IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol.-7, Special Issue-18, May 2019 E-ISSN: 2347-2693

Quantum Key Distribution Protocol for Knapsack Cryptosystem

Partha Sarathi Goswami[1*], Tamal Chakraborty[2], Abir Chattopadhyay[3]

[1]Dept. of CST, Gaighata Government Polytechnic, Government of West Bengal, India
[2]Dept. of Computer Science, Mrinalini Dutta Mahavidyapith, Kolkata, India
[3]Dean Research, University of Engineering & Management, Kolkata, India

[*]*Corresponding Author: goswamipsg@rediffmail.com, Tel.: +91-9230649935*

Available online at: www.ijcseonline.org

Abstract: The major threat in data communication in present day is security. To reduce the threat caused in the communication channel quantum cryptography is emerging as a replacement to its classical counterpart. This paper focuses on a quantum key distribution protocol for the knapsack cryptosystem using a one-way trapdoor function by qubit rotation. The protocol exploits a qubit in superposition state for a single bit message communication. The security of the protocol is owing to the fact that any random quantum state cannot be replicated.

Keywords — Quantum Cryptography, Knapsack Sequence, Quantum Key Distribution Protocol.

I. INTRODUCTION

Security has become a foremost priority in data communication in this modern world. Quantum cryptography is emerging as a new direction in information security. A trapdoor one-way function is simple to compute but complicated to crack. This is because it offers the true user with a tractable problem and simultaneously any intruder has to face a computationally infeasible problem. This is why; asymmetric cryptography relies heavily on it. In the public-key cryptosystem, plain text is encoded by the public key and the decoding is done by the private key. Thus the generation and exchange of the pair of keys (public and private) is the most important part in the cryptosystem. This paper introduces the concept of key distribution among the authentic users based on the principles of quantum theory. A quantum bit or qubit is the unit of quantum information. A single qubit has two quantum polarization states namely vertical polarization of a photon and horizontal polarization of a photon. In case of classical computing a bit can be in one state or the other whereas in a quantum bit or qubit it can exist as the superposition of two quantum states namely |0> and |1>. The proposed algorithm first converts the plain text to an encoded binary message using the concept of super increasing Knapsack sequence and thereafter using the proposed quantum key distribution protocol with rotation like in one-way trapdoor function on the qubit to encrypt the message. Similarly, the qubit is inversely rotated and applying knapsack sequence the encrypted plain text is decrypted to get the original message.

Rest of the paper is organised as follows. Section II gives a brief overview of the related works in the field of Quantum cryptography. Sections III and IV introduce the concepts of quantum cryptography and quantum session key distribution protocol respectively. Section V puts forward the proposed algorithm of encryption and decryption using Knapsack sequence and quantum key distribution protocol. Section VI mathematically illustrates the encryption and decryption of a plaintext message using the proposed protocol. Section VII focuses on the security issues of the protocol and finally Section VIII concludes the paper.

II. RELATED WORK IN QUANTUM CRYPTOGRAPHY

Bennett et al. [1] first introduced the concept of quantum cryptography and named them as "BB84" after their names Bennett and Brassard respectively. The background of the algorithm was that of the Principle of Uncertainty by Heisenberg. Bennett [2] later suggested a further enhancement to the basic version of "BB84" and named it as "B92". Yang et al. [3] gave a modified form of quantum key exchange protocol using "BB84" and "B92" where they improved the efficiency of the algorithm to 42.9% and the average complexity obtained by them was $O(n^{2.86})$. Houshmand et al. [4] proposed an updated version of Cabello's definition of efficiency of quantum key distribution rules that was used to compare between their procedure and "BB84". Odeh, et al. [5] proposed a modern concept for Quantum Key Distribution (QKD) between three parties in which there was a trusted centre to provide the clients with the vital information to securely transmit between each other. The performance was enhanced by

eliminating redundant rounds of checking the quantum bases and verification. Aldhaheri et al. [6] proposed a scheme that incapacitated the errors in "BB84" and "B92". The session key was exchanged over the quantum channel in their algorithm. Also, the users' verification and privacy was conserved by exchanging of the arbitrary basis and nonce. Gueddana et al. [7] compared BB84 Quantum Key Distribution (QKD) with the optimised version of Quantum Dense Coding.

