The Impact of Quantum Computing on Encryption in Case of J.P. Morgan Chase & Co.

Joel Gilpin

Department of Computer Science

Scholars Thesis

Supervisor: Dr Eric Click

April 21st , 2024

Abstract

The approach of quantum computing presents both unprecedented opportunities and immense challenges, particularly in the realm of encryption technologies. This paper explores the impact of quantum computing on traditional encryption methods, focusing on the vulnerabilities of the Rivest-Shamir-Adleman (RSA) algorithm. As quantum computers draw nearer to achieving practical application, their potential to break current cryptographic systems could drastically undermine data security. The purpose of this study is to evaluate and propose methods to adapt existing encryption frameworks to withstand the computational prowess of quantum technologies. The case study illustrates the proactive measures taken by J.P. Morgan Chase & Co. to preserve confidential financial information. This includes the strategic planning as well as the modification of their security infrastructure to incorporate quantum-resistant solutions. The case study serves as a concrete example of how theoretical risks are being addressed in real-world scenarios, emphasizing the importance of forward-thinking in corporate security strategies. The findings of J.P. Morgan's efforts show how to approach quantum readiness holistically, which could serve as a template for other businesses. The study underscores the need for continuous research, development of robust systems, and collaboration across industries and academia to foster a secure transition to quantum-resistant encryption. The recommendations provided aim to assist organizations in navigating the complexities of this new technological frontier, ensuring that they remain resilient against both current and future cybersecurity challenges.

Table of Contents

Introduction

Numerous benefits, impacts and technological adaptations will arise from quantum computing which will be thoroughly explored in this research paper. Namely, cryptography, software design and computer security. The development of quantum computational technology has been in progress for the past 30 years and it is nearing its full potential (*IBM*, 2023). The advancement of this quantum technology is going to vastly alter the landscape of modern-day computer security and algorithmic design, creating both issues of security and innovative solutions

(Kanamori & Yoo, 2020, p.3-4). Encryption is the basis of computer security, making sure personal data cannot be stolen, such as passwords and bank details. Still, these contemporary algorithms will soon be redundant, and a new era of quantum algorithmic design will emerge (Skinner & Chang, 2007, p.192-193). This quantum technology will render current security systems in use obsolete, but perhaps, in doing so, it may allow for more sophisticated quantum security algorithms to be developed and far more impregnable than their predecessors (Tyson, M. 2022).

Problem Statement

The problem is that modern-day Rivest, Shamir, Adleman Encryption is flawed and still widely in use, it will be rendered redundant as a consequential result of quantum computational technology.

Purpose of the study

The purpose is to identify the optimal ways to improve contemporary computer encryption algorithms to adapt to the encryption cracking capabilities of quantum computing technology.

Significance of the study

This study's significance is to identify how computer systems can be improved to deal with the change in computational power. Firstly, this could highlight various potential vulnerabilities in contemporary encryption systems. Secondly, this new understating of how quantum computers exploit modern encryption methods could impact the fundamental design approaches for encryption algorithms. Thirdly, the potential findings of this research could have significant impacts on educational institutions teaching computer science. Lastly, discovering a superior method of encryption or design approach could yield significant monetary value.

Research Question

This study aims to answer the following question:

How will the increasing availability of Quantum Computing technology impact Rivest, Shamir, Adleman Encryption at J.P. Morgan Chase & Co?

Literature review

Introduction

Technology has advanced to the point that processing power is continuously pushing beyond the limits of what was previously thought to be impossible. The paradigm-shifting technology known as quantum computing has shown promise for unmatched computational power and is set to completely change several industries. The field of quantum computing and its consequences for cryptography are examined in this overview of the literature, with a focus on the creation of quantum-safe algorithms and well-known encryption techniques like Rivest, Shamir, Adleman (RSA).

This literature review has been subdivided into 5 key themes: Quantum computing, Quantum algorithms, Cryptography, RSA Encryption and Quantum safe Algorithms. It delves into the interaction between quantum computing and cryptography, highlighting the urgent need for quantum-resistant cryptographic systems. It investigates the creation and testing of quantum-resistant cryptography algorithms, which are designed to survive the computing power of quantum computers. Investigating post-quantum cryptography entails looking into lattice-based cryptography, code-based cryptography, multivariate polynomials, hash-based signatures, and other novel technologies that provide robust security against quantum adversaries.

Quantum Computing

Quantum computers harness the principles of quantum mechanics to process information. This technology has the potential to solve certain problems far more quickly than classical computers. Quantum computing was first proposed in 1980 by physicist Paul Benioff, although it is currently in the research phase. Despite this, scientists are investigating possible uses that might revolutionize a number of facets of human existence (Kanamori, Y., & Yoo, S.-M. ,2020, p.3-4). Not only may quantum computers solve problems at significantly faster speeds, but they can also solve problems that even the most potent supercomputers are unable to solve (Alshi et al., 2023, p.1-2).

Quantum computing represents a paradigm shift from classical computing by utilizing quantum bits, or qubits, instead of classical bits that can only be 0 or 1. Qubits are unique in that they can conduct calculations more efficiently due to properties like entanglement and superposition (Kanamori, Y., & Yoo, S.-M. ,2020, p.5-6). A register of n qubits expressing 2n distinct values concurrently can result from superposition, which enables a qubit to store values of 1 and 0. In contrast, n bits can only successively represent 2n unique values in traditional computers (Alshi et al., 2023, p.1-2).

Entanglement, another quantum phenomenon, allows the values of correlated qubits to change simultaneously. This feature is especially helpful for computing activities where quantum computers can perform better than classical counterparts, such as factorization and database searches. Many methods are being investigated for building quantum computers, including topological qubits, trapped ions, and superconducting circuits (Alshi et al., 2023, p.2).

