Quantum Cryptography

Deborah K. Mathews
Younghun Chae

1. Introduction

While RSA is a secure public key cryptosystem at this time, its ability to protect data confidentiality and provide secure authentication and non-repudiation relies on the computational infeasibility of factoring very large numbers or finding the discrete logarithm of C^d(mod n). Its security against man-in-the-middle attacks also relies on the trustworthiness of the CA.[1] For communications that requires an even higher degree of security, quantum cryptography offers the ability to do a key exchange of a one time pad while allowing the detection of eavesdropping. Its security does not rely on computational infeasibility, but on the indeterminate nature of quantum particles and the fact that observation changes their properties.

Quantum cryptography was first proposed in the early 1970's by Stephen Wiesner, then at Columbia University. In 1984 Charles Bennett and Gilles Brassard published a protocol in 1984, known as BB84 after the two authors, using Wiesner's idea of "conjugate observables."[1] A conjugate observable is a pair of states where gathering any information about one of the pairs destroys information about the other. BB84 is a prepare and measure protocol, where Alice chooses what to send, and Bob measures what has been sent, and they compare what was sent to what was measured. In 1991 Artur Ekert published a protocol, E91, based on entangled states, where both Alice and Bob measure the quantum particle they receive and compare results.

In this paper we shall discuss the theory behind quantum cryptography, how the protocols work and why they are theoretically secure against eavesdropping. We shall then discuss attacks, including attacks on specific hardware, to show where quantum cryptography has vulnerability.

2. How Does Quantum Cryptography Work?

Quantum Mechanics is based on Heisenberg's uncertainty principle, which states that certain pairs of properties, like position and momentum, cannot both be known to arbitrary precision. The more one can be known, the less the other can be known. The act of measuring one of that pair of properties makes the other property indeterminate. The idea behind quantum cryptography is that no one can determine what the state of the quantum particle is without measuring it, but that measurement may very well change the state being measured. If Alice sends Bob a quantum particle prepared in one state, if he measures it using the same basis with which it was prepared, assuming no interference, his result will be the same state that Alice sent it in. If Eve measures it in that same state and then sends Bob a quantum particle in that state, Bob would not be able to detect that Eve has intercepted the quantum particle (qubit) that Alice sent. But if Eve measures it in a different state there is a reasonable likelihood that when Bob measures it, it will no longer be in the same state that Alice sent it in.

While it appears to be left to chance whether or not Eve can safely intercept Alice's message without detection, it is actually the laws of probability that make detection almost guaranteed. To avoid sharing any information that could compromise security, Alice and Bob do not confer ahead of time on the basis in which Alice is going to encode the qubit she prepares. Bob guesses the basis for each qubit and measures according to his guess. By probability, he'll guess right half the time. Likewise, Eve has to guess as well. The likelihood is that she'll guess right only half the time as well, and the likelihood of her guessing correctly on the same half that Bob guessed correctly on is very, very low. If Eve guesses incorrectly on a qubit which Bob guessed the correct basis for, Eve will prepare the qubit for Bob in the wrong basis, which means it is indeterminate in the basis in which Bob will measure it. Half the time when Bob measures it, it will resolve to the same state as the one in which Alice originally sent the qubit. But the other half of the time it will resolve to the opposite state. So half the time when Eve intercepts it it will be fine, since she guessed the same basis as Alice and Bob, and of the other half, only half of those will resolve incorrectly when Bob measures it, leaving a 25% error rate. But although for a single qubit the likelihood of Eve's going undetected is 3/4, for two qubits, it's $(\frac{3}{4})^2$. For n qubits, it's $(\frac{3}{4})^n$. The more qubits that Eve intercepts, the lower the likelihood of her going undetected becomes. This is known as the no-cloning theorem[2].

[1] On March 24, Christopher Soghoian and Sid Stamm released a draft of a forthcoming research paper that CA's were issuing false certificates to allow law enforcement agencies to forge signatures so they can do man-in-the-middle attacks on SSL connections.[26]

There are two types of protocols in quantum cryptography: prepare and measure protocols and entanglement based protocols. In both types there are two channels: a quantum channel and a classical channel. The qubits are sent through the quantum channel, and then over the classical channel Alice and Bob communicate about the basis for each qubit and compare a sample to determine whether or not Eve has been eavesdropping. If they determine that Eve has not been eavesdropping, they further communicate over the classical channel to do error checking and privacy amplification so each of them has a copy of the same final key. The final key is then xor'ed with the message to produce the ciphertext, and the ciphertext is in turn xor'ed with the key to get back the original message.

