Low-cost, Scalable and Practical Post Quantum Key Distribution

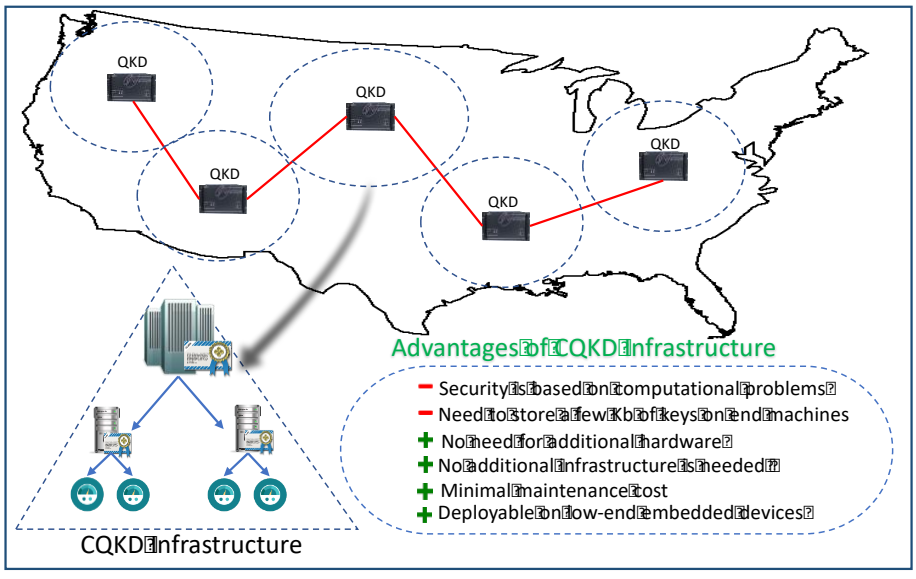
Website: https://cred-c.org/researchactivity/cqkd

Researchers (OSU): Attila A. Yavuz and Rouzbeh Behnia

Industry Collaboration:

- Physical (hardware-based) QKD is being researched and developed at Oak Ridge National Laboratory (ORNL) and Los Alamos National Laboratory (LANL).
- Our proposed software-based QKD effort is complementary to these efforts and aims to significantly reduce deployment hurdles and monetary costs. We will follow a two-pronged strategy for transitioning our technology. One prong is to publish and disseminate the algorithms and open-source the implementations so they are available for interested vendors. The second prong is to actively engage vendors in the EDS space on this technology through meetings and demonstrations of the technology. Some examples include but are not limited to, GE Global Research and ID Quantique. ***Vendors who are interested in engaging with this prong are encouraged to contact Attila Yavuz.***

Description of research activity: We will develop an efficient and authenticated Computationally-secure QKD (CQKD) infrastructure, which will be bootstrapped by QKD hardware only minimally but strategically. Our proposed CQKD will provide post-quantum key distribution via lattice-based public key encryption techniques that are supported by hash-based signatures to prevent quantum man-in-the-middle attacks. Hence, our CQKD will offer a post-quantum communication backbone that can cover a vast majority of critical EDS infrastructure without the need of expensive QKD hardware and costly dedicated fiber optic deployments. Moreover, CQKD will enable key distribution not only among substations, but also between substations and peripheral devices; and therefore, eliminate the hurdles of manual symmetric key distribution. CQKD will harness QKD hardware to deliver only the master CQKD certification keys, which will be used as the root keys in the certification hierarchy. As a result, only a fraction of EDS infrastructure will need QKD, while the rest of the infrastructure will be protected with CQKD. This is expected to offer significant cost reductions.



How does this research activity address the Roadmap to Achieve Energy Delivery Systems Cybersecurity?
Our proposal is toward strategy "3. Develop and Implement New Protective Measures to Reduce Risk" in the Roadmap.

More specifically, our proposal is toward strategy 3.5 “capabilities that enable security solutions to continue operation during a cyber attack available as upgrades and built-in to new security solutions.”

