Hybrid Low-Cost Quantum-Safe Key Distribution

[1]Attila A. Yavuz, [2]Duncan Earl, [2]Scott Packard, [1]Saif Eddine Nouma
[1] *University of South Florida, 4202 E Fowler Ave, Tampa, FL 33620, USA*
[2] *Qubitekk, 1216 Liberty Way, Vista, CA 92081, USA*
[1] *{attilaayavuz, saifeddinenouma}@usf.edu*, [2] *{dearl, spackard}@qubitekk.com*

Abstract: A hybrid approach to quantum-safe cyber security that leverages the strengths of Quantum Key Distribution (QKD) and post-quantum computation while mitigating the weaknesses of both can enable quantum-safe cyber-infrastructures for improved security of defense, finance/banking, and utility systems.

1. Introduction

Advances in quantum computing present both opportunities and threats. The computing power of quantum processors, leveraging superposition, will complete tasks exponentially faster than existing classical computers. Such tasks include unraveling the complex math that many of the current public key encryption schemes are based on (e.g., factorization of large integers into primes, discrete logarithm problem). Conversely, the security of Quantum Key Distribution (QKD) is based on physical processes, sans mathematical complexity assumptions. The specific physical processes are employed to generate shared symmetrical encryption keys between two users, with security based on the principles of quantum physics, ensuring that information cannot be copied or manipulated without being detected. If an eavesdropper attempts to hack the quantum channel, the photons quantum state is unavoidably collapsed, and the attack is revealed. Moreover, an encryption key generated from QKD that is secure today will remain secure against advances in computing power (i.e., "Forward Security"). A quantum-protected network will enable long-term data security of public, private, and commercial data [1]. Complementary to QKD approaches, post-quantum cryptography focuses on developing algorithms that rely on mathematical intractability assumptions currently considered to be secure against quantum computers. Spearheaded by NIST Post-Quantum Cryptography (NIST PQC) standardization effort [2], lattice-based cryptography (e.g., [3,4]) offers an ideal balance between performance and security among other alternatives (e.g., hash-based, isogeny-based, etc.).

Defense command and control, finance and banking, and utility industrial control systems require both security and surety of information under the most rigorous conditions of access control and user authentication. Users and decision-makers must trust the integrity of information while ensuring that only approved users have access. The actual or anticipated employment of a quantum computer, capable of decrypting sensitive information now or in the near future raises concerns about operational security as well as the integrity of stored or transmitted data. Similarly, access to those systems would allow a malefactor to wreak havoc on national security, economic stability, and public safety.

Physical QKD (PQKD) provides the highest level of information security, based on keys generated from true randomness rather than mathematical computation while revealing eavesdropping attempts. However, there are real hurdles to implementation, absent pending developments in quantum repeaters. The distance over the required dedicated fiber optical cable logarithmically degrades the qubit error rate, greatly limiting key distribution beyond 100 kilometers. Free space transmission, via ground-to-space platforms, can potentially address this limitation. An additional challenge is the cost of equipment – which remains expensive, though costs are reducing as production scales. NIST PQC standards are widely deployed to ensure software-based foundational security services in real-life applications. They offer high scalability with Public Key Infrastructures, which need high-quality randomness and initial key distribution. Hence, NIST PQC approaches require a highly secure bootstrap for trustworthy deployments.

2. Our Proposed Hybrid QKD (HQKD) Architecture and Prototype

We propose a new *Hybrid QKD (HQKD)* that can harness the best aspects of PQKD and NIST PQC, thereby paving for scalable, low-cost yet secure quantum-safe cyberinfrastructures. We outline our prototype HQKD operations in Figure 1. In offline certificate authority phase, we bootstrap computational-secure PKIs with Quantum Random Numbers (QRN)s generated by Qubitekk's 810nm Quantum Key DataLoc™ Server. In this use case, Qubitekk used a variation of the BBM92 protocol [5] to generate the entangled photons used to produce the AES256 symmetrical keys. This allows the lattice-based master private/public key in our PKI to be high-quality (avoidance of side channels) and permits their initial quantum-safe distribution within the PQKD network. In the online hop-by-hop wireless key transfer phase, we vastly extend the coverage of the optical network only PQKDs by conveying symmetric keys (i.e., QRNs) via lattice-based authenticated KEM/DEM strategies proposed in NIST PQC [2]. This permits scalable and safe key distribution to the embedded devices even with wireless connection only.

