Quantum Cryptography

University of Illinois Springfield

Introduction

Cryptography is the study and practice of secure communication between two or more parties. The security goal of cryptography is authentication, confidentiality, integrity and non-repudiation. Public-key authentication plays an important role in various consumer products to verify the user and to regulate access control (Panko, 2004). Two of the common methods of modern cryptography are symmetric-key cryptography and asymmetric or public-key cryptography.

Symmetric-key cryptography allows both parties to share a digital key used to encrypt outgoing messages and decipher incoming messages. The process involves taking a plaintext message and choosing a cipher to encrypt the message. After the message has been encrypted with the cipher, the plaintext becomes the ciphertext and the message is sent to the corresponding intended party. The recipient uses the same cipher to decipher the message. Public-key cryptography is primarily used for confidentiality and authentication. Instead of having one shared key there are four keys, but only two keys are used at any given time. The sender encrypts the message with the receiver's public key and the receiver decrypts the message with their own private key. When encrypting for authentication, the outgoing message is encrypted with the sender's private key. The receiver decrypts the message with the true party's public key to ensure that the sender is the person they claim to be (RSA Laboratories, 2013).

These systems are efficient but have potential flaws. Other keying mechanisms are being developed using principles of quantum physics. The security of mathematical algorithms used in traditional public-key cryptosystems has not been proven to be infallible, but quantum cryptography security is considered proven (Gisin, et al, 2002).

Quantum Cryptography

Practical uses of quantum cryptography (QC) are limited to being a provable solution for sharing symmetric keys between communication partners. Similar to asymmetrical encryption, QC is slow and not practical for communication, but is more secure for sharing the symmetrical key used for encrypted communication.

As mathematical capabilities of computers constantly improve the traditional encryption algorithms may eventually be compromised by eavesdroppers. Quantum cryptography's use of quantum physics would be the only proven secure way to solve the key distribution problem (Gisin, et al, 2002). QC is based on the quantum physics principle that a measurement cannot be made of a system without perturbing the system; if someone intercepts the encryption message and attempts to decode it, it becomes useless.

The key in QC is initiated by the first person, commonly referred to as Alice, when she selects random bits in different orthogonal states. These quantum bits are referred to as qubits. Alice sends the qubits to Bob, who uses randomly selected orthogonal states to determine the qubits received. Statistically, Bob and Alice select the same states half the time. If the error rate is too great, that is an indication that there was probably an eavesdropper on their communication (referred to as Eve) and the key is discarded. If Eve intercepts and retransmits the message, Eve's attempt will have the same success ratio, and Bob will match half of Eve's qubits, and therefore only a quarter of Alice's qubits will match. There are multiple protocols that explain different ways for the qubits orientation and how they are used for the key. (Gisin, et al., 2002).

Heisenberg's Uncertainty Principle

One of the most widely recognized concepts in quantum physics is the "uncertainty principle" first stated by Werner Heisenberg in 1927. The principle has been described in a number of ways, the most common being a quantum object's location or speed may be known, but not both at once. Measuring speed requires multiple measurements over time, but the act of observing a quantum particle's location disrupts its motion and vice versa (Furuta, 2012). This presents a significant constraint on quantum computing, since the state of the particles must be controlled in order to be useful.

Despite its importance, empirical testing for Heisenberg's principle has been sparse and inconclusive. Busch, Heinonen, & Lahti (2007) found a wide disparity among the findings of such testing; with some tests showing quantum objects behaving in a way that violates Heisenberg's rules. Busch, et al (2007) suggest the principle may not be as strictly limiting as generally considered. Exact measurements cannot be made without disrupting the quantum object, but arbitrarily precise measurements can be made for both position and movement and the measurement can be optimized to provide the most useful combination of the two measures.

