FIKRESEKHEL

RESEARCH TODAY, SHAPING TOMORROW

Quantum Threat Report

August/2025

www.fikresekhel.com

Quantum Threat Report: Navigating the Post-Quantum Cryptography Era

The Imminent Threat to Digital Security

Introduction

The advent of quantum computing heralds a new era of technological advancement, promising to revolutionize fields from medicine to artificial intelligence. However, this transformative power also casts a long shadow over the foundational pillars of global digital security: cryptography. The cryptographic algorithms that currently safeguard our communications, financial transactions, and sensitive data are, in large part, vulnerable to attacks from sufficiently powerful quantum computers. This report aims to comprehensively explore the nature of this threat, the profound risks associated with inaction, and the urgent imperative to prepare for the post-quantum cryptography era. FikreSekhel, with its extensive experience and leadership in cybersecurity and advanced cryptography, stands at the forefront of this critical transition, offering unparalleled solutions and expertise to mitigate these risks and ensure the digital resilience of its clients.

Our digital world is built upon a complex web of cryptographic protocols that ensure confidentiality, integrity, and authenticity. From securing online banking and e-commerce to protecting national defense secrets and personal privacy, cryptography is the invisible shield that underpins modern society. The security of these protocols relies on the computational difficulty of certain mathematical problems, such as factoring large numbers or solving discrete logarithms. Classical computers would require an astronomical amount of time—often billions of years—to break these cryptographic puzzles, rendering them practically secure. However, quantum computers, leveraging the principles of quantum mechanics, possess the theoretical capability to solve these problems with unprecedented speed, effectively dismantling the security assurances we currently rely upon. This report will delve into the specific quantum algorithms that pose the most significant threats, examine their implications, and outline the strategic responses necessary to safeguard our digital future.

The Quantum Menace: Shor's Algorithm and the RSA Cryptosystem

At the heart of the quantum threat to modern cryptography lies Shor's algorithm, a groundbreaking quantum algorithm developed by Peter Shor in 1994. This algorithm has the potential to render many of the most widely used public-key cryptosystems, including the ubiquitous RSA algorithm, obsolete. The security of RSA is predicated on the immense difficulty of factoring large composite

numbers into their prime factors. For classical computers, this task is computationally infeasible for sufficiently large numbers, forming the basis of RSA's security. However, Shor's algorithm can perform this factorization exponentially faster than any known classical algorithm, posing a direct and existential threat to RSA-based security.

Shor's algorithm achieves this remarkable feat by leveraging the principles of quantum Fourier transform. It can efficiently find the period of a function, which is a crucial step in factoring large numbers. The algorithm's ability to perform this calculation in polynomial time, as opposed to the exponential time required by classical algorithms, is what makes it so powerful. The implications of this are staggering. A sufficiently powerful quantum computer running Shor's algorithm could break a 2048-bit RSA key, a standard for secure communications today, in a matter of hours or even minutes. This would expose a vast amount of sensitive data, from financial transactions and government secrets to personal emails and private messages, to unauthorized access.

The threat is not merely theoretical. While large-scale, fault-tolerant quantum computers are still under development, the progress in this field is accelerating rapidly. Governments and corporations worldwide are investing billions of dollars in quantum research, and it is only a matter of time before a quantum computer capable of breaking RSA becomes a reality. This looming threat necessitates a proactive and urgent transition to quantum-resistant cryptography, a new generation of cryptographic algorithms designed to be secure against attacks from both classical and quantum computers. FikreSekhel is at the forefront of this transition, developing and implementing post-quantum cryptographic solutions to ensure the long-term security of our clients' digital assets.