Following is the summary of benefits and advantages provided by the new system as compared to the state of the art:

1. **Ultra Low-Cost Post Quantum Resiliency:** The proposed CQKD Infrastructure and crypto suites will minimize the reliance on costly special QKD hardware, and its associated installment, infrastructure deployment (e.g., dedicated optical network) and maintenance overhead. QKD will be used to bootstrap CQKD, and *therefore, only a small fraction of smart-grid infrastructure will need QKD, while the vast majority of nation-wide infrastructure will be protected by CQKD with no extra infrastructure cost*.
2. **Rapid Deployment:** CQKD can be rapidly deployed on the existing smart-grid infrastructure.
3. **Post-Quantum Keying for Peripheral Devices:** QKDC not only permits substation-to-substation, but also substation-to-peripheral device post-quantum key establishment with a resiliency against man-in-the-middle attack. Therefore, it substantially reduces the overhead of distributing symmetric keys to smart-meters and PMUs, and allows immediate software updates and revocations with minimal cost.
4. **Broader Impact on Nationwide Critical Cyber-Infrastructure:** QKDC has a potential to enable a nation-wide post-quantum public key infrastructure, and therefore, can offer certification services, not only for EDS but a vast range of other application domains including other critical infrastructures identified by DHS. Our proposed QKDC can serve as a backbone for all these systems, providing a low cost post-quantum protection for a wide range of critical US infrastructures.

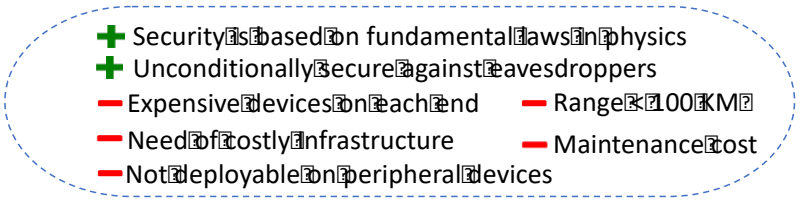
Summary of EDS gap analysis: With the latest advancements on quantum computers (e.g., D-Wave 2000Q [1]), the need for post-quantum security is gaining urgency especially in critical infrastructures such as energy delivery systems (EDS) (e.g., electricity, oil & gas). Quantum computers can break most of the existing cryptographic schemes (e.g., ECDH, RSA, etc.) that are based on traditional hard problems (e.g., factoring, DLP). Therefore, standard public key primitives (e.g., encryption/signatures), and hence key distribution and public key infrastructures that rely on those primitives will be ineffective. However, symmetric key primitives with larger key sizes remain secure against quantum computers (e.g., AES-256, SHA-512) [7]. Hence, physical Quantum Key Distribution (QKD) is proposed for distributing symmetric keys between high-end devices securely [19,20,21,22,23,24,25]. While QKD can provide high security based on the laws of physics, scalability issues hinder its wide adoption. Our proposed approach will help physical QKD scale and significantly reduce deployment and infrastructure costs.

Full EDS gap analysis: The importance of aforementioned research gap has already been recognized by DoE as there are current research activities about physical QKD as described in DoE roadmap [20] including collaborations [22,23,24] with ORNL and LANL. This research gap is critical for various NESCOR failure scenarios [27], including but are not limited to "Weaknesses in Authentication Process or Authentication Keys (6.5.1.4)" and "Use of Insecure Protocols (6.3.1.21)". Not addressing this research gap will lead into the following vulnerabilities, including but are not limited to “Cryptographic Vulnerability (6.3.1.4)" , "Use of Inadequate Security Architectures and Designs (6.4.1.1)", "Use of Insecure Protocols (6.3.1.21)" and "Weaknesses in Authentication Process or Authentication Keys (6.5.1.4) as described in Appendix D of [27]. Below, we further detail our full EDS gap analysis.