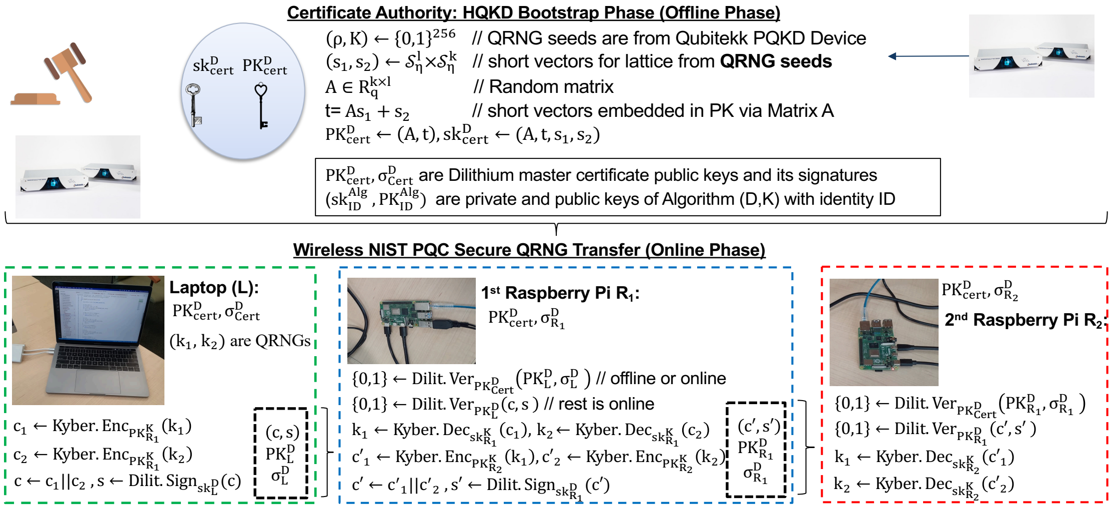

Fig 1. The proposed prototype: HQKD

3. Prototype Implementation and Conclusion

Table 1 outlines the performance of our HQKD. We used a laptop with Quad-Core Intel Core i5 CPU@1.4GHz, 16 GB memory, and 512GB SSD Drive. Embedded Raspberry Pi 4s devices are equipped with quad-core Cortex-A72 64-bit @1.5GHz and 4GB memory. All devices are connected via Wi-Fi (35.2Mbps download, 36.6Mbps upload, and 20 msec average latency). We used Open Quantum Safe Prototyping Library. The end-to-end delay is the time (in msec) it took for QRNs (k_1, k_2) to be conveyed from Laptop to R_1 and then R_1 to R_2 wirelessly via our Qubitekk bootstrapped certificates with Dilithium [3] and Kyber [4] as the signature and KEM/DEM, respectively. It includes key encapsulation/decapsulation, signature generation, and ciphertext and certificate verification times. The network delay to send the intermediary data varies from 22.39 ms to 82.82 ms depending on the Wi-Fi consistency.

Table 1. Experimental performance of our HQKD. Execution time and sizes are msec and KB, respectively

	KEM/DEM	Sign/Ver	Certificate Ver	Crypto End-to-End	Transmission Size
Laptop	0.02/-	0.14/-	-	0.16	9.7
R_1	4.65/4.05	9.01/3.56	1.81	23.08	9.7
R_2	-/4.05	-/3.56	1.81	7.61	

Our prototype HQKD shows that it is possible to securely transfer QRNs to be used for symmetric cryptography from commodity hardware to an embedded device with wireless hop-by-hop transmission only with a total cryptographic delay of 30.85 msec with less than 10 KB cryptographic payload. The communication delay is excluded as it only depends on the network properties (varies between 9 msec to 80 msec depending on hardware and network conditions). R1 incurs the highest cryptographic delay since it has to verify the received packet (from Laptop) while also encrypting/certifying the keys to send it to R2. Hence, our HQKD is a fully practical, cost-effective, and trustworthy alternative to deploy critical cyber-physical infrastructures in the post-quantum era.

Acknowledgments: This research is funded by the Department of Energy Award DE-OE0000780 at USF.

4. References

[1] "Products - Post Quantum Security Brief." Cisco. Cisco, July 16, 2020. https://www.cisco.com/c/en/us/products/collateral/optical-networking/solution-overview-c22-743948.html.
[2] "Post-Quantum Cryptography Standardization.". National Institute of Standards and Technology (NIST), January 3, 2017. https://csrc.nist.gov/Projects/post-quantum-cryptography/post-quantum-cryptography-standardization.
[3] Léo Ducas, Eike Kiltz, Trancéde Lepoint, Vadim Lyubashevsky, Peter Schwabe, Gregor Seiler, and Damien Stehlé. "CRYSTALS-Dilithium: A Lattice-Based Digital Signature Scheme." IACR Transactions on Cryptographic Hardware and Embedded Systems, 2018, 238–68.
[4] Joppe Bos, Léo Ducas, Eike Kiltz, Trancéde Lepoint, Vadim Lyubashevsky, Peter Schwabe, Gregor Seiler, and Damien Stehlé. "CRYSTALS - Kyber: A CCA-Secure Module-Lattice-Based KEM." In 2018 IEEE European Symposium on Security and Privacy (EuroS&P), 353-367, 2018. https://doi.org/10.1109/EuroSP.2018.00032.
[5] Charles H.Bennett, Gilles Brassard, and N.David Mermin. "Quantum Cryptography Without Bell's Theorem", American Physical Society, February 3, 1992, 557-559. https://doi.org/10.1103/PhysRevLett.68.557.