New Comprehensive Study to Assess Comparatively the QKD, XKMS, KDM in the PKI encryption algorithms

Bilal Bahaa Zaidan
Department of computer science and information technology
University of Malaya
Kuala Lumpur, Malaysia

Aws Alaa Zaidan
Department of computer science and information technology
University of Malaya
Kuala Lumpur, Malaysia

Harith Mwafak
Faculty of Electronic Engineering
International Islamic University of Malaya
Kuala Lumpur, Malaysia

***Abstract*—protecting data is a very old art and wide use since the Egyptian when they identify the 1st encryption method in this world, the spiciest people categorize protecting data under computer forensic and others locate it under network security, cryptography methods are the backbone of this art, nowadays many of new techniques for the attacker's beings develops, a lot of methods for information protecting start dropping down such as RSA and stander encryption methods, in the same time a new methods has been appeared such as Quantum cryptography, the new methods has faced problems in the key distribution or key management and some time such as RSA there is a function may estimate the keys, In this paper we will make a comparative study between the key management distribution methods, in fact we will talk about QKD Encryption in the fiber optic area vice verse the KDM in the normal networks, for instant there are two known methods, KDM "Diffi- Hellman" and XKMS.**

Keywords- QKD, KDM, XKMS, PKI, Encription, Fiper Optics

I. INTRODUCTION

Cryptography is the name for the study of procedures, algorithms, and methods to encode and decode information.

Cryptanalysis is the study of methods and means to defeat or compromise encryption techniques. Cryptology is the study of both of cryptology and cryptanalysis combined, and is derived from the Greek kryptos logos, which translates into “hidden word.” Encryption usually requires the use of a hidden transformation that requires a secret key to encrypt, as well as to reverse the process or decrypt. In its originality Cryptography is the art of keeping information secret by transforming it into an unreadable/unusable format (encryption) by using special keys, then rendering the information readable again for trusted parties by using the same or other special keys. Modern cryptography however, does not confine itself to only maintaining the secrecy of information but goes beyond that by ensuring the identity of communicating parties (authentication), ensuring that information has not been tampered with (integrity), and preventing that any of the communicating parties denies having received or sent information (non-repudiation)[1][2]

Cryptography is a general word for many sub categories, as it shows below

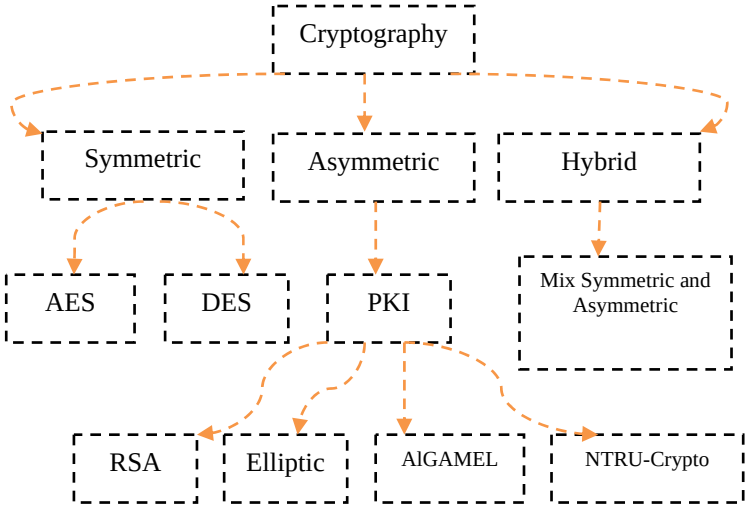

Figure 1 shows cryptography tree

For the Quantum Cryptography some researcher classify it as Public key and others said it is shearing secret key its mean it is symmetric, we will consider Quantum Cryptography as PKI, hence the mechanism depend on multi keys on its schema

The main construction in the public key infrastructure involve many component as it shown below

