

Free-Space Quantum Key Distribution

Chris Erven

November 26, 2007

1 Introduction

Quantum key distribution is the most advanced technology to arise from the emerging field of quantum information. In fact, a few companies (MaqiQ Technologies and id Quantique) already offer commercial quantum key distribution products. But why so much excitement over QKD when our standard techniques serve just fine? Well the thing is that our standard techniques are safe only under certain assumptions. Even worse, we already know that these assumptions are false if we have a quantum computer at our disposal.

To see this, let's take the classic example that anyone working in QKD will give you. One of the most popular and common encryption algorithms is the RSA encryption algorithm. The beauty of the RSA algorithm is that it's extremely simple (searching for RSA on Google returns a plethora of tutorials on the algorithm) and relies on one basic fact: factoring large numbers seems to be a hard task on a classical computer. Here, the word hard is used to mean that as the size of the number grows linearly in bits, the time to factor it grows exponentially. The RSA

algorithm works by encrypting data with a public key, comprised of the product of two large prime numbers. The message can then only be decrypted efficiently (on a classical computer) if the two prime factors are known. The size of the numbers are chosen so that it would take roughly twice the lifetime of the universe to factor their product on a classical computer. However, this rosy outlook all changed in 1994 when Peter Shor came up with his famous factoring algorithm [1] implementable on a quantum computer that's able to factor large numbers in a polynomial amount of time.

At first site it doesn't seem like such a big deal, we'll just turn to some other encryption scheme. Well as it turns out, almost all cryptographic schemes rely on the computational complexity of certain mathematical problems, almost all of which can be reduced to the problem which Shor's algorithm solves. So while scalable quantum computers are still a number of years from being built, we are faced with the very real possibility that they will break almost every practical cryptography system that we have in use today. Alright, so we won't be able to do things like

shop online but our parents survived without that just fine. But once you start to think about it, the problem starts to become bigger and bigger: no online banking, in fact no interact and credit card transactions at stores (those phone lines need encryption too); no private email; no handy encryption for BitTorrent that prevents internet providers from capping your downloads and the MPAA from printing out your download history (ah see, I knew I'd find one to scare you!). Luckily though it turns out that just as quantum mechanics gives you the possibility of quantum computing and breaking all the cryptosystems in use today, it also provides you with new tools to use in order to create new cryptosystems that only rely on the validity of quantum mechanics for their security.

2 The BBM92 Protocol

2.1 Classical Security

There is one provably secure encryption scheme invented by G.S. Vernam in 1926 called the One-Time Pad [2], which Claude Shannon proved was secure in his two famous papers on the theory of information back in 1949 [3]. The scheme is very simple, two parties called Alice and Bob can communicate securely between each other if they share a secret random key that's as long as the information which they want to send to each other. Then Alice can encrypt the information she wants to send to Bob by using something as simple as the exclusive-OR (XOR, see Table 1) operation as the encoding mech-

anism. Since the key is random (a very im-

XOR		
A	B	$A \oplus B$
0	0	0
0	1	1
1	0	1
1	1	0

Table 1: The XOR truth table.

portant requirement) and the XOR operation is a balanced operation, then the resulting encrypted message is completely random. This renders statistical attacks useless and thwarts any potential eavesdropper from learning the contents of the message, so long as Alice and Bob are the only ones who have a copy of the secret key. Bob can then recover the message Alice sent him by doing the inverse operation (in this case the XOR operation again) with his copy of the key. Take a look at Table 2 to see how this works.

So now the problem becomes distributing these secret keys securely to Alice and Bob. In the past for very sensitive information you'd literally have a government agent with an attaché case handcuffed to his wrist travelling between Washington and Moscow with the keys. Not only is this scenario incredibly impractical in today's digital age with huge amounts of data needing to be communicated securely, but it also suffers from the very fundamental problem that, in theory, any classical key always has the possibility that it was copied by a third party. This would immediately make any communication between Alice and Bob insecure.

Alice		
Message	01000001	\Leftarrow "A"
Key	00010111	
Encrypted	01010110	\Rightarrow "V"
Bob		
Coded Message	01010110	\Leftarrow "V"
Key	00010111	
Decrypted	01000001	\Rightarrow "A"

Table 2: Implementation of the Vernam Cypher with the XOR operation. Alice encodes the letter A which she wishes to send to Bob by XOR'ing the ascii bit string representing A with her key. Bob decrypts the letter by applying the inverse operation to the coded message.

