Contribution ID : **105** Type : **Poster**

Post-Quantum Cryptography and the Foundation of Quantum2Pi

The advent of quantum computers threatens to render traditional cryptographic systems, based on problems like prime factorization and discrete logarithms, obsolete. This challenge is not only technological but also fundamentally physical, as quantum computing leverages the unique properties of quantum mechanics. The scientific community is developing advanced post-quantum cryptography (PQC) techniques alongside complementary physical approaches like Quantum Key Distribution (QKD) to address this.

Lattice-based cryptography, one of the pillars of PQC, relies on mathematical problems that remain intractable even for quantum computers. Specifically, the complexity of lattice problems—such as the Learning With Errors (LWE) and the Shortest Vector Problem (SVP)—is deeply connected to profound geometric and numerical properties. These algorithms offer resistance to future quantum attacks and promise for applications like homomorphic encryption, paving the way for secure computations on encrypted data.

On the other hand, **Quantum Key Distribution** (QKD) represents an innovative paradigm that leverages fundamental principles of quantum mechanics, such as the no-cloning theorem and entanglement, to ensure intrinsically secure key generation. Unlike purely mathematical algorithms, QKD is grounded in physical laws, offering unconditional security at the physical level.

At the crossroads of advanced mathematics, computer science, and physics, these challenges demand innovative solutions that combine cutting-edge research with practical applications. This is why I founded the startup **Quantum2Pi**, an ambitious initiative dedicated to redefining security standards in the quantum era. The foundation of Quantum2Pi stems from realizing the need to unify mathematical and physical approaches to build resilient security in the quantum era. The goal is to develop solutions that integrate lattice-based cryptography with technologies like QKD, creating a security ecosystem that not only withstands quantum computing but also reflects a deep understanding of our universe's physical laws. At Quantum2Pi, we aim to bridge advanced theoretical research with practical applications, addressing not only the technological domain but also engaging the scientific community to collectively shape the future of quantum security.

Primary author(s) : Dr. CHIRICO, Ugo (Federico II and Quantum2pi)

Presenter(s) : Dr. CHIRICO, Ugo (Federico II and Quantum2pi)