At the Frontiers in Optics convention of the Optical Society (2012) it was suggested researchers were able to measure photons' polarization states by performing measurements that caused only minor disturbance to the particles, less than Heisenberg's formula predicts. A single measurement provides little information, but several sequential measurements can be assembled into a bigger picture. In 1927, Earle Kennard stated that some level of quantum fluctuation will always exist regardless of whether the object is measured. If this fluctuation can be accounted for, both position and speed can be known within certain limits (Furuta, 2012).

Protocols

Many of the QC protocols were developed in 1980s and 1990s based on Heisenberg's Uncertainty Principal and Bells Inequality (Elboukhari, et al., 2010). The first QC protocol developed by Charles Bennett and Gilles Brassard and published in 1984 is known as BB84, based on the men's initials and publishing year (Gisin, et al., 2002). BB84 pertains to photon polarization states used when transmitting data through quantum communication channels like optical fiber, but QC uses clear channels as well, such as Internet or radio transmission (Elboukhari, et al., 2020). BB84 uses two pairs of conjugate states representing for example up and down, and right and left. The bits themselves are binary with values of 0 and 1 and the polarization states are described as horizontal, vertical, and ± 45°. The protocol is initiated when Alice randomly selects a string of binary bits (0 / 1) and randomly selects a string of bases. Alice selects a string of 1s and 0s and then encodes the states (ie. left ← state). Alice sends Bob the photons in quantum state over the quantum communication channel with the bases and bits. Bob randomly measures the state of each quantum bit (qubit) of the string individually using randomly selected bases. When Alice and Bob use the same bases for a qubit they have matching results. If they use differing bases for any qubit they have uncorrelated results for that qubit. The probability that Bob will randomly select the same bases that Alice randomly selected is about 50% of the time. Bob's result is referred to as the *raw key*. See the table below for a small example using only 6 bits.

	Qubit 1	Qubit 2	Qubit 3	Qubit 4	Qubit 5	Qubit 6
Alice randomly selects binary	1	1	0	1	0	0
Alice sends orientation	↑	←	↓	↑	→	→
Bob randomly selects orientation	→	←	↑	↑	→	↓
Result (raw key)	--	1	--	1	0	--

Alice then communicates over the public classical channel the specific base values she used, and Bob confirms if he used the same base for his measurement. Alice sends a random subset of the remaining matched bits over the Internet, and if they do not match Bob's bits, then eavesdropping has occurred. If the bits match, then the remaining matched bits that have not been shared between Alice and Bob are used as the *final key*. If an eavesdropper, commonly referred to as Eve, intercepted the communication on the quantum channel, her presence would be detected. She would perform the same random selection of bases that Bob performs in the example above, with similar results. Statistically, she would have an equal probability of determining the bases used by Alice. But as she passes the quantum bits on to Bob, the probability that she and Bob will use the exact same random bases to get the same results is nearly impossible. It is likely Bob will only match about half of Eve's bits sent, which would be less than a quarter of what Alice sent. This quantum error rate (QBER) suggests that the messages were intercepted and the process is dropped and started again on another quantum communication channel (Gisin, et al. 2002).

In 1992 Bennett published a protocol based on his work with BB84, the four-state protocol. He developed the Two-state protocol also referred to as B92. Simply stated, only two non-orthogonal states are needed. The disturbance resulting from an external person measuring the states would be equally detected with fewer states, and therefore simplifying experimentation. However, Gisin et al. suggest there is a proven possibility to unambiguously distinguish the states, however remote (2002). The conclusion is two-states are sufficient, but four-states are the recommended standard set by BB84. There has also been a six-state protocol that uses three bases. The six-state protocol probability that Alice and Bob select the same base is ⅓ rather than ½, and if there is an eavesdropper, the QBER increases from 25% to 33%, insuring with more confidence Eve has or has not been eavesdropping.

The EPR protocol, named for the authors (Einstein, Podolsky, and Rosen) of a paper published in 1935 that describes a paradox about pairs of particles suggests measurement of one quantum particle determines measurement of the other, even over great distances. This is referred to as “action at a distance” (Elboukhari, et al. 2010). Interestingly, as recent as March 2013, a team of Chinese physicists have measured the reaction of quantum particles that take place four orders of magnitude faster than the speed of light (Yin, et al. 2013).

