University of Essex

Essex Futures BT– Masters Scholarship 2026-27

Project information: Developing a Post-Quantum 5G-AKA for quantum safe authentication and key exchange in 5G.

5G-AKA, or 5G Authentication and Key Agreement, is a security protocol in 5G networks used for mutual authentication between the user device and the network. It establishes shared keys, ensuring secure communication. However, 5G-AKA is not inherently resilient to future quantum attacks. Within a cyber immune security framework, solutions must be resilient to entire classes of threats, including emerging ones like quantum attacks. Current deployment of 5G-AKA relies on cryptographic primitives vulnerable to quantum attacks. Therefore, it is crucial to migrate to a quantum-safe variant of 5G-AKA. Note that the UK's National Cyber Security Centre (NCSC) and has recommended adopting Post Quantum Cryptography to safeguard against future quantum-enabled cyber threats.

Outcomes:

This project aims to develop a post-quantum variant of the 5G-AKA protocol (PQ-5G-AKA) using NIST-standardized post-quantum algorithms. It will ensure forward secrecy, mutual authentication, and efficient key derivation under quantum-resistant assumptions. A prototype implementation will be developed and tested for performance and compatibility within the 5G architecture. PQ-5G-AKA will be developed to meet strict 5G performance constraints such as low latency and limited SIM card resources. The outcome will contribute to standardization efforts and future-proof mobile network authentication