PQ-REACT: Post Quantum Cryptography Framework for Energy Aware Contexts

Marta I. García-Cid*
migarcia@indra.es
Indra Sistemas S.A. and Universidad Politécnica de Madrid
Spain

Michail-Alexandros Kourtis
George Xilouris
National Centre for Scientific Research DEMOKRITOS
Greece

David Domingo
Indra Sistemas de Comunicaciones Seguras
Spain

Nikolay Tcholtchev
Fraunhofer Institute for Open Communication Systems
Germany

Evangelos K. Markakis
Hellenic Mediterranean University
Greece

Marcin Niemiec
AGH University
Poland

Vicente Martín
Laura Ortiz
Javier Faba
Universidad Politécnica de Madrid
Spain

Diego López
Telefónica Investicación y Desarrollo
Spain

Maria Gagliardi
Scuola Superiore Sant'Anna
Italy

José González
MTU Autralo Alplha Lab
Estonia

Miguel García
Splorotech S.L.
Spain

Giovanni Comande
SMARTEX SRL
Italy

Nikolai Stoianov
Bulgarian Defence Institute
Bulgaria

ABSTRACT

Public key cryptography is nowadays a crucial component of global communications which are critical to our economy, security and way of life. The quantum computers are expected to be a threat and the widely used RSA, ECDSA, ECDH, and DSA cryptosystems will need to be replaced by quantum safe cryptography. The main objective of the HORIZON Europe PQ-REACT project is to design, develop and validate a framework for a faster and smoother transition from classical to quantum safe cryptography for a wide variety of contexts and usage domains that could have a potential interest for defence purposes. This framework will include Post Quantum Cryptography (PQC) migration paths and cryptographic agility methods and will develop a portfolio of tools for validation of post quantum cryptographic systems using Quantum Computing. A variety of real-world pilots using PQC and Quantum Cryptography, i.e., Smart Grids, 5G and Ledgers will be deployed to validate the defined framework.

CCS CONCEPTS

• **Security and privacy** → **Digital signatures**; *Network security*; • **Computer systems organization** → *Firmware*.

KEYWORDS

Post-Quantum Cryptography, Digital Signatures, Systems Migration

ACM Reference Format:
Marta I. García-Cid, Michail-Alexandros Kourtis, George Xilouris, David Domingo, Nikolay Tcholtchev, Evangelos K. Markakis, Marcin Niemiec, Vicente Martín, Laura Ortiz, Javier Faba, Diego López, Maria Gagliardi, José González, Miguel García, Giovanni Comande, and Nikolai Stoianov. 2024. PQ-REACT: Post Quantum Cryptography Framework for Energy Aware Contexts. In *The 19th International Conference on Availability, Reliability and Security (ARES 2024), July 30-August 2, 2024, Vienna, Austria.* ACM, New York, NY, USA, 7 pages. https://doi.org/10.1145/3664476.3670868

1 INTRODUCTION

In the last three decades, cryptography has become an indispensable component of global communication digital infrastructures. These networks support a plethora of applications that are important to our economy, security, and way of life, such as mobile phones, internet commerce, social networks or cloud computing. In such a connected world, the ability of individuals, businesses and governments to communicate securely is of the utmost importance.

