Neural, Parallel, and Scientific Computations 18 (2010) 391-400

THE RELEVANCE OF QUANTUM CRYPTOGRAPHY IN MODERN NETWORKING SYSTEMS

KHALIL DAJANI, ROBERT OWOR, AND ZEPHYRINUS OKONKWO
Albany State University, Department of Mathematics & Computer Science,
Albany, Georgia 31705

ABSTRACT. The combination of physics, mathematics, and computer science in quantum computing has developed from a visionary idea to one of the most fascinating and promising areas of quantum mechanics in the past two decades. Research in the field of quantum cryptography promises extremely fast, robust, and impenetrable electronic and photonic security; almost unbreakable! Moreover, the long standing eavesdropping problem of the “man in the middle” attack may finally be solved once and for all. As computing power increases, and as hackers and attackers become more sophisticated, it is feared that sooner or later, traditional cryptography based on mathematically intractable algorithms may be no match for parallelized quantum based processors. For this reason, quantum cryptography, based on the laws of quantum statistical mechanics provides a welcome solution to this fear. This paper explores the basic tenets of quantum cryptography and how the mathematical principles therein apply to the quantum key distribution problem; a central concern in the implementation of quantum cryptography in distributed networks. The quantum key distribution protocol implemented in BB84 protocol is also described and compared to traditional cryptographic systems. A short overview of recent commercial implementations of quantum cryptography is presented with the encountered successes and limitations discussed. This paper explores the development of quantum networks, from the onset of the development of secure communication based on quantum cryptography and concludes with a brief outline of the key challenges facing quantum cryptography implementation in wireless applications and long haul communications.

Keywords. Quantum Networks, Quantum Cryptography, Secure Communication, Quantum Protocol, Authentication, Quantum Key Distribution.

1. INTRODUCTION

The influence of quantum mechanics over the last century is clear in a host of technologies. Lasers, MRI machines, integrated circuits and fluorescent lights are just a few of the everyday applications of quantum effects. Quantum encryption has, since the inception of the BB84 protocol, become one of the most captivating applications of quantum mechanics, with a large number of potential uses. Quantum systems that manipulate, store and transmit quantum information based on laws of quantum physics are now being exploited in many physical systems. Quantum effects such as entanglement and superposition of quantum states, the no-cloning theorem, non-locality principles, etc are widely exploited in quantum cryptography, quantum communication, and quantum computation. The most heavily utilized of these, quantum cryptography, uses the no-cloning property to implement unbreakable Quantum Key Distribution (QKD) cryptosystems (Zhao et al., 2006; Gottesman et al., 2004). The system architecture for a quantum network has, over the years, evolved from a single, stand-alone QKD link to both trusted and untrusted QKD networks. The quantum network combines a variety of QKD techniques with well-established internet security protocols to build a secure key distribution system employed in conjunction with the public internet or, more likely, with private networks that employ the internet protocol suite. In its simplest form, a quantum network distributes keys for a virtual private network (VPN) overlay running atop an underlying public or private internet. Geographic constraints would make it necessary to have QKD relays or repeaters at intervals along the fibre-optic network, due to signals weakening during transmission, possibly due to absorption or decoherence. The best current systems can support distances of up to 150 km through fibre (though at very low bit-rates), or 32 km through free-space quantum cryptography (Gottesman et al., 2004).

Received April 25, 2010

2. QUANTUM COMMUNICATION

In using a cryptographic protocol, the sending party has to use a cryptographic key to encode the information, and the receiving party decodes it using a key. There are two distinct ways to distribute the keys; *private* and *public*. In *private* or *symmetrical* key cryptosystems, the parties have to share a key before they send and receive the message. If the key is the same length as the message, randomly generated every time, and is used only once, it constitutes a *Vernam cipher* or *one-time pad*, the only provably secure cryptosystem at this time. Modern *public* or *asymmetric* cryptosystems use two matching keys – a public key, accessible by anyone, and a private key. Only the owner of the private key can easily decrypt a message encrypted with the public key. The security of this system is based on the difficulty of calculating the inverse of so-called "one-way" functions, where computational complexity grows exponentially with the number of bits in the key (Bennett & Brassard, 1984).

