International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459 (Online), An ISO 9001:2008 Certified Journal,Volume 3, Special Issue 2, January 2013)
National conference on Machine Intelligence Research and Advancement (NCMIRA, 12), INDIA.

The New Approach of Quantum Cryptography in Network Security

Avanindra Kumar Lal[1], Anju Rani[2], Dr. Shalini Sharma[3]
(Avanindra kumar)

Abstract

There are multiple encryption techniques at present time but they cannot provide sufficient security. Thus security is still a challenging issue of communications. By the Since now –a-days security is the primary concern for any organization. This paper suggest a new approach of quantum computation. In this approach fingerprint and quantum mechanical affect creates new and highly secure network.

***Keywords*-- Quantum cryptography, quantum computation, public key encryption ,quantum computers. BB84 protocol**

I. INTRODUCTION

Cryptography means that we Keep a message secret during transmission through untrusted and insecure channel. Its simple means- encoding and decoding messages and has existed as long as people have distrusted each other and sought forms of secure communication. This encoding and decoding is perform by the some special key which is Secret key.The main concept of cryptography is to transmit information at the perfect node or actual receiving node. Originally the security of a cryptosystem or a cipher depended on the secrecy of the entire encrypting and decrypting procedures. In Cryptography cipher means that the encoded message or it is also called the encrypted message. In such ciphers a set of specific parameters, called a key, is supplied together with the plaintext or original text as an input to the encrypting algorithm, and together with the cryptogram as an input to the decrypting algorithm. This can be written as

Me(P) = C;
and conversely,
Mdk (C) = P;

Where P stands for plaintext, C for cryptotext or cryptogram, k for cryptographic key, and Me and Md denote an encrypted and a decrypted messages respectively. It was shown, that as long as the key is truly random, has the same length as the message, and is never reused then the one-time pad is perfectly secure.

So, if we have a truly unbreakable system,.

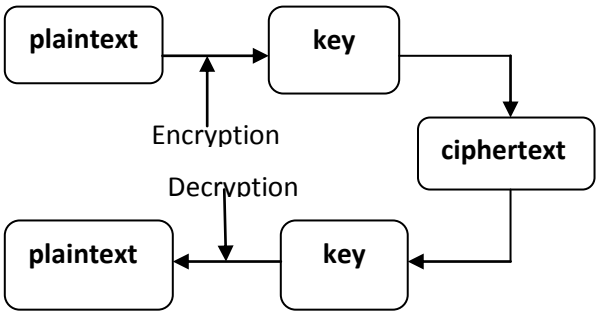
what is wrong with classical cryptography?

In classical cryptography use the concept of key distribution. In this when the key is established, sub-sequent communication involves sending cryptograms over a channel.

However in order to establish the key, two users, who share no secret information initially, must at a certain stage of communication use a reliable and very secure channel.

In principle any classical key distribution can always be passively monitored, without the legitimate users being aware that any eavesdropping has taken place.

In classical cryptography concept use the secret key encryption technique.



International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459 (Online), An ISO 9001:2008 Certified Journal,Volume 3, Special Issue 2, January 2013)
National conference on Machine Intelligence Research and Advancement (NCMIRA, 12), INDIA.

The interesting solution for the concept of key distribution problem proposed by the Whitfield Diffie and Martin Hellman.

It involved two keys, one public key for encryption and one private key for decryption:

E(P) = C, and, D(C) = P

Key distribution problem method is that do not use the same key for encryption and decryption of the message. For encryption which is sender node side use the public key and receiver side use the private key for decrypt the message. Every user has his own two keys; the public key is publicly announced and the private key is kept secret. This concept is perform by using the RSA algorithm. Suppose that Alice wants to send an RSA encrypted message to Bob (Alice and Bob are two individuals who want to communicate secretly). This method is generally called the Public Key Cryptography.

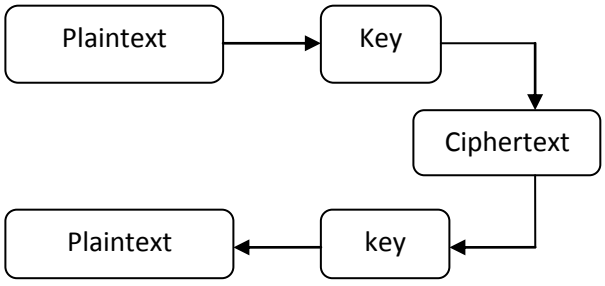
The RSA encryption scheme works as follows:

Encryption: Alice obtains Bob public key = (e; n) from some sort of yellow pages or an RSA public key directory. Alice then writes her message as a sequence of numbers.

Encryption: Alice obtains Bob public key = (e; n) from some sort of yellow pages or an RSA public key directory. Alice then writes her message as a sequence of numbers.