2.1 Prepare and Measure Protocols

The first quantum cryptography protocol, BB84, is a prepare and measure protocol. While any pair of conjugate states can be used, commonly the qubits are polarized photons. Two polarization angles that are orthogonal (90° apart) create two states that are completely determined with respect to one another. If a photon is polarized to 0° it can not be seen by a filter reading 90° polarized photons, and vice-versa. Likewise, if a photon is polarized to 45° it can not be seen by a filter reading 135° polarized photons, and vice-versa. However, there is an indeterminacy relationship between polarizations that are 45° apart. A pair of polarizations that are orthogonal form a basis, and two bases which are not orthogonal to each other form a conjugate pair.

In BB84, Alice uses both states in both the rectilinear basis, (0° and 90°), and the diagonal basis, (45° and 135°). For each basis, she and Bob decide ahead of time which state represents 0 and which state represents 1. Alice then decides for each qubit which basis and whether it will be a 0 or a 1, and polarizes the photon accordingly. So if she wants to send a 0 in the diagonal basis, if she and Bob decided that 135° represents 0 and 45° represents 1, she'll polarize her photon using the 135° filter.

Bob uses a calcite crystal that is calibrated to a basis, not to a single degree. So it should always receive a photon as one of the two angles. He randomly chooses which basis to use, and measures the results.

After Alice has sent all of the photons, Bob tells Alice over the classical channel which basis he used to measure each photon. Alice then tells Bob which of those to keep, since he used the same basis in measuring them that she used in preparing them. They then compare a random subset of the photons they are keeping. If the error rate is above an acceptable threshold, (20% as of 2007)[1], they conclude there is an eavesdropper, and they close communication.

Assuming there is no eavesdropper, they then go through an error correction phase, on the classical channel, where they check the even/odd parity of subsets of the key. Whenever they disagree on the parity, they know there's an error somewhere. They zero in, using a recursive algorithm, until they locate where the error is. They use overlapping segments, and if they determine that there is an error in a section that had been previously checked and found with the same parity, they know that there must be another error in that section as well.[28]

After they finish error correction, they then do privacy amplification, which involves taking the error-corrected bits and doing a hash on them to come up with a new key that is smaller than the original. If Eve has been listening on the classical line, whatever information she was able to glean is no longer useful since the key is radically changed by the hash.

Bennett offered another prepare and measure protocol in 1992, (B92). In B92 Alice uses one each of the angles in the rectilinear and diagonal basis, and Bob uses calcite crystals attuned to the angles Alice doesn't use. They decide ahead of time which angle signifies 1 and which signifies 0. Like BB94, Alice then randomly chooses which of those two angles to use to polarize the photons she sends, and Bob randomly chooses which of the two calcite crystals to use to measure the photons.

In BB84, because Bob's crystal is attuned to both angles of a basis, if Alice sends a photon polarized to 90°, then if Bob uses the rectilinear calcite crystal he'll measure a photon of 90°. But in B92, Bob doesn't have a filter that is set to the same angle that Alice is polarizing the photons in. If Alice polarizes her photon to 90° and Bob is measuring it with a crystal set to 0°, he won't receive anything. If, on the other hand, he measures it with a crystal set to 45° there is a 50% chance that it will resolve to

45° and be visible. If it resolves to 135° instead, Bob won't see it. But this means that if Bob is able to measure the photon with his filter, he knows what basis Alice would have sent it in, assuming there's no eavesdropper.

Over the classical channel Bob informs Alice which photons he measured. They then go through a subset of those to make sure he measured them with the opposite basis that she sent it in. Again, if the error rate is above a given threshold, they will know that Eve has been in the middle, intercepting and resending the photons. If Bob receives a photon in the same basis in which Alice sent it, that means that Eve must have measured it in the other basis and resent it in the other basis, and it resolved to the opposite state than the one that Alice originally sent it in.

After Alice and Bob determine that Eve wasn't eavesdropping, they do the same error correction and privacy amplification that they did in BB84.

2.2 Entanglement Based Protocols

Unlike prepare and measure protocols, where Alice prepares the photon and sends it to Bob, entanglement based protocols involve the entanglement of two quantum states, one of which Alice measures and one of which Bob measures. When two states are entangled, when one is measured with regard to a property, the other will have the same property. This is due to quantum mechanics, and it works based on the violation of Bell's inequality.

