Welcome to MILCOM 2025!

6–10 October 2025 // Los Angeles, CA, USA

Pioneering the Future of Space and Terrestrial Networks

Post-Quantum SIM-Less Authentication: Scalable and Secure Solutions for FutureG IoT Networks

Abhisek Jha[1], SeyedMohammad Kashani,[2] Sang Wu Kim[2], Ashfaq Khokar,[2] and Farid Nait-Abdesselam[3]

University of Texas at Arlington[1], Iowa State University[2], Universite Paris Cit ´e, France[3]

5G as the default communication method for IoT

IEEE MILCOM

Maintaining and changing physical SIMs is inconvenient because it requires manual access to each device.

IEEE ComSoc
IEEE Communications Society


5G
SIM 1
SIM 2

Why SIM-Less?

Flexibility: No physical SIM provisioning

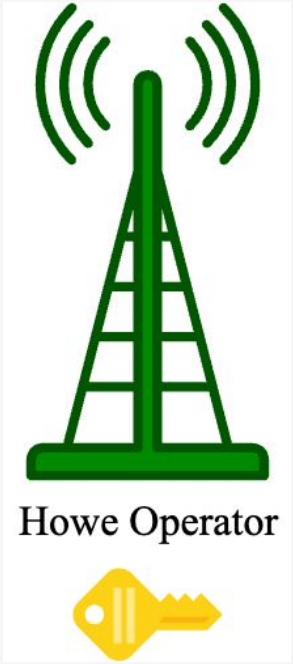
Agility: Supports revocation and short-lived credentials

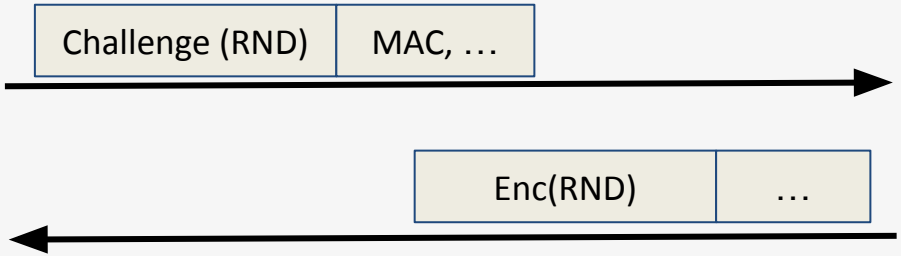
Interoperability: Works across operators