ARES 2024, July 30-August 2, 2024, Vienna, Austria

ACM ISBN 979-8-4007-1718-5/24/07…$15.00
https://doi.org/10.1145/3664476.3670868

Cryptographic protocols have the main objectives of guaranteeing confidentiality, authenticity and integrity of the information exchanged along the different communication channels, relying for that on two core cryptographic functionalities: encryption and digital signatures. Currently, these functionalities are primarily implemented using different cryptographic techniques that can be included in two large groups: symmetric and asymmetric cryptography. A symmetric encryption protocol, such as the Advanced Encryption Standard (AES), is one in which the same secret key is used by both communicating parties in order to encrypt and decrypt information. In contrast, an asymmetric encryption protocol, such as the Diffie-Hellman key exchange, the RSA (Rivest-Shamir-Adleman) cryptosystem, and elliptic curve cryptosystems, is based on an interrelated public-private key system that is generated from a mathematical problem. Today, (pre-quantum) asymmetric techniques are essentially based on factorization of large prime numbers, discrete logarithm computation and Elliptic Curve Discrete Logarithm Problem (ECDLP). Both are dimensioned to be virtually impossible to solve with our current computing resources and mathematical knowledge. These fundamental problems, will no longer remain unsolvable if a large-scale and fault-tolerant quantum computer is built and thus the security of currently deployed pre-quantum public key cryptography could potentially collapse. Indeed, in 1994, P. Shor introduced a quantum algorithm able to solve these problems quite efficiently thereby rendering all pre-quantum public key cryptosystems based on such assumptions vulnerable [17]. Thus, a cryptographically-relevant quantum computer (CRQC) will put many forms of modern communication — from key exchange to encryption to digital authentication — in peril. Encryption systems based on AES are not affected by Shor's algorithm. Nevertheless, in the last two decades, increased speedups have been developed for broad classes of problems related to searching, collision finding, and evaluation of Boolean formula. In particular, Grover's search algorithm [8], running in a quantum computer, proffers a quadratic speedup on unstructured search problems. While such a speedup does not render cryptographic technologies obsolete, it can have the effect of requiring larger key sizes, even in the symmetric key case (i.e. AES). Quantum computers available today are not a threat. However, classified information systems could be suffering another type of attack called *store now, decrypt later*. Through this type of attack, a malicious actor could be storing encrypted information with current protocols, waiting to have enough computational capacity to break that encryption. If, in addition, we wait until quantum computers really pose a threat to start implementing quantum safe systems, we could be under the risk of experiencing a scenario like the one introduced by Mosca's Theorem [11] shown in Figure 1, in which during the time of implementation of the new systems, the critical classified information would no longer be protected.

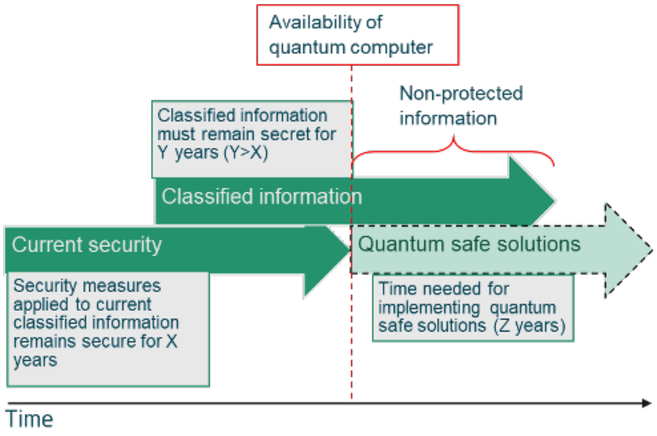
Availability of quantum computer
Non-protected information
Classified information must remain secret for Y years (Y>X)
Classified information
Current security
Quantum safe solutions
Security measures applied to current classified information remains secure for X years
Time needed for implementing quantum safe solutions (Z years)
Time

Figure 1: Temporal evolution of the security of cryptosystems.

The need for addressing this problem early enough was recognized by the National Institute of Standards and Technology (NIST) who started the identification, evaluation and standardization of cryptographic algorithms able to withstand quantum computer attacks.

While efforts for identifying which PQC algorithms are robust enough to provide suitable alternatives for the threat of quantum computers are still on going, the major problem of migration from today's widely deployed algorithms to future PQC alternatives across the diversity of computer systems that serve our society needs to be handled simultaneously. Today, there are more than 4.1 billion Internet users, nearly 2 billion websites, and more than 3 trillion dollars in retail activity associated with the Internet [18]. The extensiveness of public key cryptography usage across the Internet means that an industry-wide migration to quantum safe cryptography standards (i.e., PQC) will be a massive undertaking. The difficulty of this task relies on the layered complexity and heterogeneity of the worldwide computing infrastructures. In other words, there is a need for trade-offs among the number of configurable parameters of PQC algorithms (key size, ciphered text size, computation time, communication overhead etc.) and the requirements of the cryptographic systems and applications in various contexts (delay, memory, CPU, bandwidth, power consumption etc.), before the PQC migration can be adopted in practice and at a large scale.

To solve the above challenges, the international consortium financed by the European Commission (EC) will develop the 3-years project PQ-REACT. The main objective of PQ-REACT project is to design, develop and validate a framework for a faster and smoother transition from classical to post-quantum cryptography for a wide variety of contexts and usage domains. This framework will include PQC migration paths and cryptographic agility methods and will develop a portfolio of tools for validation of post quantum cryptographic systems that will allow users to switch to quantum safe solutions, taking under consideration their individualities and various contexts.

