ISSN 2250-3153

Research Directions in Quantum Cryptography and Quantum Key Distribution

Ms. Deepa Harihar Kulkarni

Assistant Professor, SKN College of Engineering
University of Pune, Maharshtra, India
deepakulkarniskn@gmail.com

Abstract- Quantum cryptography is an approach to securing communications by applying the phenomena of quantum physics. Quantum cryptography provides secure communication whose security depends only on the validity of quantum theory. Interesting characteristics of quantum mechanics includes the existence of indivisible quanta and of entangled systems, both of which lie at the root of the quantum cryptography (QC). QC is one of the few commercial applications of quantum physics at the single quantum level. Computers and Telecommunications system would become safe havens for criminal activity. Even may himself unknowns that crypto anarchy provides a means for tax evasion money laundering, espionage (with digital dead drops), contract killings, and implementation of data havens for Monitoring and marketing illegal or controversial material. Encryption also threatens national Security by interfering with foreign intelligence operations.

Index Terms- Quantum Cryptography, Quantum level

I. Classical Cryptography

To achieve cryptography an algorithm also called (cryptosystem or cipher) is used to combine a message with some additional information (known as the key) and produce a cryptogram. The primary application of cryptography is to send secret messages. Many cryptographic systems are based on computational assumptions. Decrypting is equivalent to solving some computationally difficult problem. Based on mathematics is the classical cryptography and one based on physics quantum cryptography. Classical cryptography relies on the computational difficulty of factoring large integers; quantum cryptography relies on what we believe to be the universal laws of at quantum mechanics.

These classical cryptosystems come in two flavors: Symmetric systems and asymmetric systems. The security of public key cryptosystem is based on competition complexity.

II. Symmetrical (Secret Key) Cryptosystems

Symmetrical ciphers require the use of a single key, both for encryption and decryption. The symmetrical cryptosystems in use for routine applications such as e-commerce employ rather short keys.

Asymmetrical allegorizing is used not so much for encryption, because of their slowness, but rather for distribution of session keys for symmetric cryptosystems such as DES. Barriers of classical cryptography

2.1 Secret key cryptography

- Require secure channel for key distribution.
- In practice principle every classical channel can be monitored passively.
- Security is mostly based on complicated, non proven algorithms.

2.2 Public key cryptography

- Security is based on non proven mathematical assumptions (ex. in RSA cipher, difficulty of factoring large numbers.

III. Quantum Cryptography

The main advantage of quantum cryptography is that it gives us perfectly secure data transfer the first successful quantum cryptographic device could translate a secret key over 30 centimeters using polarized light, calcite crystals(s), and other elect optical devices.

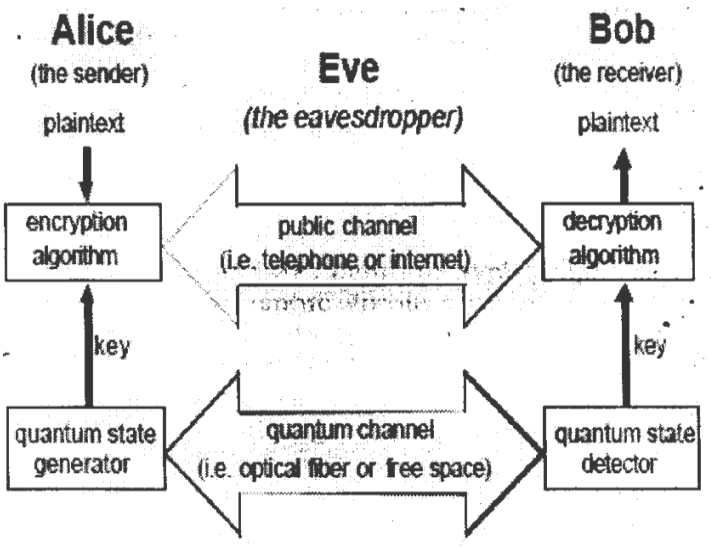

Figure 3.1: A Quantum Cryptographic Communication System for Securely Transferring Random Key

IV. QUANTUM ENTANGLEMENT

Entanglement is a kind of quantum correlation that is stronger, in certain sense, than any classical one. If some quantum system, consisting of several subsystems, then it is in entangled state (even in a pure entangled state) its individual subsystems cannot be described by pure quantum stages. Entangled states can be used to serve for quantum key distribution and quantum teleportation.