IEEE MILCOM

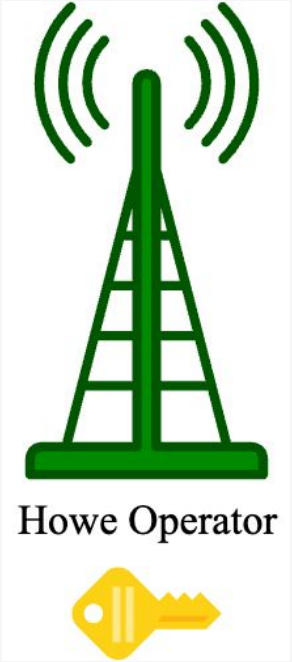
IEEE ComSoc
IEEE Communications Society

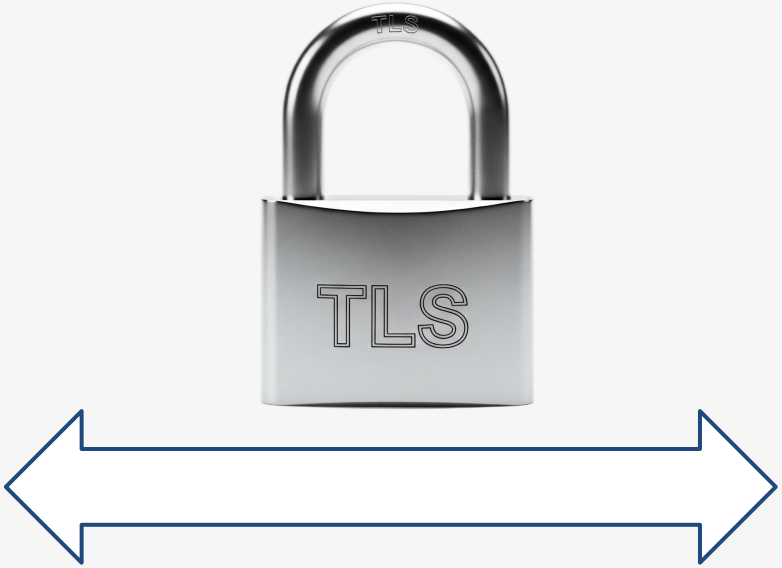
AKA ⟶ AUTHENTICATE

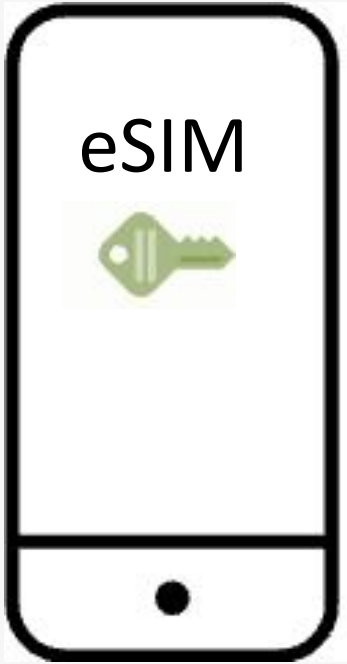




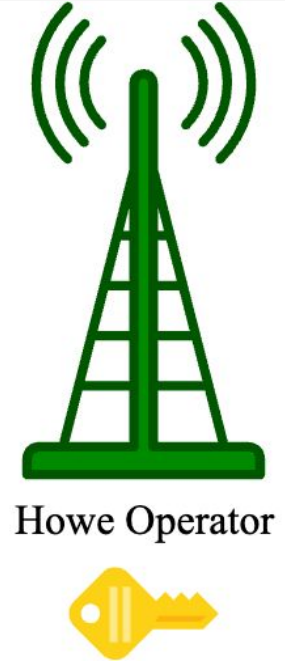
How the Key is Shared in eSIM?

