SCHOLARLY REVIEW ONLINE

Scholarly Review Online - Winter 2024/2025

Quantum Computing and the Future of Encryption

By Gavin Seiler

AUTHOR BIO

Gavin Seiler is a student at Los Gatos High School with a passion for quantum computing, cryptography, machine learning, and defense. He plans to attend West Point and pursue a career in the military. Gavin is also involved in the corporate development of Munin, a defense startup.

ABSTRACT

Quantum computing is rapidly advancing, and it presents an unprecedented threat to modern encryption. Within the next two decades, quantum computing may lead to a global cybersecurity crisis dubbed Q-day. This is when quantum computing will be capable of breaking the encryption methods underpinning the internet and other digital processes. This scenario threatens individual privacy, global economic stability, and national security infrastructures. The actual timeline for quantum threats is uncertain, but it is urgent that quantum-resistant cryptography is developed and implemented. The paper examines the current state and projected growth of quantum computing capabilities by focusing on metrics including quantum volume, coherence time, and coherence gain. The paper also highlights the period from 2025 to 2030, as significant breakthroughs in quantum computing may occur during that time due to enhanced qubit scaling, error correction, and algorithm efficiency. Looking ahead a decade from now, 2034, the landscape of cryptography will be significantly different. By then, it is highly probable that quantum computers will achieve a quantum volume of around 10^7 qubits, with a low error rate of 10^{-3} or better. This level of quantum computing power makes widely used cryptographic systems, for instance, RSA-1024, vulnerable to disruption. Consequently, there is a narrow window of opportunity to adapt and prepare. This applies to areas such as Public Key Infrastructure (PKI), Post-Quantum Cryptography (PQC), and Quantum Key Distribution (QKD). The paper underscores the importance of a coordinated global effort to develop, standardize, and implement quantum-resistant cryptographic solutions before it is too late.

Keywords: Quantum Key Distribution (QKD), Quantum Cryptography, Secure Communication, Quantum Mechanics, Eavesdropping Detection, Post-Quantum Cryptography (PQC), Encryption Algorithms, Quantum Fourier Transform (QFT), Public Key Infrastructure (PKI), Q-day, Elliptic Curve Cryptography (ECC), Rivest-Shamir-Adleman (RSA)

INTRODUCTION

Cryptography plays a critical role in safeguarding everything from personal communications to financial transactions and infrastructure. There are two main types of cryptography: symmetric and asymmetric. Symmetric encryption, such as the Advanced Encryption Standard (AES), employs a single key for both encryption and decryption. This method is widely used to protect sensitive data, including instant messages and cloud storage (TutorialsPoint, 2019). AES enhances security by utilizing various key sizes, with larger keys adding complexity to potential decryption efforts (CyberNews, 2022). It also employs multiple rounds of encryption, incorporating processes such as substitution, permutation, and key addition to bolster data protection (Precisely, 2022). Currently, AES is considered secure. However, the rise of quantum computing presents a looming threat. Quantum computers, harnessing algorithms like Grover's, could exponentially accelerate the process of searching for encryption keys, weakening AES's effectiveness. As a result, larger key sizes will be necessary to maintain security in the quantum era (Precisely, 2022). In contrast to symmetric encryption methods like AES, asymmetric encryption techniques such as Rivest-Shamir-Adleman (RSA) and Elliptic Curve Cryptography (ECC) use separate public and private keys to secure communications, such as for emails and online banking (1Kosmos, 2023). RSA's security is based on the difficulty of factoring large composite numbers, while ECC relies on the algebraic complexity of elliptic curves over finite fields (CyberNews, 2022). These mathematical problems are currently considered infeasible for classical computers to solve efficiently. However, Shor's algorithm poses a significant threat, as it can find solutions to these problems in polynomial time through rapidly factoring large numbers and computing discrete logarithms. Thus, the security of RSA and ECC become vulnerable (1Kosmos, 2023). To address this quantum threat, researchers are developing post-quantum cryptography (PQC). PQC focuses on creating cryptographic systems that can withstand attacks from both classical and quantum computers (Rambus, n.d.). There are five main types of PQC algorithms: lattice-based, multivariate, hash-based, code based, and isogeny-based cryptography. The National Institute of Standards and Technology (NIST) is currently working to standardize PQC algorithms, recognizing the urgency of preparing for quantum computing's impact on security. While the timeline for practical quantum computing remains uncertain, the accelerating pace of quantum research makes it essential to develop cryptographic systems capable of withstanding quantum threats (Btq.com, 2023).

