Pioneering Security in the Quantum Era: Preparing Travelers Insurance for a Post-Quantum Future

Samuel T. Oakes
Sacred Heart University
oakess2@mail.sacredheart.edu

Ryan J. Novara
Sacred Heart University
novarar@mail.sacredheart.edu

Maniraj Chahal
Sacred Heart University
chahalm@mail.sacredheart.edu

Anthony M. Scardigno
Sacred Heart University
scardignoa@mail.sacredheart.edu

EXECUTIVE SUMMARY

The emerging transformations related to Quantum Computing are reshaping the fields of business and technology with the same level of digital disruption and potential that presented itself with the rise of widespread-use Artificial Intelligence (AI) systems. As AI shifted the paradigms of business operations into a new era of automation and predictive analysis which enabled rapid advancements in a broad range of industries, Quantum Computing promises to redefine computational limits and tackle tasks that modern classical computing cannot solve today. Quantum computing technologies will have an immense impact on humanity's ability to conquer our society's most difficult problems, including medical research to pursue a cure for cancer and other deadly diseases. However, the foreseen benefits of this emerging technology are not without risks. Any rapidly developing technology poses risk for disruption, and quantum computing is no different. According to the World Economic Forum, "These advances in computational power will also introduce significant risks via the potential threat of disruption to some widely used encryption standards." [8]. In this white paper, we provide some background information regarding Quantum Computing technologies and evaluate a variety of relevant responses to provide recommendations and integration strategies for our Quantum CT Challenge corporate partner, Travelers Insurance. In the words of the late Jack Welch of General Electric, the namesake for our College of Business & Technology, we hope that our recommendations empower you to *"change before you have to"*.

KEYWORDS

Quantum Computing, Digital Transformation, Risk Mitigation, Emerging Technologies, Data Security

Oakes, S. T., Novara, R. J., Chahal, M., Scardigno, A. M., & Santorelli, C. J. (2024). *Pioneering Security in the Quantum Era: Preparing Travelers Insurance for a Post-Quantum Future*. Sacred Heart University.

1. INTRODUCTION

As we prepare for the next generation of cybersecurity challenges posed by advancements in quantum computing, a forward-thinking security posture focused on developing resilient strategies to safeguard the people, assets, and data of Traveler's stakeholders is necessary.

The Quantum Lockdown challenge aims to address how to fortify the future of cybersecurity standards and practices in the Post-Quantum Cryptography (PQC) era.

2. BACKGROUND

Quantum computing is an evolving field which leverages properties of quantum mechanics to find solutions for complex problems that are impossible to solve with traditional computers which process data using binary bits (zeroes and ones). Quantum computers operate on a new paradigm, using qubits which can represent multiple states simultaneously due to superposition. The difference between these two ways of computational thinking is best described using analogy, "Quantum computing is like having a special umbrella that can stretch and adapt instantly to cover any number of storms or weather conditions at once. While traditional computing looks at risks one at a time, and only handles one scenario".

The power of this new technology suggests that it has the potential to bring forth significant disruptions in a multitude of industries, most notably the insurance sector. The Cybersecurity and Infrastructure Security Agency (CISA) emphasized how disruptive quantum computing may become stating that a cryptoanalytically-revant quantum computer (CRQC), a computer powerful enough to break modern encryption standards using complex mathematics, "would have the potential to break public-key systems (sometimes referred to as asymmetric cryptography) that are used to protect information systems today" [10]. A CRQC in the hands of an

adversary would pose an industry-wide critical infrastructure threat, breaking the protocol which protects our most sensitive data. With respect to our stakeholders in the insurance sector, not only would this undermine customer privacy and impact public trust, but it also would have a monstrous impact on closely guarded trade secrets and confidential business operations.

To mitigate these risks, the next critical step for Travelers is the development and adoption of post-quantum cryptography standards (PQS) outlined in this white paper. This focus is crucial for the company's ongoing commitment to ensure the safety and security of their sensitive data, proprietary information, and business operations, safeguarding the company's integrity and infrastructure for the uncertain future.

