Prototyping QKD BB84 protocol demonstration

Keio University Van Meter Laboratory **AQUA: Advancing QUantum Architecture**
Iori Mizutani(iomz@sfc.wide.ad.jp), Koji Murata(malt@sfc.wide.ad.jp) http://aqua.sfc.wide.ad.jp

Motivation

Quantum Key Distribution enables secure key generation when the era of quantum computation arrives and Shor's algorithm can be used to crack RSA keys and Diffie-Hellman key exchanges. What is wonderful about QKD is that it can be easily demonstraed to those who are not very familiar with quantum technologies without any quantum mechanics. We have made a small gadget and the WEB interface to show the actual procedure to produce and distribute a quantum key.
This is an open-source project and is being developed on GitHub. We are hoping to see a lot more people find quantum technologies interesting from reproducing it or even joining us.

Demonstration apparatus

Transmission of phase encoded states is the key to the BB84 protocol. We have implemented a laser module and polarizer frames to represent two orthogonal states (*bit*) in two conjugate phases (*basis*). Alice's polarizer frame rotates by 0°, 45°, 90° or 135° using a servo motor to encode a state into the laser. For example, if the laser passes through in area C, the laser is polarized corresponing to [Bit 0 : Basis ×]. On the other hand, Bob's and Eve's polarizer frames only rotate by 0° and 45° as explained later.

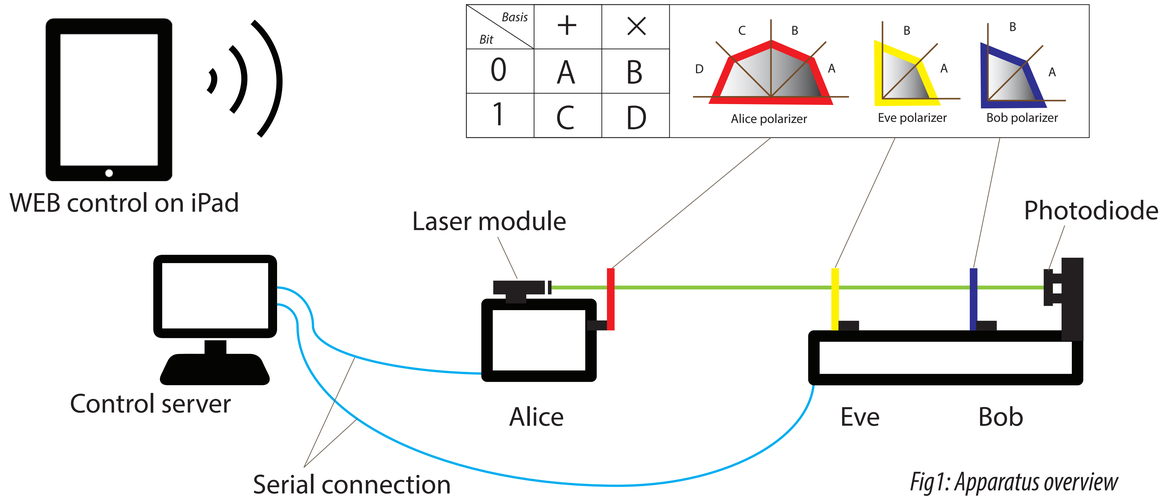

Fig1: Apparatus overview

Step-to-step procedure along with BB84 protocol

1 To generate and distribute a key, Alice and Bob first needs to decide how to send and receive bits. In this demo, they use twenty bits to generate the key so Alice chooses a combination of bits and bases while Bob and optionally Eve choose only bases to detect or eavesdrop the laser.
Our web interface is optimized for iPad with AJAX + HTML5 + CSS3. Once all the users finished input, the combination of bits and bases are pushed to Control Server, and then the apparatus start the distribution.

2 As soon as the combination is sent to the apparatus, Alice fires up the laser and rotate the polarizer to the first position generated by the user input. For instance, if the first choice of Alice is to send [Bit 1: Base ×], the polarizer rotate to D.

