Cryptographic Telemetry

A Cornerstone of Zero Trust Architecture in the Quantum Era

November 11, 2024

Weiyee In, Chief Information Officer, Protego Trust Bank
Kurt Hardesty, Chief Information Security Officer, Protego Trust Bank
Jefferson Dance, Chief Innovation Officer Eclypses

Abstract

This white paper examines the critical role of cryptographic telemetry in implementing Zero Trust Architecture (ZTA) and defending against quantum computing threats in light of recent developments in the industry. We look at the intersection of NIST ZTA guidelines, from a Quantum Computing risk and data security perspective against requirements for financial institutions from NIST 800-53 Rev. 5, FedRAMP High SAF, EU DORA, and the EU AI Act to provide a comprehensive framework for financial institutions and other critical infrastructure sectors. The paper argues that robust cryptographic telemetry is essential for maintaining security, compliance, and operational efficiency in an increasingly complex and heterogeneous threat landscape.

Introduction

As quantum computing advances threaten to undermine current cryptographic standards, financial institutions globally face an urgent need to adapt and strengthen their security postures. Zero Trust Architecture, as outlined by NIST SP 800-207, provides a framework for this adaptation, emphasizing continuous verification and least-privilege access. However, the effective implementation of ZTA relies heavily on high-quality, real-time telemetry data, particularly in the realm of cryptographic operations and threat analysis. This paper explores how cryptographic telemetry serves as a linchpin in ZTA implementation, quantum threat mitigation, and regulatory compliance across multiple standards.

Quantum Wake up Calls

In the third quarter of 2024, Chinese researchers made advancements using the Canadian quantum computing pioneer, D-Wave's Advantage quantum computer, that had far-reaching implications for global cybersecurity and several significant implications for financial services institutions. A team of researchers from Shanghai University, leveraging D-Wave's Advantage quantum system, successfully factored a 22-bit RSA[1] integer. This achievement, detailed in the

[1] (Rivest-Shamir-Adleman)

Chinese Journal of Computers[2], represents a significant step forward in quantum computing's potential to challenge current encryption standards and has far-reaching implications globally.

The approach used by the researchers, transforming cryptographic attacks into combinatorial optimization problems leverages the strengths of D-Wave's quantum annealing systems. The team's work focuses on Substitution-Permutation Network (SPN) structured algorithms, and delved into the vulnerabilities of several key block ciphers, including Present, Rectangle, and Gift-64. Substitution-Permutation Networks are a fundamental design principle in modern cryptography. They form the backbone of many widely-used encryption standards, including the Advanced Encryption Standard (AES). The basic structure of an SPN involves alternating layers of substitution (S-boxes) and permutation (P-boxes), creating a complex relationship between the plaintext, key, and ciphertext. The specific block ciphers studied (Present, Rectangle, and Gift-64) are lightweight cryptographic algorithms, often used in resource-constrained environments like IoT devices or RFID tags.

The use of D-Wave's quantum annealing system to attack widely-used encryption algorithms suggests that quantum threats to cybersecurity may materialize far sooner than previously anticipated. While the 22-bit RSA integer factored is arguably far smaller than many of the real-world keys currently in use and definitely not military grade[3] it clearly demonstrates quantum computers' potential to solve cryptographic problems far earlier than expected. Aside from highlighting the rapidly growing capabilities and accessibility of quantum computers in cryptanalysis the work exposes the potential vulnerability of current encryption methods to quantum attacks. Published on the heels of the announcement of the final versions of NIST's first three Post-Quantum Cryptography Standards[4], released on August 13, 2024, it has already driven the cybersecurity community towards developing and implementing post-quantum cryptographic solutions to protect sensitive information in the impending era of widely accessible quantum computing.

Cryptographic Vulnerability

Whether the mass media "overstatements" and "hyperbole" are damaging and deflating to quantum research, and that RSA (Rivest-Shamir-Adleman) is indeed one of the oldest encryption technologies in the industry, there are several cryptographic vulnerabilities that need to be addressed. Financial institutions often face more significant challenges in securing their legacy technologies, networks, and other systems that rely heavily on RSA encryption. The widespread use of RSA across various critical applications, from "secure" communications to digital signatures for transactions, creates a complex landscape of cryptographic assets

---

[2] Wang Chao et al., "*Quantum Annealing Public Key Cryptographic Attack Algorithm Based on D-Wave Advantage*," Chinese Journal of Computers, published September 30, 2024

[3] Forbes: "*Debunking Hype: China Hasn't Broken Military Encryption With Quantum*" By Craig S. Smith

[4] National Institute of Standards and Technology. (2024, August 13). FIPS 203: Module-Lattice-Based Key-Encapsulation Mechanism Standard; National Institute of Standards and Technology. (2024, August 13). FIPS 204: Module-Lattice-Based Digital Signature Standard; National Institute of Standards and Technology. (2024, August 13). FIPS 205: Stateless Hash-Based Digital Signature Standard

pervasively interconnected and intermingled across legacy technologies that all become potentially vulnerable to quantum computing threats.