Einstein’s understanding of quantum-correlated particles is the foundation of Ekert’s EPR protocol. Unlike the BB84 and B92 protocols that use Heisenberg’s uncertainty principle, Ekert’s ERP is a three-state protocol that uses Bell’s Inequality principle. However, ERP uses communication over a quantum communication channel and a second public channel. Alice and Bob randomly select and use one of the three possible measurements for their respective photons. The measured bit is recorded by Alice and its complement by Bob, and repeated as often as necessary. Alice and Bob communicate over the public channel to determine which bits were measured using the same base. The correlated bits are collectively called the raw key, and the uncorrelated bits are called the rejected key. The rejected key is used to detect Eve’s presence. Alice and Bob continue communication over the public channel to compare rejected keys; if Bell’s Inequality is not satisfied then Eve has not been detected. The EPR protocol can also be used with a single particle or as a two-state protocol. (Elboukhari et al., 2010).

In each of these protocols there is the requirement of a quantum communication channel like fiber optics to share the keys and public communication channels, like the Internet or radio transmissions. Ordinary light can become polarized by passing it through a Polaroid filter or calcite crystal, where the polarization is determined by the angle of the apparatus; polarized photons can then be picked out of the polarized beam (Bennet & Brassard, 1984). Fiber optic cabling is the most logical conduit to transmit light beams.

A filter is used to polarize the photon for the transmissions over a fiber optic cable. The photon recipient must have a device to receive the photon in its polarized state. The receptor uses angles to determine the sent polarized state. If both axes are parallel then the photon's polarization is confirmed. An eavesdropper cannot simply tap into the fiber cable like copper wiring. If one tried to intercept and pass along the photons using a filter, randomly selecting the polarization for each photon will inevitably change the polarization for some of the photons. Further complicating eavesdropping, the laws of quantum mechanics prevent cloning the photons into identical photons (Bennett & Brassard, 1984).

There are primarily two difficulties for transporting polarized photons over fiber optics. There is a cable length limitation before the light is depolarized due to a phenomenon referred to as polarization mode dispersion; tested fiber optics in the 1990s could successfully transmit polarized light through fewer than 20 miles of fiber (Muller, et al., 1995). Secondly, time dependency for the polarization at the end point exists, due to stress and vibrations on the fiber cable. The emitter and receiver must be designed to allow for timing references and time delays while factoring the distance.

The timing and cable length issues were successfully tested by transmitting polarized photons from Geneva to Nyon in Switzerland for a total distance of 22.7 km (14 miles). The fiber optic cable was standard telecommunication cabling run under Lake Geneva. Low-intensity pulses were polarized, sent across the cable, and received with only a 3.4% bit error rate (BER);

considered low enough to guarantee the key with error correcting and privacy amplification techniques (Muller, et al., 1995).

Quantum Cryptography vs. Traditional Cryptography

QC uses a single key that is shared at the beginning of the transmission much like symmetric cryptography methods Advanced Encryption Standard (AES) or Triple Data Encryption Standard (TripleDES). However, while QC creates one time use keys, traditional symmetric key transmissions rely on both parties retaining the same symmetric key only while they are certain the key has not been compromised.

To be secure, the key may be as long as or longer than the message. However, generating these keys requires a lot of processing power and storing them requires a lot of memory. The shared key is unique between each sender and receiver. A single device used to send messages to multiple parties needs to store numerous symmetric keys and a means to distinguish them (Ezeobika, 2010). Despite extensive security, a quantum computer is powerful enough to hack symmetric key encryption. The keys generated by QC devices are longer and messages encrypted through quantum key distribution are less susceptible to brute attacks (Tyson, 2012).