FUNDAMENTALS OF QUANTUM COMPUTING

Quantum computing leverages quantum mechanics to solve complex problems that are intractable for classical computers. Instead of using bits as the basic unit of information and processing data sequentially through logic gates, quantum computers use quantum bits (qubits) which can exist in multiple states simultaneously due to superposition (IBM, 2024). Qubits enable quantum computers to perform parallel computations, vastly increasing their processing power compared to classical bits, which can only represent one state at a time. Qubits enable quantum computers to process data in parallel, which significantly enhances their computational power (IBM, 2024). Classical bits can only be binary (0 or 1). But qubits can represent both states at once. Therefore, quantum computers can test multiple solutions simultaneously. Quantum computers also leverage interference and entanglement. Quantum interference occurs when the probabilities of different quantum states combine, amplifying the chances of the correct solution while canceling out the wrong ones. This is similar to how waves in water can either reinforce each other or cancel each other out depending on their alignment (Trend Micro, n.d.). Interference in quantum computing helps isolate the correct solution by increasing its likelihood while reducing the likelihood of incorrect solutions, much like constructive interference in waves. In more intuitive terms, imagine trying to find a way through a maze. Quantum interference helps the quantum

computer narrow down the path to the correct solution by eliminating paths that lead to dead ends. Likewise, quantum entanglement connects particles, no matter how far apart they are, allowing them to amplify the probability of correct solutions while suppressing incorrect ones. Entanglement means that the state of one particle is directly related to the state of another, even if they are separated by vast distances. This allows quantum computers to work on multiple aspects of a problem simultaneously, coordinating results to achieve the correct solution faster (Trend Micro, n.d.). Overall, these quantum mechanical effects work together to enable quantum computers to solve incredibly hard problems.

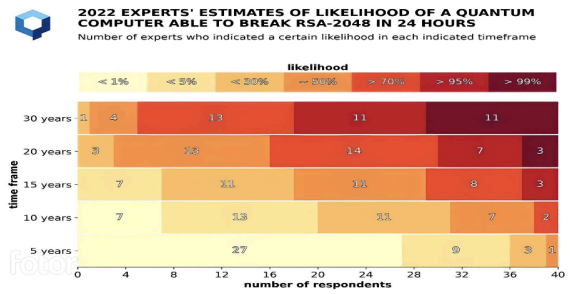
KEY QUANTUM ALGORITHMS (SHOR'S AND GROVER'S)

Quantum computing introduces two notably powerful algorithms that impact cryptographic security: Shor's and Grover's. Shor's algorithm, developed by Peter Shor in 1994, leverages the Quantum Fourier Transform (QFT) to identify periodic structures within quantum states, enabling the factoring of large integers (Shor, 1997). In simpler terms, QFT allows the quantum computer to extract hidden patterns in numbers, which classical computers would struggle to identify, enabling faster factorization of large primes. The algorithm also utilizes Quantum Phase Estimation (QPE) to extract phase information from quantum states, which assists the factorization process (Shor, 1997). QPE helps the quantum computer determine the phase or periodicity of a quantum state, a crucial step for Shor's algorithm to efficiently find the prime factors of a large number. A key quantum operation in Shor's algorithm is modular exponentiation, allowing the algorithm to simultaneously evaluate the function for multiple values of variable x. This means that the quantum computer can test many possible solutions at once, drastically reducing the time required to find the correct solution. Additionally, Shor's algorithm deploys quantum parallelism to achieve its exponential speedup over classical methods (Shor, 1997). Quantum parallelism allows the algorithm to run many computations at the same time, using superposition to explore multiple possibilities in one go. Likewise, Grover's algorithm leverages quantum superposition to create a uniform distribution of all possible states representing an entire search space simultaneously (CNOT.io, n.d.). In essence, quantum superposition allows Grover's algorithm to evaluate all possible solutions in parallel, significantly speeding up the search process. It employs a quantum oracle to mark the target solution state(s) within this superposition and applies a phase shift to distinguish the desired outcome (CNOT.io, n.d.). The quantum oracle is like a pointer that identifies the correct solution, and the phase shift makes that solution stand out from the others, allowing it to be more easily found. However, the crux of Grover's algorithm is the Grover diffusion operator, which performs amplitude amplification by inverting the state vector about the mean (Towards Data Science, 2021). This step increases the probability of finding the correct solution by making its amplitude stronger compared to the incorrect ones. Consequently, the probability of measuring the correct solution is increased (Towards Data Science, 2021). Iterative application of the oracle and diffusion operator achieves a quadratic speedup over classical search methods, making it very powerful (Towards Data Science, 2021). This quadratic speedup means that Grover's algorithm can find the correct solution in about the square root of the time it would take a classical algorithm. Both Shor's and Grover's algorithms are enabled by quantum gates and circuits (CNOT.io, n.d.). Unlike classical computers, which use logic gates (AND, NOT, OR, XOR), quantum computers use unitary gates to manipulate qubits (IBM, 2024). Unitary gates are different from classical gates because they perform operations that can be reversed without losing information, making quantum computations more flexible and powerful. These gates can perform reversible operations, a property not shared by classical gates (IBM, 2024). Quantum circuits leverage these gates to explore multiple computational paths simultaneously (quantum parallelism), which enables much more processing power (IBM, 2024).