3. KEY BUSINESS HYPOTHESIS AND CUSTOMER IMPACTS

The development of quantum cryptography presents significant opportunities for technological advancements that can greatly impact society. However, quantum computing has the capabilities to render most classical computing encryption methods obsolete, thus posing a massive threat to businesses and the customers whose data they are responsible for safeguarding.

For Travelers Insurance:

1. A proactive adoption of PQC methods offers an approach that will preemptively address these evolving threats, securing customer data, implementing effective cybersecurity standards and working towards integrating post-quantum encryption standards (PQS) with the current classical ones to protect against adversarial attacks that could lead to severe profit loss, significant downtime and leaks of confidential customer and employee data.

This proposal is centered on three critical principles *Recognize*, *React*, and *Respond.* Travelers must *Recognize* the consequences of failing to adopt quantum-safe measures, particularly as they regard data breaches customer trust/transparency and business continuity.

Then, they must *React* accordingly to rapid advancements in quantum computing by positioning themselves in the forefront of PQC implementation. Finally, they must *Respond* with a well-planned, phased approach that ensures policy alignment and minimal disruption to business processes allows the organization to respond in an orderly and efficient manner.

Through this strategic phasing of PQC integration, Travelers can establish a sustainable foundation for safeguarding customer data, and work towards securing its cybersecurity infrastructure against emerging adversarial attacks that could pose a severe threat to the confidentiality of customer information and the continuous flow of business operations.

4. KEY BENEFITS OF PQC FOR TRAVELERS' CUSTOMER BASE

Enhanced Data Security

As mentioned, the benefits of adopting PQC extend beyond the immediate risk mitigation offered through its implementation. It also offers advantages to Travelers' customers through the continuity and resilience of insurance services. ensuring that customers' personal and financial data remain safeguarded as cryptographic vulnerabilities evolve. PQC solutions, designed to withstand quantum attacks, contribute to robust data protection that surpasses traditional encryption, building a foundation of secure data practices that will protect customers for years to come.

The proactive integration of PQC demonstrates Travelers' dedication to staying ahead of technological risks and securing customer data through advanced solutions. By leading the insurance industry in adopting these security measures, Travelers can strengthen customer confidence, reinforcing loyalty and trust in its ability to protect sensitive information. This commitment to data integrity differentiates Travelers in the marketplace, appealing to security-conscious customers who value robust protection.

Future-Proof Insurance Services

PQC allows continued resistance to the cryptographic challenges posed by quantum computing, also allowing Travelers to provide future-proofed insurance services. Customers can expect continuous, reliable protection even as technology advances, with a higher likelihood of minimal disruptions to policy coverage, claims processing, and customer service availability. This integration reassures customers that their data and transactions will remain secure despite potential shifts in cybersecurity threats.

Reduced Financial Risk for Customers
The strength of PQC in mitigating risks related to identity theft and fraud has direct financial implications for customers. Enhanced defenses against cyber-attacks lower the likelihood of breaches that could lead to personal losses, thus supporting customers' financial stability. By proactively securing data against quantum threats, Travelers offers a more resilient environment for customer information, helping to minimize the financial impact of security incidents on its clientele. A 2022 study conducted by Market.us found that, "only 19% of organizations reported having cyber insurance coverage that extends beyond $600,000" [11].

Aligned Security and Regulatory Compliance
As regulatory expectations for cybersecurity grow, particularly in the face of emerging quantum risks, Travelers' adoption of PQC serves to meet these evolving requirements. Customers benefit from knowing that their data is not only protected by state-of-the-art encryption methods but is also safeguarded in a manner consistent with national and international regulatory standards. This alignment with security and compliance standards further strengthens the credibility and reliability of Travelers' customer data protection policies. According to Cisco's 2022 Consumer Privacy Survey, "81% of users believe the way a company treats their personal data is indicative of the way it views them as a customer" [12].

5. EVALUATION CRITERIA

Business Alignment
With the integration of any cybersecurity practices, ensuring that security aligns with the goals of the business allows for an approach that provides the necessary security of the business from adversarial attacks without interfering with operational procedures. Implementing the proper PCE methods to the appropriate business elements adopting the idea to "Defend diamonds like diamonds and pencils like pencils" [13].