Decryption: Receiving the cryptogram C; Bob decrypts it by calculating

D(C) = C^dmod n = P



II. QUANTUM CRYPTOGRAPHY

It describes the use of quantum mechanical effects (in particular quantum communication and quantum computation) to perform cryptographic tasks or to break cryptographic systems.

The Well-known examples of quantum cryptography are the use of quantum communication to securely exchange a key (quantum key distribution) and the (hypothetical) use of quantum computers that would allow the breaking of various popular public-key encryption and signature schemes (e.g., RSA and ElGamal).

The advantage of quantum cryptography lies in the fact that it allows the completion of various cryptographic tasks that are proven or conjectured to be impossible using only classical (i.e. non-quantum) communication (see below for examples). For example, quantum mechanics guarantees that measuring quantum data disturbs that data; this can be used to detect eavesdropping in quantum key distribution.

Quantum computers will break today's most popular public-key cryptographic systems, including RSA, DSA, and ECDSA. This book introduces the reader to the next generation of cryptographic algorithms, the systems that resist quantum-computer attacks: in particular, post-quantum public-key encryption systems and post-quantum public-key signature systems. Leading experts have joined forces for the first time to explain the state of the art in quantum computing, hash-based cryptography, code-based cryptography, lattice-based cryptography, and multivariate cryptography. Mathematical foundations and implementation issues are included.

Quantum cryptography can be used to distribute the secret digital keys important for protecting our personal data, such as bank statements, health records, and digital identity. Its security relies upon encoding each bit of the digital key upon a single photon (particle of light). If a hacker intercepts the single photons, they will unavoidably disturb their encoding in a way that can be detected. This allows eavesdropping on the network to be directly monitored.

International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459 (Online), An ISO 9001:2008 Certified Journal,Volume 3, Special Issue 2, January 2013)
National conference on Machine Intelligence Research and Advancement (NCMIRA, 12), INDIA.

To perform quantum computations, one should have the following basic conditions:

(i) a two-level system (|0> and |1>) as a qubit
(ii) the ability to prepare the qubit in a given state, say |0>
(iii) the capability of measuring each qubit,
(iv) construction of basic gate operations such as conditional logic gate (the control-not gate)
(v) sufficient long DE coherence time. It is very important for a QC to be well isolated from any environmental interaction because they destroy the superposition of states. Furthermore, one has to use quantum error corrections, which have been invented in recent years.

Quantum key distribution

To understand QKD we must first move away from the traditional key distribution, we should have in mind a more symmetrical starting point, in which Alice and Bob initially generate their own, independent random number sets, containing more numbers than they need for key material that will ultimately share. Next, they compare these sets of numbers to get a shared subset, which will become the key material. Alice prepares a sequence of tokens, one kind of a "0" and a different kind for a "1", and sends a token to Bob for each bit in her set. Bob proceeds through his set bit-by-bit in synchronization with Alice, and compares Alice token with his bit, and replies to Alice telling her whether the token is the same as his number (but not the value of his bit). With Bob information Alice and Bob can identify the bits they have in common. They keep these bits, forming the key, and discard the others. If one of Alice tokens fails to reach Bob this does not spoil the procedure, because it is only tokens that arrive which are used in the process.

The obvious problem with this procedure is that if the tokens are classical objects they carry the bit values before they are observed by Bob, and so they could be passively monitored by Eve (an eavesdropper). However, we shall now see that it is possible to generate a secure key if the tokens are quantum objects.

III. FINGERPRINT

Since now-a-days security key is also the most challenging issue for computer industry. Thus fingerprint is one of the best options for this. It is thoroughly verified and user friendly also. Friction ridge of the fingerprint Fingerprint authentication is possibly the most sophisticated method of all biometric technologies Fingerprint authentication has particularly proved its high efficiency. Even features such as a person's gait, face may change with passage of time and may be fabricated or imitated. However, a fingerprint is completely unique to an individual and stayed unchanged for lifetime. This exclusivity demonstrates that fingerprint authentication is far more accurate and efficient than any other methods of authentication. Also, a fingerprint may be taken and digitalized by relatively compact and cheaper devices and takes only a small capacity to store a large database of information.

Fingerprint identification process is the process of comparing of two friction ridge from human finger. The analysis of fingerprints for matching purposes generally requires the comparison of several features of the print pattern. These include patterns, which are aggregate characteristics of ridges, and minutia points, which are unique features found within the patterns. It is also necessary to know the structure and properties of human skin in order to successfully employ some of the imaging technologies. The three basic patterns of fingerprint ridges are the arch, loop, and whorl. Arch: refers that type of ridges which enter from one side of the finger, rise in the center forming an arc, and then exit the other side of the finger. Loop denotes the ridges which enter from one side of a finger, form a curve, and then exit on that same side. Whorl represents that Ridges which form circularly around a central point on the finger. In general, a fingerprint examiner relies on details of ridge structures of the fingerprint in order to make fingerprint identifications. And the structural features are composed of the points where ridges end or bifurcate, that are called minutiae. The major Minutia features of fingerprint ridges are: ridge ending, bifurcation, and short ridge (or dot).

