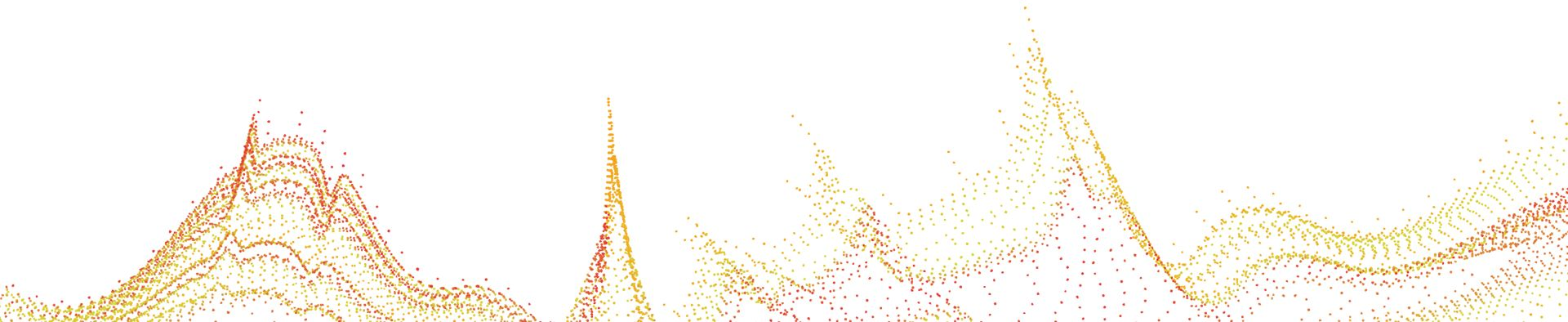
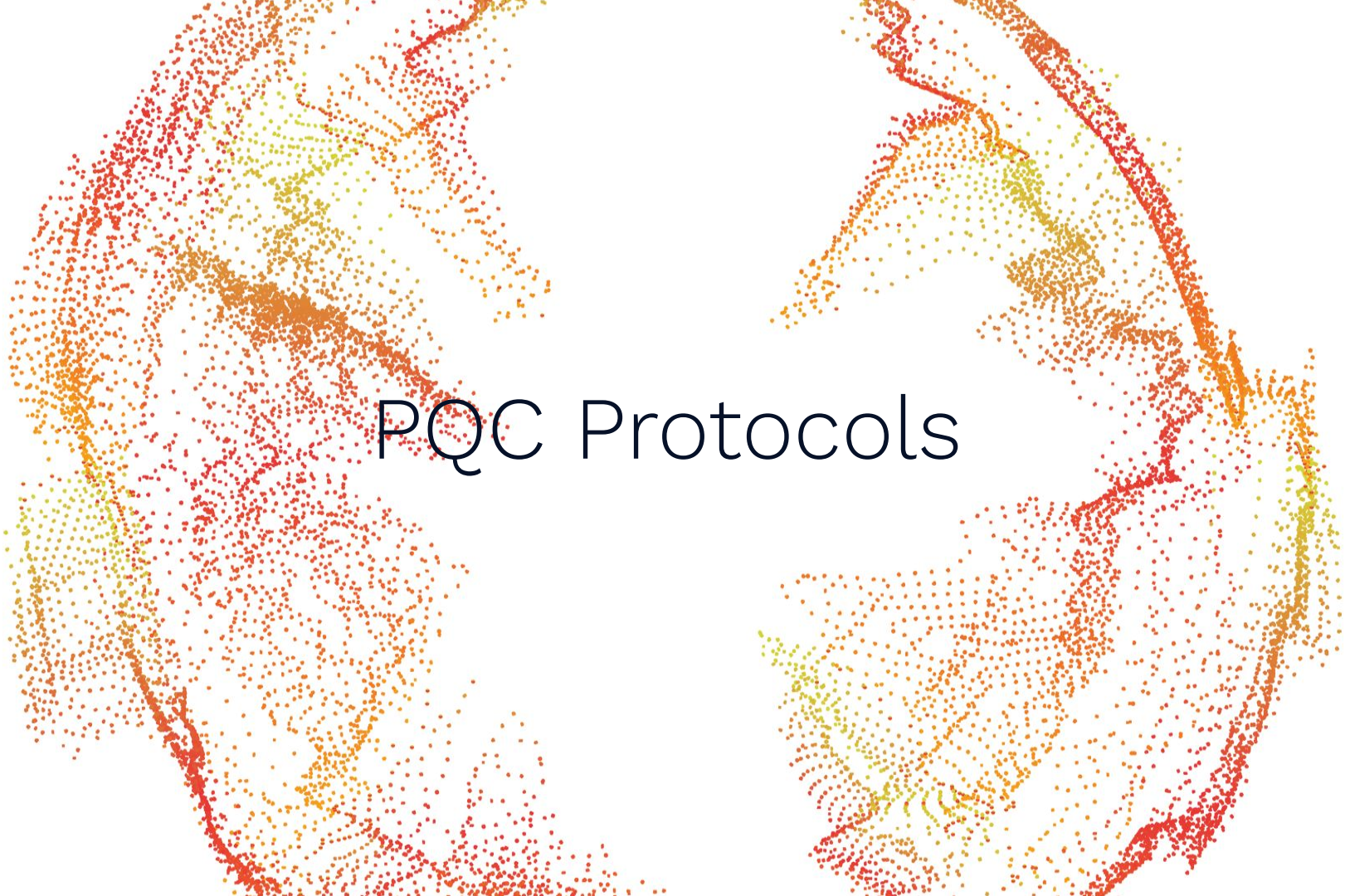
PQSHIELD

