Interested in learning more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Securing Key Distribution with Quantum Cryptography

Quantum cryptography recently made headlines this year when European Union members announced their intention to invest $13 million in the research and development of a secure communications system based on this technology. The system, known as SECOQC (Secure Communication based on Quantum Cryptography), will serve as a strategic defense against the Echelon intelligence gathering system used by the United States, Australia, Britain, Canada and New Zealand 1. In addition, a handful of quantum information processing compa...

Copyright SANS Institute
Author Retains Full Rights

AD

Securing Key Distribution with Quantum Cryptography

Bradford C. Bartlett
Submitted: June 30, 2004
GSEC Practical Assignment
Version 1.4B, Option 1

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Abstract

Quantum cryptography recently made headlines this year when European Union members announced their intention to invest $13 million in the research and development of a secure communications system based on this technology. The system, known as SECOQC (Secure Communication based on Quantum Cryptography), will serve as a strategic defense against the Echelon intelligence gathering system used by the United States, Australia, Britain, Canada and New Zealand [1]. In addition, a handful of quantum information processing companies, including MagiQ Technologies and ID Quantique, are implementing quantum cryptography solutions to meet the needs of businesses, governments, and other institutions where preventing the unauthorized disclosure of information has become a critical success factor in maintaining a competitive advantage over adversaries.

Therefore, the focus of this paper is quantum cryptography and how this technology contributes value to a defense-in-depth strategy pertaining to completely secure key distribution. The scope of this paper covers the weaknesses of modern digital cryptosystems, the fundamental concepts of quantum cryptography, the real-world implementation of this technology along with its limitations, and finally the future direction that quantum cryptography is headed towards. The scope will not include the costs of implementing respective solutions or the legal and regulatory context of deploying such a system.

Limitations of Modern Cryptosystems

Before exploring quantum key distribution, it is important to understand the state of modern cryptography and how quantum cryptography may address current digital cryptography limitations. Since public key cryptography involves complex calculations that are relatively slow, they are employed to exchange keys rather than for the encryption of voluminous amounts of date. For example, widely deployed solutions, such as the RSA and the Diffie-Hellman key negotiation schemes, are typically used to distribute symmetric keys among remote parties. However, because asymmetric encryption is significantly slower than symmetric encryption, a hybrid approach is preferred by many institutions to take advantage of the speed of a shared key system and the security of a public key system for the initial exchange of the symmetric key. Thus, this approach exploits the speed and performance of a symmetric key system while leveraging the scalability of a public key infrastructure.

---

[1] Willan, http://www.computerworld.com/securitytopics/security/privacy/story/0,10801,93220,00.html?SKC=privacy-93220

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

However, public key cryptosystems such as RSA and Diffie-Hellman are not based on concrete mathematical proofs. Rather, these algorithms are considered to be reasonably secure based on years of public scrutiny over the fundamental process of factoring large integers into their primes, which is said to be “intractable”. In other words, by the time the encryption algorithm could be defeated, the information being protected would have already lost all of its value. Thus, the power of these algorithms is based on the fact that there is no known mathematical operation for quickly factoring very large numbers given today’s computer processing power.

This is where the technology of quantum cryptography may address a shortcoming of modern digital encryption. While current public key cryptosystems may be “good enough” to provide a reasonably strong level of confidentially today, there is exposure to a handful of risks. For instance, advancements in computer processing, such as quantum computing, may be able to defeat systems such as RSA in a timely fashion and therefore make public key cryptosystems obsolescent instantly. As another example, while the DES algorithm, which has a 56 bit key, was once considered to be secure, it is no longer thought of as such since advancements in technology have made it trivial to defeat. The fact that powerful computers may crack DES in a few hours served as a catalyst for the development of the replacement Advanced Encryption Standard. Hence, one area of risk is that public key cryptography may be vulnerable to the future technology developments in computer processing.

Secondly, there is uncertainty whether a theorem may be developed in the future or perhaps already available that can factor large numbers into their primes in a timely manner. At present, there is no existing proof stating that it is impossible to develop such a factoring theorem. As a result, public key systems are thus vulnerable to the uncertainty regarding the future creation of such a theorem, which would have a significant affect on the algorithm being mathematical intractable. This uncertainty provides potential risk to areas of national security and intellectual property which require perfect security.

In sum, modern cryptography is vulnerable to both technological progress of computing power and evolution in mathematics to quickly reverse one way functions such as that of factoring large integers. If a factoring theorem were publicized or computing became powerful enough to defeat public cryptography, then business, governments, militaries and other affected institutions would have to spend significant resources to research the risk of damage and potentially deploy a new and costly cryptography system quickly.

