NEW APPROACH TO COMBINE SECRET KEYS FOR POST-QUANTUM (PQ) TRANSITION

Kunal Meher
Research Scholar at Lincoln University College, Malaysia and Assistant Professor at Xavier Institute of Engineering, Mumbai.
kunalmeher@gmail.com

Divya Midhunchakkaravarthy
Associate Professor in Lincoln University College, Malaysia
divya@lincoln.edu.my

Abstract

Many companies are working to build a powerful quantum computer. Once quantum computer with large qubits is reality, asymmetric-key cryptosystem will be vulnerable for Shor's algorithm. The transition from one cryptosystem to another is very slow process and consumes many years. National Institute of Standards and Technology (NIST) is working on standardization of post-quantum cryptographic (PQC) algorithms. Security of current PQC algorithms cannot be fully verified today. So, in coming years we need to rely on both traditional algorithms and PQC algorithms. Hybrid mode consisting of one traditional algorithm and one post quantum algorithm is a best solution for smooth migration to quantum-safe cryptosystem. For key exchange, it means using two or more key exchange encapsulation algorithms for generating session key [Meher and Midhunchakkaravarthy (2019)]. For authentication, it means using two or more digital signature algorithms [Meher and Midhunchakkaravarthy (2019)]. There are number of approaches to combine secret key from traditional algorithm and PQC algorithm to make key encapsulation mechanism quantum-proof. In the paper we propose a new approach of using secret master key generated from one of the KEM algorithm as a salt for hash-based key derivation function (HKDF) to drive session keys from secret master key generated from another KEM algorithm.

***Keywords*:** PQC; HKDF; Hybrid; KEM

1. Introduction

There are three operations that use public key cryptography: encryption, key establishment and digital signatures. Within key establishment, there are two common methods: key agreement and key transport. With advance in quantum computer all these operations which uses asymmetric-key will be vulnerable. There is need of post quantum cryptographic asymmetric-key algorithms. Given that the NIST will take some years for PQC standardization, there are essentially two viable options to handle this problem:

1.1 Hybrid Scheme

A hybrid scheme is a combination of a traditional and a post-quantum scheme, meaning that the resulting scheme is at least as secure as one of the schemes used. The use of hybrid schemes can protect against more types of future dangers and threats. It is highly recommended in order to ease the transition into the post-quantum era.
For instance, Google experimented with using a hybrid of an Elliptic Curve key agreement along with a Ring Learning with Errors key agreement into the Google Chrome Canary browser.

1.2 Protective Measures for Pre-Quantum Cryptography

The second option is to employ the conceptionally easy, but organizationally complicated measure of mixing pre-shared keys into all keys established via public-key cryptography. The users who do not want to deploy PQC primitives before standardization can protect their systems by including retained shared secret data in the key derivation, in addition to the key material obtained by a public key operation [3].

2. Implementation of Hybrid Scheme for PQ transition

The main objective of hybrid mode is the required security attributes remain intact provided one of ingredient schemes remains safeguard.

2.1 Hybrid key exchange (Hybrid KEM)

It means that the session key should remain secure (and thus application data confidential) as long as one of the ingredient key exchange mechanisms is unbroken. In this paper, number of approaches for the hybrid key exchange is discussed and a new approach is proposed.

2.2 Hybrid digital signature

It means that the protocol should provide secure authentication as long as one of the digital signatures schemes is unbroken at the time of session establishment.
Two signatures are formed from the message (M) to be authenticated – one using traditional signature algorithm and another using post-quantum signature algorithm as follows:
s1 = traditional_signing(M) and s2 = PQ_signing(M).
The message (M) and signatures (s1 & s2) are sent to receiver where both signatures are verified. Only if both signatures are verified message is accepted as authenticate message.

2.3 Hybrid encryption

It means that the encrypted message remains secure as long as one of the encryption algorithms remains secure. There are two approaches possible for hybrid encryption to encrypt plaintext (PT) to get ciphertext (CT):
• CT = Traditional_Encryption(PQ_Encryption(PT))
• CT = PQ_Encryption(Traditional_Encryption(PT))

3. Hash-based Key Derivation Function (HKDF)

HKDF is a simple key derivation function (KDF) based on a hash-based message authentication code (HMAC). The main approach HKDF follows is the “extract-then-expand” paradigm. It logically consists of two stages. In the first stage it takes potentially weak input keying material (IKM) and an optional salt (acting as a key), then extracts from it a fixed-length pseudorandom key using an HMAC (e.g. SHA-256). The extraction step is used to smooth the entropy in some key material like a Diffie-Hellman key. In the second stage expands this key into several additional pseudorandom keys which is cryptographically strong output key material (OKM) [4] [Fischlin M., et al (2018)]. In the paper, we have ignored info field or considered as NULL.