This approach aims to find a cohesive solution to security that allows the business to operate in a way that it is not hindered from overly stringent security measures but also for cybersecurity to be an afterthought that then in turn cripples the business and leads to significant profit loss.

Quantum Resistance
An essential criterion for post-quantum cryptographic algorithms is their resilience against quantum-based attacks, particularly Shor's and Grover's algorithms. This involves assessing the algorithm's foundational structure—such as lattice-based, hash-based, or error-correcting code-based—which influences its resistance to quantum computation techniques. An ideal quantum-resistant algorithm should demonstrate immunity to Shor's algorithm for public-key attacks and should mitigate vulnerabilities exposed by Grover's search algorithm, which affects symmetric keys.

Classical Resistance
Alongside quantum resistance, an algorithm must show strong classical resistance to traditional attacks. Evaluating this aspect ensures that algorithms provide immediate protection against current threats during the transitional period before quantum computing becomes prevalent. Classical resistance can be assessed through the algorithm's historical performance against well-known attack methods in public cryptographic testing environments, as well as its reliance on proven mathematical principles.

Key Generation, Encryption/Decryption
The efficiency of an algorithm is crucial for high-demand applications that require rapid response times, such as real-time communications. Algorithms should be evaluated based on the time taken for key generation, encryption, decryption, and signature processes, as well as on their suitability for environments requiring low latency. Performance benchmarking should reflect the algorithm's practicality in both high-performance and constrained computing environments. For performance testing, metrics such as latency, CPU load, and energy consumption are critical, as they provide a comprehensive view of the algorithm's operation impact. Algorithms that optimize these performance metrics without compromising security are highly suitable for scenarios where both speed and security are non-negotiable.

Computational Complexity
Post-quantum algorithms often have increased computational demands due to the additional security layers needed for quantum resilience. Evaluating computational complexity involves analyzing the resources required for processing, such as memory, CPU, and energy consumption. Algorithms suitable for low-complexity requirements—especially in resource-constrained environments are those with efficient operations that balance security with reduced computational load. An algorithms computational demands can be evaluated through factors like the number of operations required per cycle and the algorithms compatibility with hardware optimizations. Hash-based systems, for example, often have a tree structure that, while secure, adds computational overhead that may limit their usability in resource-constrained applications.

Key and Signature Sizes
Quantum-resistant algorithms typically require larger key sizes than their classical counterparts. An effective evaluation criterion should consider how key size impacts storage, transmission bandwidth, and system memory usage. Smaller key sizes are generally more practical for environments with limited storage, while larger key sizes may still be acceptable if the application has sufficient resources. The consideration of key size is crucial in cloud-based and distributed environments, where key management scalability is essential.

For signature-based algorithms, signature size can significantly impact data transmission efficiency and suitability for applications with frequent authentication requirements. Algorithms should be assessed based on the length of their signatures relative to their security levels, particularly in environments with bandwidth limitations. Smaller signatures sizes, while maintaining security, are advantageous in real-time or high frequency communications. Signature schemes are thus evaluated not only on security but also on their practicality for high volume or bandwidth limited applications.

In security critical applications like electronic voting or digital rights management, the choice of algorithms must balance signature size with the need for practicality and reliable authentication.

Forward Secrecy and Key Rotation
Forward secrecy is essential for applications that require long-term confidentiality, such as secure archival or government communications, as it ensures that previous communications remain secure even if current keys are compromised.

Forward security is often achieved through session based key agreements or one time use signatures, as seen in hash-based algorithms, which prevent retroactive exposure of data. When evaluating an algorithm, forward secrecy is a critical security component, particularly in applications where confidentiality over an extended period of time is paramount. Assessing an algorithm's structural ability to prevent retrospective decryption, even in the event of key compromise, is essential for security-critical data and communication systems.

Key management and Rotation Complexity
Efficient key management and rotation are vital for dynamic systems that regularly update security parameters. Algorithms with smaller, more manageable key sizes facilitate easier rotation, which is essential in environments with high-security requirements. Complex key rotation processes, especially in algorithms with extensive key sizes, may challenge performance efficiency. An ideal post-quantum algorithm offers both secure key rotation and user-friendly management procedures, reducing the need for extensive resources or intervention. For security sensitive applications, key rotation should minimize operational disruption while maintaining stringent security, allowing organizations to adapt encryption keys regularly without compromising system performance.