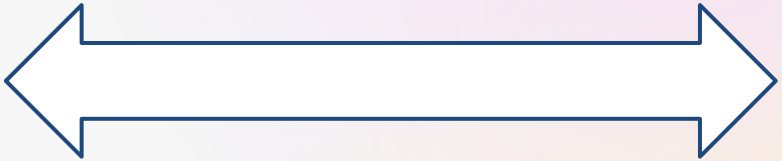


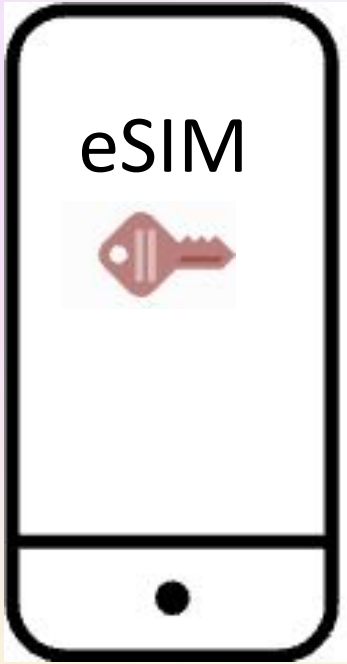




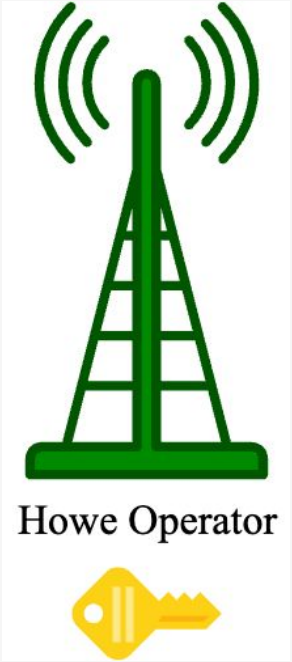
Post-Quantum Threats

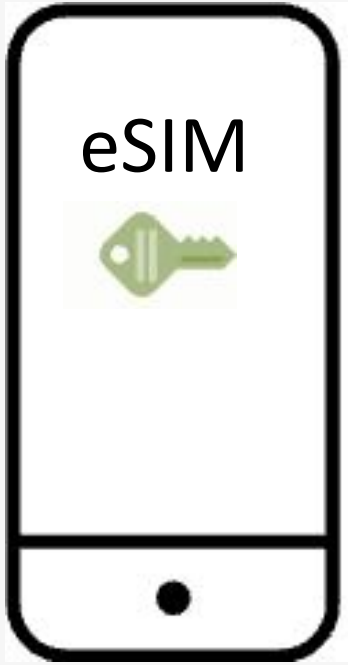




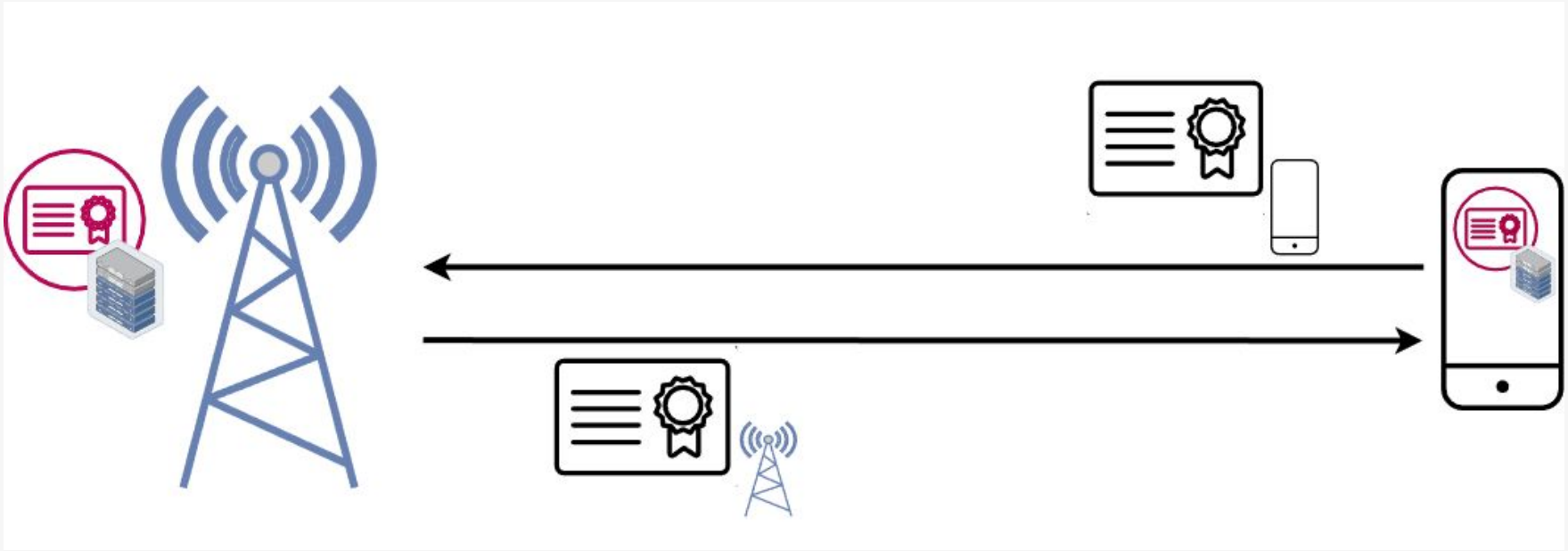


Post Quantum Cryptography





Direct Sim-less Authenticate using PQC



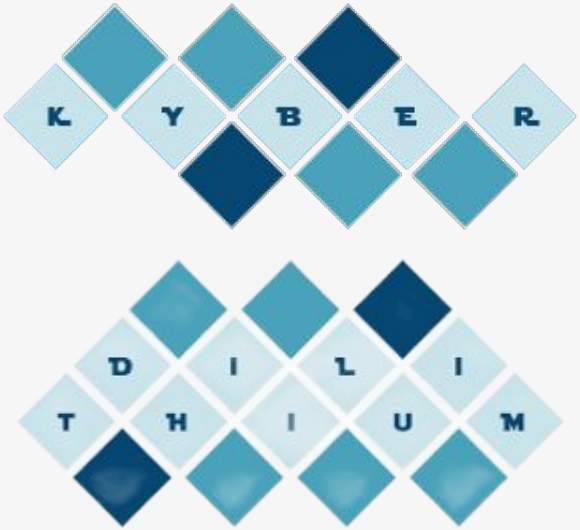
