Efficient quantum cryptography technique for key distribution

Kranthi Kumar Singamaneni[1,*], Pasala Sanyasi Naidu[1], Pasupuleti Venkata Siva Kumar[2]

1. Department of CSE, GITAM Institute of Technology, GITAM Deemed to be University, Vishakhapatnam, India

2. Department of CSE, VNR Vignana Jyothi Institute of Engineering and Technology, Hyderabad, Telangana, India

kkranthicse@gmail.com

ABSTRACT. *In today's digital era, electronic communication is leading us to have more secure data transmission. Key distribution algorithm is one of the main pillars of modern cryptography techniques. It is the function that delivers a key to two parties who wish to communicate with each other in secure manner. Therefore, key distribution must be secure enough to thwart any attempts to compromise the system. RS A and Diffie-Hellman are classical key distribution algorithms based on mathematics. These algorithms provide security by manipulating large prime numbers and its calculation, which takes thousands of years to solve. These algorithms are NP-complete. But once P=NP is proven; these algorithms can be solved in polynomial time. Many laboratories doing research on Quantum computer are promising exponential speed in computation. With advancement in computing technology, existing techniques that solely relies on mathematics will collapse. Quantum cryptography uses physics which offers ultimate security assurance with photon polarization property. Key distribution using Quantum cryptography is about to share key with photons and its polarization property, which gives secure key and also informs about eavesdropper attempt. Implementation of Quantum key distribution algorithm is very complex and expensive. Experimental setup in this paper is suitable with photon stream. Laser light generates photon stream and stepper motor with arduino provide polarization to photon stream. Optical fiber cable is used to carry light from sender to receiver. At receiver side, photodiode is used to capture light.*

RÉSUMÉ. *A l'ère numérique de nos jours, les communications électroniques nous conduisent à une transmission de données plus sécurisée. L'algorithme de distribution de clé de chiffrement est l'un des principaux piliers des techniques de cryptographie modernes. C'est la fonction qui fournit une clé de chiffrement à deux parties qui souhaitent communiquer entre elles de manière sécurisée. Par conséquent, la distribution des clés de chiffrement doit être suffisamment sécurisée pour contrecarrer toute tentative de compromettre le système. RSA et Diffie-Hellman sont des algorithmes classiques de distribution de clés de chiffrement basés sur les mathématiques. Ces algorithmes fournissent une sécurité en manipulant de grands nombres premiers et leur calcul, ce qui prend des milliers d'années à résoudre. Ces algorithmes sont NP-complets. Mais une fois que P = NP est prouvé, ces algorithmes peuvent être résolus en*

temps polynomial. De nombreux laboratoires effectuant des recherches sur le calculateur quantique promettent une vitesse de calcul exponentielle. Avec les progrès de la technologie informatique, les techniques existantes qui reposent uniquement sur les mathématiques vont s'effondrer. La cryptographie quantique utilise la physique qui offre une sécurité ultime avec la propriété de polarisation de photons. La distribution de clé de chiffrement à l'aide de la cryptographie quantique est sur le point de partager la clé avec les photons et sa propriété de polarisation, ce qui sécurise la clé et informe également sur les tentatives d'espionnage. L'implémentation de l'algorithme de distribution de clé quantique est très complexe et coûteuse. La configuration expérimentale de cet article convient au flux de photons. La lumière laser génère un flux de photons et le moteur pas à pas avec arduino assure la polarisation du flux de photons. Un câble à fibres optiques est utilisé pour transporter la lumière de l'expéditeur au récepteur. Du côté du récepteur, la photodiode est utilisée pour capturer la lumière.

KEYWORDS: *diffie-hellman, RSA, quantum cryptography, quantum key distribution.*

MOTS-CLÉS: *diffie-hellman, RSA, cryptographie quantique, distribution de clés quantiques.*

DOI:10.3166/JESA.51.283-293 © 2018 Lavoisier

1. Introduction

Security is ubiquitous. We are living in information age of e-commerce and electronic transactions. This led to the need for development of secured system tremendously. Solution to this problem is “Cryptography” - a technique used to generate message in encoded form and to decode it as well. This technique is used to build cipher to ensure two goals of security - confidentiality and integrity of information. For this purpose, cryptography uses concept of “KEY”. There are three mechanisms:

Asymmetric-key encipherement

Symmetric-key encipherement

Hashing

In asymmetric-key encipherement, two keys are used: Public key and Private key. To have secure communication, sender needs to encode message using public key of receiver. To decrypt message, receiver needs to use his own private key. In Hashing technique, a fixed-length message digest is created from a message having variable length. Digest is much smaller than actual message. Both message and digest need to send (Buschhorn and Wess, 2004). On receiver side, receiver needs to generate message digest and verify it with digest of sender.

