White Paper

Quantum Hardware - QKD Enabled Chips

anaxa.tech

Abstract

We are currently living in a connected world powered by the Internet that consists of billions of different nodes or IoT devices. The data stored within our network is centralized, which results in the common occurrence of data breaches and cybersecurity threats. There are over 80,000 cyber attacks made per day (Purplesec, 2019) and in the healthcare space specifically, data breaches that target EMRs and other documents containing sensitive information result in 40 million stolen records each year (Seh, 2020), resulting in industry losing over $6 billion (CMS, 2017).

Current solutions that attempt to enforce security are only limited to software-based platforms, when the root cause in this ongoing problem lies in the current hardware capabilities of our devices. To address this, Anaxa proposes to utilize the concept of quantum key distribution (QKD) enabled chips that can be implemented to our current IoT devices. The advantage that QKD brings is an unhackable and latency-free connection, which has the potential to eliminate all security concerns when transferring data containing sensitive information.

Anaxa utilizes silicon and indium phosphide based platforms to test the BB84 (QKD) protocol. The transmitter starts the entanglement and produces the randomly generated key before transmission, while the receiver receives and verifies the key. The efficacy of this solution is determined by measuring the key rate, count rate, and coincidence probability.

Problem:

The Internet currently is a distributed network that consists of billions of different nodes. Though the Internet itself is not centralized, most of the data available online is stored and controlled by a few technology companies that are able to build these massive data centers that can handle a vast amount of information. As a result, concerns such as cybersecurity threats and data breaches are common. The convenience and affordability of the Internet has provided many the opportunity of leveraging different platforms across the network that allows for global communication and interaction.

There is a continually increasing number of devices within the Internet of Things (IoT) in both the individual and industry levels, with a total of 9.5 billion devices connected to the Internet as of 2019. The industry is only increasing, and is expected to have 24 billion devices by 2030 at a compound annual growth rate of 11% per year. However, as a cost of this, with the growing number of devices adding to our network, rising security hacks and latency delays are both major concerns. As of 2018, there are 80,000 cyberattacks being made per day or over 30 million attacks per year.

IoT devices are currently being used extensively in the healthcare industry, where over 40 million records get stolen or lost each year, resulting in the industry losing over $6.2 billion. Each data breach can account for more than $3.7 million. One of the biggest reasons for this is due to the current IoT infrastructure. Most IoT networks do not enforce security between the IoT device and communication gateway, where the protection of data is only applied and enforced between the gateway and receiving endpoint.

Quantum Key Distribution (QKD) Enabled Chips

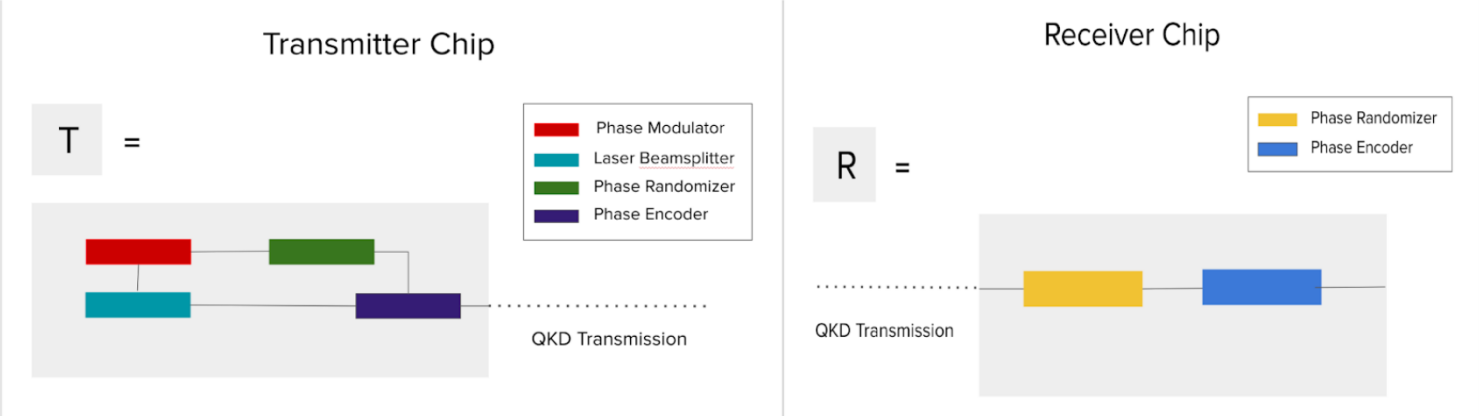
In order to achieve a solution where the transmission of data between IoT devices, specifically with electronic medical records (EMRs) in the healthcare space, Anaxa utilizes an indium-phosphide based transmitter chip and silicon oxynitride-based receiver chip to be implemented in the IoT devices that store patients' health records and the data centers within the health data ecosystem. A QKD link is formed between the two types of chips generated through quantum entanglement and tunneling, which ensures an unhackable, secure and latency-free connection where no third party can intercept during the transmission of patients' data.