2.1. DESIRABLE ATTRIBUTES OF A QKD NETWORK

Since the outset of quantum cryptography with the BB84 experiments (Zhao et al., 2006; Gottesman et al., 2004), the protocols and structure of quantum communication have been determined by the need that the network meet some basic requirements. These requirements are summarized in the following sections.

2.1.1. KEY CONFIDENTIALITY

Public key systems suffer from an ongoing uncertainty that the mathematical principles behind it might one day become solvable, leading to a loss of ability to communicate securely and exposing already-encrypted systems to the rest of the world. Secret key systems suffer from the logistical problems of key control and distribution. If properly embedded into an overall secure system, QKD offers automatic key distribution that would offer far superior security. QKD by itself is not an authentication scheme. Current authentication strategies include prepositioned secret keys at pairs of devices, or hybrid QKD-public cryptosystem means of authentication. Neither of these is free from the weaknesses of the underlying protocol, i.e. key distribution logistics and denial of service attacks, and the onslaught of advances in mathematics on seemingly complex formulas, respectively. Authentication is currently one of the more difficult aspects of QKD communication.

2.1.2. RAPID DELIVERY AND DETECTION OF KEYS

Key distribution systems must be able to deliver keys fast enough that encryption devices do not run out of keying material. The difference is the rate at which keying material is produced as opposed to the rate at which it is used for encryption and decryption. In current quantum key distribution implementations, pseudo-single photon sources such as attenuated laser pulses or photon pairs generated by Spontaneous Parametric Down-Conversion are used (Lo & Zhao, 2009). The efficiency of these two is low, mostly in the 1.0 Mbps range, and often lower, resulting in a significant reduction in key production. True on-demand single-photon sources are required for a truly robust QKD system. Current research is aimed at increasing key generation throughput rates to 10Gbps, and efforts into the development of single photon sources are currently looking at physical systems such as semiconductor structures, color centers in diamond and cavity quantum electrodynamics. Single photon detection also provides an area that needs improvement. Current technologies use a variety of techniques, such as avalanche photo-diodes (APDs), photo-multipliers, multichannel plates and superconducting Josephson junctions. None of these existing approaches can provide high quantum detection efficiency over a broad spectral range, a small dark count, good timing resolution and small recovery/dead time, which are all required for reliable QKD systems.

2.1.3. QUANTUM RAM AND REPEATERS

Establishing a key becomes increasingly difficult as the distance between parties increases. Photon loss during transmission is bound to even further reduce already low key generation rates. The challenge therefore becomes repeating an arbitrary quantum signal while taking into consideration the no-cloning and Uncertainty properties of quantum particles. This is achieved by *shared distant entanglement* (Huttner et al., 1995), which enables teleportation of a quantum state. Distributing quantum data over long distances is hindered by two key issues, viz. (1) photon absorption in the fiber, which, as stated, is exponential to distance, and (2) degradation of the fidelity of quantum state of a photon due to decoherence, also exponential to length (Bennett & Brassard, 1984).

3. QUANTUM NETWORK PROTOCOLS

The emergence of quantum computing and networking has led to the desire to create a quantum internet, i.e. quantum computers (nodes) connected by quantum and classical channels. While BB84 and successive protocols dealt with a maximum of two nodes, quantum networks require that the possibility be defined for multiple nodes of distribution (Lo & Zhao, 2009). Defining a quantum network protocol would require, among others, designing a network architecture that would allow a node to control the time at which it chooses to accept a qubit particle. To create a truly OSI-compatible model, a number of issues have to be determined, i.e.:

a. Routing implications of a disassociated header
b. Physical properties affecting routing (e.g. time-to-live of qubits in a network, short-term storage of qubits, decoherence time of qubits and no-cloning, non-regenerative property of qubits).
c. Implications of scaling from a manageable or experimental number of nodes to an infinitely large or randomly changing number of nodes and storage of qubits for long periods of time.