The Quantum Search Problem: Grover's Algorithm and Its Implications

Grover's algorithm, developed by Lov Grover in 1996, is another powerful quantum algorithm that poses a significant, albeit different, kind of threat to our digital infrastructure. Unlike Shor's algorithm, which targets the mathematical foundations of public-key cryptography, Grover's algorithm provides a quadratic speedup for unstructured search problems. This means it can find a specific item in an unsorted database of N items in approximately $\sqrt{N}$ steps, whereas a classical computer would require, on average, N/2 steps. While this may not seem as dramatic as the exponential speedup offered by Shor's algorithm, its implications are far-reaching and impact a wide range of applications, including symmetric-key cryptography and database security.

Symmetric-key algorithms, such as the Advanced Encryption Standard (AES), are not directly vulnerable to Shor's algorithm. However, they can be theoretically broken by a brute-force attack, where an attacker tries every possible key until the correct one is found. The security of these algorithms relies on the key space being so large that a brute-force attack is computationally infeasible for classical computers. Grover's algorithm, however, can be used to speed up this

brute-force search, effectively reducing the security of a symmetric-key algorithm. For example, a 128-bit AES key, which is considered secure against classical brute-force attacks, would only offer the equivalent of 64-bit security against an attacker with a quantum computer running Grover's algorithm. This reduction in effective key strength necessitates a re-evaluation of key lengths for symmetric-key algorithms in the post-quantum era.

Beyond cryptography, Grover's algorithm has implications for any application that relies on searching large, unstructured databases. This includes a wide range of fields, from scientific research and data analysis to financial modeling and artificial intelligence. The ability to search these databases quadratically faster could lead to significant breakthroughs, but it also raises security concerns. For example, an attacker could use Grover's algorithm to more quickly find sensitive information in a compromised database, or to reverse-engineer proprietary algorithms. As with the threat from Shor's algorithm, the solution lies in developing and deploying quantum-resistant solutions. FikreSekhel is actively engaged in this effort, providing our clients with the expertise and tools necessary to secure their data against all forms of quantum attack.

Beyond Algorithms: Quantum Side-Channel Attacks

While Shor's and Grover's algorithms represent direct algorithmic threats to cryptographic systems, the quantum threat landscape extends beyond these. Quantum side-channel attacks (SCA) exploit information leaked by the physical implementation of cryptographic systems, rather than attacking the mathematical properties of the algorithms themselves. These leaks can come in various forms, such as power consumption, electromagnetic emissions, or even timing variations during cryptographic operations. While SCAs are not new to classical cryptography, the unique characteristics of quantum systems introduce new avenues for such attacks.

Quantum computers and quantum cryptographic devices, by their very nature, are highly sensitive to environmental factors. This sensitivity, while crucial for their operation, can also be a source of unintended information leakage. For instance, the precise timing of quantum gate operations, the power fluctuations during qubit manipulation, or even the faint electromagnetic signals emitted by superconducting circuits could potentially reveal sensitive information about the cryptographic keys being used. An attacker with sophisticated quantum measurement capabilities could potentially exploit these side channels to extract secret keys, even from quantum-resistant algorithms.

The challenge with quantum SCAs is twofold. First, the physical implementations of quantum systems are still in their nascent stages, and their precise side-channel characteristics are not yet fully understood. This makes it difficult to design effective countermeasures. Second, traditional SCA countermeasures, such as masking and shuffling, may not be directly applicable or sufficient in the quantum realm due to the unique properties of quantum information. This necessitates a new paradigm for designing secure quantum hardware and software, one that inherently considers and mitigates side-channel leakage.

FikreSekhel recognizes the critical importance of addressing quantum side-channel vulnerabilities. Our research and development efforts extend to exploring these emerging threats and devising robust countermeasures. We work closely with hardware manufacturers and quantum researchers to understand the physical characteristics of quantum systems and to integrate security-by-design principles into the development of post-quantum cryptographic solutions. Our expertise in both classical and quantum cybersecurity positions us uniquely to identify and mitigate these subtle yet potent threats, ensuring that our clients' systems remain secure against even the most advanced quantum attacks.

