Authentication using Secure Node Signature Verification Algorithm with Quantum Cryptography

Darnasi Veeraiah
Assistant Professor
Department of Computer Science
Vignan University, Guntur

R.Upendar Rao
Assistant Professor
Department of Computer Science
Vignan University

K V Ranga Rao
Assistant Professor
Department of Computer Science
VignanUniversity

ABSTRACT
In now a days, most of the communication takes place through Internet. Most of the users are used to transmit their information through insecure channels that are interconnected throughout world. Thus, security must be provided to achieve confidentiality, access control, integrity and authentication. To ensure all these services, various cryptography and steganography techniques like RSA, AES, MD5 and RC5 have been used. Even though, cryptanalysts reinforcing it using some mathematical computation and misused information. Currently, quantum computers have been used to increase the speed of computation and to provide more security for data. It exploits quantum mechanics to provide secure communication. Quantum cryptography (QC) technique has been used to share the key among the participants who wish to share the data. This paper discusses various cryptographic key distribution protocols and quantum mechanics. In this paper we proposed "Secure Node Signature Verification Algorithm"(SNSVA) based on Quantum cryptography technique that describes how authentication can be verified with network nodes. In addition, it explains an approach to improve the performance of cryptography technique.

General Terms
Sharing, Intrude, Securing, Sender, Receiver, Transceiver, information.

Keywords
Quantum Cryptography, Security, Authentication, Entanglement, BB84 protocol.

1. INTRODUCTION
Cryptography allows the user to share their secret information all over the world through insecure network in secure manner. It secures web sites and electronic transfer and provides various services like authentication, access control, confidentiality, integrity and non-repudiation. Many algorithms have been evolved to protect the user data from intruders. It uses two forms of encryption/decryption techniques: symmetric cryptography and asymmetric cryptography.

Symmetric cryptography also called as private key cryptography. It uses a single key for encryption and decryption. But it is vulnerable to plain text attack and linear cryptanalysis. So intruder can easily decode the information. Sharing the secret key through insecure channel and maintenance of keys are major drawbacks of symmetric cryptography. Some of the algorithms are DES, AES, 3DES, IDEA, RC5, Blowfish, etc. To overcome disadvantages of private key cryptography, asymmetric cryptography was evolved and used. It is also termed as public key cryptography. It uses different keys for encryption and decryption. The user maintains only two keys: public and private key unlike in symmetric cryptography. The sender uses receiver's public key for encryption and receiver decrypt the information with their private key. Private keys should not be derived from public key. It is widely used all over the world. Public key cryptography applied in public key encryption and digital signature. Algorithms like RSA, ECC and DSS are used to implement public key cryptography. Many techniques have been used to distribute the public keys. Private and public keys used in asymmetric cryptography are mathematically related. In both of the methods, sender or receiver should select key which is larger in size to provide more security to the information.

In addition, Diffie-Hellman algorithm, hash functions like MD5, SHA algorithm have been used in public cryptography. Diffie-Hellman algorithm is used to exchange the secret key between the users for secure communication using the concept of public key cryptography.

The development of computer system starts from resistor and transistor to IC (Integrated chip). Today advance techniques are applied to create chips of size fraction of micron wide [13]. Now research is going on to exploit even smaller parts than IC i.e. atoms. Atomic scale matter obeys the rules of quantum computers, which are different from classical rules. If computer become smaller in future, quantum technology replaces all. They have the potential to perform certain calculations significantly faster than any silicon-based computer. Cryptography techniques are used in quantum computer to achieve secure communication. Mainly it is used to exchange the secret between the users like Diffie-Hellman algorithm.

This paper describes how authentication can be achieved in quantum cryptography and it explains an approach to improve the performance of cryptography technique. This paper is organized as follows: Next section provides details about quantum cryptography. Section 3 describes the protocols used in quantum cryptography. Section 4 compares classical key exchange algorithm with quantum cryptography. Section 5 explains how authentication can be achieved with quantum cryptography. Section 6 describes how the user can be mutually authenticated. Section 7 concludes the paper.

