University of Essex

Essex Futures BT– Masters Scholarship 2026-27

Project information: An Isogeny Based Post Quantum Secure Framework for UAVs

Classical cryptography, while effective in today's environments, faces significant challenges with the advent of quantum computing. Quantum computers have the potential to easily break many of the cryptographic schemes currently in use, such as Rivest-Shamir-Adleman (RSA) and Elliptic Curve Cryptography (ECC), by allowing for rapid factorization and solving discrete logarithm problems. As a result, there is a critical need to transition to post-quantum cryptography, which is designed to be secure against the capabilities of quantum attackers.

In this context, our focus on isogeny-based and certificateless cryptographic solutions aims to provide robust alternatives that can withstand the evolving landscape of computational threats, ensuring the security of our digital infrastructure for the future. Isogeny-based cryptography is becoming the preferred choice among post-quantum cryptographic methods, surpassing NIST-recommended schemes such as lattice-based, code-based, and hash-based cryptography. This preference is due to its smaller key sizes and the difficulty of computing isogenies, which provide strong defense mechanisms against both classical and quantum attacks.

The efficiency of isogeny-based systems is particularly important for resource-constrained environments, like Unmanned Aerial Vehicles (UAVs). Additionally, these systems can support a wide variety of cryptographic protocols, including encryption, digital signatures, and key exchange. This versatility offers greater flexibility for different applications compared to other NIST-recommended post-quantum cryptographic methods.

Objectives:

1. We will explore existing isogeny-based key management schemes. Next, we will analyze their cost and security vulnerabilities. Additionally, I will design new methods by refining isogeny-based protocols for practical use, focusing on efficient elliptic curves and innovative constructions of super singular

isogenies. These approaches aim to maintain a strong level of security while enhancing efficiency. Consequently, the schemes we develop will feature compact key sizes, making them promising solutions for resource-constrained devices in UAVs.

2. Traditional public key cryptosystems face challenges with certificate management, while identity-based cryptography is hindered by key escrow issues. To address these problems, we will design certificateless key management schemes that circumvent these issues.

3. We will be using the AVISPA tool for formal security analysis of the proposed research work, Random Oracle Model for provable security analysis, and using python language/C++ to implement the major operations utilizing the resource contain device. We will assess the proposed schemes in terms of computational cost, communication cost, memory overheads, and security requirements.