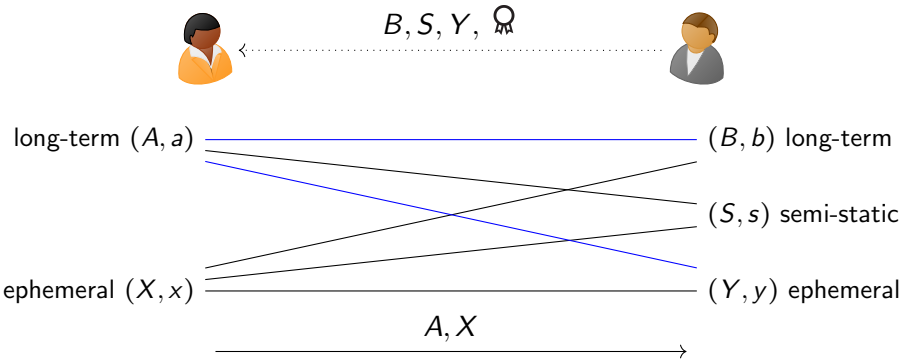
(S, s) semi-static

ephemeral (X, x)

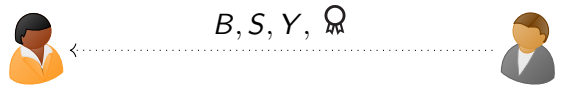
(Y, y) ephemeral

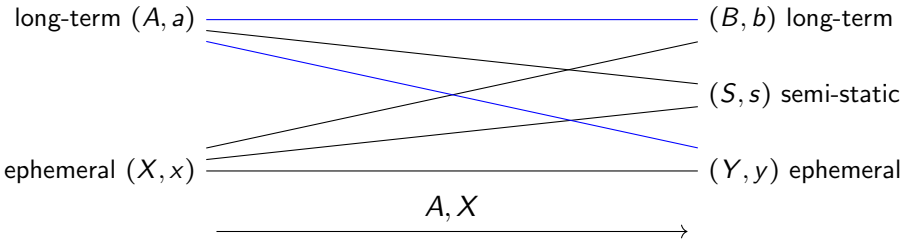
A, X

Improving the classical handshake: XHMQV



Improving the classical handshake: XHMQV



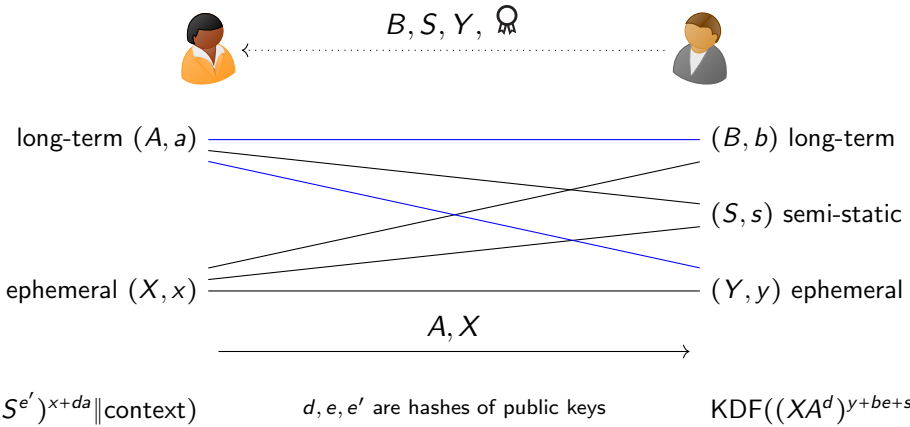


$\mathrm{KDF}((YB^eS^{e'})^{x+da} \| \text{context})$

d, e, e' are hashes of public keys

$\mathrm{KDF}((XA^d)^{y+be+se'} \| \text{context})$

Improving the classical handshake: XHMQV