First Step: HKDF-Extract(extsalt, IKM) = HMAC(extsalt, IKM) -> PRK (Pseudo Random Key)
Second Step: HKDF-Expand(PRK, info, len) -> k (k1 || k2 || k3 ……..)

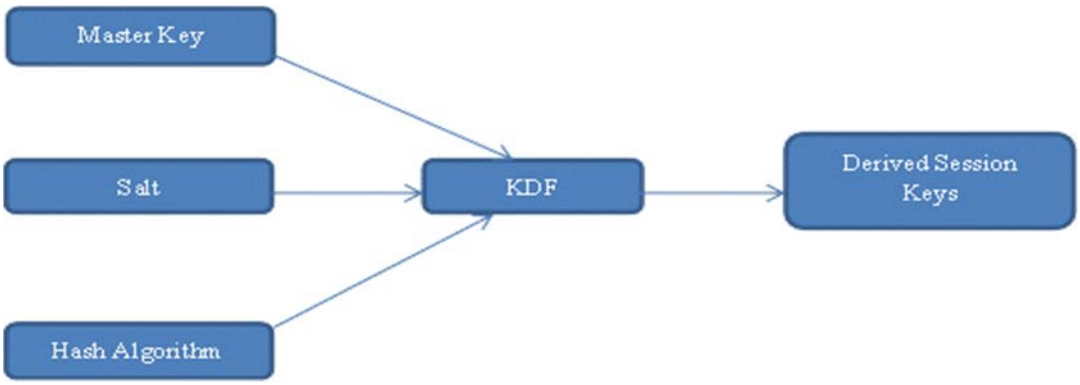

Fig 1: HKDF

3.1 Implementation of HKDF

3.1.1. Using HKDF-Extract and HKDF-Expand separately

- Some application required to extract once and expand several times with different info fields.
- If a strong key with enough entropy is available extract step can be skipped and apply expand directly.
- It makes key derivation logic more explicit which helps conveying the rationale of each operation. It helps analyzing the protocol.

3.1.2 Use HKDF as a single function

In this case both HKDF extract and expand are combined in a single function.

3.2 Importance of salt in KDF

The same salt needs to be used in order for the derived key to be the same at both ends of communication. A salt randomizes the KDF's output. It is optional, but highly recommended. Ideally as many bits of entropy as the security level of the hash. Shorter salt with less entropy can still meaningfully contribute to security. The salt value may be reused. It does not have to be secret, but may cause stronger security guarantees if kept secret.

- The purpose of the salt is to prevent pre-computed attacks on the hash like Rainbow-table.
- The salt allows re-using the same master key for multiple derived keys.
- Extract (XTR) can be deterministic or keyed via an optional "salt value" [Krawczyk H. (2010)]

4. Different Approaches for Hybrid Key Encapsulation Mechanism (KEM)

In all approaches, two master shared keys are generated one by applying traditional algorithm and one with post quantum algorithm.

4.1. HKDF_then_XOR

HKDF is applied on both master shared keys separately to derive two set of session keys. Final session key is obtained by applying XOR operation on session keys which is then used by symmetric-key cryptosystem. The disadvantage of this approach is HKDF need to be applied twice.

4.2. XOR_then_HKDF

In this approach, the XOR operation is applied on two master shared keys generated. The output of the XOR operation is given as input to HKDF to generate shared session keys which can be used by symmetric-key algorithm for encryption and decryption. Only one HKDF operation is required.

4.3. Concat_then_KDF

In this approach, two master shared keys generated are concatenated to make single key. This concatenated key is given as input to HKDF to generate shared session keys which can be used by symmetric-key algorithm for encryption and decryption. Only one HKDF operation is required [Giacon F., et al (2018)] [Bindel N., et al (2019)].

4.4. Proposed Approaches

One secret key as salt and another secret key as input to HKDF for deriving session key. There are two approaches in this case.

4.4.1 Traditional secret key as salt to HKDF

In this case, HKDF is applied on master shared key generated from post quantum KEM algorithm. For the HKDF, master shared key generated from traditional key exchange algorithm is used as a salt. Then, derived session keys are used for symmetric cryptosystem. There is no need to send salt over the network as same salt (master shared key using traditional algorithm) is generated at both ends of communication.