The remainder of this article is structured as follows. Section 2 reviews the framework designed to accomplish the different project objectives. Section 3 gives an overview of the final project pilots that will serve as a scenario for demonstrating the results. Section 4 describes the project expected outcomes and challenges to be overcome. Section 5 analyses the synergies with other related projects. Finally, Section 6 depicts the conclusions.

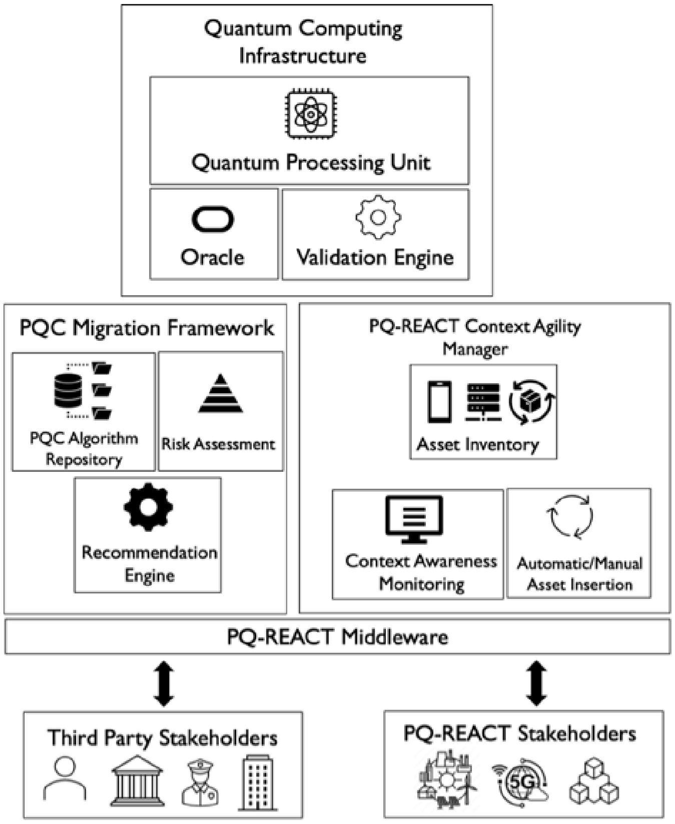

Figure 2: PQ-REACT Architecture.

2 PQ-REACT FRAMEWORK

PQ-REACT is aimed to design and build a framework for a faster and smoother transition from classical to PQC for a wide variety of contexts and usage domains. To accomplish this objective, a preliminary architecture was designed, taking into account innovative approaches and tools to enable crypto-agility and migration to new cryptographic algorithms and standards. The overall framework architecture is depicted in Figure 2
As a result, an open platform will be built to provide a portfolio of tools, including an actual quantum computer, for evaluation of PQC algorithms and cryptanalytical methods.

This type of framework has the potential to provide significant benefits in terms of easier migration, increased quantum computing infrastructure and enhanced crypto-agility. The main functional blocks of the framework architecture are described in the following subsections.

2.1 PQ-REACT Context Agility Manager

The notion of context agility considers cryptographic agility frameworks that automatically select among algorithms and configurations based on their context of use. The context-aware (CA) Manager uses data classification collected from the underlying infrastructure's assets and their security specifications to drive algorithm and parameter choices, managing trade-offs in specific ways. This framework contemplates the design and implementation of a Context Manager to seamlessly identify security assets with their context and automatically assess and provision the suitable algorithm and configuration for a given scenario. As part of the context agility manager, three building blocks are defined:

- **Context Awareness Monitoring.** A context-aware scheme able to choose the right set of algorithms and parameters for a particular regulatory environment or based on the availability of specific algorithms, the desired security level and the cost. In order to collect the required information and specifications of the system to be migrated, an agile data collection needs to operate to probe the specific security parameters.
- **Asset Inventory.** An appropriate inventory for collecting different assets and capabilities of the system under migration, as well as their different security parameters in a timely and agile manner.
- **Automatic/Manual Asset Insertion.** Installation of multi-agents and probes on the different systems and hardware and software components to be able to extract data and metadata from the assets for later integration in the system.

The Context Agility Manager is also aware of the underlying device platform and feed the collected data to the PQC Migration Framework to make decisions that better comprehend available computational and communication resources and the state of the system.