QC’s ability to maintain confidentiality over the traditional symmetric key encryption is another consideration. Traditionally encrypted messages can be intercepted and decrypted without either of the parties being aware of the situation. However, QC provides the assurance if the message is intercepted both the parties will be aware. Of course, in both quantum and symmetric key cryptography, there is no means to ensure the authenticity of the sender and receiver.

To avoid vulnerabilities of sharing a single key, public key cryptography relies on using two keys, a public key and private key, as previously described. The key pairs are generated using prime numbers of long length making them considerably secure and having infinite possibilities. This makes using public key encryption slow compared to symmetric key encryption. Public key encryption provides authentication services which QC doesn't necessarily have, however QC can detect eavesdroppers.

Public key encryption relies heavily on the integrity of the keys. If private keys are acquired by a hacker, they will have full access to all messages and there will be no easy way to know that the key has been compromised. Additionally, if the receiver loses their private key, then the messages can never be decrypted (Ezeobika, 2010). This is similar to QC where if the receiver doesn't have the right key the message can never be decrypted. In both cases, the only solution is to regenerate keys, re-encrypt and resend the messages.

Quantum Cryptography Limitations

QC sets itself apart with the ability to protect the confidentiality of the quantum key. In theory QC cannot be hacked. If the quantum key is intercepted, the photons transmitting the information will be disrupted beyond the acceptable quantum bit error rate (QBER) of 20%, signifying tampering has occurred. However, some amount of environmental noise is introduced when the key is generated and sent and can affect the QBER.

Any form of interception of the QC channel will introduce noise, signifying the presence of an eavesdropper. If the hacker intends to prevent sharing of information, not intercepting it, he can manipulate the hardware to create more noise indistinguishable from environmental noise (Houston, 2007). The sender and receiver would increase their error threshold or use a less secure system. The hardware might be adjusted to create random photons through a random generator and not through the quantum cryptographic device. Since the photons are transmitted through fiber optic lines, the simpliest means of denial of service is cutting the line or tapping into it.

The Man in the Middle (MITM) attack requires a great deal of knowledge in quantum mechanics and expensive equipment, and therefore is less likely. There are two forms of MITM attacks (Houston, 2007). In practical applications of QC, small bursts of coherent light are used instead of photons. This gives Eve opportunity to split and retrieve singular photons from each burst without detection. Or, a variation of the intercept and resend attack Eve intercepts the communication with Alice and resends the communication to Bob. Eve cannot intercept the message without being detected, but she can send and receive undetected. Once she knows Alice's key, she can decrypt the message and re-encrypt it with the key meant for Bob and send it to Bob.

Researchers from the University of Toronto successfully intercepted a commercial ID-500 Quantum Key Distribution system manufactured by a Swiss company "id Quantique" (Dunn, 2010). Researchers from the University of Toronto manipulated the noise in the system resulting in a time delay between the reference and signal pulses. This allowed them to mask their interception of the message by keeping the QBER as low as 19.7% which is below the acceptable QBER of 20% (Xu, Qi & Lo, 2010). They were able to successfully intercept the message and resend it without detection. However, the experiment assumes the message was sent without any errors, leaving enough room for error when intercepted.

Researchers from the Norwegian University of Science and Technology in Trondheim found an alternate means to hacking the system without disrupting the signal by sending a blinding laser light into the receiving device, disabling the quantum detector. While the quantum detector was disabled, they intercepted and decrypted the message. When the quantum detector stopped working, the device worked as a regular detector registering bursts of light as 1 or 0 without detecting changes in the quantum state of the message (Merali, 2010).

Known attacks can be avoided. Different anticipated and detected kinds of hacking to quantum key distribution systems can be patched. However, the most damage is done when the vulnerabilities of the system are not known. Companies manufacturing these systems welcome researchers who test the machines and find vulnerabilities. However, many companies insist the commercial grade quantum key distribution systems are more secure than systems provided to researchers (Merali, 2010).

