"Comparative study of hybrid cryptographic solutions (classical + post-quantum) for maintaining performance and security in IaaS in the face of quantum threats in a transitional period towards fully PQC[1] solutions."

Author: TCHIO TCHINDA MARTIN GUILLAUME, PhD student at the Institute of University Pedagogy de KABALA (MALI). And student of MS CYBERSECURITY at LINDENWOOD UNIVERSITY MISSOURI (United States of America).

Co-author: Dr Dioba Sacko Chef MC Teacher-researcher Abderhamane Baba Touré National School of Engineering (ENI-ABT)

Contacts emails: MT449@lindenwood.edu / tchiomartin@gmail.com /diobasacko@yahoo.fr

ABSTRACT

It is imminent that the arrival of quantum computing is a real threat to data security in IaaS, in transit as well as at rest. To find cryptographic schemes capable of dealing with powerful quantum algorithms such as Shor and Grover, this article proposes an evaluative study of hybrid cryptographic solutions, which combines classical algorithms such as RSA[2], ECC[3], with post-quantum algorithms such as Kyber and Dilithium, capable of maintaining the same performance levels in an IaaS environment, and at the same time face the power of quantum systems. To do this, several metrics will be analyzed, including latency, CPU[4] load, RAM[5] saturation, and resistance to quantum attacks to have an objective idea of their possible adaptation (hybrid solutions) in the different IaaS environments of our main IaaS resource providers around the world, with a view to ensuring a transition to fully PQC solutions.

[1] PQC: Post quantum cryptography
[2] RSA: Rivest–Shamir–Adleman
[3] ECC: Elliptic Curve Cryptography
[4] CPU: Central Processing unit
[5] RAM: Random Access Memory

Keywords: Post-quantum cryptography, IaaS[6], cloud security, PQC, hybrid cryptography, quantum transition

I. INTRODUCTION

There is a serious and serious threat to the triad of digital data in IaaS (Confidentiality, Integrity and Authenticity), mainly due to the rise of quantum computing. This threat mainly targets classic cryptographic systems, which are an important part of maintaining data security in IaaS. This can be observed with the appearance of quantum algorithms such as Shor and Grover, which would break classical cryptographic systems such as RSA and ECC, the main cryptographic means of data in IaaS, in record time. Before the birth of these so-called "quantum" threats, these classical cryptographic systems were virtually unbreakable. Faced with this imminent threat, hybrid cryptographic solutions combining classical and post-quantum systems are gradually emerging. The goal of this article is to evaluate these classic cryptographic schemes in IaaS across different vendors and environments, capable of transitioning to fully PQC solutions.

II. STATE OF ART

Many researchers have sufficiently proven the limits of classical algorithms such as RSA, DSA[7] or ECC in the face of quantum computer attacks. Peter Shor, so the algorithm also goes by the name: "Shor" in his book entitled: *Algorithms for quantum computation: discrete logarithms and factoring*. Published in 1994 proves enough the compromise of its algorithm on the RSA, DSA, ECC which are based on the difficulty of solving complex mathematical problems.

A. Classic Cryptography

[6] IaaS: Infrastructure as a service
[7] DSA: Digital Signature Algorithm

The guarantee of the digital data triad in IaaS is mainly based on RSA (Digital Signature and Data Encryption), DSA (Digital Signature) and ECC (Data Encryption and Digital Signature). Their vulnerability to Shor's algorithm is now sufficiently documented. These cryptographic solutions, which are based on mathematical problems that are difficult to solve with a classical computer, are confronted with Shor's algorithm, which exploits the superposition properties of quantum quantum to factor large numbers into polynomial time.

B. Post-quantum cryptography

Faced with this incessant and intensive threat linked to quantum computing, many cryptographic systems such as Kyber, Dilithium or Falcon, called post-quantum cryptographic systems, have emerged. They are said to be post-quantum not because they exploit the properties of quantum systems, but because they will lead the revolt against the power of quantum. These solutions have shortcomings related precisely to the performance of IaaS, which is decreasing due to their use (high CPU usage, high RAM saturation, significant increase in key and certificate sizes that have a direct impact on bandwidth and latency).

C. Hybrid solutions

To address the performance challenge of all-PQC solutions, we offer hybrid solutions. These hybrid solutions are the combination of traditional solutions and PQC solutions ensuring a double guarantee of security in IaaS with the possibility of maintaining the same level of resource performance.

III. METHODOLOGY

The combination of applied research with an experimental and analytical approach, aiming on the one hand to propose an evaluation of the hybrid solutions studied in a real IaaS context;

and on the other hand, to test the performance, resilience and security of these combinatorial solutions.

A. Selection of tested solutions and test environment

We tested and evaluated three hybrid solutions in three different IaaS environments representing the three largest cloud providers in the world namely (Amazon, Google cloud, Azure). These three hybrid solutions are:

- X25519 (*ECC)* + Kyber 768 in Azure on a Standard D4S v3 VM[8] (4 vCPUs, 16 GB[9] RAM- Intel Core i7 processor, Linux
- RSA-2048 +Kyber-512 in Google cloud on a VM type n2-standard-4 (4 vCPUs, 16 GB RAM- Intel Core i7 processor, Ubuntu 22.10 (64-bit).
- ECDSA[10] (extension of ECC) + Dilithium in AWS[11] on an EC2[12] VM (t3.large, vCPU-4 threads, 16 GB RAM, WINDOWS SERVER 2016 (64-bit).