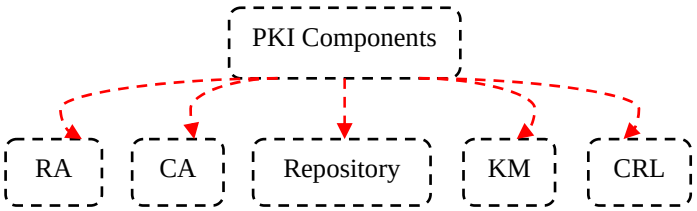

Figure 2 PKI Component

In this paper we will spotlight on the key management component, although there are other component related such as the trusted authority, working gathering for insure the right key has been used with the authorize person

ISSN : 0975-3397

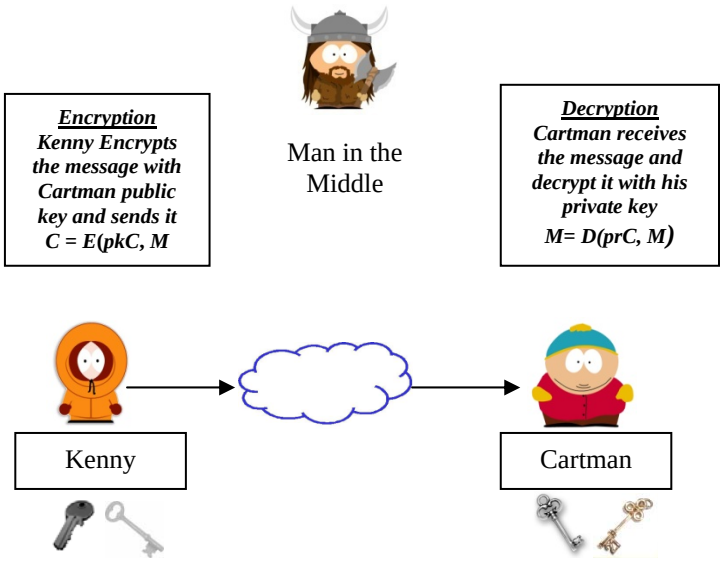

Figure 3 send and receive massages through the two ends, its shows how Kenny encrypt the massage and send it to Cartman , the figure above shows also the man in the middle waiting to have any information may help to decrypts the massages

II. KEY MANAGEMENT

One of the drawbacks with symmetric encryption is key distribution and management.

For each pair of encrypting devices, a separate key should be used.

If a given device has many encryption partners, distribution of the keys becomes logistically inconvenient. For each pair of devices, a key must be generated then transported via some secure means to each device. Even if one device generates the key, the problem remains of delivering or communicating the key to the companion device via special courier or other secure transport method. When large numbers of devices are involved, this burden becomes unwieldy very quickly. Consider the case where it might be desirable to encrypt email to multiple parties or casual parties on a one-time basis, but key distribution must be performed first.

The Kerberos protocol partially solves this problem by using the concept of a key distribution center (KDC), but Kerberos is more appropriately used for a distributed computing environment that has a central management.

Kerberos is also notorious for the administrative effort required to manage and maintain the environment. A complete discussion of Kerberos is beyond the scope of this material, and will not be presented here.[2][1]

III. KEY DISTRIBUTION MANAGEMENT (KDM)

Public-key cryptography has been said to be the first truly revolutionary advance in encryption in literally thousands of years [5]. Public Key Cryptography was first described publicly by Stanford University professor Martin Hellman and graduate student Whitfield Diffie in 1976. In their paper "New Directions in Cryptography" they described a two-key crypto system in which two parties could securely communicate over a non-secure communications channel without having to share a secret key. Asymmetric cryptography was born to address the problem of secret key distribution by using two keys instead of a single key. In this process, one key is used for encryption, and the other key is used for decryption. It is called asymmetric because both the keys are required to complete the process. These two keys are collectively known as the key pair. One of the keys (The public key) is freely distributable and used for encryption. Hence, this method of encryption is also called public key encryption. The second key is the secret or private key, is not distributable and is used for decryption. This key, like its name suggests, is private for every communicating entity [2][1]. PKC depends upon the existence of so-called one-way functions, or mathematical functions that are easy to computer whereas their inverse function is relatively difficult to compute