The Current State of Quantum Computing and the Urgency of Migration

The discussion of quantum threats often leads to the question: how far are we from a quantum computer capable of breaking current encryption? While a large-scale, fault-tolerant quantum computer is not yet a reality, significant progress is being made globally. Major technology companies, governments, and academic institutions are investing heavily in quantum research and development. We are currently in the Noisy Intermediate-Scale Quantum (NISQ) era, where quantum computers have tens to hundreds of qubits but are still prone to errors. However, advancements in qubit coherence, error correction techniques, and quantum algorithm development are rapidly pushing the boundaries of what is possible.

Estimates for when a cryptographically relevant quantum computer (CRQC) will emerge vary, but many experts predict it could be within the next 10 to 15 years, or even sooner. This timeline, while seemingly distant, is critical when considering the lifespan of sensitive data. Information encrypted today, if intercepted and stored by an adversary, could be decrypted in the future once a CRQC becomes available. This concept, known as 'Harvest Now, Decrypt Later' (HNDL), poses a significant risk to long-lived sensitive data, such as government secrets, intellectual property, and personal health records. The time it takes to transition to new cryptographic standards is also a major factor. Migrating complex IT infrastructures to new cryptographic algorithms is a monumental task that can take years, if not decades, for large organizations.

Therefore, the urgency of migration to post-quantum cryptography (PQC) cannot be overstated. Organizations must begin assessing their cryptographic inventory, identifying vulnerable systems, and developing a migration roadmap. The National Institute of Standards and Technology (NIST) has been leading an international effort to standardize PQC algorithms, and the first set of algorithms has already been selected. This provides a clear path forward for organizations to begin their transition. FikreSekhel is actively tracking these developments and is uniquely positioned to guide organizations through every step of their PQC migration journey, from initial assessment and

planning to implementation and ongoing management. Our proactive approach ensures that our clients are not caught unprepared when the quantum threat fully materializes.

FikreSekhel: Pioneering Solutions in Post-Quantum Security

In the face of these multifaceted quantum threats, FikreSekhel stands as a beacon of expertise and innovation, leading the charge in securing the digital future. Our commitment to understanding, anticipating, and neutralizing quantum-driven cybersecurity risks is unwavering. We recognize that the transition to a post-quantum world is not merely a technical upgrade but a strategic imperative that demands foresight, deep technical knowledge, and a comprehensive approach to risk management. Our team comprises world-renowned cryptographers, quantum physicists, and cybersecurity architects who are not only abreast of the latest advancements in quantum computing but are actively contributing to the development of quantum-resistant solutions.

FikreSekhel's expertise spans the entire spectrum of post-quantum cryptography (PQC), from fundamental research to practical implementation. We are actively involved in the global PQC standardization efforts, collaborating with leading academic institutions and industry bodies to shape the future of secure communication. Our solutions are designed to be agile, scalable, and adaptable, ensuring that our clients can seamlessly integrate PQC into their existing infrastructure without disrupting critical operations. We offer a holistic suite of services tailored to address the unique challenges posed by the quantum era:

Quantum Risk Assessment and Strategy Development

Before any migration, a thorough understanding of an organization's exposure to quantum threats is paramount. FikreSekhel conducts comprehensive quantum risk assessments, identifying critical assets, vulnerable cryptographic dependencies, and potential attack vectors. Our experts analyze an organization's current cryptographic inventory, evaluating the strength of existing algorithms against known quantum attacks and assessing the lifespan of sensitive data. Based on this assessment, we develop tailored PQC migration strategies, outlining clear roadmaps, timelines, and resource requirements. This strategic planning ensures a phased and orderly transition, minimizing disruption and maximizing security posture.

PQC Implementation and Integration

The implementation of PQC algorithms requires specialized knowledge and careful integration into diverse IT environments. FikreSekhel provides end-to-end PQC implementation services, from selecting the most appropriate NIST-standardized algorithms to deploying them across an organization's entire digital ecosystem. Our engineers possess extensive experience in integrating PQC into various applications, including secure communication protocols (e.g., TLS/SSL), virtual private networks (VPNs), digital signatures, and data encryption at rest and in transit. We prioritize interoperability and backward compatibility, ensuring that new PQC solutions can coexist with legacy systems during the transition phase.