Quantum entanglement was one of the aspects of quantum physics that disturbed Einstein and other physicists. One of the explanations for why two indeterminate particles that were at a distance would behave exactly the same way was that they had hidden local variables. (In this case the particles are determined, but we can't discern the causality.) Bell argued that if there are local variables that determine the behavior of these quantum particles, then when the particles are too far apart to communicate, then either they must communicate faster than the speed of light or classical probability will determine the behavior of each particle individually. He calculated the classical probability of the particles being in the same state, and the probability according to quantum physics that they would be in the same state, and the probability according to quantum physics was higher than the classical probability. This allowed for empirical tests to be performed to see if the actual cases violated classical probability or not. Since most of the tests that have been run have given results in violation of Bell's inequality, (the classical probability prediction), the local variables theory has little empirical support.

Entanglement based protocols use Bell's inequality to ensure that no one has been eavesdropping. If the coincidence of Alice's and Bob's measurements when they choose the same basis for that measurement is within classical probability, that is consistent with an eavesdropper measuring the photon intended for Bob and then sending Bob another photon, whose state is not entangled with the photon measured by Alice. Only if there is a high degree of agreement between Alice's and Bob's measurements, violating Bell's inequality, can they be sure that Eve has not been listening.

Artur Ekert proposed a protocol based on entangled states in 1991, E91. In this, a trusted authority generates the pair of entangled photons, (or other entangled quantum states), and sends one to Alice and one to Bob. Other than that Alice, like Bob, measures, rather than choosing the state, the process of comparison over the classical channel is the same as the prepare and measure protocols.

3. Why is this Secure?

It is assumed that neither the quantum channel nor the classical channel is secure. The quantum channel is secure because if Eve measures the quantum states, this will increase the error rate of the bits measured by Bob. Eve's measuring the qubits means that the bits Bob measures will on average be in the same state that Alice sent them in ¾ of the time, which is above the acceptable threshold for errors. If enough bits are sampled, the error rate will be found to be too high.

Over the classical channel there are a few issues, which we'll discuss in the section on attacks. But the first question is why, if Alice and Bob are going over the sample bit by bit, Eve can't find out the code from this. While Eve could theoretically find that portion of the code, the portion sampled is still a small proportion of the whole. And while the parity checks done when doing error checking may give some information, they are not specific enough to allow Eve to determine every bit. Furthermore, since Alice and Bob do a hash on the code to produce the final key, if Eve doesn't have all of the bits correct, even if she knows the algorithm to produce the hash from the key, she would not be able to derive the same key, since similar inputs produce radically different outputs.

Nonetheless, without authentication over the classical channel and other uses of public key cryptosystems, quantum cryptography is still vulnerable to attack.

4. Attacks on Quantum Cryptography

In this section, we will introduce possible attacks on quantum cryptography. The attacks can be implemented not only on protocols, but also for quantum cryptography devices. Thus, we should consider the online defense scheme with offline defense scheme together.

4.1. Attacks on protocols

In this section, we will introduce some attacks target on protocols and countermeasures of them.

4.1.1. Intercept and resend[1]

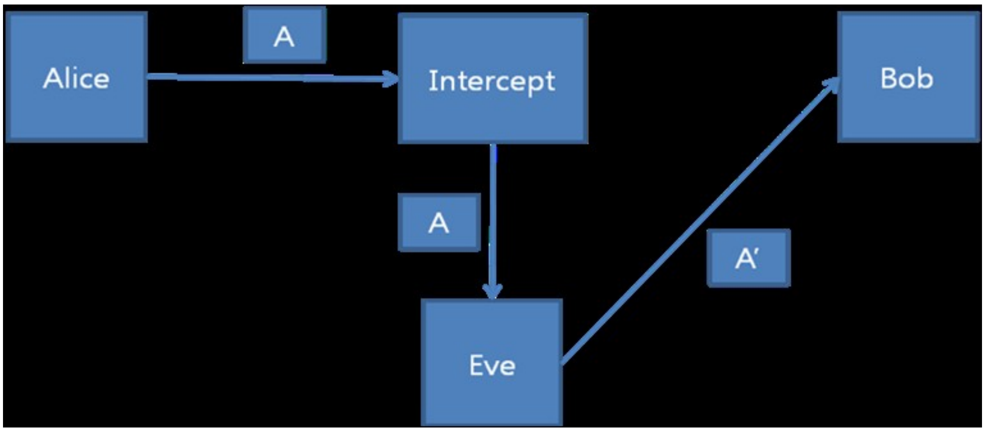
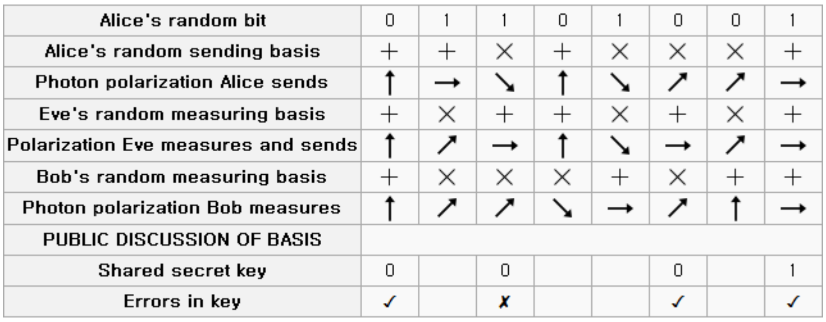