In both of above techniques, key distribution is not a problem. Problem of key distribution arises with Symmetric key encipherement. Here, only one secret key is used for encipherement. Sender and receiver can communicate over insecure channel with assumption that Eve cannot understand the message by simply intercept or eavesdrop it from channel (Pranav and Ritika, 2013). Eve will be in need with key that is used to encode message. Sender will encode message using traditional encoding algorithm and shared key, receiver will decode message using traditional decryption algorithm and same key that is used for encryption. No other key will be able to

decrypt message. Here, encryption decryption can be public (Scarani *et al*., 2004). i.e. We can assume that Eve knows encryption decryption algorithm as per Kerckhoff's law. Message can be sent over insecure channel, but we need to keep shared key secret (Muhamad and Zukarnain, 2009). Shared key cannot be sent over public channel, we need secure channel communication for shared key. Here, secure channel is key exchange problem.

2. Traditional approach

Most common used algorithm for key exchange is Diffie- Hellman key exchange algorithm and RSA Cryptosystem.

2.1. Diffie-Hellman key exchange algorithm

In 1976, Whitfield Diffie and Martin Hellman proposed an algorithm as solution to key distribution algorithm, which is known as Diffie Hellman Key Exchange Algorithm. To ensure key, this algorithm uses fundamental of mathematics - algebra of exponent and modulus arithmetic (Vejendla *et al*., 2017).

Process of Diffie -Hellman is described as follows: Here, Alice and Bob are two participants.

Alice and Bob agree upon two values P and G, where P is large prime number and G is base or generator.

Alice takes a secret number a

Bob takes secret number b

Alice compute her public value as X = G^a mod P

Bob computes his public value as Y = G^b mod P

Alice and Bob exchanges theirs numbers. Now Alice has P,G,a,X,Y and Bob has P,G,b,X,Y

Alice computes K = Y^a mod P

Bob computes M = X^b mod P

Fortunately, Numbers calculated by Alice and Bob will be same by laws of algebra. i.e. K = M

2.2. RSA cryptosystem

In 1978, Ron Rivest, Adi Shamir, and Leonard Adleman introduced a cryptographic algorithm for key distribution. Main operation of RSA is to compute modular exponentiation. RSA is an asymmetric key cryptosystem relies on the assumption that it is difficult to find the factors of large integers (Huang *et al*., 2009).

It distributes key to sender and receiver. Key distribution here involves sending public and private key to sender and receiver, who wants to communicate, to encrypt and decrypt the message respectively (Hiroaki *et al*., 2015). RSA involves Key generation, Message encryption and message decryption.

The algorithm is as follows:

2.2.1. Key generation

Two distinct random prime numbers p and q are taken.

n = p x q. Here, n will be in bits with same key length.

φ(n) = (p - 1) x (q - 1) Here, φ = Euler's totient function.

Calculate e based on the following conditions:

1 < e < φ(n)

GCD (e, φ(n)) = 1 i.e., e and φ(n) are co-p rime.

e must have a short bit-length

Find out d which satisfies (e x d) Mod (n) = 1

Now, the Public Key includes e and n i.e., (e, n). The Private Key includes d and n. i.e., (d, n).

2.2.2. Message encryption

The sender will generate encoded message C, from actual message M using following:

Cipher text C = M^e Mod (n) where C is the cipher text generated after encryption.

2.2.3. Message decryption

The receiver will decode encrypted message C using following:

The original message M = C^d Mod(n).

3. Limit ations of traditional approach

The classical cryptography relies on mathematical computations and its manipulations. This leads us to following limitations:

3.1. Computing technology advancements

Current cryptography system is having key size is so large. For billions of computer working simultaneously, which calculates billions of instruction per second, would still take trillions of years to crack key. In near future, development of Quantum computer will provide speed at which no computer in use now could possibly perform. Quantum computer will be able to perform calculations at exponential speed up, the codes that would take a trillion years to break with conventional computers could possibly be cracked in polynomial time.

As the keys can be cracked easily, the encryption algorithms would be of no use.

3.2. P=NP is proven

Classical Cryptography is having key distribution algorithms – Diffie-Hellman and RSA, which are considered as NP-Complete. But once P=NP is proven; current security systems, which are based on it will collapse.