Within the last few years, QKD links have been demonstrated over increasingly impressive distances over fiber-optic networks. They have been shown to work remarkably well when implemented over conventional Dense Wavelength Division Multiplexed data networks which combine multiple optical signals over one fiber cable, using different wavelengths over the 1550-nm band to carry the different signals. This implies qubit distribution is possible in LANs, MANs and limited WANs. Typically, storage and processing of qubits is physically implemented through *material* qubits, such as trapped ions or atoms, electron or nuclear spins, or Josephson junction superconducting qubits. Transmission is best realized through *flying* qubits, for example, polarization states of photons (Elliott, 2002).

3.1. Cryptography Mechanisms

The most common cryptographic techniques can be identified as "traditional" or "modern". The traditional known techniques date back for centuries, and are tied to operations of *transposition* (reordering of plaintext) and *substitution* (alteration of plaintext characters). In addition, traditional techniques were designed to be much simple, and if they were to be used with great secrecy extremely long keys might be needed. On the other hand, modern techniques rely on the convoluted algorithms or intractable problems to achieve assurances of security.

Two branches of modern cryptographic techniques known as *public-key* and *secret-key* encryption. In public-key cryptography, messages are exchanged using keys that depend on the assumed difficulty of certain mathematical problems; typically the factoring of the product of two extremely large (100+ digits) prime numbers. Each participant has either a public key and/or a private key. The former is used by others to encrypt messages, and the latter by the participant to decrypt them (Bennett & Brassard, 1984).

In secret-key encryption, a *k*-bit secret key is shared by two users, who use it to transform plaintext inputs to an encoded cipher. When designing transformation algorithms, each bit of the output can be made to depend on each bit of the input. Such an arrangement, the key of 128 bits is used for encoding results in a key space of 2^{128} or about 10^{38}. If we assume that brute force, along with some parallelism, is to be employed, then the encrypted message should be secured enough. A major practical problem with secret-key encryption is how to determine a secret key. Any two users, in theory, who wished to communicate, could agree on a key in advance, but in practice for several users this might require secure storage and organization of an awkwardly large database of the specified keys. One possible solution is to agree on the key at the time of communication, but it is problematic since if a secured key hasn't been established, it would be difficult to make up one in a way that foils eavesdroppers. This is referred to as the *key distribution problem* in the cryptography literature.

A known method for solving the key distribution problem is to appoint the central key distribution center. For every potential communicating party he/she must register with the server and establish the shared secret key. As shown in Figure 1, if party A; referred to as *Alice* wishes to establish a secret key with party B; referred to as *Bob*, this request is sent to the central server. The server is often called *Big Brother* can then inform Bob that Alice wishes to establish communication, and to re-encrypt and re-transmit the key she has sent. The secret key can be agreed upon even without a central server. For example: the *Diffie-Hellman key exchange* is an algorithm for agreeing on a secret key based on publicly-discussed large prime numbers. Its security issues are based on the assumed difficulty of taking discrete logarithms modulo of large prime numbers (Elliott, 2002). One of the major objectives in quantum encryption is to provide a way of agreeing on secret key without making such assumption.

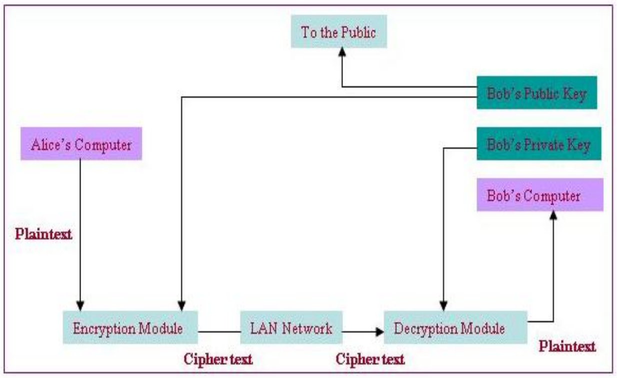
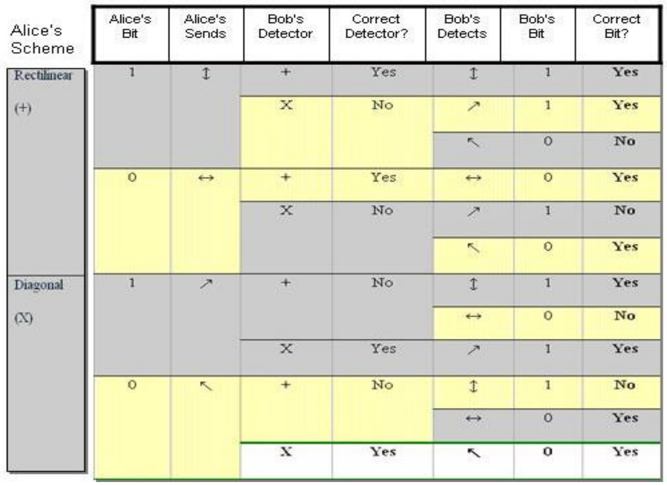


