International Journal of
Soft Computing And Software Engineering (JSCSE)
e-ISSN: 2251-7545
Vol.2,No.8, 2012
Published online: Sep 25, 2012

DOI: 10.7321/jscse.v2.n8.6

An Introduction to Distributed Cryptography Based on Quantum Cryptography

[*1]Leila Pashaie Bonab, [2]Jaber Karimpour, [3]Mohamdali Jamali, [4]Ayaz Isazadeh

[1]I.A.U., Shabestar Branch, Iran
[2]Department of Computer Sciences,University of Tabriz, Iran
[3]Asistant Professor of Computer group, I.A.U., Shabestar Branch, Iran
[4] Department of Computer Science, University of Tabriz, Tabriz, Iran.

Email:[1]*Pashaie88@gmail.com* , [2] Karimpour@tabrizU.ac.ir, [3]m_jamali@itrc.ac.ir ,
[4] isazadeh@ tabrizu.ac.ir

Abstract. **Cryptography is important part of a security plan system. So, if we have a secure cryptography in a system, we have an opportunely to have a secure system and make a system by stability of 99.9% on the network. In this paper we will review the Quantum Cryptography as base model in our idea and after that we'll extend it for use on the network for distributed machine. Therefore we will show that cluster of machine which use distributed quantum machine, how it works base on our idea and how we can have a secure machine.**

Keywords: Quantum Cryptography, Security Systems, Distributed Systems, Cryptography

** Corresponding address:*
Leila Pashaie Bonab,
I.A.U, Shabestar Branch, Iran
Email: *Pashaie88@gmail.com*

1. Introduction

The purpose of the Digital Distributed System Security Architecture is to permit otherwise secure standalone systems to interoperate in a distributed environment without reducing the level of security and assurance of those systems [23]. In this paper we'll review Quantum Cryptography as base model and how it works and after that we'll review how we can use it as base model in distributed machine as a cluster of machine. Therefore we have a secure cluster of machine that works together as a cluster for be secured than independent machine.

Quantum cryptography, or quantum key distribution (QKD) [4,8], is an emerging technology in the field of cryptographic systems where quantum mechanics is used to guarantee secure communication between two parties [1]. In simple terms, quantum cryptography uses the principles of quantum mechanics to provide communication between two parties where eavesdropping can be detected by both the sender and the receiver. The first commercial application is applied towards securing electronic ballots. [1, 2]

An important and unique property of quantum cryptography is the ability of the two communicating users to detect the presence of any third party trying to gain knowledge of the key. This results from a fundamental part of quantum mechanics [9]; the process of measuring a quantum system in general disturbs the system. A third party trying to eavesdrop

International Journal of
Soft Computing And Software Engineering (JSCSE)
e-ISSN: 2251-7545
Vol.2,No.8, 2012
Published online: Sep 25, 2012
DOI: 10.7321/jscse.v2.n8.6

on the key must in some way measure it, thus introducing detectable anomalies. Using quantum superposition's or quantum entanglement, a communication system can be implemented which detects eavesdropping. If the frequency of eavesdropping is below a certain threshold, secure communication can take place.

The security of quantum cryptography relies on the foundations of quantum mechanics, in contrast to traditional public key cryptography which relies on the unproven computational difficulty of certain mathematical functions.

It should be noted that quantum cryptography is only used to produce and distribute a key, not to transmit any message data. This key can then be used with any chosen encryption algorithm to encrypt (and decrypt [10,11]) a message, which can then be transmitted over a standard communication channel. The algorithm most commonly associated with QKD is the one-time pad, as it is provably unbreakable when used with a secret, random key[3].

2. 2. Quantum Information

The power contained in the potential for quantum computation, lies in the fact that the measurement of the quantifiable part of a quantum computer, called a 'qubit', can have more than one value at any given time. In fact, according to the laws of quantum physics, it exists in all possible states at one instance of time.

Contrast this to a measurement of the quantifiable part of a classical computer, called a 'bit' or a binary digit, which is only capable of existing in exactly one of two states at a time[5].

