A QUANTUM CRYPTOGRAPHY PROTOCOL FOR ACCESS CONTROL IN BIG DATA

Abiodun O. Odedoyin [1], Helen O. Odukoya [2] and Ayodeji O. Oluwatope[3]

[1]Information Technology and Communications Unit, Obafemi Awolowo University, Ile-Ife, Nigeria.
[2,3]Department of Computer Science and Engineering, Obafemi Awolowo University, Ile-Ife, Nigeria.

ABSTRACT

Modern cryptography targeted towards providing data confidentiality still pose some limitations. The security of public-key cryptography is based on unproven assumptions associated with the hardness /complicatedness of certain mathematical problems. However, public-key cryptography is not unconditionally secure: there is no proof that the problems on which it is based are intractable or even that their complexity is not polynomial. Therefore, public-key cryptography is not immune to unexpectedly strong computational power or better cryptanalysis techniques. The strength of modern cryptography is being weakened and with advances of big data, could gradually be suppressed. Moreover, most of the currently used public-key cryptographic schemes could be cracked in polynomial time with a quantum computer. This paper presents a renewed focus in fortifying the confidentiality of big data by proposing a quantum-cryptographic protocol. A framework was constructed for realizing the protocol, considering some characteristics of big data and conceptualized using defined propositions and theorems.

KEYWORDS

Quantum cryptography, protocols, access controls, confidentiality, big data.

1. INTRODUCTION

According to [1], there are three distinct master categories of access controls namely "Physical", "Administrative" and "Technical" access controls. These categories define the main objectives of proper security implementation. Technical access controls encompass technologies as encryption, smart cards, network authentication, access control lists (ACLs), file integrity auditing software etc. This research study dwells within the use of technical access control, specifically using encryption, often used to protect data as a means of implementation. Thus, the entrance of cryptography which is the study and practice of encryption and decryption. Cryptography is also defined as the practice and study of techniques for secure communication in the presence of third parties called adversaries [2]. Cryptography is about constructing and analyzing protocols that prevent third parties or the public from reading private messages [3]. Four basic types of modern cryptography have been identified namely *symmetric*, *asymmetric*, *hybrid cryptography* and *hash functions*. This is shown in Table 1. The security of contemporary cryptographic systems being used in public communications channels is based on the secrecy of the key(s) which is being shared or exchanged among a set of legitimate users. For secure key establishment, an unauthorized user should not know or gain access to the key. This notion of secure key establishment in public key cryptography is based on unproven assumptions associated with the hardness/complicatedness of certain mathematical problems (meaning no algorithms are known to solve the problems in efficient time) [4].

DOI:10.5121/ijcis.2018.81021

Table 1. Overview of Modern Cryptography.

S/N	Type	Feature	Description	Benefits	Limitations
1.	Symmetric Key Cryptography aka Private Key (PKC) or Secret Key Cryptography (SKC).	Categorized as *stream ciphers* or *block ciphers* Depend on mathematical techniques; involves the complexity of factoring large numbers.	Both parties use same key to encrypt and decrypt data. Encryption algorithm generates key and sends to receiver for decryption [5].	Fast, simple and effective approach. Smallest change in secret key will not decrypt encrypted message.	An intruder can use leaked key to decrypt communication between two trusted devices or persons. Communication can be intercepted and altered. Present huge computing power can be used to crack key.
2.	Asymmetric Key Cryptography aka Public Key Cryptography (PKC).	Key is obtained from certificate authority that issues a digital certificate containing the public key of the certificate holder and other identification information. Depend on mathematical techniques; involves the complexity of factoring large numbers.	Two sets of keys are generated; a *public key* - to encrypt data and a *private key* -to decrypt the data. Encryption algorithm uses different keys for encryption and decryption. [6].	The public key can be shared to send the encrypted data, while the private key is stored safely with the owner and is used for decryption. Method is more secured when compared to private key cryptography.	New pair of public and private keys are generated when key gets lost/leaks. Due to increased complexity and computational unit, overheads are high. Not usually used in practical implementation for encryption because of its slowness. Because the security of these algorithms are not proven, the security of the whole implementation can be compromised.
3.	HASH Function	A one-way encryption. Uses no key for encryption and decryption.	Uses a mathematical transformation to irreversibly "encrypt" information, providing a digital fingerprint.	Provides a digital fingerprint of a file's content to ensure file has not been altered. Used by operating systems to encrypt passwords.	A hash cannot be decrypted in order to find the original string that created it. Primarily used for message integrity.
4.	Hybrid Cryptography	A combination of public key and private key cryptography. A pair of public and private keys are used to encrypt and decrypt the data [7].	Have salient features of Private key and Public key Cryptography.	Fast speed, easy to process. Users can generate their own keys of variable length and can upgrade key at any interval of time	Operates on binary bit sequences. Relies on publicly known mathematical algorithms for coding information. Secrecy is obtained through a secrete key (seed) for algorithm. Relies on unproven assumption

