Bank Transfer over Quantum Channel with Digital Checks

Yoshito Kanamori
Department of Computer Information systems
University of Alaska, Anchorage
Anchorage, AK99508, USA
yoshitok@cbpp.uaa.alaska.edu

Seong-Moo Yoo
Electrical and Computer Engineering Department
The University of Alabama in Huntsville
Huntsville, AL 35899, USA
yoos@ece.uah.edu

Frederick T. Sheldon[†]
Computational Sciences and Engineering Division
Oak Ridge National Laboratory
Oak Ridge, TN 37831, USA
SheldonFT@ornl.gov

Abstract - **In recent years, many quantum cryptographic schemes have been proposed. However, it seems that there are many technical difficulties to realize them (except Quantum Key Distributions) as practical applications. In this paper, we propose a bank transfer (i.e., funds or Electronic Funds Transfer) system utilizing both classical and quantum cryptography to provide theoretically unbreakable security. This system can be realized using current technologies (e.g., linear polarizers and Faraday rotators) and requires no additional authentication and no key distribution scheme. However, a trusted third party must keep all member banks' private keys for encryption, authentication and also for functions to generate classical digital signatures.**

Keywords: Digital signature, encryption, photon, polarization, quantum cryptography.

I. INTRODUCTION

Most practical encryption algorithms rely on computational complexity. These algorithms are only secure when malicious users do not have computational power enough to break security within a practical amount of time. In 1994, P.W. Shor showed that a quantum algorithm could factor large integers and find discrete logarithms in polynomial time [1], whereas classical (non-quantum) algorithms can do so only in much slower exponential time. Therefore, if a quantum computer [2] is built, the existing popular public-key encryption algorithms (e.g., Rivest-Shamir-Adleman (RSA), elliptic curve cryptography [3].) may be compromised. Shor's discovery with such consequent speculations has accelerated the research on quantum cryptography, which theoretically promises an unbreakable cryptographic system. Thus, many quantum cryptographic schemes (e.g., authentication [4], key distribution [5], secret sharing [6]) have been proposed for the last decade.

The major difference between quantum and classical cryptography is the physical resource for data transmission. Instead of electrical (and optical) signals used in classical computer networks, quantum cryptography uses particles and therefore, does not rely on computational complexity, but on quantum mechanical properties such as the no-cloning theorem [2, 7] and quantum entanglement [8]. For example, the proposed BB84 quantum key distribution (QKD) protocol [9] uses the polarization or phase of a photon.

QKD schemes with both phase [10] and polarization encoding have been implemented in free space [11] and in optical fiber [12]. Gobby implemented a QKD system with a phase encoding of over 122 Km in a standard telecommunication optical fiber network [13]. Also, there are some commercial products of QKD schemes [14, 15].

In 2004, the first real bank transfer utilizing a QKD system took place [16]. The QKD system using polarization entangled photon pairs was installed between the headquarters of an Austrian bank and the Vienna City Hall, which were connected by 1.45 Km of optical fiber. Accordingly, QKD protocols seem to be the most practical quantum cryptographic schemes at the present time.

Unfortunately, because key distribution protocols do not generally guarantee that the origin of the message is genuine, they are subject to compromise (i.e., malicious user masquerades as legitimate). In fact, if an eavesdropper is capable of intercepting all data from a sender on both the quantum and classical channels and sending quantum data as well as classical data to a receiver without being detected, the man-in-the-middle attack against QKD schemes is possible [17]. As a result, a secure communication system with QKD still requires the security of authentication. Even if the sender can authenticate the receiver prior to key distribution using classical or quantum authentication protocols, the possibility that the eavesdropper is capable of applying the man-in-the–middle attack right after the authentication, cannot be neglected. Therefore, cryptographic systems using QKD (e.g., one-time pad with QKD) can be considered vulnerable to the man-in-the-middle attack, though QKD itself is unconditionally secure.

The proposed bank transfer system described here is immune to man-in-the-middle attacks utilizing both classical and quantum cryptography which *theoretically* provide unbreakable security. Our scheme requires neither an additional authentication nor key distribution scheme. Still, a trusted third party must keep all member banks' reusable shared keys (for both encryption and authentication) and functions to generate digital signatures. This scheme can be realized using current technologies (e.g., linear polarizers and Faraday rotators) similar to the quantum authentication protocol described in [18].