Many banks and financial services companies have built their infrastructure over decades of mergers, acquisitions and regulatory changes, resulting in a heterogeneous mix of modern, legacy and some sunsetted systems. These older environments are often heterogeneous and often continue to use older implementations of RSA with shorter key lengths that would now be considered insecure or at bare minimum vulnerable. The challenge lies not only in identifying and upgrading all instances of potentially vulnerable RSA implementations across a financial institutions' entire technology stack but also in managing the interconnected nature of financial systems where RSA is used for data encryption, authentication, digital signatures, and secure key exchange. The weakest link in this ecosystem often comes from traditional data transmission methods that may still be in use. For instance, older protocols for interbank transfers or customer-facing applications might rely on RSA implementations that are no longer considered secure against advanced computational attacks, let alone quantum threats.

Challenges in Identifying Vulnerabilities

These legacy systems and protocols create potential vulnerabilities that could be exploited, compromising the fundamental integrity of financial transactions and sensitive customer data. Moreover, the decades long-standing trust in RSA's security has led to its deep integration into a myriad of financial processes and regulations. To address these challenges, financial institutions need to implement comprehensive solutions that encompass a range of critical components. These include detailed cryptographic asset inventory processes, in-depth Security Information and Event Management (SIEM) integration, integrated threat analysis and detection mechanisms, and real-time monitoring and response capabilities. These measures collectively support early detection and efficient event or incident response management, helping to protect cryptographic periods and cipher mechanisms from potential attacks. While this approach may not fully address internal threat actors or direct attacks, the implementation of real-time detection mechanisms can significantly reduce overall risk of a financial institution.

By adopting a more holistic approach to security that combines modernization efforts with advanced monitoring and response capabilities, financial institutions can better protect their complex infrastructures against both current and emerging cryptographic threats. The challenge is that transitioning away from RSA to quantum-resistant algorithms is not just a technical challenge but also a regulatory and core operational one. Financial institutions must navigate complex compliance requirements while ensuring uninterrupted service to their customers during any cryptographic upgrades. The situation is further complicated by the global nature of financial networks. While some institutions might be proactive in upgrading their systems, they still need to maintain compatibility with partners and clients globally who may be slower to adopt new cryptographic standards.

This complex landscape creates a challenging scenario where even modernized systems might need to fall back or revert to less secure methods to ensure interoperability across the network

for commercial reasons. Such compromises potentially expose the entire infrastructure to vulnerabilities. As a result, when the risk associated with a particular algorithm increases, financial institutions face a critical decision point that is not always security or technology focused. They must either decrease the key cryptographic period, effectively shortening the lifespan of potentially vulnerable keys, or implement alternative mechanisms to wrap and secure communications. While this adaptive approach may be feasible in maintaining a balance between system-wide compatibility and robust security, it further highlights the need for a more holistic and dynamic security strategy that can rapidly respond to emerging threats while preserving the functionality of interconnected systems.

Legacy Systems and Regulatory Compliance

In essence, the decades-long ubiquity of RSA in financial systems, combined with the challenges of legacy infrastructure and the need for seamless global operations, creates a much more significant hurdle for financial institutions in securing their systems against emerging quantum threats. The task of conducting a comprehensive cryptographic asset inventory, upgrading identified vulnerable systems, and ensuring end-to-end security in data transmission represents a monumental challenge that requires not only careful planning, substantial resources, but also a coordinated industry-wide effort including regulatory alignment. Compound to these challenges is the advent of generative AI and the drive towards automation.

Into the fourth quarter of 2024, researchers and vendors in the financial services industry across the globe have been aggressively working on cryptanalysis leveraging what quantum computing is currently available and accessible to attackers. The challenge for financial institutions is that some legacy systems in financial institutions may be using versions of RSA encryption that are not only older and shorter key lengths that are now considered insecure but have bespoke adaptations that make them less discoverable and accessible to asset management tools. As computing power increases, these older implementations not only become more vulnerable to attacks but also become more difficult to upgrade without rip and replace strategies. Financial institutions often face significant challenges in upgrading their legacy systems due to both the complexity and interconnectedness of their infrastructure but also internal political challenges or genuine fear, uncertainty and doubt.

Early Days of Security

Originally, data sent over networks wasn't encrypted, making it easy for hackers to intercept sensitive information like credit card numbers and passwords. Security tools like intrusion detection systems (IDS) helped detect such risks, leading to improvements. The evolution of current network security practices aligns closely with various regulatory frameworks and standards. NIST's Zero Trust Architecture (ZTA) adopts an "assume breach" position, recognizing the limitations of traditional perimeter-based security. This principle is complemented through NIST 800-53 r5's control SC-8, emphasizing the protection of data in transit.

The need for automation led to the creation of intrusion prevention systems, which evolved from IDS and could automatically create firewall rules to block threats. This also led to the rise of Next Generation Firewalls (NGFW), which combined IDS and firewall functions to offer more comprehensive protection. Intrusion Prevention Systems (IPS) align with ZTA's principle of continuous monitoring and validation, emphasizing real-time threat detection and response. This approach is reinforced throughout the financial services industry by leveraging FedRAMP High SAF's control SI-4, which requires continuous monitoring of information systems, and FFIEC CAT's "Detect" domain, highlighting the importance of threat detection capabilities.