Disadvantages of Quantum Cryptography

QC transmission rates are slow, in 2009 at 10 kbps over a 20-kilometer channel (Shields, 2009). Slow transmissions are because, to ensure perfect security the transmission includes a cipher that will be used only once and discarded called a one-time pad. This adds significant overhead to the message (Shields, 2009). Reusing the cipher would allow for faster transmission, but reduces security; as Panko noted, an attacker has a better chance of cracking the code if there is a larger pool of messages to analyze (2004). Recent breakthroughs have yielded much better results, like Toshiba’s 1 Mbps transmission over 50km in 2010 (Leyden, 2010). This is exceptional progress, but 1 Mbps is less than the bandwidth needed by banks, governments, and other large entities likely to finance early expansion of a quantum network.

Despite belief that QC is uncrackable, a Swedish research team proved an eavesdropper could listen in on quantum messages and reset them to their original state by manipulating both the message itself and the physical channel upon which the messages rely. The attack is similar to an evil-twin attack; the eavesdropper obtains at least partial keying information at the beginning of the conversation, and then uses that knowledge to copy the message. The original message is changed, but the eavesdropper can still recode the message and resend it to the intended recipient without being noticed. The researchers concede this would be difficult in practice, given the frequent back-and-forth of real world communication. They propose keying information be sent after the message; the attacker cannot read the message without changing it (Cederlof & Larsson, 2008). This theoretical weakness implies other weaknesses may exist that have simply not been found yet.

Conclusion

Despite the excitement surrounding quantum computing and cryptography, research has struggled for results. One achievement occurred in 2001 when a team of researchers at IBM created a quantum computer that reduced the number 15 to its prime factors (Anderson & Brady, 2013). In August 2012, a team at the UC Santa Barbara announced that their machine could correctly factor the number 15, but only 48% of the time (UCSB, 2012). The lack of measureable progress over the last decade and the inherent imprecision of quantum factoring suggests that quantum computing is no closer to a practical deployment (UCSB, 2012; Anderson & Brady, 2013).

Despite signal loss over long distances, in 2012, messages have been transmitted through 90km of busy optical fiber (Merali, 2012) and quantum states have been transmitted through the air over 143km using large telescopes in the Canary Islands (Ma, et al., 2012), pointing to the possibility of satellite-based quantum transmission. A prototype network has been built between two laboratories about 20 meters apart, and has successfully transmitted a qubit from one node to the other. Though it will be many years before quantum cryptography is practical for widespread use, current research continues to overcome hurdles and bring this technology closer to realization.

References

Bennett, C. H., & Brassard, G. (1984, December). Quantum cryptography: Public key distribution and coin tossing. In Proceedings of IEEE International Conference on Computers, Systems and Signal Processing (Vol. 175, No. 0). Bangalore, India.

Busch, P., Heinonen, T. & Lahti, P. (2007). Heisenberg's uncertainty principle. Physics Reports, 452 (6). Retrieved from http://eprints.whiterose.ac.uk/3610/

Cederlof, J. & Larsson, J. (2008). Security aspects of the authentication used in quantum cryptography. *IEEE Transactions on Information Theory*, 54(4), 1735-1741. doi: 10.1109/TIT.2008.917697

Dunn, J. (2010, May 20). Quantum key security hacked for first time. Researchers show weakness in commercial system. Retrieved from http://www.itworld.com/security/108472/quantum-key-security-hacked-first-time

Elboukhari, M., Azizi, M., & Azizi, A. (2010). Quantum Key Distribution Protocols: A Survey. IJUCS International Journal of Universal Computer Sciences, 1(2), 59-67.

Ezeobika, C. (2010, Jul 2). Advantages and Disadvantages of Symmetric and Asymmetric Key Encryption Methods. Comparing Symmetric and Asymmetric Key Encryption Systems. Retrieved from http://voices.yahoo.com/comparing-symmetric-asymmetric-key-encryption-6329400.html

Furuta, A. (2012). One thing is certain: Heisenberg’s uncertainty principle is not dead. Scientific American, March 8, 2012. Retrieved from http://www.scientificamerican.com/article.cfm?id=heisenbergs-uncertainty-principle-is-not-dead

Gisin, N., Ribordy, G., Tittel, W., & Zbinden, H. (2002). Quantum cryptography. *Reviews of modern physics*, *74*(1), 145-195.