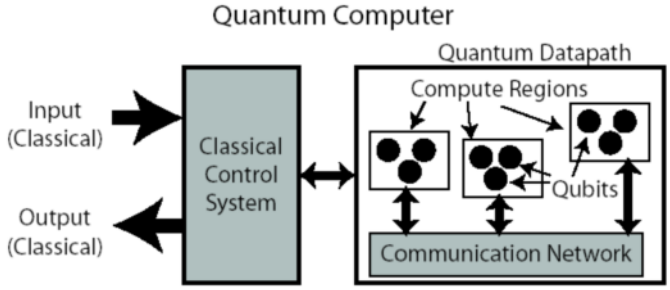


Figure 1. High-level view of a quantum computer architecture. [6]

If you prefer your vectors to be expressed in terms of components, note that we can represent the two orthogonal states of a single Cbit [7].
$|0\rangle$ and $|1\rangle$, as column vectors

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \qquad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \qquad (1)$$

In the case of two Cbits the vector space is four-dimensional, with an orthonormal basis

$$|11\rangle, |10\rangle, |01\rangle, |00\rangle \qquad (2)$$

The alternative notation for this basis,

International Journal of
Soft Computing And Software Engineering (JSCSE)
e-ISSN: 2251-7545
Vol.2,No.8, 2012
Published online: Sep 25, 2012
DOI: 10.7321/jscse.v2.n8.6

$$|1\rangle\,|1\rangle\,,\ |1\rangle\,|0\rangle\,,\ |0\rangle\,|1\rangle\,,\ |0\rangle\,|0\rangle \tag{3}$$

is deliberately designed to suggest multiplication, since it is, in fact, a short-hand notation for the tensor product of the result is illustrated here for a three-fold tensor product:

$$\begin{pmatrix} x0 \\ x1 \end{pmatrix} \otimes \begin{pmatrix} y0 \\ y1 \end{pmatrix} \otimes \begin{pmatrix} z0 \\ z1 \end{pmatrix} = \begin{pmatrix} x0 & y0 & z0 \\ x0 & y0 & z1 \\ x0 & y1 & z0 \\ x0 & y1 & z1 \\ x1 & y0 & z0 \\ x1 & y0 & z1 \\ x1 & y1 & z0 \\ x1 & y1 & z1 \end{pmatrix} \tag{4}$$

On applying this, for example, to the case $|5\rangle_3$, we have:

$$|5\rangle = |101\rangle = |1\rangle \otimes |0\rangle \otimes |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} \tag{5}$$

3. Qbits and their states:

The state of a Cbit is a pretty miserable specimen of a two-dimensional vector. The only vectors with any classical meaning in the whole two dimensional vector space are the two orthonormal vectors $|0\rangle$ and $|1\rangle$, since those are the only two states a Cbit can have. Happily, nature has provided us with physical systems, Qbits, described by states that do not suffer from this limitation. The state $|\psi\rangle$ associated with a Qbit can be any unit vector in the two-dimensional vector space spanned by$|0\rangle$ _ and $|1\rangle$ _ over the complex numbers. The general state of a Qbit [12,13] is

$$|\psi\rangle = \alpha 0\,|0\rangle + \alpha 1\,|1\rangle = \begin{pmatrix} \alpha 0 \\ \alpha 1 \end{pmatrix} \tag{6}$$

International Journal of
Soft Computing And Software Engineering (JSCSE)
e-ISSN: 2251-7545
Vol.2,No.8, 2012
Published online: Sep 25, 2012
DOI: 10.7321/jscse.v2.n8.6

where α_0 and α_1 are two complex numbers constrained only by the requirement that $|\psi\rangle$, like $|0\rangle$ and $|1\rangle$, should be a unit vector in the complex vector space – i.e. only by the normalization condition $|\alpha 0|^2 + |\alpha 1|^2 = 1$.