Figure 1: Communication model with public and quantum channels.

BB84 quantum system utilizes polarized light photons to transfer data. Photons are mass less, carry energy, momentum and angular momentum, and vibrate perpendicularly to their plane of movement. This vibration, contained in the angular momentum is known as *polarization* (Gottesman et al., 2004). A polarization filter allows only light of a particular polarization to pass through. A pair of orthogonal and reliably measurable polarization states is referred to as a *basis*, and two bases are *conjugate* if measuring one property completely randomizes the other. Heisenberg's Uncertainty principle dictates that measuring a photon using a rectilinear (horizontal vs. vertical) basis would completely randomize its diagonal (45° and 135°) polarization, and vice versa. Since the two-dimensional polarization Hilbert space allows complex coefficients, a third basis of right- and left-polarized photons that exists, and it also follows the Heisenberg principle. For this explanation, the rectilinear and diagonal bases are used.

Table 1 shows two parties, Alice and Bob, use a quantum channel to send qubits. They are also connected by a conventional channel, insecure but unjammable. They will use the aforementioned bases to produce four quantum states, using ↕ to represent 1, while ↔ represent 0. The protocol begins with Alice sending a sequence of polarized photons to Bob, with the basis (polarization scheme) chosen randomly. Bob, with his choice of basis (or detector) randomly chosen and independent of Alice's (since he doesn't know her schemes at this point), measures the polarization of the photons received. He will, sometimes, use the right detector, and at other times the wrong one and therefore incorrectly interpret Alice's photon.



Alice's Scheme	Alice's Bit	Alice's Sends	Bob's Detector	Correct Detector?	Bob's Detects	Bob's Bit	Correct Bit?
Rectilinear (+)	1	↕	+	Yes	↕	1	Yes
			X	No	↗	1	Yes
					↖	0	No
	0	↔	+	Yes	↔	0	Yes
			X	No	↗	1	No
					↖	0	Yes
Diagonal (X)	1	↗	+	No	↕	1	Yes
					↔	0	No
			X	Yes	↗	1	Yes
	0	↖	+	No	↕	1	No
					↔	0	Yes
			X	Yes	↖	0	Yes

Table 1: The various possibilities of the results of photon exchange between Alice and Bob.

Using the insecure channel, Bob announces to Alice the polarization basis he used to measure the photons, *but not the results of the measurements*. Alice tells him, again publicly, whether he made the correct scheme (i.e. rectilinear or diagonal). Alice and Bob then agree to discard all photons for which Bob used the wrong basis to measure the polarization. They also discard all bit positions where Bob's detectors did not detect a photon.

Bob and Alice then translate the resulting polarizations as 1 for 90° and 45°, and 0 for 135° and 180°. In effect, they now both have a shorter, relatively secret and secure string of bits, known as a *raw quantum transmission* (Zhao et al., 2006). Table 2 below summarizes the process. Based on the Alice codes, Bob decodes and the QKD secret code is generated for communication. The crucial property of this sequence is that it is random, because it was derived from Alice's random initial sequence, and Bob's choice of detector is also random. As Alice transmits the photons, an eavesdropper Eve attempts to measure them. Not knowing what polarization scheme Alice used, she too will randomly choose between the rectilinear and diagonal detectors.