2.2 Quantum Key Distribution

Quantum key distribution provides the solution to distribute keys extremely quickly, efficiently and most importantly securely. Alice and Bob will *always* be able to know whether anyone tried to look at the key as it was being distributed. In the following we'll be describing the BBM92 entangled quantum key distribution protocol developed by Bennett, Brassard, and Mermin [4].

This approach relies on the maximally entangled Bell state

$$|\psi^-\rangle = \frac{1}{\sqrt{2}}(|H_1V_2\rangle - |V_1H_2\rangle) \quad (1)$$

realized in a two photon system where H and V refer to horizontal and vertical polarization (the direction of the \vec{E} field vector) and the subscripts refer to photons 1 and 2. For

a good discussion on how to produce states like this, see Kevin Resch's recent article in the last issue of Phys 13. This state has the property that measuring one of the photons would randomly return either H or V with a 50% probability; however, if you measured both photons you would find the first H polarized and the second V polarized or vice versa. In other words, you're guaranteed when you measure both photons to get opposite results for their polarization.

Now you can start to see how we might use pairs of photons in this $|\psi^-\rangle$ state to distribute a key to Alice and Bob. We send one photon from each pair to Alice and Bob, have them measure the polarization of their photons, convert their measurements into bits with the prescription $H \rightarrow 0$ and $V \rightarrow 1$, and then have Bob invert his bits. If Alice and Bob each do this for a stream of photons in this entangled state they'll be able to build up two identical random bit strings due to the correlated nature of the state, see Table 3.

Alice		Bob		
Measure	Bit	Measure	Bit	Invert
H	0	V	1	0
H	0	V	1	0
V	1	H	0	1
H	0	V	1	0
V	1	H	0	1
V	1	H	0	1
\vdots	\vdots	\vdots	\vdots	\vdots

Table 3: Alice and Bob's correlated measurements which form the first steps towards a QKD protocol.

3 Security

So far Alice and Bob have a way of building up a shared random key; however, it's very easy to see that its not secure yet. Any eavesdropper, usually called Eve, would be able to get a copy of the key using a simple intercept-resend attack. Eve would intercept the stream of photons meant for Bob, measure their polarization, create a new photon of the same polarization and then resend it to Bob. While creating a single photon of a particular polarization is still currently a hard technological task, it is possible by the laws of quantum mechanics, and for complete security one has to plan for the situation where an attacker has all of the technology which quantum mechanics allows them at their disposal. In this scenario Alice and Bob would still end up with a random key, but Eve would also have a copy of the key. So far we haven't taken care of the secret requirement in the key distribution process.

3.1 Securing the Protocol

It turns out that turning this into a secure protocol only requires one slight wrinkle to the current protocol we have, which is to have Alice and Bob randomly choose one of two possibly bases to measure their photons in. By basis here, I mean the angle they tilt their detectors at to measure the polarization of the photons (since the polarization of a photon is relative to the coordinate system you're using). First, let's take a look at what happens to the $|\psi^-\rangle$ state if we choose to measure it in the diagonal basis by rotating our detec-

tors by 45° . We get

$$|\psi^-\rangle = \frac{1}{\sqrt{2}}(|+1 -2\rangle - |-1 +2\rangle) \quad (2)$$

where + and - refer to $+45^\circ$ and -45° polarization and the subscripts again refer to photons 1 and 2 (you can verify this very easily with the relations that $|H\rangle = \frac{1}{\sqrt{2}}(|+\rangle + |-\rangle)$ and $|V\rangle = \frac{1}{\sqrt{2}}(|+\rangle - |-\rangle)$, try drawing them out on an xy axis if you wonder where the relations come from). So the state has exactly the same structure with measurement results always being anti-correlated between the two photons in the pair.

Alright, so if Alice and Bob both measure in the H/V basis they should get anti-correlated results and if they both measure in the +/- basis they should also get anti-correlated results which they can turn into a key. If they happen to measure in different bases, they'll get random results and won't see any correlations. So Alice and Bob are also going to have to add the step that they tell each other which basis they measured each photon in, in order to filter down to those cases where they measured in the same basis. Take a look at Figure 1 to see the complete protocol in action.

