International Journal of Information Technology and Knowledge Management
July-December 2009, Volume 2, No. 2, pp. 297-303

AMNI'09 PROTOCOL

B. Amutha[*] & V. Nivedha Devi[**]

This protocol is used to maintain security in networks for secure communication by overcoming some of the drawbacks in existing security protocols. Integration of both classical and quantum cryptography techniques takes place. Quantum cryptography is used for secure optical transmission which employs quantum mechanisms to distribute session keys Classical cryptography provides convenient techniques that enable efficient key verification and user authentication. This protocol used both implicit user authentication and explicit mutual authentication. A Trust centre is used to generate a secret key and public key by using RSA algorithm and it will develop the random key for each session of transmitting data these key develop a QUIBIT values which develop Session key. By using these keys user translate the messages between the other users securely. Error rate gets reduced when compared to the existing quantum cryptography protocol. Bayesian filtering method is integrated to reduce the external noise. The merits of this new protocol are,

- Secures against attacks as man-in-the-middle, eavesdropping and replay.
- Online guessing attacks can be avoided.
- Efficiency is more since the proposed protocol contain the fewest number of communication rounds.
- Two parties can share and use a long-term secret key by a trusted center.
- Error due to noise gets reduced.

Keywords: Quantum Cryptography, Classical Cryptography, RSA, Session Key, Bayesian Filtering, Noise, Error Rate, Eavesdropping.

1. Introduction

Today's (symmetrical) cryptography algorithms rest upon secure key transmission. In general this key has to be transmitted through the internet (or some public channel) and an eavesdropper (Eve) can easily intercept the communication, catch the key and the whole encoding is for nothing. And what's worse: Alice and Bob never know that they have another listener. One solution to key distribution is to use asymmetrical algorithms like RSA to encode the symmetric key. RSA uses a public key for encoding and a private (secret) key for decoding. This way, the secret key doesn't have to be sent through the internet. It's as difficult for Eve to compute the inverse RSA algorithm as it is to factor large integers or discrete logarithms (prohibitively difficult with current technology). Symmetrical algorithms would be safer, if only the key transmission problem weren't there. And that's where quantum cryptography comes in.

In optical communications, optical signals suffer distortions from the linear and nonlinear properties of matter. In dense wavelength division multiplexing (DWDM), accurate optical power loss and distortion estimation is critical to network engineering as it influences the selection of path during set up, protection, or dynamic wavelength re-assignment Link engineering assures that the optical signal arrives at the receiver at an expected quality and bit error rate (BER) that meets performance requirements [17].

Today, QC is limited in terms of bit-rate, distance, and extension from dedicated point-to-point links to multi-user networks. The goal of the Chair research program is to conduct leading edge research into high bit-rate and long-distance quantum cryptography and to investigate the building of a quantum secured communication network to the benefit of the Albertan and ultimately Canadian society. This includes the:

- Development of high-speed, point-to-point quantum cryptographic systems based on attenuated laser pulses and operating on widely available standard telecommunication fibres over distances.
- Integration of quantum cryptographic systems with secure encoding algorithm for the building of complete, quantum secured communication systems.
- Extension of point-to-point system to networks.
- Development of versatile and robust quantum communication primitives like sources of entangled photons and quantum teleportation units.
- Development of a quantum memory as needed for a quantum repeater. [13]

[*,**]Computer Science, S.R.M. University, Tamilnadu, India
E-mail: bamutha62@gmail.com[*], E-mail: nivedha.v@gmail.com[**]

Conventional data transmission uses electrical signals to represent a binary '1' or '0'. QC uses the polarization, or phase states of individual photons of light to represent the binary digits. Scientists claim that QC theoretically offers absolute security through the basic laws in quantum physics. Two approaches are possible. The first of these relies upon the 'uncertainty principle', which states that a single photon cannot be detected and its polarization (or phase state) measured simultaneously. In other words the superposition of a pair of quantum 'observables' cannot be measured without interfering with the measurement of the other. Moreover, under the 'no cloning' theorem it is not possible to clone a photon so that one can be measured and the other passed on to the recipient. By the use of suitable protocols, involving additional communication over a conventional public communications channel, any attempt to intercept the data may therefore be detected. The first provably secure QC protocol, known as BB84, was proposed by C H Bennett and G Brassard of IBM, in 1984. [10]

