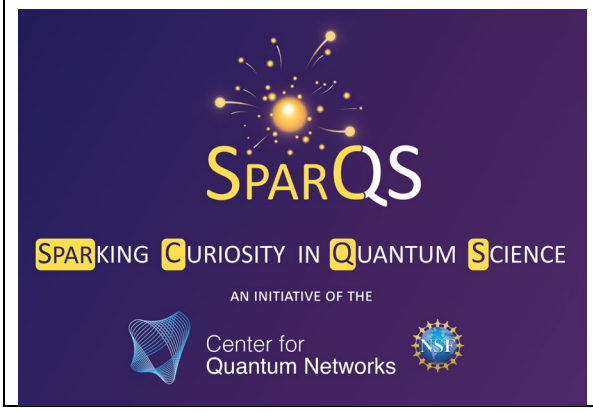
CS486C – Senior Capstone Design in Computer Science

Project Description

Project Title: BB84 – Can you catch Agent E?	
Sponsor Information: 	Inès Montaño, Associate Professor, APMS QPEP – Quantum Photonics and Emerging Phenomena Center for Materials Interfaces in Research and Applications (¡MIRA!) Center for Quantum Networks (CQN) Ines.montano@nau.edu

Project Overview:

Our key idea:

To introduce a broader audience to the fascinating and mind-boggling world of quantum science, we recently implemented the pre college initiative SPARCQS - **Spar**king **C**uriosity in **Q**uantum **S**cience. The goal of SPARQS is to bring 'hands on' quantum science experiences to schools and communities, provide students with the opportunity to observe engaging demonstrations, perform experiments, learn about career opportunities in STEM, and most importantly – have fun with quantum science!

One of the modalities of SPARCQS is a 10' Van Trailer, a mobile quantum laboratory to bring 'hands on' quantum science experiences to schools and communities, which we implemented over the summer of 2022. The idea behind the SPARCQS trailer is to facilitate meaningful outreach that does exactly that – it reaches out to pre college students. Traditional outreach initiatives largely rely on the participants coming to the outreach providers to be educated and thus are often limited to urban populations.

The SPARCQS trailer allows us to bring quantum science to the participants, to schools as well as communities in general. Bringing a mobile quantum laboratory equipped with conceptual 'hand's on' quantum science experiences to schools and community events, we will be able to increase quantum awareness in urban as well as rural and other underserved communities. Over the summer, SPARCQS has visited kids at a local summer camp (K-6), an all-girls Quantum Computing summer camp in Tucson (middle/high school students), students participating in the NAU C.A.R.E. program (high school students) and a week-long STEAM event at the Mall of America in Minnesota! It has been an incredible experience and we are excited to introduce even more people to SPARCQS in the future!

Figure 1: SPARCQS - Summer 2022

However, already over the course of this summer we have received requests for visits that are hard or impossible to meet. Even though our SPARCQS trailer allows us to travel to remote places, it is not feasible for us to simply travel, e.g., back to Minnesota to visit a high school there. SPARCQS was really implemented to visit remote communities in Arizona/New Mexico, not to travel cross-country to schools 1500 miles away. Additionally, there are other factors such as Covid restrictions that can prevent an in-person visit even at schools closer to us.

For this reason, we have been developing the concept of 'virtual visits' where students receive a visit by the SPARCQS team - via zoom. The challenge of a 'virtual visit' is to capture the benefits of an in-person visit with actual hands on experiences. We believe that a reason for the appeal of SPARCQS is that students can actually interact with our demos. In our Quantum Cryptography setup, e.g., students get to use lasers and polarizers to send secret messages! Who would not have fun playing with actual lasers!

Using simulations of demos is an option but it would be so much more impactful if the students could actually control the actual equipment – just remotely. To pilot this idea, we have been working on retrofitting our Quantum Cryptography setup with remote control options.

To illustrate what is needed, below we give a quick overview over the physics behind the Quantum Key Distribution, specifically BB84, and how we use our Quantum Cryptography setup at an in-person SPARCQS visit to introduce students to this cool technology.

Basics of BB84:
We all know that encryption of data is an important topic. In many systems, data is encrypted using a public key which is basically a large number resulting from multiplying two prime numbers. If these two prime numbers are known (i.e., the private key is known), the encrypted message can easily be decrypted. Generally, this is a safe system since it is very difficult to find the private key. However, quantum computers are predicted to allow hackers to quickly find private keys since they are very great at factorizing large numbers. That is a problem!