Today, a significant portion of the internet is encrypted by default, including social media, news, and shopping sites. The HTTP/2 protocol even requires encryption. Tools like Telnet have been replaced by secure alternatives (like SSH) for safer data transfers. The financial services industry's drive towards encryption is further reflected in several regulatory frameworks. GDPR's Article 32 mandates appropriate technical measures, with encryption being a key component for protecting personal data. Similarly, PCI DSS 4.0's Requirement 3 mandates encryption for cardholder data, while EU DORA's Article 10 emphasizes strong encryption in financial services.

Encryption has rendered traditional deep packet inspection (DPI) ineffective, as it can't inspect encrypted packets. To adapt, some security systems use SSL inspection (also known as SSL bump), which acts as a "man-in-the-middle" to decrypt, inspect, and re-encrypt data. NIST 800-53 r5's control SI-4(25) addresses the need for effective traffic analysis in encrypted environments, recognizing the complexities introduced by widespread encryption.

SSL inspection allows organizations to see users' private data without their knowledge, which raises privacy concerns. It can undermine trust between users and security teams, as users expect encryption to keep their data private. Privacy concerns are central to multiple frameworks. GDPR's Article 5 requires careful management of SSL inspection to comply with data protection principles. PSD2's Strong Customer Authentication requirements emphasize secure, privacy-preserving authentication methods. FFIEC TPRM guidelines stress the importance of managing and disclosing SSL inspection practices by third-party providers, ensuring appropriate security controls are maintained throughout the supply chain. While SSL inspection may have valid use cases, it often risks user trust and privacy, suggesting that it should be avoided in most cases. The focus should be on user education to enhance safe computing practices.

Impact of Quantum Threats

The continued use of vulnerable implementations in legacy systems including older RSA, especially in light of emerging threats from generative AI and quantum computing, poses significant security risks for financial institutions. This situation creates a complex, heterogeneous attack surface that is growing in breadth and depth that malicious actors can potentially exploit. Legacy systems in financial services often rely on much older versions of RSA encryption with shorter key lengths or outdated padding schemes that are now considered insecure even ahead of quantum computing. The challenge lies in the fact that these systems are deeply integrated into the core operations, policies, procedures and parameterization of systems of many financial institutions, making them difficult and costly to replace or upgrade. As a result, vulnerable RSA implementations persist in critical infrastructure, creating weak points in the overall security posture.

Role of Generative AI

The introduction of generative AI and advancements in quantum computing further exacerbate these risks. Generative AI could potentially be used to analyze patterns in encrypted traffic or generate sophisticated user focused social engineering or endpoint attacks that exploit known vulnerabilities in legacy RSA implementations. These AI tools can dramatically enhance the capabilities of malicious actors targeting financial institutions. While Generative AI is growing in popularity for its natural language interface, this ease of use also significantly widens and deepens the malicious actor universe or populace as they no longer even need to have years of coding experience to develop more targeted and effective attacks against financial systems. Coupled with quantum computing, this poses an even more significant threat. While current quantum computers may not yet be capable of breaking large parameter RSA encryption at scale, the development of sufficiently powerful quantum computers could render many current RSA implementations obsolete.

This heightens the "harvest now, decrypt later" scenario risk where malicious actors are able to collect encrypted data with the intention of decrypting it once quantum computers become more advanced. The combination of known vulnerabilities in legacy systems and these emerging technologies creates a particularly dangerous scenario. Attackers could potentially use a variety of AI to identify and exploit combinations of vulnerabilities that might not be obvious to human analysts. For example, they might use Generative AI to combine a weakness in an old RSA implementation with other vulnerabilities in legacy systems to gain unauthorized access to sensitive financial data or systems. LLMs like GPT-4, Claude, and open-source alternatives present a significant threat vector for banks, particularly in the context of exploiting vulnerabilities in legacy systems using outdated RSA implementations.

LLMs can be used to rapidly analyze and interpret complex cryptographic documentation and research papers, giving even novice bad actors a deeper and more powerful understanding of vulnerabilities in legacy RSA implementations or other details of legacy technologies in large financial institutions worldwide. This knowledge can be leveraged to identify weaknesses that might not be immediately apparent to human analysts, potentially uncovering novel attack

vectors. One of the most concerning applications of LLMs is their ability to generate highly sophisticated and personalized phishing emails or social engineering scripts. These AI-generated messages can be tailored to target specific individuals within a bank who have access to legacy systems. By incorporating details gleaned from public information or previous data breaches, these phishing attempts can be incredibly convincing, increasing the likelihood of successfully compromising employee credentials which may lead to gaining unauthorized access to sensitive systems.

Newer versions of LLMs can assist attackers with low-code or no-code in writing exploit code by providing code snippets or explaining complex cryptographic concepts. This capability in most of the newer Generative AI chatbots lowers the barrier to entry for even the least skilled attackers, potentially leading to an increase in the sheer number but also in the sophistication of attacks against financial institutions. An attacker could, for instance, use an LLM to help research and craft a custom exploit that combines a weakness in an old RSA implementation with other vulnerabilities in legacy banking software or with other sophisticated phishing attempts.