Given the distributed nature of EDS, the following issues may greatly affect the rapid, scalable and cost-effective adoption of QKD technology in its current state:

Limitations of the Existing QKDs for Ubiquitous Smart-Grid Systems: *i) Requirement to purchase (around $70K per machine) and install costly devices at each end.* The total cost can be significant for hundreds of sub-stations, especially considering the extra installation overhead on top of the cost of the devices. *ii) Requirement of dedicated fiber optic cables (SMF-28) between end points.* This is an expensive requirement for sub-stations in rural areas. Deployment of high quality optic network infrastructure nation-wide, which is dedicated only for QKD purposes can introduce significant monetary costs. *iii) The maximum length of quantum channel that keys can securely travel is only around 65 miles [13]*. This implies that potentially a large number of post-quantum devices must be used to enable communication

for distant locations, which may substantially increase the aforementioned device and infrastructure cost. *iv) Maintenance costs due to the moderate (<10 years) life expectancy of the devices.* The continuous maintenance and replacement of aforementioned infrastructure may introduce significant cost, and potential vulnerability periods since physical replacements require a non-negligible down time. *(v) Deployability issues in peripheral devices.* QKD only offers key exchange among major sub-stations, but the produced symmetric keys must be distributed to peripheral devices manually. Given the large number of low-end peripheral devices, this process demands significant man-power, and also introduces difficulties for key management and update.



Limitations of Existing Post-Quantum Cryptography for EDS: Post-quantum cryptographic key distribution requires a post-quantum authenticated Key Public-Infrastructure (PKI). Therefore, we need computationally secure post-quantum key exchange and digital signatures to offer authenticated PKI and certification authorities. This is necessary to prevent man-in-the-middle attacks for computationally secure post-quantum key exchange (as in traditional (non-post) quantum PKI). Although computationally secure post-quantum technologies exist (e.g., code-based, multivariate-quadratic-equations), they are known to be highly inefficient due to their large key/signature sizes and heavy computation overhead. However, recent progress on lattice-based cryptography yielded more efficient public key encryption schemes [17, 15]. NIST, NSA and EU initiated standardization efforts [7, 10, 18] to move towards post-quantum Internet communication standards. Despite these developments, it is a challenging task to develop post-quantum public-key encryption for smart-grids. Moreover, encryption *must* be supported with authentication to achieve a PKI, which requires other cryptographic techniques (e.g., hash-based signatures).

Research Gaps and Challenges: Specifically, we aim to answer the following research questions:

1) *Is it possible to create a practical Computationally-secure Quantum Key Distribution (CQKD) framework, which permits key exchange/distribution without depending on special hardware?*
2) *How can we create a full-fledged CQKD infrastructure by providing a post-quantum authentication mechanism, which is necessary to protect CQKD systems from man-in-the-middle attacks?*
3) *How can we harness the ideal security provided by QKD hardware [13] to support CQKD, so that we minimally, but strategically utilize QKD device, but achieve scalable and efficient key management with CQKD?*
4) *Is it possible to securely instantiate CQDK schemes even on low-end smart-grid devices?*

Complementary Cyber-Security Efforts to Proposed Techniques: There are ongoing efforts to reduce the cost of physical QKDC infrastructure (e.g., [20,21,22,23,24,25]). In one of the attempts to reduce the cost of such devices, Los Alamos National Laboratory (LANL) proposed a small portable device called QKarD [26] that can be connected (via a fiber optic cable) to a central trusted authority (TA) to receive secret keys. While the device is small (in size), it still requires a dedicated connection to the quantum key generator (the TA, in this case) via fiber optic cable. Moreover, since key generation happens at the TA, for every new key, the device needs to have a direct connection to the server to receive a new (session) key. While QKarD technology can be highly attractive for single users that require to only transmit highly sensitive information on demand, since it still requires the costly infrastructure for QKD, and given its limited capabilities, it cannot mitigate the current obstacles in the adoption of QKD in smart grids.

