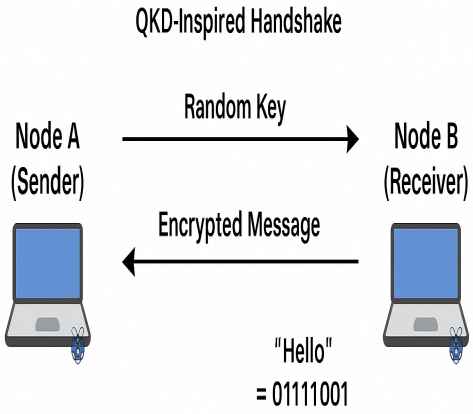
OTTO VON GUERICKE UNIVERSITÄT MAGDEBURG | INF | FACULTY OF COMPUTER SCIENCE | Communication and Networked Systems

Master Thesis
Lightweight Secure Message Exchange Using QKD-Inspired Handshakes

Motivation

In many IoT environments, especially low-power networks such as those using Raspberry Pis or LoRa devices, using traditional encryption (e.g., TLS or standard AES protocols) can be too resource-intensive.
This thesis proposes a lightweight security framework inspired by Quantum Key Distribution (QKD) protocols like BB84, but implemented in a classical (non-quantum) environment.
The aim is to simulate a secure handshake protocol to exchange symmetric keys, which are then used to encrypt communication between nodes. This will be tested directly in our MIoT-Lab at the University of Magdeburg.



The key exchange is performed using a secure handshake, and the actual data exchange is done using symmetric encryption. The key exchange will be based on the QKD protocol, but the actual data exchange will use a lightweight symmetric encryption algorithm (e.g., AES or XOR). The goal is to create a secure communication channel that is efficient enough for low-power devices, while still providing a high level of security.

Project type	Master Thesis	Contact	M.Sc. Ibrahima Ndiaye
Duration	6 Months	E-Mail	ibrahima.ndiaye@ovgu.de
Language(s)	English	Room	G29-320
Field	Computer Science	Tel.	+49 391 67-54925

Objective

The objective of this thesis is to design and evaluate a QKD-inspired, lightweight secure message exchange protocol for low-power devices within our campus IoT testbed.
Steps to be completed:

- **Step 1 – Literature Review:** Study QKD (e.g., BB84) protocols and current secure messaging systems (TLS, AES, MQTT over TLS).
- **Step 2 – Protocol Design:** Implement a QKD-style key handshake using XOR or AES encryption for actual communication.
- **Step 3 – Implementation:** Use Raspberry Pi nodes and available LoRa/Wi-Fi hardware to build the system.
- **Step 4 – Evaluation:** Compare energy, latency, and security metrics vs. traditional methods.

Prerequisites

- Background in computer networks and cryptography
- Basic understanding of IoT protocols (MQTT/HTTP)
- Familiarity with Python or C, and Linux environments
- Motivation to work with real hardware and testbeds

References

[1] **I. F. Akyildiz et al.**, "A survey on sensor networks," *IEEE Communications Magazine*, 2002.

[2] **C. H. Bennett and G. Brassard**, "Quantum cryptography: Public key distribution and coin tossing," *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, 1984.

[3] **T. Weigold et al.**, "Resource-Efficient Quantum-Inspired Key Exchange for IoT," *IEEE Access*, 2022.

Project type	Master Thesis	Contact	M.Sc. Ibrahima Ndiaye
Duration	6 Months	E-Mail	ibrahima.ndiaye@ovgu.de
Language(s)	English	Room	G29-320
Field	Computer Science	Tel.	+49 391 67-54925