Triple Ratchet: a secure and bandwidth-efficient hybrid Signal protocol

Yevgeniy Dodis (NYU), Daniel Jost (NYU), Shuichi Katsumata (PQShield + AIST),
Thomas Prest (PQShield), Rolfe Schmidt (Signal Messenger)




PQC Protocols

PQC: What is done & What's next

PQ SHIELD

2017 — NIST PQC Process (69 candidates)

2022 — 4 Standards Announced

2024 — FIPS 203 (ML-KEM)
FIPS 204 (ML-DSA)
FIPS 205 (SLH-DSA)

2027 — FIPS 206 (FN-DSA)?
FIPS 207 (HQC-KEM)?

~2030 — ANSSI, BSI, NSA: migration complete for critical systems

What do we need to do?

Migrate products

Software and hardware IPs,
side-channel protections,
formal verification, certification, etc.

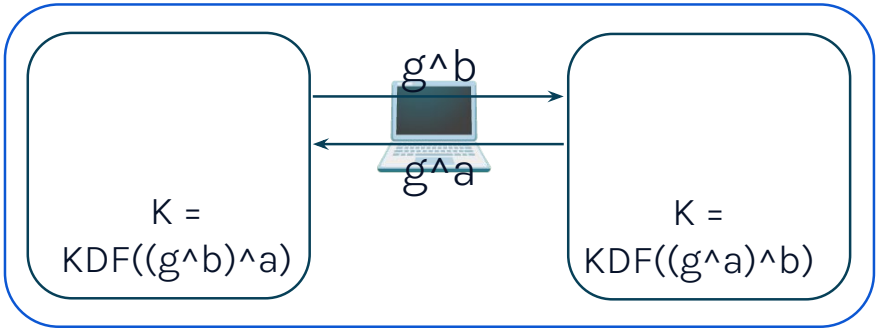
Migrate protocols

- TLS & DNSSEC
- **Signal (this talk)**
- VPN protocols (WireGuard, IKEV2)
- etc.

