Open Access License Notice

Quantum Key Exchange Simulator

Michael McGregor
mcgrmic2@isu.edu

Michael Haney, PhD
mhaney@uidaho.edu

University of Idaho
875 Perimeter Road
Moscow, ID 83844

Abstract - Quantum cryptography and key exchange is an important and challenging topic for cybersecurity and information assurance students, and one that is difficult to teach without an appropriate demonstration platform. In this paper, we describe the background of quantum key exchange (QKE) theory, modern implementations of QKE, and the role it plays in classical, symmetric key cryptography. We present a QKE simulator that can be used by educators to aid in the teaching of quantum key exchange concepts and processes. The simulator provides a hands-on learning mechanism with which the participants interact. It is designed to be engaging and practical for students to use by supporting the ability to walk through phases of quantum key exchange, pausing at each step, to facilitate discussion and comprehension of this complex security topic.

Keywords

Quantum key exchange, simulator, cryptography, key exchange, teaching

1 INTRODUCTION

Quantum key exchange is the science of replacing the key exchange phase of classical cryptographic systems with technology from the field of quantum mechanics to achieve a provably secure and private key exchange medium. After the key exchange has taken place, the two parties then proceed to communicate over open or untrusted channels using classical cryptographic technologies.

The field of quantum key exchange was pioneered in 1984 by Bennett in the seminal work *Quantum cryptography: Public key distribution and coin tossing* [1]. In this work, Bennett describes how existing technologies for transmitting information with quantum technologies involving polarized photons can be extended to provide for secure cryptographic exchanges. Prior to this, the use of quantum technologies to transmit information had not realized a cryptographic application. Bennett pioneered the cryptographic application by explaining that the uncertainty principle inherent in quantum physics presents a perfect opportunity for cryptography.

2 QUANTUM KEY EXCHANGE

In 1964, John S. Bell published his famous "Bell inequality," now known as Bell's Theorem, which requires that "No physical theory of local hidden variables can ever reproduce all of the predictions of quantum mechanics." [2] At the heart of Bell's Theorem is an EPR pair, named after Einstein, Podolsky, and Rosen and their work on the EPR paradox of 1935. [3] An EPR pair is a pair of qubits that are quantum entangled, meaning they exhibit a perfect correlation, regardless of distance between them. [4]

In 1991, Artur Ekert published *Quantum Cryptography Based on Bell's Theorem*. [5] In this publication, Ekert describes a system of using EPR pairs to confidently generate a secret key between two hypothetical communicators Alice and Bob. Ekert's system uses a source that generates a pair of entangled spin- ½ particles and sends them down a pair of channels towards Alice and Bob, respectively. Alice and Bob then proceed to measure the particle for its spin component in one of three directions. The measurements are made at either 0°, 45°, or 90° from the positive

x axis. Alice and Bob choose their measurements independently and randomly and note which measurement they applied, if they were able to measure anything, and if so, if the particle was spin-up or spin-down.

Once all the measurements have been made, Alice and Bob publicly communicate to each other which orientation they chose for each measurement. Alice and Bob throw out any measurements that did not result in a particle detection. Then, Alice and Bob reveal to each other the results of the measurements where their respective orientations are different. This set of data can be used to verify statistically that the particles were not directly or indirectly disturbed. The remaining measurements, where Alice and Bob both used the same measurement orientation, are converted into binary (e.g., 1 for spin-up, 0 for spin-down) and are subsequently used as a shared secret key for a symmetric cryptographic communication.

The strength of this method lies in one of quantum mechanics' principles. Any attempt by an eavesdropper to measure or intercept the particle leaving the source or en route to either party will result in the particle being modified. Thus, when the particle is measured by Alice for instance, it will no longer match the particle sent to Bob, and this particle will not make it into the final cut for the secret key. Thus, by the laws of physics, this system can be guaranteed to be free from eavesdropping. Ekert also shows how this system is also guaranteed to resist monkey-in-the-middle attacks as well. [5]

In 1992, Charles Bennett wrote a critique [6] of Ekert's publication *Quantum Cryptography Based on Bell's Theorem* [5]. Bennett describes that Ekert's design is sufficient but not necessary to ensure a cryptographically secure key exchange can take place between two distant parties. Further, Bennett explains that his proposed revision of Ekert's system is more efficient and more easily implemented than Ekert's.