Standardization and Maturity
Algorithms that have achieved advanced status in standardization processes, particularly those endorsed by the NIST Post-Quantum Cryptography Standardization project, offer greater confidence in their security and usability. Standardized algorithms indicate reliability, as they have undergone extensive public scrutiny and peer-reviewed testing. In selecting post-quantum algorithms, adherence to standards is critical for interoperability and trust.

Standardization status can provide organizations with assurance in the algorithm's robustness and readiness for real-world implementation, helping to ensure consistent protection against both current and future quantum threats. This status also enhances the algorithm's credibility for long-term deployment, especially in fields requiring strong regulatory compliance, such as finance and healthcare.

Algorithms with solid theoretical foundations and extensive histories of public testing demonstrate cryptographic maturity. Algorithms based on well-established mathematical structures, such as lattice or hash-based designs generally exhibit greater reliability due to their theoretical robustness and empirical performance. A track record of rigorous testing and public analysis in diverse environments provides confidence in the algorithm's stability, as potential vulnerabilities have been vetted and addressed. In the assessment framework, maturity is a valuable criterion, highlighting the importance of selecting algorithms that have shown resilience through extensive analysis and practical application, thus reducing the likelihood of unknown weaknesses.

6. ALGORITHM RANKINGS & RECOMMENDATIONS

CRYSTALS Kyber

CRYSTALS Kyber comes out as the first choice for Travelers Insurance for its complete alignment with the assessment criteria. First, for the business alignment, Kyber is integrated into the already existing system with minimum hardware alteration while offering the required security for the continuity of the business "without interfering with operational procedures." This aspect is of prime importance to get security while communicating with external parties in support of continuity. Kyber owes its quantum resistance to lattice-based construction, providing very high resistance against most powerful quantum attacks like Shor's and Grover's algorithms, hence enabling the long-term security in a quantum future.

Further, its classical resistance protects it against conventional cryptographic threats immediately, making the algorithm relevant today and in a quantum-enabled future.

Kyber is also highly effective at key generation, encryption, and decryption efficiency, allowing for real-time communication demands that must have fast response times. More importantly, it does help in Travelers because the latency needs to be pretty low in the exchange of data. Computationally, Kyber achieves a very good balance between security and computational load and can be light enough not to put stress on current resources, another important consideration in a resource-aware environment. Its key sizes are comparatively small, thus making it very suitable for environments that have very limited storage and bandwidth. This further supports high-frequency communications without overwhelming the system. Kyber as well offers forward secrecy, simplification of key rotation, and management, ensuring that even if a key gets compromised, the protection of past communications is maintained, which is a vital factor for the maintenance of long-term confidentiality. Due to the fact that NIST has endorsed Kyber, its standardization and maturity provide confidence in its reliability and resilience. Therefore, it is suitable for finance and insurance applications that require robust real-world security.

CRYSTALS Dilithium

CRYSTALS Dilithium is a second-best digital signature algorithm more worth using for securing transaction authentication inside the customer service portal. Regarding business alignment, Dilithium is a good choice to authenticate customers. It gives authenticated encryption without incurring excessive operational complexity to develop trust in transactions. Its lattice-based structure offers high quantum resistance, mainly against attacks like Shor's algorithm, and guarantees reliability in high-stake transaction integrity. Its classical resistance is just as strong, harnessed from a design tested adequately within cybersecurity and quantum computing community and hence serving immediate protection against today's threats during transition to quantum-safe solutions.

Dilithium allows key generation and decryption to be highly efficient. This opens the possibility of fast and secure digital signatures, which is very critical on real-time interactions, particularly on service portals that experience high demand.

