International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 6 Issue IV, April 2018- Available at www.ijraset.com

Simulation of Securable Network Three-party Protocol Using Quantum Key Distribution in PHP

UNP. Gangadhar Raju[1], R. Venkateshwar Reddy[2], B Sravanthi Reddy[3], K Gopi Chand[4]
[1, 2, 3, 4]*CSE, Vignan Institute of Technology and Science*

Abstract*: *Encryption and decryption are the part of cryptography, which include both classical cryptography and quantum cryptography. In the existing study of third party protocol, for information transformation has very less security against attacks such as eavesdropping, man-in-the-middle and so on. In this paper, we proposed a new protocol with quantum key distribution(QKDP) which is one hundred present un-hackable and accurate. In this protocol it uses traditional QKDP to send and receive keys between parties, it uses our algorithm to get accurate results and two parties can share and use secret key for long-1term repeatedly.

Keywords*: *Encryption, Decryption, Cryptography, QKDP, Eavesdropping, Man-in-the-Middle

I. INTRODUCTION

In this day and age we have a lot of Secrets and we're constantly having to give them away to the Internet like Amazon has my credit card number, I typed it in voluntarily so I could order something online but I don't even know where my information is kept how can I trust that Amazon doesn't accidentally give it away this challenge of secret keeping is an important problem for companies and governments that's why encryption or translating information into a code only the right people can read is so important that it was put on the United States munitions list along with flamethrowers and bombs as a weapon regulated for national security that was until a student took the United States government to court and encryption was ruled free speech now most of the focus is on improving encryption because as computers get smarter and faster these codes become easier to unscramble that's why we need to turn to cutting-edge physics to improve encryption. Quantum cryptography is the science of exploiting quantum mechanical properties to perform cryptographic tasks. The best-known example of quantum cryptography is quantum key distribution which offers an information theoretically secure solution to the key exchange problem. Currently use popular public key encryption and signature schemes for example RSA and El Gamal can be broken by quantum adversaries. The advantage of quantum cryptography lies in the fact that it allows the completion of various cryptographic tasks that are proven or conjectured to be impossible using only classical that is non-quantum communication. It is impossible to copy data encoded in a quantum state and the very act of reading data encoded in a quantum state changes the state, this is used to detect eavesdropping in quantum key distribution. One of the protocol in quantum key distribution is BB84 protocol. Bennett and Brassard developed in 1984 the BB84 communication protocol which uses different non-orthogonal quantum states submitted via a quantum channel to transmit bits of Alice's random key. Quantum key distribution is a quantum technology which is already present in the market. This technology will become an essential point to secure our communication system and infrastructure, when today's public key cryptography will be broken by a mathematical algorithm or by, eventually, the development of quantum computers. Quantum key distribution is a security technology that exploits the laws of quantum mechanics to achieve information-theoretic secure key exchanging. Quantum key distribution enables two parties to "grow" a shared secret key without placing any limits on an adversary's computational power and is unique in its ability to detect the presence of any third-party eavesdropping on the key exchange. Due to the fundamental laws of quantum mechanics, any third-party eavesdropping on the key exchange will introduce detectable errors. If the errors are below a defined threshold, an unconditionally secure key can be distilled. When Quantum key distribution is used in conjunction with the one-time pad symmetric cryptographic algorithm, the result is an unconditionally secure cryptographic system.

II. QUANTUM KEY DISTRIBUTION

A technology that hides information in photons or the particles of light here's how it works say you want to enlighten pick a chosen stranger on our mantra or this instead of deciding upfront what the secret multiplication factor or key is you use quantum mechanics to make one randomly and send it to your recipient here's how the random key is made. Alice the message sender sends photons that are polarized or vibrating in four different directions horizontal vertical diagonal left or right. Bob the recipient measures which direction they're polarized note by using two differently polarized detectors for each photon one at a time back and forth guessing which detector to use randomly the detectors translate the photons into bits like a horizontal measurement could register as a one and a vertical as a zero on this detector and eventually. Bob will get the multiplication key from this set of bits so now bob has a

measurement, for each photon keeping in mind that he measured them on two different detectors randomly now he compares with Alice and for each photon he'll tell her which detector he used and she'll tell him wrong right wrong right based on which filter she used to send the photons because Alice sent either vertical horizontal photons or diagonal photons and if Bob uses a diagonal detector on a horizontal or vertical photon according to quantum mechanics he will have a 50% chance of measuring a zero and 50% chance of a one that's why Bob's detectors need to match Alice's filters after they go through this public check of the order the detectors were used they throw out each result from when Bob guessed incorrectly and now they have a sequence of identically polarized and measured photons that sequence is the key Alice can now send the actual encrypted message through a traditional channel and use the quantum key to decrypt it and mathematicians have proven that if you make a truly random numerical key you can theoretically make a code called a one-time pad that is unbreakable so why can the order of polarized detectors used by Bob be public well it's not the ones and zeros that he obtains that are being shared it's just the order of detectors you would still need to send the polarized photons in through those detectors in the correct order to figure out the key but those photons were polarized randomly so the eavesdropper is out of luck and things on this scale a thousandth of the width of a human hair get weird as they say because of quantum mechanics. If an eavesdropper hacks into the system and tries to copy some of the photons using the wrong order of detectors they'll change the key Bob and Alice will know because they can check for errors in a subset of the bits in a key and they can try again.

