Simulation of BB84 Quantum Key Distribution Protocol

Branton DeMoss

May 7, 2016

1 Introduction

Designed in 1984 by Charles Bennett and Gilles Brassard, BB84 is the first ever quantum cryptography protocol, designed to take advantage of principles of quantum mechanics to securely share so-called "keys" used in public key cryptography, which can be used to encrypt and decrypt secret messages.

Classical key distribution protocols rely on the computational complexity of reversing so-called "one way functions", which have no known reversible algorithms which can be computed efficiently (i.e. in at most super-polynomial time). However, this does not preclude the existence of efficient means of reversing these functions. In short, classical cryptography relies on the hope that no one has come up with an efficient solution to a very difficult problem. On the other hand, quantum key distribution is guaranteed to be secure.

A unique advantage of quantum cryptographic protocols such as BB84 is their provable security, which allows for the detection of intruding listeners due to measurements on a quantum state disturbing the system, a property not at all seen in classical computation. In fact, the degree of eavesdropping on the system is quantifiable, such that if it exceeds a given level, the communication can be aborted and tried again until security is established. Therefore, one does not need to presuppose the existence of any classically secure communication channel for the quantum key distribution to take place.

2 Overview of Protocol

2.1 No Cloning Theorem

The security of the protocol relies on the famous No Cloning Theorem, which we present a proof of:

Suppose you have a state

$$|\phi\rangle_A \in \mathcal{H}_A$$

which you wish to make a copy of into some blank or unknown state

$$|e\rangle_B \in \mathcal{H}_B$$

where $\mathcal{H}_A = \mathcal{H}_B = \mathcal{H}$ so the joint state of the system is initially

$$|\phi\rangle_A \otimes |e\rangle_B \ \epsilon \ \mathcal{H}^{\otimes 2}$$

Since we obviously cannot measure the system via some Hermitian operation without collapsing the state to an eigenket of the observable, we are looking for some Unitary operator $U : \mathcal{H}^{\otimes 2} \to \mathcal{H}^{\otimes 2}$, such that

$$U(|\phi\rangle_A |e\rangle_B) = e^{i\theta(\phi,e)} |\phi\rangle_A |\phi\rangle_B$$

Where the phase factor $\theta \ \epsilon \ \mathcal{R}$ is unphysical. We now show that such a unitary cannot exist:

Take two arbitrary states $|\psi\rangle_A$, $|\phi\rangle_A$ in the Hilbert Space $\mathcal{H}$

$$\langle\phi|\psi\rangle \langle e|e\rangle = \langle\phi|_A \langle e|_B |\psi\rangle_A |e\rangle_B = \langle\phi|_A \langle e|_B U^\dagger U |\psi\rangle_A |e\rangle_B$$

which is, applying the action of the unitaries:

$$e^{i(\theta(\phi,e)-\theta(\psi,e))} \langle\phi|_A \langle\phi|_B |\psi\rangle_A |\psi\rangle_B = e^{i(\theta(\phi,e)-\theta(\psi,e))} \langle\phi|\psi\rangle^2$$

since $|e\rangle$ is normalized, implying $\langle e|e\rangle = 1$, we have

$$\| \langle\phi|\psi\rangle \| = \| \langle\phi|\psi\rangle \|^2$$

$$\implies \| \langle\phi|\psi\rangle \| = 1 \quad \text{or} \quad \| \langle\phi|\psi\rangle \| = 0$$

Therefore either $|\phi\rangle = e^{i\alpha} |\psi\rangle$ or $|\phi\rangle \perp |\psi\rangle$ which cannot be true in general for arbitrary states. Therefore, a Unitary operator cannot clone a general arbitrary state.

□

[Note that it is possible to find specific pairs of states that satisfy the above requirements, such as $|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ and $|\phi\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ where $\langle\psi|\phi\rangle = 0 = \langle\psi|\phi\rangle^2$ but this relationship clearly does not hold for arbitrary states.]