This paper is organized as follows: In section 2, we introduce classical commutative encryption and a brief overview of quantum commutative encryption (QCE) [18]. We present our bank transfer scheme in section 3, and the

[†]A contractor of the U.S. Government (USG) under DOE Contract DE-AC05-00OR22725 has co-authored this manuscript. The USG retains a non-exclusive, royalty-free license to publish or reproduce the published form of this contribution, or allow others to do so, for USG Purposes.

security analysis in section 4. Finally, conclusions are presented in section 5.

II. CLASSICAL AND QUANTUM COMMUTATIVE ENCRYPTION

When data are encrypted more than once by a commutative encryption algorithm, the cipher text is generated irrespective of the order of encryptions. For example,

$$D_{Ka}[D_{Kb}[E_{Kb}[E_{Ka}[M]]]] = D_{Ka}[D_{Kb}[E_{Ka}[E_{Kb}[M]]]] = M \ ,$$

where Ka and Kb are encryption keys, E and D represent encryption and decryption, respectively. Most encryption algorithms are not commutative, but there are some commutative encryption algorithms. For example, in [19, 20], a commutative encryption system is introduced as $E_k[M] = M^k \bmod p$, where k is a secret key and p is a large public integer.

$$\begin{aligned} E_{k_A}[E_{k_B}[M]] &= (M^{k_B} \bmod p)^{k_A} \bmod p = M^{k_B \cdot k_A} \bmod p \\ &= (M^{k_A} \bmod p)^{k_B} \bmod p = E_{k_B}[E_{k_A}[M]] \end{aligned}$$

Clearly, the cipher text can be determined irrespective of the order of encryptions. The weakness of this scheme is that the security of these classical commutative encryption schemes depends upon computational complexity, as mentioned above.

Recently, a quantum commutative encryption (QCE) scheme has been proposed and used in a quantum authentication protocol [18]. The encryption scheme uses a single photon to transfer one-bit information. Unlike BB84, one orthogonal polarization base (e.g. {horizontal, vertical}) is used for encoding and decoding (i.e., measurement). Here, the horizontally and vertically polarized photons represent the logic-zero and logic-one states, respectively. Encryption and decryption are performed by rotating the polarization of each encoded photon. The angle of the rotation is considered as an encryption key. (Henceforth, key and angle are used interchangeably.) When a polarized photon is represented as a vector: $|\psi\rangle = |0\rangle = (1 \quad 0)^T$ and $|1\rangle = (0 \quad 1)^T$, the rotation can be represented as $R(\theta) = \begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix}$, where θ is a rotation angle. Therefore, when the data bit $M = |0\rangle$, the encrypted data bit is represented as $E_\theta[M] = R(\theta) \cdot |0\rangle = \cos\theta |0\rangle - \sin\theta |1\rangle$, or more generally $E_\theta[M] = \alpha |0\rangle + \beta |1\rangle$, $|\alpha|^2 + |\beta|^2 = 1$, where α and β are called "probability amplitude," which are determined by θ and $|\psi\rangle$. This state is called the quantum superposition state. According to quantum mechanics, the measurement of the superposition state collapses the original state and only one of two states (i.e., $|0\rangle$ or $|1\rangle$) will be observed; $|0\rangle$ will be observed with the probability $|\alpha|^2$, and $|1\rangle$ with $|\beta|^2$. No information regarding the angle of rotation is left after the measurement. Therefore, when eavesdroppers try to read the quantum state, they will obtain zero or one randomly because the rotation angles were chosen randomly for each transmitted photon. Since the measurements by the eavesdroppers cause an increase of the transmission error rate, we can also detect the existence of eavesdroppers by observing the transmission error rate. Moreover, an eavesdropper cannot make a copy of the transmitted data based on the no-cloning theorem. This property makes it extremely difficult (if not impossible) for eavesdroppers to apply cryptanalysis to the transmitted data.