III. QUANTUM CRYPTOGRAPHY

Quantum cryptography is the branch of cryptography that uses the basic knowledge of physics that is fully secure against being negotiated without the awareness of the sender's or the receiver's messages. The word quantum refers to the most basic comportment of the smallest particles of matter and energy. Based on the concept of quantum physics and the theory of classical information theory Quantum key distribution is built. The distributed key is both public and secret. Quantum key distribution guarantees secrecy of confidential data transmission.

IV. QUANTUM SESSION KEY EXCHANGE PROTOCOL

Here the Sender executes XOR operation on a plain text, say Q with his key αS and sends ($Q \oplus \alpha_S$) to Receiver. Here '⊕' signifies XOR operation. The Receiver then does XOR of ($Q \oplus \alpha_S$) with his key α_R and sends ($Q \oplus \alpha_S \oplus \alpha_R$) to Sender. Sender on receiving the text performs XOR on ($Q \oplus \alpha_S \oplus \alpha_R$) with his key α_S and sends the resulting message ($Q \oplus \alpha_R$) to the Receiver. Receiver computes XOR of ($Q \oplus \alpha_R$) with his key α_R and gets Q from the Sender securely. This method facilitates secure communication among the Sender and the Receiver without sharing their secret keys.

V. ENCRYPTION AND DECRYPTION ALGORITHM

Step 1: Convert the Plain Text to its equivalent binary form, let it be P_T.

Step 2: Using the concept of Knapsack [8] sequence convert P_T to its equivalent decimal form.

Step 3: Convert the decimal form to binary form and apply 1's complement on it.

Step 4: The Sender's text say P_Q has "k" bits that can be represented as an encoded quantum qubit which is defined as $P_Q = |i_1\rangle \otimes |i_2\rangle \otimes |i_3\rangle \otimes \ldots\ldots \otimes |i_j\rangle$, where $\{i_j \mid i_j = \{0 \text{ or } 1\}, j = 1,2,3, \ldots, k\}$ and '⊗' represents a tensor product.

Step 5: The k-bit message is encrypted into "k" qubits and the states of each qubit is rotated by an angle $\Phi(\varphi_i)$where $\varphi_i = \frac{\pi}{2^{i-1}}$ for any constant natural number "k" chosen arbitrarily for each qubit. The angle $\Phi(\varphi_i)$ is the encryption key. As every single qubit has a different angle, this encryption is like the one-time pad key but unlike it in the quantum session key exchange protocol the key is not shared between users.

Step 6: The Sender (S) and the Receiver (R) generates their own secret keys let them be α_S and α_R respectively where $\alpha=\{\Phi(\varphi_i) \mid 0 \leq \Phi(\varphi_i) < \pi, i=1,2, \ldots, k\}$ for every individual session. The session keys are confidential and never disclosed to anyone. With the end of each session the old key gets invalid and a new one is generated to evade hackers from retrieving any information in terms of the session key and/or data.

Step 7: The text will be a qubit and will be encoded as $Q= |0\rangle$. S initiates a key distribution. Now both S and R will create their own session keys $\alpha_S=\varphi_S$ and $\alpha_R=\varphi_R$. S encrypts P_Q with his encryption key α_S.

Step 8: Now S will generate a superposition state and sends the subsequent qubit to R.

Step 9: R will receive the qubit state and will encrypt it with his key α_R.

Step 10: R will now generate a subsequent superposition qubit state and sends it back to S.

Step 11: S decrypts the qubit by inversely rotating it with an angle $(-\varphi_S)$ and sends the subsequent superposition state to R.

Step 12: R will accepts and decrypts it by rotating it with the inverse angle $(-\varphi_R)$ to get Q.