Figure 1. Intercept and resend Attack

The simplest attack, already discussed, is Intercept and Resend. In this attack Eve measures the quantum states (photons), which are sent by Alice, and then sends replacement states to Bob, as shown in Figure 1. In quantum mechanics, there is only one chance to measure a single photon because of the No-cloning theorem[2] and Wave function collapse[3]. Thus, the attackers have to choose the correct basis state every time. If we use BB84 protocol, this attack causes errors in the key Alice and Bob share. Since Eve does not know the encoding state, which is sent by Alice, she has to choose the basis state randomly. By chance, she may choose the correct basis, and then she will measure the correct photon polarization state as sent by Alice. At this time, she is able to resend the correct state to Bob. However, if she chooses the incorrect basis, the state sent to Bob is not the same as that sent by Alice. If Bob measures this incorrect state in the same basis Alice sent, he may get a distorted message. When Bob and Alice verify their sample they will become aware of Eve's presence. The table below shows how this works.



Alice's random bit	0	1	1	0	1	0	0	1
Alice's random sending basis	+	+	×	+	×	×	×	+
Photon polarization Alice sends	↑	→	↘	↑	↘	↗	↗	→
Eve's random measuring basis	+	×	+	+	×	+	×	+
Polarization Eve measures and sends	↑	↗	→	↑	↘	→	↗	→
Bob's random measuring basis	+	×	×	×	+	×	+	+
Photon polarization Bob measures	↑	↗	↗	↘	→	↗	↑	→
PUBLIC DISCUSSION OF BASIS								
Shared secret key	0		0			0		1
Errors in key	✓		✗			✓		✓

Table 1. The example of Intercept and resend [1]

The probability that Eve chooses the incorrect basis is 50%. The probability that Bob chooses the correct basis state is also 50%. Thus, the probability that the intercepted photon causes an error is 50% x 50% = 25% and the probability that Bob will receive the same state that Alice encoded is 75%. Moreover, the probability that the eavesdropper is detected is like below, if there are *n* bits data.[1]

$$\boxed{P_d = 1 - \left(\frac{3}{4}\right)^n}$$

Therefore, Alice and Bob can detect an eavesdropper with probability = 0.999999999 when they compare n = 72 key bits. [1]