Bennett describes in [6] how two parties Alice and Bob can establish a shared secret key. In this scheme, Alice randomly generates a particle in one of four states

$|\uparrow\rangle$, $|\downarrow\rangle$, $|\leftarrow\rangle$, or $|\rightarrow\rangle$. Bob is able to measure along either the x-axis or the y-axis, which he decides randomly for each particle. After Bob has attempted measurement of the particle, he will either learn that he failed to correctly choose the measurement axis, or, if he did correctly choose the measurement axis, he will learn in which of the two corresponding states Alice sent the particle.

After Alice has finished sending Bob all the necessary particles to establish a key, Alice then publicly announces to Bob for each particle if it was oriented on the x-axis or the y-axis. Bob publicly announces which filter he used for each particle sent from Alice, and they both agree to throw out those particles of which Bob measured along a different axis from what Alice sent. Of the remaining particles, Alice and Bob choose a subset of particles to publicly compare the sent and measured states, respectively. Through these comparisons, Alice and Bob are able to determine if an eavesdropper was successful in disturbing the particle during transmission. This only shows if an eavesdropper disturbed a particle, not if he was successful in gathering information on the particle. But the laws of quantum mechanics guarantee that any measurement of a particle which fails to disturb the particle also yields no information about the particle. If Alice and Bob are able to determine through the subset of particles publicly compared that no eavesdropping took place, it is statistically likely that the rest of the particles were not intercepted either. Bennett surmises bluntly the security of a system such as this by saying "the only attack that can avoid detection is the one that yields no information."

Now Alice and Bob can proceed to use the shared secret key they have generated in a conventional symmetric cryptographic algorithm. Bennett shows in his publication that through this method, he has increased the security of Ekert's system by preventing the ability for an attacker to substitute the source of the EPR pairs used in Ekert's system. Since Alice is generating the particles and sending them to Bob, it would be impossible for an attacker to substitute the source.

Bennett published another paper in 1992 titled *Quantum cryptography using any two nonorthogonal states* [7] in which he produced another quantum key distribution system different from his previous work. Bennett produces a system in which Alice

sends to Bob a random binary sequence of quantum particles. After Bob has randomly measured each particle, he announces publicly which particles he was able to measure successfully, but not which measurements he made. Since Alice knows which measurements Bob should have made for each particle, and Bob knows which measurements yielded no information, they can privately throw out any sequences which Bob measured incorrectly. Even though this was done privately, the final sequences should match. Now, just like before, Alice and Bob publicly compare a subset of the particles to ensure the key exchange is free from eavesdropping. In this publication, Bennett postulates the use of specially phase-shifted lasers and attenuators to achieve the desired quantum effect. This system also proves the inability of an eavesdropper to successfully gain any knowledge of the generated shared secret key.

After investigating both of the above methods, the first using Bell's Theorem [5], [4], and the second using a system void of Bell's Theorem in nonorthogonal states [1], [6], [7], we see that both of these methods establish a way of transmitting a key between two parties while ensuring the key is not intercepted or eavesdropped, at least not without detection. Interception of the secret key is completely acceptable, as long as both parties are made aware of the attack. The parties can simply dispose of that key and start the generation over again, presumably after taking measures to better avoid attack. The ability for these systems to guarantee that an attack is detectable is not conditional upon the correct implementation of a technical standard. Rather, the guarantee is afforded by the laws of physics and specifically of quantum mechanics itself. Thus, during a key exchange, it can be proved that the key has not been intercepted and the two parties are the only holders of that secret key.

3 QUANTUM KEY EXCHANGE SIMULATOR

The topic of quantum key exchange not normally taught in cryptography classes, potentially due to the hard to understand underlying physics enabling QKE and the cost-prohibitive nature of full-scale, physical demonstrations. Additionally, quantum key exchange is often confused with, or thought to be dependent on,

quantum computing. The quantum key exchange simulator was built with the purpose of trying to make this topic more accessible and understandable, and to debunk any myths that quantum key exchange is still decades away.

The quantum key exchange simulator demonstrates, step by step, the processes that take place to allow a quantum key exchange to happen. The simulator is designed to operate as independent processes communicating over network sockets allowing for "Alice" and "Bob" to actually run on different computers, by different participants, to establish a shared key. This key can then be used in the simulator to encrypt test data and send it to the other participant over a public channel where it can be decrypted. Students are made aware that the keys generated in the simulator are not actually protected by the laws of physics and should not be used for sensitive data.