2.2 PQC Migration Framework

The proposed PQC migration framework stands on three main pillars:

- **PQC Algorithm Repository.** Serving as a live and dynamic library of PQC algorithms. The repository will be constantly updated thanks to the experience and lessons learned after the execution of the different use cases and pilots. The PQC catalogue includes information for the different specifications of the algorithm, its compatibility against different protocols and systems as well as a multi-modal characterization, referring to energy, computational complexity, etc.
- **Risk Assessment.** Providing an inventory of the main threats (ex. Privacy, information integrity, authority, traceability, etc.) is critical. This threat identification is connected to the use of different algorithms in various contexts, including specifications for the regulatory environment and legal requirements during the changeover to define the migration framework. Therefore, it provides instruments for adding (to the asset inventory) a list of recommendations and warnings related to the various parameters and requirements needed and used in the analysed legal framework.
- **Recommendation Engine.** Provides an approach to recommend or audit cryptographic algorithms and configurations. The recommendation engine considers the assets' characteristics as presented in the inventory and proposes the appropriate PQC algorithm, along with its configuration, for the cryptographic system under migration. The recommendation engine will contribute towards the vision of self-configuring cryptography, a vision that could drive a

new generation of cryptographic protections across a variety of infrastructure types and time scales. The important challenge is identifying where public key cryptography is being used in an organization's complex infrastructure and which algorithms and versions are deployed.

2.3 Quantum Computing Infrastructure

To be able to implement and provision tools for the automated benchmarking of PQC algorithms, several metrics, concepts and processes for the theoretical and practical validation of PQC algorithms are under definition. This objective will be reached thanks to the access to the IBM-FHG's quantum computer deployed in Ehningen [7]. The IBM-FHG quantum infrastructure is a reference deployment and technology ready to host and test different external tools and algorithms. For the quantum computing infrastructure of PQ-REACT the following building blocks are defined:

- **Quantum Processing Unit.** A QPU is the core processing module of the Quantum Computer, the component that performs the requested computations.
- **Quantum Oracles and APIs.** Quantum algorithms often operate on input information encoded in oracles, which are callable black box circuits. The PQ-REACT quantum API translates incoming requests (to a quantum computer) into quantum oracles to be used as the gateway for different algorithms and mechanisms to be tested and validated on the QPU.
- **Validation Engine.** Automated testing tools are sorely needed to test different parameters of PQC migration mechanisms, and to explore cryptographic failure modes, whether PQC algorithm specific or migration framework based. The development of a framework for synthesizing migration and validation code is needed, inserting test cases into the developer toolchain, modifying binary images for legacy software, and so on. The validation engine will also implement check mechanisms to prevent malicious algorithms and implementations for a given usage domain.

3 PQ-REACT PILOTS

As a validation and demonstration methodology of the theoretical and technological outcomes, three pilots will be carried out: 1) Smart Grid deployments, 2) Hybridization of QKD and PQC keys for 5G Networks and 3) Distributed Ledger Technologies (DLT) for E2E Network Services. For each scenario, assets are identified as different components from the defined use cases, e.g. IoT meters for Smart Grid, and generate different security requirements, with different cryptographical capabilities. The asset inventory will generate a catalogue of assets from each of the use cases to detail their specifications and compatibility with different PQC algorithms, which based on the PQ-REACT workflow will be properly selected for usage.

The recommendation engine and its supporting modules will be employed for the three pilots, and will be demonstrated in complex and multi-layered cryptographic environments.

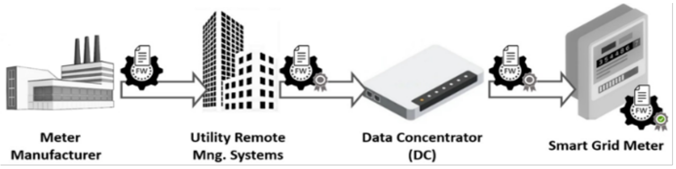

Figure 3: Smart Grid Pilot Overview.

3.1 Pilot 1: Application of Quantum Resistant Crypto to Smart Grid deployments

Secure Firmware (FW) Update process for deployed Smart Meters, when protected by asymmetric crypto, usually relies on ECDSA in order to address the devices limitations on processing, storage, and/or bandwidth capacity. Figure 3 shows a diagram of pilot 1. For the use case, FW images will be signed by the Utility, relying in its private key, before being distributed to the deployed meter devices. For its part, the meters will be responsible to verify the FW signature, based on the possession of the corresponding Utility FW public key. Finally, the Utility FW public key stored in the Meters will be regularly updated.

