Theoretical Overview of the G12 Protocol for Quantum Key Distribution

William E. Graydon

University of Toronto

Abstract

The G12 Protocol, short for "Graydon 2012" by the conventional naming system, is a quantum key distribution protocol, making use of quantum superposition, that allows secure sharing of an encryption key. G12, using only superposition, is not only possible but inexpensive and uncomplicated to set up with our current technology, and does not require a secure classical channel.

Algorithm Overview

1. First, Alice chooses a classical binary key.
2. She then encodes it into a set of bases. We will use 0/1 and +/- here, however any two with 45° rotation will do. This set, and thus the key, is of a predefined length that does not have to be private.
3. After this, Alice's only job is to receive signals from Bob, measure them in her basis, and send them back in that basis. It is now up to Bob to determine Alice's bases, and thus, the key. For now, we will assume no Eve.
4. Bob now chooses a random string of qubits, in random bases, and sends them to Alice, who measures them and sends them back.
5. Bob now compares what he received with what he sent: if a bit is the same, he does not know what Alice's basis is for that one. However, if it is different, he knows that her basis is different than his:

Bob's Qubit	Alice's Basis	Bob's Received Qubit	Bob's Conclusion
$\|+\rangle$	+/-	$\|+\rangle$	Unknown
$\|0\rangle$	+/-	$\|1\rangle$	Alice's basis is different: +/-
$\|-\rangle$	0/1	$\|-\rangle$	Unknown
$\|0\rangle$	+/-	$\|0\rangle$	Unknown
$\|0\rangle$	0/1	$\|0\rangle$	Unknown
$\|-\rangle$	0/1	$\|+\rangle$	Alice's basis is different: 0/1
$\|1\rangle$	+/-	$\|0\rangle$	Alice's basis is different: +/-
$\|-\rangle$	0/1	$\|-\rangle$	Unknown
$\|0\rangle$	0/1	$\|0\rangle$	Unknown
$\|1\rangle$	+/-	$\|1\rangle$	Unknown

6. Bob then sends out a string of random qubits, only in a different basis than he used the first time:

Bob's Qubit	Alice's Basis	Bob's Received Qubit	Bob's Conclusion
$\|0\rangle$	+/-	$\|0\rangle$	Unknown
$\|-\rangle$	+/-	$\|-\rangle$	Alice's basis is +/-
$\|1\rangle$	0/1	$\|1\rangle$	Unknown
$\|+\rangle$	+/-	$\|+\rangle$	Unknown
$\|-\rangle$	0/1	$\|+\rangle$	Alice's basis is now 0/1
$\|0\rangle$	0/1	$\|0\rangle$	Alice's basis is 0/1

$\|+\rangle$	+/-	$\|+\rangle$	Alice's basis is +/-
$\|0\rangle$	0/1	$\|0\rangle$	Unknown
$\|+\rangle$	0/1	$\|-\rangle$	Alice's basis is now 0/1
$\|+\rangle$	+/-	$\|+\rangle$	Unknown

Note that by using the opposite sequence of bases the second time, Bob maximises the probability of gaining helpful information the second time (i.e. the chance of having a different basis returned to him)

7. Bob then repeats this, sending out strings in alternating bases, until he knows all of Alice's bases. This is now the key they use.
8. Until now, we assumed no Eve. Eve's presence can do two things:
    a. If Alice's basis is different than Bob's, and the qubit she sends Bob is different than the one he sent, and Eve measures it in a different Basis than Alice's, it can revert to its original state, telling Bob nothing.
    b. If Alice's basis is the same as Bob's, she will send back the same qubit he sent. If Eve measures it in a different basis than it was sent in, and it collapses to a different qubit than Bob sent, this will erroneously tell him that Alice has a different basis.
9. In case a, Bob cannot deduce anything about Alice's basis, and therefore cannot detect Eve. However, in case b, Bob will think that Alice's basis is different than it is. However, later on, he will send one in the other basis, the one he thinks Alice is using for that bit, and it will come back different than he sent it. Given that it came back different for both bases, and given that Alice is using the same basis, Bob concludes that Eve measured one of these bases, and discards that key.

Example, to find a one-bit key:
Without Eve:

- Bob chooses the 01 base, and sends a 0
- Alice's basis is 01. She receives the 0, and sends it back.
- Bob receives the zero, which is what he sent. This tells him nothing.
- Bob now uses +-, and sends a -.
- Alice measures this in 01, and it collapses to a 1.
- Bob receives the 1, measures it in +-, and it collapses to a +.
- Bob now knows that Alice must have a 01 basis, since if she measured it in +-, it could not possibly have been different than what he sent.

With Eve:

- Bob chooses the 01 base, and sends a 0.
- Eve intercepts this, and measures it in +-; it collapses to a +, which she passes on.
- Alice receives the +, and measures it in 01. It collapses to a 1, which she sends on.
- Bob receives the 1, and concludes that Alive's base must be +-.
- Bob now uses a +- basis, and sends a -.
- Alice measures this in 01, and it collapses to a 1.
- Bob receives the 1, measures it in +-, and it collapses to a +.
- This tells Bob that Alice must have a 01 basis.

- However, the result of the first exchange told Bob that Alice was using +-, and the second tells him that she is using 01. The only way this contradiction can be introduced is if the bits were measured on the way, and thus they catch Eve.

Probability Assessment

Without Eve:

- If Bob sends a qubit in the basis Alice is using, there is a 100% probability that it will return in the same state.
- If Bob sends a qubit in the basis Alice is not using, there is a 50% probability that it will return in the same state, since a qubit in a different basis is returned to Bob, who measures it in his own; There is a 50% chance that it collapses to what he sent, 50% that it will not.
- After Bob has sent a qubit in each basis, there is a 50% chance that he will know Alice's basis for that qubit.
- If Alice and Bob need a key of length n, and the number of times they send a string back and forth twice (once on each basis), is m, they have a $(1-(1/2)^m)^n$ chance of Bob knowing the complete key.
- If Alice and Bob wish to share a key of length n, the expected (average) number of times they will have to go back and forth twice to have an α probability of having the entire key is $\log_{1/2}\left(1-\sqrt[n]{\alpha}\right)$, which has an efficiency of O(1).

Excel Demonstration

The excel sheet shows what happens as Bob sends a qubit, it is possibly intercepted by Eve, Alice measures it and sends it back and it is possibly intercepted by Eve. Bob does this multiple times, to figure out what base Alice has for each, and whether Eve is listening.

Edit cells L1 and L2 to edit the probability that Eve will read a qubit on the way from Bob to Alice, and from Alice to Bob, respectively.