Gottesman, D., Lo, H. K., Lutkenhaus, N., & Preskill, J. (2004). Security of quantum key distribution with imperfect devices. In *Information Theory, 2004. ISIT 2004. Proceedings. International Symposium on* (p. 136). IEEE.

Houston, L. (2007, December 2). Secure Ballots Using Quantum Cryptography. 2.3. Quantum Cryptographic Attacks. Retrieved from http://www.cse.wustl.edu/~jain/cse571-07/ftp/ballots.pdf

Leyden, J. (2012) Security boffins build broadband speed quantum crypto network. The Register. http://www.theregister.co.uk/2010/04/20/broadband_quantum_crypto/

Ma, X. et al. (2012). Quantum teleportation over 143 kilometres using active feed-forward. Nature, 489.

http://www.nature.com/nature/journal/v489/n7415/full/nature11472.html?WT.ec_id=NATURE-20120913

Matson, J. (2012). Bits of the future: First universal quantum network prototype links 2 separate labs. Scientific American (web site). http://www.scientificamerican.com/article.cfm?id=universal-quantum-network

Merali, Z. (2012). Quantum cryptograph conquers noise problem. *Nature* (web page). http://www.nature.com/news/quantum-cryptography-conquers-noise-problem-1.11849

Merali, Z. (2010, August 29). Hackers blind quantum cryptographers. Lasers crack commercial encryption systems, leaving no trace. nature. International weekly journal of science. Retrieved from http://www.nature.com/news/2010/100829/full/news.2010.436.html

Muller, A., Zbinden, H., & Gisin, N. (2007). Quantum cryptography over 23 km in installed under-lake telecom fibre. EPL (Europhysics Letters), 33(5), 335.

Panko, Raymond. *Corporate Computer and Network Security*.
2nd. Saddle River, New Jersey: Prentice Hall, 2004. Print.

Shields, A. (2009). Record quantum-cryptography bit rate enables ultrasecure fiber networks. SPIE (web site). http://spie.org/x34398.xml

Stark, A. (2012). More certainty on Uncertainty's Quantum Mechanical Role (press release). The Optical Society. Retrieved from http://www.osa.org/en-us/about_osa/newsroom/newsreleases/2012/more_certainty_on_uncertainty%E2%80%99s_quantum_mechanical/

Tyson, J. (2012). How Encryption Works. Public Key Encryption. Retrieved from http://computer.howstuffworks.com/encryption3.htm

Tyson, J. (2012). How Encryption Works. Symmetric key. Retrieved from http://computer.howstuffworks.com/encryption2.htm

UC Santa Barbara (2012). "UCSB researchers prove that 15=3x5 about half of the time" (press release). http://www.ia.ucsb.edu/pa/display.aspx?pkey=2803

Vignesh, R., Sudharssun, S., & Kumar, K. (2009). Limits of quantum & the versatility of traditional cryptography: a comparative study. IEEE Computer Society, 2009 Second International Conference on Environmental and Computer Science. Retrieved from http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=5383498

"Why is cryptography important?." *RSA Laboratories*.
RSA. Web. 23 Mar 2013. <http://www.rsa.com/rsalabs/node.asp?id=2162>.

Yin, J., Cao, Y., Yong, H. L., Ren, J. G., Liang, H., Liao, S. K., ... & Pan, J. W. (2013). Bounding the speed of ‘spooky action at a distance'. arXiv preprint arXiv:1303.0614.

Xu, F., Qi, B & Lo, H. (2010, May 13).Experimental demonstration of phase-remapping attack in a practical quantum key distribution system. Retrieved from http://arxiv.org/PS_cache/arxiv/pdf/1005/1005.2376v1.pdf