Summer Research Project: Hardware Security of Superconducting Quantum Computing Systems

Faculty Supervisor: Selcuk Kose

This project explores the hardware security of superconducting quantum computers, focusing on the classical control and readout electronics that interface with the quantum processor. As quantum systems grow in scale and move toward shared cloud platforms, securing the underlying hardware becomes as important as securing the quantum algorithms themselves. The control electronics in these systems rely on Single Flux Quantum (SFQ) circuits—a specialized, ultra-fast cryogenic logic family whose security properties remain largely unexplored.

The project may investigate one of the following three hardware security challenges in this context. The first is side-channel vulnerabilities: whether physical signals such as current or power fluctuations in the control electronics inadvertently reveal information about qubit states. The second is hardware Trojans: the possibility that malicious logic inserted into SFQ circuits during design or fabrication could corrupt qubit operations or leak data undetected. The third is Physical Unclonable Functions (PUFs): whether the natural manufacturing variations of Josephson junctions can serve as unforgeable device fingerprints for authentication. The student will use circuit simulation tools to model SFQ circuits and assess the feasibility of these threats and defenses.

Prerequisites: Basic circuit theory and digital logic. Familiarity with Python or a similar scripting language is helpful. No prior background in quantum computing or hardware security is assumed.

Learning Outcomes: Introduction to superconducting quantum computing hardware, hardware security concepts (side-channel attacks, hardware Trojans, PUFs), SFQ circuit simulation, data analysis, technical documentation and research communication.