IV. KDM PROTOCOLS

The earlier protocol has been provided with the 1st public key was Diffie- Hellman. The Diffie-Hellman protocol in their paper does not actually use the trapdoor property, only one-way. The public key for each Alice and Bob is created from the secret key using a function which cannot be easily undone. Alice creates a new random key, passes through the one-way function and publicly gives Bob the result. Bob does likewise. Now each Bob and Alice is in possession of their own secret key and the other's public key. Any bystander has knowledge of both public keys but of neither secret key, because the function is one-way. The type of one-way function proposed by Diffie-Hellman allows each Alice and Bob to combine what they know to generate a common secret. This secret is not known to any one else, since it requires knowledge of at least one of the private keys. This common secret is used as a key in any standard symmetric cipher for the ongoing, private, communication between Alice and Bob [5][1]

V. QUANTUM KEY DISTRIBUTION(QKD)

A point-to-point quantum key distribution (QKD) system takes advantage of the laws of quantum physics to establish secret keys between two communicating parties. QKD offers unconditional security, which makes it attractive for very high security applications. Nowadays the only garneted 100% secure system may locate at QKD systems, last researches at the moment talking about QKD in the free space or End to End wireless QKD, However, this unprecedented level of security is mitigated by the inherent constraints of quantum communications, such as the limited rates and ranges of an individual point-to-point QKD link. Although a QKD network, which can be built by combining

ISSN : 0975-3397

multiple point-to-point QKD devices, can alleviate the constraints and enable point-to-multi-point key distribution based on QKD technology [3]
In this part we will choice the most popular protocols for QKD; in particular we will describe the principle of BB84, BB92 as an example for the QKD recognized protocols

VI. QKD PROTOCOLS

In the vein of the other key distribution management QKD has many protocols, this protocols depend on the way which the protocol used to encode the data or the states of polarizations used on the protocol. In this part we will choice the most popular protocols used in QKD

VII. BB84 PROTOCOL

In BB84 a polarization of 0 degrees in the rectilinear bases or 45 degrees in the diagonal bases [CKI-BB84] [Gisin02] define a binary 0; similarly a binary 1 can be 90 degrees in the rectilinear bases or 135 in diagonal bases.

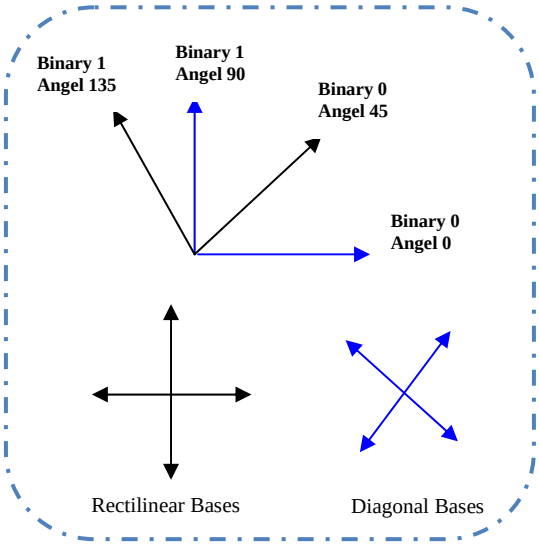

Figure 4 shows the bases for the encodes in BB84

In BB84 there is a mechanism for shearing the secure communications, in this phase we will describe how Alice and Bob doing the secure tunnel.

- First of all Alice will communicate to Bob over a quantum channel. Alice begins by choosing a random string of bits and for each bit; Alice will randomly choose a basis, rectilinear or diagonal, by which to encode the bit. She will transmit a photon for each bit with the corresponding polarization, as just described to Bob.
- For every photon Bob receives, he will measure the photon's polarization by a randomly chosen basis. If, for a particular photon, Bob chose the same basis as Alice, then in principle, Bob should measure the same polarization and thus he can correctly infer the bit that Alice intended to send.

If he chose the wrong basis, his result, and thus the bit he reads, will be random.

In the second phase, Bob will notify Alice over any insecure channel what basis he used to measure each photon. Alice will report back to Bob whether he chose the correct basis for each photon. At this point Alice and Bob will discard the bits corresponding to the photons which Bob measured with a different basis. Provided no errors occurred or no one manipulated the photons, Bob and Alice should now both have an identical string of bits which is called a sifted key.