B. Metrics identified during the assessment

The metrics to be noted are:

- CPU load
- La saturation de la RAM
- Latency
- Key/certificate size
- Resilience to attacks
- Bandwidth

[8] VM: Virtual Machine
[9] GB: GigaBit
[10] ECDSA: Elliptic Curve Digital Signature Algorithm
[11] AWS: Amazone Web Service
[12] EC2: Elastic Compute Cloud

D. Tools Used for Cryptography

After the choice of hardware, it will be necessary to choose the software capable of supporting these hybrid solutions, and which will be responsible for the encryption/decryption of the sensitive data to be secured. We have opted for the OpenSSL+liboqs tool

NB: it is important to note that as of today, there is no executable cryptographic application tool that contains both classical cryptographic solutions and so-called post-quantum cryptographic solutions. To remedy this problem (because the tool is important for our testing phases), we used the OpenSSL tool. It is a tool that only uses classic cryptographic solutions. To make a hybrid cryptographic tool, we had cloned it by integrating post-quantum cryptographic solutions (Dilithium, kyber).

IV. RESULTS AND DISCUSSION

A. Results

- For the X25519 (*ECC)* + Kyber 768 hybrid solution in Azure cloud we obtained: latency ~0.6-0.7 ms[13]; public key size ~1216 bytes; bandwidth ~4-5KB[14] (certificate + key exchanges), RAM ~10 KB /session, CPU ~5% utilization.
- For an RSA-2048 + Kyber-512 solution in Google cloud we get latency ~2.5-3 ms; key size ~1050 bytes for public keys and ~5-8 KB for certificates; ~3-4 KB bandwidth; ~7-10% CPU load on the server side; RAM saturation: ~10 KB/session.
- For an ECDSA + Dilithium solution in AWS we get latency: ~2-3 ms; size of public keys: ~1370 bytes and about 3-4 KB for certificates (two signatures); bandwidth: ~5-

[13] ms: microsecond
[14] KB: KiloBit

6 KB TLS[15] certificates; CPU load: ~5-7% server-side load and ~5-6% client-side load (validation); RAM saturation: ~ 12-15 KB/session.

B. Discussions

- For the X25519 +Kyber solution, there is an increase in the size of the public keys compared to ECC (lighter) and Kyber (heavier) taken individually. This has a direct impact on the bandwidth and latency that allows the water solution to fall within the range of ECC and Kyber. The same is true for RAM and CPU resources, less important for ECC and much more important for Kyber. Resilience: Security of the exchange guaranteed even if Shor breaks ECC Kyber provides backup.
- For the RSA-2048 + Kyber-512 solution, the public keys are higher than that of the RSA and less Kyber taken individually. The same is true for certificates, which are three times higher than the simple RSA alone. This allows for a slight increase in latency and nearly double the bandwidth usage for TLS initialization. Resiliency: Assured protection for key exchange.
- For the ECDSA + Dilithium case, the size of the certificate is important for the simple reason that the certificate contains both public keys and the combined signature. The bandwidth almost triples and the latency also exceed more than 2 to 3 ms on average, which can be degrading for the quality of service. The saturation of the RAM is significant 93 times compared to a classic ECDSA session). Resiliency: Effective security for signature validation.

V. CONCLUSION

[15] TLS: Transport Layer Security

This paper proposed an objective evaluation of some hybrid cryptographic combinations (classical system and PQC system) capable of coping with the power of quantum systems. Our work demonstrates that a combinatorial approach between these two systems offers a real alternative capable of effectively guaranteeing data security in IaaS while maintaining the level of resource performance and keeping the principle of scalability and load balancing very dear to IaaS environments. However, our results expose real limitations of these solutions such as latency, bandwidth and load. CPUs that should not be negligible. It is therefore important to conduct additional studies to further optimize these hybrid solutions.

REFERENCES

1- 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
2- 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.
3- Demir, E. D., Bilgin, B., & Onbasli, M. C. (2025). *Performance analysis and industry deployment of post-quantum cryptography algorithms*. arXiv preprint arXiv:2503.12952.
4- 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)*.
5- Anastasova, M., Kampanakis, P., & Massimo, J. (2022). *PQ-HPKE: Post-Quantum Hybrid Public Key Encryption*. Cryptology ePrint Archive, Paper 2022/414.
6- 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*. arXiv preprint arXiv:2501.0702

PROFESSIONAL RESOURCES

1- Cloud Security Alliance. (2019). *Mitigating the quantum threat with hybrid cryptography*. https://cloudsecurityalliance.org/artifacts/mitigating-the-quantum-threat-with-hybrid-cryptography Home | CSA
2- Senetas. (2025). *Adopting a hybrid approach to post-quantum security*. https://www.senetas.com/blog/adopting-a-hybrid-approach-to-post-quantum-security/ senetas.com

3- Xiphera. (2025). *Hybrid models connect the post-quantum with the classical security*. https://xiphera.com/hybrid-models-connect-the-post-quantum-with-the-classical-security/ Xiphera
4- Tatananni, M. (2025, March 17). *Cloudflare is bulking up to fight the quantum attack*. Barron's. https://www.barrons.com/articles/cloudflare-quantum-computers-cybersecurity-7e41dbaa

i

i