Step 13: R applies 1's complement on Q and converts the subsequent text to its decimal form.

Step 14: R again applies Knapsack sequence and gets the desired plain text P_T.

VI. MATHEMATICAL ANALYSIS OF THE ALGORITHM

Let P_T = 110011.
Let {3, 5, 11, 23, 43, 87} be a super increasing knapsack sequence, and multiply all of the values by a number (n mod m).

Let the modulus be 191 which is greater than the sum of all the numbers in the sequence. Let the multiplier be 53 as it has no factors in common with 191. Then the normal knapsack sequence will be
3 * 53 mod 191 = 159

5 * 53 mod 191 = 74
11 * 53 mod 191 = 10
23 * 53 mod 191 = 73
43 * 53 mod 191 = 178
87 * 53 mod 191 = 27

Therefore, the knapsack is {159, 74, 10, 73, 178, 27}.

Hence, P_T = 110011 = 159+74+178+27 = 438

Now the binary form of 438 is 110110110.
Perform 1's complement of it to get 001001001.

Let P = 001001001. Now the text is a qubit and let it be encoded as P = Q = |0>.

Since each qubit is rotated by an angle $\Phi(\varphi_i)$, the rotation operation takes the form

$$R(\Phi(\varphi_i)) = \begin{pmatrix} \cos\varphi_i & \sin\varphi_i \\ -\sin\varphi_i & \cos\varphi_i \end{pmatrix}$$

Now,

$E_{\alpha_S}[Q]: R(\varphi_S)\ |0> = \begin{pmatrix} \cos\varphi_S & \sin\varphi_S \\ -\sin\varphi_S & \cos\varphi_S \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix}$

$= \begin{pmatrix} \cos\varphi_S \\ -\sin\varphi_S \end{pmatrix}$

$= \cos\varphi_S\ |0> - \sin\varphi_S\ |1>$

$= |\rho'>$, say

S sends $|\rho'>$ to R.

R receives the qubit in $|\rho'>$ and encrypts it with his key α_R.

$E_{\alpha_R}[E_{\alpha_S}[Q]]: R(\varphi_S)\ |\rho'>$

$= \begin{pmatrix} \cos\varphi_R & \sin\varphi_R \\ -\sin\varphi_R & \cos\varphi_R \end{pmatrix}\begin{pmatrix} \cos\varphi_S & \sin\varphi_S \\ -\sin\varphi_S & \cos\varphi_S \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix}$

$= \begin{pmatrix} \cos(\varphi_S+\varphi_R) & \sin(\varphi_S+\varphi_R) \\ -\sin(\varphi_S+\varphi_R) & \cos(\varphi_S+\varphi_R) \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix}$

$= \begin{pmatrix} \cos(\varphi_S+\varphi_R) \\ -\sin(\varphi_S+\varphi_R) \end{pmatrix}$

$= \cos(\varphi_S+\varphi_R)|0> - \sin(\varphi_S+\varphi_R)\ |1>$

$= |\rho''>$, say

R sends it back to S. S decrypts it by rotating it with an angle $(-\varphi_S)$.

S sends this superposition state $|\rho'''>$ to R.

Now,

$D_{\alpha_S}\left[E_{\alpha_R}\left[E_{\alpha_S}[Q]\right]\right] = E_{\alpha_R}[Q]:R(-\varphi_S)\ |\rho''>$

$= \begin{pmatrix} \cos(-\varphi_S) & \sin(-\varphi_S) \\ -\sin(-\varphi_S) & \cos(-\varphi_S) \end{pmatrix}\begin{pmatrix} \cos(\varphi_S+\varphi_R) \\ -\sin(\varphi_S+\varphi_R) \end{pmatrix}$

$= \begin{pmatrix} \cos\varphi_R \\ -\sin\varphi_R \end{pmatrix}$

$= \cos\varphi_R\ |0> - \sin\varphi_R\ |1>$

$= |\rho'''>$

Here D_{α_S} denotes decryption with α_S.