3.2 Pilot 2: Converged QKD and PQC Application for Next-Generation Networks (5G and beyond)

PQC and QKD are the two battle horses for a future-proof quantum-resistant network infrastructure. While they are completely different, one based on computational security and other on the laws of quantum physics, and leading to different implementations with different strengths and weaknesses, their combination seems the natural way to follow in complex systems like 5G networks and its future successors. Their application to significant use-cases will be investigated, especially related to edge applications in industrial environments, addressing the security requirements in highly-pervasive, critical networked environments. The use of low latencies and high security achieved by QKD technology is planned in core network elements, combined with the use of PQC at the edge and terminal elements. By means of integrated key management procedures, supported by Software Defined Network (SDN) and network virtualization concepts (see Figure 4), the hybridization of both technologies and the advantages of an elastic approach to edge security hardening will be demonstrated.

The use cases of this pilot will be demonstrated on the MadQCI environment [10], currently the largest QKD network deployed in Europe, connected to the 5TONIC testbed [1], an experimental infrastructure for next-generation network technologies and services, instrumental in the execution of many European projects. Both infrastructures are part of the proposed EuroQCI-Spain network, and therefore suitable to extend experiments beyond, through the HellasQCI [9].

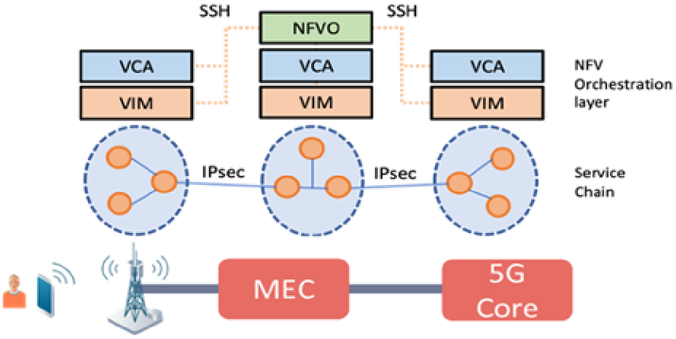

Figure 4: QKD-5G Pilot Overview.

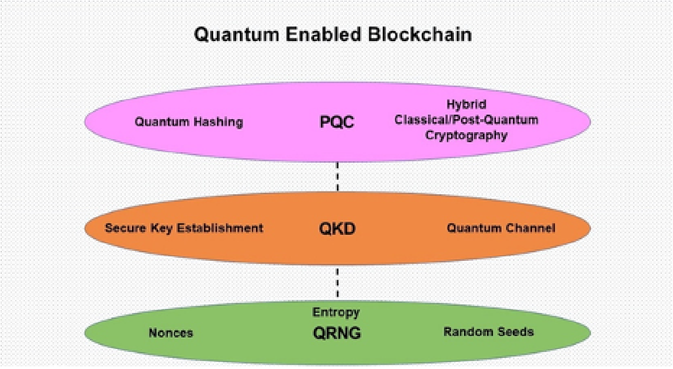

Figure 5: PQC Blockchain Pilot overview.