Quantum Cryptography in Theory

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Rather than depending on the complexity of factoring large numbers, quantum cryptography is based on the fundamental and unchanging principles of quantum mechanics. In fact, quantum cryptography rests on two pillars of 20th century quantum mechanics – the Heisenberg Uncertainty principle and the principle of photon polarization. According the Heisenberg Uncertainty principle, it is not possible to measure the quantum state of any system without disturbing that system. Thus, the polarization of a photon or light particle can only be known at the point when it is measured. This principle plays a critical role in thwarting the attempts of eavesdroppers in a cryptosystem based on quantum cryptography. Secondly, the photon polarization principle describes how light photons can be oriented or polarized in specific directions. Moreover, a polarized photon can only be detected by a photon filter with the correct polarization or else the photon will be destroyed. It is this "one-way-ness" of photons along with the Heisenberg Uncertainty principle that make quantum cryptography an attractive option for ensuring the privacy of data and defeating eavesdroppers.

Charles H. Bennet and Gilles Brassard developed the concept of quantum cryptography in 1984 as part of a study between physics and information. Bennet and Brassad stated that an encryption key could be created depending on the amount of photons reaching a recipient and how they were received. Their belief corresponds to the fact that light can behave with the characteristics of particles in addition to light waves. These photons can be polarized at various orientations, and these orientations can be used to represent bits encompassing ones and zeros. These bits can be used as a reliable method of forming one-time pads and support systems like PKI by delivering keys in a secure fashion.

The representation of bits through polarized photons is the foundation of quantum cryptography that serves as the underlying principle of quantum key distribution. Thus, while the strength of modern digital cryptography is dependent on the computational difficulty of factoring large numbers, quantum cryptography is completely dependent on the rules of physics and is also independent of the processing power of current computing systems. Since the principle of physics will always hold true, quantum cryptography provides an answer to the uncertainty problem that current cryptography suffers from; it is no longer necessary to make assumptions about the computing power of malicious attackers or the development of a theorem to quickly solve the large integer factorization problem.

A Quantum Key Distribution Example: Alice, Bob and Eve

The following is an example of how quantum cryptography can be used to securely distribute keys. This example includes a sender, "Alice", a receiver, "Bob", and a malicious eavesdropper, "Eve".

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Alice begins by sending a message to Bob using a photon gun to send a stream of photons randomly chosen in one of four polarizations that correspond to vertical, horizontal or diagonal in opposing directions (0,45,90 or 135 degrees). For each individual photon, Bob will randomly choose a filter and use a photon receiver to count and measure the polarization which is either rectilinear (0 or 90 degrees) or diagonal (45 or 135 degrees), and keep a log of the results based on which measurements were correct vis-à-vis the polarizations that Alice selected. While a portion of the stream of photons will disintegrate over the distance of the link, only a predetermined portion is required to build a key sequence for a one-time pad.

Next, using an out-of-band communication system, Bob will inform Alice to the type of measurement made and which measurements were of the correct type without mentioning the actual results. The photons that were incorrectly measured will be discarded, while the correctly measured photons are translated into bits based on their polarization. These photons are used to form the basis of a one-time pad for sending encrypted information. It is important to point out that neither Alice nor Bob are able to determine what the key will be in advance because the key is the product of both their random choices. Thus, quantum cryptography enables the distribution of a one-time key exchanged securely.

Now let us suppose that a malicious attacker attempts to infiltrate the cryptosystem and defeat the quantum key distribution mechanisms. If this malicious attacker, named Eave, tries to eavesdrop, she too must also randomly select either a rectilinear or diagonal filter to measure each of Alice's photons. Hence, Eve will have an equal chance of selecting the right and wrong filter, and will not be able to confirm with Alice the type of filter used. Even if Eve is able to successfully eavesdrop while Bob confirms with Alice the protons he received, this information will be of little use to Eve unless she knows the correct polarization of each particular photon. As a result, Eve will not correctly interpret the photons that form the final key, and she will not be able to render a meaningful key and thus be thwarted in her endeavors.