There is a large gap created between the speed that the legitimate users compute the key and the speed which with the intruder finds out its value. The computing resources needed to solve these problems become totally unachievable when long enough keys are used. This is termed “provable computational security” and is tightly associated with the opponent’s computational power. Public-key cryptography is however not unconditionally secure: there is no proof that the problems on which it is based are intractable or that their complexity is not polynomial [8].

Traditional (pre-computer) cryptography, categorized as earlier methods of encryption and decryption, whose roots were found in Roman and Egyptian civilizations, which include Hieroglyph, Caesar Shift Cipher [9], Steganography, Vigenere Coding and Enigma rotor machine

had major drawbacks. They manipulated traditional characters, i.e., symbols, letters, and digits directly and used substitution and/or transposition techniques. Thus, these methods were relatively easy to break especially for those who could read and write. Along with numerous German operator errors, the Enigma rotor machine had several built in weaknesses that allied cryptographers exploited. The major weakness was that it's substitution algorithm did not allow any letter to be mapped to itself. This allowed the allied cryptographers to decrypt a vast number of ciphered messages sent by Nazi Germans[10]. Steganography [11], which is a bit different from the list, embeds data into other media in an unnoticeable way, instead of employing encryption. Mediums used for steganography include objects such as picture, audio, video files, web pages, communication protocols, data streams and many more. A major discovery of steganography implementations is that it carries with it significant trade-off decisions. Some limitations include that messages are hard to recover if used medium is subject to attack such as translation and rotation. Also significant damage may be made to medium used, thus the message becomes difficult to recover. In other ways some of the embedded data are relatively easy to detect while, some media may become distorted making the message become easily lost if such media are subjected to compression such as JPEG. This research study proposes a quantum cryptographic protocol for big data. In contrast to several other related work, the protocol would be adapted for big data taking into consideration, major characteristics of big data. The rest of the paper is organized as follows: Section 2 gives a brief overview of some major protocols used in public communication. Section 3 presents the proposed scheme and finally, Section 4 concludes the paper.

2. OVERVIEW OF PROTOCOLS USED IN COMMUNICATION

For a long time cryptographic protocols like Telnet, FTP, the old UNIX utilities, rlogin, rsh and rcp have been used but they do not provide a secure way for the interchange of data in public networks as each tends to be used in different areas, thus they are considered weak. The growth and broad expansion of the World Wide Web has changed its intended use from the beginning. In order to avoid hackers & eavesdroppers stealing personal information, people demand web security, which is mainly provided majorly through two methods : Secure Sockets Layer (SSL) - (known now as Transport Layer Security - TLS) and Secure Shell (SSH) [12]. Over the years, other cryptographic protocols have evolved for communicating through public networks such as the internet and many are presently in use. Examples include Internet Protocol Security (IPSec) and Kerberos. Though many of them overlap somewhat in functionality, each tends to still be used in different areas. SSL and SSH are both public key cryptography tunnelling protocols, thus the dependence on the use of mathematical techniques which involves the complexity of factoring large numbers leading to the uncertainty problem that modern cryptography suffers from. Though, both aim to secure confidential data in that they allow communication with remote computers through an encrypted channel and can do file transfers, yet, they have different applications in practice. Table 2 states a brief overview of some cryptographic protocols in use.

