International Journal of Chemical, Materials and Biomolecular Sciences
ISSN: 2415-6620
Vol:12, No:12, 2018

An Authentication Protocol for Quantum Enabled Mobile Devices

Natarajan Venkatachalam, Subrahmanya V. R. K. Rao, Vijay Karthikeyan Dhandapani, Swaminathan Saravanavel

***Abstract*—**The quantum communication technology is an evolving design which connects multiple quantum enabled devices to internet for secret communication or sensitive information exchange. In future, the number of these compact quantum enabled devices will increase immensely making them an integral part of present communication systems. Therefore, safety and security of such devices is also a major concern for us. To ensure the customer sensitive information will not be eavesdropped or deciphered, we need a strong authentications and encryption mechanism. In this paper, we propose a mutual authentication scheme between these smart quantum devices and server based on the secure exchange of information through quantum channel which gives better solutions for symmetric key exchange issues. An important part of this work is to propose a secure mutual authentication protocol over the quantum channel. We show that our approach offers robust authentication protocol and further our solution is lightweight, scalable, cost-effective with optimized computational processing overheads.

***Keywords*—**Quantum cryptography, quantum key distribution, wireless quantum communication, authentication protocol, quantum enabled device, trusted third party.

I. Introduction

QUANTUM cryptography is an active area of research and development that spreads the use of quantum key distribution technology in a larger scale. Modern quantum communication technology [1] enables novel key exchange capabilities such as software defined quantum information distribution that cannot be offered by the existing communication channels [10], [12].

The design of commercial quantum communication channel is an important step towards realizing the theoretically proven unconditionally secure quantum computing technologies. In particular, software defined contactless quantum communication will become the next generation secret communication medium which minimize the negative effects of the classical key exchange techniques. The implementation of software defined quantum key exchange [2], [7], [10] have proven useful for providing flexibility in the design and integration with the conventional crypto systems. In this research work we extend the wireless quantum information exchange paradigm in to the design and development of quantum crypto systems.

Natarajan Venkatachalam, Subrahmanya V. R. K. Rao, Vijay Karthikeyan Dhandapani and Swaminathan Saravanavel are associated with the Global Technology Office, Cognizant Technology Solutions India Private Limited, Chennai, India (e-mail: Natarajan.v4@cognizant.com, SubrahmanyaVRK.Rao@cognizant.com, VijayKarthikeyan.Dhandapani@cognizant.com, Swaminathan.S2@cognizant.com).

Quantum key distribution utilizes the basic principles of quantum physics and security relies on the fact that observation causes perturbation. The advantage of the quantum crypto system is completely independent of the traditional mathematical computing capability of adversary. In the Quantum key exchange two legitimate parties i.e., Sender and Receiver can share a secure private key under the quantum communication channel as a qubits using the properties of photonic carriers. The main power of the quantum channel is that if these communication channels are eavesdropped then the receiver can observe the state changes in the qubits. In addition, the prior established authenticated classical channel provides the post processing and key distillation to finalize and agree the secret key between sender and receiver.

Section II gives a short introduction to secure quantum communication. Basic principles and QKD and its support to key exchange are discussed. Section III describes the proposed mutual authentication protocol in greater details. Section IV then builds upon the security and performance analysis. The last section summaries the work and outlines possible further enhancements.

II. Analysis of Software Defined Quantum Key Distribution

This section briefs a conceptual overview of software defined wireless QKD system [5] and gives brief outline of the private key exchange procedures and objectives. This followed by a short note about the wireless QKD system design and its construction details [1]. The QKD system consists of three components: key exchange, key sifting and key distillation. Software component controls both Sender and Receiver and is capable of executing commands that results in operations related to quantum information exchange.

Key Exchange: The qubits which are sent by Sender to Receiver through quantum channel constitutes the quantum raw key(photons).

Key Sifting: The quantum raw key then undergoes the sifting process in which photonic carrier with same bases are filtered and rest of the photons are discarded thus, results in a sifted key.