4.1.2. Man in the middle attack[1]

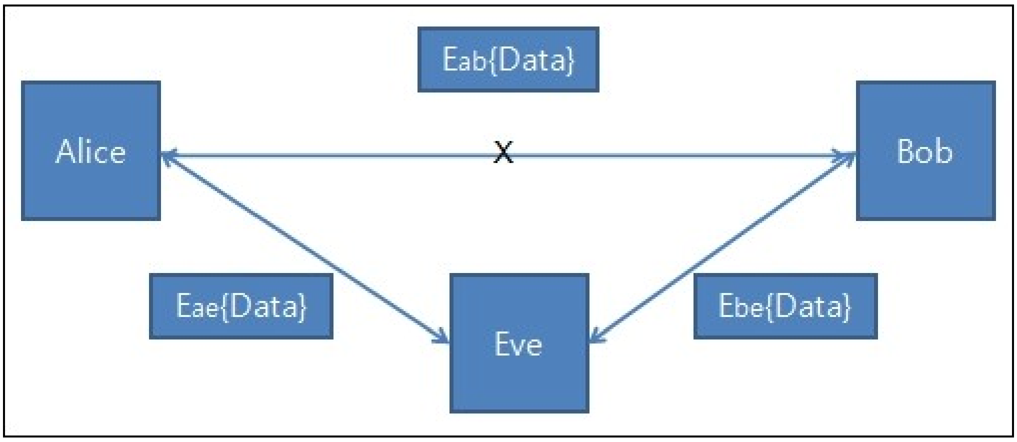


Figure 2. Man in the middle attack

Eve can lie to Alice that she is Bob, and to Bob that she is Alice. Quantum cryptography is vulnerable to the man-in-the-middle attack when Alice and Bob do not use authentication. After this attack succeeds, the network is set up like Figure 2. All data flows through Eve instead of having a direct connection between Alice and Bob. In this case, Eve can try everything, such as eavesdropping, or manipulating data. Therefore, Alice and Bob need to authenticate each other. After they have done this authentication, Eve can no longer impersonate Alice and Bob. In addition to public key cryptosystems, there are several researches to create this initial shared secret, for example using a 3rd party[4] or chaos theory[5].

4.1.3. Photon number splitting attack[1]

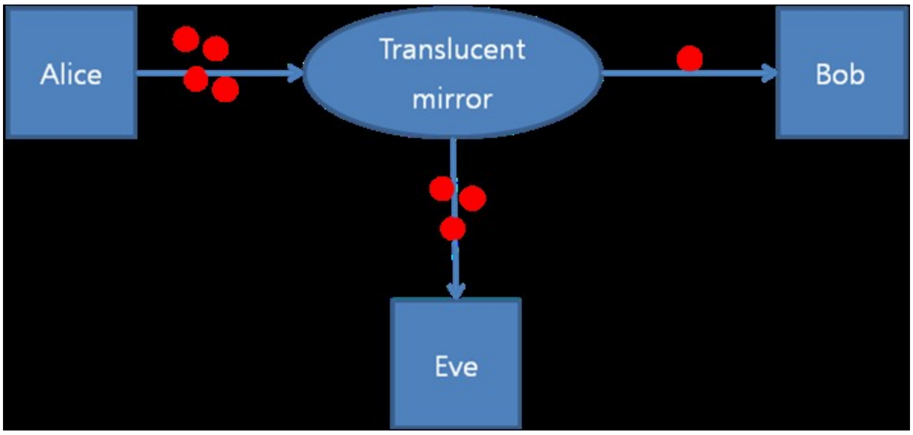


Figure 3. Photon number splitting attack

In the BB84 protocol Alice desires to send quantum states to Bob using a single photon. However, in practice, many implementations use laser pulses attenuated to a very low level to send the quantum states[1]. A very small number of photons, for example 0.2 photons per pulse are contained in these laser pulses, which are distributed according to a Poissonian distribution[6]. This means that some pulses can contain 2 or more photons. If the pulse contains more than one photon, then Eve can split off the extra photons by using a translucent mirror as shown as Figure 3, and transmit the remaining photon to Bob without distorting it. This is the basis of the photon number splitting attack[7], and Eve stores these extra photons in a quantum memory until Alice reveals the encoding basis after Bob detects the remaining single photon. Then, Eve can measure her photons in the correct basis and obtain information on the key without disclosing her existence[1]. Therefore, they have to use a true single photon source instead of an attenuated laser, which is the most obvious solution. Another solution is the modified BB84 protocol, which is done by the SARG04 protocol[8]. [1] addressed that the most promising solution is the decoy state idea[9], in which Alice randomly sends some of her laser pulses with a lower than average photon number. These decoy states are useful to detect a PNS attack, since Eve does not have way to know which pulses are signal and which decoy. This research has been implemented first at University of Toronto[10-11], and in several follow-up Quantum key distribution experiments[12].

4.2. Attacks on quantum cryptography devices

There are several attacks not only for protocols, but also on devices. In this section, we will introduce some attacks that target the specific commercial device InGaAs[13]. Detailed specification is described in Appendix 1. These kinds of attacks target on imperfections of the quantum cryptography devices instead of the protocol directly.

4.2.1. Trojan horse attack[14]

An inserted Trojan horse in a user's system may break the employed cryptosystem and obtain information by the feedback information of the ‘robot horse’. For example, the case of sending light pulses into the fiber and entering legitimate user's apparatuses allows the attacker to obtain useful information, such as basis state, by analyzing the back reflected light[15]. The system can defend against this attack with an isolator.