2.2 BB84 Protocol

Say Alice wishes to send Bob a key which they can use to communicate. Alice creates two strings, a and b, each n bits long. Then, she encodes the strings a and b as a string of n qubits:

$$|\psi\rangle = \bigotimes_{i=0}^{n-1} |\psi_{a_i b_i}\rangle$$

where a_i and b_i are the i^{th} bits of a and b. The pair $a_i b_i$ index into the computational and Hadamard basis according to:

$$|\psi_{00}\rangle = |0\rangle$$

$$|\psi_{10}\rangle = |1\rangle$$

$$|\psi_{01}\rangle = |+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$
$$|\psi_{11}\rangle = |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

Noting that the value of b_i determines the basis a_i is encoded in:

$$b_i = 0 \rightarrow \text{Computational Basis}$$
$$b_i = 1 \rightarrow \text{Hadamard Basis}$$
(Hint: b stands for basis)

Now Bob generates a new random string b' and measures each qubit he received from Alice in the basis governed by b'_i, noting each result in a binary string a'_i. Alice is now free to publicly announce the string b, so Bob can discard all the b'_is measured in the incorrect basis, publicly announcing the index of the bits which he has thrown away. In principle, we are done and Bob and Alice share the set of bits a which were not thrown out.

However, since this is a protocol designed for security from attacks, we wish to consider the action of an eavesdropper, Eve. Because of the No Cloning Theorem proved above, Eve cannot capture a state sent by Alice while also copying and sending it to Bob, avoiding detection of her intrusion. What Eve can do is measure a qubit sent by Alice, which of course collapses the state. Eve must randomly guess which basis to measure each qubit in, so that on average her probability of measuring in the correct basis is only $\frac{1}{2}$. Eve now creates the state she measured again and sends it along to Bob, who is apparently unaware of any tomfoolery.

To combat this, Alice actually announces some (say k) of the a_is. Bob compares his a'_is with these, which due to Eve's intrusion will be incorrect $\frac{1}{2}$ of the time. Bob and Alice test whether their randomly chosen k qubits agree, and so can quantify the error/intrusion rate, and discard if it exceeds whatever value they wish. With the comparison of more qubits comes greater certainty of security and validity, which can be increased arbitrarily. Therefore we have unconditional security.

Eve measures Alice's qubit in the correct basis 50% of the time. When she measures in the incorrect basis and sends a random result on to Bob, there is still a 50% chance he will measure Alice's originally intended bit. Therefore the probability Eve is not detected is given by:

$$P(\text{Eve not detected}) = (\frac{3}{4})^N$$

where N is the number of times Bob and Alice compare their qubits which were measured in the same basis. Solving for N, we can find the number of times we need to sample results to get a desired confidence level that Eve is detected:

$$N = \frac{\log(P(\text{Eve not detected}))}{\log(\frac{3}{4})}$$

where P(Eve not detected) is the maximum acceptable probability of Eve going undetected.

3 Simulation of Toy Algorithm

A standard method of visualizing qubits physically is as photons in a polarization state. There are rectilinear and circular polarizations of the photon, representative of the Computational and Hadamard bases. We first present a table of a small sample run. Taking "x" to be the Hadamard (circular polarization) Basis and "+" to be the Computational (rectilinear) Basis:

Alice's Qubit	0	1	1	0	1	0	0	1
Alice's Basis	+	+	x	+	x	x	x	+
Alice Sends	$\|0\rangle$	$\|1\rangle$	$\|-\rangle$	$\|0\rangle$	$\|-\rangle$	$\|+\rangle$	$\|+\rangle$	$\|1\rangle$
Eve's Basis	+	x	+	+	x	+	x	+
Eve Measures and Sends	$\|0\rangle$	$\|+\rangle$	$\|1\rangle$	$\|0\rangle$	$\|-\rangle$	$\|1\rangle$	$\|+\rangle$	$\|1\rangle$
Bob's Basis	+	x	x	x	+	x	+	+
Bob Measures	$\|0\rangle$	$\|+\rangle$	$\|+\rangle$	$\|-\rangle$	$\|1\rangle$	$\|+\rangle$	$\|0\rangle$	$\|1\rangle$
Public Reveal of Basis								
Secret Key	0		0			0		1
Key Error?	No		Yes			No		No

In the above sample, Eve's interference generated one error in the secret key, and Eve has $(\frac{2}{3})^{\text{rds}}$ of the valid secret key bits. As discussed above, and according to:

$$\text{Probability}_{detection} = 1 - (\frac{3}{4})^N$$

To detect Eve with Probability = 0.999999999 Alice and Bob would need to compare $N = 72$ key bits.