The indium-phosphide transmitter chip starts the entanglement and produces the randomly generated key before transmission. The components within the chip include an encoder, randomizer and modulator which are used to encode the different states with phase values and random numbers to generate pulse trains of information to be sent to the receiver chip.

The transmitter chip would be implemented to an IoT device by integrating the chip onto a development board attached to the device within a hospital or health insurance agency. A cryptographic API will then be implemented into a cloud service where the health data information is stored. If this solution were to be implemented in an actual ecosystem that stores patient EMRs including a hospital and datacenter or health insurance agency, a few of the devices with the transmitter chip would be connected to a central node where the information would be transmitted over a regular telecom fiber using QKD onto the devices with the receiver chips.

The receiver chip is implemented onto the other end of the transmitter (an IoT device in the data center, for example), which is made of components including a phase decoder and randomizer. Its function is to receive and verify the key sent from the first transmitter so that the entanglement and transmission is complete. Because of the newly established QKD connection, anything that tries to break into the connection between the transmitter and receiver would automatically stop the transmission.

The importance of QKD comes from its effectiveness in detecting an eavesdropper instantaneously. According to the No Cloning Theorem, quantum particles are also unable to be duplicated. When photons containing packets of information are generated into random states and are then able to be transmitted between two separate locations which create entanglement and share an encryption key.



Connection Link

Silicon and indium phosphide based platforms for the chips will be used to test the BB84 protocol, a type of QKD scheme. The chip provides decoy-state modulation and polarization encoding.

Generating the entanglement to establish the QKD link: Gain-switched lasers, wavelengths are stabilized with tunable temperature controllers. The photons are injected into the cavity of the slave laser, which generate phase-randomized light pulses. A master gain-switch laser will inject photons into a slave gain-switched laser. The indium phosphide based transmitter chip generates phase-randomized light pulses, from the beam splitters, phase modulators and intensity modulators. The VOA consists of a PIN diode which is used for current injection to attenuate the pulses to a single-photon level. The VOA output is connected to a polarization modulator which will prepare 4 BB84 states. The BB84 states are generated with a beam splitter and single photon detectors in order to establish the QKD link.

Detection: There will be a second chip acting as the silicon-oxynitride receiver, that measures the bell states generated from the BB84 protocol sent from the transmitter. The Mach-Zehnder interferometer acts as a tunable beamsplitter, routing to a single photon detector. The receiver is able to publicly announce the successful events that indicate the encoding knowledge without revealing information about the secret key. The receiver is now able to infer what the secret key from the basis states given from the transmitter. From there, an intensity modulator, polarization modulator and variable optical attenuators are used to measure the quantum states' count rate, coincidence probability, and key rate in order to measure the effectiveness of the QKD link.