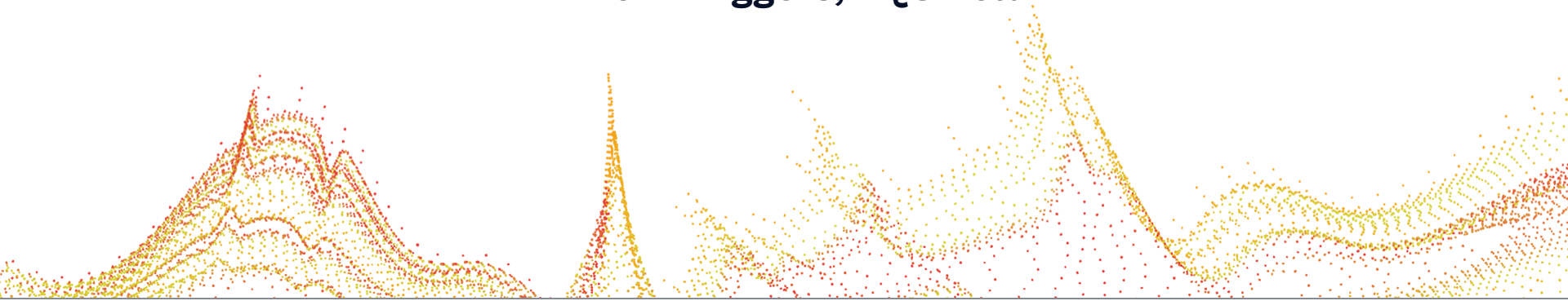
Bundled Authenticated Key Exchange:
A Concrete Treatment of (Post-Quantum) Signal's Handshake Protocol

Keitaro Hashimoto, AIST
Shuichi Katsumata, PQShield & AIST
Thom Wiggers, PQShield



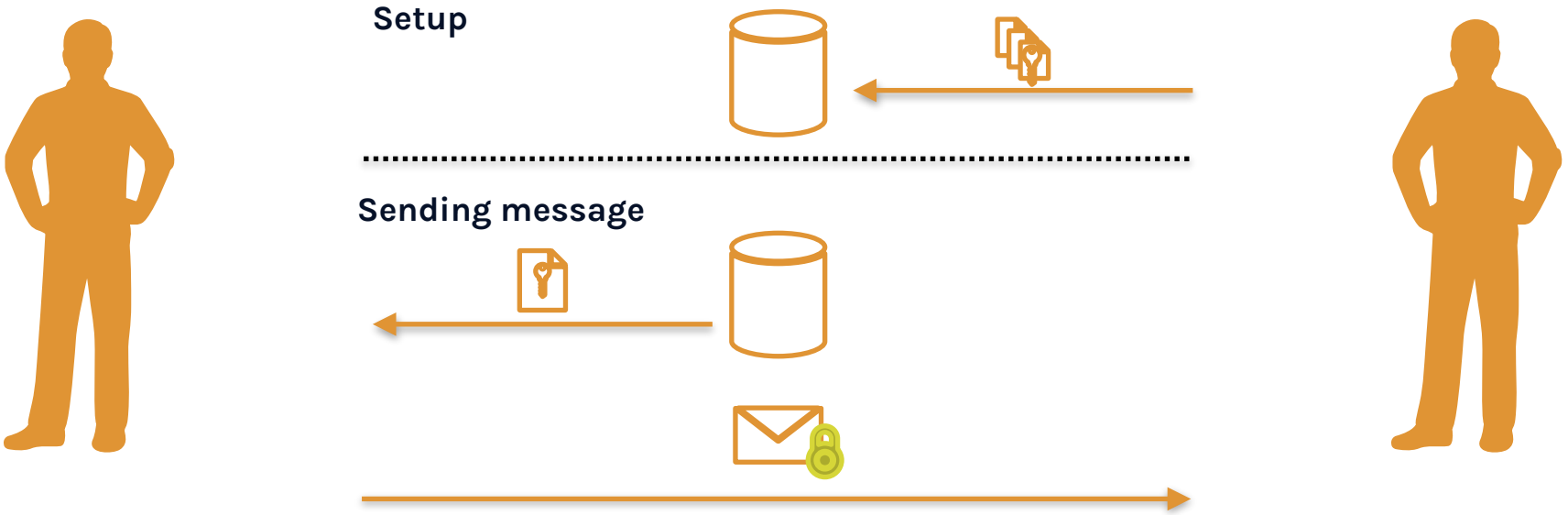
This presentation is based on results obtained from a project, JPNP24003, commissioned by the New Energy and Industrial Technology Development Organization (NEDO)

Messaging

Messaging

How do I still send messages when the recipient is unavailable?

Signal's solution: prekey bundles



Why a New Model for Signal Handshake Protocols

- Post-Quantum motivated new Signal handshake protocols
  - X3DH (Marlinspike & Perrin): Classic confidentiality and authentication
  - PQXDH (Kret & Schmidt, 2023) : Hybrid confidentiality and classic authentication
  - What is the next Signal protocol?
- Existing proofs of Signal handshake protocols:
  - All bespoke models
  - Prekey bundles not modeled in the way that they are uploaded to the server
  - Not all models consider *last-resort prekey bundles*
  - Harvest-Now-Decrypt-Later adversaries not modeled
  - **Very difficult to compare security properties**

Bundled Authenticated Key Exchange (BAKE)

- Model specifically for key exchange in protocols that use prekeys
- Fully models prekey bundle upload
  - Allows representing protocols that optimize prekey bundle uploading (our RingXKEM)
- Treat forward secrecy including last-resort prekey bundles
- Treat correctness, authentication, and confidentiality
- Provide a framework for comparing security properties

Table 5: Security comparison of BAKE protocols.

Protocol	Adversary	Forward Secrecy	User-State Compromise Impersonation	Protocol-specific adversary restrictions
X3DH	Classical	Sender: weak Receiver: full	Receiver vulnerable	No quantum/HNDL adversaries.
PQXDH	HNDL	Sender: weak Receiver: full	Receiver vulnerable	KEM secret can not be revealed to HNDL adversary.
RingXKEM	Quantum	Full	Secure	No RingXKEM specific restrictions.

RingXKEM

- Build on prior work by Brendel et al., Hashimoto et al. using PQ **Ring Signatures for deniability**
- **Reduce prekey upload bandwidth** by using Merkle Trees
- Full post-quantum security

Bundled Authenticated Key Exchange

One model for current and future Signal handshake protocols

- Compare security properties
- Properly treat prekey bundles
- Harvest-now Decrypt-Later adversaries
- Can represent protocols not fitting in prior approaches

An optimised, deniable PQ protocol

- RingXKEM based on Ring Signatures
- Full forward secrecy
- PQ confidentiality and authentication

Full version:
https://ia.cr/2025/040

This presentation is based on results obtained from a project, JPNP24003, commissioned by the New Energy and Industrial Technology Development Organization (NEDO)