4.2.2. Fake state attack [16]

Standard InGaAs detectors have a detection efficiency mismatch problem[17]. InGaAs detectors are often operated in a gated mode, and the detection efficiency of each detector is time-dependent. Thus, the detector efficiencies of the two detectors would differ, if the signal arrives at some unexpected time. The faked state attack proposed by Makarov and co-workers[18] is an intercept-resend attack. Eve randomly chooses one of the two BB84 bases, and then sends to Bob a wrong bit in the wrong basis at a time when the detector for the wrong bit has a low detection efficiency. However, [17] addressed that this attack is hard to implement in practice, although it is conceptually interesting. This is because it is an intercept-resend attack and as such involves finite detection efficiency in Eve's detectors and precise synchronization between Eve and Alice-Bob's system. For this reason, the faked state attack has never been implemented in practice.

4.2.3. Phase remapping attack

This attack was proposed in [19], and it uses an imperfection in InGaAs's communication scheme. A bi-directional implementation of Quantum key distribution, such as the "Plug and Play" set-up[20], could be attacked. Eve may try to distort Alice's preparation process, so Alice prepares four wrong states, instead of the four standard BB84 state. In "Plug and Play" system, Alice and Bob follow below sequences.

1. Alice receives a strong pulse from Bob.
2. Alice attenuates it to a single-photon level.
3. The photon would be encoded to one of the BB84 state.

Bob's strong pulse supposed to arrive at the plateau region of the phase modulation. However, if Eve tries a time-shift to Bob's strong pulse, so it arrives in the rise region instead of the plateau region, Alice will wrongly encode her phase. Bob's strong pulse has been affected by the time-shifting attack, Eve can make Alice to prepare the four state with wrong phases[21]. This shows that Eve can break the security of the Quantum key distribution system without alerting Alice and Bob[17].

4.2.4. Time-shift attack[17]

[20] proposed the time-shift attack. Since Eve does not need to measure the photon, the time-shift attack is feasible with current technology; the attacker just needs to keep the photon until the timing cause problems. This attack uses the detection efficiency mismatch in the time-dependency, and this is easier to implement than the faked states attack. Since InGaAs detectors operate in a gated mode, if the photon arrives to the detector at unexpected time, the detector efficiencies of the two detectors would differ, like we mentioned at the Fake state attack. Therefore, Eve can try the arrival time of each signal, and creates efficiency mismatch between "0"s and "1"s. The time-shift attack has been successfully implemented on a commercial Quantum key distribution system in [22].

4.2.5. Large pulse attack [17]

This attack is proposed in [23]. The basic idea of this attack is like the Trojan horse attack in measuring the reflected light or pulse from Alice's device. The only difference is that Eve sends a strong pulse of laser signal to Alice's device, while the Trojan attack, above, tries to get the reflected light from Bob's laser. Eve tries to read Alice's basis state setting from a reflected pulse, and Eve may learn which BB84 state Alice is sending to Bob. However, this attack can be frustrated by install an isolator in Alice's system, like Trojan horse attack.

4.2.6. Attack by passive listening to side channels [17]

Listening to the sounds made by the source is one of the possible attacks, that is called as passive listening to side channels[17]. Another possible attack is timing side channel attack [24]. Thus, the system administrator needs to carefully locate the devices.

4.2.7. Saturation Attack [17]

[25], which is studied by Makarov, showed experimentally how Eve can blind Bob's InGaAs detector by sending a moderately bright pulse. This attack is prevented by Bob to measure the intensity of the incoming signal[17].

4.2.8. High Power Damage Attack [17]

In Makarov's thesis, it was proposed that Eve may try to make controlled changes in Alice's and Bob's system by using high power laser damage through sending a very strong laser pulse. Again, a simple counter-measure would be for Alice and Bob to measure the intensity of the incoming signals and monitor the properties of various components from time to time to ensure that they perform properly.

4.3.Other attack

In this section, we will introduce a possible attack on both protocols and devices.

4.3.1. Denial of service

Denial of Service is implemented by overloading the communication line, and makes the communications difficult or impossible. The most obvious attack is cutting the line. Also, a traditional DoS attack is possible on the public channel[1]. Therefore, the communication lines need to be securely protected. Moreover, if the traditional DoS attack is detected, the communications can be through the other channel.