3.2 Example

To see how this has helped the security of the scheme let's look at what Eve now has to do. Taking the example of the simple intercept-resend attack again, when Eve intercepts the photon meant for Bob, she's now faced with a choice: what basis to measure the photon

photon looks like $|V\rangle = \frac{1}{\sqrt{2}}(|+\rangle - |-\rangle)$ in the +/- basis; that is, V is an equal superposition of $|+\rangle$ and $|-\rangle$. So Eve has a 50% chance of measuring a $+45^\circ$ photon and 50% chance of measuring a -45° photon. Her result doesn't really matter, so let's take the case that she measures a $+45^\circ$ photon. As far as Eve's concerned that's the "correct" measurement result (since that's what her measurement device told her, she has no way of knowing that Alice and Bob were going to measure in the H/V basis), so she creates a $+45^\circ$ photon and sends it along to Bob. Now Bob makes his measurement in the H/V basis and the $+45^\circ$ photon looks like $|+\rangle = \frac{1}{\sqrt{2}}(|H\rangle + |V\rangle)$ in this basis, so he'll measure H with a 50% probability or V with a 50% probability. So here's where Eve has revealed herself, if she had not listened in, Bob would have measured a V photon with 100% certainty, but now that Eve has listened in he will measure a V photon with a probability of 75% (Equation 3) and an H photon with a probability of 25% (Equation 4).

$$\begin{aligned} \text{Prob}(V) &= 0.5_{\text{H/VBasis}} \times 1 + \\ & 0.5_{+/-\text{Basis}} \times 0.5 \end{aligned} \quad (3)$$

$$\begin{aligned} P(H) &= 0.5_{\text{H/VBasis}} \times 0 + \\ & 0.5_{+/-\text{Basis}} \times 0.5 \end{aligned} \quad (4)$$

Bob can now get an error (according to the state we originally put the entangled photons in) with a probability of 25% which is something that shouldn't happen as long as no one eavesdrops on the photons. So security comes from Alice and Bob, after their key distribution session, publically revealing about 10%

of their key to estimate an error rate and discover any eavesdroppers that might have been listening in.

3.3 Discussion

This is an example of one of the first things you're told about quantum mechanics: measurement disturbs a quantum system. Eve by measuring the photon, disturbs the state of the two photons (in this case it collapses it to one of the two possibilities). The only reason that Alice and Bob didn't see any errors in the one basis protocol is that in that case Eve's measurement commuted with Bob's (like measuring S_X and then S_X again, where S_X is the spin X operator). But now in the two basis situation, the two measurements don't commute, Eve by measuring in the +/- basis has randomized a measurement in the H/V basis (something like measuring S_Z and then S_X). And the key is *there's nothing that Eve can do to get around this, this is a direct result of the rules of quantum mechanics!*

Now attacks can get quite a bit more complicated than the simple intercept-resend strategy presented here (the two main classes of attacks are symmetric individual attacks and coherent attacks for anyone wanting to read more about them). However, even for the more sophisticated attacks Eve has to interact, however weakly, with the photons meant for Bob as they fly by and this interaction will disturb their state and show up in the error rate which Alice and Bob measure.

Now a system which required a 0% error rate in order to be considered secure wouldn't

be that practical, since nothing is ever perfect in the real world. This is where some very clever mathematicians came up with security proofs which show that a QKD system can be secure as long as the error rate is below a certain threshold. For the symmetric individual attacks this threshold is an error rate of 14.6% while for the coherent attacks it's 11%. The intuition behind the system still being secure with a non-zero error rate is that so long as Alice and Bob have some advantage over Eve in terms of the information they share between each other then they should be able to use it form a secure key. So long as the error rate is low enough, Alice and Bob can play some mathematical tricks, called privacy amplification, to reduce Eve's knowledge about the key to an exponentially small amount. As the error rate increases it becomes harder and harder for Alice and Bob to privacy amplify since Eve is learning more and more about their key, until finally Alice and Bob no longer have an advantage because Eve knows too much about the key. But *Alice and Bob will always know if their key was insecure before using it by looking at the error rate the was observed during the generation of the key, and thus will never transmit information with a key that could have been compromised!*

4 Experimental Setup

So after much ado, we now have a QKD protocol, known as the BBM92 protocol, which is provably secure according to the laws of quantum mechanics that allows us to dis-

tribute a secret key to two parties which they can then use to encrypt and decrypt data using the One-Time Pad. Now we'll see what the system actually looks like, for a more thorough discussion please refer to my Masters Thesis [5].

Let's start with the source of entangled photons which is sitting on the 6th floor of the CEIT building at the University of Waterloo. Figure 3 shows a type-II parametric down-conversion polarization-entangled photon source (for more details refer to Kevin Resch's recent article in the last issue of Phys 13) that produces entangled photons in a non-linear β - BBO crystal which come out at a small 6° angle to one another, and are split off with one photon being sent to Alice and one to Bob.