To take full advantage of quantum computing, specific software and algorithms are needed. Achieving usable quantum computation requires overcoming obstacles such as error correction, scaling up qubit numbers, and combining quantum and classical computing. Notwithstanding these

challenges, governments, universities, and businesses across the world are actively working to build quantum computers and have made significant strides (Alshi et al., 2023, p.4).

Quantum decoherence is a major obstacle for quantum computers; it can cause computational errors and disturb qubit states as a result of interactions with the environment. This is especially problematic for algorithms such as Shor's algorithm. This is addressed by quantum error correction, which uses quantum information encoding to identify and correct errors resulting from these disruptions. The goal of this procedure is to recover the initial quantum state in spite of errors caused by the environment. It uses syndrome extraction operators and error correcting codes. These methods efficiently detect and rectify errors in quantum systems by utilising particular error correction techniques—like state mapping and inverse error transformations—and show how quantum error correction can restore encoded quantum states when decoherence is present (Rieffel & Polak, 1998, p.302-303,328-329).

IBM unveiled Quantum Safe technology, an end-to-end solution that assists organizations including governmental agencies—in getting ready for the post-quantum era. The advancement of quantum technology presents security risks due to its potential to breach commonly used security protocols. With the help of its knowledge in cryptography, quantum computing, and critical infrastructure, IBM has developed Quantum Safe technology, which includes tools like Quantum Safe Explorer, Quantum Safe Advisor, and Quantum Safe Remediator (IBM, 2023). These tools help organizations with quantum-safe remediation patterns, cryptographic inventory creation, and code scanning. To assist clients with the security transition, IBM also presents the Quantum-Safe Roadmap, which emphasizes observation, transformation, and discovery. The roadmap aligns with the National Institute of Standards and Technology's quantum-resistant algorithms and addresses U.S. government requirements for quantum-safe transitions (IBM , 2023).

Quantum Algorithms

Quantum algorithms that have been developed since the 1980s illustrate the growing influence of quantum computing on businesses. Glover's database search and Shor's integer factoring are two notable algorithms that outperform their classical counterparts and put commonly used encryption systems at risk. Businesses such as Daimler Mercedes-Benz, Volkswagen, ExxonMobil, JPMorgan Chase, Goldman Sachs, and ExxonMobil are investigating the use of quantum computing in tasks like material discovery, energy optimization, option pricing, and data protection (Kanamori, Y., & Yoo, S.-M , 2020, p.11-15).

Grover's algorithm works by adjusting the amplitudes of superposed states to raise the probability of seeing the intended result. Grovers algorithm is designed for searching an unsorted database or solving an unstructured search problem faster than classical algorithms. An oracle function, a quantum black box that identifies the solution states, is used by Grover's algorithm. The oracle function would, in the database search example, flip the sign of the amplitude of the state corresponding to the right solution, thereby marking it (Butler & Hartel, 1999, p.422-427). Although it is theoretically faster for unstructured search problems, decoherence and quantum error correction pose practical implementation challenges (Bernhardt, 2019, p.176-181).

Similarly, Shor's algorithm computes discrete logarithms and factors large composite numbers efficiently (Shor, 1997, p.15,19). It poses a direct risk to the safety of popular public-key encryption schemes like RSA. Additionally, by effectively resolving the discrete logarithm problem, Shor's algorithm undermines other public-key cryptosystems, like elliptic curve cryptography (ECC). This puts in danger the security of cryptographic methods that depend on these. Shor's algorithm affects digital signatures as well because it can breach the cryptographic mechanisms that underpin systems that use algorithms like RSA or ECC. Digital signatures are essential to secure communication. With the introduction of Shor's algorithm, post-quantum

cryptography becomes even more important, accelerating the creation of algorithms that withstand quantum attacks and guarantee security in the event that large-scale quantum computers become a reality. Organizations may need to think about temporarily increasing the length of the keys in their current cryptographic systems until stronger post-quantum cryptographic algorithms are developed (Bernhardt, 2019, p.174-176).

Another couple of algorithms that illustrate the capabilities of quantum are Deutsch's algorithm and Simon's algorithm. Although these algorithms don’t impact cryptography to the same extent as the algorithms mentioned prior, they effectively demonstrate the computational prowess of quantum computing. Deutsch's algorithm is a key tool in proving the superiority of quantum computing over classical computing in certain problem-solving situations. This quantum algorithm tackles a black-box function that takes a single bit as input and outputs a single bit, elegantly demonstrating quantum parallelism and interference. Deutsch's algorithm uses quantum properties to speed up the solution process by determining whether the function is constant or balanced with only one query, in contrast to classical methods that require two function evaluations. Deutsch's algorithm highlights the special benefit of quantum computing by utilising quantum concepts like superposition and entanglement to show how quantum computers can solve problems more quickly than their classical counterparts in specific situations (Bernhardt, 2019, p.145-157).

Lastly, Simon's algorithm highlights how, for certain problem sets, quantum computation can compute exponentially faster than classical methods. This algorithm tackles the problem of finding a hidden bit string with certain properties, which would require an exponential amount of function queries in classical computing. But Simon's algorithm uses quantum features like entanglement and superposition to identify the hidden bit string much faster than any known classical algorithm, with an exponential time complexity. Simon's algorithm, which effectively takes advantage of quantum phenomena, exemplifies the potential of quantum computing in

solving problems tenfold faster and reveals a significant difference in computational power between quantum and classical systems for some problem-solving scenarios (Bernhardt, 2019, p.157-165).