Bayesian Filtering:

Owing to analytical intractability, sequential Monte Carlo methods provide an appealing means of addressing the Bayesian filtering task. For the variance minimizing importance function $p(Xt|Xit–1, Yt)$, we have the weight recursion $wit = wit–1p(Yt|Xit–1)$ and hence must find $p(Yt|Xit–1) = ZVk, mp(Yt|Xt)p(Xt|Xit–1)dXt$. In the case of filtering on the Stiefel manifold considered here, this integral cannot in general be evaluated analytically and must be approximated. Hence, we choose as importance function $p(Xt|Xit–1)$, providing the simple weight recursion $wit = wit–1p(Yt|Xit)$. This requires only that we sample each particle $Xit = p(Xt|Xit–1)$, a von Mises-Fisher distribution, and evaluate $p(Yt|Xit)$, a matrix Gaussian distribution. [5]

Use of low-noise detectors can both increase the secret bit rate of long-distance quantum key distribution (QKD) and dramatically extend the length of a fiber optic link over which secure key can be distributed. [12]

Authentication can be accomplished in many ways. The importance of selecting an environment appropriate Authentication Method is perhaps the most crucial decision in designing secure systems. Authentication protocols are capable of simply authenticating the connecting party or authenticating the connecting party as well as authenticating itself to the connecting party. [15]

2. RELATED WORK

BB84 and Ekert91 Protocols:

Benett und Brassard proposed a protocol for a secret key exchange between Alice and Bob in 1984 (BB84). Alice wants to send the key to Bob. She has two bases with polarized Photons She chooses an arbitrary basis for her bits and sends them over the Quantum Channel to Bob. Bob measures in an arbitrary chosen basis, too. If he has no detection he deletes this register. Then he sends this information and information on what bases he chose over a public channel to Alice and keeps the outcome of each measurement secret. After Alice gets Bob's info, she can compare it to her own chosen bases and select the coincidences. She sends the information on the coinciding bases back to Bob and he just looks in his protocol, checks whether he had 0 or 1 for this register and the result forms the key. Now, they can use the key and encrypt the message. The key should be as long as the plaintext and be used only once (one-time-pad). Eve can wiretap the public channel, but that won't do her any good. She gets information on the bases and not on the outcome of the measurement. In case Eve attempts to measure part of the Quantum Channel she betrays herself by a high Quantum Bit Error Rate (QBER) and Alice and Bob are warned. Two parties using BB84 know that Eve is listening and will not use this key for transmitting the actual message.

Researchers built SARG04 when they noticed that by using the four states of BB84 with a different information encoding they could develop a new protocol which would be more robust when attenuated laser pulses are used instead of single-photon sources. SARG04 was defined by Scarani et al in 2004.

3. PROPOSED WORK

Principle:

Integration of quantum cryptography for secure optical transmission and classical cryptography for identity and authentication. In existing quantum cryptography, communication rounds are more and identity of the user is not specified.

Assumptions:

- Number of users are 5.
- Any user can communicate with any other user at any point of time.
- Trusted center should approve based on the number of requests.

Possible Combinations:

Consider 5 users are there in an authenticated community and the authentication between those users will be done by using a trusted center (TC). Each and every user can communicate through trusted center for getting a key. Between each user communication channel was available to transmit message after authentication, so the number of communication channel will be $n(n–1)$. (i.e.) 5(5–1).

A1→A2	A2→A1	A3→A1	A4→A1	A5→ A1
A1→A3	A2→A3	A3→A2	A4→A2	A5→ A2
A1→A4	A2→A4	A3→A4	A4→A3	A5→ A3
A1→A5	A2→A5	A3→A5	A4→A5	A5→ A4

Out of 5 users, the possible communication channels are 4 per user. Therefore for *n* number of users then *n* (*n*–1) channels are required. This is applicable for one time communication among the users. Number of session keys for one time communication is *n* (*n*–1). *M* number of times if communication among the users, irrespective of time then Total number of communications among the users at any point of time is *M*(*n*(*n*–1)). Session key generation is done by the trusted center.