In sum, there are three significant advantages of this system. First, the Heisenburg Uncertainty principle means that information regarding photons cannot be duplicated because photons will be destroyed once they are measured or tampered with. Since photons are indivisible, once it hits a detector, the photon no longer exists. Secondly, Alice and Bob must calculate beforehand the amount of protons needed to form the encryption key so that the length of the one-time pad will correspond to the length of the message. Since mathematically Bob should receive about 25 percent of transmitted photons, if there is a deviation for the predetermined fixed number, Bob can be certain that traffic is being sniffed or something is wrong in the system. This is the result of the fact that if Eve detects a photon, it will no longer exist to be detected by Bob due to Eve's inability to copy an unknown quantum state. If Eve attempts to create and pass on to Bob a photon, she will have to randomly choose its orientation, and on

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

average be incorrect about 50 percent of the time – enough of an error rate to reveal her presence.

Ongoing Research and Development

While quantum cryptography may sound good in theory, the real test of the cryptosystem is the effectiveness and efficiency of a real-world implementation. The first prototype to incorporate quantum cryptography for key distribution was developed in 1989 by Charles Bennet and fellow colleagues at IBM. This prototype successfully employed quantum key distribution over a distance of 30 centimeters through the air and at a rate of 10 bits/second in a laboratory experiment. While this experiment proved the theory of quantum cryptography, it also raised several questions. For instance, the rate of information exchange was significantly slow, the distance of transmission was short, and therefore this experiment did not demonstrate quantum cryptography to be viable for mass deployment in the marketplace.

However, since that first prototype was constructed, other developments have followed at such places as the Los Alamos National Laboratory in New Mexico, the UK Defense Evaluation and Research Agency, and at the University of Geneva at Switzerland. These institutions have worked to push the limits of quantum transmission both through the atmosphere via satellite connections and through fiber optical cables. It is the advancements in quantum cryptography research and development that are playing an integral role in bringing to fruition practical models that can provide encryption systems for a range of customers, including cities, businesses, military organizations, and government sites.

Advances by these research institutions in addition to commercial organizations have led to significant improvements in the quality and speed of photon transmissions. For example, developments in the area of laser technology for proton identification enable higher transmission rates and thus longer one-time pads. On the other hand, fiber optics allows increased distance transmission. However, the distance limitation still remains from the fact that the signal needs to be boosted by amplifiers, but amplifiers alter the polarization of photons. Therefore, work is ongoing into the development of quantum repeaters to address this shortcoming.

Implementing Quantum Cryptography: MagiQ Technologies

One of companies developing solutions based on quantum cryptography is MagiQ Technologies, a technology start-up with headquarters in New York City. Target customers of MagiQ's solutions include the financial services industry along with both academic and government labs. MagiQ's business philosophy is that quantum cryptography is not a replacement for traditional encryption

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

technologies such as PKI, but rather a complement to current cryptography algorithms to provide a hybrid model for the delivery of a more secure system.

MagiQ's solution is called the Navajo QPN Security Gateway. The quantum-key distribution hardware box is claimed by MagiQ to be the first commercially available quantum key distribution (QKD) system. It comprises a 40 pound chassis that is mountable in a standard 19 inch rack that sells for about $50,000 a unit. Included in the unit are a photon transmitter and receiver, and the electronics and software required for quantum key distribution. These "black boxes" that are used by remote parties are connected by a fiber optic link that implements the BB84 quantum encryption code proposed by Brassard and Bennet. Navajo is intended to change randomly generated keys once a second to prevent unauthorized access to data traveling over fiber optic lines. Again, MagiQ's solution is not intended to replace current methods of cryptography such as the Public Key Infrastructure. Rather, it is intended to complement current algorithms and is even being shipped with AES.

MagiQ technologies states that the return on investment for customers is completely secure key distribution, total intrusion detection, and overall a lower total cost of ownership. MagiQ's most significant selling point is that their product is "future-proof" because progress in computational computing and new discoveries of mathematical algorithms will not adversely affect nor compromise the security of the system. Additionally, while most cryptosystems rarely refresh their keys, MagiQ's system helps to protect against an assortment of attack vectors, including Trojans and sniffers. Even if a key were to be compromised, the damage would be contained since the system provides continuous key regeneration.

Areas of Improvement

While advances in the field of quantum key distribution at MagiQ look promising, there are still numerous hurdles that must be overcome for quantum cryptography to become a practical solution for widespread deployment. Firstly, the maximum guaranteed transmission distance between remote parties for a solution such as MagiQs is about 120 KM or 75 miles. Because optical fibers are not perfectly transparent, a photon will at times get absorbed and therefore not reach the end of a fiber. While this distance limitation may be suitable for business and academic campuses, it is not practical for deployment on a global level. Therefore, continued research and development in the areas of "quantum repeaters" is necessary to increase transmission distances. A proposed solution to the distance problem may be to "chain" quantum cryptography links with secure intermediary stations. Otherwise, an alternative solution is transmission through free space or low orbiting satellite. In this scenario, the satellite acts as the intermediary station, and there is less attenuation of photons in the atmosphere. Research into this area is still ongoing and work is underway in

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

both the US and Europe to be able to send quantum keys up to satellites and then down to another destination securely.