the general state $|\psi\rangle$ that nature allows us to associate with two Qbits is any normalized superposition of the four orthogonal classical states,

$$|\psi\rangle = \alpha 00|00\rangle + \alpha 01|01\rangle + \alpha 10|10\rangle + \alpha 11|11\rangle = \begin{pmatrix} \alpha 00 \\ \alpha 01 \\ \alpha 10 \\ \alpha 11 \end{pmatrix} \quad (7)$$

$$|\alpha 00|^2 + |\alpha 01|^2 + |\alpha 10|^2 + |\alpha 11|^2 = 1$$

This generalizes in the obvious way to *n* Qbits, whose general state can be any superposition of the 2^n different classical states, with amplitudes whose squared magnitudes sum to unity: [7, 8]

$$|\psi\rangle = \sum_{0 \le x \le 2^n} \alpha x \, |x\rangle_n \,, \quad \sum_{0 \le x \le 2^n} |\alpha x|^2 = 1 \quad (8)$$

4. Quantum Gates

X operation: The only nontrivial reversible operation we can apply to a single Cbit is the NOT operation, denoted by the symbol X, which interchanges the two states $|0\rangle$ and $|1\rangle$: [7]

$$X : |x\rangle \to |\tilde{x}\rangle \;; \qquad \tilde{1} = 0 \;,\; \tilde{0} = 1; \qquad X^2 = 1. \quad (9)$$

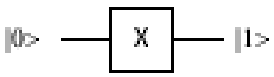


Figure 2: X gate[6]

C-NOT operetion: The 2-Cbit operator whose extension to Qbits plays by far the most important role in quantum computation is the *controlled-NOT* or C-NOT operator **C***i j*.

$$S10|xy\rangle = |xy\rangle \quad (10)$$

International Journal of
Soft Computing And Software Engineering (JSCSE)
e-ISSN: 2251-7545
Vol.2,No.8, 2012
Published online: Sep 25, 2012
DOI: 10.7321/jscse.v2.n8.6

$$S10 = S01 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \tag{11}$$

$$C_{10}|x\rangle|y\rangle = |x\rangle|y \oplus x\rangle \quad , \quad C_{01}|x\rangle|y\rangle = |x \oplus y\rangle|y\rangle \tag{12}$$

$$Y \oplus 0 = Y \quad , \quad Y \oplus 1 = \tilde{Y} = 1 - Y \tag{13}$$

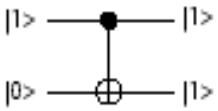


Figure 3: CNOT gate [6]

Hadamard operation: Manipulating operations by *X Gate* and *C-NOT Gate*.
Let Z is a help operations then:

$$Z = \tilde{n} - n = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \tag{14}$$

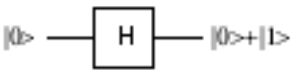
$$ZX = -XZ \quad (17) \tag{15}$$

$$n = \tfrac{1}{2}(1 - Z) \quad , \quad \tilde{n} = \tfrac{1}{2}(1 + Z) \tag{16}$$

$$C_{ij} = \frac{1}{2}(1 + Z_i) + \frac{1}{2}x_j(1 - Z_i) \tag{17}$$

$$= \frac{1}{2}(1 + x_j) + \frac{1}{2}Z_i(1 - x_j)$$

$$H = \tfrac{1}{\sqrt{2}}(X + Z) = \tfrac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \tag{18}$$



International Journal of
Soft Computing And Software Engineering (JSCSE)
e-ISSN: 2251-7545
Vol.2,No.8, 2012
Published online: Sep 25, 2012
DOI: 10.7321/jscse.v2.n8.6

Figure 4: Hadamard gate [6]

5. Quantum Cryptography

The basic quantum cryptography (QC) technology was originally developed by Charles Bennett, an IBM research staff member and IBM fellow, along with Giles Brassard of the University of Montreal in 1984. Their initially developed quantum cryptographic box was called BB84. The BB84 has been the basis for the majority of current implementations of quantum cryptographic systems. As implied in the name, quantum cryptographic technology uses quantum mechanics (specifically the Heisenberg Uncertainty Principle and Quantum Superposition or Quantum Entanglement). These fundamental quantum mechanics principles are used in combination with Privacy Amplification and Information Reconciliation to make quantum cryptography secure. Information exchange within a quantum cryptographic system consists of encoding information into protons in a way that interception or monitoring by a third party is detectable by the sender and recipient. [1, 7]