Each encryption for a photon requires a rotation with an angle. We can represent the data encrypted more than once as follows:

$$\begin{aligned} & E_{\theta_1}[E_{\theta_2}[\ \dots E_{\theta_{i-2}}[E_{\theta_{i-1}}[E_{\theta_i}[M]]] \dots]] \\ &= E_{\theta_1}[E_{\theta_2}[\ \dots E_{\theta_{i-2}}[E_{\theta_{i-1}}[R(\theta_i) \cdot |\psi\rangle]] \dots]] \\ &= E_{\theta_1}[E_{\theta_2}[\ \dots E_{\theta_{i-2}}[R(\theta_{i-1}) \cdot R(\theta_i) \cdot |\psi\rangle] \dots]] \\ &= E_{\theta_1}[E_{\theta_2}[\ \dots E_{\theta_{i-2}}[R(\theta_{i-1} + \theta_i) \cdot |\psi\rangle] \dots]] \\ &= R(\theta_1 + \theta_2 + \dots + \theta_{i-2} + \theta_{i-1} + \theta_i) \cdot |\psi\rangle , \end{aligned}$$

where θ_i (i = 0, 1, 2….) is an arbitrary angle chosen randomly as an encryption key. Evidently, the encrypted data are irrespective of the order of encryptions. The decryption requires the rotation by $-\theta_i$ (i.e., the rotation by θ_i in the opposite direction of encryption). Therefore, the commutative relation of decryptions is trivial.

Similar to classical one-time pad schemes, this encryption scheme allows users to modify the original message (plain text) in the encrypted data (cipher text) without decrypting the cipher text if the users know the plain text. For example, let us assume that the plain text is a single bit, say, logic-one (i.e., $M = |1\rangle$). Now, a sender encrypts it with an angle θ , $E_\theta[M] = R(\theta) \cdot |1\rangle = \sin\theta |0\rangle + \cos\theta |1\rangle$. If the sender wants to change the plain text, logic-one to logic-zero after the encryption, they simply rotate the quantum state by $\pi / 2$.

$$\begin{aligned} & R(\pi/2) \cdot E_\theta[|1\rangle] = R(\pi/2) \cdot R(\theta) \cdot |1\rangle = R(\theta + \pi/2)|1\rangle \\ &= \cos(\theta)|0\rangle - \sin(\theta)|1\rangle = R(\theta) \cdot |0\rangle = E_\theta[|0\rangle] \end{aligned}$$

By using this technique, receivers can perform exclusive-OR (XOR) operations between the encrypted states and classical bits. For instance, if a receiver wants to perform an XOR operation between three encrypted photons $E_\theta[M']$ and three binary bits "101", they simply rotate the first and the third photons by $\pi / 2$ without decrypting $E_\theta[M']$.

Note that, although the receivers can change the original message, they can not read the data without errors nor can they make copies of the data unlike a one-time pad. Such quantum superposition states could be realized by linear polarizers and faraday rotators. An example of experimental realization of the QCE scheme was given in [18].

III. BANK TRANSFER OVER QUANTUM CHANNEL

In this section, we introduce a bank transfer system, which is theoretically unbreakable and can be realized using current emerging technologies. We assume a simple realistic scenario as follows: there are many member banks and a trusted third party (Carol) that will verify all transactions. A member bank (Alice) transfers money from her account to another member bank (Bob) by endorsing and transmitting an encrypted digital check to Bob. Bob endorses the received check and sends it to Carol. Carol verifies the validity of Alice's check and signature. Then, Carol sends a confirmation notice to Bob. This scenario can be implemented as follows:

1) Carol knows all information about the member banks' identification. Each identification consists of a set of encryption keys and a function f (e.g., one-way hash, symmetric encryption [21]) that generates a digital signature since an encryption does not guarantee the integrity of the message. A transaction starts with Alice's request. Carol generates both a set of random numbers (R_{S1}, R_{S2}, R_{S3}) and a set of session keys (K_{S1}, K_{S2}, K_{S3}). She encrypts (R_{S1}, R_{S2}, R_{S3}) with (K_{S1}, K_{S2}, K_{S3}), respectively. Then, Carol sends $\{(a) \,||\, (b) \,||\, (c)\}$ as a blank check to Alice.