The use of LLMs in this context also significantly amplifies the "harvest now, decrypt later" threat. Attackers can use these AI tools to more efficiently discover, access, collect and analyze encrypted data from legacy systems, with the intention of decrypting it once quantum computers become more advanced. This long-term threat is particularly concerning for banks, as financial data often retains its value and sensitivity for extended periods and is often held for regulatory compliance reasons. To mitigate these risks, financial institutions must prioritize upgrading legacy systems, implementing robust AI-powered defensive measures, and providing ongoing training to staff about evolving AI-driven threats. Additionally, financial institutions should consider implementing quantum-resistant cryptographic algorithms to protect against future decryption attempts using quantum computers. The biggest hurdle many financial institutions still face remains visibility challenges associated with legacy systems that make it difficult for financial institutions to conduct comprehensive cryptographic asset inventories. This lack of visibility means that vulnerable RSA implementations may exist in unexpected places within the infrastructure, creating blind spots in security efforts.

These activities not only have broad significant implications for global cybersecurity and financial institutions, it fundamentally suggests that the timeline for quantum computers to pose a credible threat to current encryption methods may be far closer than previously anticipated. The more recent flurry of activity also highlights the urgent need for quantum-safe or post-quantum cryptographic solutions. In the financial services industry many have argued for global cooperation and knowledge sharing among researchers, industry experts, and government agencies to accelerate the development and adoption of quantum-resistant cryptography. For financial institutions quantum-resistant solutions for different applications and segments of finance must be tailored because of unique commercial requirements and constraints of regulations, not to mention the plethora of legacy technologies in the installed base.

The now imminent advent of quantum computing accessibility poses a significant threat to many widely-used cryptographic algorithms, particularly those relying on the difficulty of certain mathematical problems. This vulnerability is not merely theoretical but represents a looming reality that could undermine the security of digital communications and data storage on a global scale.

Key Vulnerable Cryptographic Systems

RSA (Rivest-Shamir-Adleman)

RSA encryption, because it has been such an entrenched cornerstone of modern cryptography, has not only been widely but also deeply deployed across financial institutions and payment processing systems and infrastructure. Its security is predicated on the computational difficulty of factoring large composite numbers into their prime factors, a task that has long been considered infeasible for classical computers at scale. However, as cited above the advent of quantum computing poses a significant threat to this fundamental assumption. Quantum computers, leveraging Shor's algorithm, have already demonstrated the potential to factor these large numbers exponentially faster than their classical counterparts.

The vulnerability of RSA to quantum computing hacking is profound. A sufficiently powerful quantum computer could break RSA encryption by efficiently factoring the public key, thereby compromising the associated private key. This capability would effectively nullify the security guarantees that RSA and its concomitant infrastructure has provided for decades. The impact of such a disruption would be far-reaching, affecting a wide array of critical security infrastructure. Secure communications channels, digital signature systems, and key exchange protocols across financial services institutions globally that rely on RSA would all be rendered vulnerable. This compromise would extend beyond just data confidentiality as it also threatens the integrity and non-repudiation aspects of digital transactions and “secure” communications that are fundamental to the trust mechanisms underpinning global financial systems and e-commerce.

The implications of this vulnerability are particularly acute for cross border transactions globally because RSA is deeply embedded in transaction processing, identity verification, and data protection systems across the financial sector. As quantum computing capabilities advance, financial institutions face the urgent need to assess their cryptographic infrastructures, assets and devices and begin planning for a post-quantum cryptography era. This transition is not merely a technical upgrade but a fundamental shift in how digital security is conceptualized and implemented in an age where classical cryptographic assumptions no longer hold. For RSA, the combination of known vulnerabilities in legacy systems and emerging technologies creates a particularly dangerous scenario for financial institutions.

ECC (Elliptic Curve Cryptography)
Elliptic Curve Cryptography (ECC) is a powerful and widely adopted approach across financial institutions globally to public-key cryptography that derives its security from the inherent complexity of the Elliptic Curve Discrete Logarithm Problem (ECDLP). The ECDLP poses a

significant challenge for classical computers, historically making ECC a robust choice for securing various cryptographic protocols throughout today's digital landscape. The problem involves finding a scalar k such that Q = kP, where P and Q are points on an elliptic curve, and the operation is repeated point addition.

The strength of ECC lies in the fact that, for carefully chosen elliptic curves, solving the ECDLP is computationally impractical and often infeasible with current classical computing technologies. This property has led to the widespread adoption of ECC in numerous security-critical applications, including secure key exchange protocols, digital signature schemes, and encryption systems. ECC offers comparable security to traditional methods like RSA but with significantly smaller key sizes, making it particularly attractive for resource-constrained environments and has become widely deployed across financial institutions. However, again the advent of quantum computing poses a severe threat to the security foundations of ECC. Shor's algorithm, a quantum algorithm designed to solve integer factorization and discrete logarithmic problems, can be adapted to efficiently solve the ECDLP. A quantum computer implementing Shor's algorithm could break all manner of ECC-based cryptosystems in polynomial time, a feat that has heretofore been considered practically impossible with traditional computers.