VIII. BB92 PROTOCOL

In 1992, Charles Bennett proposed what is essentially a simplified version of BB84 in his paper, "Quantum cryptography using any two non-orthogonal states" [Bennett92]. The key difference in B92 is that only two states are necessary rather than the possible 4 polarization states in BB84. As shown in figure 2, 0 can be encoded as 0 degrees in the rectilinear basis and 1 can be encoded by 45 degrees in the diagonal basis [CKI-BB92] [Gisin02]. Like the BB84,

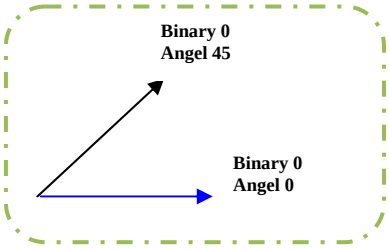

Figure 5 shows the bases for the encodes in B92

- Alice transmits to Bob a string of photons encoded with randomly chosen bits but this time the bits Alice chooses dictates which bases she must use.
- Bob still randomly chooses a basis by which to measure but if he chooses the wrong basis, he will not measure anything; a condition in quantum mechanics which is known as an erasure [Bruss07].
- Bob can simply tell Alice after each bit she sends whether or not he measured it correctly.

IX. QKD ENVIRONMENT

There are two environments QKD may deal with, both belong to optical networks, the 1st environment is the fiber optics "wire", many research has done on this area, and its

ISSN : 0975-3397

wide use nowadays, most of researches try to increase the length of wire communication with guarantee the quality of the photon polarizations which represent the mean component in the QKD, practically the researchers overtake the 150 KM with some methods, these system has offered 100% secure system, however its represent a very highly cost, in term of the hardware and fiber itself, the 2nd environments is the free space "wireless", currently it very hot topic and many research try to develop QKD in the free space, in deed QKD in the free space also faced a problems, such as the impact of the environment in the photon polarization, in other word "noisy", other challenge for implement QKD in free space is the cost and finally the destines between the two ends. From the review most of the researches didn't pass a cable of kilometers or maybe three, in fact it appears limitations on that type of security systems.

As a conclusion QKD very good in term of fast transmission secure data, guarantee 100% protecting data, suitable with optical networks

X. XKMS

This new open architecture enables practically all developers to easily integrate secure services directly into their applications. At present, developers have to upgrade their office and e-commerce applications, using the kits provided by a great many software producers, to enable them to support digital authentication keys and digital signatures. Functions such as digital certificate processing, revocation status control and certificate location and validation are not always compatible with the entire range of PKI solutions available on the market. The new XKMS standard enables these functions to be integrated directly into the servers and accessed using easily-programmed XML messages.One standard that may meet the listed goals for an Certificate Validation Service is XKMS [XKMS]. XKMS has the potential to bind attribute to Public Keys as well as to Kerberos principals. Further investigation is needed to see if XKMS provides all the required features for such an assertion validation service. The XKMS-specification is currently being revised within the W3C [W3C].

The XKMS standard is compatible with the emerging standard for digital signatures in the XML language. XKMS version 1.1, which is designed to be implemented in the same way as a Web service, is based on the WSDL (Web Services Description Language) 1.1 and SOAP (Simple Object Access Protocol) 1.1 protocols. Future versions of the XKMS standard will be compatible with encryption, signature and XML language protocols

XI. XKMS PROTOCOL

The XML Key Management Specification (XKMS) is a Web Service that provides an interface between an XML application and a Public Key Infrastructure (PKI). XKMS greatly simplifies the deployment of enterprise strength Public Key Infrastructure by transferring complex processing tasks from the client application to a Trust Service.

The XML Key Management Specification (XKMS) is the coming version for PKI, this version solves the problem of the vendors; XKMS comprises two parts -- the XML Key Information Service Specification (X-KISS) and the XML Key Registration Service Specification (X-KRSS).

These protocols do not require any particular underlying public key infrastructure (such as X.509) but are designed to be compatible with such infrastructures.

XII. TWO-PHASE REQUEST PROTOCOL

XKMS requests may employ a two-phase request protocol to protect against a denial of service attack. The two-phase request protocol allows the service to perform a lightweight authentication of the source of an XKMS request; specifically the service determines that the client is able to read messages sent to the purported source address. Although this mechanism provides only a weak form of authentication it prevents an attacker performing a Denial of Service attack by forcing the service to perform a resource intensive form of authentication such as the verification of a digital signature.