III.BB84

Meet Alice and Bob they would like to send encrypted messages between each other so that their messages can securely be made private. To do this they need a cryptographic key that is only known to them and which they'll use to encrypt their messages. Unfortunately, they know that somewhere out there, name Eve may try to intercept their messages and spoil their secret plans. Alice assures Bob however that they needn't worry about Eve she will teach Bob about the protocol and it will allow them to come up with a secret key they can both use and trust, but Bob says Eve may be listening right now what if she hears us, not to worry says Alice, even if eavesdropping it won't do her any good. To follow the protocol Alice and Bob will make use of two fundamentally different communication channels a classical channel and a quantum Channel. The classical channel allows them to send individual bits of information back and forth just as they would if they were using say the Internet as the bits travel across the classical channel it is possible for Eve to intercept them. Eve can observe the bits and then send copies of them on to their regular destination when communicating over the classical channel. Alice and Bob have no way to detect Eve's intrusion on their privacy the quantum Channel behaves quite differently instead of transferring bits the quantum channel transfers qubits. The qubits represent bits and can be generated by either of two processes let's call them process A and process B the protocol takes advantage of some special properties of the qubits, first a qubit cannot be copied and second it is not possible to determine whether a qubit was produced by process A or by process B. There exists a very special machine for observing qubits that were produced by process A, let's call it machine A. When a qubit representing the bit is fed into machine A the machine will output A. When a qubit representing the bid is fed into machine A, the machine will output A in both cases the qubit will also be destroyed in the process. On the other hand if machine A is fed a qubit produced by processed B its output will be random half the time is 0 half the time 1 and the qubit will still be destroyed likewise a special machine exists for observing qubits produced by process B let's call it machine B when given a qubit produced by process B machine B will output the correct bit but when fed a qubit produced by process a machine B's output will be random just as with machine A the qubit will be destroyed so when Bob receives a qubit over the quantum Channel. He won't know which machine to use to observe it he will decide via A coin toss half the time feeding the qubit to machine A half the time feeding it to machine B the protocol begins with Alice sending Bob a very large number of qubits over the quantum Channel. Bob records all of the outputs he receives as he feeds the qubits randomly to his qubit measuring machines since he will choose the correct machine half the time on average 50% of his measurements will be correct of the remaining qubits for which he used the wrong machine he will still end up with the correct bit half the time just by chance. This means that 75% of Bob's measurements will agree with the corresponding values used by Alice however if Eve intercepts the qubits before they reach Bob she will also have to make random guesses as to which machine is the correct one for measuring each qubit half the time she will use machine A and then use process A to generate a new qubit to pass on to the channel the other half of the time she will use machine B to observe the qubit and process B to generate a substitute to pass on down the channel thus with Eve attempting to listen on the quantum Channel half of the substitute qubits she sends to Bob will have been generated correctly and half of them will have been generated incorrectly and are therefore simply random qubits this means that only 75% of the qubits that reach Bob will represent the same bits that Alice intended. Now when Bob finally receives these qubits he will still be making random guesses as to how they should be measured half of the qubits will jibe with those that Alice sent and we know Bob will get 75% of those correct the other half will have been generated incorrectly by Eve and are thus completely random Bob will only get the correct bit from those half the time just my chance alone this gives Bob a new accuracy of only 62.5% on average. Bob however doesn't know this yet so he and Alice will have to communicate some information

between each other to work out what kind of accuracy Bob is getting once bob has finished measuring all the qubits he received. He will open the classical channel and send Alice a stream of bits that indicate to her which machine he used to measure each of her qubits once she receives that message from Bob she will cross-reference her personal records and send Bob a stream of bits telling him which of his qubits he should have ended up measuring correctly. Now Bob can throw away the bits for which he used the wrong machine Alice can do the same provided that Eve was de tempting to confound their efforts they should now be in possession of a string of bits that is known only to them and no one else they need to verify however that this is indeed the case since they have a very large sequence of bits they can afford to sacrifice a random subset of them in order to determine whether Eve was listening over the classical channel they choose a subset of the bits and compare them if they are satisfied that the communication was secure they can use the remaining bits to form a secret cryptographic key if they observe an accuracy of percent they can be reasonably confident that their shared bits are secure and they can begin using them good crypt further communication if they observe an accuracy rate slightly below percent they will know that Eve intercepted some or all of their qubits and the communication is not yet secured using this protocol Alice and Bob can generate a cryptographic key and can determine whether their secrecy has been compromised.