3.3. Eavesdropping

Eavesdropping is an act of stealing data packets transmitted by others on network (Sabri *et al*., 2014). Eave can use this data content in search of sensitive information like passwords, session tokens, or any other kind of confidential information. In classical cryptography, both the sender and the receiver of information will have absolutely no idea that they are being hacked.

These limitations can be easily overcome by switching over to Quantum Cryptography.

4. Key distribution using quantum cryptography

4.1. Quantum cryptography

Quantum cryptography uses physics in place of mathematics to develop a cryptosystem. i.e. One that is completely secure against being compromised without knowledge of sender and receiver.

The foundation of quantum cryptography lies on the Heisenberg uncertainty principle, which can be interpreted as certain pairs of physical properties are related in such a way that measuring one property prevents the observer from simultaneously knowing the value of the other.

Quantum cryptography differs from Classical cryptography by following two reasons:

It relies more on physics rather than mathematics.

It is based on usage of individual particles/waves of light and their quantum property.

Here, photons are used for security purpose. It is theoretically possible that other particles could be used such as Fermions, Quarks or Leptons. But photon offers all necessary quality needed. (Song and Wang, 2017). Their behavior is comparatively well-understood and they are information carriers in optical fiber cable, the most promising medium for extremely high bandwidth communication.

Quantum key distribution algorithm is about to produce the key and to securely distribute the key. It is not for encoding and transmission of any message data (Nakouri *et al*., 2017). This key, generated by quantum procedure, can then be used with any chosen encryption algorithm to encrypt (and decrypt) a message. Then we can transmit it over a standard communication channel or public channel. Based on the laws of physics, quantum cryptography allows exchange of cryptographic key between two remote parties with unconditional security. Quantum cryptography obtains its fundamental security from the fact that each qubit of information is carried by a single photon, and that each photon will be altered as soon as it is read once. Any attempt to intercept key bits can be easily detected (Gan *et al*., 2018).

4.2. Quantum key distribution algorithm

In 1983, wiesner traced that single photon can be used to store information. Bennet and Brassard realized that instead of storing information, they can use this single photon for transmitting information (Yang *et al*., 2011). In 1984, they proposed their first key distribution algorithm based on Quantum theory names as BB84. In this paper, we have used BB84 protocol based on photon stream for experimental purpose.

Many Quantum key distribution algorithms exist such as: BB84, B92, Six-state, SARG04, MSZ96, etc.

Any information in computer is stored using bits. Each bit will have value either 0 or 1. When the system is quantum then, we have to store values in quantum particles known as qubits. We can represent a qubit as: spin of the atom or polarization of the photons.

For key distribution purpose, we will use 4 photon polarization states as information bit at sender side. We can set polarizat ion of photon at different angle. Here, we will use polarization at 0, 45, 90 and 135.

0 - → 1 - ↑

0 - ↖ 1 - ↗

At receiver side, to measure this photon polarization, we will have two detectors.

Linear - To measure horizontal-vertical state

Diagonal - To measure diagonal state

Some commonly used quantum key distribution algorithms are BB84 and B92. In 1984, Bennett and Brassard published key distribution protocol, which works as follows:

(a) Alice sends photon stream, which is polarized randomly into four different states.

(b) Bob measures in which direction they are polarized by using two detectors randomly.

(c) Detectors translate photon into bits. Like, Linear Detector registers Horizontal measurement as 1 and vertical as 0.

(d) Bob will eventually receive key from this set of bits.

(e) Now, Bob will compare with Alice on public channel, which detector he used for measuring photon polarization.

(f) Alice will reply publically with 'Wrong'-'right' 'wrong'-'right' based on which filter she used.

(g) After public check, they will throw out wrong measurement and left with correctly polarized photon both the sides.

This correctly photon measurements forms the key used for encryption-decryption of message. Alice can now encrypt actual message using quantum key and send through traditional scheme. Bob can decrypt it using quantum key.

4.2.1. Here, Bob's detectors are need to match with Alice's filter

If Bob uses Diagonal detector on horizontal photon, According to Quantum mechanics, he will have 50% chances of measuring 1 and 50% chances of measuring 0.

4.2.2. Bob's detector will be public

Bob will send which detector he used for mapping photon polarization. It is just detector list, not 1 and 0 that he obtained are being shared. You will still need to send polarized photon into that detector to obtain secret key.

4.3. Possible attack on system

This attack is performed by individual attackers. The eavesdropper tries to sense the data from communication channel. Same as Man-in-the middle-attack it is referred as intercept-resend attack which gives bit error rate of 25%, which is readily detectable by two parties.