QUANTUM THREATS TO CLASSICAL ENCRYPTION

The combination of Shor's and Grover's algorithms presents a formidable threat to current asymmetric and symmetric cryptography systems.

Starting with asymmetric systems, Shor's algorithm poses a significant threat to ECC (Kudelski Security Research, 2021). Microsoft Research estimates that only about 2500 qubits are needed to crack a standard 256-bit ECC key, compared to around 4000 qubits for 2048-bit RSA (Btq.com, 2023). This vulnerability stems from ECC's shorter key lengths (Wikipedia, 2019). ECC's smaller key sizes are efficient for classical computers, but they leave the system highly vulnerable to quantum attacks, where the smaller the key, the easier it is to break. This is advantageous in classical computing but becomes a liability in the quantum context (Shor, 1997). RSA is also vulnerable, but it has a longer timeline before practical attacks become feasible, as the number of qubits required to break that cryptosystem is larger. However, the number of qubits could be reduced to around 2000 by 2030 (Btq.com, 2023).



Likelihood to Break RSA-2048 in 24 Hours (Reproduced from Global Risk Institute, 2024).

Experts surveyed in 2022 believe a quantum computer could break RSA-2048 encryption within the next 10-20 years. The darker the color on the chart, the more experts believe it's likely. This suggests a growing consensus that quantum computers could pose a significant threat to current encryption methods.

Moreover, Grover's algorithm reduces the effective strength of symmetric encryption by roughly half. For example, AES-256 could be reduced to the security level of AES-128, which makes it more vulnerable to brute-force attacks. For instance, AES-256 could be reduced to the security level of AES-128, making it exposed to brute-force attacks by quantum computers. Meanwhile, hash functions, used for digital signatures and data integrity verification, are also susceptible, with Grover's algorithm potentially finding two different inputs that produce the same output hash value twice as fast as classical methods (SolveForce, 2024). This could allow attackers to generate collisions (two inputs that produce the same hash) at a faster rate, undermining the integrity of digital signatures and blockchain technologies. This threatens the security of widely used hash functions like SHA-256, which underpins digital signatures and blockchain technologies (Trend Micro, 2024). The potential impact on hash functions might materialize sooner than the threat to symmetric encryption, as it requires fewer qubits (Trend Micro, 2024).

HARVEST NOW, DECRYPT LATER (HDNL) THREAT

Quantum computers could also lead to a HDNL scenario, where malicious actors store encrypted data now to decrypt it once quantum computers become available. In this process, they can capture, and store encrypted network traffic or data at rest, along with associated public keys and digital signatures (CB Insights Research, 2018). By saving encrypted data now, attackers can exploit future quantum advancements to decrypt this data, leading to significant risks if sensitive data is stored improperly. Then, they wait for powerful quantum computers to become available (years later) (CB Insights Research, 2018). Once quantum systems become feasible, attackers could use Shor's or Grover's algorithm to break the cryptographic systems protecting this data. Using these quantum systems, attackers could run Shor's algorithm or Grover's algorithm to break the underlying cryptographic primitives and decrypt the stored data. This strategy poses an immense risk, particularly for sensitive information that retains its value over time, such as government data, intellectual property, and healthcare records. To mitigate this threat, larger key sizes are needed for current encryption methods (see Fig. 2) and a transition to

post-quantum cryptography (PQC) algorithms will be requisite.