Table 2. Overview of Modern Cryptographic Protocols.

S/N	PROTOCOLS	OFFERS	STRENGTHS	DRAWBACKS
1.	Internet Protocol Security (IPSec).	Provides encryption and/or authentication at the IP packet level of two communicating hosts, not of the users.	Requires low-level support from the operating system. Very useful for building Virtual Private Network (VPN) and remote machine connection.	Requires special software at the client and server side, careful and detailed configuration makes it an inappropriate solution compared to SSL based VPNs.
2.	Secure Sockets Layer (SSL) - known now as Transport Layer Security (TLS). enabled by default on major browsers and e-mail clients. Uses lock icon, green address bar and https (not http).	Application-layer, widely connection-oriented mechanism for Internet client /server communication. The browser and the web server establish SSL connection using an "SSL Handshake". Uses the public, private and session keys for connection.	Recently the simplicity of SSL has caused a vast amount of new VPN (Virtual Private Network) products to use SSL as the communication protocol instead of the IPSec (IP Security) protocol.	Vulnerabilities abound which makes it susceptible to version rollback attack: ciphersuite rollback attack : key-exchange algorithm rollback attack. Certificates can be forged.
3.	Secure Shell - SSH. Widely used by network administrators to control the web and other kinds of remotely encrypted servers	A program and an internet protocol used to log into remote computer over a network.	Both ends of the client/server connection are authenticated using a digital certificate, and passwords are protected by being encrypted.	Vulnerable to different kinds of attacks: man in the middle attack: A connection between a client and the server can be sniffed leading to session key recovery.
4.	Kerberos - works by giving authenticated users "tickets", granting them access to various services on the network.	A protocol for single sign-on and authenticating users against a central authentication and key distribution server.	Kerberos is a primary method for securing and supporting authentication on a LAN, and for establishing shared secrets.	Used with other algorithms for actual protection of communication. The client and server have to include code to use it. Since not everyone has a Kerberos setup, this has to be optional - complicating its use in some programs.

2.1. Quantum Cryptographic Protocols

Quantum Cryptography (QC) applies the phenomena of quantum physics (quantum mechanics) to securing communications in the existence of adversaries. It uses photons and physics to generate a cryptographic key which is used in the transmission of data between a sender and a receiver using a suitable communication channel. QC is also known as Quantum Key Distribution (QKD) because it pertains to completely securing key distribution. Thus, while the strength of modern digital cryptography is dependent on the computational difficulty of factoring large

numbers and processing power, quantum cryptography is completely dependent on the rules of physics. Since the principle of physics will always hold true, quantum cryptography provides an answer to the uncertainty problem that modern cryptography suffers from; it is no longer necessary to make assumptions about the computing power of malicious attackers or the development of a theorem to quickly solve the large integer factorization problem. Quantum cryptography involves the use of specialized protocols used in quantum key distribution. A brief review of some of these protocols are showcased in Table 3. Some of these protocols like BB84 [13], B92 [14] and SARG04 [15] are based on the Heisenberg's Uncertainty Principle of securely communicating a private key from one party to another for use in one-time pad encryption, while others like E91 [16] and COW [17], are based on quantum entanglement. All these protocols are implemented using either single photon sources, multi-photon sources or modifications of these photon sources. In reality, a perfect single photon source does not exist. Instead, practical sources, such as weak coherent state laser sources, are widely used for QKD. A serious security loophole that exists when multi-photon sources are used is that they are susceptible to photon number splitting (PNS) attacks. In order to minimize this effect, extremely weak laser sources are used which results in a relatively low speed of QKD. This significantly limits the secure transmission rate or the maximum channel length in practical QKD systems. A successful PNS attack requires maintaining the bit error rate (BER) at the receiver's end, which cannot be accomplished with multiple photon number statistics.