As shown in Table 2, Alice's result is another string of random bits, just as Bob gets. However, Alice will tell Bob what scheme he should have used. No measurement the eavesdropper can make on one of these photons while it is in transit from Alice to Bob can yield more than ½ expected bit of information on its polarization, meaning Eve will have at least half of the keys wrong for the final key. *Privacy amplification* is another method Bob and Alice can use to ensure their key is private. For instance, being aware that Eve has at least 10% of the key, Alice and Bob could agree to use modular arithmetic to add each adjacent pair, chosen through an algorithm of their choice (e.g. physically adjacent, every third photon, etc) to get a shorter key which Eve will know much less about. In general, let a *deterministic bit* of information about *x* be the value *e(x)* of an arbitrary function *e* that maps an n-bit string *x* onto {0, 1}. If an eavesdropper knows at most *t* deterministic bits of the string, then a randomly and publicly chosen hash function, *h* can be used to map *x* onto a new string *h(x)* of length *n - t - s* for any selected positive *s*. Eve will therefore end up knowing less than $\left(2^{-s}/\ln 2\right)$ bit of information about the new key *h(x).*

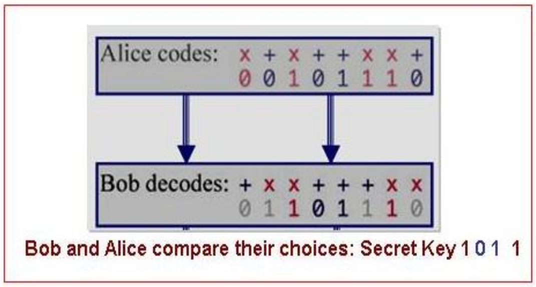

Alice codes: x + x + + x x +
0 0 1 0 1 1 1 0
Bob decodes: + x x + + + x x
0 1 1 0 1 1 1 0
Bob and Alice compare their choices: Secret Key 1 0 1 1

Table 2: Secret code generation for communication.

3.2. QUANTUM CODING

The most common application of quantum cryptography is in the distribution of secret keys. The amount of information that can be transmitted is not very large, but it is provably very secure. By taking advantage of existing secret-key cryptographic algorithms, this initial transfer can be leveraged to achieve a secure transmission of large amounts of data at much higher speeds. Quantum cryptography algorithms are thus an excellent replacement for the Diffie-Hellman key exchange method. The elements of quantum information exchange are observations of quantum states; typically photons are put into a particular state by the sender and then observed by the recipient. Because of the Uncertainty Principle, certain quantum information occurs as *conjugates* that cannot be measured simultaneously.

3.3. QUANTUM STOCHASTIC MODEL FOR QKD ANALYSIS AND SIMULATION OF WIRELESS DISTRIBUTED NETWORKS

From the Heisenberg Uncertainty Principle, the relationship between the wave and particle natures of photons is that the intensity of a wave at any point gives the relative probability of finding the particle at that point. The equation of a wave with a precise wavelength is given by:

$$\varphi(x,t) = A\sin\left(2\pi x/\lambda - 2\pi f\right)$$

Where *f* is the frequency, λ is the wavelength, *t* is time and *x* the displacement. This plane sine wave, however, has an infinite spatial reach. We cannot localize the position of a particle on it. To localize a particle, we superpose waves of different wavelengths (Elliott, 2002).

Taking the period as, $k = 2\pi/\lambda$ and angular velocity as, $\omega = 2\pi f$, can be modeled using formula;

$$\sin\{(k-\Delta k)x - (\omega - \Delta\omega)t\} + \sin\{(k+\Delta k)t - (\omega + \Delta\omega)t$$
$$= 2\sin(kx - \omega t)\cos\{(\Delta k)x - (\Delta\omega)t\}$$