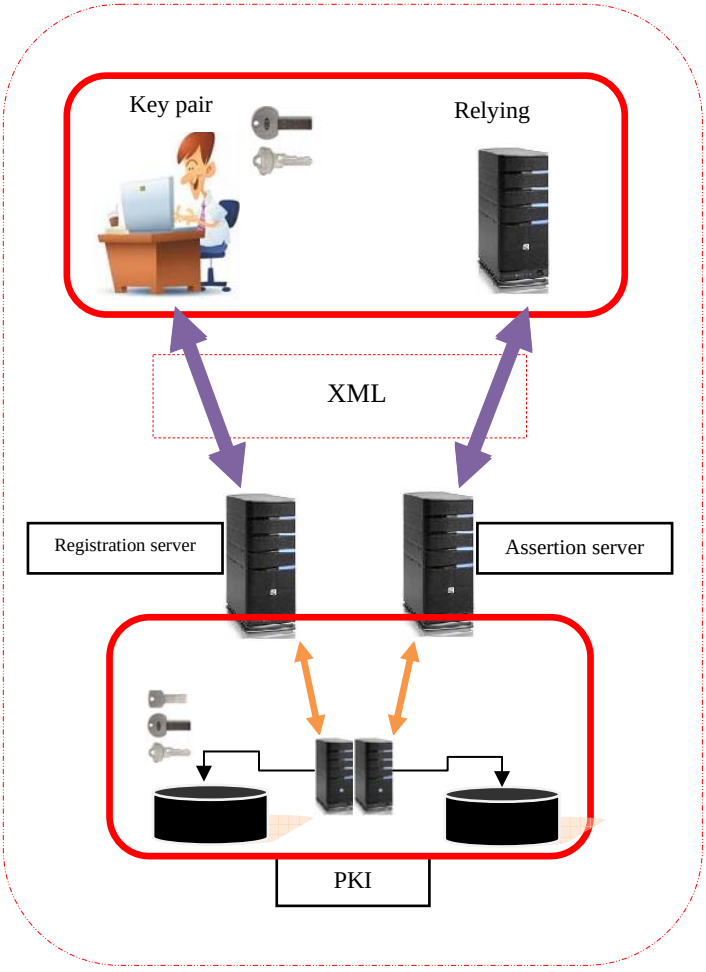

Figure 6 Simple configuration for XKMS

ISSN : 0975-3397

QDK	Public/Private Key
Requires dedicated Hardware and communication lines	Can be implemented in software, very Portable
Security is based on basic principles, does not requires changes in future	Requires using longer P/P keys as computer power increases
Will still be as secure even if Quantum Computer will be built	If a Quantum Computer will be built, it will be able to break it instantaneously
High cost	Low cost
Work in both wire and wireless but only with optical network	With all type of networks

XIII. DISCUSSION

Finally there are some discussions about these principles above; the best way of protecting data is cryptography, as a conclusion asymmetric algorithms shows a very good performance, QKD comparing Public key, more secure, and more expensive, however there is some limitation on QKD, this limitation represented in the distance, both of QKD approaches is not far enough to be in spied of PKI, at the same time, some of the PKI methods start to drop down, such as RSA, in this case what is the solution, an other problem in the network encryption methods which is the number of vendors, it is an other serious problem, as we have learned most of QKD application is special, what is the new coming, the new version of XML encryption which can deal with PKI is in part a very good solution currently, XML key method can deal with the current vendor problems, it may also solve part of the security issues, although there will be a problems if Quantum computers will be offered in the market , the table below show QKD VS Public Key

In this paper we overview the most popular methods for encryption, in fact this paper has focused in the Key Management Distribution in a different environment and different approaches , also this paper overview the known protocols for each approaches, and finally we have finished with XML key distributions and its protocols.

XIV. ACKNOWLEDGEMENT

The Author would like to thank the entire workers on this project, spicily for the scientist Prof. Khalid Alkhateeb, the spiciest on Quantum Mechanism, with out his course and his advice this project paper will not appear.