Table 1. Overview of major Quantum Cryptographic Protocols.

S/N	Protocols, Year and Inventors	Uniqueness	Contrast	Limitations
1.	BB84 , 1984 by Charles Bennett & Gilles Brassard	A 0° polarization of photon in the rectilinear basis or 45° in the diagonal basis is used to represent a binary 0. A 90° polarization in the rectilinear basis or 135° in diagonal basis is used to represent a binary 1. Proven to be secure, relying on quantum property that information gain is only possible at the expense of disturbing the signal if the two states to be distinguished are not orthogonal.	Use single photon sources. The components of BB84 protocol are two bases that are to specify rectilinear (R) and diagonal (D) and four states of polarized photons.	In reality, a perfect single photon source does not exist.
2.	B92 , 1992 - modified BB84 by Charles Bennett	A photon polarization of 0° in the rectilinear basis is used to represent binary 0 and 45° in the diagonal basis is binary 1.	only two states are necessary	In reality, a perfect single photon source does not exist.
3.	SARG04,2004 - derived from BB84 by Scarani.V, Acin, A. Ribordy, G. and Gisin. N.	Uses the four states of BB84 with a different information encoding when attenuated laser pulses are used instead of single-photon source	Identical to BB84 in the first phase but differs in second phase, where a pair of non-orthogonal states are announced by the sender, who uses one of them to encode the bit rather than announcing the bases directly.	Attenuated laser pulses contain multi-photon components, which are susceptible to photon number splitting (PNS) attacks.
4.	Decoy State [18], [19].	Uses multi-photon sources and different multiple photon intensity levels at the transmitter's source, instead of one., i.e randomly chosen intensity levels (one signal state and several decoy states) are used resulting in varying photon number statistics throughout the channel	By monitoring BERs associated with each intensity level, the two legitimate parties will be able to detect a PNS attack, with highly increased secure transmission rates or maximum channel lengths, making QKD systems suitable for practical applications.	No available detailed literature showcasing the implementation of this protocol.

2.2. Implementations of Quantum Cryptography

Different systems have successfully implemented quantum cryptography technologies, but limited to Virtual Private Networks (VPNs). The DARPA Quantum Network is an example of a quantum cryptography implementation. In this network, the key is used for the first time in IPSec based VPNs. It is used in the processing of traffic and key agreement protocol [20]. A virtual private network uses a public network like the internet to connect to a private system, usually something within the company. Basically, a VPN is a secure tunnel enabling those with authorization to access internal servers and data. Cloud computing is all about connecting people as well. Instead of using a private network, like a VPN does, the cloud uses online services by connecting to a server, usually one provided by a third-party vendor. From there, businesses can use the cloud to access enterprise applications, email services, storage space, and a host of other options from where big data is being generated and that is why the cloud serves as the infrastructure for big data. Another company is MagiQ Technologies, Inc. of Bosto. MagiQ's solution is called the Navajo QPN Security Gateway. The quantum-key distribution hardware box is claimed by MagiQ to be the first commercially available quantum key distribution (QKD) system. It comprises a 40 pound chassis that is mountable in a standard 19 inch rack unit. Included in the unit are a photon transmitter and receiver, and the electronics and software required for quantum key distribution. These "black boxes" that are used by remote parties are connected by a fiber optic link that implements the BB84 quantum encryption code proposed by Brassard and Bennet. The SEcure COmmunication based on Quantum Cryptography (SECOQC) is an European project. The SECOQC offers networks with QKD with an emphasis on the prototype with trusted repeater. The topology consists of 8 network links which are connected point-to-point. They used three plug and play systems. The Tokyo QKD network is a star network pattern linking various centers. It comprises of 3 layers: the quantum layer, key management (KM) layer and the communication layer. Los Alamos National Laboratory developed a hub and spoke network in 2011. The hub is used to route messages. Each node in the network has quantum transmitters. The quantum messages are received only by the hub. The communication commences when all the nodes issues a one-time pad which is received by the hub. Other Companies that manufacture quantum cryptography systems include ID Quantique of Geneva, Switzerland, Quintessence Labs (Canberra, Australia) and SeQureNet (Paris).