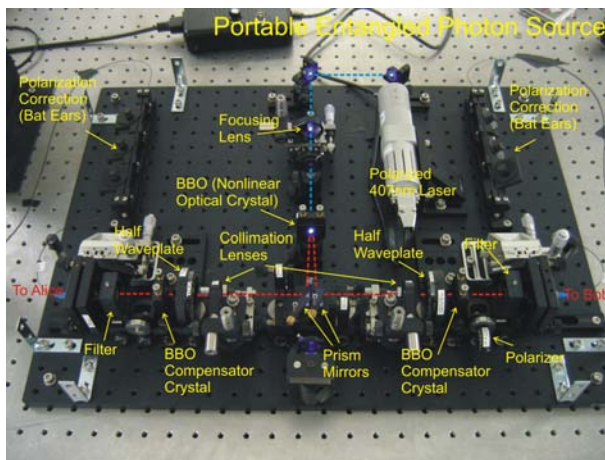


Figure 3: The Type-II Parametric Down-Conversion Entangled Photon Source.

The photons are taken from the source via single-mode fibre optic cable (which is fastened down so that its random polarization

rotation is constant and can be compensated for) to two optical telescopes, see Figure 4, on the rooftop of the CEIT building. The tele-

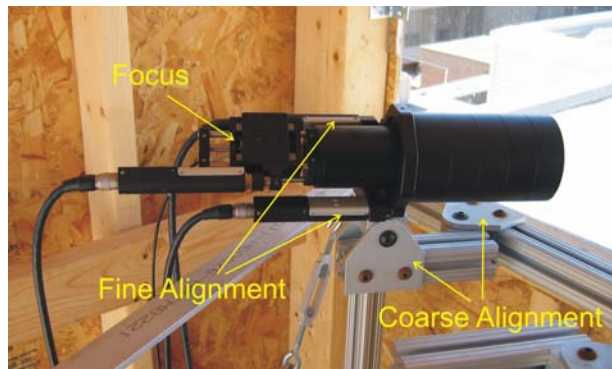


Figure 4: The sender telescope

scopes are pointed at the BFG building (IQC headquarters) and an office at the Perimeter Institute. Receiver telescopes at those two locations, see Figure 5, collect the photons sent over the free-space link and channel them into a detector box. Inside the detector box the photons first pass through a 50:50 beamsplitter (BS) which makes the random basis choice. In the reflected path of the 50:50 BS the photons pass through a polarizing beamsplitter (PBS) which transmits H photons and reflects V photons. In the transmitted path of the 50:50 BS the photons pass through a 1/2-waveplate (which rotates them by 45°) and then through a PBS, the combination of which effectively measures the photons in the diagonal basis.

At this point the photons have effectively had their polarization measured, they're collected into multi-mode optical fibres and sent to single photon detectors. The single pho-

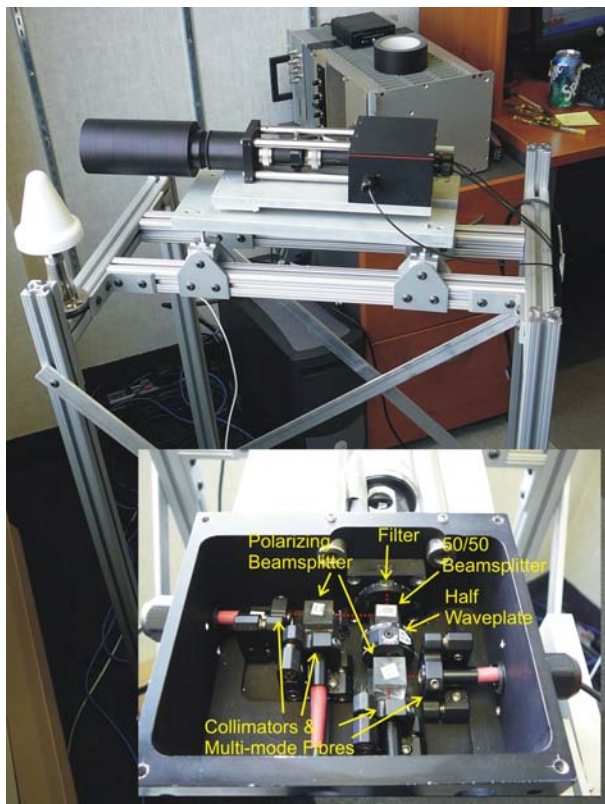


Figure 5: The receiver telescope and detector box.

ton detectors transform the photons into a TTL (5 volt) pulse, which is then fed into highly accurate time-stampers (accurate to 156.25ps) which stamp each event with a measurement result and time of arrival. All of this information is then fed into custom written software on Alice and Bob's laptops which then perform the steps of the protocol described above in order to generate a secure key which they can use to communication between themselves.