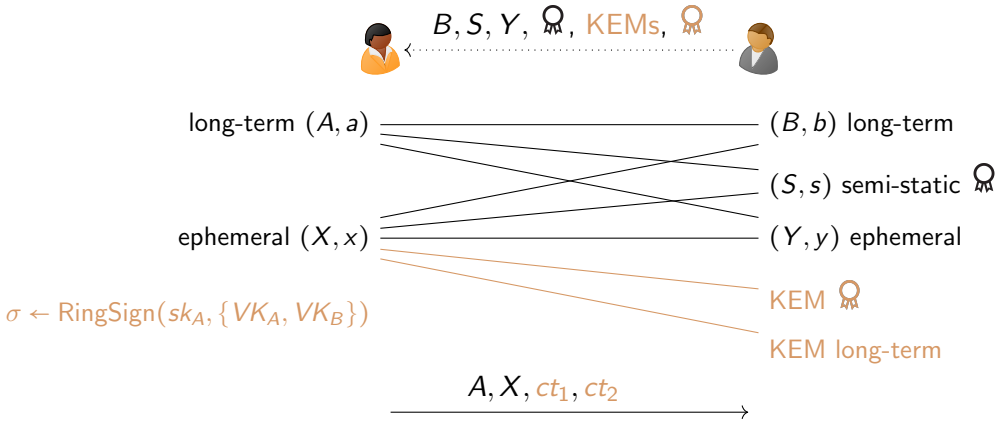
- better efficiency than X3DH: 5 group exponentiations instead of 8
- stronger maximum-exposure security than X3DH: 6 combinations instead of 4
- comparable deniability to X3DH

XHMQV: Security and Efficiency Comparison

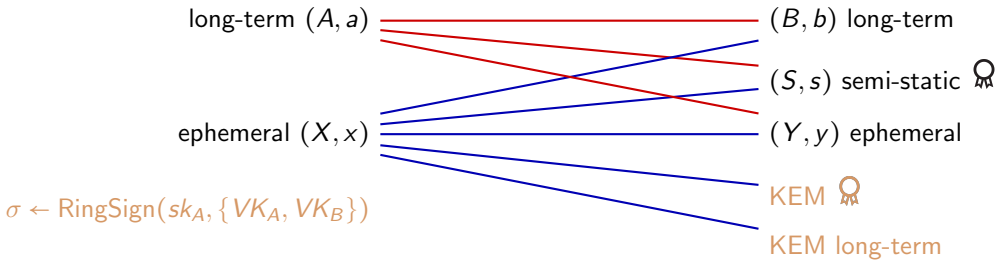
Scheme	#Exp	Combinations contributing to security						Analysis	Key reuse?
		LT-SS	E-LT	E-SS	E-E	LT-LT	LT-E		
X3DH	8 (6)	✓	✓	✓	(✓)	✗	✗	[CCD+17]	✗
XHMQV	5 (4)	✓	✓	✓	(✓)	✓	(✓)	[FGPZ25]	✓