Key distillation: The sifted key will be abundant in errors which are generated either by an eavesdropper or due to imperfections in the QKD device and transmission channel. Key distillation comprise mainly of error correction and privacy amplification.

Error correction or Reconciliation: This is a process where Sender and Receiver with a given sifted key agree

a common sequence. Initially the sifted key is divided into blocks, after that parity bits are calculated and compared. If the results does not match then the error identified and corrected using binary search algorithm, however this process continues till Sender and Receiver have identical quantum secret keys. The process of error correction is accompanied by leakage of information due to continuous interaction hence further security is provided by privacy amplification. The reconciled key is further processed to final key by compressing the key to an appropriate factor. This process decreases the chance of Eavesdropping and enhances the security of the private key.

A. QKD Architecture Overview

The software defined wireless quantum communication framework by considering a single Sender and Receiver with quantum enabled communication channel [4]. A functional decomposition of QKD system is shown in Fig. 1.

The QKD system uses the design of polarization encoding and decoy state protocol, as well as a synchronization scheme of sync-light involving Sender and Receiver. The system needs two kinds of wireless communication channels, one is classical channel used for the transmission of cipher-text data and quantum key related meta data; the other is the individual channel used for quantum key transmission. The secret key constructors of two parties converts the qubits into binary code according to the key sifting rule of negotiation by using different basis [8], [11]. Using the quantum encryption method, the plain text data and the other sensitive information are encrypted using secret key, and transmitted over the classical channel. At the receiver end, decryption method can decrypt the received cipher text us the secret key which has been synchronized.

B. Wireless Quantum Communication Channel

In the basic model of quantum secure communication ecosystem, the photons emitted by Sender is used as a medium for building up the quantum communication channel. Specially, wireless QKD method is to setup a communication channel between Sender and Receiver, which will be an unconditionally secure stealthy channel. The private key exchange between Sender and Receiver only be in the QKD channel.

C. Application scenario

Quantum technology is in the development stage, many of the quantum applications are not fully matured. The power of the quantum communications yet to be utilized fully by industry [3], [9]. The secure software quantum communication technology is developing rapidly. Considering the future demand and the security needs in e-commerce industries are forced to move away from traditional systems and the secure quantum technology can be alternative for them. The usage of quantum communication technology in Power sector and in the field of Communications can significantly improve the safety and security of power grid operations [6].

III. Proposed Mutual Authentication Protocol Using Wireless QKD Channel

Our main idea is to design a light weight secure electronic authentication protocol to protect communication device and servers against the cyber-attacks. Quantum Cryptography is the main mechanism that should be used to protect sensitive informations and crypto keys. In the case of contactless IoT device communication ecosystem, the physical device is replaced by which the secure quantum communication device emulates the classical IoT device and stores the user data into the server.

A. Mapping of Roles

This section explores how the mutual quantum device authentication protocol can be implemented. At first, we focus on the overall architecture of the solution. Further, it goes into details about the authentication, certificate and key exchange.

Quantum enabled device: Quantum information Sender is represented by a quantum enabled software defined smart device/ quantum Device.

Server Terminal: For the sake of simplicity of the implementation, the server permanently connected to the quantum receiver and the central server. The main difference is that in mutual quantum device authentication method, the communication between the quantum smart device and server is contact less secure quantum communication. Even though the conditions would be different in a real world implementation, we believe that this communication is done over a fast channel, so the speed difference in the protocol execution would be small. Data stored into the sender and receiver could be managed by central control systems and different applications can be executed using these devices.

B. Registration Phase

Server and the trusted third party (TTP) should register and obtain certificates from the certification authority before they communicate. Quantum device should register and obtain a unique device id from the TTP before the device involve in the secure quantum communication protocol.

C. Authentication Phase

We describe our proposed solution which aims to provide a secure quantum solution, Our solution aims to prevent the security attacks that are related to secret key exchange in traditional crypto systems.