Secondly, quantum key distribution is not the weakest link in a security system. What malicious attackers cannot break directly, they simply bypass and identify easier means of attack, such as social engineering, weak passwords, or poorly implemented security policies. Since the solutions available in the marketplace today for key distribution are "good enough" for most companies, many business executives may feel that there is no significant business driver for a company to implement MagiQ's solution. Also given that Magiq's solution is a first mover into the marketplace, many company leaders may make the decision to wait for a maturation of this technology before investing in a costly enterprise solution.

While there remain hurdles in the path for quantum cryptography to gain critical mass as a widely deployed system, there are strengths and opportunities to help this technology gain momentum in the future. For instance, current digital cryptography is suitable for today, yet it may not be sufficient for the future based off of new developments in cryptanalysis and faster computer power such as quantum computing. Moreover, the cost of having to redeploy a new solution makes quantum cryptography an attractive option in the long run. In fact, MagiQ's position has been that a weakness of competing cryptography solutions is their over reliance on computational difficulty as the underpinning of their protection.

Thus, the value-proposition for start-up quantum information processing companies such as MagiQ is that their product provides insurance and protection against future threats in addition to current threats. By addressing current as well as emerging threats, MagiQ's solution provides a "competitive advantage" over their competitors. It is a source of differentiation with the benefit of being a more cost-effective solution in the long-term. Moreover, due to the nature of quantum cryptography, MagiQ's solution furnishes premium services over traditional modern digital cryptography such as built-in IDS functionality to quickly spot malicious tampering, and frequent key regeneration up to 100 times per second to prevent "stale" keys and thwart compromise.

Another advantage according to MagiQ is that there is an abundance of laid fiber in the ground which can be leveraged by their Navajo system to deliver quantum key distribution at less costly prices. Additionally, the continued development of quantum repeater devices that boost or regenerate quantum signals should help to overcome distance transmission limitations. However, a senior scientist at Hewlett-Packard's European research laboratory believes that these devices are still about five years away[2].

[2] Schenker, http://www.iht.com/articles/126822.html

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

The Road Ahead

While there have been substantial advancements in the field of quantum cryptography in the last decade, there are still challenges ahead before quantum cryptography can become a widely deployed key distribution system for governments, businesses, and individual citizens. Namely, these challenges include developing more advanced hardware to enable higher quality and longer transmission distances for quantum key exchange. However, the advances in computer processing power and the threat of obsolescence for today's cryptography systems will remain a driving force in the continued research and development of quantum cryptography. In fact, it is expected that nearly $50 million of both public and private funds will be invested in quantum cryptography technology over the next three years[3]. In addition, according to BusinessWeek Online, MagiQ estimates the quantum cryptography market to be around $200 million within the next few years[4].

Businesses realize how essential strong encryption is in order to promote the growth of electronic commerce. In order for customers to feel comfortable completing business transactions online, they need to have a high degree of confidence in the security of the organization. Moreover, nothing can be worse or more embarrassing than having private and sensitive company information, or worse, customer information, being stolen. The negative publicity can be devastating to the financial well-being of a company.

Furthermore, while quantum cryptography will add substantial value to an organization's defensive posture, it should not be relied upon as a sole means of protection. Cryptography is only one aspect of a layered defense-in-depth strategy, which begins with the establishment of appropriate security policies to help understand threats to critical assets. Encryption protocols are another security architecture element that can be added at many layers within a system. But, encryption by itself is not a panacea. Defense-in-depth is required to build a reasonable level of security. Regardless, layered security architecture is advantageous whether quantum cryptography is deployed or not.

Quantum cryptography is still in its infancy and so far looks very promising. This technology has the potential to make a valuable contribution to e-commerce and business security, personal security, and security among government organizations such as in the Washington Beltway. If quantum cryptography turns out to eventually meet even some of its expectations, it will have a profound and revolutionary affect on all of our lives.

---

[3] Schenker, http://www.iht.com/articles/126822.html
[4] Salkever, http://www.businessweek.com:/print/technology/content/jul2003/tc20030715_5818_tc047.htm?tc

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

References

1. Dejesus, Edmund X. "Quantum Leap." Information Security Magazine. August 2001. URL: http://infosecuritymag.techtarget.com/articles/august01/features_crypto.shtml (15 May 2004).