For example, some eavesdropper tries to hack system and acquire photon stream. To have photon steam is pointless, still he needs to map this photon polarization and need to cross check with sender. If eavesdropper performs mapping randomly using

detectors, he cannot obtain key until he map his detector list with sender. He cannot obtain key only with photons.

If eavesdropper performs man-in-middle attack and acquire photon stream, try to map them with random detectors, and again send back to receiver, this will increase bit error rate. Here, polarization of each photon will be changed while eavesdropper tries to map them. This changed state of photon will give errors while performing public check. If error rate gets beyond threshold, both sender and receiver will discard key and try again.

Here, detector list sent by receiver and true-false list sent by sender will be public. This will create no issue because if eavesdropper got both, he cannot come up with key. He still needs to send photon in them.

5. Experimental setup

In real time, practical implementation of Quantum cryptography is not as simple as theory. To have a single photon is very complex procedure. To propagate this photon is also challenging task. Here, we will work on photon stream.

Information is being stored in photon stream rather than single photon. Here, we have developed arduino based security system which supports Quantum theory, using laser light and stepper motor used to generate photon based key distribution system.

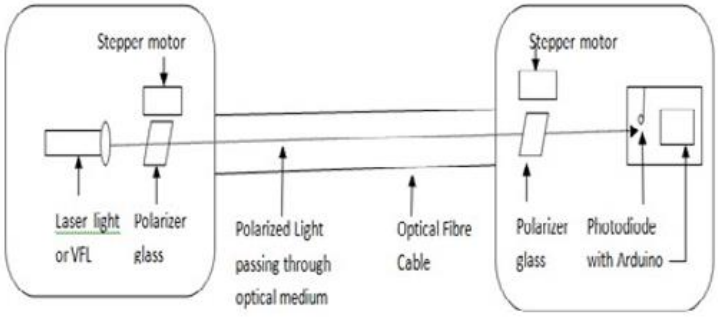

Figure 1. Experimental setup of Key distribution using quantum cryptography

5.1. General overview of setup

Photon Source

Polarizer glass

Arduino

Stepper Motor

Optical fiber cable

Photodiode with arduino

Photon beam is generated through laser pointer or VFL – Visual Fault Locator. This photon beam is then passed through polarizer glass. Here, polarizer glass is connected with stepper motor, which rotates polarizer glass in one of four angles. Polarizer glass set photon stream in one of four states as information bit 0 or 1. Stepper motor is used for positioning purpose of polarizer glass. This polarized light is sent to receiver through optical fiber cable. At receiver end, polarized light is again passed through polarizer glass with stepper motor to map the polarization of photon. Photodiode is used to map intensity of light. Here, photodiode is used to carry out the information bit in light with intensity measurement.

5.2. Detailed description of setup

5.2.1. Photon source

Photon stream is generated with 5 mW diode laser emitting at 650nm. Here, wavelength of light is needed higher because of optical fiber requirement. Laser Pointer can be used for generating photon stream, which emits at 650 nm with 5 mW. Visual Fault Locator is also used for having better optical fiber communication.

5.2.2. Polarizer glass

Polarizer glass is used to set polarization of photons. Polarization is nothing but an angle, at which photon spins. Each photon can spin in any direction. We can set photon spin in specific direction with use of polarizer glass. By having polarizer glass at specific angle, we can set angle of photon spin. Here, we need to set polarizer glass at 0, 45, 90, 135 degrees for acquiring photon states.

At receiver side, we need to set polarization at 45 and 90, which will lead us to map in formation bit in photon.

5.2.3. Arduino

Arduino is an open-source electronics platform. It is based on easy to use hardware-software. Arduino boards are able to read inputs - light on a sensor, a finger on a button, or a Twitter message - and turn it into an output - activating a motor, turning on an LED, publishing something online.

Here, we have used arduino UNO board to run stepper motor for positioning purpose. We need to set polarizer glass at specific angle. For sending photon stream in four distinguish state, we have used arduion with stepper motor at sender side. At receiver side also we have used arduino to set position of polarizer glass as detector. To catch light with photodiode, we need to set photodiode with arduino.

5.2.4. Stepper motor

Stepper motor is mainly used for positioning purpose. Here, we will use stepper motor to acquire photon state through polarizer glass. Stepper motor will set polarizer glass at specific angle and we can set photon spin direction.

Receiver side also we need to set polarizer glass to map photon polarization with stepper motor.

5.2.5. Optical fiber cable

Optical fiber cable is used to carry light from one place to another. Optical fiber consists of a core and cladding layer, selected for total internal reflection – Principle on which optical fiber works. Polarized light is sent through optical fiber cable from sender to receiver.