International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459 (Online), An ISO 9001:2008 Certified Journal,Volume 3, Special Issue 2, January 2013)
National conference on Machine Intelligence Research and Advancement (NCMIRA, 12), INDIA.

The Arch Patern of ridge of fingerprint

IV. PROPOSED METHOD

The Ekert scheme uses entangled pairs of photons. These can be created by Alice, by Bob, or by some source separate from both of them, including eavesdropper Eve. The photons are distributed so that Alice and Bob each end up with one photon from each pair. The scheme relies on two properties of entanglement. First, the entangled states are perfectly correlated in the sense that if Alice and Bob both measure whether their particles have vertical or horizontal polarizations, they always get the same answer with 100% probability. The same is true if they both measure any other pair of complementary (orthogonal) polarizations. However, the particular results are completely random; it is impossible for Alice to predict if she (and thus Bob) will get vertical polarization or horizontal polarization. Second, any attempt at eavesdropping by Eve destroys these correlations in a way that Alice and Bob can detect. The original Ekert protocol consist of using three possible states and testing Bell inequality violation for detecting eavesdropping.

V. MERITS OF PROPOSED APPROACH

The **Quantum key distribution** gives guarantee to secure communication.

It enables two parties to produce a shared key known only to them, which can then be used to encrypt and decrypt messages. An important and unique property this approach is the ability of the two communicating users to detect the presence of any third party trying to gain knowledge of the key. The security of this approach relies on the foundations of quantum mechanics, in contrast to traditional approach which relies on the computational difficulty of certain mathematical function, and cannot provide any indication of eavesdropping or guarantee of key security.

Proposed method is secure from any classical attack. It also detect if someone is listening. This system secure from any quantum attack and also much efficient. Since here fingerprint is used thus it creates more secure network also.

VI. CONCLUSION

This paper provides the most secure way for communication. Biometric uses in quantum, computer makes computation and communication cost is most cheaper and user friendly. Thus it can provides new way of data security also. It can also area of research to secure network

REFERENCES

[1] Ardehali, M., H. F. Chau, and H.-K. Lo, 1998, ‘‘Efficient quantum key distribution,’’ preprint quant-ph/9803007.

[2] Aspect, A., J. Dalibard, and G. Roger, 1982, ‘Experimental test of Bell’s inequalities using time-varying analyzers,’’ Phys.Rev. Lett. **49**, 1804–1807.

[3] Bechmann-Pasquinucci, H., and N. Gisin, 1999, ‘‘Incoherent and coherent eavesdropping in the 6-state protocol of quantum cryptography,’’ Phys. Rev. A **59**, 4238–4248.

[4] Bechmann-Pasquinucci, H., and A. Peres, 2000, ‘‘Quantum cryptography with 3-state systems,’’ Phys. Rev. Lett. **85**,3313–3316.

[5] Bechmann-Pasquinucci, H., and W. Tittel, 2000, ‘‘Quantum cryptography using larger alphabets,’’ Phys. Rev. A **61**, 062308.

[6] Bell, J. S., 1964, ‘‘On the problem of hidden variables in quantum mechanics,’’ Rev. Mod. Phys. **38**, 447–452 [reprinted in Bell, J. S., 1987, Speakable and Unspeakable in Quantum Mechanics (Cambridge University, Cambridge, England)].

[7] Bennett, C. H., 1992, ‘‘Quantum cryptography using any two nonorthogonal states,’’ Phys. Rev. Lett. **68**, 3121–3124.

[8] Bennett, C. H., F. Bessette, G. Brassard, L. Salvail, and J. Smolin, 1992, ‘‘Experimental quantum cryptography,’’ J. Cryptology **5**, 3–28.

[9] Bennett, C. H., and G. Brassard, 1984, in Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India, (IEEE, New York), pp.175–179. 190 Gisin et al.: Quantum cryptography

[10] Shor, P.W. Algorithms for Quantum Computation: Discrete Log and Factoring. Proceedings of the 35th Annual Symposium on Foundations of Computer Science. IEEE press. pp. 124-134 (1994)

[11] http://www.cs.bris.ac.uk/Tools/Reports/Keywords/Quantum_Information_Theory.html

[12] http://www.iop.org/EJ/journal/QSO/7

[13] http://www.idquantique.com/qkd.html