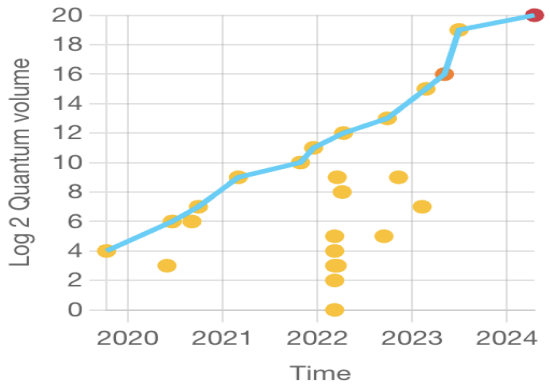
Cryptographic Algorithm	Type	Purpose	Impact from large-scale quantum computer
AES	Symmetric key	Encryption	Larger key sizes needed
SHA-2, SHA-3	----------	Hash functions	Larger output needed
RSA	Public key	Signatures, key establishment	No longer secure
ECDSA, ECDH (Elliptic Curve Cryptography)	Public key	Signatures, key exchange	No longer secure
DSA (Finite Field Cryptography)	Public key	Signatures, key exchange	No longer secure

Recommendations for PKI Key Lengths and Validity Periods with Configuration Manager (Reproduced from the Microsoft Tech Community, 2018).

The table shows that quantum computers will break current encryption methods. RSA, ECDSA, and ECDH will become insecure. AES and SHA-2/3 will need larger keys and outputs to stay secure.

CURRENT STATE OF QUANTUM COMPUTING

Quantum Volume

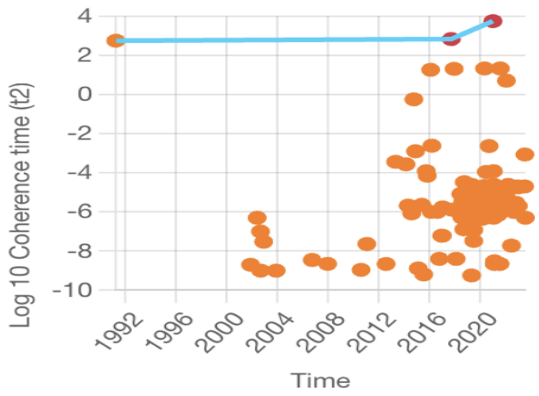


Time vs. Log_2 Quantum Volume (Reproduced from Metriq, 2024, Community-driven Quantum Benchmarks).

The blue line shows the increase in quantum volume over time. The different colored points represent data from different sources or experiments. This data suggests that quantum computing technology is rapidly advancing.

Quantum volume gauges the overall performance and reliability of quantum computers (Forbes, 2019). The metric is calculated by running increasingly complex random quantum circuits and determining the largest square circuit that can be reliably executed (Forbes, 2019). The process involves measuring the quantum computer's ability to produce expected outputs and ultimately expressing the result as two raised to the power of the number of qubits in the largest successful circuit (Honeywell, 2020). The continuing increase (see Fig. 3) in quantum volume not only implies an accelerated timeline to Q-day, but also highlights the rapid pace of quantum computing development compared to classical computing's historical trajectory. This pace of advancement is largely due to the exponential nature of quantum systems. Unlike the linear scaling of classical computing, which followed Moore's Law for decades, quantum volume is increasing exponentially. For instance, a quantum computer with just 300 qubits can represent more states than there are atoms in the observable universe (CB Insights Research, 2018). This means that small increases in qubit count can lead to significant leaps in computational capability, enabling quantum computers to perform tasks that are impossible for classical supercomputers.

Coherence Time

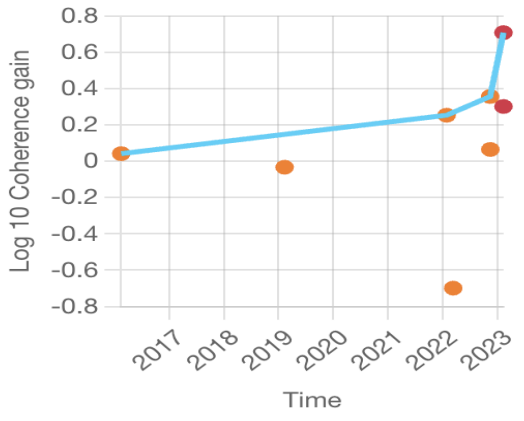


Time vs. Log_{10} Coherence Time (t_2) in Seconds (Reproduced from Metriq, 2024, Community-driven Quantum Benchmarks).

The blue line shows a plateau in coherence time from 1992 to 2016. The orange points represent data from different experiments, showing a decrease in coherence time over time.

Coherence time measures how long a qubit can maintain its quantum state (The Quantum Insider, 2022). As coherence time improves, qubits are becoming better isolated from environmental noise, resulting in reduced error rates. The achievement of a four-second coherence time (see Fig. 4) suggests that quantum computers are rapidly approaching the threshold necessary for executing highly complex computations, as a longer coherence window allows for longer sequences of quantum operations to be performed before decoherence occurs (IonQ, n.d.). Since 2020, there has been a decrease in coherence times (see Fig. 4). A key driver of this trend could be the use of materials that are more susceptible to decoherence. For example, superconducting qubits are becoming more prevalent in quantum computers due to their ability to stay in their quantum state for a longer period. However, these qubits are very sensitive to electromagnetic interference, potentially causing them to collapse into a definite state prematurely, leading to shorter coherence times.