Though these algorithms are theoretically feasible and capable of cracking encryption, they are not yet implemented in practice. This is a result of error correction's implementation being difficult. When interactions with the environment cause a quantum system to lose coherence, it enters a state known as decoherence. Error correction is the set of methods used to fix mistakes that occur during quantum computations. The reliable functioning of quantum computers depends on the management and mitigation of the effects of decoherence, which is made possible by error correction (Rieffel & Polak, 1998, p.302-303,328-329).

Cryptography

Encryption models and decryption models are the two primary categories of cryptographic models. According to the encryption model, symmetric (private) or public keys are used to convert plaintext into ciphertext. With symmetric encryption, plaintext is encrypted using particular techniques and a single key for transmission. The Decryption model rewrites ciphertext into plaintext using symmetric and asymmetric decryption. Asymmetric decryption uses two separate keys for communication, whereas symmetric decryption uses just one key (Chandran, 2022, p7-8).

Quantum Key Distribution (QKD) is a secure communication method using quantum principles. It involves sending particles (photons) with quantum properties between two parties (Alice and Bob). If Bob's measurements match Alice's plans and if there isn't an eavesdropper, they can generate a shared secret key. With QKD's ability to identify eavesdropping attempts, it's a secure communication technique that's especially important in the age of potential threats to classical cryptography from quantum computing (Rieffel & Polak, 1998, p. 307-308).

RSA Encryption

Rivest, Shamir, Adleman (RSA) encryption is a widely used public-key cryptosystem. Every user in RSA creates a set of keys, a private key for decryption and a public key for encryption. User A encrypts a message using User B's public key in order to send it to User B securely. Only B can decrypt and read the message with the matching private key (Skinner, G., & Chang, E. 2007, p.190-191). The difficulty of factoring the product of two large prime numbers forms the foundation of RSA's security. Moreover, RSA is used to create digital signatures, in which data integrity and authenticity are guaranteed by the sender signing a message with their private key and the recipient verifying the signature with the sender's public key. Despite RSA seeming like a secure method of encryption. Its security depends on how hard it is to factor big prime numbers. RSA could be threatened by developments in factorization algorithms or the emergence of potent quantum computers. Longer key lengths are eventually required for security because shorter key lengths are more vulnerable to brute-force attacks. The random number generators used to create keys must be of a high quality; predictable or faulty generation reduces security. Vulnerabilities may be introduced by timing attacks, taking advantage of differences in the times at which cryptography operates, and implementation errors such as insecure protocols (Kritsanapong Somsuk, 2020, p. 3843-3845). Although it isn’t a threat right now, the development of strong quantum computers in the future could make RSA vulnerable to effective factorization, which would affect the security of encrypted data. This is just one of several commonly used encryption techniques that appear safe but have vulnerabilities that can be exploited. When quantum computing becomes more widespread, this will only get worse (Kritsanapong Somsuk, 2020, p. 3843-3845).

Quantum safe Encryption

In order to counteract attacks utilising Quantum Computing (QC), Post-Quantum Cryptography (PQC) aims to supersede current cryptographic techniques while maintaining compatibility with pre-existing systems. Shor's algorithm, which solves the prime factorization problem quickly using the Quantum Fourier Transform, threatens RSA encryption on conventional computers. Although the speedup of the algorithm does not make classical cryptographic techniques obsolete, it does require larger key sizes, which has an impact on symmetric-key methods. The expanding global community emphasises the necessity of quantum-resistant primitives to preserve information security against possible quantum risks (Golchha et al., 2023, p. 266-268).

Cryptography has been evolving for centuries from the ancient Ceaser Cipher to contemporary computer systems. This evolution only needs to continue with the approach of quantum computers, Lattice-based cryptography (LBC) is a low-latency solution that shows promise against QC (Golchha et al., 2023, p. 269). The idea that a lattice, represented by the letter L, is a geometric structure made up of a group of n independent vectors arranged in a periodic grid with n dimensions. The lattice is mathematically expressed as a linear combination of these vectors, which are represented as [b1, b2,..., bn]. The lattice's geometrical parameters can be affected by the presence of various bases, some of which are regarded as good and others as bad. Lattices are used in conjunction with cryptography because of their robust primitives, easy-to-understand structure, and capacity for both linear and parallel operations (Golchha et al., 2023, p. 270).

The lattice presents several advantages in the field of cryptography, such as its ease of use, effectiveness, resilience against quantum and sub-exponential attacks, and potential for faster decryption and encryption methods. The idea of Learning with Errors (LWE) proposed by O. Regev is discussed as a means to introduce random errors into lattice problems and improve their

security. LWE entails generating a public key, adding random errors, and generating a secret key value. Because of the variable and distributed nature of the error perturbation in LWE, recovering the solution through Gaussian elimination is challenging. Because polynomial Quantum Computing (QC) algorithms have not yet been discovered and LWE is thought to be difficult for current algorithms, it is deemed appropriate for use in Public Key Cryptography (PKC) applications (Golchha et al., 2023, p. 271).

Conclusion

The convergence of quantum computing and cryptography heralds a pivotal juncture in the realm of information security and computational capabilities. This literature review highlights the fundamental implications of quantum computing on existing cryptography systems, notably the vulnerabilities of widely used encryption algorithms like RSA to quantum attacks. As quantum computers offer exponential computational speed via methods such as Shor's algorithm, the vulnerability of present encryption systems becomes clear.