Piecing it all together

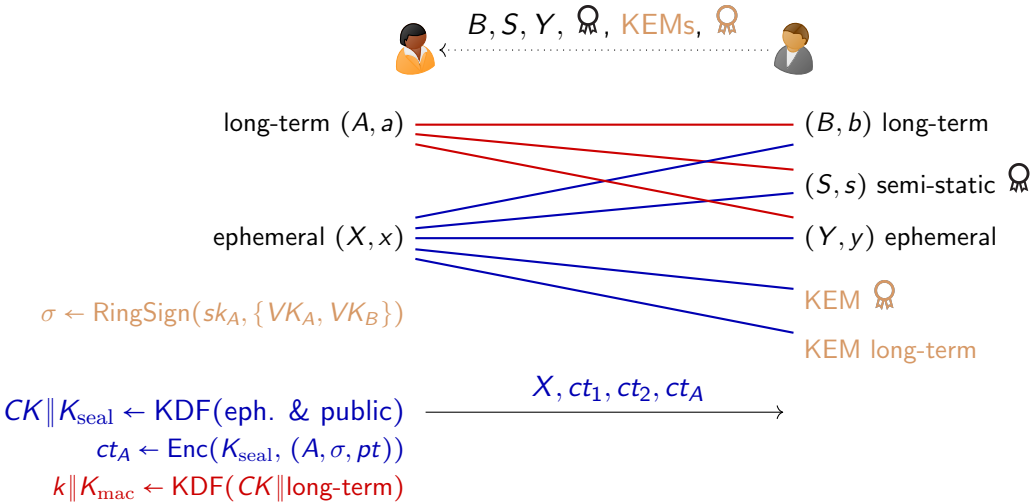
Sealed XHMQV-RingXKEM



Sealed XHMQV-RingXKEM



Sealed XHMQV-RingXKEM



Sealed XHMQV-RingXKEM

long-term (A, a)

ephemeral (X, x)

(B, b) long-term

(S, s) semi-static

(Y, y) ephemeral

KEM

KEM long-term

$\sigma \leftarrow \text{RingSign}(sk_A, \{VK_A, VK_B\})$

X, ct_1, ct_2, ct_A

$CK \| K_{\text{seal}} \leftarrow \text{KDF}(\text{eph. \& public})$

$ct_A \leftarrow \text{Enc}(K_{\text{seal}}, (A, \sigma, pt))$

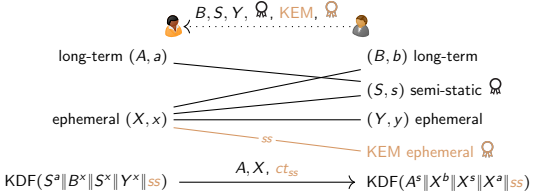
$k \| K_{\text{mac}} \leftarrow \text{KDF}(CK \| \text{long-term})$

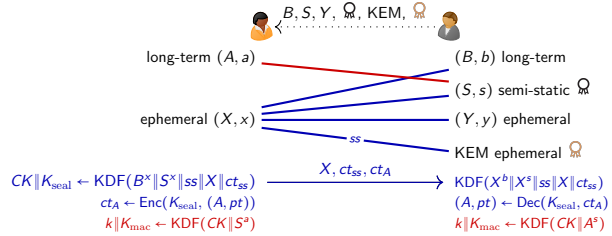
$\text{KDF}(\text{eph. \& public})$

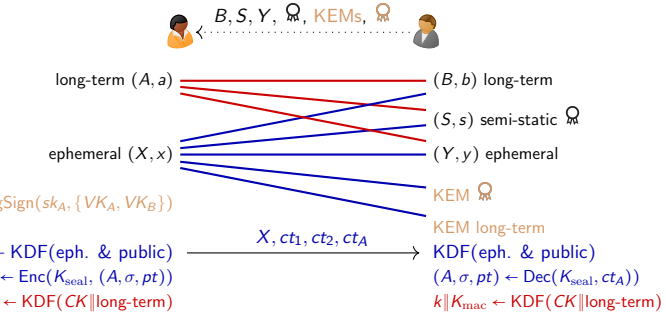
$(A, \sigma, pt) \leftarrow \text{Dec}(K_{\text{seal}}, ct_A))$