Table 1
Distance Specification for Each User

User	*Distance between user and trust center*
User 1	50
User 2	35
User 3	20
User 4	15
User 5	65

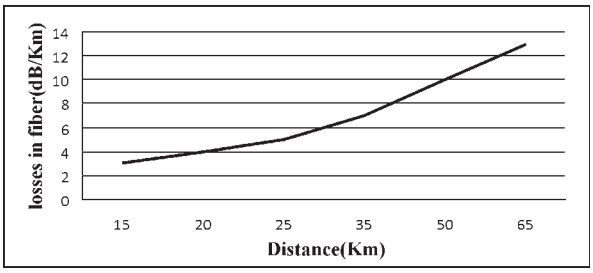

Figure 1: Graph Ranging between Distance and Losses in Fiber

Step 1:

Trusted center maintain a log record for each user (password or facial or RFID or any Biometrics). Through comparison user authentication is done. For each and every user, a private key and public key was created at the time of registration by using RSA algorithm.

1. Choose two large prime numbers *P* and *Q*.
2. Compute $N = P*Q$.
3. Choose *e* (less than *N*) such that *e* and (*P*–1)(*Q*–1) are relatively prime (having no common factor other than 1), Public key is (*N*, *e*).
4. Choose *d* such that (*e***d*) mod [(*P*–1)(*Q*–1)] is equal to 1, Private key is (*N*, *d*).

Private Key and public key will be known to the trusted center and the corresponding user. All user information is stored in trusted center.

Table 2
Private and Public Key Generation using RSA Algorithm

User	*P*	*Q*	*N=P*Q*	*A=(P–1)(Q–1)*	*e<N*	*d {(e*d)modA=1}*
User1	5	11	55	40	3	27
User2	11	3	33	20	3	7
User3	47	71	3337	3220	79	1019
User4	7	17	119	96	5	77
User5	137	131	17947	17680	3	11787

Step 2:

If number of requests are < = 1, no problem for TC to approve for communication.

Else Select user according to the time of request.

Request Packet:

Source id	time units	Destination id

The trusted center gives response based on First-In-First-out basis.

Step 3:

Creation of session key: Trusted center creates a session key and distribute to both the source and destination. A random number is generated by using Random () function.

Random number generation: Shennon entropy based random number generation.

- All bits are random
- Uncertainty
- Zero entropy

Table 3
Random Numbers for User 1

x_n	*P1*	*P2*	*N*	*B=P1*x_n+P2*	*SK=BmodN*
28	9	15	55	267	47
47	9	15	55	438	53
53	9	15	55	492	52
52	9	15	55	483	43
43	9	15	55	402	17

This session key is unique for each communication between users. The session key gets encrypted by using the public key of source and destination by using the formula,

$$C = P \wedge e \bmod N$$

Where P is the session key and C is the encrypted key. These encrypted session key should be converted into quibits and send to the corresponding user.

Table 4
Encryption of Session Key for User 1

Session Key (SK)	*Public Key*	*N*	*ESK=(SK)^e Mod N*	*Binary value of ESK*
47	3	55	38	100110
53	3	55	47	101111
52	3	55	28	11100
43	3	55	32	100000
17	3	55	18	10010

Step 4:

Generation of Quibits: 4 types of polarizing filters,

1. Vertical represents 0
2. Horizontal represents 1
3. Down left to upper right '/' represents 1
4. Down right to upper left '\' represents 0

Single photon is separated from the light source by using any one of the polarizing filter. This will be done in TC. Based on the private key of sender and receiver these quibits will be passed through the quantum channel. The quibits passed through the beam splitter and avalanche photodiode is used to capture the photon. In trusted center a laser diode is used to produce photon by passing it through the polarizing filter. If the encrypted session key contains '*n*' number of bits then '*n*' number of photons should be generated. The polarizing filter for polarization of photon will be selected based on the *i*th bit of the private key of the user and the *i*th bit of the session key of the same user. If number of bits in private key is *m* and number of bits in encrypted session key is *n*, where $m < n$,

(i.e.) private key bits are 1, 2, 3… *m*, Public key bits are 1, 2… *m*, *m* + 1…*n*

Till *m*th bit the corresponding values will be taken and for (*m* + 1)th bit the first bit of private key will be considered and so on.

