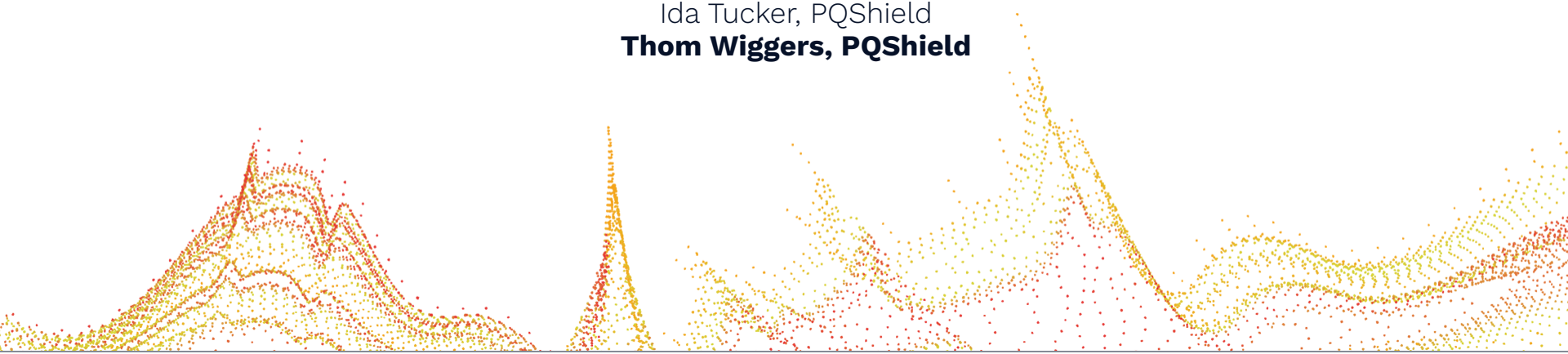
Comprehensive Deniability Analysis of Signal Handshake Protocols:

X3DH, PQXDH to Fully Post-Quantum with Deniable Ring Signatures

Shuichi Katsumata, PQShield & AIST;
Guilhem Niot, PQShield & Univ Rennes, CNRS, IRISA;
Ida Tucker, PQShield
Thom Wiggers, PQShield



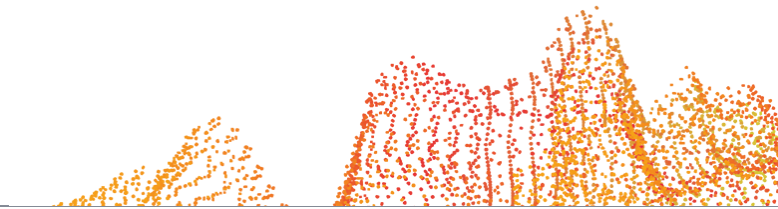
This presentation is based on results obtained from a project, JPNP24003, commissioned by the New Energy and Industrial Technology Development Organization (NEDO)

Deniability

The ability to argue against **presented evidence**

In secure messaging:

deny participating in a conversation



Deniability: Argue Against Presented Evidence

Deniability in Secure Messaging

Why a New Model for Signal's Deniability?

- Post-Quantum: What new protocol provides the best guarantees / performance?
- Prior analyses fragmented and incomparable
- Build on BAKE abstraction

Flavors of Deniability

Local deniability

- Accuser is one of the participants
- Semi-Honest vs Malicious

Global deniability

- Accuser is not one of the participants
- Semi-Honest vs Malicious

Practical Deniability

- Traditional deniability: perfect indistinguishability
- Proposal: “plausible” deniability is good enough
- Enables much more efficient constructions in post-quantum setting
- Based on hockey-stick divergence

Table 1: Signal key exchange protocols and their deniability and security properties

Signal handshake protocol deniability properties

	Protocol:	**X3DH** Classic $\mathcal{A}$/D	**PQXDH** Classic $\mathcal{A}$/D	**PQXDH** Classic $\mathcal{A}$ Quantum D		**RingXKEM** Classic or Quantum $\mathcal{A}$/D		**SignXKEM** Classic or Quantum $\mathcal{A}$/D	
	Deniability Level	**Leakage** leak	**Leakage** disc	**Leakage** leak	**Leakage** disc	**Leakage** leak disc	**QROM**	**Leakage** leak disc	**QROM**	**Leakage** leak disc	**QROM**
	local	●	●	●	●	● ●	✓	● ●	✓	◕ ◴	✓
	global	◕	●	◕	●	◕ ●	✓	● ●	✓	◕ ◴	✓
strong-	local	●†	●	●†	●	$●^{SO}$ ●	?	$●^{SO}$ ●	?	$◕^{SO}$ ●	?
strong-	global	◕†	●	◕†	●	$◕^{SO}$ ●	?	$●^{SO}$ ●	?	$◕^{SO}$ ●	?
	Security [HKW25]	Classical		Harvest-Now Decrypt-Later				Fully post-quantum			

Legend

Icon	**Last-resort prekey: No** leak or disc	**Yes** leak or disc
●	high	high
◕	high	med
◴	med	low
?	Open problem	
$○^{SO}$	Accusers $\mathcal{A}$ restricted to being senders, no deniability otherwise.	
†	Proof using GGM.	

Example: RingXKEM is local deniable with leakage leak = high and disclosure disc = high even if a last-resort prekey bundle was used. SignXKEM is local deniable with leak = high and disc = med, but restricted to leak = med and disc = low if a last resort prekey bundle is used.

Remark: For strong deniability, we always set disc = high, since we have no control over the information a malicious accuser may reveal.

Update: we made a small mistake in global deniability for RingXKEM, see the full version

New PQ Ring Signatures

- Small variations on Falcon & MAYO
- Efficiently constructable and fast
- Use our hockey-stick divergence deniability model

Comprehensive Deniability Analysis of Signal Handshake Protocols

One Model for Deniability of BAKE Protocols

- Compare deniability properties
- Practical notion of deniability
- Classic or Quantum adversaries
- Harvest-now-**judge**-later deniability

New Deniable Ring signatures

- Based on Falcon and MAYO
- Close to proposed standards
- Efficient instantiation of RingXKEM

Full paper: https://ia.cr/2025/1090

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