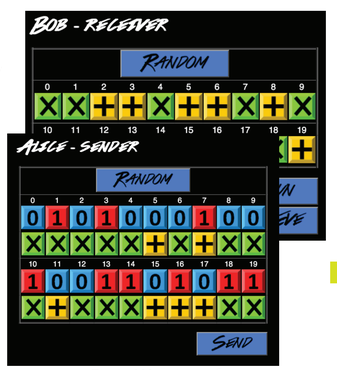

Fig2: Web interfaces

3 Bob rotates the polarizer to the position pushed, then measure the illuminance by the photodiode. If Eve is present, she rotates her polarizer just before Bob and interfere the communication. Bob decodes the laser by measuring the illuminance of the laser at either 0° or 45° position. Here, two positions can give enough information — when Alice encodes at 0° and Bob (or Eve) tries to detect at 90°, the laser is completely blocked before it reaches the photodiode since states in (0°, 90°) and (45°,135°) are orthogonal within the pairs. Bob's measurement is based on the two calibration values calculated in prior to the demonstration; the bit is "0" if the illuminance is darker than LOW threshold value, the bit is "1" if it's brighter than HIGH threshold, and if it doesn't fall into either of them, the bit is at random. (See the figure on the right) This scheme is required to simulate the behavior of single photons and not derived from BB84. We are using strong laser pulses instead of serial single photon emission.

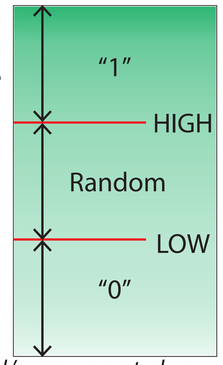

Fig3: Bob's measurement scheme

4 Repeat **2** and **3** until all twenty bits are transmitted. After completion, the values measured by Bob are sent back to Control server, which compares them with the bases actually used in Alice and Bob. Take only those transmitted in the same basis and make them into a key. Discard the bit if bases disagree.

Alice bit	1	1	1	1	1	0	0	0	1	0	0	1	1	1	1	0	1	1	1	1
Alice base	×	×	×	+	×	+	×	+	+	+	×	×	+	+	×	+	×	+	+	+
Bob base	+	×	+	×	×	×	×	+	×	+	×	×	×	+	×	+	+	×	+	×
Bob bit	1	1	0	1	1	0	0	0	1	0	0	1	0	1	1	0	1	0	1	0
Key		1			1		0	0		0	0	1		1	1	0			1	

Fig4: Key generation table
Notice that when the bases disagree, the bit measured by Bob is totally at random and not valid for the key.

5 Optional. When Eve is present in the transmission path, the value measured by Bob differs from what it is supposed to be. To discover the eavesdropping, Alice and Bob choose several bits from the key generated, exchange them, and then compare. If a particular bit does NOT agree, it is a sign of the presence of an eavesdropper. In reality, we change the quantum channel (in this case the path of the laser) to avoid eavesdropping once Eve's presence is discovered. See how it works in the demonstration!

Developing on GitHub

We are developing this project on GitHub under the terms of the MIT License. So anyone can easily reproduce the apparatus and modify the source code of firmware, web script, and any part in this project. Please see the detail at ...

https://github.com/iomz/qkd-laser-experiment

Wikipedia translation

Articles in Wikipedia are always good start to understand something new. To introduce more about QKD, we have translated the English article "Quantum key distribution" into Japanese.

3D animation of QKD

Computer graphics is another way of demonstration. Before this project we produced a 3-minute long 3D animation of QKD. The video is available from our web site. Go to http://aqua.sfc.wide.ad.jp !

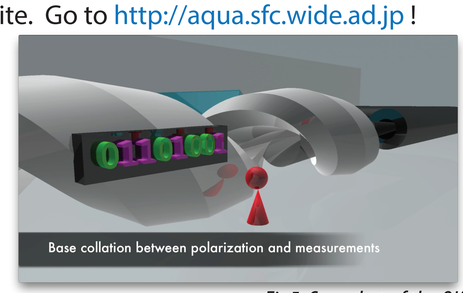

Fig5: Snapshot of the QKD animation

References

[Wikipedia - 量子鍵配送] http://ja.wikipedia.org/wiki/量子鍵配送
[AQUA's animation] http://aqua.sfc.wide.ad.jp/ORF2011/ORF2011-teaching-videos.html
[Demo's GUI] http://aqua-cat.sfc.wide.ad.jp/FIRST2012