Despite the potential threat posed by quantum computing, this review highlights the collaborative efforts and progress made in the development of quantum-resistant or post-quantum cryptography algorithms. These unique cryptographic approaches, which are based on different mathematical structures such as lattice-based cryptography, code-based cryptography, multivariate polynomials, and hash-based signatures, have the potential to strengthen digital security against quantum adversaries. While great work has been made in conceptualizing and testing quantum-resistant cryptographic algorithms, the road to standardized, widely recognized post-quantum cryptographic standards remains unfinished. To enable a smooth transition to quantum-safe encryption, further research, rigorous testing, and consensus-building across the cryptographic community and industry stakeholders are required.

Finally, the advent of quantum computing presents the area of cryptography with both a disruptive problem and an opportunity. The symbiotic relationship between quantum computing and encryption emphasises the importance of ongoing innovation and proactive steps to protect sensitive information in an increasingly quantum-enabled environment. This literature review exemplifies the ever-changing technological landscape, emphasising the importance of establishing robust, quantum-resistant cryptographic frameworks to protect the integrity and confidentiality of our digital communications.

Methods

Research design

This paper uses the mixed methods approach described by Creswell, J. W., & Creswell, J. D. (2023, p.227-255). In an effort to gain a comprehensive understanding of the complex relationship between quantum computing and cryptography. This methodological framework combines quantitative and qualitative approaches, taking advantage of each one's advantages to provide a comprehensive grasp of the topic. Additionally, this paper follows the outline of a research proposal as stated by Pajares, F. (2007).

Methodology

This research will utilise the case study methodology. A case study is a research methodology that involves an in-depth investigation of a specific individual, group, event, or phenomenon within its real-life context (Yin, 2018). It's a detailed examination aimed at understanding the complexities, dynamics, and nuances surrounding the chosen subject. In this case between quantum computing and cryptography in the scenario of J.P. Morgan.

Data collection

The data collection process for the literature review consisted of gathering reputable and reliable, peer reviewed sources from the Webster library databases: CiteSeerX, Computer Science (Gale OneFile), CoRR - Computing Research Repository, and Science of Security Search Page. The majority of papers utilized in this research have been mixed-method papers and several explanatory qualitative papers.

The case study of this research will utilize sources from the official website of J.P. Morgan, respectable Business publications and reports from the National Institute of Standards and Technology (NIST). J.P. Morgan's understanding of the financial applications of quantum computing will offer important industry-specific information for a thorough examination of the interplay between quantum computing and encryption in the financial sector.

Data analysis

This paper's literature was split into various key themes to adequately encapsulate the complexities of quantum technology on modern encryption. The analysis of this information will involve identifying patterns, themes, and insights that contribute to a deeper understanding of the case's unique characteristics, and any recurrent themes found from this case study can be related back to the literature to identify the impact of quantum computing on cryptography. The data analysis process for this research will be purely qualitative. Quantitatively this paper is limited, despite the topic being heavily mathematically based for the specific research being done it would yield little benefit. The Qualitative analysis will include a narrative analysis and identifying recurring themes.

Limitations and delimitations

The limitations of this research are numerous, a lack of funds, time, or access to specialized technology. Additionally, as Quantum computing is yet to be fully functional it is difficult to accurately identify ways to secure systems or develop encryption methods without being able to practically test them.

The delimitations of this research are related to the scope of the research, as the impacts of quantum computing will affect numerous areas it would take extreme amounts of time to cover everything, so this research will focus on the impacts within the financial sector. Lastly, as both cryptography and quantum computing are very mathematically complex this research will be limited to the extent of math covered in these fields.

Case Study

Context of J.P. Morgan Chase & Co.

J.P. Morgan Chase & Co is a global financial services firm with a broad range of expertise. Operating in over 100 countries with a significant global presence. J.P. Morgan is a leader in various financial sectors, including investment banking, commercial banking, financial transaction processing, and asset management. They aim to support economic growth and stability by investing in communities, promoting environmental sustainability, and leveraging technology (*J.P. Morgan France | About Us*, n.d.-b).

Quantum computing's impending arrival will cause a significant transformation in the financial industry. It is anticipated that this technology will transform several industry processes, most notably risk and portfolio management. But it also presents a lot of difficulties, particularly in terms of cybersecurity. The majority of current encryption techniques may become outdated due to quantum computing, jeopardising consumer protection as well as the integrity of digital economies and infrastructures (*Quantum Security for the Financial Sector: Informing Global Regulatory Approaches*, 2024). The complexity of addressing quantum-enabled cybersecurity risks in the financial sector stems from the interconnectedness of the industry, legacy infrastructure, and the nature of quantum technology. These risks are significant, and the timeline for switching to new security models is uncertain (*Quantum Security for the Financial Sector: Informing Global Regulatory Approaches*, 2024).

Embracing Future Technology for Secure Financial Infrastructure

Despite J.P. Morgan being an investment firm they are heavily focused on improving and developing their technological infrastructure. The organisation needs to be built upon a secure

infrastructure to adequately manage the millions of transactions that occur each second. As part of their forward-thinking approach, J.P. Morgan is also actively involved in adapting to emerging technologies like quantum computing, with a focus on developing quantum-safe encryption methods to enhance security and protect against future technological advancements (Potter, 2023). The company is driven by the goal of achieving quantum advantage - outperforming classical computers in processing real-world problems. To this end, the Global Technology Applied Research group within J.P. Morgan is evaluating potential quantum computing applications such as portfolio optimization, risk analysis, option pricing, and fraud detection (Potter, 2023). Despite the current impracticality of quantum computing in these areas, J.P. Morgan is strategically preparing for future readiness. The head of the research group within J.P. Morgan, Marco Pistoia, acknowledges the distance to achieving quantum advantage or supremacy but emphasizes the tangible progress in hardware and the shift from theory to practical experimentation. This approach will ensure J.P. Morgan is quantum-ready when the time comes. Furthermore, in a proactive measure against quantum-supremacy threats, J.P. Morgan recently appointed a quantum computing expert to lead a new department, reflecting Pistoia's view on the urgency of preparation against potential future decryption by malicious entities using more advanced quantum computers (Potter, 2023).