Quantum Key Distribution (QKD) is a communication protocol that allows two parties to share a RANDOM secret key which can be used to encrypt/decrypt messages. In contrast to the public/private keys mentioned before, the keys in QKD protocols are un-hackable since they are RANDOM, there is no pattern.
BB84 is a specific QKD protocol that uses polarized light to generate and send such a random key.

Here is how it works in more detail:
The sender (Alice or as SPARCQS calls it 'Agent A') wants to send a secret key of ones and zeros to the receiver (Bob or 'Agent B'). To do so, Agent A uses linearly polarized photons. Using a polarizer, Agent A can encode zeros and ones by choosing the polarization of a light source. There are two different ways to polarize the light. Option 1) the light is polarized horizontally/vertically (0 deg/90 deg). This is called the '+ basis'. Option 2) the light is polarized diagonally (-45 deg/45 deg). This is called the 'x basis'. Agent A can now send a 'zero' by setting the polarizer to either 0 deg (+ basis) or -45 deg (x basis) and a 'one' by setting the polarizer to either 90 deg (+ basis) or 45 deg (x basis). Agent B then uses the two bases (+ and x) to interpret the incoming light as either a zero or a one. Whenever Agent A and Agent B made the same choice for their basis (both choosing the + basis or both choosing the x basis), the message gets transmitted correctly. If they choose different bases, the message has to be discarded. Figure 2 shows one of our SPARCQS stickers that sketches out the basic concept.

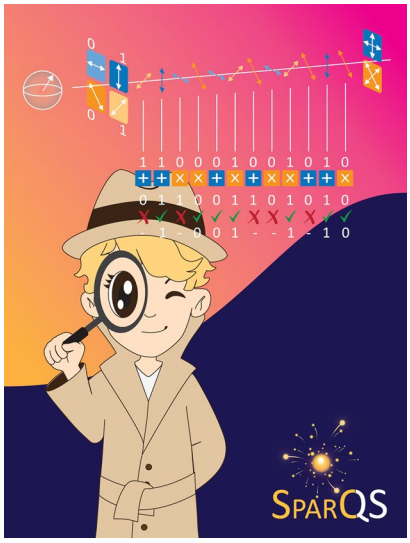


Figure 2 BB84 concept

Note also that thanks to this system, Agent A and Agent B will be able to actually tell if someone was trying to spy on the message! That's the power of Quantum Mechanics!

The BB84 protocol can be challenging but it is much easier to understand when students try it out using the actual optics setup! In a SPARCQS visit, we first introduce the idea of communicating through light, concept of light polarization and then in steps work our way towards a full BB84 run.

Figure 3 BB84 demo

Project Description:

For our 'virtual visits' we would like the students to remotely control the polarizers and see the results of the detectors so that they can run through a complete BB84 protocol. Just like they would during an in-person visit. We are configuring all of the devices (e.g., the lasers, polarizers, etc.) so they are operated electronically via Arduino controllers.

We need your Capstone team to provide a web page with control buttons that would communicate remotely (ultimately via the Internet) to the Arduino devices so the students can conduct the experiments themselves. They will be able to see how the encryption gets through, and in some cases how it doesn't, and make their next experimental decisions from there.

At this point, creating the web page with the control buttons that could work in concert with a Zoom connection must be the minimum component. However, a great, and achievable stretch goal would be to display the equipment operation being monitored by the local cameras

Another advanced possibility would be to get feedback from the Arduino devices and display that on the screen as well.

This being an innovative system, there may be more and/or other operations that could be included. We can discuss this as you begin the design process

Knowledge, skills, and expertise required for this project:

- Network/Internet communication
- Web page development with quality UI/UX presentation that creates a friendly and easy to use interface
- Web page development that manages two-way communication to the devices, including potentially video display

Equipment Requirements:

- There should be no equipment or software required other than a development platform and software/tools freely available online.
- However, if the team identifies equipment that could be used, the Sponsor has the potential to fund purchase of item(s) as needed

Software and other Deliverables:

- A strong as-built report detailing the design and implementation of the product in a complete, clear and professional manner. This document should provide a strong basis for future development of the product.
- Complete architecture, connectivity, and device management instructions must also be provided as needed
- Complete professionally-documented codebase, delivered both as a repository in GitHub, BitBucket, or some other version control repository; and as a physical archive on a USB drive.