For example, private key is, 11000100, Encrypted session key is, 1000011111

Private key	1	1	0	0	0	1	0	0	1	1
Session key	1	0	0	0	0	1	1	1	1	1
Basis	D	D	R	R	R	D	R	R	D	Ê
Polarizing filter	/	\	|	|	|	/	_	_	/	/
Quibits	/	\	|	|	|	/	_	_	/	/

Table 5
Creating Quibits for User 1 for Different Session

Binary value of ESK	*Binary value of Secret Key(e)*	*Quibit Basis*	*Quibit Values*
100110	11011	D D R D Ê	/ \ | / / \
101111	11011	D D R D Ê	/ \ - / / /
11100	11011	D D R D Ê	/ / - \ \
100000	11011	D D R D Ê	/ \ | \ \ \
10010	11011	D D R D Ê	/ \ | / \

Table 5.1
Selection of Quibit Basis

Bit Value of SK	*Bit Value of Secret Key*	*Quibit basis*	*Quibit Value*
0	1	D(Diagonal)	\
1	1	D(Diagonal)	/
0	0	R(Rectilinear)	|
1	0	R(Rectilinear)	_

These quibits will pass through the quantum channel to the corresponding user. The packet consists of

Source id	time units	Destination id

Step 5:

Decrypting the session key: In both sender and receiver the quibits are converted based on the photon direction. Thus session key was known. In the user, polarizing beam splitters (PBS) were used which is of rectilinear basis and diagonal basis. Avalanche photodiode (APD) is used to separate '0' and '1' in quibit.

Quibits	/	\	|	|	|	/	_	_	/	/
Polarizing filter	D	D	R	R	R	D	R	R	D	Ê
Result bits	/	\	|	|	|	/	_	_	/	/
Binary value	1	0	0	0	0	1	1	1	1	1

Which is the encrypted session key; this will be converted into its decimal value,

$$512 + 0 + 16 + 8 + 4 + 2 + 1 = 543$$

Decrypting the session key will be done by,

$$P = c \wedge d \bmod N$$

This value gives the session key and the binary value is calculated.

Table 8
Receiving Quibits and Decrypting the Session Key

Quibit Basis	*Quibit Values*	*ESK Binary Value*	*ESK*	*SK=(ESK)^d Mod N*
D D R D Ê	/ \ | / / \	100110	38	47
D D R D Ê	/ \ - / / /	101111	47	53
D D R D Ê	/ / - \ \	11100	28	52
D D R D Ê	/ \ | \ \ \	100000	32	43
D D R D Ê	/ \ | / \	10010	18	17

Step 6 :

Security Checks and Transfer Messages:

Users do a security check with the trust center by adding their Bits (0 + 1 + 0 + 0 + 0 + 1...) and both must have an either odd or even result. This key is used for encrypting the messages to be transformed. Similarly, the session key was identified by receiver and it will use that key for decrypting the messages received during that session.

Quantum Bit Error Rate: 2 parameters are considered,

1. Data rate
2. Transmission Length

$$R_{raw} = ½\ V\ \mu\ \eta_t\ \eta_d$$

Where, ½ is incompatibility, V is pulse rate, μ is average number of photons per pulse, η_t is transfer efficiency, η_d is detector efficiency.

Table 6
Calculating Raw Rate

User	*Pulse Rate (V)*	*Mean number of Photons (μ)*	*Transmitter Efficiency (η_t)*	*Receiver Efficiency (η_d)*	$R_{raw} = ½\ V\ \mu\ \eta_t\ \eta_d$
User1	10^6	0.02	0.01	0.00003	0.003
User2	10^6	0.02	0.03	0.00006	0.018
User3	10^6	0.02	0.1	0.00019	0.19
User4	10^6	0.02	0.25	0.00035	0.875
User5	10^6	0.02	0.002	0.000018	0.00036

$$\eta_t = 10^{-L_f\ l + L_b\ / 10}$$

Where, L_f is losses in fiber in dB/km,

l is length of the fiber,

L_B is internal losses in dB.

