Contribution ID: **73** Type: **Contributed Oral**

Q-PUF: Scalable, Hardware-Based Authentication for Quantum Processors

Tuesday 2 December 2025 11:25 (15 minutes)

Cloud-based quantum computing is transforming how sensitive algorithms are executed, enabling remote access to shared hardware—but also introducing new risks of device impersonation and unauthorized access. We present a hardware-intrinsic authentication scheme based on Quantum Physical Unclonable Functions (Q-PUFs), which exploit fabrication-induced variations in quantum devices to create unclonable hardware fingerprints.

We begin by fingerprinting quantum devices through stable, intrinsic physical properties that are unique to each individual device, forming the basis for our Q-PUF protocol. While adaptable to different quantum hardware modalities, we prototype and validate it on IBM Quantum devices using qubit frequency as the primary fingerprinting feature. To demonstrate the robustness of our protocol across many devices of the same technology—each possessing distinct physical characteristics—we used Monte Carlo simulations to model large populations of superconducting processors with realistic fabrication variability. This allowed us to assess scalability and key-generation performance in scenarios representative of a wide range of individual machines. The protocol employs fuzzy extractors to transform noisy fingerprint data into cryptographically secure keys while concealing raw hardware properties.

To enable scalability, we introduce q-tuples—qubit subsets that generate exponentially many challenge–response pairs—transitioning from weak to strong PUF behavior. Evaluation via Hamming weight and distance analysis confirms high entropy, uniqueness, and robustness. We also explore additional intrinsic quantum properties to strengthen security and resistance to compromise.

Beyond superconducting platforms, the protocol can be extended to other modalities, including silicon-based devices and neutral-atom systems, and adapted to future logical Q-PUFs for authenticating fault-tolerant qubits. These advances position Q-PUFs as a core security primitive for trusted quantum–classical networks, enabling scalable, verifiable, and hardware-rooted quantum cloud infrastructure.

Author: Dr TONEKABONI, Behnam (Infleqtion Australia)

Co-authors: Dr SMITH, Kaitlin (Northwestern University); Dr GOKHALE, Pranav (Infleqtion)

Presenter: Dr TONEKABONI, Behnam (Infleqtion Australia)

Session Classification: Quantum Science and Technology

Track Classification: Topical Groups: Quantum Science and Technology