Specifically, DoE, in collaboration with Oak Ridge National Laboratory (ORNL), GE Global Research and ID Quantique, develops upgrades for QKD referred to as AQCESS [20,21]. AQCESS permits multiple clients to communicate over a single quantum channel using quantum modulators in a ring network topology. While reducing the cost by allowing multiple devices to securely communicate on a single ring, this approach still requires a costly network infrastructure and the presence of quantum modulators. However, it can serve as a suitable bootstrapping framework for our proposed CQKD PKI infrastructure. In a different line of research, ORNL develops secure communication techniques for smart-grid networks [22], which focuses on the security at the lower layer of network stack. Particularly, ORNL works on spread

spectrum techniques to provide secure physical and multiple access layer specific protocols. These techniques can be added on top next generation radio networks.

Remark that our proposed CQKD not only reduces the cost of QKD, but also complements the aforementioned efforts. That is, CQKD operates the higher level of network stack, specifically at TCP and/or application layer. Therefore, it is a software only solution, and does not assume the presence of any special physical hardware and/or wireless/wired channel condition, and therefore is free from any relevant assumptions on the adversaries. Hence, CQKD is expected to complement the lower layer security solutions by operating at the higher layer of the network stack. Finally, CQKD will harness any available QKDC solution (e.g., AQCESS [20,21]) to bootstrap its master PKI infrastructure, but will offer very low-cost (software only) post-quantum key distribution for the rest of nation-wide EDS infrastructure without depending on a special hardware and/or optical network infrastructure.

How the Candidate Activity will Address This Gap.

Our roadmap to achieve a secure and efficient CQKD for smart grids is as follows:

- Develop Efficient CQKD Key Distribution Strategies (year 1):
    - We will determine the most suitable set of lattice-based encryption techniques for key exchange purposes on sub-station-2-sub-station and sub-station-peripheral device settings.
    - A critical element of current lattice-based encryptions is the sampling strategies [12, 13, 9, 8]. We will identify a sampling mechanism that is suitable for smart-grid systems. We will further investigate constant-memory pre-computation techniques, which can substantially reduce the computational overhead of sampling for lattice structures.
    - We will develop efficient instantiations with fine tune parameterization and mathematical structures to reduce the key exchange overhead. Some options include but not limited to: (i) The NTRU [11] over $(\mathbb{Z}/q)[x]/(x^p - 1)$ for a prime p and q is a power-of-two [4], (ii) The Ring-LWE-based cryptosystems over $(\mathbb{Z}/q)[x]/(x^p + 1)$ where p is a power-of-two and $q \in 1 + 2p\mathbb{Z}$ [1], (iii) NTRU prime over $(\mathbb{Z}/q)[x]/(x^p - x - 1)$ for a prime p and q [2].
    - We will analyze the security of our selected techniques and tools to determine acceptable security parameters and performance trade-offs for realistic smart-grid settings. We will also investigate the overhead of potential side-channel countermeasures for these cryptosystems.
- Optimized Realization of CQKD Key Distribution Deployments (year 2): The efficient realization and optimization of lattice-based cryptographic tools is a crucial necessity for the practical deployments. (i) We will harness efficient number theoretical software libraries via various optimizations to ensure high performance on both low-end and sub-station devices (e.g., desktop). (ii) In sub-station-2-sub-station key exchange setting, both sides have a capability to employ commodity hardware such as GPUs to speed up the process. We will exploit extreme parallelizability of new lattice-based tools (e.g., FFT based operations) to push their performance to edge via GPUs, which are available for desktops with very low costs.
- CQKD with Certification Infrastructure (year 2): The existing lattice-based encryption schemes [6, 5, 1] only provide unauthenticated key exchange. Therefore, they cannot resist against the quantum man-in-the-middle attacks, in which an adversary can impersonate any sub-station or peripheral in the system. This completely invalidates the security of CQKD key distribution. To ensure security against man-in-the-middle attacks, the CQKD system needs to be accompanied with a post-quantum signature scheme to provide authentication. We will create an authenticated post-quantum CQKD infrastructure with a long-term certificate resiliency: The current lattice-based digital signatures are still highly costly, and therefore their direct combination with lattice-based encryption might not be suitable for smart-grids. Hash-based signatures are post-quantum resilient, but their preliminary variants only offered limited signing capability. The recent stateless hash-based signatures are considered for post-quantum certification purposes [4], but their key and signature sizes are very large. We will

develop novel hash-based signatures, which keep state but offer significantly smaller signature/key sizes with better efficiency.