Key agreement: ECDH vs ML-KEM

PQSHIELD

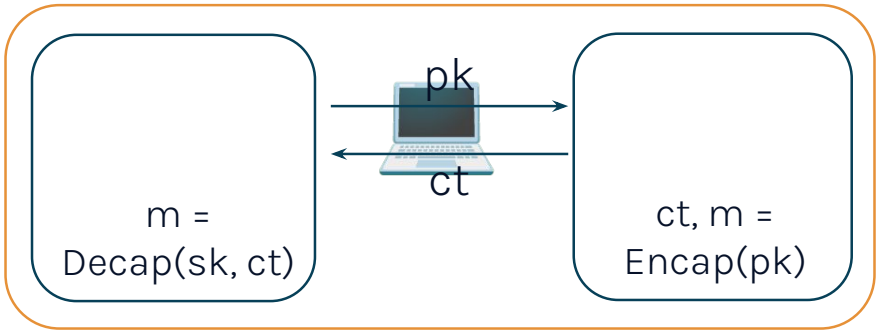
ECDH: 32B + 32B



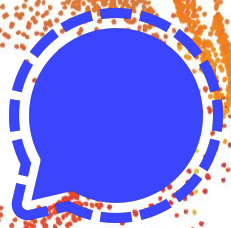
Many protocols were designed for ECDH...

... and ML-KEM does not always fit.

ML-KEM: 1184B + 1088B



The Signal Protocol



Secure Messaging Protocols

PQ SHIELD

Use cases = secure messaging apps:

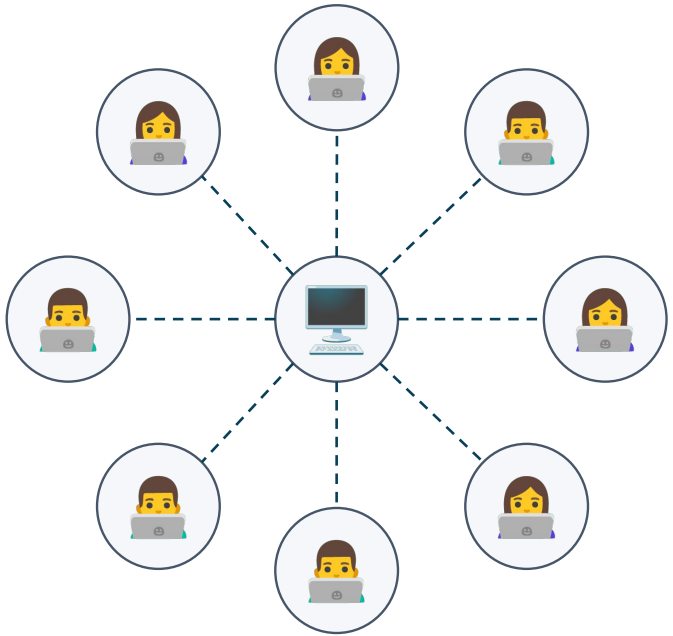
- WhatsApp
- Messenger
- iMessage
- Signal
- etc.

Characteristics:

- Asynchronous
- Long-lived sessions (years!)
- Untrusted server

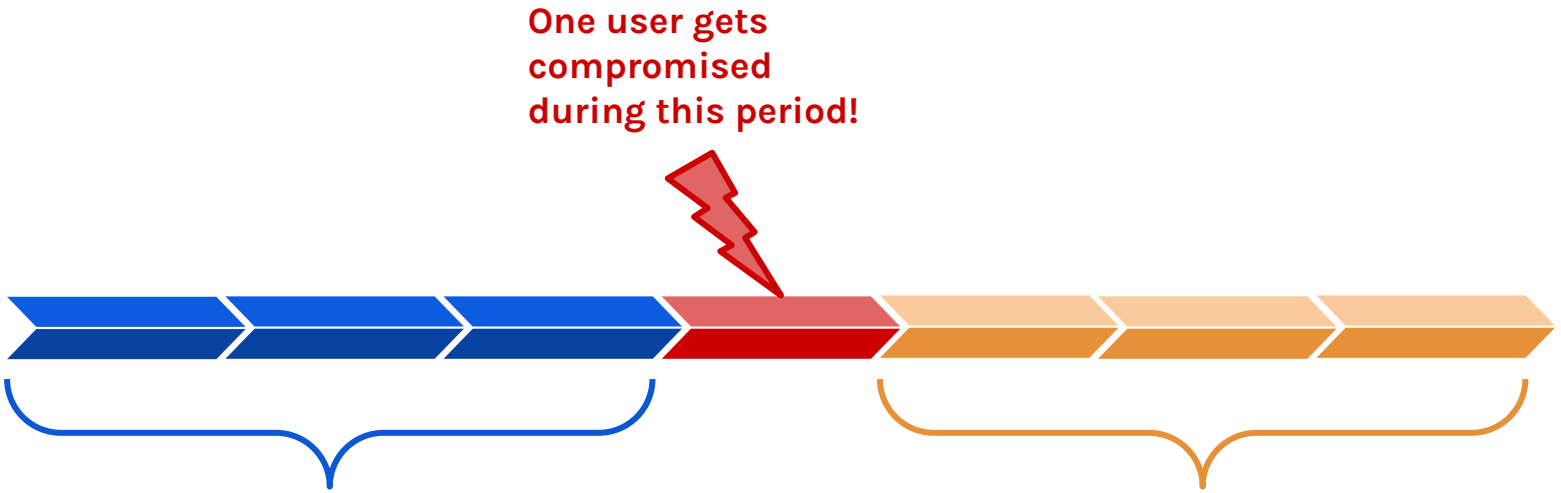
Criteria = characteristics, plus:

- Low bandwidth requirements
- Forward secrecy (next slide)
- Post-compromise security (same)



Forward secrecy & Post-Compromise security

PQ SHIELD



Forward secrecy:
messages exchanged before