Security Frameworks

J.P. Morgan successfully implemented the Workforce Framework for Cybersecurity (NICE Framework) (NICE Framework Success Story: JPMorgan Chase & Co. | NIST, 2022). This framework was designed by the National Institute of Standards and Technology. This framework facilitates continuous learning and workforce development within the Cybersecurity & Technology divisions of J.P. Morgan. The company aimed to improve employee development, mobility, and retention while nurturing a culture of continuous learning. The process involved

evaluating the NICE Framework's components, collaborating with experts to create role profiles, and integrating these with their learning ecosystem. This initiative led to more targeted training suggestions and improved strategic decision-making within the organization. The project, spearheaded by Leo Van Duyn in the Cybersecurity & Technology Controls Workforce Development Strategy, showcases JPMorgan's dedication to evolving its workforce in line with contemporary cybersecurity challenges such as that of Qunutm computing and the broader technological landscape (NICE Framework Success Story: JPMorgan Chase & Co. | NIST, 2022).

To prepare for emerging post-quantum threats, data owners need to assess, classify, and prioritize their critical assets. Recent actions by the US government highlight the urgency of this task. The Cybersecurity and Infrastructure Security Agency (CISA), the National Security Agency (NSA), and the National Institute of Standards and Technology (NIST) issued guidelines for managing critical infrastructure security (*Migration to Post-Quantum Cryptography | NCCOE*, n.d.). These agencies recommend that organizations initiate this process now by developing quantum-readiness roadmaps, performing comprehensive inventories, conducting risk assessments, and liaising with vendors. This proactive approach is necessary as future quantum computing advancements could enable decryption of currently secure data (*Migration to Post-Quantum Cryptography | NCCOE*, n.d.). Key steps include forming a project management team to oversee the migration to Quantum-safe Encryption and identifying dependencies on quantum-vulnerable cryptographic systems, which are often found in digital signature mechanisms and in software and firmware updating processes. Creating an inventory of these quantum-vulnerable systems will help in prioritizing migration efforts and risk assessment strategies (*Migration to Post-Quantum Cryptography | NCCOE*, n.d.). President Biden signed the Quantum Computing Cybersecurity Preparedness Act (Sanzeri, 2023), emphasizing the need for proactive measures. Fortunately, progress is underway in developing post-quantum cryptography (PQC) technologies,

with the NIST leading efforts to standardize PQC algorithms (*NIST to Standardize Encryption Algorithms That Can Resist Attack by Quantum Computers | NIST*, 2023). Financial services organizations must be prepared to update their encryption systems accordingly once new standards are released. The repercussions of cyber breaches in the financial sector are severe, as evidenced by past incidents costing millions of dollars and damaging reputations. Regulatory oversight has increased in response, emphasizing the importance of robust cybersecurity programs. (Guarrera & Khan, 2023).

Data Analysis & Findings

As quantum computing evolves, it's becoming increasingly crucial for financial institutions, offering the ability to solve complex issues at an unprecedented pace (Devadiga, 2024). It's imperative for these organizations, particularly in finance where security is paramount, to proactively implement quantum-resistant security measures (Guarrera & Khan, 2023b). By staying current with quantum computing advancements and adopting quantum-secure protocols, financial firms can ensure the protection of their critical and sensitive data (Guarrera & Khan, 2023).

The finance industry is thought to be the first industry sector to benefit from quantum computing in the long, medium, and short term. This is because there are a lot of use cases in finance that can benefit from quantum computing. Additionally, because time is of the essence in the finance industry, accurate results are needed quickly. (jpmorgan, 2022). However, this progress in quantum computing poses a 2 substantial challenges. The first being a lack of preparedness to this new emerging technology and the second being, that as quantum computing will be able to break public key encryption (jpmorgan, 2022). Companies / industries may have the approach to wait for the Quantum threat to materialize, this would be far from the right choice as it would take too long to adapt once the technology is available (jpmorgan, 2022). At J.P. Morgan they have the diametrically opposite approach. They have employed various Quantum computing experts and

follow closely the NIST security framework which outlines the best practices to employ for the coming Quantum revolution.

Using Quantum Safe Encryption is one issue but converting legacy code and systems to a quantum safe environment is an immense task to carry out, fortunately the Global Technology Applied Research group with J.P. Morgan have incorporated a compiler into their software stack for quantum computing, enabling them to recompile algorithms and code for possibly every quantum computer out there, this will eliminate the need to rewrite or completely redesign the current systems in place (jpmorgan, 2022). Despite estimates suggesting it will take five to ten years for quantum computers to break RSA encryption, the potential for large state actors to achieve quantum capabilities first, followed by rapid democratization of the technology by rogue actors, underscores the need for action now (Guarrera & Khan, 2023). Of particular concern are "harvest now, decrypt later" attacks, where encrypted data is intercepted and stored for decryption once quantum computers become available. Deploying post-quantum cryptographic systems that can resist both classical and quantum attacks, are necessary to mitigate these risks (Guarrera & Khan, 2023).