IV. PROPOSED ALGORITHM

To address these limitations of BB84 protocol, we proposed a new protocol with quantum key distribution(QKDP) which is one hundred present un-hackable and accurate in sending key and receiving key and messages. Algorithm is as follows: Step 1: Alice generates a key and encrypt the message.

E=Q (M, K), Where E is encrypted message, M is original message, K is the key and Q is encryption algorithm.

Step 2: Alice send the key to TC(trusted center).

Step 3: Trusted Center convert the normal key into quantum key by using two machines Machine A and Machine B.

BASIS	0	1	Machine A and Machine B are chosen in random basis, as bits are in binary format,
A	90^0	0^0	they are converted into photos on respective basis and sent in quantum channel. If,
B	45^0	135^0	someone tries to access those bits they convert into random angles half of the time

correct and remaining half of times incorrect with 75% accuracy measurement.

Step 4: Trusted Center sends the quantum bits in quantum channel for P times (P is chosen based on key size).

Step 5: Bob receives the key and send subkey in classical channel to check the measurement Trusted Center.

Step 6: If it is measuring 75% accuracy he again sends the same key for P number of times.

Step 6.1: Next, Bob put the key in array and compares the keys takes most repeated bit. After this process key is 99.99% accurate.

Step 6.2: Bob receives the encrypted message in classical channel and decrypt the measurement.

Step 7: If Bob's subkey is 62.5% accurate then Trusted Center understands that Eve intercepted the key.

Step 7.1: The process is terminated. Go to step 1.

V. CONCLUSIONS

Of course getting quantum cryptography to work in the real world is not so easy small disturbances can change photon polarization and when creating photons if you get them off by even just a degree those errors will add up physicists have only been able to send quantum keys over 200 kilometers you can even sabotage quantum detectors by shining a bright light on them and even if quantum encryption does become commercially viable much of the Internet's infrastructure would have to be rebuilt but still think of how powerful this technology would be an eavesdropper has to measure in order to get the key but when measured the key changes you can know if you've been hacked even before you send the message because of this fundamental aspect of nature the universe is based on probabilities quantum cryptography hides information not by besting a computer but by stowing it within the unknowability of nature..

REFERENCES

[1] C. Bennett and G. Brassard, "Quantum Cryptography: Public Key Distribution and Coin Tossing," International Conference on Computers, Systems, and Signal Processing, Bangalore, India, 1984.S. M. Metev and V. P. Veiko, Laser Assisted Microtechnology, 2nd ed., R. M. Osgood, Jr., Ed. Berlin, Germany: Springer-Verlag, 1

[2] Ekert, Artur. "What is Quantum Cryptography?" Centre for Quantum Computation –Oxford University.Conger., S., and Loch, K.D. (eds.). Ethics and computer use. Commun. ACM 38, 12 (entire issue).M. Wegmuller, J. P. von der Weid, P. Oberson, and N. Gisin, "High resolution fiber distributed measurements with coherent OFDR," in Proc. ECOC'00, 2000, paper 11.3.4, p. 109.

[3] C. H. Bennett, G. Brassard, C. Crépeau, and M.-H. Skubiszewska, "Practical quantum oblivious transfer", Lecture Notes in Computer Science 576, 351 (1991)

[4] Mullins, Justin. "Quantum Cryptography's Reach Extended." IEEE Spectrum Online. 1 Aug. 2003.

[5] M. Bellare and P. Rogaway, ―Provably Secure Session Key Distribution: The Three Party Case,‖ Proc. 27th ACM Symp. Theory of Computing, pp. 57-66, 1995.
[6] H.A. Wen, T.F. Lee, and T. Hwang, ―A Provably Secure Three- Party Password-Based Authenticated Key Exchange Protocol Using Weil Pairing,‖ IEE Proc. Comm., vol. 152, no. 2, pp. 138- 143, 2005FLEXChip Signal Processor (MC68175/D), Motorola, 1996.
[7] "PDCA12-70 data sheet," Opto Speed SA, Mezzovico, Switzerland.
[8] System Analysis and Design, Ellias M Award
[9] M. B. Hastings, "A counterexample to additivity of minimum output entropy", Nature Physics 5, 255 (2009).
[10] SQL Server 7-The Complete Reference, Gayle Coffman