5.2.6. Photodiode

Photodiode is used to sense light. Photodiode is semiconductor device that converts light to current. The current is generated when photons are absorbed. A small amount of current is also produced when no light is present. Here, photodiode will sense light and gives result in intensity. Light coming through optical fiber cable have different intensity based on different state. To convert light into information bits, we need to sense light intensity, which can be done by photodiode.

6. Conclusion

Key Distribution using Quantum cryptography provides a secure way to exchange or distribute key for encryption and decryption of message. Quantum key distribution algorithm takes advantage of inviolability of low of nature to assure higher security. Eavesdropper detection is also possible with quantum cryptography. This technique fulfils the limitations of classical key distribution techniques. Also, it gives security assurance with quantum computer. Practical implementation of quantum key distribution is very complex procedure. To have single photon and propagation of photon is also very challenging. Experimental setup of quantum key distribution works with photon stream distinguished by timestamp.

Reference

Buschhorn G. W., Wess J. (2004). Fundamental physics - Heisenberg and beyond. *Springer-Verlag, Berlin*. http://doi.org/10.1007/978-3-642-18623-3

Gan H., Xiao S., Zhao Y. (2018). A novel secure data transmission scheme using chaotic compressed sensing. *In IEEE Access*, Vol. 6, pp. 4587-4598. https://doi.org/10.1109/ACCESS.2017.2780323

Hamdi N. M., Kim T. H. (2017). A new biometric-based security framework for cloud storage. *2017 13th International Wireless Communications and Mobile Computing Conference (IWCMC), Valencia*, pp. 390-395. https://doi.org/10.1109/10.1109/IWCMC.2017.7986318

Huang X., Wijesekera S., Sharma D. (2009). Quantum cryptography for wireless network communications. *IEEE Xplore*. http://doi.org/10.1109/ISWPC.2009.4800604

Muhamad N. A., Zukarnain Z. A. (2009). Implementation of BB84 quantum key distribution protocol's with attacks. *European Journal of Scientific Research*, Vol. 32, No. 4, pp. 460-466. http://doi.org/10.1564/ejsr.145623

Narayana V. L., Bharathi C. R. (2017). Identity based cryptography for mobile ad hoc networks. *Journal of Theoretical and Applied Information Technology*, Vol. 95, No. 5, pp. 1173-1181. http://doi.org/10.1564/jatit.24715

Pranav V., Ritika L. (2013). A comprehensive survey on: quantum cryptography. *International Journal of Science and Research (IJSR)*, Vol. 4, No. 4, pp. 2214-2220. http://doi.org/10.1423/ijsr.23113

Rohit M., Kaushal S., Saurabh M., Durai R. V. (2013). An algorithm to enhance security in RSA. *VIT University, IEEE – 31661*, pp. 1-4. http://doi.org/10.1109/ICCCNT.2013.6726517

Sabri H. M., Ghany K. K. A., Hefny H. A., Elkhameesy N. (2014). Biometrics template security on cloud computing. *2014 International Conference on Advances in Computing, Communications and Informatics (ICACCI)*, pp. 672-676. https://doi.org/110.1109/ICACCI.2014.6968607

Sasaki H., Matsumoto R., Uyematsu T. (2015). Key rate of the B92 quantum key distribution protocol with finite qubits. *Information Theory (ISIT), 2015 IEEE International Symposium*. https://doi.org/10.1109/ISIT.2015.7282544

Scarani V., Acin A., Ribordy G., Gisin N., (2004). Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations. *Phys. Rew. Lett*. Vol. 92. https://doi.org/10.1103/PhysRevLett.92.057901

Song X., Wang Y. (2017). Homomorphic cloud computing scheme based on hybrid homomorphic encryption. *2017 3rd IEEE International Conference on Computer and Communications (ICCC), Chengdu, China*, pp. 2450-2453. https://doi.org/10.1109/CompComm.2017.8322975

TechTarget-searchsecurity.techtarget.com Quantum Cryptography Dianna Cowern, Physics Girl-Quantum Cryptography explained– www.youtube.com.

William S. (2010). Cryptography and network security. Prentice Hall. http://www.doc88.com/p-6099876366756.html

Yang Y., Chen X., Chen H., Du X. (2011). Improving privacy and security in decentralizing multi-authority attribute-based encryption in cloud computing. *In IEEE Access,* No. 99, pp. 1-1. https://doi.org/10.1124/ieee.12471