The vulnerability of ECC to quantum attacks has far-reaching implications in financial institutions. The quantum threat would compromise the security of a vast array of modern cryptographic protocols and systems that rely on ECC. This includes widely used secure communication protocols, digital signature schemes used for authentication and non-repudiation, and key exchange mechanisms that form the backbone of secure internet communications. The potential impact of this vulnerability extends across multiple sectors and applications throughout financial institutions, e-commerce platforms, secure messaging apps, and many other systems that depend on ECC for their security. The compromise of ECC would necessitate a rapid and widespread transition to quantum-resistant cryptographic algorithms, a process that presents significant discovery, asset management, logistical and technical challenges.

In response to this looming threat, the financial services industry and the cryptographic community have been aggressively researching and developing post-quantum cryptographic solutions. These efforts aim to create new cryptographic systems that can withstand attacks from both classical and quantum computers, ensuring the continued security of digital communications and transactions in the quantum era. As the development of quantum computers progresses, the urgency to implement quantum-resistant cryptography, including alternatives to ECC, becomes increasingly critical for maintaining the integrity and confidentiality of sensitive information in the world of digitally interconnected transactions.

Diffie-Hellman Key Exchange

The Diffie-Hellman protocol is also core to modern secure communications in financial services, providing a method for two parties to establish a shared secret key over an insecure channel without prior knowledge of each other. This protocol's security is fundamentally based on the

computational intricacies and difficulty of solving the discrete logarithm problem, a mathematical challenge that has long been considered intractable for classical computers when sufficiently large numbers are used. The discrete logarithm problem, in the context of Diffie-Hellman, involves finding an exponent given a base and a result in a finite field. More specifically, given a prime p, a generator g, and a value h, the problem is to find x such that g^x ≡ h (mod p). The security of Diffie-Hellman relies on the assumption that this problem is computationally infeasible to solve for large primes.

Quantum computers, leveraging Shor's algorithm, have been able to solve the discrete logarithm problem on which Diffie-Hellman's security is based, with far greater alacrity than the financial services community had expected. This algorithm's ability to break the protocol in polynomial time fundamentally undermines the security assumptions upon which Diffie-Hellman is built, a sufficiently powerful quantum computer could use Shor's algorithm to compute the private keys from the public information exchanged during the Diffie-Hellman protocol. The vulnerability of Diffie-Hellman to quantum attacks has far-reaching implications for cybersecurity.

While not specific just to quantum computing as a risk, Diffie-Hellman's increasing fragility makes it vulnerable to communications attacks. Quantum computing, however, exacerbates this vulnerability by making it easier for an attacker to impersonate legitimate parties. Many "secure" communication protocols that form the backbone of internet security and communications among financial institutions rely on Diffie-Hellman for key agreement including:

- Transport Layer Security (TLS): Heavily used to secure web browsing, email, and other internet communications.
- Internet Protocol Security (IPsec): Employed for securing Virtual Private Networks (VPNs).
- Secure Shell (SSH): Widely used for secure remote system administration.

The compromise of Diffie-Hellman affects each of these protocols, potentially exposing encrypted communications to interception and decryption by adversaries with access to quantum computing. This threat extends beyond just the confidentiality of current communications; it also poses a more fundamental risk to the long-term security of data that has been previously encrypted and stored, as such data could be decrypted in the future when quantum computers become more readily available. The "harvest now, decrypt later" attack scenario becomes a far greater threat. Malicious actors could capture and store encrypted data today and decrypt it when sufficiently powerful quantum computers become available, compromising long-term data confidentiality. Moreover, the impact also extends to the integrity and authenticity of digital communications and the integrity or provenance of data.

Many financial institutions still use Diffie-Hellman technologies as part of their authentication processes, and its compromise leads to increased vulnerability to man-in-the-middle attacks and impersonation. If a bad actor can break the Diffie-Hellman exchange, they could intercept and modify communications between parties and in financial institutions this could result in unauthorized transactions or access to sensitive data, data theft, fraud or manipulation of financial records. At bare minimum such a compromise would undermine the legal validity and

provenance of financial agreements and contracts. From a regulatory perspective, failure to protect personal financial data due to cryptographic vulnerabilities could lead to severe penalties and legal action under GDPR, CCPA, and other data protection laws and non-compliance with required security standards for financial institutions under PCI DSS, FFIEC guidelines, Basel or others could result in fines, loss of licenses, or restrictions on operations.

Historical financial data could also be decrypted or tampered with, compromising not only long-term confidentiality of transactions and strategic information but also poisoning AI models. Even basic operations of financial institutions under SEC regulations, Sarbanes-Oxley Act or other CCAR reporting could all be compromised due to data integrity which could lead to inaccurate financial reporting, potentially resulting in regulatory actions and penalties.