This work was supported in part by the International Islamic University Malaya and University of Malaya/ Kuala Lumpur Malaysia;

XV. AUTHOR INFORMATION

Bilal Bahaa Zaidan

He obtained his bachelor degree in Mathematics and Computer Application from Saddam University/Baghdad followed by master from Department of Computer System & Technology Department Faculty of Computer Science and Information Technology/University of Malaya /Kuala Lumpur/Malaysia, He led or member for many funded research projects and He has published more than 40 papers at various international and national conferences and journals. His research interest on Steganography & Cryptography with his group he has published many papers on data hidden through different multimedia carriers such as image, video, audio, text, and non multimedia careers such as unused area within exe. file, he has done projects on Stego-Analysis systems, currently he is working on Quantum Key Distribution QKD and multi module for Steganography, he is PhD candidate on the Department of Computer System & Technology / Faculty of Computer Science and Information Technology/University of Malaya /Kuala Lumpur/Malaysia.

Aos Alaa Zaidan

He obtained his 1st Class Bachelor degree in Computer Engineering from university of Technology / Baghdad followed by master in data communication and computer network from University of Malaya. He led or member for many funded research projects and He has published more than 40 papers at various international and national conferences and journals, he has done many projects on Steganography for data hidden through different multimedia carriers image, video, audio, text, and non multimedia carrier unused area within exe. File, Quantum Cryptography and Stego-Analysis systems, currently he is working on the multi module for Steganography. He is PhD candidate on the Department of Computer System & Technology / Faculty of Computer Science and Information Technology/University of Malaya /Kuala Lumpur/Malaysia

Harith Mwafak

He has obtained his 1st Class Bachelor in the electronic engineering from technology university- Baghdad / Iraq. Currently he is master candidate at the Faculty of Electronic Engineering/ department of communication/ International Islamic University of Malaya, Kuala Lumpur, Malaysia. His research interest on Quantum Cryptography, video streaming encryption, network security

ISSN : 0975-3397

XVI. ABBREVIATIONS

DES	Data Encryption Standerd
AES	Advanced Encryption Standard
CA	Certificate Authority
D-F	Diffie- Hellman
PKC	Public Key Cryptography
PKI	Public Key Infrastructure
RA	Registration Authority
RC	Rivest Ciphers
RSA	Rivest Shamir Adleman
QKD	Quantum Key Distribution
XML	Extensible Markup Language
XKMS	XML Key Management Specification
KDM	Key Distribution Management

XVII. REFERENCES

[1] Kahn, David , (1980). Cryptology Goes Public, Communications Magazine, IEEE, available from: http://ieeexplore.ieee.org/iel5/35/23736/01090200.pdf?tp=&isnumber=&arnumber=1090200. (Accessed April 28, 2008).

[2] Bilal Bahaa Zaidan, Aos Alaa Zaidan, Alaa Yasen Taqa, Fazidah Othman , Miss Laiha Mat Kiah, 2009 “An Empirical Study of Impact of the Increment of the size of Hidden Data on the Image Texture” International Conference on Fu`ture Computer and Communication

[3] Quantum Cryptography, N.Gisin, G.Ribordy, W.Tittel, H.Zbinden, Reviews of Modern Physics, Vol. 74, p. 145 (2002), http://arXiv.org/abs/quant-ph/0101098 (this is a very technical introduction to Quantum Cryptography)

[4] M. Riaz and H. M. Heys. The FPGA implementation of the RC6 and CAST-256 encryption algorithm. In *Electrical and Computer Engineering*, Edmonton, Alberta, May 1999. IEEE Canadian Conference on Electrical and Computer Engineering CCECE ’99. http://www.engr.mun.ca/~howard/PAPERS/fpga.ps.

[5] Diffie , Whitfield & Hellman, Martin E, (1976) . New Directions In Cryptography, IEEE TRANSACTIONS ON INFORMATION THEORY, available from: http://www-ee.stanford.edu/~hellman/publications/24.pdf. .

[6] Cypher Research Laboratories, (2006). A Brief History of Cryptography, available from: http://www.cypher.com.au/crypto_history.htm.

ISSN : 0975-3397