Coherence Gain



Time vs. Log_{10} Coherence Gain (Reproduced from Metriq, 2024, Community-driven Quantum Benchmarks).

The blue line shows a slight increase in coherence gain over time. The orange and red points represent data from different experiments. The data suggests that coherence gain is slowly improving.

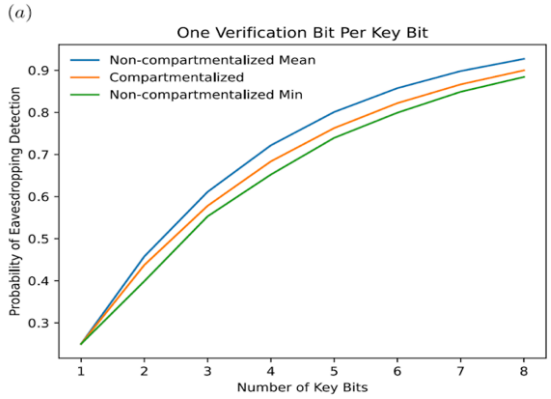
Coherence gain shows how effectively a system can protect quantum information from errors (Riverlane, n.d.). A higher coherence gain indicates that the quantum computer is becoming more capable of performing complex calculations without losing information to environmental disturbances (Riverlane, n.d.). This is crucial for enhancing the performance and reliability of quantum computers, as it directly impacts their ability to maintain quantum states over longer periods (Google, 2022). The improvement from roughly 0.4 to 0.7 Log 10 (see Fig. 5) indicates that quantum systems are quickly becoming more robust against errors and that quantum computers can perform more complex operations with higher fidelity. Consequently, as error rates decrease, the ability to implement effective quantum error correction improves. Thus, more precise qubit manipulations can be achieved, enabling the execution of more sophisticated algorithms.

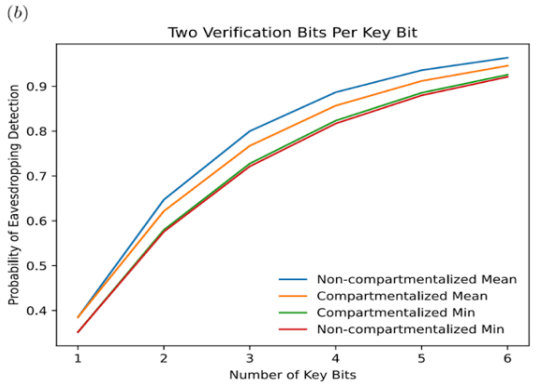
QUANTUM KEY DISTRIBUTION (QKD)

Quantum Key Distribution (QKD) is a secure communication method that employs quantum mechanics to produce a shared secret key for encrypting and decrypting messages (QNu Labs, 2024). A core feature of QKD is its ability to detect eavesdropping. When detecting an eavesdropper over many key qubits, QKD uses quantum superpositions or quantum entanglement to transmit information (QNu Labs, 2024). If an eavesdropper tries to intercept and measure these qubits, the disturbance caused by the measurement can be statistically detected through the quantum bit error rate (QNu Labs, 2024). This rate is found by comparing subsets of the transmitted qubits between the communicating parties to check for anomalies that would indicate eavesdropping (Toshiba Quantum Technology, n.d.). By analyzing error patterns, it is possible to estimate the amount of information potentially leaked and the type of attack being employed. However, QKD's primary goal is not to gather intelligence on the attacker but to ensure the integrity and confidentiality of the key distribution process

(Toshiba Quantum Technology, n.d.). QKD's strength lies in its ability to create a communication channel where any attempt at eavesdropping becomes detectable, allowing for immediate countermeasures (QNu Labs, 2024).

Quantum Key Distribution (QKD) is a secure communication method that employs quantum mechanics to produce a shared secret key for encrypting and decrypting messages (QNu Labs, 2024). A core feature of QKD is its ability to detect eavesdropping. When detecting an eavesdropper over many key qubits, QKD uses quantum superpositions or quantum entanglement to transmit information (QNu Labs, 2024). If an eavesdropper tries to intercept and measure these qubits, the disturbance caused by the measurement can be statistically detected through the quantum bit error rate (QNu Labs, 2024). This rate is found by comparing subsets of the transmitted qubits between the communicating parties to check for anomalies that would indicate eavesdropping (Toshiba Quantum Technology, n.d.). By analyzing error patterns, it is possible to estimate the amount of information potentially leaked and the type of attack being employed. However, QKD's primary goal is not to gather intelligence on the attacker but to ensure the integrity and confidentiality of the key distribution process (Toshiba Quantum Technology, n.d.). QKD's strength lies in its ability to create a communication channel where any attempt at eavesdropping becomes detectable, allowing for immediate countermeasures (QNu Labs, 2024).