Organizations and standards bodies have been working to develop and standardize post-quantum cryptographic algorithms, with the goal of ensuring the continued security of digital communications in the quantum era. These post-quantum cryptographic methods aim to provide secure key exchange mechanisms that can withstand attacks from both classical and quantum computers. However, the transition to these new protocols presents significant challenges, including ensuring backward compatibility, managing the performance impact of more complex algorithms, and updating a vast array of existing systems and software. As quantum computing technology advances, the urgency to implement quantum-resistant cryptography increases. This effort represents one of the most significant challenges in the field of cryptography since the advent of public-key cryptography itself.

Digital Signature Algorithms

Digital Signature Algorithms (DSA) and many of their variants, such as the Elliptic Curve Digital Signature Algorithm (ECDSA), are already heavily deployed and integrated across financial institutions for digital authentication and integrity verification. DSA, developed by NIST, bases its security on the discrete logarithm problem. ECDSA, an elliptic curve variant of DSA, leverages the elliptic curve discrete logarithm problem. Both of these, along with the integer factorization problem used in RSA, have historically also been believed to be intractable for classical computers when sufficiently large parameters are used. Even ahead of the recent flurry of activity, quantum computers, leveraging Shor's algorithm, have demonstrated the potential to efficiently solve these underlying mathematical problems. This capability could allow any bad actor with access to a sufficiently powerful quantum computer to forge digital signatures, effectively breaking the security guarantees provided by these algorithms.

Impacts to Financial Institutions

The vulnerability of digital signature schemes to quantum attacks, combined with the prevalence of legacy technologies in banks and the emerging threat of generative AI and Large Language Models (LLMs) being used by attackers, presents a multifaceted challenge with significant business, security, and data impacts for financial institutions is merely the tip of the iceberg. However it is quite indicative of many of the business implications of the current landscape. Legacy or “traditional” systems often form the backbone of critical financial operations.

Upgrading or replacing these systems to address these heterogeneous vulnerabilities could lead to significant operational disruptions and downtime. Even the process of identifying, upgrading, or replacing vulnerable systems will likely incur substantial costs, including hardware, software, and personnel expenses. Because very often regulations are not harmonized and not consistent across industries and geographies financial institutions continually struggle to meet evolving regulatory requirements related to data security and privacy. All the while financial institutions are still relying on legacy systems vulnerable to the combination of obsolete legacy systems, quantum vulnerabilities, and AI-powered attacks significantly expands the attack surface that they must defend.

The vulnerability of these digital signature schemes to quantum attacks also has far-reaching implications across financial institutions:

- Secure Email Communications: Digital signatures are crucial for verifying the authenticity and integrity of email messages. As quantum computing advances even further, attackers may be able to break encryption and digital signatures used in legacy systems in real time, compromising “secure” communications and financial transactions, especially where legacy technologies are deployed. Upgrading or replacing these systems to address quantum vulnerabilities could lead to significant operational disruptions and downtime. A compromise of these systems could lead to widespread email spoofing and the inability to trust the origin of electronic communications.
- Software Distribution: Many software companies use digital signatures to verify the authenticity of their software packages and updates. The ability to forge these signatures could lead to the widespread distribution of malicious software masquerading as legitimate updates. The "harvest now, decrypt later" approach enabled by quantum computing threatens not only the long-term confidentiality of sensitive financial data but software packages and patches.
- Financial Transactions: Digital signatures are extensively used in electronic financial transactions to ensure non-repudiation. The ability to forge signatures could undermine the legal and financial frameworks built on these cryptographic guarantees. Weaknesses in digital signature schemes could allow attackers to forge signatures, potentially compromising the integrity of financial transactions, legal documents, and regulatory filings. Data privacy violations aside, the integrity and provenance of the data for model training and model implementation can become compromised.
- Legal and Regulatory Compliance: Many legal and regulatory frameworks, such as eIDAS in the European Union, rely on the integrity of digital signatures. A compromise of these systems could have significant legal and compliance implications.
- Internet of Things (IoT) Security: Many IoT devices use digital signatures for secure boot processes and firmware updates. The combination of traditional systems and infrastructure, quantum vulnerabilities, and AI-powered attacks significantly expands the attack surface that banks must defend. IoT exacerbates that exponentially. Vulnerabilities in these signature schemes could lead to widespread compromise of IoT networks.
- Blockchain and Cryptocurrencies: Many blockchain systems, including popular cryptocurrencies, rely on ECDSA for transaction signing. The ability to forge signatures

could potentially allow for theft of cryptocurrency assets and manipulation of blockchain records. AI toolkits and Generative AI LLMs have already assisted bad actors in rapidly developing and deploying exploits targeting specific vulnerabilities in blockchains.

- Secure Communication Protocols: Protocols like TLS, which underpin secure internet communications, use digital signatures as part of their handshake process. Vulnerabilities in these signature schemes could compromise the security of a wide range of internet communications.