Quantum-Safe Hardware and Software Development

Recognizing that software-only solutions may not be sufficient to counter all quantum threats, particularly side-channel attacks, FikreSekhel also engages in the development of quantum-safe hardware and software components. This includes designing cryptographic modules that are inherently resistant to physical attacks and developing secure coding practices that minimize information leakage. Our research in this area is focused on creating robust, tamper-resistant solutions that provide an additional layer of security against sophisticated quantum adversaries. We work with clients to embed quantum-safe principles into their product development lifecycle, ensuring that security is built in from the ground up.

Training and Awareness Programs

Successful PQC migration is not just about technology; it's also about people. FikreSekhel offers comprehensive training and awareness programs to educate an organization's workforce about quantum threats and the importance of PQC. These programs are tailored to different audiences, from executive leadership to technical teams, ensuring that everyone understands their role in securing the post-quantum future. We empower organizations with the knowledge and skills necessary to manage their PQC infrastructure effectively and to respond proactively to emerging threats.

Continuous Monitoring and Threat Intelligence

The quantum threat landscape is dynamic and constantly evolving. FikreSekhel provides continuous monitoring and threat intelligence services, keeping our clients informed about the latest advancements in quantum computing, new attack methodologies, and updates to PQC standards. Our experts analyze global quantum research, track the development of quantum computers, and assess the implications for our clients' security posture. This proactive threat intelligence enables organizations to adapt their PQC strategies as needed, ensuring long-term resilience against future quantum challenges. With FikreSekhel, you gain a trusted partner dedicated to safeguarding your digital assets in an increasingly quantum world.

The 'Harvest Now, Decrypt Later' Threat: A Ticking Time Bomb

One of the most insidious aspects of the quantum threat is the concept of 'Harvest Now, Decrypt Later' (HNDL). This refers to the practice where malicious actors, including state-sponsored entities, are currently collecting and storing vast amounts of encrypted data. Their objective is not to decrypt this data today, as current classical computing power makes it infeasible. Instead, they are banking on the future advent of cryptographically relevant quantum computers (CRQCs) that will possess the power to break today's encryption algorithms. Once these CRQCs become available, the stored, encrypted data can then be decrypted, revealing sensitive information that was thought to be secure.

The HNDL threat is particularly concerning for data with a long shelf life. This includes, but is not limited to:

- **Government Secrets:** Classified communications, intelligence data, and military strategies that need to remain confidential for decades.
- **Intellectual Property:** Research and development data, trade secrets, and proprietary algorithms that represent a company's competitive advantage.
- **Personal Health Information (PHI):** Medical records, genetic data, and other sensitive health information that, if exposed, could lead to severe privacy violations and identity theft.
- **Financial Records:** Long-term financial transactions, investment strategies, and banking details.
- **Critical Infrastructure Data:** Information related to the operation and security of power grids, water systems, and transportation networks.

The implications of HNDL are profound. Organizations and governments that fail to transition to post-quantum cryptography (PQC) risk having their most sensitive historical data compromised in the future. This creates a ticking time bomb scenario, where the longer the delay in adopting PQC, the greater the volume of vulnerable data that accumulates. The time window for action is shrinking, not just because CRQCs are approaching, but because the data being harvested today will become decryptable tomorrow.

Mitigating the HNDL threat requires immediate action. It's not enough to simply wait for CRQCs to emerge before implementing PQC. Organizations must identify their long-lived sensitive data, assess its exposure to HNDL, and prioritize its protection with quantum-resistant encryption. This often involves a comprehensive data inventory, classification, and a phased migration strategy. FikreSekhel provides the expertise to help organizations navigate this complex challenge, ensuring that their valuable data remains secure, both today and in the post-quantum future.