UtilitasMathematica
ISSN 0315-3681 Volume 122 (2), 2025

Methodology for the Seamless Integration of Post-quantum Hybrid Cryptographic Solutions into TLS-secured RESTful APIs in cloud Environments

Dr TCHIO TCHINDA
Martin Guillaume of INSTITUT DE PEDAGOGIE UNIVERSITAIRE (KABALA-MALI)
Email: tchiomartin@gmail.com

Abstract :

At the dawn of the rise of quantum systems, the scientific community is faced with a real security problem of TLS (Transport Layer Security) protocols, a central element for secure exchanges in the cloud. Indeed, the security basis of the TLS protocol is the use of classical asymmetric cryptographic algorithms such as RSA and ECC, which have become vulnerable to the factorization and discrete logarithm resolution power of the Shor and Grover algorithms by exploiting the strength of quantum systems. This has a direct impact on RESTful APIs in cloud environments because their security also depends mainly on TLS. In order to remedy this problem, the research community has turned to so-called post-quantum cryptographic solutions.

It is important to make the nuance because these solutions are rightly called post-quantum are not because they are based on the strength of quantum, but because they appear in an era where quantum systems already exist, hence the post-quantum therm. These solutions are of course able to resist attacks using the force of quantum calculations. However, its integration into cloud infrastructures remains a major challenge due to the compatibility constraints and performance requirements that cloud services require, including latency and scalability.

In order to keep the performance level of cloud services almost intact, the article proposes a methodology for integrating hybrid cryptographic solutions within TLS-secured RESTful APIs. It is a combinatorial solution of classical algorithms such as X255119 and ECDSA which is an outgrowth of ECC and post-quantum systems such as Kyber768 and Dilithium at the TLS level without however modifying the structure of the application layer. The experiments demonstrate in this article that the hybrid solution perfectly keeps the security of exchanges robust while maintaining performance almost intact for cloud services requiring high availability.

Keywords : post-quantum, TLS, Cloud, RESTful API, hybrid cryptography, integration, methodology.

I. Introduction :

Today more than ever, cloud computing offers services that are highly sought after by companies for hosting, processing and securing data and especially for the allocation of network resources. Three main services are at the heart of this transformation ; these are PaaS, IaaS and SaaS so the

exchanges between them are largely based on RESTful APIs so the security is protected by protocols such as TLS (Transport Layer Security). For a long time, this protocol remained infallible in the face of classic threats because the classic cryptographic algorithms (asymmetric and symmetric) played the role of shield with perfection. But the arrival of quantum systems is now calling into question the ability of these classical cryptographic systems to ensure the security of these interdepartmental exchanges in the cloud.

Faced with this new challenge, research has been carried out ; this has led to the appearance of new so-called post-quantum cryptographic schemes (PQC) capable of rigorously dealing with threats or attacks using the power of quantum systems. However, a real problem of implementing these post-quantum algorithms in the cloud, and particularly for APIs, arises in an environment where performance, which is intimately linked to availability, is a survival issue.

In order to remedy the problem of implementing post-quantum cryptographic solutions in the cloud, the scientific community is increasingly exploring hybrid approaches that have the ability to deal with quantum-type attacks, but also to keep the level of performance of infrastructures almost intact. It is also a transitional opportunity that these hybrid solutions offer, allowing post-quantum solutions to be gradually improved, thus having guaranteed compatibility in the cloud.

This article provides a methodical proposal for the integration of post-quantum hybrid cryptographic solutions into TLS-secured RESTful APIs that are particularly suitable for cloud environments. The general objective is to evaluate and compare the best hybrid cryptographic solutions (classical cryptography + post-quantum cryptography) capable of ensuring data security in RESTful APIs while maintaining the same current level of performance (latency, throughput, scalability, load balance) in a transitional period towards fully post-quantum solutions based on the assumption that a combinatorial cryptographic layer model can ensure a smooth transition to post-quantum systems without breaking the cloud service.

II. State of art

A. Post-quantum cryptography

Two major dates are important in the genesis of post-quantum cryptography ; 1994 and 1996. 1994 Scientist Peter Shor publishes an article in the SIAM Journal Computing entitled : "*Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum compute".* In this paper, the author demonstrates that a universal quantum computer can factor an integer *N* in polynomial time, by exploiting the quantum Fourier transform (QFT). He also shows in the same paper that the discrete logarithm problem can be solved under the same conditions ; which weakens the robustness of asymmetric cryptographic algorithms such as RSA and ECC. In 1996, it was another scientist named Lov Kumar Grover in his article entitled : "*A fast quantum mechanical algorithm for database search.* In *Proceedings of the 28th Annual ACM Symposium on Theory of Computing"* shows that a quantum computer can perform an unstructured search on a database of *N* elements in only √N operations, unlike a classical computer which does so in *N* operations ; and here again, symmetric cryptographic algorithms

(AES, 3DES) that were thought to be impassable are put to the test. Therefore, the quantum threat is felt on classical cryptographic systems (asymmetric and symmetric).