Quantum entanglement is a quantum mechanical phenomenon in which the quantum of two or more objects has to be described with reference to each other, even though the individual objects may be spatially separated. This leads to correlations between observable physical properties of the systems. As the results, measurements performed on one system seen to be instantaneously influencing. Other systems entangled cipher.

V. QUANTUM KEY DISTRIBUTION

Quantum mechanics has multiple cryptographic applications as well. The best known is quantum key distribution (QKD) which enables Alice and Bob to create a secure classical secret key despite the potential presence of an eavesdropper. QKD requires only an insecure quantum channel and authenticated classical channels, but unfortunately requires multiple rounds of back and forth communication between Alice and Bob.

QKD is a means of distributing keys from one party to another, and detecting eavesdropping. It always two parties to establish a common random secret key by taking advantage of the fact that quantum mechanics does not allow for distinguishing non-orthogonal states with certainty.

The primary proposed application of QKD is to create a secret key, which is then used with the one-time pad to send unconditionally secure messages.

One of the best-known protocols for quantum key distribution is usually called BB84. (In 1984, by Bennett and Brassard) In BB84, Alice sends Bob a random sequence of quantum bits (on cubits). These quantum bits are equally likely to be in one of four possible states, as follows

State	Basis		value
0	0>		Z
1	1>		Z
0	0>+	1>	X
1	0>-	1>	X

VI. INTEGRATION OF QUANTUM CRYPTOGRAPHY IN 802.11 NETWORKS

Quantum cryptography is considered as a promising solution towards absolute security in long term cryptosystems. The application of quantum cryptography in fiber networks has significant advances.

The appealing characteristics of quantum cryptography is the possibility of distributing secret key between two users in a manner that it is impossible for a third party to eavesdrop without disturbing the quantum transmission and hence the eavesdropping is detected by legitimate users. With this characteristic, quantum cryptography is considered as a promising key distribution solution towards long-term unconditionally secure cryptosystems.

In fiber networks, some products have been commercialized to provide a turnkey service for widely used encryption algorithms. While the application of quantum cryptography in fiber networks has significant advances, the application of quantum cryptography in fiber networks has significant advances; the application of quantum cryptography in mobile networks is still premature. Some advanced topics in this field concern satellite communications. In satellite networks, the ground stations and the satellites are main communication entities of the quantum key distribution process.

There are a large verity of kinds of mobile wireless network such as GSM (Global System for Mobile communications), GPRS (General Packet Radio Service, WLAN (Wireless Local Area Network) has its own characteristics concerning the mobility level of the users, the environment where it could be deployed, the size of the coverage area *etc*. our first tentative is towards WLAN 802.11 networks because of the four following reasons. First, WLAN 802.11 is mainly used in office and campus environments (*e.g.* offices, class rooms, meeting rooms, halls in airports). This building oriented environment facilitates the deployment of a quantum key distribution network with a high density of quantum apparatus if necessary.

Second, the mobility speed of mobile users in WLAN 802.11 is relatively slower in comparison with cellular networks. Third WLAN 802.11 terminals (*e.g.* laptop) usually have more computational capacity and more energy for the autonomy than cellular network's terminals (*e.g.* cell phones). This characteristic may allow a sufficient amount of control and protocol related tasks in the quantum key distribution process.

Fourth, from on application point of view, WLAN 802.11 is usually used to provide access to the internet through an access point installed by an organization or by a wireless ISP (Internet Service Provider). In comparison with another kind of network such as Bluetooth which is mainly used only to replace the wired links between personal devices (*e.g.* mouse, PDA, desktop), the WLAN 802.11 in an apt environment for an enhancement of security provided by quantum cryptography.

We are interested in the aspect of network protocol design for the integration of quantum key distribution in currently specified 802.11 security mechanisms.

In 802.11 we distinguish three aspects: Authentication, encryption key establishment and encryption algorithm.802.11 Security Mechanisms.