2. QUANTUM CRYPTOGRAPHY
The fundamental nature of quantum theory is the realization of elementary particles such as electrons, protons, neutrons, etc. Quantum cryptography uses quantum communication and quantum computation to perform cryptographic tasks. It is used to share the secret key between communication parties.

Quantum Key Distribution (QKD) is widely used in quantum cryptography. It is only used to produce and distribute a key, not to transmit any message or data. This key can then be used with any chosen encryption algorithm to encrypt and decrypt a message, which can then be transmitted over a standard communication channel as figure.1. The algorithm most commonly associated with QKD is the one-time pad, as it is provably secure when used with a secret, random key.

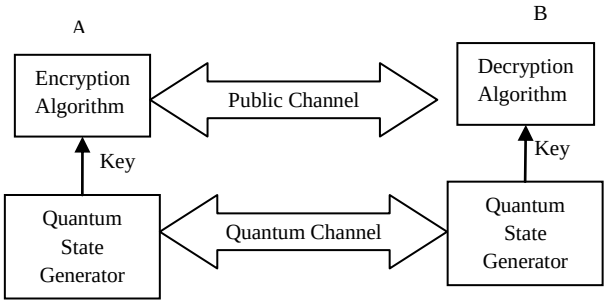


Fig.1. Quantum key Distribution

Computer system uses two states either 0 or 1. But quantum computer uses qubits called quantum bits. They are implemented using quantum mechanical state systems in which values are not confined to two basic states but also exists in superposition: means that qubit is both in state 0 or state 1. Quantum cryptographic devices typically employ individual photons of light and take advantage of either Heisenberg Uncertainty principle or Quantum Entanglement. It provides means for two parties to exchange key over a private channel with complete security of communication.

Unlike in classical physics, the act of measurement is an integral part of quantum mechanics. So it is possible to encode information into quantum properties of a photon in such a way that any effort to monitor them disturbs them in some detectable way. The effect arises because in quantum theory, certain pairs of physical properties are complementary in the sense that measuring one property necessarily disturbs the other. This statement is known as the Heisenberg uncertainty principle [1]. The two complementary properties that are often used in quantum cryptography, are two types of photon's polarization, e.g. rectilinear (vertical and horizontal) and diagonal (at 45° and 135°).

Entanglement [1,2] is a state of two or more quantum particles, e.g. photons, in which many of their physical properties are strongly correlated. The entangled particles cannot be described by specifying the states of individual particles and they may together share information in a form which cannot be accessed in any experiment performed on either of the particles alone. This happens no matter how far apart the particles may be at the time.

In quantum cryptosystem, transmitter and receiver have been used to pass the photons. Sender sends photons in one of four polarizations: 0, 45, 90, or 135 degrees to the receiver. A recipient at the other end uses the receiver to measure the polarization. According to the laws of quantum mechanics, the receiver can distinguish between rectilinear polarizations (0 and 90), or it can quickly be reconfigured to discriminate between diagonal polarizations (45 and 135). In key distribution, sender sends photons with one of the four polarizations which are chosen at random. For each incoming photon, the receiver chooses the type of measurement randomly either in rectilinear or diagonal. The receiver records the results of the measurements but keeps them secret. Subsequently, the receiver publicly announces the type of measurement (but not the results) and the sender tells the receiver which measurements were of the correct type. Sender and receiver keep all cases in which the receiver measurements were of the correct type. These cases are then translated into bits (1's and 0's) and become the key.

Quantum hackers have performed the first 'invisible' attack using lasers on the systems, which uses quantum states of light to encrypt information for transmission. Quantum cryptography is often touted as being perfectly secure. It is based on the principle that the user cannot make measurements of a quantum system without disturbing it. So, in theory, it is impossible for an eavesdropper to intercept a quantum encryption key without disrupting it in a noticeable way, triggering alarm bells. Eavesdropper will get only 50% of chance to detect the key. Sender or receiver detects any intruder, it initialize the key exchange process again.