3.3 Pilot 3: Quantum Resistant Distributed Ledger for E2E Network Services

The concept of network slicing in telecommunications is continually evolving, with blockchain technology adding a new layer of possibilities and challenges. As detailed by [14], network slicing provides an efficient, service-oriented infrastructure, an attribute made possible by the inherent flexibility of Software Defined Networks (SDN) and Network Function Virtualization (NFV). These technologies facilitate the abstraction of network functionality into manageable slices, creating customized and optimized network resources to meet specific service demands. The integration of blockchain into this network slicing framework is considered a significant strategic shift, transforming the delivery of services from providers to users across varied administrative domains. Nevertheless, the rise of quantum computing presents significant challenges to the security of cryptographic systems, including those used in distributed ledger technologies. As noted in [19], the advent of quantum computing has profound implications for cryptographic systems, raising concerns about their quantum resilience. The rapidly evolving field of Post-Quantum Cryptography (PQC) seeks to address these threats, opening the door to the integration of PQC into existing network technologies. This progression represents a pivotal step in the development of quantum-secure telecommunications infrastructure, securing ledger technologies against quantum threats, and enabling the creation of robust, scalable, and quantum-resistant telecommunications infrastructure. The potential to develop cost-effective, on-demand end-to-end (E2E) network slices that can be allocated to various services forms a fundamental attribute of high-quality telecommunications networking services. E2E network slicing represents a strategic paradigm shift, aiming to streamline the delivery of services from providers to consumers across diverse administrative domains. In essence, a network slice amalgamates resources that originate from distinct infrastructure providers. The Network Operations Centre (NOC) incorporated within HellasQCI, furnished with Quantum Key Distribution (QKD) capabilities, currently provides a range of connectivity services to various academic partners. A fresh perspective in managing service agreements and efficiently supervising Service Level Agreements (SLAs) involves employing Distributed Ledger Technologies (DLTs)/Blockchain. DLTs currently operate on several cryptographic protocols, which unfortunately are not fortified against quantum attacks. This scenario will examine the potential of Post-Quantum Cryptography (PQC) algorithms embedded within ledgers for establishing agreements amongst a multiplicity of network providers, as depicted in Figure 5. The focus will be directed towards the creation and integration of Quantum Resistant Ledgers (QRLs) into a network slicing framework. QRLs offer a novel strategy for mitigating potential vulnerabilities in current cryptographic protocols, securing ledger technologies against quantum threats. Their integration into the network slicing framework may signify an essential step towards creating robust, scalable, and quantum-resistant telecommunications infrastructure. The prospective enhancement in handling service agreements could lead to a more resilient network and expedite a more reliable service delivery across diverse administrative domains. This study underscores the significance of integrating quantum-resistant technology in modern telecommunication systems, thus offering a viable solution to the potential threats posed by quantum computing advancements.

4 PQ-REACT OUTCOMES AND CHALLENGES

A series of theoretical and technical objectives are expected to be accomplished, associated with the different frameworks that allow establishing the fundamentals for a controlled and friendly implementation of quantum safe solutions.

Specifically, the construction of a secure cryptographic framework for different vertical applications, combining both existing quantum and post-quantum mechanisms, is envisioned. The framework will be based on a hybrid Quantum and Post-Quantum cryptography system, which according to different use cases and context agility will be able to assess, validate and recommend a specific cryptography algorithm considering a multi-variant security environment.

In addition, the design and implementation of an open cryptography repository, detailing the specification of different pre-quantum and post-quantum algorithms, in terms of energy consumption, complexity, applications and compatibility to different end devices. The repository part of the complete Post-Quantum framework will analyse the gaps of different algorithms and using the described use cases' requirements will address different practical barriers towards the wider adoption of quantum resistant mechanisms.

For that, a holistic framework for classical and quantum resistant algorithm analysis and integration will be designed and developed. Its different layers and individual components will cover context agility. Each step of the process (pre-quantum to PQC migration, algorithm recommendation, risk assessment and use case deployment) takes into account different factors regarding energy, complexity, compatibility, and proceeds to make the suitable recommendation for deployment. The migration framework will investigate the different strategies and mechanisms required to migrate from pre-quantum systems to quantum resistant ones. This includes different key sizes and configuration parameters. Additionally, the hybridization of QKD with PQC in 5G communication networks will be investigated, in order to further fortify telco channels and render them future-proof cryptographically. The project will also validate the proposed solutions on a state-of-the-art group of testbeds.

The aim is not only the proposal of different mechanisms to introduce new quantum resistant mechanisms, but also their measurement and testing on high-performance and quantum computing infrastructures (e.g. the IBM-FHG computer). This will ensure the applicability and feasibility of the tests against a cutting-edge setup and will accelerate the reporting of different compatibility and integration issues and challenges that may arise. Furthermore, the description and development of three different use cases in the frame of the project will help the implemented framework to be tested and validated on a large scale of scenarios and test cases.

In addition to the design of the different frameworks and technological developments, the scope of all the objectives described is linked to a series of challenges that have been detected and that will need to be addressed. The first of them is the lack of tight coordination among CERTs, CISRTs, and NOCs. The inter-organization intelligence sharing features privacy preservation by design and exposure control built in, which will assist alleviate worries about privacy violations in the involved organizations during intelligence sharing. The second challenge is the scarcity of trustworthy PQC solutions for security, particularly for automated operations. To alleviate this problem, security management operators with the Quantum Validation option will be provided.

