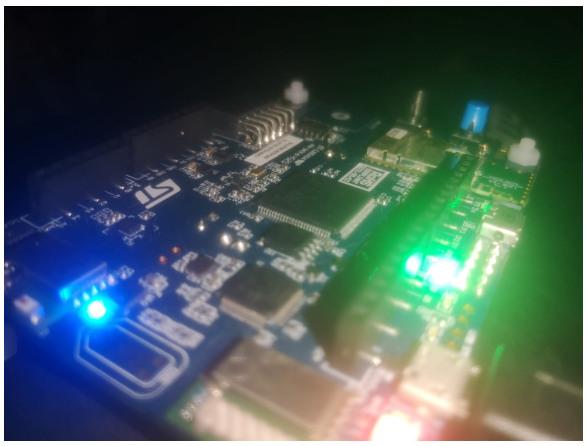
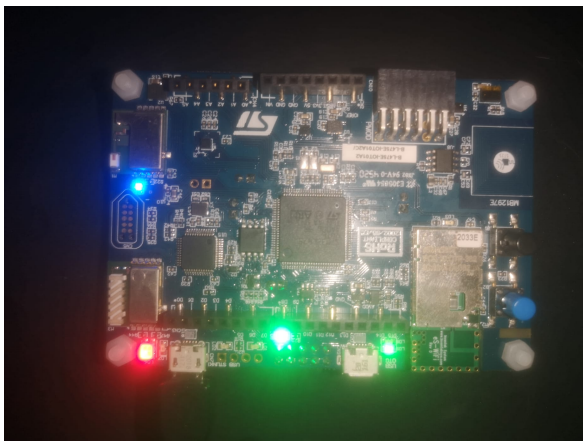
Nano Satellite Post Quantum Cryptography

Nano Satellites are used for Quantum Key Distribution (QKD) in order to create secure cryptographic systems for communication safe against the rise of quantum computers. Therefore, a low-power embedded system was designed that incorporates Post Quantum Cryptography algorithms that are also secure against quantum computers in order to assist QKD systems.



STM32 IoT Node dev board from the side



STM32 IoT Node dev board from the top

Task

Quantum Computers are getting more sophisticated and threaten to break today's cryptographic system. An alternative is Quantum Key Distribution (QKD), which establishes keys using quantum particles such as photons. With the BB84 or E91 protocol a symmetric key can be established. Since photons are sent with optical communication technology, they are heavily dependent on good weather conditions. It turns out, for authentication, Post Quantum Cryptographic (PQC) algorithms can be used as to assist QKD Satellites, so the task was to develop a device running on low-power hardware that shows such PQC algorithms running.

Solution

A Raspberry Pi 4 Model B was chosen to develop a proof of concept software. The software was designed with a real-time operating system to encapsulate the core functionalities into separate tasks that could be executed with commands passed into a command line interface. A critical part was the entropy needed for the PQC algorithms to work securely, this could be solved using the on chip hardware random number generator (RNG) which outputs 32-bit random values using an analogue circuit that samples noise.

How it works

The Raspberry Pi simulates the nanosatellite, any computer can connect to it and over a TCP protocol in which all the PQC functionality is embedded start comunicating post-quantum securely. The host needs the PQC software in order to communicate with it. The procedure is as follows: Firstly the TCP connection is established using traditional encryption schemes, then the authentication algorithm Dilithium establishes a post-quantum safe authentication, and after that is done, the Kyber algorithm comes into play and generates a shared key between both parties in order to exchange one AES256 master key, after which communication can commence.

Random Number Generators

Random Number Generators (RNG) are algorithms or devices that produce values which are as random as possible. There are three types of RNGs: pseudo random number generators, true random number generator, and quantum random number Generators. The first one is used in games and other applications where perfect randomness is not required and no security is at risk. However, for cryptography pseudo RNGs should not be used as they might get exploited. True RNGs are used that work with electrical noise that behaves truly randomly. A new way to generate even more random numbers are Quantum Random Number Generators which work on the principle of quantum mechanical processes where for example an electron's spin is measured, which is either up or down with each having a probability of 50 %.

Project Team:
Adrian Grana Nunes Rodrigues

Client:
SpeQtral Pte Ltd, Singapur

Coaches:
Prof. Dr. Christoph Wildfeuer,
Prof. Dr. Willi Meier