compromise remain confidential.

Post-compromise security:
messages exchanged after
compromise remain confidential.

(Old) Signal Protocol = X3DH + Double Ratchet





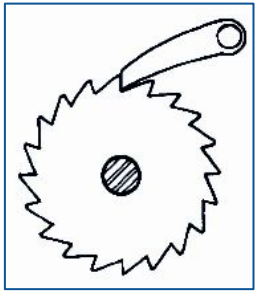


Establish shared key

X3DH

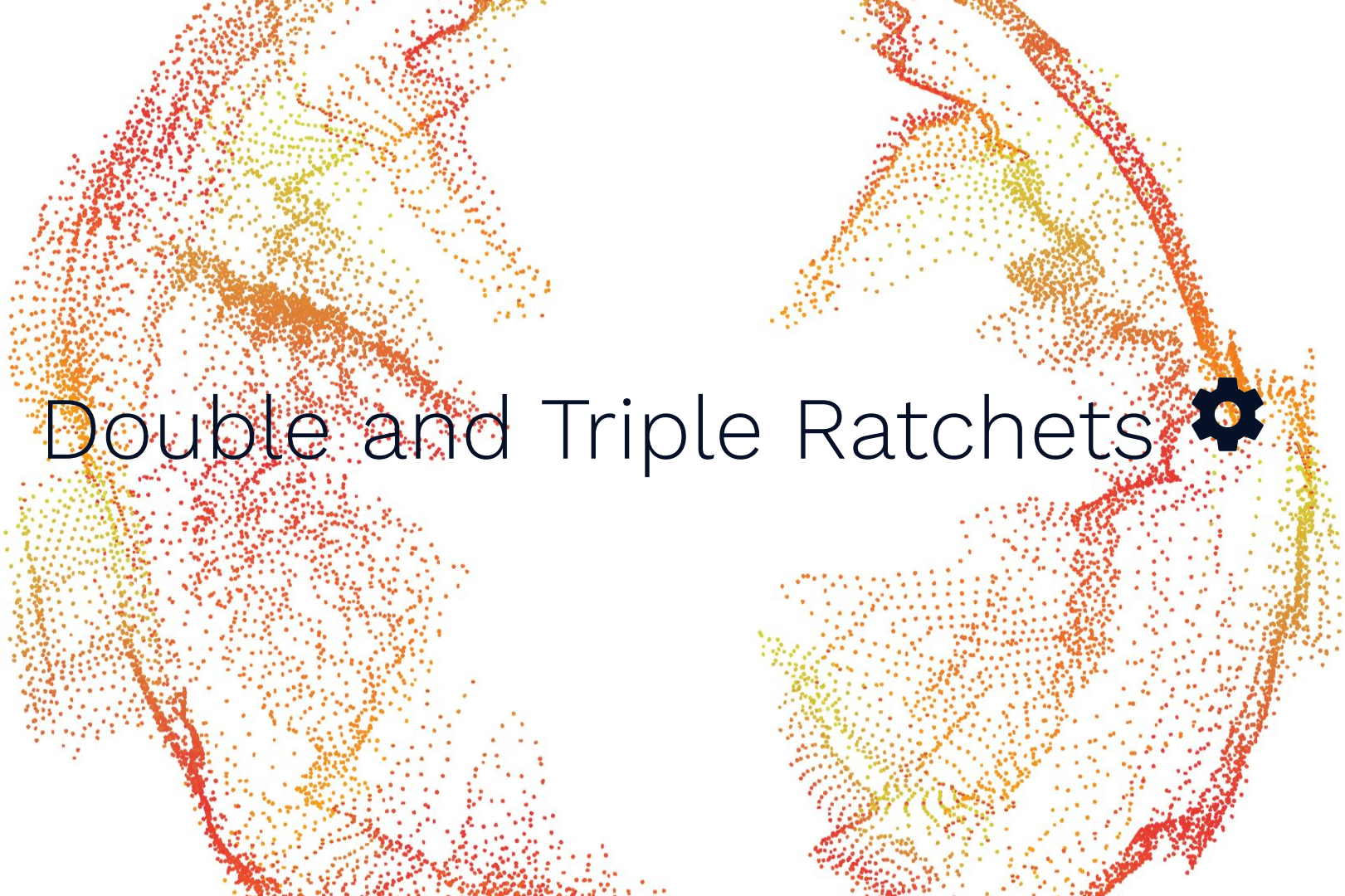
Encrypt messages using key + refresh key