Dilithium's resource demands are reasonable, making it suitable for resource-constrained environments. For this reason, high-frequency communications such as transaction authorizations can be secure and responsive. The small key and signature sizes improve transmission efficiency and are therefore helpful to bandwidth-limited applications, decreasing potential latency. Although Dilithium doesn't provide any forward secrecy, its design itself does save the past data due to the proper key management practice. That keeps the customer authentication safe and protects older data from getting exposed. Key management and rotation complexity remains low due to the manageable key sizes in Dilithium, allowing routine updates securely without resource overloads. Its standardization and maturity, as evidenced by the endorsement of NIST, further the reliability of Dilithium to make it practical for authenticating transactions where security and trust are paramount.

AES-256

AES-256 comes third in the ranking, hence a good choice for encrypting sensitive internal data such as customer records or financial data at Travelers Insurance. This business alignment puts "defending diamonds like diamonds," where the algorithm operates with high security for the most important data, not interrupting other operations. AES-256 remains viable in a quantum context and in particular with respect to Grover's algorithm, although the application is presently
limited to symmetric encryption and "is still doing quite a robust database encryption against current and foreseeable quantum threats.". The AES-256 is also large in classical resistance, with its secure usage across many industries, securing data against all known cryptographic attacks.

Efficiency at key generation, encryption, and decryption of AES-256 rounds allows for very high speeds, suitable even in high-demand applications, such as data-at-rest encryption, for which it should not slow down other business functions. The computational complexity is low as well, being applicable in environments when protecting data without excessive resource consumption.

Smaller key sizes for AES-256 also make it practical for both storage and management; thus, the implementation becomes simpler in constrained resource environments. While AES-256 does not have forward secrecy, the capability for key rotation performs well with respect to data-at-rest applications and ensures that compromised keys do not expose all stored data. The complexity related to key management and its rotation remains really simple for the algorithm owing to smaller key sizes, reducing the operational load while maintaining strong security. Finally, standardization and maturity, validated by extensive real-world use and analysis, make AES-256 a credible standard of security for internal database protection that can be deployed for the long term at Travelers Insurance.

Kyber, Dilithium, and AES-256 provide Travelers Insurance with a comprehensive security approach, meeting all evaluation criteria and ensuring efficient, long-term protection for both external and internal data.

7. INTEGRATION STRATEGY (Transition)

Implementing a strategic approach for Crystals Kyber, Crystals Dilithium, and Advanced Encryption Standard (AES) to strengthen cybersecurity against both quantum and classical threats, while ensuring compatible integration with business practices. These procedural implementations allow an efficient and ultimately secure transition to PCE standards while ensuring the continuance of everyday operations.

Crystals-Kyber

Evaluate the current set of encryption protocols to determine effective implementation points for Crystals Kyber. Develop protocols enabling seamless integration with existing encryption methods to ensure security is maintained throughout the transition. Run a pilot in a controlled environment to validate the performance and security of Crystals-Kyber in realistic conditions.

Crystals-Dilithium

Conduct orientation sessions for users on the digital signature features of Crystals Dilithium. Upgrade existing digital signature infrastructures to host Crystals Dilithium, providing better security. Continuously keep track of the effectiveness of Crystals Dilithium in defending against unauthorized access and signature forgery.

Advanced Encryption Standard (AES)
Upgrade AES implementations to AES-256 for better security. Periodic audits should be performed to identify vulnerabilities in AES. Study the hybrid models of encryption that couple AES with post-quantum algorithms to improve the protection against both classical and quantum threats.

Next Steps
Establish a timeline for each encryption method's integration and allocate resources and personnel accordingly. Encourage cross-functional teams to provide input throughout the process to iterate on developments and adjust accordingly.
Define key performance indicators (KPIs) to track each integration phase, ensuring measurable security improvements that can be evaluated and examined by both cybersecurity and business executives. Keeping cryptographic advances up to date to enable adaptation strategies for emerging technologies. Ensuring adamant threat intelligence is conducted to examine attack surface, possible threats, and vulnerabilities in systems.

Integration of Crystals-Kyber, Crystals-Dilithium, and AES is a proactive approach to reinforce cyber-security against existing and future quantum attacks. The proper integration and iteration of these will significantly improve an organization's security posture, hardening resilience against evolving vulnerabilities.