2. Dornan, Andy. "Quantum Cryptography: Security Through Uncertainty." Network Magazine. 5 February 2004. URL: http://www.networkmagazine.com/shared/article/showArticle.jhtml?articleId=17602011 (22 May 2004).

3. Ekert, Artur. "What is Quantum Cryptography?" Centre for Quantum Computation – Oxford University. URL: http://www.qubit.org/library/intros/crypt.html (17 May 2004).

4. Johnson, R. Colin. "MagiQ employs quantum technology for secure encryption." EE Times. 6 Nov. 2002. URL: http://www.eetimes.com/article/showArticle.jhtml?articleId=16506194 (22 May 2004).

5. Mullins, Justin. "Making Unbreakable Code." IEEE Spectrum Online. May 2000. URL: http://www.spectrum.ieee.org/WEBONLY/publicfeature/may02/code.html (20 Apr. 2004).

6. Mullins, Justin. "Quantum Cryptography's Reach Extended." IEEE Spectrum Online. 1 Aug. 2003. URL: http://www.spectrum.ieee.org/WEBONLY/wonews/aug03/quant.html (20 Apr. 2004).

7. Petschinka, Julia. "European Scientists against Eavesdropping and Espionage." 1 April 2004. URL: http://www.quantenkryptographie.at/European%20Scientists%20against%20Eavesdropping%20and%20Espionage.pdf (7 Jun. 2004)

8. Salkever, Alex. "A Quantum Leap in Cryptography." BusinessWeek Online. 15 July 2003. URL: http://www.businessweek.com:/print/technology/content/jul2003/tc20030715_5818_tc047.htm?tc (3 Jun. 2004).

9. Schenker, Jennifer L. "A quantum leap in codes for secure transmissions." The IHT Online. 28 January 2004. URL: http://www.iht.com/articles/126822.html (5 May 2004).

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

10. "Uncrackable beams of light." Economist.com. 4 September 2003. URL: http://www.economist.com/science/tq/displayStory.cfm?story_id=2020013 (27 May 2004).

11. Willan, Philip. "EU seeks quantum cryptography response to Echelon." Computerworld. 17 May 2004. URL: http://www.computerworld.com/securitytopics/security/privacy/story/0,10801,93220,00.html?SKC=privacy-93220 (20 May 2004).

12. MagiQ Technologies Press Release. 23 November 2003. http://www.magiqtech.com/press/Magiq_Navajo_Launch.pdf

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Last Updated: May 19th, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Malaysia @ MCMC 2013	**Cyberjaya, MY**	**Jun 03, 2013 - Jun 08, 2013**	**Live Event**
SANS Pen Test Berlin 2013	**Berlin, DE**	**Jun 03, 2013 - Jun 08, 2013**	**Live Event**
Industial Control Systems Security Training - Houston	**Houston, TXUS**	**Jun 10, 2013 - Jun 15, 2013**	**Live Event**
Security Impact of IPv6 Summit 2013	**Washington, DCUS**	**Jun 14, 2013 - Jun 16, 2013**	**Live Event**
SANSFIRE 2013	**Washington, DCUS**	**Jun 14, 2013 - Jun 22, 2013**	**Live Event**
SANS Canberra 2013	**Canberra, AU**	**Jul 01, 2013 - Jul 13, 2013**	**Live Event**
SANS London Summer 2013	**London, GB**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
Digital Forensics & Incident Response Summit 2013	**Austin, TXUS**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS Rocky Mountain 2013	**Denver, COUS**	**Jul 14, 2013 - Jul 20, 2013**	**Live Event**
SANS Mumbai 2013	**Mumbai, IN**	**Jul 22, 2013 - Jul 27, 2013**	**Live Event**
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	**Washington, DCUS**	**Jul 22, 2013 - Jul 26, 2013**	**Live Event**
SANS San Francisco 2013	**San Francisco, CAUS**	**Jul 29, 2013 - Aug 03, 2013**	**Live Event**
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	**Bangalore, IN**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
SANS Boston 2013	**Boston, MAUS**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
Critical Security Controls Summit	**Washington, DCUS**	**Aug 12, 2013 - Aug 18, 2013**	**Live Event**
Industrial Control Systems Security Training - DC	**Washington, DCUS**	**Aug 12, 2013 - Aug 16, 2013**	**Live Event**
Mobile Device Security Summit 2013	**OnlineCAUS**	**May 30, 2013 - Jun 06, 2013**	**Live Event**
SANS OnDemand	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**