The potential impact of quantum computers on digital signature schemes underscores the growing urgency and need not only the development of tailored post-quantum cryptographic algorithms but their implementation and integration. NIST is already in the process of standardizing quantum-resistant cryptographic algorithms, including digital signature schemes, to address these vulnerabilities. In the interim, cryptographers and security professionals are exploring hybrid approaches that combine classical and post-quantum algorithms to provide a transition path and maintain backwards compatibility while enhancing security against potential quantum attacks. Organizations handling sensitive data or long-lived assets are advised to begin planning for this transition, considering the potential long-term implications of current vulnerabilities in the face of advancing quantum computing capabilities.

Long-Term Data Confidentiality

The "capture/harvest now, decrypt later" attack scenario poses a significant threat to financial institutions, highlighting the importance of long-term data confidentiality. This threat involves malicious adversaries gathering and storing encrypted data today with the intention of decrypting it when quantum computers become available, potentially compromising sensitive information in the future. Several regulatory frameworks and guidelines for financial institutions address these and related concerns, emphasizing the critical role of encryption in protecting data and the overhanging risk of "capture/harvest now, decrypt later" attack scenarios:

- The FFIEC Cybersecurity Assessment Tool (CAT) directly addresses this issue in Domain 3: Cybersecurity Controls. Under the "Encryption" category, it states: "*The institution uses encryption to protect sensitive data in storage and in transit*." This requirement underscores the need for financial institutions to implement encryption that can withstand both current and future threats, including those posed by quantum computing.
- The FFIEC IT Examination Handbook on Outsourcing Technology Services further reinforces this point, stating: "*Financial institutions should implement encryption controls and other compensating controls to secure data in transit and at rest.*" This requirement extends to third-party service providers, necessitating a review of their long-term data protection strategies.
- The General Data Protection Regulation (GDPR) also mandates encryption as a key measure for data protection. Article 32 on "Security of processing" states: "*The controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including [...] the encryption of personal data*."

- The Payment Services Directive 2 (PSD2) aligns with these requirements. Its Regulatory Technical Standards (RTS) on Strong Customer Authentication and Secure Communication state in Article 4(1): "*Payment service providers shall ensure that sensitive payment data is encrypted in transit and at rest*."
- PCI DSS 4.0 significantly reinforces the importance of encryption and secure handling of sensitive financial data. The standard provides specific requirements for financial institutions that directly address the use of strong cryptography and proper data protection practices. The standard emphasizes the importance of strong cryptography through several key requirements. Requirement 2.2.7 mandates the use of strong cryptography for non-console administrative access, while Requirements 2.3.1 and 2.3.2 extend this to specify the need for strong cryptography in encrypting all non-console administrative access. Requirement 3.5.1 addresses the protection of cryptographic keys used for cardholder data encryption, safeguarding them against disclosure and misuse. The necessity of a documented cryptographic key management process is outlined in Requirement 3.6.1, with Requirement 3.6.1.2 specifically emphasizing secure cryptographic key distribution. Additionally, Requirements 3.7, 4.2, and 12.3.3 provide general guidelines on the implementation of strong cryptography throughout the system.
- The EU Digital Operational Resilience Act (DORA) emphasizes the importance of encryption throughout the data lifecycle. Article 6 of the Regulatory Technical Standards (RTS) states: "*Data encryption is deemed essential throughout the entire data lifecycle, covering data at rest, in transit, and in use*."

These regulatory frameworks collectively underscore the critical importance of implementing robust encryption measures to ensure long-term data confidentiality and protect against future threats, including those posed by quantum computing.

Infrastructure Security

Many critical infrastructure systems, including financial networks, power grids, and telecommunications, rely on these vulnerable cryptographic algorithms. The security of critical infrastructure systems is a paramount concern across multiple regulatory frameworks and standards. Their compromise could have far-reaching consequences for national and economic security with even more direct impact to financial services firms and not only require constant monitoring but also the use of cryptographic technologies. Several key regulatory frameworks and standards address the importance of protecting critical infrastructure through robust cryptographic measures:

- NIST Special Publication 800-207 on Zero Trust Architecture (ZTA) emphasizes that "*ZTA can be applied to any type of network and service, including critical infrastructure systems.*" It recommends "*Continuous monitoring and risk assessment of all resources, including those in critical infrastructure sectors.*"
- NIST 800-53 Rev 5 Control SC-13 (Cryptographic Protection) mandates that "*organizations implement defined cryptographic uses and types of cryptography in accordance with applicable laws, regulations, and standards*." This underscores the need for up-to-date cryptographic protection for critical systems.

- The FedRAMP High Security Assessment Framework (SAF) includes control SC-28 (1), which requires the implementation of cryptographic mechanisms to prevent unauthorized disclosure and modification of defined information on specified system components.
- The FFIEC Cybersecurity Assessment Tool (CAT) Domain 3 states that institutions must use encryption to protect sensitive data in storage and in transit, extending this requirement to critical infrastructure systems within financial institutions.
- The FFIEC IT Examination Handbook on Third-Party Risk Management emphasizes that "*Management should ensure third-party service providers implement appropriate security controls, including encryption of sensitive data,*" highlighting the need for robust cryptographic protection even when using third-party services for critical infrastructure.
- The General Data Protection Regulation (GDPR) Article 32 requires the implementation of appropriate technical measures, including encryption of personal data, to ensure a level of security appropriate to the risk. While focused on personal data, this requirement by default extends to critical infrastructure systems that process such data.
- The Payment Services Directive 2 (PSD2) Article 97 mandates strong customer authentication for electronic payment transactions, emphasizing the need for robust cryptographic methods in financial transaction systems.
- PCI DSS 4.0 Requirement 3.2 states that "*Sensitive authentication data is not stored after authorization (even if encrypted),*" highlighting the importance of protecting critical financial data through both encryption and proper data handling.
- Lastly, the EU Digital Operational Resilience Act (DORA) Article 13 requires financial entities to have internal governance and control frameworks for effective and prudent management of all ICT risks, which includes the use of appropriate cryptographic measures.