Sim-Less PQC Challenges

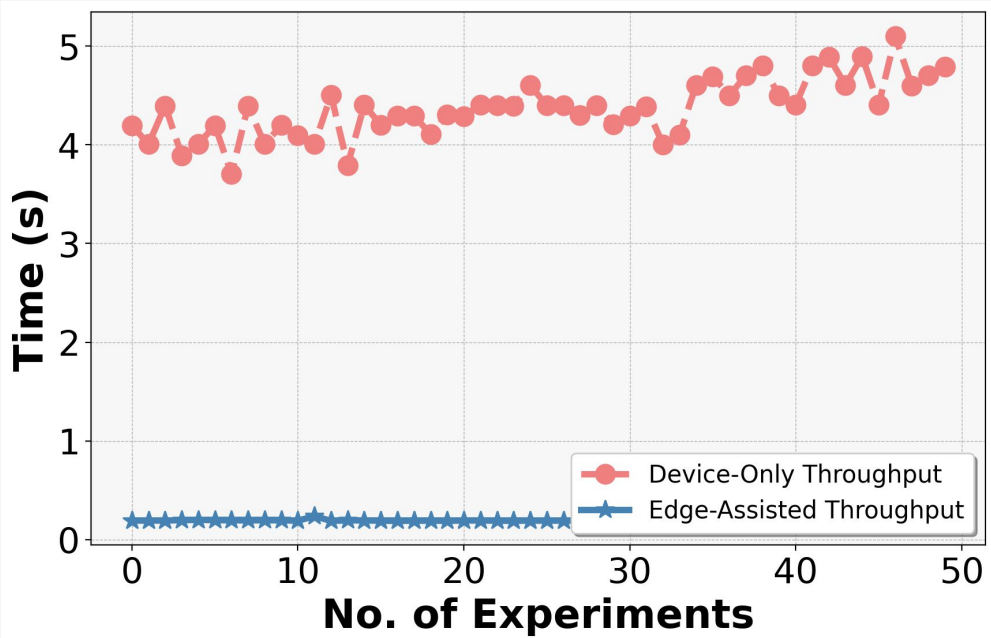
- Computationally heavy
- 10x larger

	Public Key (bytes)	Signature (bytes)
RSA-2048	**256**	**256**
Dilithium-2	**1,312**	**2,420**

Sim-Less PQC Simulation for IoT

Configuration	CPU Cores	Memory	Description
IoT Device	1 core	256 MB	constrained profile
Edge Server	4 cores	4 GB	operator edge node