8. CONCLUSION

Our white paper concludes the critical challenge that quantum computing poses to current encryption standards and the imperative for Travelers Insurance to adopt post-quantum cryptography (PQC). The central question this research attempted to answer was how Travelers can safeguard sensitive customer and company information against the next generation of threats quantum computers will pose in the coming years. While the potential is large for PQC, the technology is still in development, and the integration process brings with it limitations in terms of cost, training, and potential obsolescence of early selected algorithms as quantum computing technology continues to advance.

The first and most important finding is that quantum-resistant encryption methods, in particular CRYSTALS-Kyber are CRYSTALS-Dilithium, are feasible PQE solutions to alleviate quantum threats, which accomplishes the objective of the research. It is also worthy to note that the current classical computing encryption method AES is also sufficient in certain use cases when meeting a gicen set of criteria. The supplementary findings indicate that these protocols can solidify customer trust through better data security and regulatory compliance and support business continuity by securing critical infrastructures.

By establishing Travelers as an organization that proactively adopts PQC, the project contributes broadly to the area of cybersecurity by offering a model that others involved in insurance products could follow. The societal benefits of this research are to increase consumer confidence and trust in data protection, hence aligning with Travelers' commitment to safeguard customer data in this age of ever-evolving cyber threats. By taking these proactive steps, Travelers not only strengthens its security posture but also sets a precedent for resilience and reliability in the insurance industry.

9. REFERENCES

[1] “What Is Quantum Computing? | IBM,” Sep. 08, 2021. https://www.ibm.com/topics/quantum-computing (accessed Oct. 30, 2024).

[2] “Harvest Now, Decrypt Later (HNDL): A Look at This Current & Future Threat.” https://www.thesslstore.com/blog/harvest-now-decrypt-later-hndl/ (accessed Oct. 30, 2024).

[3] “What is Quantum-Safe Cryptography? | IBM,” Nov. 04, 2022. https://www.ibm.com/topics/quantum-safe-cryptography (accessed Oct. 30, 2024).

[4] T. Starks, “Top insurer CNA disconnects systems after cyberattack,” *CyberScoop*, Mar. 24, 2021. https://cyberscoop.com/cna-cyber-insurance-breach/ (accessed Oct. 30, 2024).

[5] “How Global Insurer AXA Uses Quantum Computing to Prepare for the Future.” https://www.classiq.io/insights/how-global-insurer-axa-uses-quantum-computing-to-prepare-for-the-future (accessed Oct. 30, 2024).

[6] K. Groenland, “The timelines: when can we expect useful quantum computers?,” *Introduction to Quantum Computing for Business*, Oct. 08, 2024. https://koengr.github.io/essentials/timelines/ (accessed Oct. 30, 2024).

[7] “Why the new NIST standards mean quantum cryptography may just have come of age | World Economic Forum.” https://www.weforum.org/agenda/2024/10/quantum-cryptography-nist-standards/ (accessed Oct. 30, 2024).

[8] “Transitioning to a Quantum-Secure Economy,” World Economic Forum. https://www.weforum.org/publications/transitioning-to-a-quantum-secure-economy/ (accessed Oct. 31, 2024).

[9] “NIST POST-QUANTUM CRYPTOGRAPHY UPDATE.” https://csrc.nist.gov/csrc/media/Presentations/2023/nist-post-quantum-cryptography-update/2a-Moody_NIST_PQC_2.pdf (accessed Oct. 31, 2024).

[10] “QUANTUM-READINESS: MIGRATION TO POST-QUANTUM CRYPTOGRAPHY.” https://www.cisa.gov/sites/default/files/2023-08/Quantum%20Readiness_Final_CLEAR_508c%20%283%29.pdf (accessed Oct. 31, 2024).

[11] “Cyber insurance statistics – payouts, claims and facts.” https://thecyphere.com/blog/cyber-insurance-statistics/ (accessed Nov. 01, 2024).

[12] “Data Transparency’s Essential Role in Building Customer Trust CISCO 2022 CONSUMER PRIVACY SURVEY.” https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cisco-consumer-privacy-survey-2022.pdf (accessed Nov. 01, 2024).

[13] “Cybersecurity in 2024,” Cybersecurity and Infrastructure Security Agency (CISA), David Palmbach, Cyber Security Advisor for Connecticut.