In addition, there are a number of security concerns about the collection and storage of data including the responsibility to ensure that the data is secure. Also, within the legal sphere, much of the data produced or used by smart grid and mobile technologies may include information about people and their behaviour and so raises issues concerning privacy. Furthermore, the power of data analysis is such that even apparently trivial data can be used to discern statistical patterns that reveal much richer personal information. These types of challenges require the implementation of security measures that protect data from inappropriate access, but also maintaining the integrity of data and the robustness and resilience of the systems that process it, as well as, when appropriate, the use of techniques for pseudo-anonymization of data.

5 RELATION WITH OTHER EU PROJECTS

PQ-REACT will leverage a wide background from existing R&D activities. The consortium partners have already a strong involvement in relevant initiatives and have identified a number of projects, in which they are already participating and whose results can be transferred and exploited for PQ-REACT. This interoperability between projects is of special interest for a hybridization of cryptographic solutions capable of integrating classical, quantum and post-quantum mechanisms with a crypto-agile approach.

Within the H2020 and Horizon Europe funding frameworks, a series of projects have been detected within the topic of cybersecurity and cyberdefence to provide new tools and processes to cyberspace as the last incorporated operational domain. Projects such as PALANTIR [13] and SANCUS [15] stand out, whose main objective is the development of cybersecurity and trust solutions for edge infrastructures in the case of PALANTIR and optimization models in SANCUS. Furthermore, the ECHO project [6] delivers an organized and coordinated approach to improve proactive cyber defence of the European Union, through effective and efficient multi-sector collaboration. As part of technological developments within the field of Information and Communication Technologies (ICT) and connectivity, the 6GStart [2] and NGI Sargasso [16] projects stand out. The former aims to facilitate the preparation activities of the European Smart Networks and Services Joint Undertaking, maintaining the European leadership achieved through the 5G PPP and to carry it forward, while the latter (NGI Sargasso) proposes open calls management to combined research projects in ICT (including cybersecurity) among EU-US and EU-Canada. Despite working on the classical cryptographic level, all the mentioned projects have a strong technological and strategic interest in the analysis of quantum safe solutions.

Within the field of quantum cryptography, the consortium has a strong scientific and technical core. Projects like OpenQKD (Open European QKD testbed) [12] or CiViQ (Continuous Variables Quantum key distribution) [5], provide the optimal infrastructure and services for the design and implementation of hybrid cryptographic solutions in near-real environments. OpenQKD is considered as the ramp-up phase of the European Quantum Communications Infrastructure and as such it has an important strategic role. It defines 4 major testbeds and about 15 minor ones. One of the major ones is the MadQCI that will be used for PQ-REACT. For its part, CiViQ is one of the only three ones awarded to the Quantum Communications pillar of the quantum flagship. It has developed basic techniques to integrate QKD devices in networks. Going further to the spatial segment, we highlight the CARAMUEL project [4], a Spanish initiative where companies, research centres and universities work together in the field of quantum technologies to accomplish the ultimate goal of including a quantum key distribution (QKD) mission as a payload hosted in the future satellite SPAceQr GEO, in order to reach large distance QKD.

Within quantum sensing technologies, the ADEQUADE Project (Advanced, Disruptive and Emerging QUAntum technologies for Defence) [3] is of special interest, since it intends to provide improvements to a whole range of quantum sensing domains such as Positioning, Navigation and Timing (PNT) quantum sensors, Quantum Radio Frequency (RF) sensing and Quantum optronic sensing. These types of projects are strongly related to PQ-REACT insofar as the information that is extracted from the sensors can be considered critical and must be secured, especially under the approach to distributed sensor network architectures.

Finally, there is a direct synergy between PQ-REACT and the NATO

Industrial Advisory Group (NIAG) SG-251 on Data Centric Security, where an in-depth analysis of the applicability and impact of PQC Crypto to NATO STANAG 4774 & 4778 Standards was carried out.

6 CONCLUSIONS

As a contribution to strengthening the EU cybersecurity capacities and European Union sovereignty in secure digital technologies under the future threat of quantum computing, PQ-REACT proposes the design, development and validation a framework for a faster and smoother transition from classical to post-quantum cryptography. Opening the possibility to combine PQC and QKD keys to address different problems. This framework provides a strategy for the migration of existing network and telecommunication infrastructures and protocols (e.g. PKI, VPN tunnels, certificate chains, etc.) to post-quantum cryptography hybridizing the solution with QKD technology as a key exchange method for symmetric cryptography related to 5G networks.

