Statement of Purpose

Modern IoT systems are resource-constrained, dynamic, and poorly served by classical cryptography. I therefore seek to build security frameworks that embed quantum principles at their core. This goal motivates my application to the PhD program in Electrical and Computer Engineering at NUS, where I aim to bridge quantum security mechanisms with next-generation distributed infrastructures.

Background. I received my undergraduate degree in Computer Science and Engineering from Seoul National University of Science and Technology (SeoulTech), where I also enrolled in its integrated MS/PhD program. My early work focused on lightweight authentication and secure deployment in constrained environments. During this time, I developed a growing interest in quantum information science, particularly its potential to redefine security from foundational principles. However, due to limited resources in this field at SeoulTech, I withdrew from the program to pursue this direction more deeply. I subsequently joined the Centre for Quantum Technologies (CQT) at the NUS. Under the guidance of **Prof. Divesh Aggarwal** and **Dr. Kishor Bharti** (from A*STAR), I worked on a unitary-inversion protocol to test the quantumness of untrusted device. While this introduced me to pure quantum theory, I realised that my strength lies not in long theoretical derivations, but in connecting abstract models with real-world constraints. Unlike theoretical research, which demands rigorous formalism and detailed proofs—sometimes extending over dozens of pages—applied system design emphasises feasible deployment and engineering soundness over exhaustive derivations.

Research Experience. Throughout my academic path, I have pursued research at the intersection of sound theory and engineering practicality. At SeoulTech, I co-authored papers on authentication, key agreement under constraints, and deployment-aware protocol design. These experiences deepened my understanding of embedded limitations and secure design trade-offs. At CQT, I worked on quantum authentication and adversarial modelling. These studies sharpened my foundation in quantum formalism, but more importantly, inspired a shift in focus: designing quantum tools that are not only provably secure but also deployable in constrained infrastructures.

Research Interest. My research interests lie in combining quantum information theory with applied system security. I aim to embed quantum primitives—such as uncloneability, entanglement, and measurement disturbance—into IoT. The goal is to construct infrastructures that provide operationally relevant security guarantees derived from quantum properties. This perspective is shaped by my dual experience in classical and quantum domains. I am particularly interested in **Prof. Biplab Sikdar**'s research on IoT security and cybersecurity. Notably, his recent work also explores quantum technologies in the context of IoT, including protocols that leverage quantum characteristics to enhance the security of constrained devices, which aligns closely with my objective.

Program Fit. Having worked at CQT, I have come to appreciate NUS's academic culture—rigorous, collaborative, and interdisciplinary—which makes it an ideal environment for my doctoral training. Within ECE, I am particularly drawn to Prof. Biplab Sikdar's group, whose work spans secure system design and the application of quantum methods to IoT scenarios. His recent publications demonstrate both theoretical depth and deployment awareness, aligning closely with my goal of building quantum-secure architectures for resource-constrained systems.