$k \| K_{\text{mac}} \leftarrow \text{KDF}(CK \| \text{long-term})$

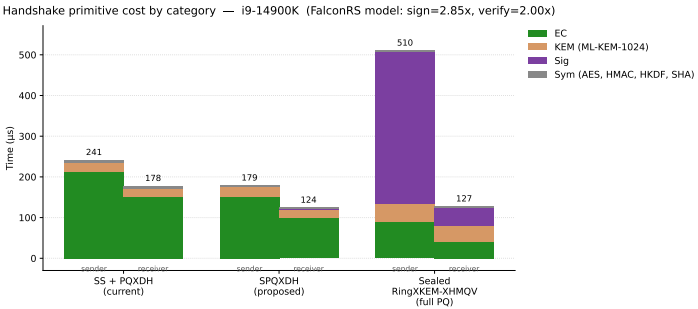
Recap: Three protocols







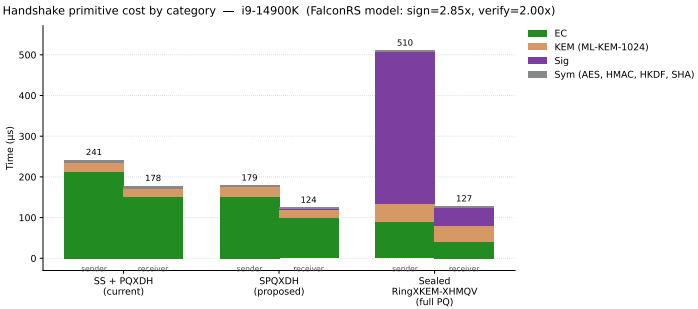
Three protocols side by side



i9-14900K; hybrid ring signature modeled via FalconRS [HKW25, KNTW25] (sign ≈2.85×, verify 2× Falcon-512).

- **SPQXDH: drop-in win.**
  Integrated sealing cuts EC waste. –**26%** sender, –**30%** receiver over SS+PQXDH.

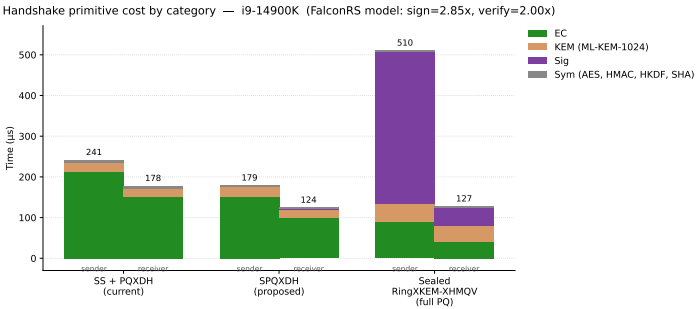
Three protocols side by side



i9-14900K; hybrid ring signature modeled via FalconRS [HKW25, KNTW25] (sign ≈2.85×, verify 2× Falcon-512).

- **SPQXDH: drop-in win.**
  Integrated sealing cuts EC waste. –**26%** sender, –**30%** receiver over SS+PQXDH.
- **Hybrid receiver ≈ SPQXDH receiver.**
  XHMQV aggregates 4 DHs into 2 scalar mults on receive. Going full PQ is basically free on that side.

Three protocols side by side



i9-14900K; hybrid ring signature modeled via FalconRS [HKW25, KNTW25] (sign ≈2.85×, verify 2× Falcon-512).

- **SPQXDH: drop-in win.**
  Integrated sealing cuts EC waste. –**26%** sender, –**30%** receiver over SS+PQXDH.
- **Hybrid receiver ≈ SPQXDH receiver.**
  XHMQV aggregates 4 DHs into 2 scalar mults on receive. Going full PQ is basically free on that side.
- **Ring-signing dominates the hybrid cost.**
  ≈ 371 μs on the sender, **73%** of the total. Any further tuning from here lives in this bar.