The first quantum-safe cryptography protocol standards were announced by the National Institute of Standards and Technology (NIST) in the United States. In 2022, NIST selected four algorithms aimed to be resilient against quantum computer attacks (*NIST to Standardize Encryption Algorithms That Can Resist Attack by Quantum Computers | NIST*, 2023). Three of these algorithms now have draft standards released, with the fourth, FALCON, expected to have its draft standard published in 2024. This development was made possible by the significant contributions of IBM scientists working with a variety of partners. CRYSTALS-Dilithium and Falcon for digital signatures and CRYSTALS-Kyber for public-key encryption are the selected standards (Osborne & Lyubashevsky, 2023). These algorithms are made to withstand potential

attacks by quantum computing on existing encryption techniques like RSA and elliptic curve cryptography. In order to create a new set of encryption standards that are both compatible with current classical computers and safe from potential threats posed by quantum computing, NIST is collaborating with experts from all over the world (*NIST to Standardize Encryption Algorithms That Can Resist Attack by Quantum Computers | NIST*, 2023). The emphasis is also on investigating novel concepts in post-quantum cryptography, particularly for digital signatures, in order to guarantee strong and varied cryptographic techniques.

While quantum-resistant algorithms are one approach to secure data, Quantum Key Distribution presents another layer of security, A thorough understanding of QKD, its useful applications, implementation challenges, and integration potential with current infrastructure could yield important insights for a comprehensive security plan. JPMorgan, in collaboration with Toshiba and Ciena, has developed a pioneering Quantum Key Distribution (QKD) network designed to secure mission-critical blockchain applications (*JPMorgan Chase, Toshiba and Ciena Build the First Quantum Key Distribution Network Used to Secure Mission-Critical Blockchain Application*, n.d.). This high-speed network is resistant to attacks by quantum computing and has been shown to work well in real life settings. Data security over distances of up to 100 kilometres is guaranteed by the QKD network's ability to identify and inhibit eavesdropping attempts (*JPMorgan Chase, Toshiba and Ciena Build the First Quantum Key Distribution Network Used to Secure Mission-Critical Blockchain Application*, n.d.). With this accomplishment, the use of QKD technology for useful, high-security applications in finance has advanced significantly and becoming feasible for large scale applications.

JPMorgan’s strategy of employing diverse data security measures is a prudent decision.

By employing and investigating a range of security protocols, JPMorgan Chase is being proactive in safeguarding its systems from potential cyber threats. Developing strong quantum algorithms,

providing comprehensive staff training to increase awareness of the risks posed by quantum computing, and utilising Quantum Key Distribution (QKD) to secure data are some of their tactics. With this approach JPMorgan guarantees complete protection by implementing several lines of defence, increasing their resilience against cyber threats and protecting against the failure of any one system.

Quantum Computing: Theoretical Foundations vs. Practical Applications

The concepts of quantum computing, including entanglement, superposition, and qubits, are covered in detail. It highlights the threat that quantum computing poses to established encryption techniques, particularly RSA encryption, by theorising that it could solve problems exponentially faster than classical computers.

J.P. Morgan's proactive actions demonstrate how these quantum computing principles are put into practice. They are actively investing in quantum-safe encryption and investigating applications such as risk analysis and fraud detection in order to get ready for the quantum era, in addition to being aware of the potential threats. This illustrates how business strategy and action are influenced by theoretical risks.

Cryptographic Vulnerability and Evolution

The literature discusses how quantum computing can potentially break widely used cryptographic protocols. It explores the development of quantum-resistant cryptography, including various algorithms designed to withstand quantum attacks.

J.P. Morgan’s implementation of quantum-safe algorithms is a direct response to these identified vulnerabilities. Their strategy serves as an example of how businesses can put the theoretical understanding of quantum-resistant cryptography systems into practice to safeguard confidential information from threats posed by quantum computing.

Industry's Role in Advancing Quantum Technology

The literature discusses how various industries—including the financial sector—may be impacted by and have opportunities to advance quantum computing.

J.P. Morgan's case shows the finance sector's tangible contributions to quantum computing advancements. By experimenting with quantum computing for various financial applications, J.P. Morgan is at the forefront of adopting this technology, reflecting the industry's role as both a benefactor and contributor to quantum computing development.

Challenges in Transitioning to Quantum-Resistant Cryptography

The literature discusses the conceptual challenges in developing and implementing quantum-resistant cryptography, and the need for new algorithms and standards.

In J.P. Morgan's scenario, the difficulties take on a tangible form as the theoretical dangers are recognised and efforts are made to switch to quantum-resistant and adaptable systems. Shown by them updating their workforce training programme and following closely the NIST cybersecurity frameworks for migrating to quantum-safe encryption, highlighting the real-world challenges and solutions in adjusting to quantum advancements.

Quantum Computing's Implications for Data Security and Privacy

The literature emphasizes how quantum computing could potentially decrypt current secure data, posing a significant threat to data security and privacy.

J.P. Morgan demonstrates awareness of these ramifications by concentrating on creating and employing quantum-safe encryption techniques. Their deeds demonstrate how businesses can effectively manage these risks to protect customer information and uphold confidence.

Conclusion

In conclusion, the case study of J.P. Morgan Chase & Co, this research paper provides a compelling and instructive example of how a major financial institution is proactively addressing

the challenges posed by the arrival of quantum computing. J.P. Morgan's initiatives demonstrate a keen awareness of the potential risks quantum computing poses to traditional cryptographic methods and an admirable commitment to safeguarding their data and systems against future threats. This case study illustrates several key takeaways, they have demonstrated a deep awareness of the future quantum threat and the need for developing cybersecurity techniques by taking a proactive stance and investing in the development and implementation of quantum-safe encryption solutions. To be at the forefront of the quantum computing revolution, it is imperative to combine knowledge and resources, as demonstrated by the partnership with industry leaders, academic institutions, and specialists.