Since the QKE simulator runs step by step, the QKE process can be broken down into phases and each phase of the QKE process can be explained to the students with each phase being observed graphically. Following are sample outputs from an early version of the QKE simulator. The first is a run with 100 particles sent from Alice to Bob, the second is a run with 1000 particles sent from Alice to Bob. The early version of the QKE simulator ran as a console application accepting command line parameters for the operation mode (Alice or Bob) and which network ports to use for the quantum and public channels.

```
./QKES -m alice -p 12345 -q 23456

Phase 1 complete, I have sent 100 randomly generated signals to Bob.

Phase 2 complete. I have publicly sent the axes of each signal to
Bob for his review.

Phase 3 complete. I have received 100 axes from Bob for comparison.

Phase 4 complete. Agreed upon key (52 bits) is as follows:

1000011111100111101001100101011110000011101000100100
```

Figure 1. Alice sends Bob 100 particles

```
./QKES -m bob -p 12345 -q 23456

Phase 1 complete, I have received 100 signals from Alice.

Phase 2 complete. I have received 100 axes from Alice for comparison.

Phase 3 complete. I have publicly sent the axes of each signal to
Alice for her review.

Phase 4 complete. Agreed upon key (52 bits) is as follows:

1000011111100111101001100101011110000011101000100100
```

Figure 2. Bob receives 100 particles from Alice

```
./QKES -m alice -p 12345 -q 23456 -n 1000

Phase 1 complete, I have sent 1000 randomly generated signals to Bob.

Phase 2 complete. I have publicly sent the axes of each signal to
Bob for his review.

Phase 3 complete. I have received 1000 axes from Bob for comparison.

Phase 4 complete. Agreed upon key (516 bits) is as follows:

1000110101100011001001110100110011111110010001111011111111101011100
1110000111111000011001001110100001011000110110011001011010010001110
0011110010111100000001100101101010010001001011010000100010100101111
0010110001110011110011111011011010011010101000100011110000011101101
1010001000011110111101101100000100111011111101100101001110101110100001
0101000100001000100010000101110010010000100001100111110010101111011
1011011011110010110010000011110111100011110111011100010100101000000
1101001101000000111101011011010000111010011001l
```

Figure 3. Alice sends Bob 1000 particles

```
./QKES -m bob -p 12345 -q 23456

Phase 1 complete, I have received 1000 signals from Alice.

Phase 2 complete. I have received 1000 axes from Alice for comparison.

Phase 3 complete. I have publicly sent the axes of each signal to
Alice for her review.

Phase 4 complete. Agreed upon key (516 bits) is as follows:

10001101011000110010011101001100111111100100011110111111111010111001
11100001111110000110010011101000010110001101100110010110100100011110
00111100101111000000011001011010100100010010110100001000101001011111
00101100011100111100111111011011010011010101000100011110000011101101
10100010000111101111011011000001001110111111011001010011101011010001
01010001000010001000100001011100100100001000011001111100101011111011
10110110111100101100100000111101111000111101110111000101001010000000
11010011010000001111010110110100001110100110011
```

Figure 4. Bob receives 1000 particles from Alice

4 CONCLUSION

Through the development of the quantum key exchange simulator, we have created a tool that can be used by educators to aid in the teaching of quantum key exchange concepts and processes in cryptography courses. The simulator is designed to be engaging and practical for students to use to easily understand each step in the process, by allowing participants to pause or walk through the phases of key exchange and discuss the mechanics of what each step provides. By doing so, instructors can facilitate a much more engaging process of comprehending a challenging and complex, but very important, subject matter.

REFERENCES

[1] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," 1984.

[2] C. Parker, *McGraw-Hill Encyclopaedia of Physics (2nd ed.)*. McGraw-Hill, 1994, p. 542.

[3] A. Einstein, B. Podolsky, and N. Rosen, "Can quantum-mechanical description of physical reality be considered complete?" *Physical review*, vol. 47, no. 10, p. 777, 1935.

[4] J. S. Bell, "On the einstein podolsky rosen paradox," 1964.

[5] A. K. Ekert, "Quantum cryptography based on bells theorem," *Physical Review Letters*, vol. 67, no. 6, p. 661, 1991.

[6] C. H. Bennett, G. Brassard, and N. D. Mermin, "Quantum cryptography without bells theorem," *Physical Review Letters*, vol. 68, no. 5, p. 557, 1992.

[7] C. H. Bennett, "Quantum cryptography using any two nonorthogonal states," *Physical Review Letters*, vol. 68, no. 21, p. 3121, 1992.