For that, an inventory of cryptographic assets and processes in the cryptographic system to be migrated will be created and integrated with a recommendation engine to propose a migration plan, taking under consideration these assets and the various contexts that PQC will be employed. The performance of PQC algorithms on various implementation platforms (from large data centres to IoT devices) can be optimized, taking under consideration delay, memory, CPU and energy consumption restrictions.

In the quantum computing segment, the usage of an IBM-FHG Quantum Computer together with additional High-Performance-Computing resources and network testbeds, as well as, the design and development of interfaces for the Quantum Computer and the provisioning of a portfolio of open tools will allow to test and benchmark new PQC algorithms and new cryptanalytical methods. All the project developments, results and recommendations will be demonstrated and validated in the project pilots.

ACKNOWLEDGMENTS

This work has been performed in the scope of the PQ-REACT European Union's Horizon Europe research and innovation programme under grant agreement No. 101119547.

REFERENCES

[1] 5TONIC. 2023. An open research and innovation laboratory focusing on 5g technologies. http://5tonic.org.

[2] 6GStart. 2023. Starting the Sustainable 6G SNS Initiative for Europe. https://5g-ppp.eu/6gstart/.

[3] ADEQUADE. 2023. Advanced, Disruptive and Emerging Quantum technologies for Defense. https://adequade.eu/.

[4] Angel Alvaro, Luis Pascual, Antonio Abad, Pedro Pinto, Alberto Alvarez-Herrero, Tomas Belenguer, Carlos Miravet, Pablo Campo, Luis F Rodriguez, Marcos Reyes, et al. 2022. Caramuel: The future of space quantum key distribution in geo. In *2022 IEEE International Conference on Space Optical Systems and Applications (ICSOS)*. IEEE, 57–65.

[5] CiViQ. 2023. Develop quantum-enhanced physical layer security services, combined with modern cryptographic techniques, to enable unparalleled applications and services. https://civiquantum.eu/.

[6] ECHO. 2023. European network of Cybersecurity centres and competence Hub for innovation and Operations. https://echonetwork.eu/.

[7] Fraunhofer. 2023. Quantum computing. https://www.fraunhofer.de/en/research/current-research/quantum-technologies/quantum-computing.html.

[8] Lov K Grover. 1996. A fast quantum mechanical algorithm for database search. In *Proceedings of the twenty-eighth annual ACM symposium on Theory of computing*. 212–219.

[9] HellasQCI. 2023. Strengthen the resilience of critical infrastructure in the Greek territory against cyber threats. https://hellasqci.eu/.

[10] D Lopez, Juan Pedro Brito, Antonio Pastor, Vicente Martín, C Sánchez, D Rincon, and Víctor López. 2021. Madrid Quantum Communication Infrastructure: a testbed for assessing QKD technologies into real production networks. In *Optical Fiber Communication Conference*. Optica Publishing Group, Th2A–4.

[11] Michele Mosca. 2015. Cybersecurity in a Quantum World: will we be ready? https://csrc.nist.gov/csrc/media/events/workshop-on-cybersecurity-in-a-post-quantum-world/documents/presentations/session8-mosca-michele.pdf.

[12] OpenQKD. 2023. https://openqkd.eu/.

[13] PALANTIR. 2023. Practical Autonomous Cyberhealth for resilient SMEs & Microenterprises. https://www.palantir-project.eu/.

[14] Y. Liang S. Bao and H. Xu. 2022. Blockchain for Network Slicing in 5G and Beyond: Survey and Challenges. *in Journal of Communications and Information Networks* 7, 4 (2022), 349–359. https://doi.org/10.23919/JCIN.2022.10005213

[15] SANCUS. 2023. Analysis Software Scheme of Uniform Statistical Sampling, Audit and Defence Processes. https://sancus-project.eu/.

[16] NGI Sargasso. 2023. https://www.ngi.eu/ngi-projects/ngi-sargasso/.

[17] P. Shor. 1997. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. *SIAM J. Comput.* 26, 5 (1997), 1484–1509. https://doi.org/10.1137/s0036144598347011

[18] WebsiteSetup. 2021. Internet Stats & Facts. https://hostingfacts.com/internet-facts-stats/.

[19] Gagan Yalamuri, Prasad Honnavalli, and Sivaraman Eswaran. 2022. A review of the present cryptographic arsenal to deal with post-quantum threats. *Procedia Computer Science* 215 (2022), 834–845.