$$E_{KS1}[R_{S1}] \qquad .....(a)$$

$$E_{KS2}[R_{S2}] \qquad .....(b)$$

$$E_{KS3}[R_{S3}] \qquad .....(c)$$

2) Alice generates a random number R_A. She decides the amount to transfer, M and calculates a digital signature $f_A(M)$. Also, she performs an exclusive-OR (XOR) operation between $\{R_A, R_A \oplus M, R_A \oplus f_A(M)\}$ and $\{(a) \,||\, (b) \,||\, (c)\}$, respectively by the method introduced in section 2. (The symbol '$\oplus$' indicates a bit-wise XOR operation.) Alice also encrypts the resulting states with her encryption keys (K_{A1}, K_{A2}, K_{A3}), respectively. Then, Alice sends $\{(d) \,||\, (e) \,||\, (f)\}$ to Bob.

$$E_{KA1}[E_{KS1}[R_{S1}] \oplus R_A] = E_{KA1}[E_{KS1}[R_{S1} \oplus R_A]] \quad .....(d)$$

$$E_{KA2}[E_{KS2}[R_{S2}] \oplus R_A \oplus M]$$
$$= E_{KA2}[E_{KS2}[R_{S2} \oplus R_A \oplus M]] \qquad .....(e)$$

$$E_{KA3}[E_{KS3}[R_{S3}] \oplus R_A \oplus f_A(M)]$$
$$= E_{KA3}[E_{KS3}[R_{S3} \oplus R_A \oplus f_A(M)]] \,.....(f)$$

3) Bob generates a random number R_B and performs an XOR operation between $\{R_B, R_B, R_B\}$ and $\{(d) \,||\, (e) \,||\, (f)\}$ respectively by the method introduced in section 2. He also encrypts the resulting states with his encryption keys (K_{B1}, K_{B2}, K_{B3}), respectively. Then, Bob sends $\{(g) \,||\, (h) \,||\, (i)\}$ to Carol.

$$E_{KB1}[E_{KA1}[E_{KS1}[R_{S1} \oplus R_A \oplus R_B]]] \qquad .....(g)$$

$$E_{KB2}[E_{KA2}[E_{KS2}[R_{S2} \oplus R_A \oplus M \oplus R_B]]] \qquad .....(h)$$

$$E_{KB3}[E_{KA3}[E_{KS3}[R_{S3} \oplus R_A \oplus f_A(M) \oplus R_B]]] \quad .....(i)$$

4) Carol knows both (R_{S1}, R_{S2}, R_{S3}) and (K_{S1}, K_{S2}, K_{S3}) and also knows all information of member banks' identifications including both $(K_{A1}, K_{A2}, K_{A3}, f_A)$ and $(K_{B1}, K_{B2}, K_{B3}, f_B)$. Since both encryption and XOR operation are simple rotating operations, she can calculate an angle for the decryption and XOR operation for each one of $(g), (h),$ and (i). (Actually, she can calculate them when she generates the session keys.) Carol performs decryptions and XOR operations with (R_{S1}, R_{S2}, R_{S3}) by rotating the polarization of $(g), (h),$ and (i), by the three calculated angles, respectively. Carol measures the resulting states (i.e., photons) $\{(j) \,||\, (k) \,||\, (l)\}$

$$R_A \oplus R_B \qquad .....(j)$$

$$R_A \oplus M \oplus R_B \qquad .....(k)$$

$$R_A \oplus f_A(M) \oplus R_B \qquad .....(l)$$

and retrieves both M and $f_A(M)$ by classical XOR operations between (*j*) and (*k*) and between (*j*) and (*l*). If she cannot verify $f_A(M)$, she aborts the transaction.

5) When Carol can verify Alice's digital signature $f_A(M)$, she keeps it and creates the confirmation notice for Bob. First, she calculates $f_B(M)$ and generates a random number R_{S4}. Carol encrypts $\{R_{S4}, R_{S4} \oplus M, R_{S4} \oplus f_B(M)\}$ with Bob's encryption key (K_{B1}, K_{B2}, K_{B3}). Then, she sends $\{(m) \,||\, (n) \,||\, (o)\}$ to Bob.

$$E_{KB1}[R_{S4}] \qquad .....(m)$$

$$E_{KB2}[R_{S4} \oplus M] \qquad .....(n)$$

$$E_{KB3}[R_{S4} \oplus f_B(M)] \qquad .....(o)$$

6) Bob decrypts $\{(m), (n), (o)\}$ and measures the resulting states. He calculates $f_B(M)$ and compares it with the measured $f_B(M)$. If he then verifies $f_B(M)$, the transaction is successfully completed. If he cannot verify $f_B(M)$, he announces the abortion of the transaction.

