Cyber Security Lab II - Experimental authentication of quantum key distribution with post-quantum cryptography

Bhardwaj Aditya[1]

[1]Department of Informatics, Eötvös Loránd University

June 10, 2023

Abstract

As part of the subject Cyber Security Lab II 2023, I have been asked to go through the paper titled Experimental authentication of quantum key distribution with post-quantum cryptography [2]. I am required to understand the involved concepts. I should be able to present the same in a way that is simple and straightforward while not losing the underlying idea. The paper discusses the use of Post-Quantum Cryptography (PQC) and Public-Key Infrastructure (PKI) as a more efficient and secure method for authentication in quantum key distribution (QKD) networks, highlighting the experimental verification of its feasibility and potential advantages for network expansion and quantum-safe communication. Over the next few weeks, I will study the paper, gather prerequisite knowledge and break it down. This will help fellow students and teachers to understand the mentioned paper in an easier and faster way. The main aim is to encourage research and develop interest in the field of Quantum Cryptography and PQC.

1 Main points

The first step is to infer the main idea from the text of the paper. I have listed the main points in a simple way that describes the essence of the paper.

1. **QKD and Security**: QKD can offer information-theoretically secure key exchange, even in the presence of quantum computers. This implies that QKD provides a strong level of security against potential attacks from quantum computers.

2. **Authentication Requirement for QKD**: QKD requires the classical channel to be authenticated to ensure secure communication. Currently, symmetric keys are used for authentication, and the text mentions that a large number of symmetric key pairs are required for a QKD network with n users (specifically $C_n^2 = n(n\text{-}1)/2$ pairs).

3. **Potential Solution – PQC and PKI**: The paper suggests that using a mature Public Key Infrastructure (PKI) and post-quantum cryptography (PQC) with quantum-resistant security can provide an alternative approach to authentication in QKD networks.

4. **Efficient and Secure Authentication**: With the help of PQC and PKI, each user in the QKD network only needs to apply for one digital certificate from a certificate authority (CA) for efficient and secure authentication. This implies that a single digital certificate can be used to authenticate multiple users, reducing the number of symmetric keys required.

5. **Short-Term Security and Long-Term Key Security**: The paper mentions that assuming short-term security of the PQC algorithm can achieve long-term security of the distributed keys. This suggests that by periodically updating the PQC algorithm, the security of the distributed keys can be maintained over time. The feasibility, efficiency, and stability of the PQC algorithm in QKD authentication have been experimentally verified. This indicates that practical experiments have been conducted to validate the proposed approach.

6. **Advantages for Network Expansion**: The paper highlights the advantages of using PQC authentication when new users join the QKD network. This implies that the proposed approach can easily accommodate network expansion and the inclusion of additional users.
7. **Trust in Certificate Authority (CA)**: By using PQC public-key infrastructure, the nodes in the QKD network need to trust only the CA to authenticate each other. This suggests that trust in the CA is crucial for ensuring the overall security of the QKD network.
8. **Application Prospects of Quantum-Safe Communication**: The paper concludes by stating that the combination of QKD with PQC authentication will significantly promote and extend the application prospects of quantum-safe communication. This suggests that the proposed approach has the potential to enhance the adoption of secure communication methods in the quantum era.

2 Progress

Here I will update the work done every week.

2.1 Week-I

After listing the main points, I moved on to studying the basic concepts required for understanding the paper. I have created a document namely `CS-Lab-Notes-Knowledge.docx`, which will be shared with the teacher. I have tried to include the major concepts and information that the reader may need to know beforehand. It is not exhaustive in nature but I will keep updating it as I progress forward.

For the upcoming week: Study the remaining concepts. It includes BB84 protocol and SM3 hash algorithm. The authors have introduced a PQC digital signature algorithm called `Aigis.Sig`. I will go through the paper in more detail and try to understand these topics.

2.2 Week-II and III

I went through the topics of BB84 protocol, decoy state, SM3 hash algorithm and started reading the paper which explains the `Aigis.Sig` [3] scheme in detail. There is some prerequisite knowledge required in order to understand the implementation of the algorithm. I updated the same in the document `CS-Lab-Notes-Knowledge.docx`. Related algorithms are present in the [1] paper.

For the upcoming week: I will focus solely on the construction and design of the `Aigis.Sig` algorithm. The papers [3] and [1] should be helpful. A separate section in the knowledge document is kept for details/text related to the signature scheme. I may add the same to this LaTex document as it is an important section.

2.3 Week IV

I focused on the design of the signature scheme and was able to understand the algorithms in more detail. I was also able to point out the mathematical structures being used in the construction.

I have made a separate document `Aigis-Sig signature scheme.pdf` and have went through each line of the algorithms and added hand-written explanations for the same.

References

[1] L. Ducas, E. Kiltz, T. Lepoint, V. Lyubashevsky, P. Schwabe, G. Seiler, and D. Stehlé. Crystals-dilithium: A lattice-based digital signature scheme. *IACR Trans. Cryptogr. Hardw. Embed. Syst.*, 2018:238–268, 2018.

[2] W. Liu-Jun, Z. Kai-Yi, W. Jia-Yong, C. Jie, Y. Yong-Hua, T. Shi-Biao, Y. Di, T. Yan-Lin, L. Zhen, Y. Yu, Z. Qiang, and P. Jian-Wei. Experimental authentication of quantum key distribution with post-quantum cryptography, 2020.

[3] J. Zhang, Y. Yu, S. Fan, Z. Zhang, and K. Yang. Tweaking the asymmetry of asymmetric-key cryptography on lattices: Kems and signatures of smaller sizes. In A. Kiayias, M. Kohlweiss, P. Wallden, and V. Zikas, editors, *Public-Key Cryptography – PKC 2020*, pages 37–65, Cham, 2020. Springer International Publishing.