5. Conclusion

The original goal of quantum cryptography was to provide unbreakable codes. There are several possible attacks not only for protocols, (which are easier to defend against), but also quantum cryptography devices. If any administrators consider only the attacks on protocols, such as intercept and resend attack, man in the middle attack, or photon number splitting attack, the system would never be perfectly secure. This is because there are still possible attacks on devices, such as Trojan horse attack, fake state attack, phase remapping attack, time-shift attack, large pulse attack, passive listening to side channel attack, saturation attack, high power damage attack, and denial of service attack. Thus, when any administrators establish quantum cryptography system, they have to consider protocol security and device security together.

However, there are companies that are offering quantum cryptography, and Toshiba's Cambridge laboratories reported in Applied Physics Letters on May 3rd the world's fastest quantum key distribution. They achieved a secure bit rate of 1 Mbit/s over 50 km fiber for 36 hours. That's an average of 1 key every 10 minutes. If you consider how many photons need to be transmitted, to account for the half that are irrelevant because Bob and Alice aren't using the same basis, the decoy pulses and the fact that the key becomes smaller during the privacy amplification stage when it is hashed, a secure key in 10 minutes is impressive. And the computation time for using the one-time-pad created is negligible, since encryption and decryption is a simple XOR operation.

Because the bigger vulnerabilities of quantum cryptography are in the hardware, we predict that the companies producing the hardware will address them, as Licel has done with the isolator for the InGaAs module. Protecting the transmission medium, if done through fiber, may always be an issue, but since a denial of service attack doesn't threaten the confidentiality of the transmission, (though it makes it impossible to transmit), those who need absolute security will see quantum cryptography as their best option. Thus we predict that even though public key cryptosystems are today secure, the market for quantum cryptography will grow.

References

[1] "Quantum cryptography," in *Wikipedia*, ed: Wikipedia.
[2] "No-cloning theorem," in *Wikipedia*, ed: Wikipedia.
[3] "Wave function collapse," in *Wikipedia*, ed: Wikipedia.
[4] H. Lee, *et al.*, "Quantum direct communication with authentication," *Physical Review A,* vol. 73, p. 42305, 2006.

[5] D. Huang*, et al.*, "Quantum secure direct communication based on chaos with authentication," *Journal of the Physical Society of Japan,* vol. 76, p. 124001, 2007.

[6] "Poisson distribution," in *Wikipedia*, ed: Wikipedia.

[7] G. Brassard*, et al.*, "Limitations on practical quantum cryptography," *Physical review letters,* vol. 85, pp. 1330-1333, 2000.

[8] V. Scarani*, et al.*, "Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations," *Physical review letters,* vol. 92, p. 57901, 2004.

[9] W.-Y. Hwang, "Quantum Key Distribution with High Loss: Toward Global Secure Communication," *Physical review letters,* vol. 91, p. 057901, 2003.

[10] Y. Zhao*, et al.*, "Experimental Quantum Key Distribution with Decoy States," *Physical review letters,* vol. 96, p. 070502, 2006.

[11] T. Chen*, et al.*, "Field test of a practical secure communication network with decoy-state quantum cryptography," *Opt. Express,* vol. 17, pp. 6540-6549, 2009.

[12] J. Dynes*, et al.*, "Practical quantum key distribution over 60 hours at an optical fiber distance of 20km using weak and vacuum decoy pulses for enhanced security," *Phys. Lett,* vol. 84, pp. 3762-3764, 2004.

[13] *InGaAs APD module*. Available: http://www.photonicsolutions.co.uk/product.asp?prodid=DETingagsapd

[14] J. Peng*, et al.*, "Trojan Horse Attack Strategy on Quantum Private Communication," *Information Security Practice and Experience,* pp. 177-186.

[15] N. Gisin*, et al.*, "Quantum cryptography," *Reviews of Modern Physics,* vol. 74, pp. 145-195, 2002.

[16] J. Shapiro and F. Wong, "Attacking quantum key distribution with single-photon two-qubit quantum logic," *Physical Review A,* vol. 73, p. 12315, 2006.

[17] H. Lo and Y. Zhao, "Quantum cryptography," *Encyclopedia of Complexity and System Science,* vol. 8, pp. 7265-89, 2009.

[18] V. Makarov*, et al.*, "Effects of detector efficiency mismatch on security of quantum cryptosystems," *Physical Review A,* vol. 74, p. 022313, 2006.