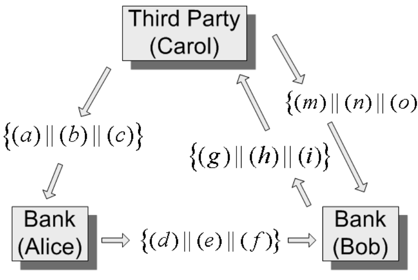
Third Party (Carol)
$\{(a) \,||\, (b) \,||\, (c)\}$
$\{(m) \,||\, (n) \,||\, (o)\}$
$\{(g) \,||\, (h) \,||\, (i)\}$
Bank (Alice)
$\{(d) \,||\, (e) \,||\, (f)\}$
Bank (Bob)

Figure 1: Bank Transfer

IV. SECURITY OF THE PROPOSED SYSTEM

4.1 Quantum Commutative Encryption (QCE)

QCE is similar to a one-time pad since it requires one encryption key (i.e., an angle) for each message bit. The significant difference between QCE and a one-time pad is that the encryption keys of QCE can be theoretically reusable if the system with QCE satisfies the two conditions: (1) no malicious user knows the plain text, and (2) the data bits $|0\rangle$ and $|1\rangle$ are used randomly for an encryption key, on average. Since an eavesdropper (Eve) cannot read the transmitted data bits without knowing the rotation angles, she has to find the encryption keys first. However, it is not possible for her to identify the rotation angle with a couple of intercepted photons (i.e., transmitted data bits) because the information regarding the rotation angle is lost when she measures it. Therefore, her only possible means of attack is to use a statistic with a large amount of sample photons. Since the transmitted data bit cannot be copied (due to the no-cloning property), Eve must intercept a large amount of transmitted photons. Furthermore, she must continue to collect a small fraction of transmitted photons spending a long period of time so that both a sender and a receiver cannot distinguish between errors caused by noise and by Eve's interceptions. If Eve knows a transmitted data (i.e., a plain text) and has collected hundreds of photons, it is not so difficult for her to identify the encryption key. For example, when the data bit is $|0\rangle$ and encrypted with an angle θ, if the transmission axis of the linear polarizer (called analyzer,) is set to horizontal, the probability that a photon is detected behind the analyzer is $P_0 = |\cos(\theta)|^2$. (When the data bit is $|1\rangle$, the probability is $P_1 = |\cos(\theta + \pi/2)|^2$.) When she measures sample photons changing the angle φ between the horizontal axis and the transmission axis from 0 to π, she can guess the angle θ from the plot of the detection counts. *However*, when Eve does not know the plain text where both data bit $|0\rangle$ and $|1\rangle$ appear randomly in the plain text, the probability that a photon is detected is

$$\begin{aligned} P &= \tfrac{1}{2}|\cos(\theta-\varphi)|^2 + \tfrac{1}{2}|\cos(\theta-\varphi+90°)|^2 \\ &= \tfrac{1}{2}\left\{(\cos(\theta-\varphi))^2 + (\sin(\theta-\varphi))^2\right\} = \tfrac{1}{2} \end{aligned}.$$

In short, even if she measures a large number of sample photons, she cannot identify the rotation angle because a flat line appears near to the probability $\frac{1}{2}$ in the plot of the detection counts.

4.2 Bank Transfer System

4.2.1 General

During transmission, all data are encrypted by QCE. Therefore, Eve cannot read the data during the transmissions. Consequently, no data during the transaction can be altered (by Eve). Also, our proposed system is designed to satisfy the two critical conditions introduced at section 4.1. No one knows the amount to be transferred except a bank that requests the transaction (Alice) and the trusted third party (Carol). The purpose of the exclusive-OR operations with random numbers in this system is to make both $|0\rangle$ and $|1\rangle$ bits appear randomly on each data bit. Although a classical digital signature is used in the protocol, it does not degrade the security level of our cryptosystem because Eve cannot apply cryptanalysis without reading the data (i.e., plain text). Also, non-repudiation is assured because a trusted third party (Carol) observes and guarantees the transaction. Carol verifies both the sender and the amount to transfer and keeps the digital signature from a bank that requests the transaction. Additionally, no classical channel is used except the transaction request from Alice. Even if Eve knows who requests the transaction, she does not have any useful attack strategy against this system because the data $\{(a) \| (b) \| (c)\}$ has no information regarding Alice. The data $\{(g) \| (h) \| (i)\}$ becomes meaningful only for Carol when $\{(a) \| (b) \| (c)\}$ is encrypted by both Alice and Bob.