- Bootstrap CQKD Infrastructure with Minimal Use of QKD (year 3): The highly secure features of QKD can be strategically utilized to provide increased security by distributing the master CQKD certifications keys, which will be used as the root keys in the certification hierarchy.
- Implementation on Embedded Systems (year 3): We will realize proper components of CQKD infrastructure at the peripheral devices so that the symmetric keys can be distributed and updated automatically by the sub-stations without manual interventions. We plan to develop highly optimized suites that can operate on ARM-based processors with a low memory usage.

Bibliography:

[1] D-Wave Systems Previews 2000-Qubit Quantum System (2016), https://www.dwavesys.com/press-releases/d-wave-systems-previews-2000-qubit-quantum-system

[2] Alkim, E., Ducas, L., Pöppelmann, T., Schwabe, P.: Post-quantum key exchange—a new hope. In: 25th USENIX Security Symposium (USENIX Security 16). pp. 327–343. USENIX Association, Austin, TX (2016)

[3] Bernstein, D.J., Chuengsatiansup, C., Lange, T., van Vredendaal, C.: Ntru prime. IACR Cryptology ePrint Archive (2016)

[4] Bernstein, D.J., Hopwood, D., Hülsing, A., Lange, T., Niederhagen, R., Papachristodoulou, L., Schneider, M., Schwabe, P., Wilcox-O'Hearn, Z.: Sphincs: Practical stateless hash-based signatures. In: Advances in Cryptology – EUROCRYPT 2015: 34th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Sofia, Bulgaria, April 26-30, 2015, Proceedings, Part I. pp. 368–397. Springer Berlin Heidelberg, Berlin, Heidelberg (2015)

[5] Bernstein, D.J., Lange, T.: eBACS: ECRYPT benchmarking of crypto- graphic systems (2016), https://bench.cr.yp.to

[6] Bos, J.W., Costello, C., Naehrig, M., Stebila, D.: Post-quantum key exchange for the TLS protocol from the ring learning with errors problem. In: 2015 IEEE Symposium on Security and Privacy. pp. 553–570 (2015)

[7] Chen, L., Jordan, S., Liu, Y.K., Moody, D., Peralta, R., Perlner, R., Smith-Tone, D.: Report on Post Quantum Cryptography . Tech. rep., National Institute of Standards and Technology (2016)

[8] Ding, J., Xie, X., Lin, X.: A simple provably secure key exchange scheme based on the learning with errors problem. IACR Cryptology ePrint Archive (2014)

[9] Ducas, L., Lyubashevsky, V., Prest, T.: Efficient identity-based encryption over NTRU lattices. In: Advances in Cryptology – ASIACRYPT 2014: 20th International Conference on the Theory and Application of Cryptology and Information Security, Kaoshiung, Taiwan. Proceedings, Part II. pp. 22–41. Springer Berlin Heidelberg (2014)

[10] ec.europa.eu: European Commission will launch 1 billion Euro quantum technologies flagship (2016), https://ec.europa.eu/digital-single-market/en/news/european-commission-will-launch-eu1-billion-

[11] Gentry, C., Peikert, C., Vaikuntanathan, V.: Trapdoors for hard lattices and new cryptographic constructions. In: Proceedings of the Fortieth Annual ACM Symposium on Theory of Computing. pp. 197–206. STOC '08, ACM, New York, NY, USA (2008)

[12] Hoffstein, J., Pipher, J., Silverman, J.H.: NTRU: A ring-based public key cryptosystem. In: Algorithmic Number Theory: Third International Symposiun, ANTS-III Portland, Oregon, USA. Proceedings. pp. 267–288. Springer Berlin Heidelberg (1998)