Table 6.1
Calculation of Transmitter and Receiver Efficiency

User	*Losses in Fiber (L_f) dB/Km*	*Length of the Fiber (l)*	*Internal losses in dB*	$\eta_t = 10^{-L_f\ l + L_B\ / 10}$	*Receiver Efficiency (η_d) = $1/4\pi l^2$*
User 1	0.2	50	10	0.01	0.00003
User 2	0.2	35	7	0.03	0.00006
User 3	0.2	20	4	0.1	0.00019
User 4	0.2	15	3	0.25	0.00035
User 5	0.2	65	13	0.002	0.000018

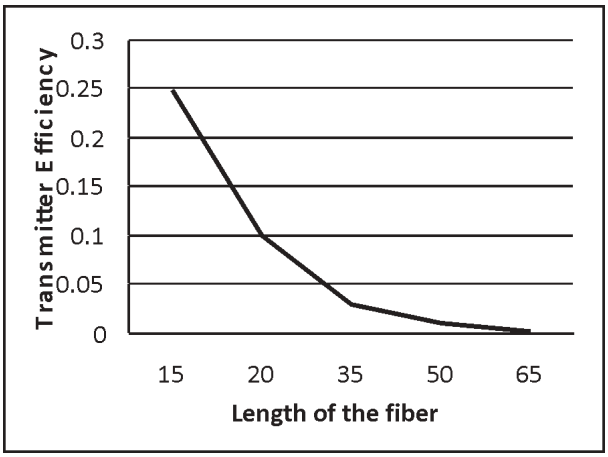

Figure 2: Variation in Transmitter Efficiency

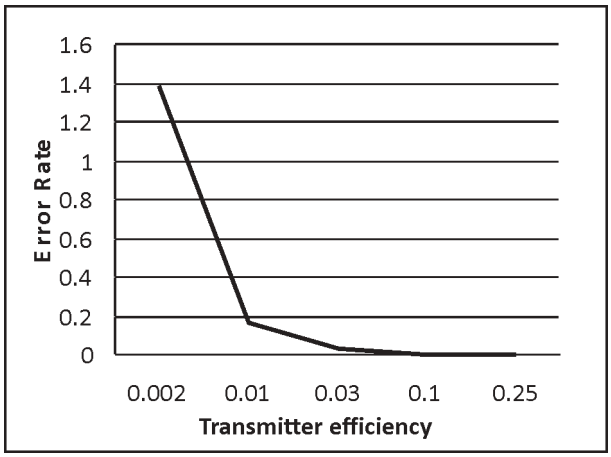

Figure 3: Variation of Error Rate

Two factors cause errors in raw key,

1. Imperfect detector
2. Dark count

Imperfect detector, $R_{opt} = R_{raw} * P_{opt}$.

P_{opt} is probability of wrong detection of polarization. Here P_{opt} is nil.

$$R_{det} = ¼ V P_{dark}$$

P_{dark} is probability to get a dark count (photon detection when there are no photons)

$$Q_{BER} = R_{wrong} / (R_{wrong} + R_{right}) = R_{error} / R_{raw} = (R_{opt} + R_{det}) / R_{raw}$$
$$= ¼ VP_{dark} / ½ V\mu \eta_t \eta_d$$
$$= P_{dark} / 2\mu \eta_t \eta_d = Q_{BERopt} + Q_{BERdet} = P_{opt} + (P_{dark} / 2\mu \eta_t \eta_d)$$

Table 7
Calculating Bit Error Rate

User	P_{opt}	P_{dark}	$C = 2\mu\eta_t\eta_{\hat{e}}$	$Q_{BER} = P_{opt} + (P_{dark} / C)$
User 1	NIL	2	$12*10^{-9}$	$0.16*10^{9}$
User 2	NIL	2	$72*10^{-9}$	$0.027*10^{9}$
User 3	NIL	2	$760*10^{-9}$	$0.002*10^{9}$
User 4	NIL	2	$3500*10^{-9}$	$0.0005*10^{9}$
User 5	NIL	2	$1.44*10^{-9}$	$1.38*10^{9}$