1. Introduction to Post-quantum cryptographic families

There are three main families of post-quantum cryptographic algorithms, namely

- Lattice
- Code-based
- Hash-based

i. **Cryptography based on Euclidean networks (Lattice-based cryptography)**

This cryptographic system family is based on difficult problems related to network geometry such as :

- Shortest Vector Problem (SVP) : Find the shortest vector in a network.
- Learning With Errors (LWE) : which consists of solving a system of noisy linear equations.

They are supposed to be resistant to classical and quantum attacks. Examples of algorithms of these types are **Kyber, Dilithium** which we will see in the third part of our work. (Ref: Peikert, C (2015). *A Decade of lattice Cryptographiy.).*

ii. **Corrector-based cryptography (code-bases cryptography)**

They rely on error-correcting codes to build cryptographic systems. The main problem is to decode a message without knowing the private keys, which is complex even for a quantum computer. We have examples such as McEliece, BIKE. (Ref: Debris-Alazard, T. (2023). *Code-based cryptography*.)

iii. **Hash-based cryptography**

They are part of the large family of hash-based cryptography, they rely solely on the security of cryptographic hash functions. The goal here is to transform a message of any size into a kind of fixed-size fingerprint. As the name suggests, hashing is a possible non-return operation. It is difficult to find two different messages with the same imprint. Or find a given message corresponding to a given fingerprint.

2. Standardization and recent work (ex. NIST PQC[1]).

In the field of new information and communication technologies, standardization occupies an important place. The post-quantum cryptographic field, abbreviated as PQC (Post-Quantum Cryptography), has also made significant progress in this direction, the importance being threefold, namely :

- Ensuring the interoperability of systems around the world.
- Protect sensitive data for the long term (for decades).
- Prepare for the transition to post-quantum solutions that can withstand quantum attacks.

[1] NIST PQC : National Institute of Standard and Technology pour le PQC

NIST PQC is one of the standards that has gotten ahead of post-quantum systems work in recent years. It is a field of research that aims to develop algorithms that can withstand attacks from quantum systems, while remaining secure and efficient on classical computers. This work is being carried out by the **National Institute of Standards and Technology (NIST),** which is a federal agency of the United States and part of the US Department of Commerce based in Gaithersburg, Maryland. (Ref : Bernstein, D. J., Buchmann, J., & Dahmen, E. (2009). *Post-quantum cryptography*.)

B. Securing RESTful APIs via TLS

RESTful APIs allow distributed applications to conduct communications over the http/HTTPS protocol, which truly exposes resources and data that are accessible through GET, POST, PUT, DELETE requests. This is an outcome that can be perfectly exploited by the man in the middle, or by identity theft by the ARP protocol, or via malicious injections. In order to remediate these types of threats or attacks, the TLS transport layer that uses both symmetric and asymmetric cryptographic schemes represents a layer of security at the level of these communications. Symmetric algorithms such as AES are used for the actual encryption of data in transit on the one hand, and on the other hand, asymmetric cryptographic algorithms such as RSA are used for the recognition of both parties (authentication and certificate).

III. Hybrid approch

In this article, we wanted to highlight the concept of RSA-2048 + Kyber-512 hybridization that can be used in a cloud environment that requires performance, including RAM load, CPU usage, latency, bandwidth and key size. This schema is used for the authentication mechanism ; i.e. signature and certificate (reserved for RSA-2048) and the encapsulation mechanism (reserved for Kyber512) which could allow us to obtain immediate resilience not only against classical attacks, but also resilience against threats using the strength of quantum. The results of the experiment will make it possible to affirm or not their interoperability in RESTful API services. The method is quite simple ; when a client wants to connect to an API, the TLS security layer negotiator offers all the cryptographic algorithms it has in its arsenal. The server will take care of choosing the hybrid solution RSA+Kyber supported on both sides. RSA will be in charge of authentication, and Kyber will be in charge of exchanging keys. So these two solutions are used at specific times for very specific roles.

IV. Experiments and results

A. Testing environnement and tools

The table below summarizes the tools, environment, and metrics we will use to carry out our experiment.