3. PROPOSED SCHEME

A conceptual perspective of the influx of data from varying data sources traversing networks through communication channels was presented. The framework envisions different data sources that generate increasing 'volume' of data. These data are heterogeneous (variety), comprising of unstructured, semi-structured and structured data being transferred at varying speeds (velocity) from one end to the other. Figure 1 displays the conceptual overview of big data in transmission.

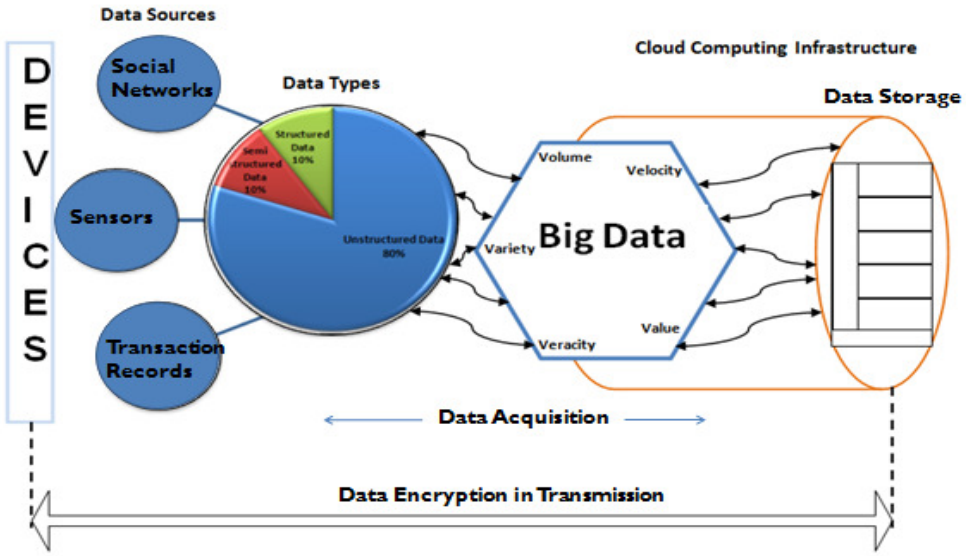

Figure 1: Conceptual overview of the flow of big data

3.1. Formalization of the proposed protocol

The protocol was abstracted using notations and propositions and formalized using temporal logic. Temporal logic was chosen because though, the meaning of the propositions were constant in time, the truth values of the same propositions can vary in time. Abstraction on the other hand means that the empirical observations, measurements etc. are translated into concepts and generalized so that it focuses on the subject of discourse. The propositions suggested in this research work are aimed at securing data during transmission. Notations used are as follows:

Alice (Sender) = A
Bob (Receiver) = B
Eve (Eavesdropper) = E
Message = unencrypted data = *plaintext* = PT
encrypted data = *ciphertext* = CT
Encryption Method = EM
Decryption Method = DM
Algorithm used = Cipher = CU
Protocol used = PU
Key = K
Known Key = K_n
Strength of Security Technique Implemented = ST_s
ST_s = (EM + DM) (CU, K, PU)
$CT=EM_k(PT)$
$PT = DM_k(CT)$

The propositions are stated thus:

α : Eve will always eavesdrop
β : Encrypted data will eventually be secured if Eve does not have access to it
δ : Encrypted data will be secured until Eve gains access to it
    δ_a : Encrypted data will be secured
    δ_b : Eve gains access to the encrypted data
λ : Eve will not gain access to the encrypted data forever