Finally, R accepts and decrypts it by rotating it with $(-\alpha_S)$ to get Q.

$D_{\alpha_R}[E_{\alpha_S}[Q]]: R(-\varphi_R)\ |\rho'''>$

$= \begin{pmatrix} \cos(-\varphi_R) & \sin(-\varphi_R) \\ -\sin(-\varphi_R) & \cos(-\varphi_R) \end{pmatrix}\begin{pmatrix} \cos\varphi_R \\ -\sin\varphi_R \end{pmatrix}$

$= \begin{pmatrix} \cos(0) \\ -\sin(0) \end{pmatrix}$

$= \begin{pmatrix} 1 \\ 0 \end{pmatrix}$

$= |0>$

$= Q$

Perform 1's complement on 001001001 to get 110110110.

The decimal form of 110110110 is 438.

Therefore, P_T =438.

As in this case (n^{-1}) is equal to173.

Therefore,
438 * 173 mod 191 = 138 = 3+5+43+87=110011

The recovered P_T is 110011.

VII. SECURITY

In the algorithm we have applied quantum superposition to avoid the hackers from tampering the text. Since it is difficult in a quantum system to duplicate any quantum state randomly [9] [10], it is impossible for an eavesdropper to break the encrypted data in this superposition states without any error. Eavesdroppers instead of copying the data may try to apply intercept-resend attack but the proposed method also negates that possibility.

Hackers may intercept a qubit tuple in logic zero state before encryption.
The state of the qubit received by him is
$|\rho' >= \cos\varphi \ |0> - \sin\varphi \ |1>$
but φ will remain unknown to the hacker.
As the probability frequency of the qubit are cos(φ) and sin(φ) respectively, therefore if the hacker tries to hack the data in this qubit, he will observe only
|0> with probability $|(\cos\varphi)|^2$ and
|1> with probability $|(\sin\varphi)|^2$.

The algorithm also guarantees the confidentiality of communication as it is tough for the eavesdropper to resend the intercepted data to the Receiver without errors because if he tries to interrupt a qubit in logic one state before it was encoded, the state of the photon received by him is

$$|\rho' >= \sin\varphi \ |0> + \cos\varphi \ |1>$$

The probability of breaking the result by the eavesdropper will be then

$$\frac{1}{2}[|(\cos\varphi)|^2 + |(\sin\varphi)|^2] = \frac{1}{2}$$

for the qubits |0> and |1>.

VIII. CONCLUSION

The paper gives a concept of Quantum Session Key Distribution protocol for Knapsack cryptosystems. The paper combines the encryption technique used in Knapsack sequence with that of quantum key distribution protocol to enhance the security level of the proposed algorithm. The paper also focuses on the security of known and practically possible security breaches. The scope for further research is opened up by the application of quantum superposition of qubit during key distribution.

REFERENCES

[1] C. H. Bennett and G. Brassard, "*Quantum Cryptography: Public Key Distribution and Coin Tossing*", Proceedings of IEEE International Conference on Computers Systems and Signal Processing, Bangalore, India, **December 1984**, pp. **175-179**.

[2] C.H. Bennett, "*Quantum cryptography using any two non-orthogonal states*" Physical Review Letters, **68**, **1992**, pp **3121–3124.**

[3] Ching-Nung Yang and Chen-Chin Kuo, "*Enhanced Quantum Key Distribution Protocols Using BB84 and B92*", **2002**.

[4] M. Houshmand and Khayat. S. Hosseini., "*An Entanglement-base Quantum Key Distribution Protocol*", Information Security and cryptology (ISCISC), 8th International ISC Conference, IEEE, **2011**, pp. **45-48**.

[5] A. Odeh, K. Elleithy, et. al., "*Quantum Key Distribution by Using Public Key Algorithm (RSA)*", London, United Kingdom: third International Conference on Innovative Computing Technology (INTECH), IEEE, **August 2013**.