The probabilities of detecting an eavesdropper over an increasing number of key qubits with (a) one and (b) two verification qubits per key qubit. (Reproduced from "Quantum advantage with noisy intermediate-scale quantum devices," by B. Bauer, S. Bravyi, M. Motta, and E. Yen-Yu Lin, 2024, *arXiv*).

As the number of key bits in a QKD system increases, the probability of detecting an eavesdropper also rises (see Fig. 6). Thus, enhanced security requires larger key sizes, and a greater number of key bits provides more opportunities to identify anomalies caused by an eavesdropper's measurements, which disturb the quantum states of the qubits (arXiv, 2024). The approach to analyzing key bits can be either compartmentalized or non-compartmentalized. In a compartmentalized approach, key bits are divided into segments, allowing for localized detection of vulnerabilities (arXiv, 2024). In contrast, a non-compartmentalized approach assesses the entire dataset (arXiv, 2024). Hence, employing sufficiently large key sizes in QKD systems, whether compartmentalized or not, is essential for maintaining high levels of security and mitigating unauthorized access. QKD systems are already commercially available, but widespread adoption faces challenges such as concerns over side-channel attacks, the need for new quantum-enabled infrastructure, and the complexity of QKD protocols (NSA, n.d.).

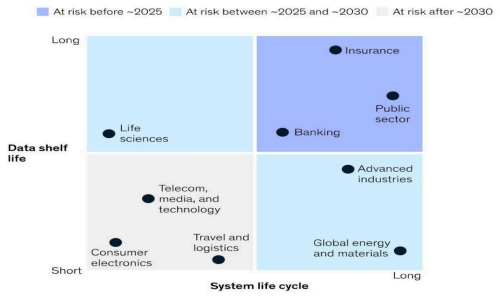
The probabilities of detecting an eavesdropper over an increasing number of key qubits with (a) one and (b) two verification qubits per key qubit. (Reproduced from "Quantum advantage with noisy intermediate-scale quantum devices," by B. Bauer, S. Bravyi, M. Motta, and E. Yen-Yu Lin, 2024, *arXiv*).

As the number of key bits in a QKD system increases, the probability of detecting an eavesdropper also rises (see Fig. 6). Thus, enhanced security requires larger key sizes, and a greater number of key bits provides more opportunities to identify anomalies caused by an eavesdropper's measurements, which disturb the quantum states of the qubits (arXiv, 2024). The approach to analyzing key bits can be either compartmentalized or non-compartmentalized. In a compartmentalized approach, key bits are divided into segments, allowing for localized detection of vulnerabilities (arXiv, 2024). In contrast, a non-compartmentalized approach assesses the entire dataset (arXiv, 2024). Hence, employing sufficiently large key sizes in QKD systems, whether compartmentalized or not, is essential for maintaining high levels of security and mitigating unauthorized access. QKD systems are already commercially available, but widespread adoption faces challenges such as concerns over side-channel attacks, the need for new quantum-enabled infrastructure, and the complexity of QKD protocols (NSA, n.d.).

PREPAREDNESS AND GLOBAL IMPLICATIONS

US Government Initiatives

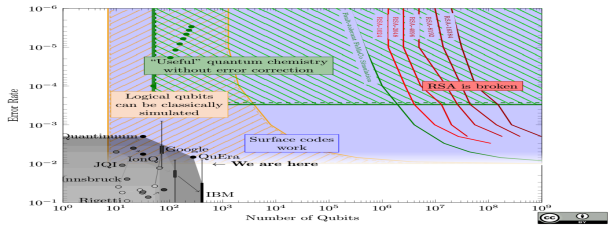
NIST is playing a significant role in preparing for the future of cybersecurity by standardizing post-quantum cryptographic algorithms (The Quantum Insider, 2024, "White House Advisor Says NIST to Release Post-Quantum Cryptographic Algorithms in Coming Weeks"). All industries will eventually be at risk to quantum-powered attacks (see Fig. 7). As a result, the agency's aim is to solicit submissions from cryptographic experts worldwide and conduct multiple rounds of evaluation to identify robust quantum-resistant algorithms (NIST, 2023, "NIST to Standardize Encryption Algorithms That Can Resist Attack by Quantum Computers"). Then, NIST will standardize several of the algorithms to ensure they meet stringent criteria such as forward secrecy and resistance to side-channel attacks (NIST, 2024, "NIST Releases First 3 Finalized Post-Quantum Encryption Standards").