Double Ratchet



...

...

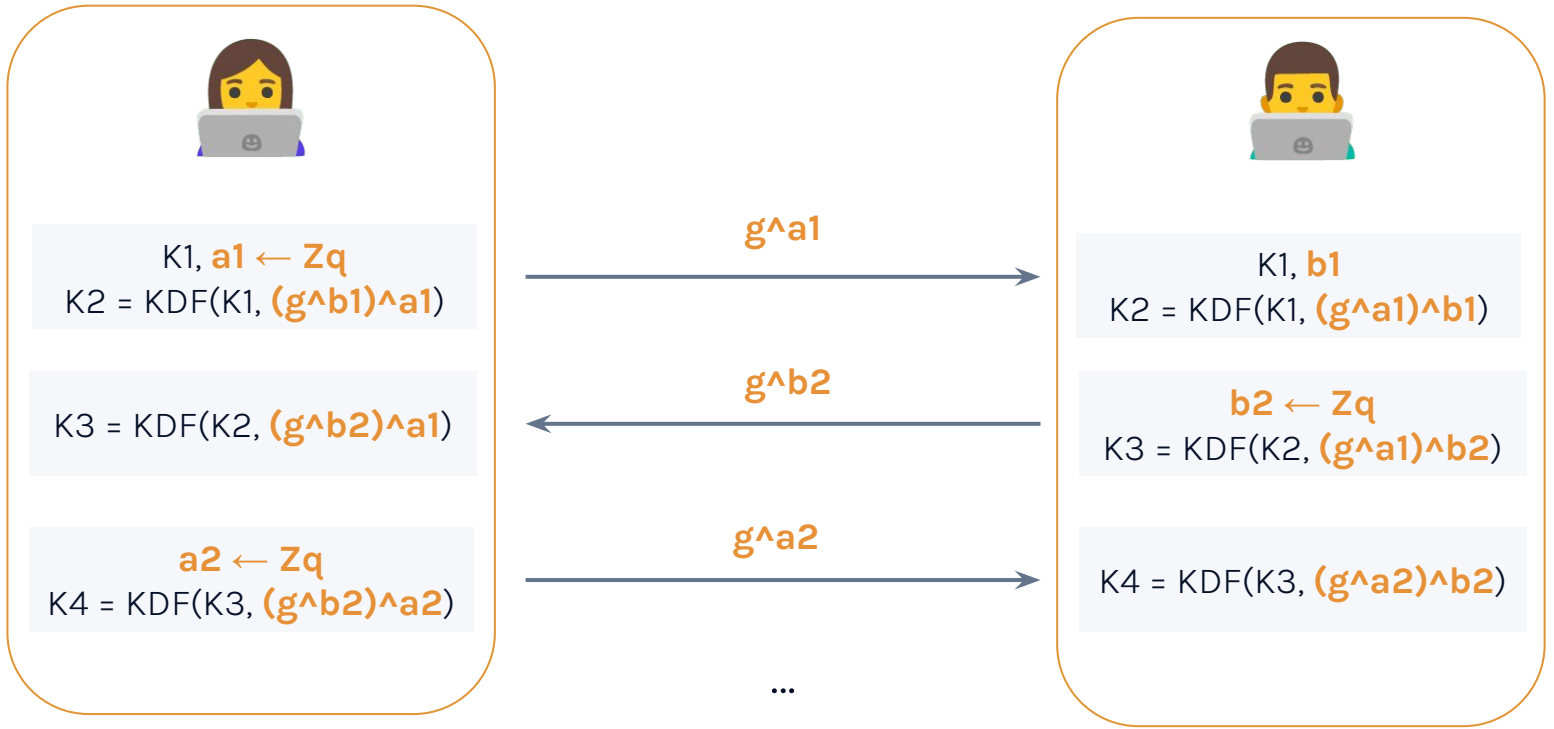

Double and Triple Ratchets

Symmetric (Local) Ratchet



Provides forward secrecy!

Diffie-Hellman (Interactive) Ratchet



Provides post-compromise security!

Simple idea: inject randomness in shared key K

Post-Quantum Ratchet



pka_1 ← Keygen()
(ct1, m1) ← Encap(pkb_1)
K2 = KDF(K1, **m1**)

m2 = Decap(ct2, ska_1)
K3 = KDF(K2, **m2**)

pka_1, ct1 →

← **pkb_2, ct2**

...



m1 = Decap(ct1, skb_1)
K2 = KDF(K1, **m1**)

pkb_2 ← Keygen()
(ct2, m2) ← Encap(pka_1)
K3 = KDF(K2, **m2**)

Provides (post-quantum) post-compromise security!

Same idea as Diffie-Hellman ratchet, only via different means.

Communication and erasure codes

PQ SHIELD

The Bandwidth Challenge

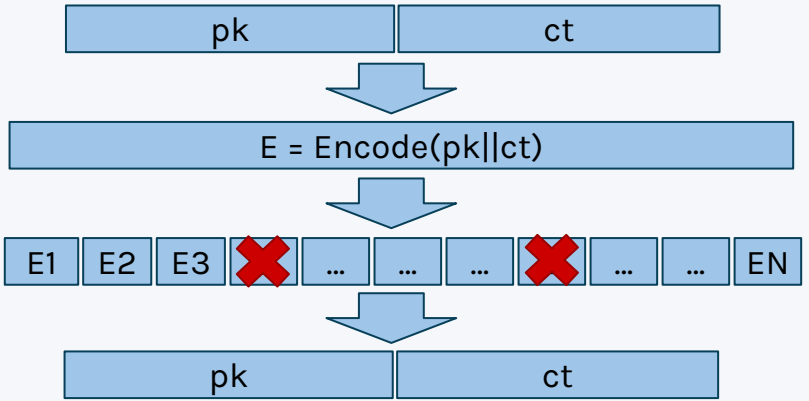
- **Diffie-Hellman:** |pk| = 32 bytes ⇒ send pk every message for immediate decryption.
- **ML-KEM-768:** |pk| + |ct| = 2 kilobytes ⇒ noticeable impact
  - **Apple PQ3:** sends (pk, ct) every ~50 messages.
    Requires resending until acknowledged, which repeats if the party is offline.