[8] D. J. Bernstein, J. Buchmann, and E. Dahmen, *Post-quantum cryptography*. Springer Science & Business Media, 2009.

[9] J. Rarity, P. Tapster, P. Gorman, and P. Knight, "Ground to satellite secure key exchange using quantum cryptography," *New Journal of Physics*, vol. 4, no. 1, p. 82, 2

[10] J. Rarity, P. Tapster, P. Gorman, and P. Knight, "Ground to satellite secure key exchange using quantum cryptography," *New Journal of Physics*, vol. 4, no. 1, p. 82, 2002.

[11] D. S. Bethune and W. P. Risk, "An autocompensating fiber-optic quantum cryptography system based on polarization splitting of light," *IEEE Journal of Quantum Electronics*, vol. 36, no. 3, pp. 340–347, 2000.

[12] C. Kurtsiefer, P. Zarda, M. Halder, H. Weinfurter, P. Gorman, P. Tapster, and J. Rarity, "Quantum cryptography: A step towards global key distribution," *Nature*, vol. 419, no. 6906, pp. 450–450, 2002.

[13] T. Jennewein, C. Simon, G. Weihs, H. Weinfurter, and A. Zeilinger, "Quantum cryptography with entangled photons," *Physical Review Letters*, vol. 84, no. 20, p. 4729, 2000.

[14] A. Muller, J. Breguet, and N. Gisin, "Experimental demonstration of quantum cryptography using polarized photons in optical fibre over more than 1 km," *EPL (Europhysics Letters)*, vol. 23, no. 6, p. 383, 1993.

[15] A. Muller, H. Zbinden, and N. Gisin, "Quantum cryptography over 23 km in installed under-lake telecom fibre," *EPL (Europhysics Letters)*, vol. 33, no. 5, p. 335, 1996.

[16] A. Muller, T. Herzog, B. Huttner, W. Tittel, H. Zbinden, and N. Gisin, "plug and play systems for quantum cryptography," *Applied Physics Letters*, vol. 70, no. 7, pp. 793–795, 1997.

[17] S. J. Phoenix, S. M. Barnett, P. D. Townsend, and K. Blow, "Multi-user quantum cryptography on optical networks," *Journal of Modern Optics*, vol. 42, no. 6, pp. 1155–1163, 1995.

[18] L.-M. Duan, M. Lukin, J. I. Cirac, and P. Zoller, "Longdistance quantum communication with atomic ensembles and linear optics," *Nature*, vol. 414, no. 6862, pp. 413–418, 2001.

[19] P. Xue, C.-F. Li, and G.-C. Guo, "Conditional efficient multiuser quantum cryptography network," *Physical Review A*, vol. 65, no. 2, p. 022317, 2002.

[20] D. Deutsch, A. Ekert, R. Jozsa, C. Macchiavello, S. Popescu, and A. Sanpera, "Quantum privacy amplification and the security of quantum cryptography over noisy channels," *Physical Review Letters*, vol. 77, no. 13, p. 2818, 1996.

[21] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, "Hacking commercial quantum cryptography systems by tailored bright illumination," *Nature Photonics*, vol. 4, no. 10, pp. 686–689, 2010.

[22] H. Chun, I. Choi, G. Faulkner, L. Clarke, B. Barber, G. George, C. Capon, A. Niskanen, J. Wabnig, D. OBrien et al., "Handheld free space quantum key distribution with dynamic motion compensation," *Optics Express*, vol. 25, no. 6, pp. 6784–6795, 2017.

[23] J. Gruska, *Quantum computing*. McGraw-Hill London, 1999, vol. 2005.

[24] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," *Reviews of Modern Physics*, vol. 74, no. 1, p. 145, 2002.

[25] A. Aspect, P. Grangier, and G. Roger, "Experimental realization of einstein-podolsky-rosen-bohm gedankenexperiment: a new violation of bell's inequalities," *Physical Review Letters*, vol. 49, no. 2, p. 91, 1982.

[26] D. M. Greenberger, M. A. Horne, and A. Zeilinger, "Going beyond bells theorem," in *Bells Theorem, Quantum Theory and Conceptions of the Universe*. Springer, 1989, pp. 69–72.

[27] A. Aspect, P. Grangier, and G. Roger, "Experimental tests of realistic local theories via bell's theorem," *Physical Review Letters*, vol. 47, no. 7, p. 460, 1981.002.