4.2.2 Man-in-the-middle-attack

There are only four places that Eve may try to apply the man-in-the-middle attack.

i) Eve takes over one of four quantum channels

In this case, any modification made by Eve results in the abortion of the transaction (i.e., denial of service). Since Eve does not know the session key nor the random number generated by Carol, Carol cannot verify $f_A(M)$. Bob cannot verify $f_B(M)$ because Eve does not know Bob's secret keys.

ii) Eve takes over both quantum channels between Carol and Alice and between Alice and Bob

Eve intercepts $\{(a) \| (b) \| (c)\}$ and sends a message with all $|0\rangle$ s. Since Alice cannot detect the existence of Eve at this point, she will process the data as described at step 2 (Section 3). The output will be as follows:

$$E_{KA1}[R_A] \| E_{KA2}[R_A \oplus M] \| E_{KA3}[R_A \oplus f_A(M)]$$

All plain texts are randomized by the XOR operation with the random numbers R_A, which is used only for this session. Therefore, the system still satisfies the conditions introduced in section 4.1.

iii) Eve takes over both quantum channels between Alice and Bob and between Bob and Carol

In this scenario, Eve intercepts $\{(d) \| (e) \| (f)\}$ and sends a message with all $|0\rangle$ s. Since Bob cannot detect the existence of Eve at this point, he will process the data as described at step 3 (Section 3). The output will be as follows:

$$E_{KB1}[R_B] \| E_{KB2}[R_B] \| E_{KB3}[R_B]$$

Although all plain text use the same random number R_B, its use is only for this session (one-time-use). This fact prevents Eve from finding the encryption key because (K_{B1}, K_{B2}, K_{B3}) are different keys and the system still satisfies the critical conditions introduced in section 4.1.

4.3 Other Issues

There are two reasons that a one-time pad cannot be replaced with QCE. First, the encryption keys of a one-time pad are not reusable. If the keys are used multiple times, Eve can compromise the system. For example, in the case described in Section 4.2.2-iii, Eve can collect $K_{B1} \oplus K_{B2}$ because she can read and copy the transmitted data if a one-time pad is used. By using $K_{B1} \oplus K_{B2}$, Eve can read "the amount to transfer" without being detected when Bob requests the transaction. Second, although we do not reuse the encryption keys of a one-time pad when a QKD protocol is introduced into the system, cryptographic systems with QKD are considered to be vulnerable to the man-in-the-middle attack [17] as mentioned in section 1.

V. CONCLUSION

We proposed a bank (electronic funds) transfer system model utilizing both a quantum commutative encryption and a classical digital signature to provide theoretically unbreakable security. We showed that the system is immune to the man-in-the-middle attack unlike systems with QKD though it is still vulnerable to the denial of service attack. The system is designed to utilize QCE with shared reusable keys, requires no additional authentication and no key distribution scheme. In this system, QCE is utilized to provide confidentiality and authentication of the transaction while the classical digital signature is used to provide authentication, integrity, and non-repudiation, assuming the third party is trusted. We did not discuss the function which generates a digital signature to simplify our discussion however it is straightforward to include such classical cryptographic techniques (e.g., time stamp) into the proposed system. Furthermore, note that a classical digital signature used in the system does not degrade the security level of the whole system because Eve cannot apply cryptanalysis without knowing the plain text. We believe that this system can be realized using current technologies (e.g., linear polarizers and Faraday rotators) and can be extended to a personal digital check system when quantum memory becomes available. (The development of quantum memory for light has been partially realized in laboratory experiments [22, 23].)

VI. REFERENCES

[1] P.W. Shor, "Algorithm for quantum computation: discrete logarithm and factoring," In Proc. 35th Annual IEEE Symposium on Foundations of Computer Science, Santa Fe, Nov. 1994, pp. 24-134.