[19] C.-H. F. Fung*, et al.*, "Phase-remapping attack in practical quantum-key-distribution systems," *Physical Review A,* vol. 75, p. 032314, 2007.

[20] Y. Zhao*, et al.*, "Quantum key distribution with an unknown and untrusted source," *Physical Review A,* vol. 77, p. 052327, 2008.

[21] V. Scarani*, et al.*, "The security of practical quantum key distribution," *Reviews of Modern Physics,* vol. 81, pp. 1301-1350, 2009.

[22] Y. Zhao*, et al.*, "Quantum hacking: Experimental demonstration of time-shift attack against practical quantum-key-distribution systems," *Physical Review A,* vol. 78, p. 42333, 2008.

[23] N. Gisin*, et al.*, "Trojan-horse attacks on quantum-key-distribution systems," *Physical Review A,* vol. 73, p. 22320, 2006.

[24] A. Lamas-Linares and C. Kurtsiefer, "Breaking a quantum key distribution system through a timing side channel," *Appl. Phys. Lett,* vol. 89, p. 101122, 2006.

[25] V. Makarov, "Controlling passively quenched single photon detectors by bright light," *New Journal of Physics,* vol. 11, p. 065003, 2009.

[26] C. Soghoian and S. Stamm, “Certified Lies: Detecting and Defeating Government Interception Attacks Against SSL,” draft, reported by Electronic Frontier Foundation, March 24, 2010, http://www.eff.org/deeplinks/2010/03/researchers-reveal-likelihood-governments-fake-ssl.

[27] Y. F. Chung, *et al.*, “Unconditionally secure cryptosystems based on quantum cryptography,” *Information Sciences*, vol. 178, p. 2044-58, 2008.

[28] C. Bennett, *et al.*, “Parity bit in quantum cryptography,” *Physical Review A*, vol. 54, p. 2675-84, 1996.

Appendix 1

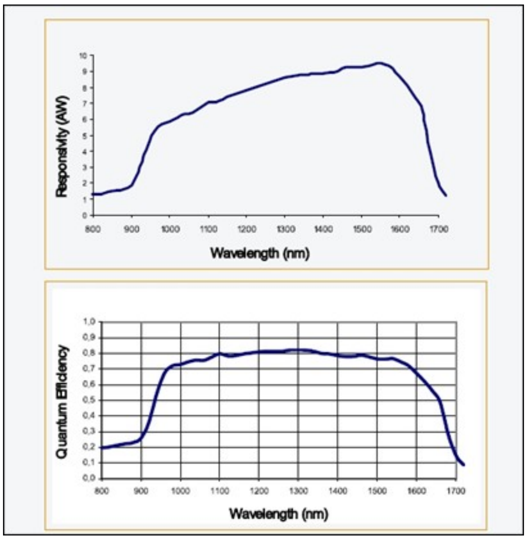
Concept:

The Licel InGaAs APD module is an integrated detector solution for eye-safe lidar systems. The detector head comprises a thermoelectrically cooled detector and preamplifier in a XYZ-translation stage.

Features:

- 0.2 mm detector size
- detector temperature -15o C
- temperature stability 0.2o C
- signal bandwidth 10 MHz
- integrated alignment optics and mechanics
- integrated preamplifier
- HV supply, AC/DC supply

Spectral Sensitivity:



Detector:

detector size: 200 µm dia.
responsivity @1550nm: 10 A//W

Preamplifier for analog detection:

bandwidth: DC-10 MHz
gain: 11mV/µA into 50 W
NEP (DC-10 MHz) 0.57pW/ÖHz
output polarity: negative
output signal: 0...-1V (max),
0...-500mV (typ.) into 50 W

HV supply:

voltage range: 0...+100V
max. current: 0.6 mA
voltage ripple: <0.005%

Mechanics:

The compact APD/preamp/TEC controller unit is mounted in a XYZ translation stage for easy integration and alignment in detection systems.
XY axis travel: 6 mm
Z-axis travel: 6 mm
precision: 4µm

Integrated TE cooler and temp. controller:

Detector temperature: -15°C
Temperature stability: <0.5 K

Power supply:

input: 100V,110V or230V, 50/60 Hz
output: +5V, -5V, +15 V

Environmental conditions:

Operating temperature: 0°C to 30°C
(non condens.)
Storage temperature: -40°C to 70°C