Triple Ratchet Solution

Encode (pk||ct) with **erasure code (Reed-Solomon),** then split into multiple chunks.

Key Advantages:

- Flexible parametrization.
- Minimal overhead per message.
- Robust against dropped messages.



From Double Ratchet to Triple Ratchet

PQ SHIELD

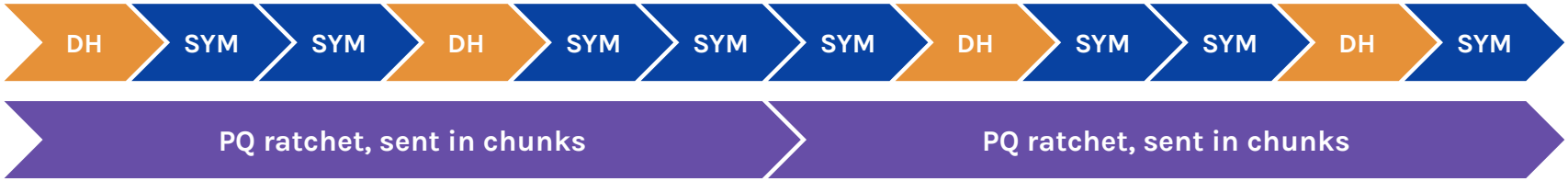
Double Ratchet

Diffie-Hellman + Symmetric ratchets, interleaved



Triple Ratchet

Diffie-Hellman + Symmetric + Post-Quantum ratchet (in parallel)



Symmetric ratchet
Every message

Public-key ratchet (ECDH)
Each time the sender changes

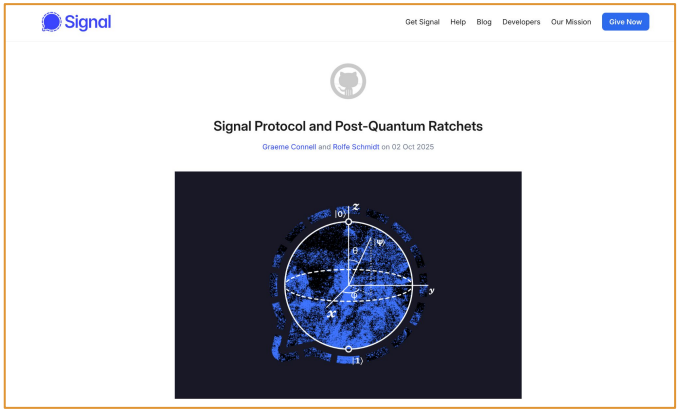
Post-quantum ratchet (ML-KEM)
Continuously (1 chunk per message)

Message keys mix all 3 ratchets: secure if ECDH or ML-KEM is secure.

Status of Signal

	Handshake	Ratchet	Post-quantum protection
Original (< 2023)	X3DH	Double Ratchet	None
Since 2023	PQXDH	Double Ratchet	Confidentiality only
Since 2025 (this talk)	PQXDH	Triple Ratchet	Confidentiality + PCS

Our ideas are deployed in Signal!
https://signal.org/blog/spqr/ ⇒



Takeaways & what's next

PQ SHIELD

Takeaways

- ML-KEM is not a drop-in replacement for Diffie-Hellman.
- Triple Ratchet:
  - Adds PQ to the Double Ratchet
  - Hybrid security
  - Deployed in Signal since 2025

Next: Group Messaging

- Same goals, but bandwidth per update grows with group size N
  - Naive solution: O(N^2)
  - TreeKEM: O(N · log N)
  - Ours (CCS'21): O(N)
- See white paper & RWC 2024 talk
- IETF RFC 9420 MLS (Messaging Layer Security)
  - Applicable to drone swarms
- **NATO workshop on MLS in Paris, 18–20 Jan. 2027.**


PQ SHIELD
think openly, build securely