These regulatory frameworks collectively underscore the critical importance of implementing robust cryptographic protection for critical infrastructure systems, particularly in the financial sector, to safeguard against potential vulnerabilities and ensure long-term security.

Digital Identity and Authentication

The potential vulnerability of digital signature schemes to quantum computing threats poses a significant risk to digital identity and authentication systems across the financial services industry. This concern is reflected in numerous regulatory frameworks and standards that emphasize the importance of robust authentication and identity verification:

- NIST Special Publication 800-207 on Zero Trust Architecture (ZTA) underscores the critical nature of authentication, stating that "*ZTA requires that no implicit trust be granted to assets or user accounts based solely on their physical or network location*" and "*User authentication is dynamic and strictly enforced before access is allowed.*"
- NIST 800-53 Rev 5 Control IA-2 mandates that information systems "*uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users).*" Control IA-5 further requires organizations to manage system authenticators by "*protecting authenticators commensurate with the security category of the information to which use of the authenticator permits access.*"

- The FedRAMP High Security Assessment Framework (SAF) includes control IA-2 (12), which specifies that information systems must accept and electronically verify Personal Identity Verification (PIV) credentials, emphasizing the need for strong, verifiable digital identities.
- The FFIEC Cybersecurity Assessment Tool (CAT) Domain 3 requires institutions to implement multifactor authentication for employees and third parties accessing internal networks and systems. Similarly, the FFIEC IT Examination Handbook on Third-Party Risk Management states that "*Management should ensure third-party service providers implement appropriate authentication and access controls*."
- The General Data Protection Regulation (GDPR) Article 32 requires the implementation of appropriate technical and organizational measures to ensure security, including "*a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing*." This encompasses the integrity of authentication and digital identity systems.
- The Payment Services Directive 2 (PSD2) Article 97 mandates that "*Payment service providers shall apply strong customer authentication where the payer [...] initiates an electronic payment transaction,*" highlighting the critical role of robust digital identity and authentication in financial transactions.
- PCI DSS 4.0 Requirement 8.3 states that "*Strong authentication methods are used for all user access to system components,*" with Requirement 8.3.1 specifying that "*All user access to system components is authenticated via an authentication mechanism that uses at least two different authentication factors.*"
- Lastly, the EU Digital Operational Resilience Act (DORA) Article 8 requires financial entities to "*implement authentication mechanisms that allow for the verification of the identity and access rights of users and systems accessing the network and internal systems.*"

These regulatory frameworks collectively underscore the critical importance of maintaining robust digital identity and authentication systems in the face of emerging threats, including those posed by quantum computing. The potential vulnerability of current digital signature schemes to quantum attacks necessitates a proactive approach to developing and implementing quantum-resistant authentication methods to ensure continued compliance with these standards and regulations.

Timeline and Urgency

Security experts project a 50% probability that quantum computers capable of breaking current encryption will be in the market by 2031, however several recent proofs of concept and activities suggest the time to Q-day may in fact be sooner. This accelerated timeline necessitates more immediate action from financial institutions to transition to quantum-resistant cryptography and implement robust monitoring systems. However, the urgency and criticality of security across financial institutions and their infrastructure is also vital for threat vectors already present in today’s hybrid and multi-cloud environments.

Cryptographic telemetry is not merely a technical requirement but a strategic necessity in the age of quantum computing and sophisticated cyber threats. By aligning cryptographic telemetry practices with ZTA principles and regulatory requirements, financial institutions can build a resilient, compliant, and future-proof security posture. As we stand on the brink of the quantum era, the integration of comprehensive cryptographic telemetry into cybersecurity strategies is imperative for long-term security, regulatory compliance, and operational resilience.

References

1 National Institute of Standards and Technology. (2022). Post-Quantum Cryptography Standardization.
2 Rose, S., et al. (2020). Zero Trust Architecture (NIST Special Publication 800-207). National Institute of Standards and Technology.
3 Gigamon. (2024). 3 Thoughts on Operationalizing Zero Trust Architecture.
4 Anderson, B., & McGrew, D. (2017). Machine Learning for Encrypted Malware Traffic Classification: Accounting for Noisy Labels and Non-Stationarity. In Proceedings of the 23rd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining.
5 National Institute of Standards and Technology. (2023). SP 800-207A: A Zero Trust Architecture Model for Access Control in Cloud-Native Applications in Multi-Location Environments.