[2] M.A. Nielsen and I.L. Chuang, Quantum computation and quantum information, Cambridge University Press, Cambridge, 2000.

[3] John Proos and Christof Zalka, "Shor's discrete logarithm quantum algorithm for elliptic curves, " QIC 3 (No. 4) (2003) pp.317-344

[4] Howard Barnum, Claude Crepeau, Daniel Gottesman, Adam Smith, and Alain Tapp, "Authentication of Quantum Messages," Proc. 43rd Annual IEEE FOCS '02, IEEE Press (2002) 449-458.

[5] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum Cryptography, " to appear in Rev. Mod. Phys, quant-ph/0101098.

[6] Z.J. Zang, Y. Li, and Z.X. Man, "Multiparty quantum secret sharing," *Phys. Rev. A* 71, 044301, 2005.

[7] W.K. Wootters and W.H. Zurek, "A single quantum cannot cloned," Nature 299, 1982, pp. 802-803.

[8] D. Bouwmeester, A. Ekert, and A. Zeilinger, The Physics of Quantum Information, Springer, New York, 2000.

[9] C.H. Bennett and G. Brassard, "Quantum cryptography: public key distribution and coin tossing," Proc. IEEE Int. Conf. on Computers, Systems and Signal Processing, Bangalore, 1984, pp. 175-179.

[10] D. Stucki, N. Gisin, O. Guinnard, G. Ribordy, and H. Zbinden, "Quantum key distribution over 67 km with a plug&play system," New J. Phys. 4, 2002, 41.1–41.8.

[11] R.J. Hughes, J.E. Nordholt, D. Derkacs, and C.G. Peterson, "Practical free-space quantum key distribution over 10 km in daylight and at night," New J. Phys. 4, 2002, 43.1-43.14.

[12] K.J. Gordon, V. Fernandez, P.D. Townsend, and Gerald S. Buller, "A Short Wavelength GigaHertz Clocked Fiber-Optic Quantum Key Distribution System," IEEE J. of Quantum Electronics, Vol. 40, 2004, pp. 900-908.

[13] C. Gobby, Z. L. Yuan, and A. J. Shields, "Quantum key distribution over 122 km of standard telecom fiber," Applied Physics Letters, Vol.84, 19, 2004, pp. 3762.

[14] MagiQ Technologies, Inc., http://www.magiqtech.com/.

[15] id Quantique SA, http://www.idquantique.com/products/network.htm.

[16] Poppe, A. Fedrizzi, T. Lorunser, O. Maurhardt, R. Ursin, H. R. Bohm, M. Peev,M. Suda, C. Kurtsiefer, H. Weinfurter, T. Jennewein, and A. Zeilinger, "Practical quan-tum key distribution with polarization entangled photons," Optics Express, vol. 12,pp. 3865–3871, 2004

[17] Karl Svozil, "Feasibility of the interlock protocol against man-in-the-middle attacks on quantum cryptography," International Journal of Quantum Information, Vol. 3, No. 4 (2005) 649-654

[18] Y. Kanamori, S.M. Yoo, D.A. Gregory, and F. Sheldon, "On Quantum Authentication Protocols," IEEE GlobeCom, St. Louis, MS, Nov. 2005.

[19] R. Agrawal, A. Evfimievski, and R. Srikant, "Information sharing across private databases," In Proc. of ACM SIGMOD International Conference on Management of Data, San Diego, CA, June 2003.

[20] J. Castellà-Roca and J. Domingo-Ferrer, "On the security of an efficient TTP-free mental poker protocol," IEEE Intl. Conf. on Information Technology: Coding and Computing, vol. 2, 2004, pp. 781-784.

[21] B. Schneier, *Applied Cryptography*, John Wiley, New York, 1996.

[22] G.-P. Guo and G.-C. Guo, "Quantum memory for individual polarized photons," Phys. Lett. A Vol. 318, Nov. 2003, pp. 337-341.

[23] B. Julsgaard, J. Sherson, J.I. Cirac, J. Fiuráek, and E.S. Polzik, "Experimental demonstration of quantum memory for light," Nature 432, 2004, pp.482-486.