International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-9 Issue-2, December, 2019

Hybrid Solution (ECDHE + NewHope) for PQ Transition

Kunal Meher, Divya Midhunchakkaravarthy

Abstract*: *It is assumed that certain mathematical or computational problems which are used in traditional cryptographic schemes are hard to solve for an attacker using today's computers. But, lots of companies are trying to build quantum computer and in coming few years commercial quantum computer will be in reality. Security of traditional asymmetric cryptographic algorithms can be broken using quantum computers. So, researchers all over the world are planning for transition to post-quantum cryptography. One solution is to build hybrid solution combining both traditional and post-quantum primitives which will provide traditional cryptographic guarantees as well as quantum resistance [1].The best and feasible hybrid solution can be used in the protocols like SSL/TLS, SSH and PGP.

Keywords* : *quantum, hybrid, cryptography, PQC

I. INTRODUCTION

Post-quantum cryptography (PQC) deals with cryptographic primitives and algorithms those are secure against an attack by a quantum computer. Widely used asymmetric cryptographic algorithms such as RSA and Diffie-Hellman are not secure against quantum computer. The quantum computer is no more theoretical but is actually in practice. Post-quantum cryptography (PQC) is used for quantum-resistant. Lattice-based cryptography is one of the types of PQC. Learning with Errors (LWE), Ring Learning with Errors (Ring-LWE), and Module Learning with Errors (Module-LWE) are the mathematical hard problems in lattice-based cryptography. NewHope is one of the Ring-LWE lattice-based cryptographic primitive which is designed to be quantum-resistant.

In this paper a lattice-based OQS project PyNewHope is tested. PyNewHope is an experimental python implementation of the NewHope quantum-safe key-exchange cryptographic scheme. PyNewHope is based on C implementation available in liboqs repository and duplicates much of the functionality of it [2].

We can get a hybrid solution by combining one of the traditional key exchange algorithms and one of the PQ algorithms. In this paper, a hybrid solution is formed by combining two independent key exchange algorithms ECDHE and NewHope. ECDHE stands for Elliptic Curve Diffie-Hellman Ephemeral and is a key exchange mechanism based on elliptic curves. This algorithm provides perfect forward secrecy in SSL.

II. MOTIVATION

There are two popular public key cryptosystems such as RSA and Diffie-Hellman (DH) key exchange protocol. RSA is based on the difficulty of Integer Factorization Problem (IFP) and Diffie-Hellman is based on the difficulty of Discrete Logarithm Problem (DLP). However, IFP and DLP can be solved within the polynomial time by Shor's algorithm using a quantum computer. Block cipher such as AES and DES can be solved using Grover's algorithm. Grover's algorithm can use data search problem. In classical computer, adversary can search database as O (2n) complexity. Using the quantum computer, the complexity of data search problem reduces just O ($\sqrt{2}$n) Therefore, current cryptosystems must be replaced by the quantum resistance cryptosystems. Lattice-based cryptography is used for an encryption scheme, signature, and key exchange protocol [3].

III. OUTLINE OF THE PAPER

In this paper, we test performance evaluation such as payload and runtime of three types of algorithm:

1. ECDHE - Classical asymmetric key exchange protocol.
2. NewHope - Lattice based Ring-LWE key exchange protocol for quantum resistance.
3. Hybrid solution - RLWE-NEWHOPE-ECDHE.

IV. BACKGROUND

A hybrid scheme is a combination of a traditional and a post-quantum scheme. The resulting scheme is at least as secure as one of the schemes used. In the example of key exchange, this would translate into performing two independent key exchanges, one with a traditional scheme like ECDHE and one with a post-quantum scheme like NreHope. The two resulting keys are then combined (e.g. with an XOR operation) to create the final secret key that is used for encryption and decryption.Now, imagine what would happen if strong quantum computers come into widespread use and ECDHE becomes insecure. The security of the key would remain as strong as that of the quantum key exchange scheme that was used, and it could therefore still be used and considered secure. On the other hand, if the chosen post-quantum scheme was proven to be faulty or to contain errors, the security of the exchanged key would be reduced to that of ECDHE, which is still what is considered secure today. The use of hybrid schemes can therefore protect against more types of future

Revised Manuscript Received on December 30, 2019.
* Correspondence Author
Kunal Meher*, Lincoln University College, Malaysia.
Divya Midhunchakkaravarthy, Lincoln University College, Malaysia.

dangers and threats. It is highly recommended in order to ease the transition into the post-quantum era [4].