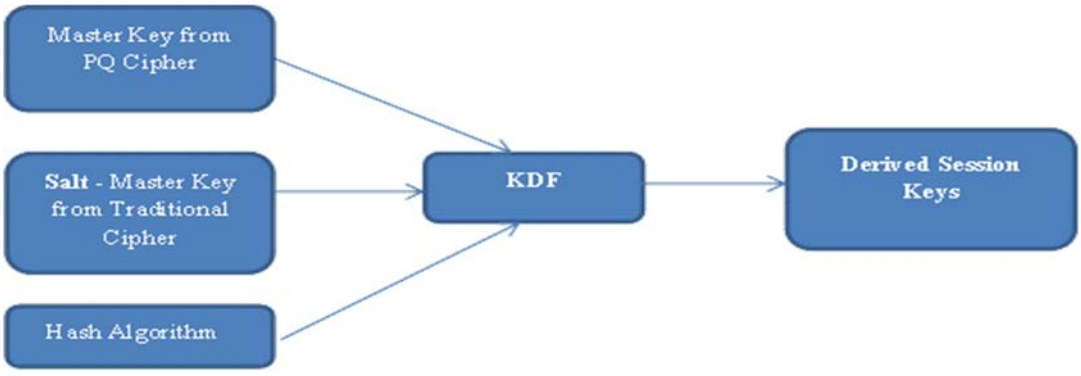

Fig 2: Traditional secret key as salt to HKDF

4.4.2 PQ secret key as salt to HKDF

In this case, HKDF is applied on master shared key generated from traditional key exchange (KEX) algorithm. For the HKDF, master shared key generated from post-quantum KEM algorithm is used as a salt. Then, derived session keys are used for symmetric cryptosystem. There is no need to send salt over

the network as same salt (master shared key using PQ KEM algorithm) is generated at both ends of communication.

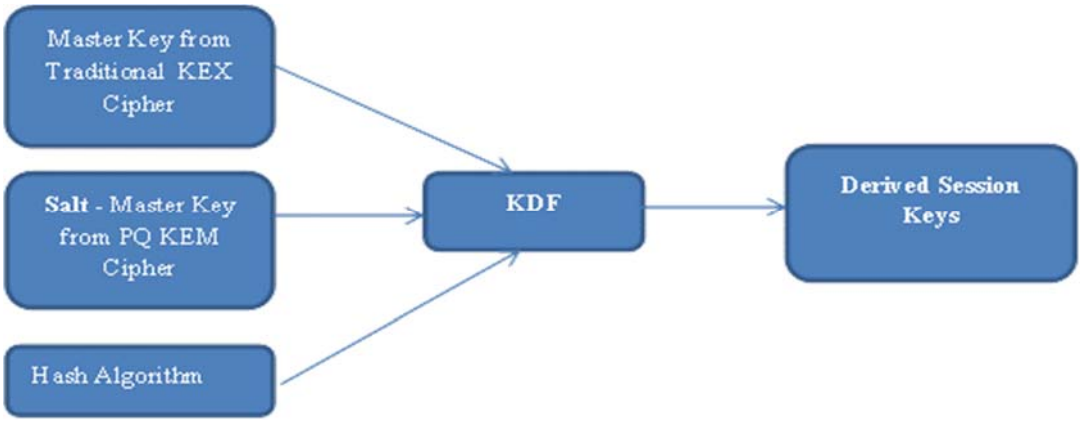

Fig 3: PQ secret key as salt to HKDF

5. Security Notions

Security of many cryptographic tasks, such as digital signatures, pseudorandom generation, and password protection, crucially relies on the security of hash functions. RFC recommendation also indicates that the salt value should be something that is authenticated during the protocol, or otherwise it can be selected by the adversary. In both proposed approached as a salt value (master key from traditional KEX cipher or PQ KEM cipher) can be derived only at client and server side and so adversary cannot select it. The use of salt adds significantly to the strength of HKDF.

6. Experiment and Conclusion

The working of the proposed approach is checked using a traditional key exchange algorithm Elliptic-Curve Diffie-Hellman (ECDH) and a post-quantum KEM Kyber-1024. The method is effective as it requires only one KDF computation and it avoids the need of XOR operation or concatenation operation.

References

[1] Meher K.; Midhunchakkaravarthy D. (2019), "Hybrid Solution (ECDHE + NewHope) for PQ Transition", International Journal of Engineering and Advanced Technology (IJEAT), ISSN: 2249 – 8958, Volume-9 Issue-2, page no.3893-3894.
[2] Meher K.; Midhunchakkaravarthy D. (2019), "Best-Fit Dual Signature for PQ Transition", ICNTE (2021).
[3] Post-Quantum Cryptography - Current state and quantum mitigation. European Union Agency for Cyber Security. (2021).
[4] Krawczyk H. (2010). "Cryptographic Extraction and Key Derivation: The HKDF Scheme"
[5] HKDF. [Online] Available: HKDF - Wikipedia
[6] Fischlin M.; Janson C.; Mazaheri S. (2018). "Backdoored Hash Functions: Immunizing HMAC and HKDF", IEEE Computer Security Foundations Symposium
[7] Giacon F.; Heuer F.; Poettering B. (2018). "KEM Combiners", page no. 1-29.
[8] Bindel N.; Brendel J.; Fischlin M.; Goncalves B.; Stebila D. (2019) "Hybrid Key Encapsulation Mechanisms and Authenticated Key Exchange", 10th International Workshop on Post-Quantum Cryptography.

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.