CRITERIA	DETAILS
Environment	VM type n2-standard-4 (4 vCPU, 16 GB RAM- intel Core i7 processor, Ubuntu 22.10 (64-bit)
Tools	OpenSSL 3.x (RSA-2048) + liboqs/OpenQuantumSafe (Kyber-512)
Tests	Simulate a TLS (mainly KEM) key exchange, certificate, signing, and session encapsulation/decapsulation
Charges	Low ↔ high (simulation of 100 to 1000 signatures

A. Results and performance

OPERATIONS	RSA-2048	KYBER-512	HYBRIDE(RSA+Kyber)
Encapsulation (key)	1.5 ms	0.3 ms	1.9 ms
Decapsulation (key)	2.8 ms	0.45 ms	3.3 ms
Public Key Size	256 bytes	800 bytes	~1056 bytes
Private key size	1190 bytes	1632 bytes	~2822 bytes
CPU Usage (Peak)	25%	10%	35%
Memory Used	~50MB	~80MB	~130MB
Exchange Size	256 bytes	768 bytes	~1024 bytes

C. Analysis of the results

- The Core i7 (or Google Cloud vCPU equivalent) reduces encapsulation/decapsulation times by 20–25% compared to an i5.
- Kyber-512 is 8x faster than RSA-2048 for encapsulation, and 6x faster for decapsulation.
- The hybrid mode combines the two without doubling the time : an additional cost of about 30% compared to RSA alone.
- Exchange and key sizes increase significantly with Kyber, but this is still manageable in a high-bandwidth cloud environment.
- Resiliency : Assured protection for key exchange.

D. Recommandations

- Viable solution in production to anticipate quantum, without loss of compatibility.
- For heavy traffic, consider Kyber alone (Kyber-768) and higher frequency servers (C2 or N2-highCPU type on GCP).
- Marginal memory overcharge ; no RAM bottleneck.

V. Conclusion

The use of the hybrid cryptographic solution to secure exchanges via RESTfull APIs in the cloud presents an opportunity to ensure the security of these exchanges for a transitional period while keeping the performance of resources in the environment almost intact. This is perfectly observable through the table of performance results where the differences between classical and post-quantum solutions taken in isolation are not significant. This solution must be perfectly feasible for cloud providers in order to continuously guarantee the level of performance of cloud services and thus anticipate attacks or threats using the power of quantum.

REFERENCES BIBLIOGRAPHIQUES

1- QIxin, Z (Janvier 2022). *An Overview and Analysis of Hybrid Encryption: The Combination of Symmetric Encryption and Asymmetric Encryption. DOI: 10.1109/CDS52072.2021.00111*.

2- Murad, S & Rahouma, K. H. (Janvier 2022). « *Hybrid Cryptography for cloud Security: Methodologies and Designs*. *DOI: 10.1007/978-981-16-2275-5_7*

3- Bernstein, D. J. & Lange, T. (2017). *Post-quantum cryptography. Nature*, *549(7671), 188–194.*

4- Fedorov, A. K. (2023). *Deploying hybrid quantum-secured infrastructure for applications: When quantum and post-quantum can work together*. Frontiers in Quantum Science and Technology, 2, Article 1164428.

5- **Baker, T. J. (2020).** *Quantum-safe cryptography: A survey of current research and trends in post-quantum cryptography*. *International Journal of Information Security*, 19(2), 159–185.

6- **Chen, L., Chen, Y., & Qian, L. (2021).** *Post-quantum cryptography: Current state and future directions*. *IEEE Access*, 9, 90822–90843.
7- **Jiang, J., & Li, Z. (2019).** *Quantum-safe cryptography for cloud computing. Journal of Cloud Computing: Advances, Systems and Applications*, 8(1), 7.
8- Zeng, P., Bandyopadhyay, D., Méndez Méndez, J. A., Bitner, N., Kolar, A., Solomon, M. T., ... & Liu, J. (2024). *Practical hybrid PQC-QKD protocols with enhanced security and performance*. arXiv preprint arXiv:2411.01086.
9- Demir, E. D., Bilgin, B., & Onbasli, M. C. (2025). *Performance analysis and industry deployment of post-quantum cryptography algorithms*. arXiv preprint arXiv:2503.12952.
10- Ghinea, D., Kaczmarczyck, F., Pullman, J., Cretin, J., Kölbl, S., Misoczki, R., ... & Bursztein, E. (2023). *Hybrid post-quantum signatures in hardware security keys*. In *Proceedings of the International Conference on Applied Cryptography and Network Security (ACNS)*.
11- Anastasova, M., Kampanakis, P., & Massimo, J. (2022). *PQ-HPKE: Post-Quantum Hybrid Public Key Encryption*. Cryptology ePrint Archive, Paper 2022/414.
12- **Gottfried, J. (2021).** *Quantum computing and cloud security: Addressing the risks in IaaS*. *Cloud Computing Journal*, 10(4), 345-358.
13- Chen, A. C. H., & Lin, B.-Y. (2025). *Hybrid scheme of post-quantum cryptography and elliptic-curve cryptography for certificates: A case study of security credential management system in vehicle-to-everything communications*.
14- L. Mark, S M (2019). *Secure, Resilient, and Agile software development.* Auerbach Publications.
15- Nelson, B., Phillips, A., & Steuart, C. (2024). *Guide to computer forensics and investigations (7e ed.).* Cengage Learning. *ISBN 978-1-337-56894-4*
16- *Maymi, F., Harris, S. (2021). CISSP all-in-one exam guide (9 e ed).* McGraw hill. ISBN: 978-1-260-46737-6.