This section provides fundamental idea about quantum cryptography. Quantum cryptography has been implemented to cover nearly 50 km in case of wired network and nearly 2-3 km in case of wireless network. In future, it may be extended. Next section deals with protocols used in quantum cryptography.

3. QUANTUM CRYPTOGRAPHY PROTOCOLS

Quantum cryptographic protocols are required to communicate two parties to share entangled particles. The correlation between particles provide shared secret key. It is used to perform some tasks without any involvement of any people and any privilege information. The first quantum cryptography was introduced by Bennett and Brassard in 1984 named as BB84. Other protocols like E91, COW, DPS, S09 and SARG04 have been used in quantum cryptography.

BB84 protocol [1, 2] uses rectilinear and circular polarization bases for photons. The sender randomly sends polarizations to the receiver. Receiver receives and measures it with their random sequence basis. Some sequence may not be correctly. The receiver sends their random measurement to the sender. Sender verifies it and sends the correct sequence to the receiver. The sequence can be converted into binary digits based on the values of polarization.

E91 protocol was introduced by Artur Erket in 1991 [12]. It uses entangled pairs of photons. It is based on three properties of entanglement: entangled states which are perfectly correlated, quantum non-locality and weaken correlations if eavesdropper attacks.

Coherent One-Way protocol (COW) [5] was initiated by Nicolas in 2004. It has been modified with an implementation with weak coherent pulses. In this method, the key has been obtained by simple time-of-arrival measurement on the data line and also an interferometer is built on an additional monitoring line to monitor the attack.

The differential-phase shift (DPS) protocol [6] is a quantum cryptography scheme proposed by Woks and Yamamoto in 2002. This protocol is suitable for fiber transmission systems and offers key creation efficiency higher than conventional fiber-based BB84.

The SARG04 [7] protocol was proposed by Scarani in 2004. The protocol would be more robust when attenuated laser pulses are used instead of single-photon sources. It is used

where the information is originated by a Poissonian source producing weak pulses and received by an imperfect detector.

S09 protocol [8] was developed by Serna in 2009. It uses two quantum channels. It combines both public key cryptography and private key cryptography. But it does not make reconciliation mechanisms of information to derive the key.

The implementation of these protocols is very difficult because qubits can be exchanged multiple times. Next section describes the comparison of quantum key exchange technique with classical algorithms.

4. KEY EXCHANGE

Many algorithms have been proposed and used for exchanging secret key between communication parties. Some of the algorithms are Diffie-Hellman algorithm, STS protocol, Shamir's Three Pass Protocol, COMSET, etc.

The Diffie–Hellman key exchange method allows two parties that have no prior knowledge of each other to jointly establish a shared secret key over insecure communication channel. The shared key can be used to encrypt subsequent communications using a symmetric key cryptography technique. It is implemented with the use of prime numbers.

Station-to-station (STS) protocol [9] is implemented based on classical Diffie–Hellman key exchange algorithm. It provides mutual key exchange and authentication. It uses no timestamps and provides perfect forward secrecy. In addition, it provides two-way explicit key confirmation with the uses of AKC (Authenticated key agreement with key conformation) protocol.

Shamir Three-Pass Protocol [14] was developed in 1980. It is also called as Shamir No-Key Protocol because the sender and the receiver do not exchange any keys. It requires the sender and receiver should have two private keys for encrypting and decrypting messages. It uses exponentiation modulo a large prime as both the encryption and decryption functions.

COMSET (COMmunication SETup) protocol allows any users to identify themselves to each other and also exchange a secret key. It uses a public key technique that is equivalent to factoring a large integer.

Encrypted Key Exchange (EKE) [10] is a combination of symmetric and asymmetric cryptography that allows two parties share a common key by plaintext equivalent mechanisms. In all the cases, intruder can decode the information.

However, quantum cryptography generates a new private key continuously and randomly between parties. A compromised key in quantum key distribution systems can only decrypt a small amount of encoded information because the private key may be changed every second or even continuously.