6.1 Authentication:

Authentication is the first thing to do when a mobile terminal wants to join a network. In order to rectify the flaw at the WEP (Wired Equivalent Privacy) based authentication mechanism specified in the 802.11 standard, 802.11 defines the 802.1x authentication based on EAP(Extensible authentication protocol) The architecture of 802.ix authentication with three elements: The supplicant, the authenticator, and the authentication server. The supplicant corresponds to the mobile terminal which wants

to join a network. The authenticator corresponds to the access point which relies the 802.1x access control and only admits data traffic from supplicants who are authenticated by the authentication server.

6.2 Key management: - 802.11i uses many keys at different levels, constituting a key hierarchy.

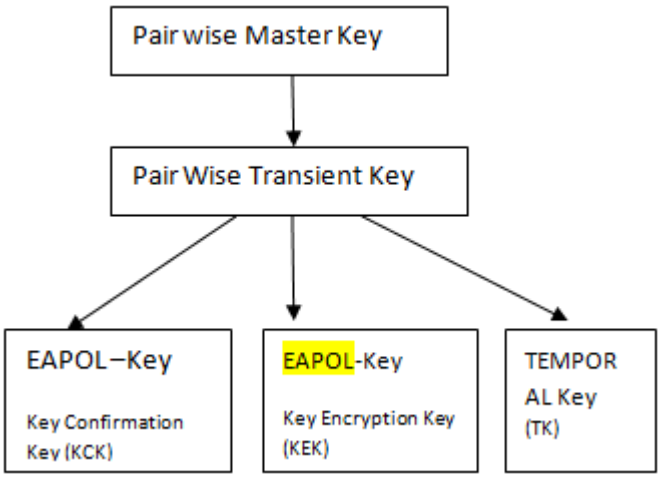

Figure 6.2: Pair Wise Key Hierarchy

Figure depicts this key hierarchy. At the top level, we have the master key called pair wise master key (PMK) which is used to derive the other keys. Upon having the PMK, the access point start the 4 way handshake with the mobile terminal to derive the PTK. This PTK is then split into three final temperate keys: EAPOL- Key key confirmation key (KCK), EAPAL – Key key Encryption key (KEK), and Temporal key (TK). The KCK is used to calculate the MIC (Message Integrity Code) at the EAPOL – Key message during the 4- way handshake. The TK is used to encrypt unicast user data traffic.

6.3 Encryption Algorithms: The 802.11i standard specifies into encryption algorithms: TKIP (Temporal Kay Integrity Protocol) and CCMP (Counter Mode with CBC – MAC Protocol). CCMP is mandatory and TKIP is optional. TKIP is considered as transient solution towards CCMP – based system because TKIP is based on the RC4 algorithm and only requires a software upgrade on WEP – based systems. CCMP is based on AES (Advanced Encryption Standard) and requires hardware modification for the translation from WEP – based systems.

VII. CONCLUSION AND FUTURE WORK

Other applications of quantum mechanics to cryptography and future scope which tend to come in three flavors:

- Quantum mechanics can be used to break classical cryptographic protocols.
- Quantum states can make possible new or improved cryptographic protocols protecting classical information.
- Cryptographic methods can be applied to protect quantum information instead of classical information. Examples would include quantum secret sharing schemes and quantum authentication protocols.

REFERENCES

[1] William Stalling, "Cryptography and Network Security (Principles and Practices)", Fourth Edition, Pearson Publishers, pp. 259-281,

[2] Othman O. Khalifa, "Communication Cryptography", IEEE transaction on Cryptography, 2004, pp. 1-15.

[3] National Bureau of Standard, Security Requirement for Cryptographic modules, Federal Information processing standards publication FIPs Publication, 1994, p.188 – 199.

[4] J. Watson, "Data Security Hits Home", IEEE micro, Oct. 1995, P 88

[5] IEEE Standard 802.1x, part based network access control, December 2004, pp. 47-53

[6] http://www.IEEEXPLORE.com

[7] SC51 User's Manual Edition 2.1

AUTHORS

Ms. Deepa Harihar Kulkarni is presently working as an Assistant Professor in Computer Department, SKN college of Engineering, Pune , Maharashtra, India. She has completed her graduate and post graduate from Maharashtra, India. Research areas are Data Mining, Pattern Recognition and Computer Networking.