Quantum Key Distribution Emulation System

Brit Riggs
Northern Arizona University
June 18, 2021

Overview We improve the BB84 protocol with the addition of decoy states, another wavelength of light, and a physical unclonable function (PUF). However, this paper will focus on the decoy states and additional wavelength of light. While our full-sized system is being assembled, we are using the custom demonstration kit from Thorlabs to emulate the full system, further develop the protocol, and study the error rates.

I BB84 Brief Review

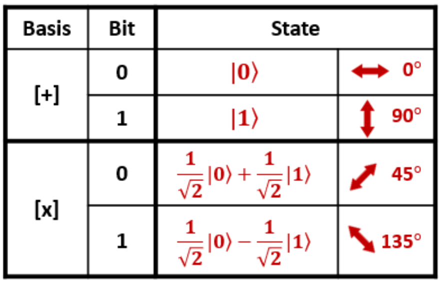
The discovery of algorithms that can be run on quantum computers to break popular secure key exchange algorithms created an urgent need for quantum resistant key exchange protocols. Charles Bennett and Gilles Brassard devised the well-known quantum key distribution (QKD) protocol, called BB84, in their 1984 paper [1]. The basic idea is that two parties, Alice and Bob, use information encoded in single photon polarization states to securely generate cryptographic keys. The security of BB84 lies in the properties of quantum mechanics whereby single photon states cannot be measured without changing the state, meaning that eavesdroppers will be unable to measure the exchanged information without changing the states and thus exposing their presence.

The BB84 protocol uses polarization states of single photons to encode information. Light is made up of electromagnetic waves, and polarization is the direction that the electric field oscillates in. We can represent a linearly polarized photon $|\theta\rangle$ in terms of the horizontal and vertical states by the equation $|\theta\rangle = \cos\theta\,|0\rangle + \sin\theta\,|1\rangle$ where $|0\rangle$ and $|1\rangle$ represent the horizontally and vertically polarized states, respectively [2].

In order to represent the linear polarization states of single photons, the protocol utilizes two bases: the rectilinear $[+]$ and diagonal $[\times]$ bases. The rectilinear basis represents either a horizontally or vertically polarized photon state and can be thought of as 0° and 90°. Similarly, the diagonal basis represents a superposition of the horizontal and vertical states and can be thought of as 45° and 135°.

Using these four states, Alice and Bob can encode a stream of bits and securely generate the same key. To encode a random stream of bits in the photons, Alice will randomly select a basis ($[+]$ or $[\times]$) and use the chart in Fig. 1 to polarize each photon accordingly and send it to Bob. Bob will measure each photon using a random basis selection and decode each bit according to the same chart in Fig. 1. Alice and Bob will then communicate specific information, discard bits accordingly, and use a subset of the key to check for errors.

Fig. 1: BB84 encoding chart summary.



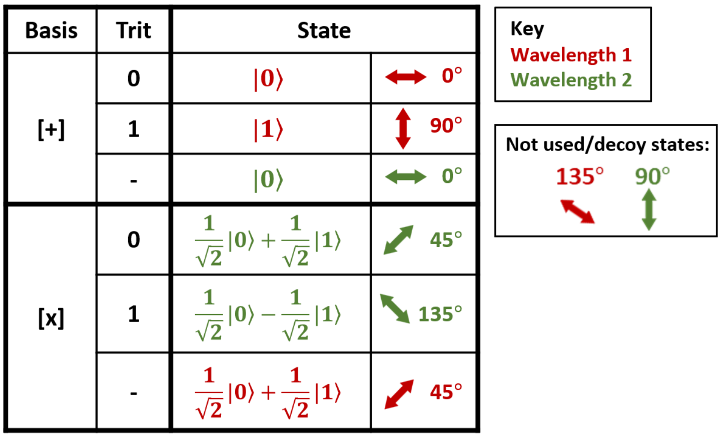
Basis	Bit	State	
[+]	0	$\|0\rangle$	↔ 0°
	1	$\|1\rangle$	↕ 90°
[x]	0	$\frac{1}{\sqrt{2}}\|0\rangle + \frac{1}{\sqrt{2}}\|1\rangle$	⤢ 45°
	1	$\frac{1}{\sqrt{2}}\|0\rangle - \frac{1}{\sqrt{2}}\|1\rangle$	⤡ 135°

II Implementation of Two Wavelengths and Decoy States

We can improve the BB84 protocol by introducing a second wavelength which doubles the amount of polarization options that Alice can encode data with (four states per wavelength). The additional states allow for the implementation of decoy states and use of ternary or quaternary state input stream values (as opposed to binary for bits). Using ternary or quaternary data means that we have three (ternary) or four (quaternary) states to send data with.

Fig. 2 shows the encoding chart for a ternary protocol. In contrast to the BB84 chart in Fig. 1, our modified protocol chart in Fig. 2 has three data states: 0, 1, and -. Notice that two states–135° for wavelength 1 and 90° for wavelength 2–were not used. These unused states act as the decoy states and, in theory, should not show up unless an eavesdropper is present. The states would not be sent intentionally, and therefore should show up if an eavesdropper interfered in a way that generated the decoy states. However, in practice, the decoy states may show up occasionally due to various error sources. The important point is that if the number of decoy state cases that we find is significantly large, then we know there must be an eavesdropper present.

Fig. 2: Ternary protocol encoding chart for two wavelengths.



Basis	Trit	State	
[+]	0	$\vert 0\rangle$	↔ 0°
	1	$\vert 1\rangle$	↕ 90°
	-	$\vert 0\rangle$	↔ 0°
[x]	0	$\frac{1}{\sqrt{2}}\vert 0\rangle + \frac{1}{\sqrt{2}}\vert 1\rangle$	↗ 45°
	1	$\frac{1}{\sqrt{2}}\vert 0\rangle - \frac{1}{\sqrt{2}}\vert 1\rangle$	↘ 135°
	-	$\frac{1}{\sqrt{2}}\vert 0\rangle + \frac{1}{\sqrt{2}}\vert 1\rangle$	↗ 45°

Key
Wavelength 1
Wavelength 2

Not used/decoy states:
135° ↘ 90° ↕

The largest advantage of adding a wavelength and using ternary and quaternary input options is eliminating the need to check for error since we can check for the existence of decoy states. Alice and Bob no longer need to waste a subsection of their key comparing for error because the presence of decoy states will be the error check.

III Conclusion

With quantum computers threatening existing key exchange protocols, the need for new methods of secure key exchange is critical. Quantum key distribution is a promising, quantum computer resistant substitution for existing key exchange protocols because of fundamental quantum mechanical properties. One of the first methods was BB84, and we are working on improvements to the protocol by adding a second wavelength and additional states to eliminate the need for wasting a subsection of the final key to compare bits for error and eavesdropper presence.

References

[1] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," *Theoretical Computer Science*, vol. 560, p. 7–11, Dec 2014. [Online]. Available: http://dx.doi.org/10.1016/j.tcs.2014.05.025

[2] J. Rothberg, "Physics 225/315 lecture introduction to quantum mechanics," 01 2008.