Each photon is encoded with a bit value of 0 or 1, in which a photon is in some superposition state, such as polarization. The stream of photons forms a secret key. The photons are generated by laser beams as pulses of light. Some pulses contain more than one photon. Losses occur when photon passes through fiber optic cable. However, this loss does not lead to any problem because only photons that reach the receiver are used. The key is generally encoded in either the polarization or the relative phase of the photon. Data carrying photons may be transmitted by laser and detected in such a way that any intervention will be distinguished.

Quantum Key distribution has more advantages over classical key exchange algorithms. But initially it is very costly to implement. Once secure quantum channel has been established, communication will be more secure over long distance also. Next section describes how authentication can be performed in quantum cryptography.

5. AUTHENTICATION

Securing message authentication is very important in quantum cryptography. Quantum cryptographic device provides authentication services over the optical (quantum) channel and the public channel. Classical cryptographic technique uses symmetric cryptographic technique (secret key sharing) and digital signature concept for authentication.

The user wants to communicate with other user through quantum channel, conventional cryptographic techniques are unusable. In particular, an authentication protocol for quantum states must protect superposition of states. To protect quantum states from a would-be forger, we need a quantum authentication scheme. Quantum authentication protocol is to encode the quantum state in a quantum error-correcting code. The receiver can detect any tampering happens during exchange.

Quantum authentication schemes are used to pass reliable quantum information through an insecure channel. In addition, it provides both encryption and authentication of quantum information. Eavesdropper is unable to copy the message during transmission. It also provides unrepeatable encryption.

Wegman-Carter authentication (WCA) [11] is the standard unconditionally secure MAC used in quantum cryptography. It is based on universal hashing techniques. It is secure even intruder knows partially known key. It is equivalent of the Vernam cipher. In the Vernam cipher, the required key needs to be at least as long as the message to be encrypted. Fortunately, in Wegman-Carter authentication, the required key grows only logarithmically with the message length. It requires more rounds to gain more key. Formally, the fundamental building block of Wegman-Carter authentication is called universal families of hash functions. In WCA, hash functions map a message in the set of possible messages to a tag in the set of tags.

Next section describes how authentication can be mutually achieved in quantum cryptography.

6. PROPOSED METHOD

Authentication is a very important issue in security. To ensure the integrity and safety of the information, it is important to identify with whom the users are dealing and the data which is received by the users should be consistent. Authentication can help to establish trust between parties involved in communication.

To achieve authentication, various techniques have been employed in classical cryptography. Quantum cryptography also employs universal hashing technique to provide authentication. In many circumstances, there is a necessity of mutual exclusion. Before exchanging the keys between two parties, it should authenticate each other. In our approach, both private and public key cryptography techniques have been used. Public key cryptography has been used for authentication and private key cryptography techniques for exchanging the message securely. In order to send the information in confidential manner with minimum cost we proposed "Secure Node Signature Verification Algorithm" named as SNSVA.

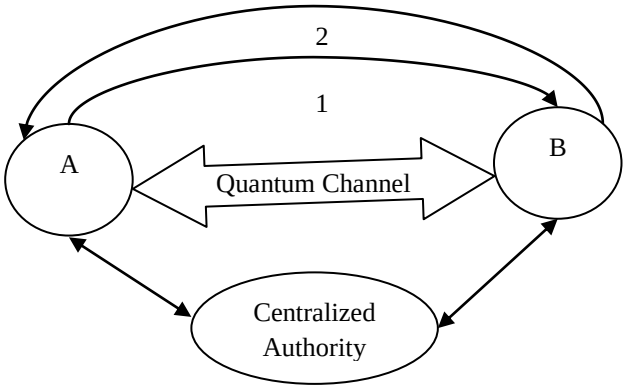
The following steps have to be followed to achieve authentication:

1. If A wants to communicate with B, it sends the request message and its signature which is encrypted using with its quantum basis for verification to B through classical channel.
2. B receives its request. If it is interested for communication, it processes the requests.
3. B verifies the signature, which can be decrypted using public key cryptography, with centralized authority. (Assume Centralized authority is a trusted one)
4. It maintains A's random basis for further communication.
5. B sends the reply message containing its digital signature to A denoting acceptance of communication.
6. A verifies it and send the quantum basis as nibble through quantum channel.
7. B verifies the quantum basis with stored basis. If it matches, it is ready to share the secret key. Send same quantum basis to A. A verifies it and ready to transfer the secret key.