Representation of Propositions

i. α : Eve will always eavesdrop
Represented symbolically as:

$$\forall \alpha \stackrel{def}{\equiv} (\mathcal{A}P_U)(ST_s)$$
$$= (\forall \alpha : \alpha_0 = ST_s \rightarrow P_U(\alpha)$$

Read as: the statement α, will hold on all paths starting from the current sender to the receiver such that at a particular point, the strength of the security technique implemented implies that P_U is a function of α.

ii. β : Encrypted data will eventually be secured if Eve does not have access to it
Represented symbolically as:

$$\Diamond \beta \stackrel{def}{\equiv} \mathcal{F}P_U(\beta)$$
$$= (true\ \mathcal{U}\ P_U)(\beta)$$

Read as: the statement β eventually has to hold provided the eavesdropper does not gain access to the data.

iii. δ : Encrypted data will be secured until Eve gains access to it

This statement consists of two parts: δ_a - Encrypted data will be secured, δ_b - Eve gains access to the encrypted data and it is represented symbolically as:

$$\delta_a\ \mathcal{U}\ \delta_b \stackrel{def}{\equiv} (P_U \mathcal{U}\ k_n)(\delta_a)$$
$$= (\exists_i : k\ (\phi_i) \wedge \forall_j < i : P_U\ (\emptyset_j)))$$

Read as : the statement δ_a holds at the current or future paths until the statement δ_b holds, at which statement δ_a ceases to hold any longer. This expresses that the strength of the protocol used in the implementation of the security framework is significant until the key is exposed or known and this is a function of the security strength of the encrypted data.

iv. λ : Eve will not gain access to the encrypted data forever
Representation symbolically as:

$$\Box\lambda \stackrel{def}{\equiv} \mathcal{G}P_U(\lambda)$$
$$= \neg\, \mathcal{F}\ \neg\, P_U(\lambda)$$

Read as : the statement λ has to hold on the entire path from the sender to the receiver. This expresses that the choice of the protocol used is a function of the effectiveness of the security framework implemented.

3.2. Proposed protocol framework

Figure 2 presents the structure showcasing the three basic steps involved in implementing quantum cryptography**:** Key Exchange, Key Sifting and Key Distillation and showcases a schematic for the proposed framework. After sifting, the emitter and the receiver jointly process the sifted key to distill a secure sequence of bits called the secret key. The process consists of three steps: error correction, privacy amplification and authentication. QKD protocols define only the first two steps namely the raw key exchange and the key sifting.