Risk of quantum-powered attack by industry. The graph shows the risk of different industries to quantum computing attacks, based on their data shelf life and system life cycle. Industries with long data shelf lives and long system life cycles, such as insurance and the public sector, are at the highest risk. Industries with short data shelf lives and short system life cycles, such as consumer electronics, are at the lowest risk. (Reproduced from "When—and how—to prepare for post-quantum cryptography," by L. Baumgärtner, B. Klein, N. Mohr, A. Pflanzer, and H. Soller, 2022, McKinsey & Company).

Different industries face varying timelines for quantum vulnerability, with financial services and government sectors likely to be impacted first, followed by energy and life sciences (see Fig. 7). NIST is working to transition high-priority systems to quantum-resistant cryptography by 2035, emphasizing the importance of early preparation to protect data that needs to remain secure for many years (NIST, 2024).

Estimated Timeline for Quantum Computing Threats



Timeline until RSA is broken. The graph shows the progress of quantum computing over time. The x-axis represents the number of qubits, and the y-axis represents the error rate. The green line shows the progress of quantum computing. The red line represents the threshold for breaking RSA encryption. The names in the grey box represent different quantum computing research groups and companies. Currently, quantum computers are not powerful enough to break RSA encryption. However, if quantum computers continue to improve at their current rate, they may eventually be able to break RSA encryption. (Reproduced from Jaques, S., 2023, Quantum Landscape 2023. Appspot.com).

Q-Day remains a future event, but in 2024, quantum computing has made significant progress. Systems are achieving around 1,000 qubits and error rates slightly above 10^{-2} (see Fig. 8). This is still far from the capabilities needed to break current encryption standards, and projections from IBM researchers suggest that substantial engineering problems, including breaking widely used cryptographic systems like RSA, may not be solvable until around 2033 (arXiv, 2023). For instance, compromising RSA-1024 would require at least 10^7 qubits and an error rate of 10^{-3} or better (see Fig. 8). This gap between current capabilities for breaking cryptographic systems like RSA indicates that while the quantum threat may not be immediate (within 5-10 years), it is becoming increasingly tangible. The period from 2025 to 2030 will likely see accelerated advancements in qubit scaling, error correction, and algorithm efficiency due to increased investment in quantum research, the development of better error correction techniques, and the diversification of qubit technologies. Q-Day will likely occur around 2035-2044, with RSA-1024 broken first, followed by RSA-2048 and RSA-4096, leading to widespread adoption of PQC (McKinsey & Company, 2022).

CONCLUSION

Quantum computing is poised to disrupt current encryption methods within the next 20 years, necessitating urgent preparation. This technological advancement leverages principles like superposition and entanglement, offering computational power far beyond that of classical computers. Key algorithms such as Shor's and Grover's threaten to break traditional cryptographic systems, potentially compromising the foundation to secure communications. Although quantum computers capable of breaking current encryption do not yet exist, rapid progress in quantum volume, coherence time, and coherence gain underscores the urgency of developing PQC. Initiatives like NIST's efforts to standardize quantum-resistant algorithms are crucial for establishing secure encryption in the quantum era. The transition to PQC presents significant challenges, including substantial investments in infrastructure upgrades and specialized training to integrate PQC algorithms with existing systems (Broadcom, 2024). Regardless of the exact timeline for quantum computing's arrival, preparations must begin now to protect information security systems (NIST, 2016). This research highlights the necessity of lowering barriers to entry for quantum-safe transitions by developing accessible, cost-effective tools that raise awareness and facilitate the adoption of secure technologies. By proactively addressing these challenges, cryptography can remain resilient and capable of withstanding the quantum revolution.

REFERENCES

20.3 Emerging Technologies >> Quantum Computing. (2023, October 5). SolveForce Fiber Internet, Cloud Computing & Telecommunications. https://solveforce.com/20-3-emerging-technologies-quantum-computing/

Diving Deep Into Quantum Computing: Computing With Quantum Mechanics - Security News. (n.d.). Trend Micro. https://www.trendmicro.com/vinfo/us/security/news/security-technology/diving-deep-into-quant

um-computing-computing-with-quantum-mechanics

Figure 3: Likelihood to Break RSA-2048 in 24 Hours (Reproduced from...). (2024). ResearchGate. https://www.researchgate.net/figure/Likelihood-to-Break-RSA-2048-in-24-Hours-Reproduced-from-Global-Risk-Institute-4_fig1_382363516