[6] A. Aldhaheri, K. Elleithy, et. al., "*A Novel Secure Quantum Key Distribution Algorithm*", University of Bridgeport, **2014**.

[7] A. Gueddana and V. Lakshminarayanan, "*Physical Feasibility of QKD based on Probabilistic Quantum Circuits*", IET Information Security, Volume **12**, Issue **6**, **November 2018**, pp. **521 – 526**.

[8] Bruce Schneir (**1996**), "*Applied Cryptography*", John Willey and Sons Inc., New York, USA

[9] W. K. Wootters and W. H. Zurek, "*A single quantum cannot be cloned*," Nature **299**, **1982**, pp. **802-803**.

[10] M. A. Nielsen and I. L. Chuang, "*Quantum Computation and Quantum Information*", Cambridge University Press, Cambridge, London, **2000**.

Authors Profile

Mr. Partha Sarathi Goswami is pursuing his Ph.D.(Engg.) from University of Engineering and Management, Kolkata. He did his graduation (B.Sc., HONS) in Mathematics in 2000, MCA in 2003, M.Phil. in Computer Science in 2007 an d M.Tech. in Computer Science and Engineering in 2010. He is an IBM certified specialist in DB2. He is an Associate Member of the Institute of Engineers, Member of International Association for Engineers and several other organizations. He is currently working as a Lecturer (W.B.G.S.) in Computer Applications at Gaighata Government Polytechnic, Govt. of West Bengal under Department of Technical Education and Training, Govt. of West Bengal. He is in the Department of Technical Education and Training, Govt. of West Bengal for the last 11 years. Previously he has worked as a Lecturer in different

Engineering and Management colleges in India and has also worked as Officer on Special Duty at WBSCVET. He has published several papers in reputed journals and conferences of International and National level. He has also reviewed several research papers and has contributed in a few books also. His research interests include Bio-informatics, Cryptography Algorithms, DNA Cryptography, Quantum Cryptography, Network Security and Computer Graphics. He has more than 16 years of teaching and research experience.

Dr. Tamal Chakraborty is an Assistant Professor, Department of Computer Science at Mrinalini Datta Mahavidyapith, Kolkata. He started his career in the IT Industry with Wipro Technologies, Flextronics Software Systems, IBM India Pvt. Limited and Infosys Technologies. His academic career begun with IEM, Kolkata. Subsequently he taught in University of Gour Banga. He did his B.Sc. (Physics Hons.), B.Tech. (Computer Science and Engineering) and M. Tech. (Computer Engineering and Applications) from Calcutta University and MS from BITS Pilani. He received his Ph.D. from Calcutta University in 2014. He has been presented with numerous awards from professional bodies and academia; including ― Feather in My Cap Award (twice) by Wipro Technologies, Spot Award by Lucent Technologies, Bravo Award & Mentor Award by IBM India Pvt. Ltd. and ― Award of Excellence & Best Teacher in CSE Award by IEM. Dr. Chakraborty is a member of the Computer Society of India. He has authored numerous papers in reputed journals and conferences. His research interests include, Bio-informatics, Programming Languages and Design and Analysis of Algorithms.

Dr. Abir Chattopadhyay did his master's degree on solid state electronics from Jadavpur University in the year 1988. He has a Ph.D. degree in low temperature electronics from Jadavpur University. He mainly concentrated on implementation of Hartee-Fock Potential in place of Max Born Potential. In this time the group in which Dr. Chattopadhyay was a scholar has got a Research Project form Department of Electronics, Govt. of India. In 2001, Dr. Chattopadhyay had gone to National University of Singapore and also Nanyang Technological Institute (NTU) for a collaborative Research work. Dr. Chattopadhyay was also a recipient of CSIR Fellowship for attending seminars/workshops in Prague, Czechoslovakia. He has worked at the Advanced Centre of Cryogenic Research as a junior scientific officer. Previously he had been associated with many reputed colleges and universities. Presently he is working as a Professor and Dean Research at the University of Engineering and Management, Kolkata.