An actual experimental run of the QKD

system is shown in Figure 6 and Figure 7, where both Alice and Bob have been collecting key for a number of minutes. Alice then

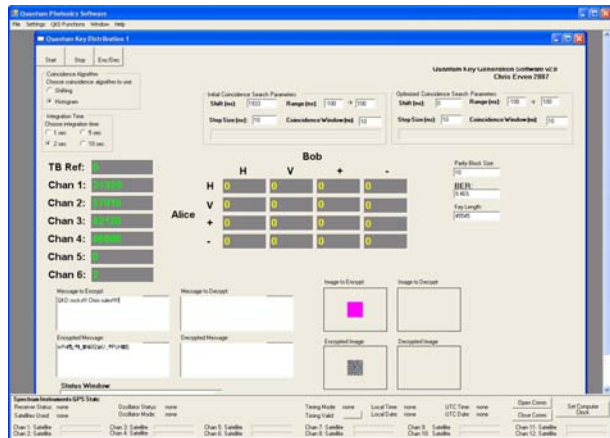


Figure 6: Alice’s screen during a QKD experimental run.

inputs a message and encrypts it with her key in Figure 6, you can see the encrypted message at the bottom left of her window. This encrypted message is then sent publicly over the internet where Bob receives it and then decrypts it using his independently generated key, and recovers Alice’s message which you can see at the bottom of his screen in Figure 7. Alice and Bob know that their communication will be secure because the error rate, shown in the middle right side of their screens, was about 9.5% which is below the threshold necessary for security against the most general coherent quantum attacks.



Figure 7: Bob’s screen during a QKD experimental run.

5 Conclusions

This article has described the BBM92 quantum key distribution protocol and the reasons behind its security. I’ve also shown that QKD is available with today’s technology and described the system we’ve built at the University of Waterloo. Because the system is more generally an entanglement distribution system, we’ve also been able to measure a Bell parameter of $S = 2.19 \pm 0.017$ (which is well over the classical value of 2) and thus also violated a Bell Inequality. A Bell Inequality violation proves the correctness of quantum mechanics over certain deterministic hidden variable theories.

So in closing, quantum mechanics isn’t a subject to be struggled through and forgotten after the exam, but rather the door to the next technological revolution. One that promises faster and more powerful computers

in the coming years. Its already shown its power in spinoff technologies such as quantum key distribution. Now all it requires is a smart new generation of students to figure out how to build a scalable quantum computer, come up with powerful new algorithms to run on it, and thus fully harness the power of the next computing revolution.

6 About the author

Chris Erven is a PhD student at the Institute for Quantum Computing in the Department of Physics and Astronomy at the University of Waterloo. He recently completed his Masters Thesis on Free-Space Quantum Key Distribution in May 2007 [5]. He completed his undergraduate degree in Systems Design Engineering in May 2005 also at the University of Waterloo. You can find more information about the project, including his Masters thesis on his website <http://www.iqc.ca/~cerven/>. For interested undergraduate students the Photonic Entanglement Group headed by Professor Gregor Weihs is always looking for coop students keen on doing interesting experimental physics projects including ones on the quantum key distribution system.

References

- [1] P.W. Shor, *Algorithms for quantum computation: Discrete logarithms and factoring*, in Proceedings of the 35th Annual Symposium on Foundations of

Computer Science, IEEE Computer Society Press, Los Alamitos, CA, pp. 124-134, (1994)

- [2] G.S. Vernam, *Cypher Printing Telegraph Systems For Secret Wire and Radio Telegraphic Communications*, J. Am. Inst. Elect. Eng. **55**, p. 109, (1926)
- [3] C.E. Shannon, *Communication Theory of Secrecy Systems*, Bell System Technical Journal, **28**, p. 657, (1949)
- [4] C.H. Bennett and G. Brassard and N.D. Mermin, *Quantum Cryptography without Bell's Theorem*, Phys. Rev. Lett., **68**, p. 557, (1992)
- [5] C. Erven, *On Free Space Quantum Key Distribution and its Implementation with a Polarization-Entangled Parametric Down-Conversion Source*, <https://uwspace.uwaterloo.ca/handle/10012/3021>, Masters Thesis, University of Waterloo, (2007)