Quantum Thread Review

The analysis underscores a critical gap in **post-quantum cryptography (PQC)** integration across all studies reviewed. A significant majority of these studies continue to rely on **pre-quantum cryptographic** methods, such as **ECDSA**, **BLS**, and **pairing-based credentials**, all of which are vulnerable to attacks from quantum computers. This emphasizes the urgent need for the research community to adopt **NIST-standardized PQC solutions**, such as **SPHINCS+**, **CRYSTALS-Dilithium**, and **lattice-based ZKPs**, into **eKYC/SSI** frameworks.

To ensure long-term security of blockchain-based identity systems, future cryptographic designs must prioritize transitioning to post-quantum cryptography (PQC) to protect against quantum decryption threats.

The following studies were analyzed, grouped into their respective quantum vulnerability categories:

1. **Traditional ZKP Systems Without Quantum Resistance**
   Several studies still rely on quantum-vulnerable cryptographic methods without addressing post-quantum alternatives:
   - **Moya et al. (2023)** implement **Feige-Fiat-Shamir/Schnorr ZKPs**, susceptible to quantum attacks.
   - **Kapsoulis et al. (2020)** use **Quorum blockchain** with **classical digital signatures**.
   - **Konkin et al. (2021)** deploy **ZKPs** for corporate **DFAs** but fail to provide a **PQC migration path**.
   - **Dieye et al. (2022)** rely on a **discrete logarithm-based MDSA scheme**, also vulnerable to quantum decryption.
2. **BLS Signatures Susceptible to Quantum Attacks**
   Several studies use **BLS aggregate signatures**, which are vulnerable to quantum attacks:
   - **Li et al. (2022)** implement **BLS** for **verifiable credentials**.
   - **Pauwels et al. (2021)** use **BLS** in their **zkKYC solution** without integrating quantum safeguards.
   - **Malik et al. (2020)** apply **BLS** in the **TradeChain supply chain framework**, underscoring the reliance on quantum-vulnerable cryptographic methods.
3. **Pairing-Based Credentials Vulnerable to Shor's Algorithm**
   Some studies continue to use **pairing-based credentials**, which are vulnerable to **Shor's algorithm**:
   - **Singh et al. (2020)** use **pairing-based self-blindable credentials**.
   - **Gilani et al. (2022)** implement a **pairing-dependent DLRep scheme**.
   - **Yang et al. (2022)** deploy **BLS signatures** in **minimal disclosure authentication**.
   - **Dragan et al. (2020)** rely on the **ECDSA foundations** of **Bitcoin/Ethereum**, all of which are susceptible to quantum decryption.
4. **Quantum-Risk Acknowledgement Without Mitigation**
   Some studies acknowledge the quantum threat but fail to provide adequate mitigation:

Takaragi et al. (2022) explicitly acknowledge the **million-qubit quantum threat** to **ECDSA** but do not propose any **post-quantum cryptographic (PQC)** alternative. This lack of mitigation highlights a significant gap in addressing quantum risks in **eKYC/SSI systems**.