Post-Quantum Cyberinfrastructure Security Readiness: Risks, Measures and Prospects

Phuong Cao[1,2] – pcao3@illinois.edu
Bach Hoang[3] – bachh2@illinois.edu
Santiago Núñez-Corrales[1,2] – nunezco2@illinois.edu
[1]National Center for Supercomputing Applications, UIUC
[2]Illinois Quantum Information Science and Technology Center, UIUC
[3]Department of Mathematics, UIUC

The problem of correctly implementing quantum resistant cryptographic network protocols is critically important to drive the adoption of quantum computers to the masses. It is urgent because practical quantum computers are on the horizon: 1,000-QUBIT quantum computer [1] will soon be offered by major industry players such as IBM in 2023, while some nations also claimed to break RSA encryption already [3]. The main challenges of implementing post quantum cryptography are: 1) complexity of implementing and verifying new cryptographic protocols, 2) wide-spectrum of client's cryptographic protocols such as IoT devices, and 3) significant performance overhead when deploying on Internet-scale networked computers. Nevertheless, how existing cyberinfrastructure will support post-quantum cryptography is largely unknown.

This paper proposes a testbed of novel networked telescopes that will be deployed at the nation's backbone (Figure 1). The networked telescopes, deployed at different vantage points, will continuously measure PQC adoption, characterize the performance overhead, and provide a real-time feedback loop to NIST in order to improve and fix potential security bugs of PQC algorithms in development. By bringing a diverse team of a cybersecurity expert, a mathematician, and an information theorist, we will initiate intellectual discussions at the workshop. This distributed network of telescope is our opportunity to stay ahead of attackers.

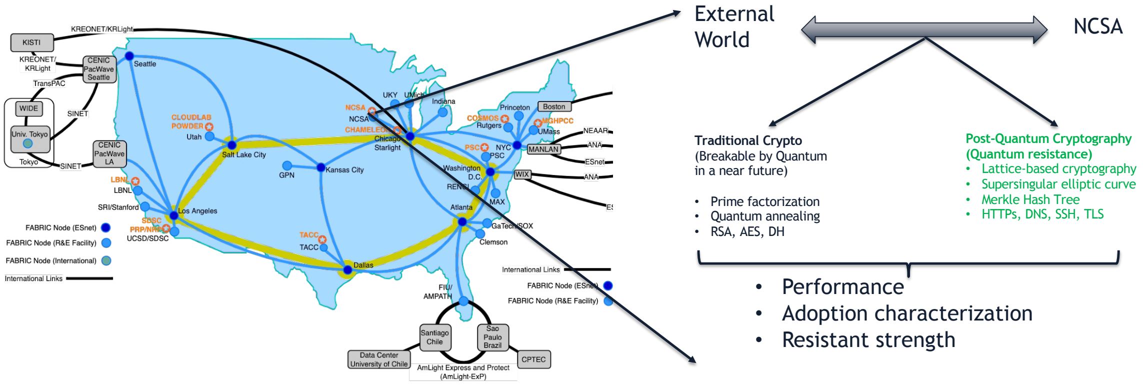

Figure 1: Networked telescope testbed to characterize deployment progress and performance overhead of post quantum cryptography algorithms.

Methods. The networked telecope testbed in Figure 1 will advances our understanding of quantum-resistant cryptographic algorithms are being deployed in the wild, e.g., TLS Post-Quantum Confidentiality key exchange algorithm in TLS (CECPQ2). Our approach is to build an array of a globally distributed network telescopes, each telescope is placed at a network border router to tap into incoming/outgoing network traffic. For example, the National Center for Supercomputing Applications (NCSA) at the University of Illinois has already been collecting network connection metadata, e.g., the packet headers, hand-shake algorithms, and cryptographic suite in encrypted protocols such as TLS, SSH, and encrypted DNS. The networked telescope will continuously measure, scan and remedy weaknesses in real world quantum implementations, as well as exchange of threat intelligence. We plan to deploy our master telescope at NCSA, a choke point of scientific traffic that would provide 360-degree, 24/7, orthogonal view of scientific network traffic. We will capture the network traffic through 400Gbps network border link. Using NIST's recommended algorithms in quantum cryptography such as CRYSTALS-Kyber for encryption, FALCON and SPINCS+ for digital signature, and KEMTALS for key exchange, we will test the usage of these algorithms in modern network protocols such as HTTPS (TLS 1.3), SSH, DNSSEC, and QUIC. This master telescope, when being connected with others in the future, will provide real-time Internet-wide scans that characterize the upcoming deployment of NIST's recommended encryption and digital signature algorithms for Post Quantum Cryptography.

Broader impact of our approach. The opportunity is to identify critical weaknesses or vulnerable implementations of quantum resistant cryptographic protocol in real time before the attackers can exploit them. Whether to fully adopt it is a controversial topic because of the added computational complexity, performance overhead, and unknown security issues. The success metric is the percentage of devices including IoT devices that correctly implement and support quantum resistant cryptography 100% of the time. Our solution is to build a globally distributed network telescope to continuously measure , scan and remedy weaknesses in real world quantum implementations.

Putting our approach in perspective. Recently, researchers have identified two Post-Quantum Algorithms that have the nest performance are Dilithium and Falcon, while Falcon seems to be more suitable for the web. One of the existing prooblem about Post-Quantum crytography when integrating with the network server is the signing, when slightly slower signing can have significant impact on the whole server. The concentration is now moved to signature and key size, as the optimization and hardware accleration improve signing performance. Some developments have been made by combining some Post-Quantum Cryptography algorithms to improve the handshake speed and leveraging ICA suppression to avoid round-trips. The future for Post-Quantum Crytography intergration to network server is to test the performance of PQ authenticated VPNs and UDP-based tunnles like QUIC and DTLS. Some experiments should be conducted to quantify the total impact of PQ algorithm under realistic conditions that include lossy networks. In addition, investigation of hybrid certificates' performance should be carried out by studying the message recovery capabilities offered by schemes such as Falcon. [2]

References

[1] An ibm quantum computer will soon pass the 1,000-qubit mark - ieee spectrum. https://spectrum.ieee.org/ibm-condor. (Accessed on 04/30/2023).

[2] George Tasopoulos, Charis Dimopoulos, Apostolos P. Fournaris, Raymond K. Zhao, Amin Sakzad, and Ron Steinfeld. Energy consumption evaluation of post-quantum tls 1.3 for resource-constrained embedded devices. Cryptology ePrint Archive, Paper 2023/506, 2023. https://eprint.iacr.org/2023/506.

[3] Bao Yan, Ziqi Tan, Shijie Wei, Haocong Jiang, Weilong Wang, Hong Wang, Lan Luo, Qianheng Duan, Yiting Liu, Wenhao Shi, Yangyang Fei, Xiangdong Meng, Yu Han, Zheng Shan, Jiachen Chen, Xuhao Zhu, Chuanyu Zhang, Feitong Jin, Hekang Li, Chao Song, Zhen Wang, Zhi Ma, H. Wang, and Gui-Lu Long. Factoring integers with sublinear resources on a superconducting quantum processor, 2022.