V. METHODOLOGY

In this paper, the performance of ECDHE algorithm, NewHope algorithm and Hybrid solution (ECDHE + NewHope) are compared. The parameters compared are payload and runtime. Python packages - cryptography and pynewhope are used for ECDHE and NewHope respectively. For the secure communication between two parties (Alice and Bob) , the key generation time and shared key generation time are measured for ECDHE algorithm, NewHope algorithm and hybrid solution.

In case of hybrid solution, XORing of shared key generated by ECDHE and NewHope is used to derive the shared key used for encryption and decryption [5].

VI. RESULT

1. Length of Payload in ECDHE = 430 bytes; It uses HMAC based KDF to derive 32 bytes key from 48 bytes.
2. Length of Payload in NewHope = 3872 bytes, Key Size = 32 bytes
3. Length of Payload in Hybrid Solution = 4302 bytes, Key Size = 32 bytes

The performance evaluation is done in various environments as shown in the Table I, Table II and Table III:

Table-I: Intel Pentium P6100 2GHz, 3GB RAM, Windows 7

Algorithm	Key Generation Time (s)		Shared Key Generation Time (s)		Total Time (s)
	Alice	Bob	Alice	Bob	
ECDHE	0.312	0.312	0.0156	0.0156	0.3856
NewHope	0.1716	-	0.078	0.2808	0.5324
Hybrid	0.468	0.296	0.093	0.312	0.608

Table-II: Intel Core i3-2120 3.3GHz, 2GB RAM, Windows 7

Algorithm	Key Generation Time (s)		Shared Key Generation Time (s)		Total Time (s)
	Alice	Bob	Alice	Bob	
ECDHE	0.0624	0.078	0.0	0.0155	0.1559
NewHope	0.0311	-	0.015	0.078	0.1246
Hybrid	0.0936	0.062	0.031	0.078	0.2652

Table-III: Intel Core i3-7100 3.90GHz, 12GB RAM, Windows 10

Algorithm	Key Generation Time (s)		Shared Key Generation Time (s)		Total Time (s)
	Alice	Bob	Alice	Bob	
ECDHE	0.0469	0.0468	0.0	0.0	0.0937
NewHope	0.0156	-	0.0156	0.0468	0.078
Hybrid	0.0625	0.0312	0.0155	0.0468	0.156

VII. CONCLUSION

It can be concluded the total time to generate shared key for encryption in Hybrid solution is approximately addition of time required in ECDHE and NewHope algorithm. It is also CPU and RAM dependent. As we use high efficient CPU or more RAM size total time required for key establishment decreases. The other hybrid cases involving other traditional primitives and PQC primitives can also be evaluated.

REFERENCES

1. Brian A. LaMacchia, “Getting Ready for the Post-Quantum Transition”, by Microsoft Utimaco Webinar, May-2019.
2. PyNewHope. [Online]. Available:
3. https://pypi.org/project/PyNewHope/
4. Hyeongcheol An, Rakyong Choi, Jeeun Lee and Kwangjo Kim, “Performance Evaluation of liboqs in Open Quantum Safe Project (Part I)", Symposium on Cryptography and Information Security Niigata, Japan, 2018, PP 1-7.
5. White Paper on Post-Quantum Cryptography, MTG.
6. Eric Crockett, Christian Paquin, and Douglas Stebila, “Prototyping post-quantum and hybrid key exchange and authentication in TLS and SSH”, 2019.

AUTHORS PROFILE

Kunal Meher has finished his masters in Computer Engineering. He is currently pursing Ph.D in Lincoln University College, Malaysia. He has subject expertise in networking and security. Currently, he is working on the area of Post Quantum Cryptography. He has total 15 years teaching and industrial experience.

Dr. Divya Midhunchakkaravarthy is an Associate Professor in Lincoln University College, Malaysia with 11 years of teaching and research experience. She received Doctorate of Philosophy in Computer Science from Avinashilingam University, India. Her research specialisation is network technology, cyber security and integrated security for cloud and Big Data. She has published a good number article in various scopus journals and also published book chapters.