Additionally, a comprehensive approach to cybersecurity is demonstrated by J.P. Morgan's implementation of extensive security standards, such as the National Institute of Standards and Technology's Workforce Framework for Cybersecurity. This strategy ensures resilience in the face of changing problems since it is strong against potential dangers as well as flexible to deal with present ones. Additionally, their industry leadership in establishing standards for other businesses emphasizes the significance of pre-emptive planning and their role to influencing the direction of cryptography and quantum computing in the future.

In essence, the case of J.P. Morgan Chase & Co. serves as a valuable model for other organizations grappling with the complexities of quantum computing and its implications for encryption. It emphasizes the need for strategic planning, investment in new technologies, and collaboration to navigate the quantum era successfully. As the quantum landscape continues to evolve, the insights gleaned from this case study will undoubtedly inform and guide organizations in their journey towards quantum resilience.

Recommendations

Based on analysis of this Case of J.P. Morgan Chase & Co., here are some recommendations for safely migrating to and adapting to the immerging quantum technology:

1. Develop Quantum-Resistant Cryptography: Invest in research and development of quantum-safe algorithms, such as lattice-based cryptography, code-based cryptography, and multivariate polynomial algorithms, to ensure future cryptographic systems are resistant to quantum attacks.

2. Continuous Risk Assessment and Monitoring: Regularly assess the security of current cryptographic systems against potential quantum computing threats. Stay informed about advancements in quantum technology to understand when existing systems might become vulnerable.

3. Invest in Quantum Computing Expertise: Build or expand a team of experts in quantum computing and quantum cryptography. This expertise is crucial for developing new cryptographic strategies and understanding the potential impact of quantum technology on current systems.

4. Quantum-Safe Transition Planning: Develop a comprehensive roadmap for transitioning to quantum-safe technologies. This plan should include timelines, resource allocation, technical strategies, and contingency plans.

5. Collaboration with Academia and Industry: Collaborate with academic institutions, industry peers, and cryptographic experts to stay at the forefront of quantum-safe cryptographic methods and share best practices.

6. Educate and Train Workforce: Educate your workforce, especially IT and cybersecurity teams, about the implications of quantum computing. Provide training on new quantum-safe practices and protocols.

7. Revise Existing Security Protocols: Reevaluate and update current encryption protocols and standards to include quantum-resistant features. This includes updating digital signature mechanisms and secure communication protocols.

8. Engage with Government and Standards Bodies: Engage with government agencies and standards bodies (like NIST) that are working on quantum-safe cryptography standards. Compliance with these standards will be crucial as they evolve.

9. Quantum Key Distribution (QKD) Implementation: Explore the use of Quantum Key Distribution for secure communications, especially for highly sensitive data transfers, to ensure security against quantum decryption techniques.

10. Data Sensitivity Classification and Prioritization: Assess and classify the sensitivity of data to prioritize encryption efforts. High-value data may require more immediate and robust quantum-safe encryption methods.

11. Regularly Update and Test Security Systems: Implement a regime of regular updates and rigorous testing of security systems to adapt to the evolving quantum computing landscape and ensure robust defence against potential threats.

12. Invest in Hybrid Cryptographic Systems: Develop and utilize hybrid systems that combine classical and quantum-resistant algorithms to ensure both current and future security.

13. Strategic Partnerships and Information Sharing: Form strategic partnerships with other organizations, research entities, and quantum technology providers for information sharing, joint research initiatives, and collaborative problem-solving.

14. Adopt a Proactive Approach to Quantum Readiness: Instead of a reactive stance, adopt a forward-looking approach to quantum readiness, focusing on the early adoption of quantum-safe practices and technologies.

Implementing these recommendations will help organizations prepare for the inevitable impact of quantum computing on cryptography and ensure a secure transition to quantum-safe technologies.

References

Alshi, M. (2023, March 31). *Taking a Quantum Leap in the future of computing*. CXOToday.com. https://www.cxotoday.com/cxo-bytes/taking-a-quantum-leap-in-the-future-of-computing

Bernhardt, C. R. (2019). Quantum computing for everyone. In *The MIT Press eBooks*. https://doi.org/10.7551/mitpress/11860.001.0001

Butler, M., & Hartel, P. H. (1999). Reasoning about Grover's quantum search algorithm using probabilistic wp. *ACM Transactions on Programming Languages and Systems*, *21*(3), 417–429. https://doi.org/10.1145/319301.319303

Chandran, A. S. (2022). Review on Cryptography and Network Security Zero Knowledge Technique in Blockchain Technology. *International Journal of Information Security and Privacy*, *16*(2), 1–18. https://doi.org/10.4018/ijisp.308306

Devadiga, K. (2024, January 29). Quantum security: Redefining financial protection in the digital era - ET Edge Insights. *ET Edge Insights*. https://etinsights.et-edge.com/quantum-security-redefining-financial-protection-in-the-digital-era/

Creswell, J. W., & Creswell, J. D. (2023). *Research design: Qualitative, Quantitative, and Mixed Methods Approaches*. SAGE Publications.