Our solution makes use of certificate based authentication between server terminal (ST) and TTP and of shared quantum secret key authentication between the server terminal and device. The secret key shared between the server and the user device is securely stored in quantum environment and that the key computation performed inside the quantum device. In addition, these quantum devices offer good tamper-resistance and can mutually authenticate the TTP, quantum device and the server terminal in our protocol as described below:

Step1: The server sends its certificate and a random value to the quantum device ($Cert_{ST}$,RV_{ST}) through classical channel.

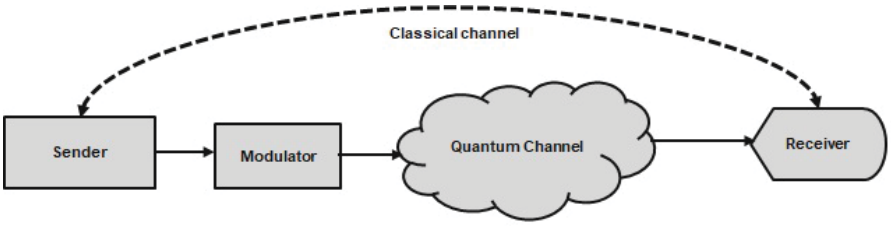

Fig. 1 Functional decomposition of secure quantum communication system consisting of a single sender-receiver pair

Step2: The customer device generates a random value RV_{CD} and generates quantum secret key QSK and symmetrically encrypts concatenation of $RV_{ST,QD}$, Quantum device ID and $Cert_{ST}$ using QSK. Customer device sends the encrypted value F to server through classical channel and the QSK will be transmitted using wireless quantum channel.
Step3: Server forwards encrypted value F and QSK to TTP.
Step4: TTP verifies the server certificate and then symmetrically decrypt F using the received QSK. Then, the TTP encrypts the concatenation of QSK and RV_{QD} using public key (Pub_{ST})and send E to server.
Step5: Upon receipt of E, the ST asymmetrically decrypts it using its private key(Pr_{ST}) by computing AsymD(E,Pr_{ST}). Next, ST symmetrically encrypts RV_{QD} using QSK and sends the encrypted value to customer device which symmetrically decrypts it and compares it for equality to the random value initially generated. If the two values are equal, then the server terminal is authenticated.

Once the authentication is successful, both Quantum device and server compute an encryption key that is derived from QSK in order to encrypt subsequent financial transactions.

IV. Security and Performance Analysis

In this section, we did an informal analysis our authentication scheme, in particular we demonstrate that it is resilient against all known attacks over public channel and quantum channel. Obviously, the QKD system is provably secure and it is fundamentally mathematical procedure and the security of the system is heavily depending on the laws of quantum physics. So our focus is mainly analyze the security of mutual authentication protocol.

A. Anonymity and Un-Traceability

In the present scheme, on the user device side there is no identity notations transmitted in the classical communication channel or stored in the quantum device. Suppose that, the adversary can capture the encrypted messages from the open channel - in order to obtain the device identity, the attacker needs to know QSK and random variable, which is not available since the quantum secret key (QSK) is computed using photonic process and transmitted through the quantum channel. Moreover, according to quantum theory, it is very difficult for adversary to guess the correct QSK. Further, even if attacker obtains the user device and extracts the information in the device, adversary cannot recover the device ID and user information since it is protected by the one-way hash function. In the process of mutual authentication, adversary has no ability to trace the users sensitive information as every transmitted data is different and does not reveal any meta information about user. Therefore, the proposed authentication protocols ensures the device anonymity and un-traceability.