The two close frequencies break up the continuous wave into a series of packets, or *beats*. Hence given a light wave, one can localize the position of the particle by adding waves of slightly different wavelengths. This transforms the wave to be modulated from infinite reach in both spatial directions to a *wave packet* of much narrower spatial extent. This can be used to localize the position of a particle over a narrower portion of the wave, which is equivalent to the width of the wave packet. This width, $\Delta\lambda$, is a function of the widths of the original and modulating waves. Given that Δx represents the spread (uncertainty) of the particle might be in, and Δp represents the uncertainty of its momentum, the product of these two gives (Gottesman et al., 2004 & Owor, et al., 2007);

$$\Delta x \Delta p = \Delta x \Delta \lambda$$

From de Broglie's experiment, we know that $p = h/\lambda$,

Where h is Planck's constant, λ the wavelength and p the momentum,
we get;

$$\Delta x \Delta p = \Delta \lambda \Delta p = \Delta \lambda \, h/\Delta \lambda$$

$$\Delta x \Delta p = h$$

Hence the spread of a particles momentum is inversely proportional to the spread of its position. The more accurately one measures the position of a particle, the more that the momentum of the particle varies. This principle can be extended to show the existence of pairs of properties that are incompatible in the sense that measuring one property completely randomizes the other. Consider the equation of a traveling wave:

$$\varphi = A\cos\left(\frac{2\pi x}{\lambda} - \omega t\right)$$

Using de Broglie's equations:

$$\lambda = \frac{h}{p} = \frac{2\pi\hbar}{p}, \; where \; \hbar = \frac{h}{2\pi}$$

$$\therefore \quad \frac{2\pi}{\lambda} = \frac{p}{\hbar}$$

Using Planck's:

$$e = hf = \frac{h\omega}{2\pi} = \hbar\omega$$

$$\therefore \quad \omega = \frac{e}{\hbar}$$

These values allow us to rewrite the wave function as $\varphi = A\cos\left(\frac{px}{\hbar} - \frac{et}{\hbar}\right)$

Taking partial derivatives of the equation with respect to position and time, two different forms of the wave function are observed, i.e.

$$-i\hbar\frac{\delta\varphi}{\delta x} = p\varphi$$

for the particle's momentum, and $-i\hbar\frac{\delta\varphi}{\delta t} = e\varphi$

for the particle's energy. These equations give the properties subject to quantum mechanism – the *observables*. In accordance to the Heisenberg principle, these pairs of observables (position/momentum and energy/time) cannot be accurately determined at the same time. One of the applications of quantum theory is quantum computing. Turing machines store information in *bits*, with each bit storing one value (represented by either '1' or '0'). A quantum state, denoted by $|\Psi\rangle$, is an element of a finite-dimensional complex vector space (or Hilbert space). Quantum states in Hilbert spaces are *orthonormal* elements, i.e.

1. The elements are *normalized*, the scalar product of two states: $\langle\Psi|\Psi\rangle = 1$ for all states that have a physical meaning.

2. The elements are *orthogonal*, i.e. with the state as a single point vector in a two-dimensional Hilbert space, its base states are represented by perpendicular vectors. Hence, given two states s_1, s_2, $\langle s_1, s_2 \rangle = 0$.

We define the quantum equivalent of a bit as the *qubit*. A qubit is an element of a two-dimensional Hilbert space. Introducing an orthonormal basis consisting of two states, $|0\rangle$ and $|1\rangle$, we can describe the quantum state $|\Psi\rangle$ of the qubit as a superposition of two states, i.e. $|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle$

α and β are normalized complex coefficients. Hence the qubit can hold the values 1, 0, both simultaneously or all values in between, meaning that computation can be done much faster than with a classical computer through *parallelism*. A 30-qubit quantum computer would equal the processing power of a 10-teraflop conventional computer, i.e. with operation-per-second in the trillions. Desktop computers with today's technology can run at speeds measured in gigaflops (billions of floating point operations per second). While quantum computers are still in the experimental realm, researchers have already found applications that can run on quantum computers, e.g. Peter Shor's polynomial-time algorithms that would, if run, effectively render current cryptographic systems void. These applications of quantum theory create an even greater need for quantum computing (Owor, et al., 2007).