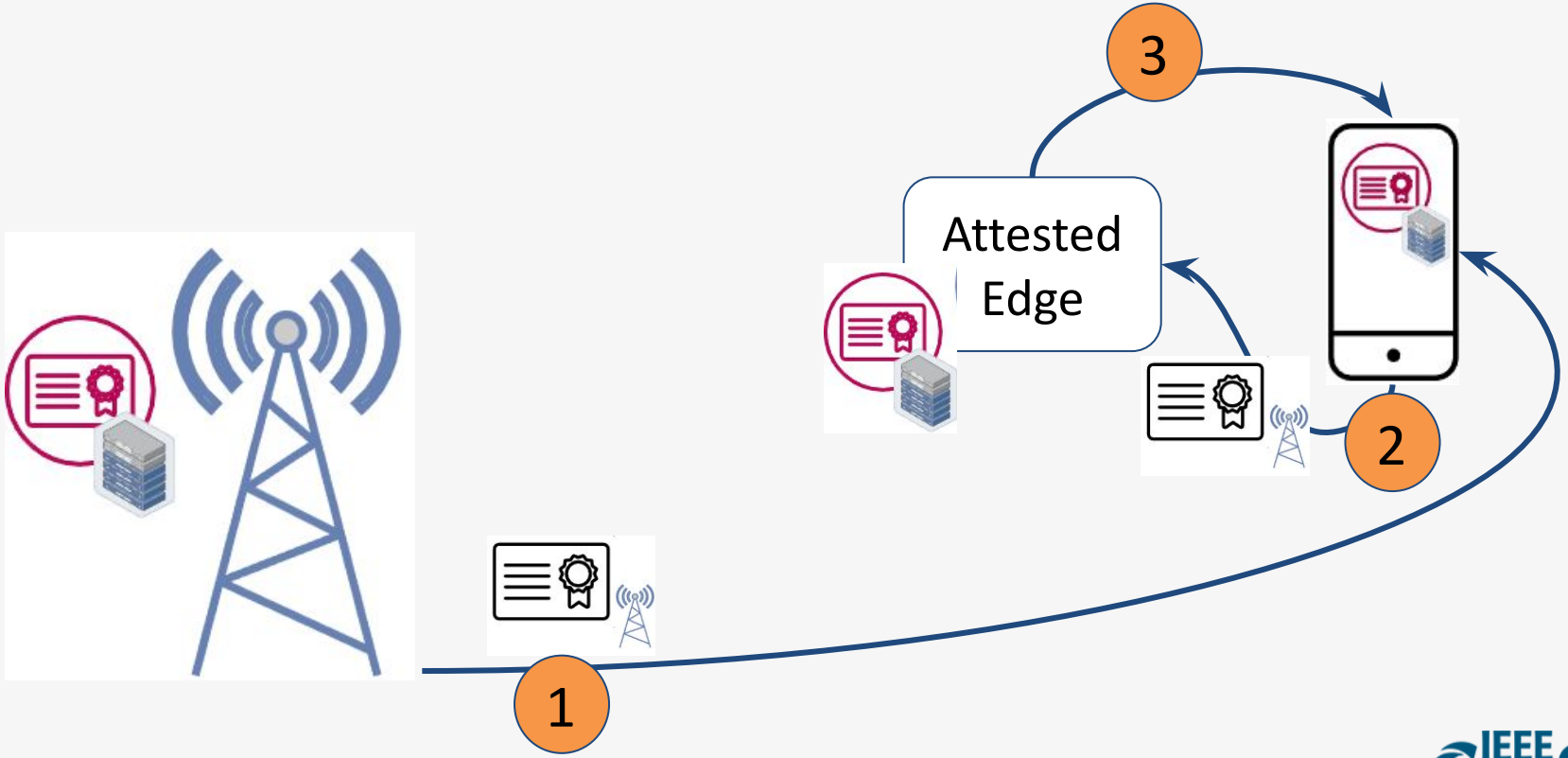
IEEE MILCOM

Our Proposed Sim-less PQC Scheme

- **Offload heavy crypto** ops to attested edge servers

- Attested edge servers could also help with **certificate storage**

Edge Assisted Sim-less PQC



Edge Assisted Improvements

Latency: 3.48s → 0.12s (96% reduction)

Resource Use: ≈0 MB extra memory

Scalability: Horizontal edge scaling supports ~182k devices/hour

Key takeaways

- Future is Sim-Less direct mutual authentication
- PQC could be computationally heavy
- Necessity of edge for PQ Sim-Less authentication
- Rigorous security analysis for attested edge servers

From SIM to Post-Quantum Sim-Less Authentication