B. Man-In-The-Middle Attack

The attacker can capture the authentication request message F and the information stored in the device. In order to perform man-in-the-middle attack, adversary needs to compute F* for sending to server terminal. Although attacker chooses a random variable RV*ST , still attacker cannot know the value of N and the real identity of the user, he cannot compute the F*. On the other hand, according to Heisenberg uncertainty principle, it is very difficult for adversary to copy the state of the qubit and thus he/she has measure it order to get a state of the qubit. Also the eavesdropping the quantum channel will generate the errors, so server can easily discard those error bits and request transmitter or user device for retransmission. Thus the attacker does have any ability to modify the quantum secret bits or the encrypted information in the classical communication channel. As a result, our proposed scheme resists the main-in-the-middle attack.

C. Denial of Service

Adversary can disrupt the photonic carries in the quantum channel by either applying simple clocking line or some unitary methods. But the attacker cannot gain any information in the process by hampers the quantum key distribution between the user device and server.

D. Pre-Verification in the Quantum Device

While in the authentication initiation phase, the device check the validity of the certificate after inputting the device ID. If it is found valid, then the device send the encrypted message to the Server. Otherwise, if declines the sessions until correct certificate and device ID are entered. This implies that in the present authentication protocol, we can save the computational cost when there exists incorrect input or illegal user entry.

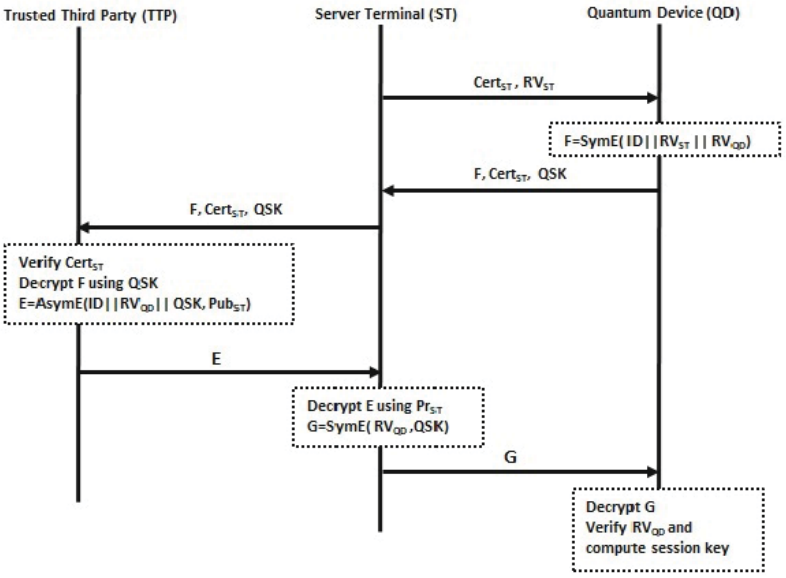

Fig. 2 Shared quantum secret and certificate based authentication protocol

E. Mutual Authentication

In this scheme, device firstly checks the validity of certificate. Afterwards, TTP authenticates user device by verifying device, server certificate and secret key. On other hand, user device authenticates the server RV_{QD}=RV^{*}_{QD}

F. Performance Analysis

The performance of the present scheme is analyzed in terms of source code size, communication cost and QKD response time. Overall computation cost of a scheme is estimated according to all the computations required in the protocol. The time complexity is estimated using the elapsed time when executing the QKD process and one round of authentication. The proposed method takes $2T_{\mathrm{SE}} + 3T_{\mathrm{QKD\_ops}} + 2T_{\mathrm{Err\_cor}} + 2T_{\mathrm{SD}} + 1T_{\mathrm{SG}} + 1T_{\mathrm{SV}}$. The computational cost of modular multiplication and XOR can be ignored. It is clear that our scheme reduces the computation time and cost greatly by using symmetric quantum cryptography for QKD distribution. Also the asymmetric key operations are executed on either the Server terminal or the TTP, due to the computational limitations in the quantum device.