Whereas classical public-key cryptography relies on the computational difficulty of certain hard mathematical problems (such as integer factorization) for key distribution, quantum cryptography relies on the laws of quantum mechanics. Quantum cryptographic devices typically employ individual photons of light and take advantage of either the Heisenberg uncertainty principle or quantum entanglement. [2]

1. 3.1 BB84 protocol

The typical way of encoding quantum information is by transmission of photons in some polarization states. Photon polarization is the quantum mechanical description of the classical polarized sinusoidal plane electromagnetic wave. Polarization in general, is the property of electromagnetic waves describing the direction of oscillation in the plane perpendicular to the direction of travel. The protocol developed using polarized photons, known as BB84, was developed by Charles Bennett and Giles Brassard [1], uses Heisenberg's Uncertainty Principle. The security of the BB84 protocol comes from encoding the quantum information [15, 16] in non-orthogonal states, where BB84 uses two pairs of states with each pair conjugate to the other and the two within a pair being orthogonal to each other. The typical polarization state pairs used are rectilinear basis of vertical (0) and horizontal (90), the diagonal basis of 45 And 135 or the circular basis of left- and right-handed. All three of these bases are conjugate to each other, so any two can be used together. The typical polarization state pairs are shown below in figure 5. The BB84 protocol uses the rectilinear and diagonal states. [1]

International Journal of
Soft Computing And Software Engineering (JSCSE)
e-ISSN: 2251-7545
Vol.2,No.8, 2012
Published online: Sep 25, 2012
DOI: 10.7321/jscse.v2.n8.6

Basis	Representation	Random Bit 0	Random Bit 1
Rectilinear	+		
Diagonal	X		
Circular	O		

Figure 5: typical polarization state pairs

2. Entanglement protocol

The Ekert scheme uses entangled pairs of photons. These can be made by Alice, by Bob, or by some source separate from both of them, including eavesdropper Eve, although the problem of certifying them will arise. In any case, the photons are distributed so that Alice and Bob each end up with one photon from each pair. The scheme relies on three properties of entanglement [20]. First, we can make entangled states which are perfectly correlated in the sense that if Alice and Bob both test whether their particles have vertical or horizontal polarizations, they will always get opposite answers. The same is true if they both measure any other pair of complementary (orthogonal) polarizations [19]. However, their individual results are completely random: it is impossible for Alice to predict if she will get vertical polarization or horizontal polarization. Second, these states have a property often called quantum non-locality, which has no analogue in classical physics. If Alice and Bob carry out polarization measurements, their answers will not be perfectly correlated, but they will be somewhat correlated. That is, there is an above-50% probability that Alice can, from her measurement, correctly deduce Bob's measurement, and vice versa. And these correlations are stronger - Alice's guesses will on average be better - than any model based on classical physics or ordinary intuition would predict. Third, any attempt at eavesdropping by Eve will weaken these correlations, in a way that Alice and Bob can detect. [2]

6. Security in Distributed Systems

Security is part of all systems which is important part in all systems. Most computer security uses the access control model [14, 20], which provides a basis for secrecy and integrity security policies[24, 25]. Figure 1 shows the elements of this model:

—Principals: sources for requests.

—Requests to perform operations on objects.

In Some complex source such as mentioned in figure 6, we can use this policy to keep protect our systems.

Distributed cryptography spreads the operation of a cryptosystem among a group of servers (or parties) in a fault-tolerant way [21].

Our idea in this paper is: we can use distributed policy base on Quantum Cryptography. It means we can have better and stronger policy when we use distributed policy rather than we have different machine to use it.