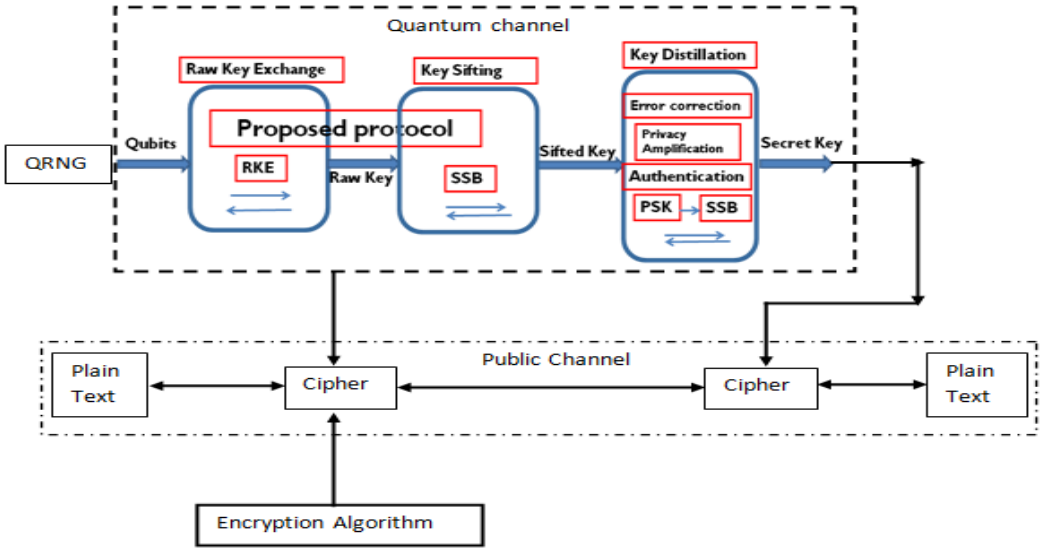

Figure 3: Schematic for the protocol framework

The proposed protocol employs the "No Cloning Theorem". The one-time pad is proposed to be selected as the encryption algorithm for the purpose of this research work. The sender and receiver must each have a copy of the same pad (a bunch of completely random numbers), which must be transmitted over a secure line. The pad is used as a symmetric key; however, once the pad is used, it is destroyed. Steps involved in achieving the proposed protocol include that:

i. The patterns of communication and data transmission in big data was considered - Client-server, peer-to-peer and/or hierarchical communication patterns which determines one-to-one, multicast or broadcast patterns of transmission.
ii. Selected characteristics of big data was considered.
iii. The format for encryption was highlighted and outlined taking into consideration the selected algorithm, processing of the plaintext;block or stream, sequences of the communication rules thus, resulting into message structure, key generation and the outcome of the process.

In this framework, the proposed protocol uses the main idea of decoy states which is that Alice changes at random, the characteristics of some extra pulses (decoy states) sent to Bob, revealing this information only at the end of the transmission. Therefore, the eavesdropper cannot adjust her attack to each pulse shared. The main idea behind decoy states is that it solves the multi-photon issue which is a security loophole for Photon Number Splitting (PNS) attack which in a bid to minimize, the sender has to use an extremely weak laser source, resulting in a relatively low speed of QKD. Decoy state QKD uses a few different photon intensities instead of one.

4. CONCLUSIONS

In this paper, a quantum cryptographic protocol is proposed for access control in big data. This protocol is active in the key exchange and key sifting steps. The flow of big data was conceptualized and a general formalization was done for the protocol. A framework was borne out of the steps involved in quantum cryptography for the realization of the protocol. This research is an on-going work which promises a protocol for access control in big data. Further aspect of this research work to be carried out include protocol verification, simulation and evaluation.

ACKNOWLEDGEMENT

The authors are grateful to all who have contributed to the success of this project. Special thanks to Stephen Olabode Odedoyin, a postgraduate research student of the Department of Economics, Faculty of Social Sciences, Obafemi Awolowo University, Ile-Ife for his contributions, technical information and support during the course of the research work.

