Technical Test - Quantum Cryptography Research Engineer

1 Quantum Key Distribution (QKD)

QKD is a communication protocol that enables two users to exchange provably secure secret classical keys via an insecure quantum communication channel, and a classical authenticated channel. A QKD network includes a "secrets plane" that delivers secret keys to other subsystems. IPsec is a standardized protocol suite for secure encrypted communication. IPsec can be configured to use any cryptography protocol for the encryption and authentication to keep data secret and to guarantee the integrity. The bulk data encryption portion of IPsec requires the use of a secret key shared only between the pair of IPsec gateways. Internet Key Exchange (IKE) provides several important functions: creation of the shared secret key, management of the use of that key, and negotiation of the details of the bulk data encryption method and conditions under which it is applied. Standard IKE uses distributed Diffie-Hellman protocol for generating the secret key.

In this assignment, our overall goal is to replace the distributed Diffie-Hellman protocol with a QKD protocol, and use the QKD keys for encrypting messages. However, the candidate can consider QKD protocol as a black-box resource that outputs a stream of keys between two users, after the initiation of the protocol.

2 Protocol Design

Design an IKE protocol for IPSec consuming QKD keys. Please read through carefully Link1. Referring to Fig.1 of Link1, the candidate will design

1. the secure local connection between QKD device and IPSec Gateway; and
2. the Initialization, Re-keying and Fallback protocols between IPSec Gateways (Fig. 5, 7, 8 of Link1).

The following are out of scope of the test:

- Operation of fallback key generation methods
- Operation of QKD network

3 Implementation

The candidate is free to select a suitable programming language for the task. Considering the implementation with production in mind, the implementation should be developed with good software engineering principles with considerations for performance optimization. The candidate may use authenticated REST API as the interface between QKD devices and IPSec Gateways. Candidate may use standard RNG functions to emulate QKD keys and fallback key generators.

4 Evaluation Criteria

1. Proper implementation of the functionalities that are mentioned within the scope of Section 2.
2. The performance efficiency of the designed protocol, and the interfaces, as well as the readability, and maintainability of the implementation.
3. Proper explanation of the design implementation choices.