Table 8
Error Rate Based on Dark Count

P_{dark}	Q_{BER}
1	$0.08*10^{9}$
2	$0.16*10^{9}$
3	$0.25*10^{9}$
4	$0.33*10^{9}$

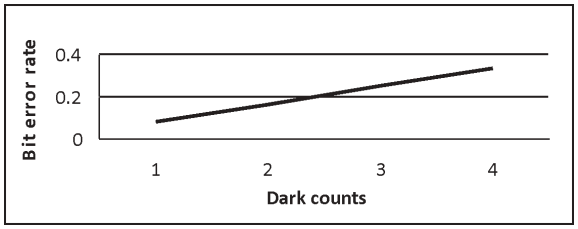

Figure 4: Increase in Error Rate with Respect to Dark Counts

Bits lost due to error correction, $r_{ec} = Q_{BER} (½ - \log_2 Q_{BER})$

Fraction of bits lost due to privacy amplification, rpa = $1 + \log_2 ((1 + 4 Q_{BER} - 4Q_{BER}^{2)} / 2)$

Final bit rate = $(1–r_{ec}) (1–r_{pa}) R_{raw}$

Noise accumulation over distance, if transmission length l increases then transfer rate η will decrease. Receiver efficiency = $1/ 4\pi r^2$, where r is the distance

Error classification:

1. Photon wrong detector
2. Detect dark counts
3. Uncorrelated photons due to imperfect photon sources.

Randomization of phase angle θ,

1 pulse = 1 state (+ive pulse and –ive pulse)

Photon number Eigen states and number of photons per signal is calculated by using Poisson distribution, $f(x) = e^{-\lambda} \lambda^x / x !$

λ = mean number of successes in a given time period

x = number of success we are interested in

e = base of natural log function (ln) ≈ 271828

Noise:

- Bayesian filter is used to reduce the noise.
- For error free common key, 2D parity check scheme is used in both sides confirmation.
- Any row or column that has different parities is discarded which occurred due to noise.
- To maintain privacy, diagonals of the matrix are discarded.
- For error correction, partial information of the key is used.

Uncertainty → variation from actual of bits. Variation with respect to amplitude, frequency and phase. Only using phase splitter, phase angle variation is due to noise which in turn related to uncertainty. (i.e.) either 0 may be represented as 1 or 1 may be represented as 0.

Beam splitter equations:

- If η = 0, zero transmission, 100% reflection.
- If η = 1, 100% transmission, zero reflection.

$$\hat{g} = \sqrt{n}\, \hat{a} + Š(1–\eta)\, \hat{c}$$
$$\hat{h} = \sqrt{(1–\eta)}\, \hat{a} – \sqrt{n}$$

â is signal, ĉ is noise, variance $(\hat{c})^2 = 1$

Two aspects,

1. Quality → entropy
2. Quantity → number of bits

If any one bit varies there is entropy. Entropy data must be incorporated at a particular position of the key bits. No bit variation → zero entropy.

Error rate is reduced in this protocol by reducing the number of bits to be transmitted and by selecting the basis correctly by the receiver.

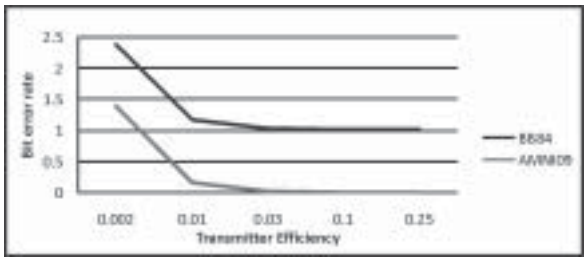

Figure 5: Comparing the Efficiency of BB84 and AMNI09 Protocol

4. CONCLUSION AND FUTURE WORK

This work demonstrates the advantages of combining classical cryptography with quantum cryptography. Compared with classical third-party key distribution protocols, the proposed Quantum Key Distribution Protocol (QKDP) easily resists replay and passive attacks. Compared with other QKDP, the proposed schemes efficiently achieve key verification and user authentication and preserve a long-term secret key between the Trust Center and each user. Additionally, the proposed QKDP have fewer communication rounds than other protocols. Although the requirement of the quantum channel can be costly in practice, it may not be costly in the future. Moreover, the proposed QKDP have been shown secure under the random oracle model. By combining the advantages of classical cryptography with quantum cryptography, this work presents a new direction in designing QKDP. Quantum bit error rate is reduced comparing with the existing quantum cryptography protocol by improving the transmitter efficiency. The motivation of the project is sending the information between source to destination in secure manner and also becomes the protection of attackers due to communication. In that condition the trust center can generate the key for new users become register. The entire communication makes through trust center, the trust center can match both the source key and destination key. Thus identification and authentication of users takes place.