[Follows general quantum cryptography Technique [1]]

1. A generate the random qubits through quantum generator and sends it to B through Quantum channel.
2. B receives qubits using its random measurement. Inform its random measurement to A.
3. A verifies it with its random measurement and sends the correct measurement to B.
4. Finally measurements are converted into random binary digits and assumed to be secret Key.
5. Secret key have been used to encrypt and decrypt the data.

In modern world, communication takes place tremendously using computers. Security is very significant to provide confidentiality, integrity and authentication. Many algorithms have been proposed and used in classical techniques. In our approach, public key cryptography technique is combined with private key cryptography. We believe that it provides more security.



1. Signature + E (Random basis of 4 bits)
2. Signature

Fig.2. Authentication procedure.

7. CONCLUSION

Now a days, all users preferring portable devices like mobile, PDA, Laptop, etc for their communication. Recently, quantum technologies have been used for faster communication. In wired communication, user replaces twisted pair cable to fiber optic cable. However, Wireless communication took part a main role in portable devices. Quantum technology uses fiber optic cable (also supports wireless communication, but for limited distance) for its communication. This paper described about how quantum cryptography works and various protocols used in QC. This paper also compared different key exchange algorithm with quantum cryptography key distribution. It also dealt with how authentication can be achieved in quantum cryptography. Finally, this paper depicted the authentication process with the support of digital signature and qubits.

REFERENCES

[1] Bennett and Brassard, G.,"Quantum cryptography: public key distribution and coin tossing", *IEEE Conference on Computer, Systems, and Signal Processing*, 1984, pp. 175-90.

[2] Bennett, C. H., "Quantum cryptography using any two non-orthogonal states". *Physics Review Letter*1992.

[3] Bennett, C. H., Bessette, F., Brassard, G., Salvail, L., & Smolin, J.,"Experimental quantum cryptography", *Journal of Cryptology*, 1992.

[4] Elliot, C., "Quantum Cryptography", *IEEE Security & Privacy Journal*, 2004.

[5] B. Hutter, N. Imoto, N. Gisin, T. Mor, *Quantum cryptography with coherent states, Physical Review pp.* 1863–1869, 1995.

[6] Inoue K, Woks E and Yamamoto Y 2002, "*Differential phase shift quantum key distribution*", *Phys. Rev. Lett*. 89 037902.

[7] Chi-Hang Fred Fung, Kiyoshi Tamaki, Hoi-Kwong Lo, "*On the performance of two protocols: SARG04 and BB84*", *Phys. Rev*. A 73, 012337 (2006).

[8] Eduin H. Serna,"*Quantum Key Distribution Protocol withPrivate-Public Key*", *Quantum Physics*, 2009.

[9] Higgins, Diffie, Strawczynski and Hoog, "*Encryption and ISDN - A Natural Fit*", *International Switching Symposium (ISS87)*, 1987.

[10] Bellovin and Merritt, "Encrypted Key Exchange: Password Based Protocols Secure against Dictionary Attacks and Password file Compromise", Proceedings of 1st ACM Conference on Computer and Communication Security, ACM Press, pp.244-250, 1993.

[11] Wegman and Carter,"*New Hash Functions and Their Use in Authentication and Set Equality*', J. Comput. Syst. Sci., Vol. 22, pp. 265-279, 1981.

[12] http://www.quantiki.org

[13] http://cam.qubit.org

[14] http://www.afn.org