Golchha, R., Lachure, J., & Doriya, R. (2023). Fog Enabled Cyber Physical System Authentication and Data Security using Lattice and Quantum AES Cryptography. *International Journal of Computing and Digital Systems*, *13*(1), 267–275. https://doi.org/10.12785/ijcds/130122

Gilliam, A., Venci, C., Muralidharan, S., Dorum, V., May, E. F., Narasimhan, R., & Gonciulea, C. (2019). Foundational patterns for efficient Quantum Computing. *arXiv (Cornell University)*. https://doi.org/10.48550/arxiv.1907.11513

Grover, L. K. (1996, May 29). *A fast quantum mechanical algorithm for database search*. arXiv.org. https://arxiv.org/abs/quant-ph/9605043

Guarrera, D., & Khan, K. A. (2023, April 12). *Preparing financial services cybersecurity for quantum computing*. https://www.ey.com/en_us/strategy/financial-services-cybersecurity-for-quantum-computing

IBM unveils End-to-End Quantum-Safe Technology to Safeguard Governments' and Businesses' Most-Valuable Data. (2023, May 10). IBM Newsroom. https://newsroom.ibm.com/2023-05-10-IBM-Unveils-End-to-End-Quantum-Safe-Technology-to-Safeguard-Governments-and-Businesses-Most-Valuable-Data

J.P. Morgan France | About us. (n.d.). https://www.jpmorgan.com/FR/en/about-us

jpmorgan. (2022, November 21). *The key to Quantum Security | J.P. Morgan* [Video]. YouTube. https://www.youtube.com/watch?v=gWpnIfUb4_o

JPMorgan Chase, Toshiba and Ciena build the first quantum key distribution network used to secure Mission-Critical blockchain application. (n.d.). https://www.jpmorgan.com/technology/technology-blog/jpmc-toshiba-ciena-build-first-quantum-key-distribution-network-critical-blockchain-application

Kanamori, Y., & Yoo, S. (2020). Quantum Computing: principles and applications. *Journal of International Technology and Information Management*, *29*(2), 43–71. https://doi.org/10.58729/1941-6679.1410

Lindsay, J. R. (2020). Demystifying the quantum threat: infrastructure, institutions, and intelligence advantage. *Security Studies*, *29*(2), 335–361. https://doi.org/10.1080/09636412.2020.1722853

Migration to Post-Quantum Cryptography | NCCOE. (n.d.). NCCoE. https://www.nccoe.nist.gov/crypto-agility-considerations-migrating-post-quantum-cryptographic-algorithms

Pajares, F. (2007). THE ELEMENTS OF A PROPOSAL. *THE ELEMENTS OF a PROPOSAL*. http://www.egyptarch.net/hishamgabr/lectures/Proposal%20Elements%20english.pdf

NICE Framework Success Story: JPMorgan Chase & Co. | NIST. (2022, December 22). NIST. https://www.nist.gov/itl/applied-cybersecurity/nice/nice-framework-resource-center/nice-framework-success-story-jpmorgan

NIST to standardize encryption algorithms that can resist attack by quantum computers | NIST. (2023, August 24). NIST. https://www.nist.gov/news-events/news/2023/08/nist-standardize-encryption-algorithms-can-resist-attack-quantum-computers

Osborne, M., & Lyubashevsky, V. (2023, January 4). *IBM scientists help develop NIST's quantum-safe standards*. IBM Research Blog. https://research.ibm.com/blog/nist-quantum-safe-protocols

Potter, J. (2023, December 7). *JP Morgan Trials Quantum for Trading, Risk Management*. https://www.iotworldtoday.com/industry/jp-morgan-trials-quantum-for-trading-risk-management

Quantum computing will redefine encryption | J.P. Morgan. (n.d.). https://www.jpmorgan.com/payments/payments-unbound/volume-2/quantum-computers-will-redefine-encryption

Quantum Security for the Financial sector: Informing global regulatory approaches. (2024, January 12). World Economic Forum. https://www.weforum.org/publications/quantum-security-for-the-financial-sector-informing-global-regulatory-approaches/

Rashid, F. Y. (2016, July 8). *Google Chrome tests future of encryption with post-quantum crypto*. InfoWorld. https://www.infoworld.com/article/3093245/google-chrome-tests-future-of-encryption-with-post-quantum-crypto.html

Rieffel, E., & Polak, W. (2000). An introduction to quantum computing for non-physicists. *ACM Computing Surveys*, *32*(3), 300–335. https://doi.org/10.1145/367701.367709

Sanzeri, S. (2023, January 25). What the Quantum Computing Cybersecurity Preparedness Act means for national security. *Forbes*. https://www.forbes.com/sites/forbestechcouncil/2023/01/25/what-the-quantum-computing-cybersecurity-preparedness-act-means-for-national-security/#:~:text=On%20December%2021%2C%202022%2C%20President,protect%20against%20quantum%20computing%20attacks.%E2%80%9D

Shor, P. W. (1997). Polynomial-Time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Journal on Computing*, *26*(5), 1484–1509. https://doi.org/10.1137/s0097539795293172

Skinner, G., & Chang, E. (2011). A projection of the future effects of quantum computation on information privacy. In *IGI Global eBooks* (pp. 138–147). https://doi.org/10.4018/978-1-60566-210-7.ch009

The new Weakness of RSA and The Algorithm to Solve this Problem. (2020). *Ksii Transactions on Internet and Information Systems*, *14*(9). https://doi.org/10.3837/tiis.2020.09.015

The mother of all data breaches. (n.d.). Hoover Institution. https://www.hoover.org/research/mother-all-data-breaches

Tyson, M. (2022, May 19). *The quantum menace: Quantum computing and cryptography*. InfoWorld. https://www.infoworld.com/article/3659837/the-quantum-menace-quantum-computing-and-cryptography.html

Yang, M., Rwabutaza, A. A., & Bourbakis, N. G. (2012). A Comparative survey on Cryptology-Based methodologies. *International Journal of Information Security and Privacy*, *6*(3), 1–37. https://doi.org/10.4018/jisp.2012070101

Yin, R. K. (2018). *Case Study Research and Applications: Design and Methods*. SAGE Publications.