[13] IDQuantique: http://www.idquantique.com/photon-counting/clavis3-qkd-platform/

[14] Klein, P.: Finding the closest lattice vector when it's unusually close. In: Proceedings of the Eleventh Annual ACM-SIAM Symposium on Discrete Algorithms. pp. 937–941. SODA '00, Society for Industrial and Applied Mathematics, Philadelphia, PA, USA (2000)

[15] Lyubashevsky, V., Peikert, C., Regev, O.: A toolkit for ring-lwe cryptography. In: Johansson, T., Nguyen, P.Q. (eds.) Advances in Cryptology – EUROCRYPT 2013: 32nd Annual International Conference on the Theory and Applications of

Cryptographic Techniques, Athens, Greece, May 26-30, 2013. Proceedings. pp. 35–54. Springer Berlin Heidelberg, Berlin, Heidelberg (2013)

[16] Peikert, C.: An efficient and parallel gaussian sampler for lattices. In: Rabin, T. (ed.) Advances in Cryptology – CRYPTO 2010: 30th Annual Cryptology Conference, Santa Barbara, CA, USA, August 15-19, 2010. Proceedings. pp. 80–97. Springer Berlin Heidelberg, Berlin, Heidelberg (2010)

[17] Regev, O.: On lattices, learning with errors, random linear codes, and cryptography. J. ACM 56(6), 34:1–34:40 (Sep 2009)

[18] Simonite, T.: NSA Says It "Must Act Now" Against the Quantum Computing Threat (2016), https://www.technologyreview.com/s/600715/nsa-says-it-must-act-now-against-the-quantum computing

[19] Walenta, N., Burg, A., Caselunghe, D., Constantin, J., Gisin, N., Guinnard, O., Houlmann, R., Junod, P., Korzh, B., Kulesza, N., et al.: A fast and versatile qkd system with hardware key distillation and wavelength multiplexing. 2013. arXiv preprint arXiv:1309.25835

[20] Department of Energy (DoE), Cybersecurity for Energy Delivery Systems (CEDS), Practical Quantum Security for Grid Automation, September 2013, accessible:

https://www.controlsystemsroadmap.net/ieRoadmap%20Documents/Practical_QKD.pdf

[21] Warren Grice, Oak Ridge National Lab (ORNL), Practical Quantum Security for Grid Automation, Cybersecurity for Energy Delivery Systems Peer Review, August 5, 2014, accessible:

https://energy.gov/sites/prod/files/2017/02/f34/ORNL_PQS_CEDS_Peer_Review_2014.pdf

[22] Energy Security Projects , Next Generation Secure Scalable Communication Network for Smart Grid, Oak Ridge National Lab (ORNL), accessible: http://web.ornl.gov/sci/electricity/research/security/projects/

[23] Los Alamos National Laboratory (LANL), High-Security, Low-Latency, Stream-Wise Authentication and Encryption of Intelligent Electronic Device (IED) Links Enabled By Quantum Cryptography, March 2011, accessible: https://www.controlsystemsroadmap.net/Efforts/Pages/High-Security-IED.aspx

[24] Los Alamos National Laboratory (LANL), Quantum Security Models for the Power Grid, October 2014, accessible: https://www.controlsystemsroadmap.net/efforts/Pages/Quantum-Security-Models-for-the-Power-Grid.aspx

[25] qubitekk Inc., Scalable Quantum Cryptography Network for Protected Automation Communication, October 2016, accessible:

https://energy.gov/sites/prod/files/2017/05/f34/Qubitekk_QKD_FactSheet.pdf

[26] Los Alamos National Laboratory (LANL), QKarD, Quantum Smart, March 2010, accessible: https://www.lanl.gov/projects/feynman-center/_assets/pdf/qkard.pdf

[27] Electric Sector Failure Scenarios and Impact Analyses–Version 3.0, Electric Sector Cybersecurity Organization Resource (NESCOR), December 2015.