Quantum Cryptography: A Step into Security's Future

Christopher C. Wallace, Dr. Osman Guzide, and Dr. Weidong Liao
Department of Computer Science, Mathematics, and Engineering
Shepherd University

Abstract

There is something special about the word Quantum. That word conjures up visions of Sci-Fi movies, Mad Scientists laboratories, and even Black Holes. Yet, in this context it can mean so much more. Quantum relates to the cutting edge of information security. This abstract is intended to introduce the reader to the world of Quantum Cryptography

Objectives

- Give an introduction to the Quantum World.
- Discuss Key Creation
- Show components of the Quantum system.
- Security risks to the quantum network
- Discuss future Quantum Cryptography research.

The Quantum World

Quantum physics has been a heated subject for decades.

- Many great scientists have dedicated themselves to finding the secrets of quantum physics.
- Photons are the base for Quantum Cryptography.
- The entangled pairs of photons make the key successful.
- How is the key created?

Key Creation

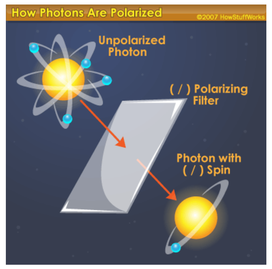
- It all starts with entropy.
- The key is generated with random numbers.
- The random numbers are translated into binary.
- The 1's and 0's are assigned to a polarized photon.
- Photons are passed through filters to create entangled pairs.
- The spin of the photon created determines if it is a 1 or a 0.

Key Creation (Continued)

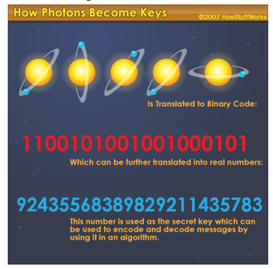
- Once the photons are polarized and the signal sent anything that comes into contact with it can change the position and orientation of the photon.
- If this happens the authentication can not be completed and the system will know it has been compromised.
- Things like heat, frequency change, or light intensity will also change the position of the photons.
- If all is successful the key will go through the decryption process.

Entanglement & Key Creation

Filtered Proton

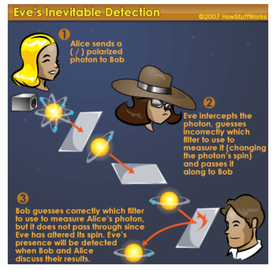


Key Creation



Entanglement

Authentication



Components

Number Generator

OEM

Encrypter

Quantum Detector

Quantum Detector

Security Risks

- The signal is secure but the connections between quantum and conventional systems are not.
- Laser used to break key authentication.

- Threat of quantum computers.

Future Research

- Using an RGB scale to create an additional layer of security.
- The advent of full quantum computers to reduce and remove hardware vulnerability.

References

[1] IDQuantique, "2nd Winter School on Practical Quantum Cryptography, 2010", Gregoire Ribordy, http://www.idquantique.com/files/winterschool/2010/ws2-session8.pdf, 2010
[2] Zhao, Yi; Fung, Chi-Hang Fred; Qi, Bing; Lo, Hoi-Kwong (2008). "Quantum hacking: Experimental demonstration of time-shift attack against practical quantum-key-distribution systems". Physical Review A.
[3] Bennett, Charles H.; Gilles, Brassard (1984). "Quantum cryptography: Public-key distribution and coin tossing". Proceedings of IEEE International Conference on Computers, Systems and Signal Processing 1984. IEEE Computer Society. pp. 175-179.
[4] Gilles, Brassard; Crépeau, Claude; Richard, Jozsa; Langlois, Denis (1993). "A Quantum Bit Commitment Scheme Provably Unbreakable by both Parties". FOCS 1993. IEEE. pp. 362-371.
[5] Watrous, John (2009). "Zero-Knowledge against Quantum Attacks". SIAM J. Comput. 39 (1): 25–58. doi:10.1137/060670997.
[6] Mayers, Dominic (1997). "Unconditionally Secure Quantum Bit Commitment is Impossible". Physical Review Letters (APS) 78 (17): 3414–3417. Preprint at arXiv:quant-ph/9605044v2
[7] Dziembowski, Stefan; Ueli, Maurer (2004). "On Generating the Initial Key in the Bounded-Storage Model". LNCS. 3027. Eurocrypt 2004. Springer. pp. 126-137. Preprint available at [1].
^ "Post-quantum cryptography". Retrieved 29 August 2010
[8] Xu, Feihu; Qi, Bing; Lo, Hoi-Kwong (2010). "Experimental demonstration of phase-remapping attack in a practical quantum key distribution system". New Journal of Physics
[9] "Hacking commercial quantum cryptography systems by tailored bright illumination". Nature Photonics. 2010
[10] Wiesner, Stephen (1983). "Conjugate coding". SIGACT News (New York, NY, USA: ACM) 15 (1): 78–88. doi:10.1145/1008908.1008920. ISSN 0163-5700. Manuscript written ca.~1970
[11] Crépeau, Claude; Joe, Kilian (1988). "Achieving Oblivious Transfer Using Weakened Security Assumptions (Extended Abstract)". FOCS 1988. IEEE. pp. 42-52.
[12] Joe, Kilian (1988). "Founding cryptography on oblivious transfer". STOC 1988. ACM. pp. 20-31.
[13] Damgård, Ivan; Fehr, Serge; Salvail, Louis; Schaffner, Christian (2005). "Cryptography In the Bounded Quantum-Storage Model". FOCS 2005. IEEE. pp. 449-458. A full version is available at arXiv:quant-ph/0508222
[14] Cachin, Christian; Crépeau, Claude; Marcil, Julien (1998). "Oblivious Transfer with a Memory-Bounded Receiver". FOCS 1998. IEEE. pp. 493-502.
[15] " Yahoo image results for Quantum detectors", Web, http://images.search.yahoo.com/search/images?_adv_prop=image&va=quantum+key+detector&fr=yfp-t-351&xargs=0&pstart=1&b=22&ni=21, Mar. 21, 2011

Acknowledgments

The West Virginia Academy of Science.
Shepherd University's CME Department.
Professor Osman Guzide