Collecting all the improvements

	post-quantum								
Scheme	conf	FS	auth	Anon	FA	MEX	deny	Compute	size
X3DH	✗	✗	✗	✗✗	✗✗	✗	✓	1×	1×
PQXDH	(✓)	(✓)	✗	✗✗	✗✗	✗	✓	1.3×	9.2×
PQXDH + SS	(✓)	(✓)	✗	✗	✗✗	✗	✓	1.8×	11.1×
Sealed PQXDH	(✓)	(✓)	✗	✓	✓	✗	✓	1.3×	10.6×
XHMQV	✗	✗	✗	✗✗	✗✗	✓	✓	0.6×	1×
RingXKEM	✓	✓	✓	✓	✗✗	✗	✓	2.1×	29.1×
Sealed XHMQV-RingXKEM	✓	✓	✓	✓	✓	✓	✓	2.7×	29.5×

Collecting all the improvements

post-quantum

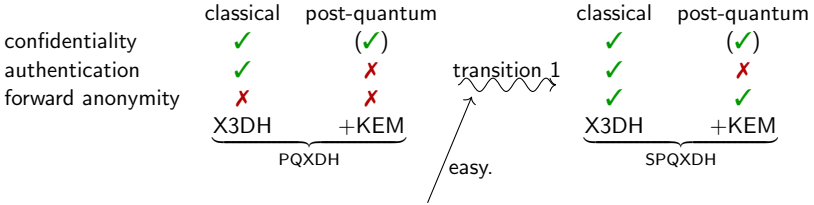
Scheme	conf	FS	auth	Anon	FA	MEX	deny	Compute	size
X3DH	✗	✗	✗	✗✗	✗✗	✗	✓	1×	1×
PQXDH	(✓)	(✓)	✗	✗✗	✗✗	✗	✓	1.3×	9.2×
PQXDH + SS	(✓)	(✓)	✗	✗	✗✗	✗	✓	1.8×	11.1×
Sealed PQXDH	(✓)	(✓)	✗	✓	✓	✗	✓	1.3×	10.6×
XHMQV	✗	✗	✗	✗✗	✗✗	✓	✓	0.6×	1×
RingXKEM	✓	✓	✓	✓	✗✗	✗	✓	2.1×	29.1×
Sealed XHMQV-RingXKEM	✓	✓	✓	✓	✓	✓	✓	2.7×	29.5×

Collecting all the improvements

post-quantum

Scheme	conf	FS	auth	Anon	FA	MEX	deny	Compute	size
X3DH	✗	✗	✗	✗✗	✗✗	✗	✓	1×	1×
PQXDH	(✓)	(✓)	✗	✗✗	✗✗	✗	✓	1.3×	9.2×
PQXDH + SS	(✓)	(✓)	✗	✗	✗✗	✗	✓	1.8×	11.1×
Sealed PQXDH	(✓)	(✓)	✗	✓	✓	✗	✓	1.3×	10.6×
XHMQV	✗	✗	✗	✗✗	✗✗	✓	✓	0.6×	1×
RingXKEM	✓	✓	✓	✓	✗✗	✗	✓	2.1×	29.1×
Sealed XHMQV-RingXKEM	✓	✓	✓	✓	✓	✓	✓	2.7×	29.5×

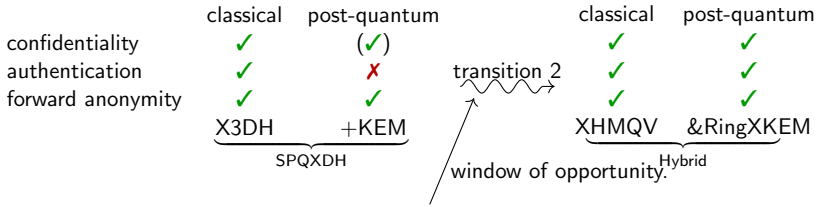
Step 1: PQXDH → SPQXDH



PQXDH → SPQXDH

Same keys. No server change. Better guarantees. Lower cost. We are building it now.