REFERENCES

[1] Rao, U.H.and Nayak,U.(2014):The InfoSec Handbook.An Introduction to Information Security Copyright © 2014 by Apress Media, LLC, all rights reserved.Pg 63 - 69.
[2] Rivest, R.L. (1990). "Cryptography". In J. Van Leeuwen Handbook of Theoretical Computer Science. 1. Elsevier.
[3] Bellare, M. and Rogaway, P. (2005): Introduction . Introduction to Modern Cryptography. Pg.10
[4] Teloni, P. P. (2011) : Analysis of BB84 protocol in the UC-framework. Final Thesis - National and Kapodistrian University of Athens, School of Science, Faculty of Informatics and Telecommunications, Athens. pg 8 - 10
[5] Crampton, J. (2011): "Time-Storage Trade-Offs for Cryptographically-Enforced Access Control", Lecture Notes in Computer Science, Springer, 2011, Volume 6879/2011, pp. 245-261.
[6] Harn, L. and Lin, H. Y. (1990): A Cryptographic key generation scheme for multi-level data security, Journal of Computer and Security, 9 (6), pages 539-546.
[7] Ohta, K., Okamoto, T., and Koyama, K. (1991): "Membership Authentication for Hierarchical Multi groups using the Extended Fiat-Shamir Scheme", In Proceedings of the Workshop on the Theory and Application of Cryptographic Techniques on Advances in Cryptology (EUROCRYPT '91), pp. 446 - 457.
[8] Alléaume, R., Branciard, C., Bouda, J., Debuisschert, T., Dianati, M., Gisin, N., Godfrey, M., Grangier, P., Länger, T., Lütkenhaus, N., Monyk, C., Painchault, P., Peev, M., Poppe, A., Pornin, T., Rarity, J., Renner, R., Ribordy, G., Riguidel, M., Salvail, L., Shields, A., Weinfurter, H. and Zeilinger, A. (2014) : Using Quantum Key Distribution for Cryptographic Purposes: A survey. Theoretical Computer Science 560 (2014), pp. 62–81 Science Direct, Elsevier.
[9] Jain, A., Dedhia, R. and Patil, A. (2015): Enhancing the Security of Caesar Cipher Substitution Method using a Randomized Approach for more Secure Communication. International Journal of Computer Applications (0975 – 8887) Volume 129 , No.13, Pages 6 - 11.
[10] McDonald, N. G. (2009): Past, Present and Future Methods of Cryptography and Data Encryption. A Research Review. University of Utah, Pg 1-21.
[11] Anderson, R. J. and Petitcolas, F. A. P. (1998) : On The Limits of Steganography. IEEE Journal of Selected Areas in Communications, 16(4):474-481.
[12] Wikstrom, E. and Lindkvist, T. (2004) : Secure Communication: Is it possible with SSL and or SSH? Information Security Project, Linkoping University
[13] Bennett, C. H. and Brassard, G. (1984): "Quantum Cryptography: Public Key distribution and coin tossing," Proc. of the IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India, pp. 175-179.
[14] Bennett, C.H. (1992): Quantum cryptography using any two non orthogonal states, Physical Review Letters 68 (21), (1992),3121-3124.
[15] Scarani, V., Acin, A., Ribordy, G. and Gisin, N. (2004): "Quantum Cryptography protocols robust against Photon number Splitting attack." Physical Review Letters, vol.92. 057901
[16] Ekert, A.K. (1991): "Quantum cryptography based on Bell"s theorem.", Physical review Letters, Vol. 67, No, 6, pp 661-663. American Physical Society, (APS Physics).
[17] Gisin, N., Ribordy, G., Zbinden, H., Stucki, D., Brunner, N. and Scarani, V. (2004): "Towards practical and fast quantum cryptography", arXiv:quant-ph/0411022.
[18] Lo, H-K, Ma, X. and Chen, K. (2005): Decoy state quantum key distribution. Physical Review Letters, 94(3): 230504.
[19] Wang, X-B.(2005): Beating the photon-number-splitting attack in practical quantum cryptography. Physical Review Letters, 94(23):230503.
[20] Elliot, C., (2004): Quantum Cryptography, IEEE Security and Privacy Journal, 2004, pp. 57-61

AUTHORS

Abiodun O. Odedoyin, is currently a network engineer with the Information Technology and Communications Unit (INTECU), Obafemi Awolowo University and a PhD. sstudent in the Department of Computer Science and Engineering, within the same University. Her research interests include Network Security, Quantum Cryptography, Big data and Network Monitoring.

Oluwatoyin H. Odukoya Ph. D (Computer Science) is a lecturer at the Department of Computer Science and Engineering, Obafemi Awolowo University, Ile-Ife. Her research interest include security and usability of computer/software systems.

Ayodeji, O. Oluwatope Ph.D (Computer Science) is an Associate Professor of Computer Science and Engineering, Obafemi Awolowo University (OAU), Ile-Ife, Nigeria. He is the Lead Researcher, Network Utility Maximisation Group, Comnet Lab., Department of Computer Science & Engineering, OAU., Ile-Ife. His research interests include network protocol performance modelling, network security and reconfigurable computing.