Grant Number	**G-202105-67836**
Title	**Quantum-Driven Security in Emerging 5G Networking**
Project Duration	**12 months, contingent upon Prime Agreement extension from September 30, 2021**
Competition	**2021 US-Ukraine Cybersecurity Competition**

Proposal Reference

The Grantee’s proposal, ***Quantum-Driven Security in Emerging 5G Networking*** is herein incorporated by reference.

II. Abstract

Cryptography is essential for securing digital networking and information processing. Recent developments in quantum computing and processing are challenging the traditional security models and mechanisms, for example, NIST is in the process of standardizing new post-quantum ciphers. This project will analyze, design, build and apply the quantum computing and quantum-resistant techniques to secure the emerging 5G networking. We plan to make significant research contributions in the following three thrusts. First, we will secure the quantum key distribution by improving the modeling and analyzing its security against the state-of-the-art quantum computing technologies such as PT symmetry. Second, we will design and build a post-quantum public-key cryptosystem by analyzing the ciphers based on logarithmic signatures and empirically validating the cryptosystem with software implementations. Third, we will apply and integrate our quantum key distribution and post-quantum cryptosystem schemes to the emerging 5G networking to test the practicality and effectiveness of our research schemes to 5G networking. We have an interdisciplinary and sizable team comprised of strategically chosen and capable researchers in order to make multi-dimensional research contributions which will altogether enable the unified goal of preparing the future networking in the post-quantum era. This project will be a collaborative effort, involving students, female researchers, and early-career scientists across multiple institutions (one institution in the US and two institutions in Ukraine). This project will provide the foundational constructions and findings for further collaborations and research in this important direction to secure the digital networking and information systems in the post-quantum era.

III. Key Objectives / Milestones

The project objective is to build and apply the quantum computing and quantum-resistant technologies to secure the emerging 5G networking. It comprises of three research thrusts: Thrust 1 for Securing Quantum Key Distribution, Thrust 2 for Post-Quantum Cipher Based on Logarithmic Signature, and Thrust 3 for 5G Networking Integration. Thrust 1 and Thrust 2 will provide the foundational bases for the 5G networking integration and application in Thrust 3. The project will focus on the basic engineering research for its objectives and achievements, as opposed to those for commercialization. While this section focuses on the thrust objectives and the project team’s strategic construction, we provide greater details about the three research thrusts in the following sections.

Gennadii Khalimov, Professor	PI for Ukrainian Sub-team of the project. Researcher in cryptographic protection of information, information security systems and postquantum cryptography. Coresponsible for the implementation and the management of the project, will supervise Post-doctoral researchers, coordinate and co-work with the project team members.