4. IMPLEMENTATIONS OF QUANTUM NETWORKS

In association with Harvard University, BBN Technologies and Boston University, the world's first quantum network was developed in December 2002 to provide high-security QKD capabilities and tested against known attacks (Huttner et al., 1995). The network was built from the basic QKD point-to-point structure. It is modeled after cryptographic virtual private networks, although it replaces the VPN public key agreement primitives with keys generated through quantum cryptography. Retaining the remainder of the VPN construct makes the network compatible with current IPSec protocols and architecture for easy data flow across different physical backdrops. The network involved organizing several QKD links into a trusted QKD network. Each QKD link was connected to a separate private enclave. In contrast to the point-to-point links of a QKD link, a meshed QKD network provides a network of relays or routers through the various QKD endpoints, which act as nodes of the network. Such QKD networks can be achieved in several ways (Lo & Zhao, 2009).

The European Union-sponsored quantum cryptography network, dubbed "the mother of all networks" (Elliott, 2002), was unveiled in Vienna in October of 2008. More complex than the Defense Advanced Research Projects Agency (DARPA) network, it encompasses 200 km over six nodes, with links varying in size from 6 to 82 km. It has demonstrated a new aspect of quantum cryptography, namely, the interoperability among different quantum cryptography schemes. Seven technologically different QKD-links, among them being plug and play, coherent-one-way, one-way, decoy states, entangled photons and continuous variables, were combined to form the SECOQC Quantum-Back-Bone (QBB) network, physically connecting five company sites of SIEMENS Austria and the neighboring capital of Lower Austria, St. Poelten (Owor, et al., 2007). Like the DARPA network, the Secure Communication Based on Quantum Cryptography (SECOQC) network is primarily based on weak-coherent link. Unlike DARPA, other key generation capabilities are interwoven into the various nodes. Like DARPA, the various nodes are connected via a mesh of QKD links which allows data transfer to resume seamlessly over another link, should the primary link fail.

5. CONCLUSION

QKD technology and IPSec standards can be combined to create viable computer networks that would far outperform classical networks. Quantum computing is a fast growing field with a lot of possible applications. While the shortcomings seem to abound at every step, various research efforts have successfully shown that most of these can be overcome. For instance, quantum communication through air has been proven over far longer distances by bouncing laser pulses from the Matera Laser Ranging Observatory, in Italy, to the Ajisai satellite, 1, 485 km away, and receiving single photons. Rudimentary quantum memory has been developed through trapping entangled photon states in atom clouds and releasing the states on demand. The wealth of applications and research into the capabilities of quantum computing has only just begun, and we are in for an exciting ride!

6. ACKNOWLEDGEMENT

This work was partially supported under National Science Foundation Grants NSF-DUE-0830241, NSF-DUE-0621307 and NSF-DUE-0516432. We also thank our colleagues at Auburn University.

7. REFERENCES

1. Zhao, Y., Qi, B., Ma, X., Lo, H.-K. and Qian, L. (2006). Simulation and Implementation of Decoy State Quantum Key Distribution over 60 km Telecom Fiber. Proceedings of IEEE International Symposium of Information Theory, pp. 2094 --2098.
2. Gottesman, D., Lo, H.-K., Lutkenhaus, N. and Preskill, J. (2004). Security of quantum key distribution with imperfect devices. Quant. Info. Compu. 4, pp. 325.
3. Bennett , C. H. and Brassard, G. (1984). Quantum Cryptography: Public Key Distribution and Coin Tossing. Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing, pp. 175-179.
4. Lo, H.-K. and Zhao, Y. (2009). Quantum Cryptography. Encyclopedia of Complexity and System Science, Springer, New York, Vol. 8, pp. 7265–7289.
5. Huttner, B. N., Gisin, N. and Mor, T. (1995). Quantum Cryptography with Coherent States. Phys. Rev. A 51, pp. 1863-1869.
6. Elliott, C. (2002). Building the Quantum Network. New Journal of Physics 4, 46.1, 2002, pp 45-89.
7. Owor, R. Dajani, K., Okonkwo, Z. and Hamilton, J. (2007). An Elliptical Cryptographic Algorithm for RF Wireless Devices**.** Winter Simulation Conference WSC07, Dec. 9-12, Washington DC. pp 85-89.