Because of the relatively simple nature of the protocol, we simply represent each qubit in javascript as an object with two parameters: basis (Computational or Hadamard), which we can represent in binary; and bit value (1 or 0):

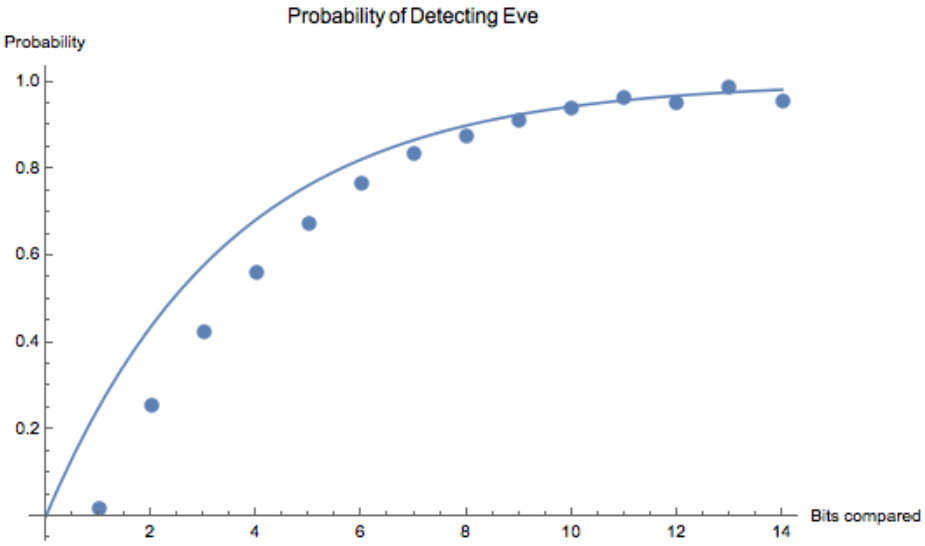
```
function Qubit (value, basis) {
    this.value = value;
    this.basis = basis;
    this.getInfo = function() {
        return this.value + ' ' + this.basis;
    };
}
```

If Eve measures the qubit in the incorrect basis, we roll the dice and get a random (with equal weighting) output of 1 or 0 in the given basis. The 50/50 coin toss in javascript is:

```
x = (Math.floor(Math.random() * 2) == 0) bool
```

where x is the resultant value. Since the basis choice can be represented in binary (0 = false = Computational Basis, etc...) we can reuse this simple method to generate every aspect of each qubit value, basis, and bad measurement result.

Runs with many qubits converge to the calculated probability of detection, as expected. We plot a histogram of times Eve was detected, along with the calculated curve (assuming Eve intercepts every qubit):



It is puzzling why Eve was detected so few times when only one bit was compared. It's far below the expected probability curve. This may be a bug in our code or transfer of data to plotting software...

4 Conclusions, outlook, current reality

BB84 is straightforward to model, and computationally easy to simulate. Intruder effects are well understood and an arbitrary level of security confidence is relatively easy to realize. One needs simply to use a few hundred qubits to achieve a very high probability of security.

The BB84 protocol relies on single-photon source and detection, neither of which exist in a cost-effective manner. There are some commercial options which currently exist (id Quantique, SeQure Net, etc...) which have Quantum Key Distribution networks already in place, and which have already been used in the case of the Swiss Quantum Network's two year test of a network installed in Geneva in 2009. With advances in precision measuring instruments and cheaper manufacturing costs, unconditionally secure distribution of keys is a very real possibility. We did not simulate the effects of errors in detection, which could play a significant role in bit errors between Alice and Bob.

Please don't Eve-sdrop on people's private communication.

5 Bibliography

The following papers were very helpful in understanding the Quantum Key Distribution Landscape, and introducing the terminology of the field:

Xiongfeng Ma. "Quantum cryptography: from theory to practice". 2008. http://arxiv.org/pdf/0808.1385.pdf

Matthias Scholz. "Quantum Key Distribution via BB84 An Advanced Lab Experiment". 2007. https://www.physik.hu-berlin.de/de/nano/lehre/f-praktikum/qkr/crypto.pdf

Charles Bennett, Gilles Brassard. "Quantum Cryptography: Public Key Distribution and Coin Tossing". 1984. http://www.physics.drexel.edu/ bob/Entanglement/BB84.pdf