Quantum repeaters can be used in the future to overcome the distance problem in sending quibits through large networks. Collision of data in wireless medium can be avoided to send high quality of data. By overcoming these problems, the whole data itself can be sending as Quibits in the future which is going to be the next generation data transmission.

REFERENCES

[1] Andrew Hammond, Anthony Citrano, MagiQ Technologies, Inc. PR 617/661-8300 x201 617/758-4140, *"MagiQ Technologies Announces New, Next Generation Quantum Cryptography Solution"*, March 28, 2005.

[2] B. Clifford Neuman and Theodore Ts'o, *"Kerberos: An Authentication Service for Computer Networks"*, 0163-6804/94, *IEEE Communications Magazine* September 1994.

[3] Daniel J. Blumenthal, *"Photon Statistics and Basics of Propagation in Dielectric Media"*, ECE 228A, Fall 2007.

[4] Dr. Mario Stip_evi, Institut Ru_er Bo.kovi_CARNet, *"New Directions in Quantum Cryptography"* Users Conference 2004.

[5] Frank Tompkins and Patrick J. Wolfe, Harvard University, *"Bayesian Filtering on the Stiefel Manifold"*.

[6] Gnacio García-Mata, Klaus M. Frahm, and Université de Toulouse, France, *"Shor's Factorization Algorithm with a Single Control Qubit and Imperfections"*, 12 December 2008.

[7] Graeme Smith, John A. Smolin, IBM TJ Watson Research Center, *"Additive Extensions of a Quantum Channel"*, 978-1-4244-2270-8/08 ©2008 IEEE.

[8] Hideki Imai, Manabu Hagiwara, *"Error-Correcting Codes and Cryptography"*, Springer-Verlag 2008.

[9] JimAlves-Foss, University of Idaho, Moscow, *"Security Implications of Quantum Technologies"*.

[10] Matthias Scholz, *"Quantum Key Distribution via BB84"*, November 27, 2007.

[11] Nicolas Gisin, Gr´egoire Ribordy, Wolfgang Tittel and Hugo Zbinden, University of Geneva, Switzerland, *"Quantum Cryptography"*, February 1, 2008.

[12] P. A. Hiskett1, D. Rosenberg1, C. G. Peterson1, R. J. Hughes, S. Nam, A. E. Lita, A. J. Miller and J. E. Nordholt, *"Long-Distance Quantum Key Distribution in Optical Fibre"* Contribution of an Agency of the U.S. Government.

[13] Professor. Wolfgang Tittel *"Quantum Cryptography and Communication"*, Icore Research Report **6**, Fall 2007.

[14] Rajni Goel, Howard University, *"Research Directions in Quantum Cryptography"* International Conference on Information Technology (ITNG'07) 0-7695-2776-0/07 © 2007.

[15] Richard Duncan, *"An Overview of Different Authentication Methods and Protocols"*, October 23, 2001.

[16] S. P. Levitan, P. J. Marchand, M. A. Rempel, D. M. Chiarulli, F. B. McCormick, University of California, San Diego, *"Computer-Aided Design of Free-Space Optoelectronic Interconnection (FSOI) Systems"*.

[17] Stamatios V. Kartalopoulos, Williams, Professor in Telecommunications Networking. *"Factors Affecting the Signal Quality in Optical Data Transmission and Estimation Method for BER and SNR"* 0-7695-2108-8/04 © 2004 IEEE.

[18] Thi Mai Trang Nguyen, Mohamed Ali Sfaxi, and Solange Ghernaouti-Hélie, University of Lausanne, Switzerland, *"Integration of Quantum Cryptography in 802.11 Networks"*, 0-7695-2567-9/06 © 2006 IEEE.

[19] Yi Zhao, Bing Qi, Xiongfeng Ma, Hoi-Kwong Lo, Li Qian Center for Quantum Information and Quantum Control, University of Toronto, Canada, *"Experimental Decoy State Quantum Key Distribution Over 15km"* March 25, 2005.