International Journal of
Soft Computing And Software Engineering (JSCSE)
e-ISSN: 2251-7545
Vol.2,No.8, 2012
Published online: Sep 25, 2012
DOI: 10.7321/jscse.v2.n8.6

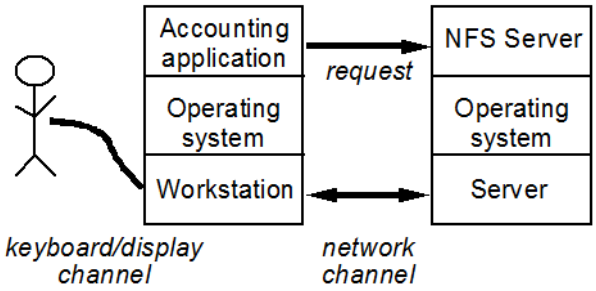


Figure 6: A request from a complex source [18]

The first significant communications application proposed using quantum effects [17, 18] is quantum key distribution, which solves the problem of communicating a shared cryptographic key between two parties with complete security [22]. Classical solutions to the key distribution problem all carry a small, but real, risk that the encrypted communications used for sharing a key could be decrypted by an adversary. Quantum key distribution (QKD) can, in theory, make it impossible for the adversary to intercept the key communication without revealing his presence. The security of QKD relies on the physical effects that occur when photons are measured [22]. However we use different method to implementation our goal. As mentioned in figure 7, we have different machines ($X_{1.i}$) which all of them use the one Quantum Machine (X_1) as base. However in this case these quantum machines (*i)* will be 4 parts ($X_{1.i}$; i=1 to 4), so we need to have 4 parts to decrypt the code for any machine.

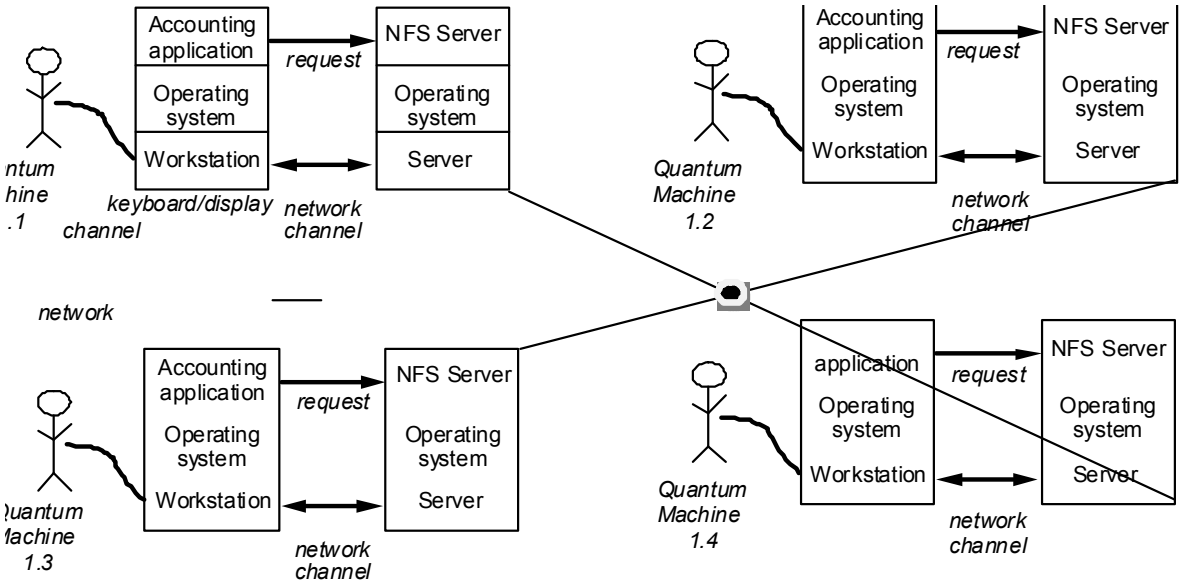


Figure 7: Distributed Quantum machines

According to (9) we have different way to show this change:

International Journal of
Soft Computing And Software Engineering (JSCSE)
e-ISSN: 2251-7545
Vol.2,No.8, 2012
Published online: Sep 25, 2012
DOI: 10.7321/jscse.v2.n8.6

$$X_{1.1} : |x_{1.1}\rangle \rightarrow |\tilde{x}_{1.1}\rangle \; ; \qquad \tilde{1}_{1.1}=0 \; , \; \tilde{0}_{1.1}=1; \qquad X_{1.1}{}^{2}=1. \tag{19}$$

$$X_{1.2} : |x_{1.2}\rangle \rightarrow |\tilde{x}_{1.2}\rangle \; ; \qquad \tilde{1}_{1.2}=0 \; , \; \tilde{0}_{1.2}=1; \qquad X_{1.2}{}^{2}=1. \tag{20}$$

$$X_{1.3} : |x_{1.3}\rangle \rightarrow |\tilde{x}_{1.3}\rangle \; ; \qquad \tilde{1}_{1.3}=0 \; , \; \tilde{0}_{1.3}=1; \qquad X_{1.3}{}^{2}=1. \tag{21}$$

$$X_{1.4} : |x_{1.4}\rangle \rightarrow |\tilde{x}_{1.4}\rangle \; ; \qquad \tilde{1}_{1.4}=0 \; , \; \tilde{0}_{1.4}=1; \qquad X_{1.4}{}^{2}=1. \tag{22}$$

In this case we have different machines and each machine -1.1 ; 1.2; 1.3 and 1.4- should be part of one machine, we called machine 1.
If we need more machine we can make it as different cluster which would be running in this network. As shown in figure 8, we have different H_i to use in one machine that is Hadamard gate.

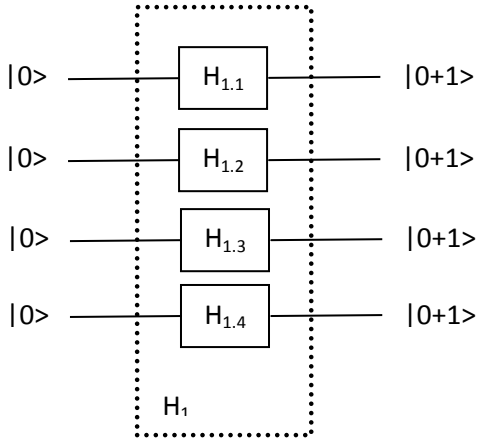


Figure 8: Hadamard Gate for H_1 Cluster

7. Conclusions

It will be at least some years, and probably longer, before a practical quantum computer can be built. Yet the introduction of principles of distributed quantum mechanics has resulted in remarkable security plan. Perhaps most significantly, it has been shown in this paper as important methods for safe and secure systems base on Quantum Machine in distributed systems. However this idea requires more practice and experiment to improve the model and be available in efficient fault tolerance in the system which uses this method and to be reliable and safe system.

International Journal of
Soft Computing And Software Engineering (JSCSE)
e-ISSN: 2251-7545
Vol.2,No.8, 2012
Published online: Sep 25, 2012
DOI: 10.7321/jscse.v2.n8.6

References:

[1]. Houston-L, "Secure Ballots Using Quantum Cryptography", Available on line at: http://www.cse.wustl.edu/~jain/cse571-07/ftp/ballots/index.html.2007.
[2]. http://en.wikipedia.org/wiki/Quantum_cryptography.2007.
[3]. Simerson-C, "Shedding Light on Quantum Cryptography", ICTN 6875,2009.
[4].M¨uller-M, " Quantum Kolmogorov Complexity and the Quantum Turing Machine" Technischen Universit ¨at Berlin , 2007.
[5]. Kenemy-J, "Quantum Cryptography: Perfect Security?", SE 4C03 Winter 2005.
[6]. Y-Patel, ''Communication and control for quantum circuit'', (California university), Available on line at: http://www.eecs.berkeley.edu/Pubs/TechRpts/2010/EECS-2010-77.html, 2010.
[7]. N- David Mermin, "Quantum Computer Science", Cornell University, 2007, Available on line at: www.cambridge.org/9780521876582.
[8]. Hirvensalo-M, "Quantum Computing", Second Edition, University of Turku, 2003.
[9]. Jacob,West."The Quantum Computer An Introduction",Available on line at: www.cs.rice.edu/~taha/teaching/05F/2005_09_16.htm .
[10]. Hong-m, "Study on promoting quantum mechanics-teaching modernization by information technology", Vol.2, No.2, 112-114, 2010.
[11]. A. Barenco, C. H. Bennett, D. DiVicenzo, N. Margolus, P. Shor,T. Sleator, J. Smolin, and H. Weinfurter, "Elementar gates for quantum computation", Phsical Review A, 52:3457{3467}, 1995. Available on line at: http://arxiv.org/abs/quant- ph/9503016
[12]. S. Goldwasser, S. Micali and C. Racko_, The Knowledge Complexity of In-teractive Proof-Systems, Siam J. on Computing, 18(1) (1989), pp. 186-208.
[13]. S. Goldwasser, A New Directions in Cryptography: Twenty something years after, an invited paper, FOCS 97.
[14] A. Herzberg, S. Jarecki, H. Krawczyk, M. Yung, Proactive Secret Sharing, or: how to cope with perpetual leakage, Advances in Cryptology { Crypto 95 Proceedings, Lecture Notes in Computer Science Vol. 963, D. Coppersmith ed., Springer-Verlag, 1995, pp. 339-352.
[15] A. Herzberg, M. Jakobsson, S. Jarecki, H. Krawczyk, M. Yung, Proactive Public-Key and Signature Schemes Proceedings of the Fourth Annual Con-ference on Computer and Communications Security, ACM, 1996.
[16] M. Ito, A. Saito, and T. Nishizeki, Secret sharing schemes realizing general access structures, In Proc. IEEE Global Telecommunications Conf., Globe-com'87, pp. 99 {102,Washington, DC., 1987. IEEE Communications Soc Press.
[17] D. Kravitz. Digital signature algorithm, U.S. Patent #5,231,668, July 27, 1993.
[18] Bulter Lampson, Martin Abadi, Michael Burrows, Edward Wobber, "Authentication in Distributed Systems: Theory and Practice", Computer Systems 10, 4 (Nov. 1992), pp 265-310. A preliminary version is in the Proc. 13th ACM Symposium on Operating Systems Principles.
[19] Comba, P. Exponentiation cryptosystems on the ibm pc. ibm Syst. J. 28, 4 (Jul. 1990), 526-538.
[20] Lampson, B. Protection. acm Oper. Syst. Rev. 8, 1 (Jan. 1974), 18-24.

International Journal of
Soft Computing And Software Engineering (JSCSE)
e-ISSN: 2251-7545
Vol.2,No.8, 2012
Published online: Sep 25, 2012
DOI: 10.7321/jscse.v2.n8.6

[21] Y. Desmedt, Threshold cryptography, European Transactions on Telecommunications 5 (1994), no. 4, 449–457.
[22] Paul E. Black, D. Richard Kuhn, Carl J. Williams, "Quantum Computing and Communication ",Advances in Computers, Marvin Zelkowitz, ed,, 2002
[23] Morrie Gasser, Andy Goldstein, Charlie Kaufman, Butler Lampson, "The Digital Distributed System Security Architecture", Proc. 12th National Computer Security Conf., NIST/NCSC, Baltimore, 1989, pp 305-319.
[24] Mehdi Bahrami, A. Faraahi, A.M. Rahmani, "AGC4ISR, New Software Architecture for Autonomic Grid Computing", Intelligent Systems, Modelling and Simulation (ISMS), pp 318-321, 2010
[25] Mehdi Bahrami, Ghazal Riahi, "Introduction to SAGC4ISR, New Software Architecture For Smart Grid Computing Networks", Australian Journal of Basic and Applied Sciences, 6(2): 148-157, 2012