T_{SE} : the time for performing symmetric key encryption

$T_{\mathrm{QKD\_ops}}$: the time for performing the QKD operations

$T_{\mathrm{Err\_cor}}$: the time for performing error correction operations

T_{SD} : the time for performing symmetric key decryption

T_{SG} : the time for performing digital signature generation operation

T_{SV} : the time for performing digital signature verification operations

The proposed solution can be easily extended to secure the secret key from attacker and customer confidential information from the eavesdropper. From this end, the quantum device and the TTP can establish probabilistically unobservable communication channel to remove the existing communication link between these to entities.

V. Conclusions and Future Works

The proposed mutual authentication technique incorporates both classical cryptographic protocol and wireless quantum key distribution by reducing the computational cost and enhancing the data security. It is relatively more secure than the conventional communication system. Hence the proposed quantum enabled device authentication technique provides unconditional security and better performance. In comparison with the traditional authentication schemes, we conclude that the proposed protocol is more secure and effective to be implemented in real-life scenarios. Our future work will design a more secure multi factor authentication protocol based on the QKD system to be implemented in many practical application scenarios.

References

[1] Bennett, C. H., Bessette, F., Brassard, G., Salvail, L. and Smolin, J., 1992. Experimental quantum cryptography. Journal of cryptology, 5(1), pp. 3-28.

[2] Cao, Y., Zhao, Y., Colman-Meixner, C., Yu, X. and Zhang, J., 2017. Key on demand (KoD) for software-defined optical networks secured by quantum key distribution (QKD). Optics express, 25(22), pp.26453-26467.

[3] Diamanti, E., Lo, H. K., Qi, B. and Yuan, Z., 2016. Practical challenges in quantum key distribution. npj Quantum Information, 2, p.16025.

[4] Hwang, T., Lee, K. C. and Li, C. M., 2007. Provably secure three-party authenticated quantum key distribution protocols. IEEE Transactions on Dependable and Secure Computing, 4(1).

[5] Humble, T. S. and Sadlier, R. J., 2014. Software-defined quantum communication systems. Optical Engineering, 53(8), p. 086103.

[6] Junwen, L., Ziyan, Z. and Jiakai, H., 2017, February. The application of quantum communication technology used in electric power information & communication system confidential transmission. In Advanced Communication Technology (ICACT), 2017 19th International Conference on (pp. 305-308). IEEE.

[7] Schmitt-Manderbach, T., Weier, H., Frst, M., Ursin, R., Tiefenbacher, F., Scheidl, T., Perdigues, J., Sodnik, Z., Kurtsiefer, C., Rarity, J. G. and Zeilinger, A., 2007. Experimental demonstration of free-space decoy-state quantum key distribution over 144 km. Physical Review Letters, 98(1), p. 010504.
[8] Slater, J. A., Branciard, C., Brunner, N. and Tittel, W., 2014. Device-dependent and device-independent quantum key distribution without a shared reference frame. New Journal of Physics, 16(4), p. 043002.
[9] Stucki, D., Legre, M., Buntschu, F., Clausen, B., Felber, N., Gisin, N., Henzen, L., Junod, P., Litzistorf, G., Monbaron, P. and Monat, L., 2011. Long-term performance of the SwissQuantum quantum key distribution network in a field environment. New Journal of Physics, 13(12), p. 123001.
[10] Vallone, G., DAmbrosio, V., Sponselli, A., Slussarenko, S., Marrucci, L., Sciarrino, F. and Villoresi, P., 2014. Free-space quantum key distribution by rotation-invariant twisted photons. Physical review letters, 113(6), p. 060503.
[11] Wang, F., Zhang, P., Wang, X. and Li, F., 2016. Valid conditions of the reference-frame-independent quantum key distribution. Physical Review A, 94(6), p. 062330.
[12] Zhang, H. F., Wang, J., Cui, K., Luo, C. L., Lin, S. Z., Zhou, L., Liang, H., Chen, T. Y., Chen, K. and Pan, J. W., 2012. A real-time QKD system based on FPGA. Journal of Lightwave Technology, 30(20), pp. 3226-3234.