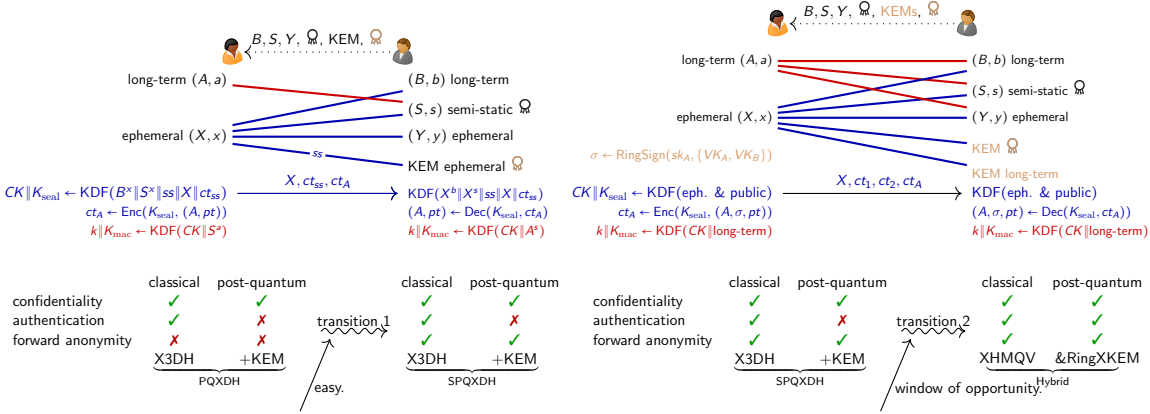
Step 2: SPQXDH → Hybrid



SPQXDH → RingXKEM-XHMQV

Full PQ transition requires server changes and versioning. So does XHMQV. Do both at once to share the expense.

Signal plans to seal PQXDH and XHMQV-RingXKEM



- XHMQV @CRYPTO 2025 [FGPZ25] `ia.cr/2025/1049`; SAKE (in submission)
- RingXKEM @USENIX 2025 [HKW25, KNTW25] `ia.cr/2025/040`, `ia.cr/2025/1090`

`rune.fiedler@inf.ethz.ch` `rolfe@signal.org` `lea.thiemt@fau.de`

References I

[CCD+17] Katriel Cohn-Gordon, Cas Cremers, Benjamin Dowling, Luke Garratt, and Douglas Stebila.
A formal security analysis of the Signal messaging protocol.
In *2017 IEEE European Symposium on Security and Privacy*, pages 451–466, Paris, France, April 26–28, 2017. IEEE Computer Society Press.

[FGPZ25] Rune Fiedler, Felix Günther, Jiaxin Pan, and Runzhi Zeng.
XHMQV: Better efficiency and stronger security for signal's initial handshake based on HMQV.
In Yael Tauman Kalai and Seny F. Kamara, editors, *Advances in Cryptology – CRYPTO 2025, Part VIII*, volume 16007 of *Lecture Notes in Computer Science*, pages 109–140, Santa Barbara, CA, USA, August 17–21, 2025. Springer, Cham, Switzerland.

[HKW25] Keitaro Hashimoto, Shuichi Katsumata, and Thom Wiggers.
Bundled authenticated key exchange: A concrete treatment of signal's handshake protocol and post-quantum security.
In Lujo Bauer and Giancarlo Pellegrino, editors, *USENIX Security 2025: 34th USENIX Security Symposium*, pages 6777–6796, Seattle, WA, USA, August 13–15, 2025. USENIX Association.

References II

[KNTW25] Shuichi Katsumata, Guilhem Niot, Ida Tucker, and Thom Wiggers.
Comprehensive deniability analysis of signal handshake protocols: X3DH, PQXDH to fully post-quantum with deniable ring signatures.
In Lujo Bauer and Giancarlo Pellegrino, editors, *USENIX Security 2025: 34th USENIX Security Symposium*, pages 6797–6816, Seattle, WA, USA, August 13–15, 2025. USENIX Association.

Icon References

- Secure messaging app icons are by Signal, WhatsApp, Google Messages, Facebook Messenger
- server icon by Alexiuz AS
- public key icon by Yannick Lung
- signature icon by PINPOINT.WORLD is licensed under CC BY 3.0