Franklin, R. (2022, November 14). AES vs. RSA Encryption: What Are the Differences? Precisely. https://www.precisely.com/blog/data-security/aes-vs-rsa-encryption-differences

Gagliardoni, T. (2021, August 24). Quantum Attack Resource Estimate: Using Shor's Algorithm to Break RSA vs DH/DSA VS ECC. Kudelski Security Research. https://research.kudelskisecurity.com/2021/08/24/quantum-attack-resource-estimate-using-shors-algorithm-to-break-rsa-vs-dh-dsa-vs-ecc/

Grover's Algorithm | CNOT. (n.d.). Cnot.io. https://cnot.io/quantum_algorithms/grover/grovers_algorithm.html

How Far Away Is The Quantum Threat? (2023). BTQ. https://www.btq.com/blog/how-far-away-is-the-quantum-threat?ref=btq-publication.ghost.io

How to Prepare for Post-Quantum Cryptography | McKinsey. (n.d.). McKinsey & Company. https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/when-and-how-to-prepare-for-post-quantum-cryptography

Recommendations for PKI Key Lengths and Validity Periods with Configuration Manager. (2018, October 16). Microsoft Tech Community. https://techcommunity.microsoft.com/t5/configuration-manager-archive/recommendations-for-pki-key-lengths-and-validity-periods-with/ba-p/272758

Jaques, S. (2023). Quantum Landscape 2023. Appspot.com. https://sam-jaques.appspot.com/quantum_landscape_2023

Maureen. (2023, April 25). What Is AES Encryption? The Complete Guide. 1Kosmos. https://www.1kosmos.com/authentication/aes-encryption/

Metriq - Community-driven Quantum Benchmarks. (2024). Metriq. https://metriq.info/

Nicholas, & Linvill, K. (2024). Increasing Interference Detection in Quantum Cryptography Using the Quantum Fourier Transform. *arXiv.org*. https://arxiv.org/abs/2404.12507

Nikhade, A. (2021, October 6). Grover's Search Algorithm | Simplified. *Medium*. https://towardsdatascience.com/grovers-search-algorithm-simplified-4d4266bae29e

NIST. (2023). NIST to Standardize Encryption Algorithms That Can Resist Attack by Quantum Computers. *NIST*. https://www.nist.gov/news-events/news/2023/08/nist-standardize-encryption-algorithms-can-resist-attack-quantum-computers

NIST. (2024, August 13). NIST Releases First 3 Finalized Post-Quantum Encryption Standards | NIST. *NIST*. https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards

NSA. (n.d.). National Security Agency/Central Security Service > Cybersecurity > Quantum Key Distribution (QKD) and Quantum Cryptography QC. *NSA*. https://www.nsa.gov/Cybersecurity/Quantum-Key-Distribution-QKD-and-Quantum-Cryptography-QC/

Pichai, S. (2023, February 22). Our Progress Toward Quantum Error Correction. *Google*. https://blog.google/inside-google/message-ceo/our-progress-toward-quantum-error-correction/

Post-Quantum Cryptography (PQC): New Algorithms for a New Era. (n.d.). Rambus. https://www.rambus.com/blogs/post-quantum-cryptography-pqc-new-algorithms-for-a-new-era/

Post-Quantum Cryptography Initiative | CISA. (n.d.). Cybersecurity and Infrastructure Security Agency. https://www.cisa.gov/quantum

Post-Quantum Cryptography: Quantum Computing Attacks on Classical Cryptography | Trend Micro (US). (2024). Trend Micro. https://www.trendmicro.com/vinfo/us/security/news/security-technology/post-quantum-cryptography-quantum-computing-attacks-on-classical-cryptography

QNu Labs Guide: Quantum Key Distribution (QKD) and How It Works? (2024). QNu Labs. https://www.qnulabs.com/guides/quantum-key-distribution-qkd-and-how-it-works

Quantum Computing 101: Introduction, Evaluation, and Applications. (n.d.). IonQ. https://ionq.com/resources/quantum-computing-101-introduction-evaluation-applications

Quantum Key Distribution - What Is QKD? How Does It Work? (n.d.). Toshiba Quantum Technology. https://www.toshiba.eu/quantum/products/quantum-key-distribution/

Quantum Volume: The Power of Quantum Computers. (2020). Honeywell. https://www.honeywell.com/us/en/news/2020/03/quantum-volume-the-power-of-quantum-computers

Rimkiene, R. (2022, August 29). What is AES Encryption and How Does It Work? *CyberNews*. https://cybernews.com/resources/what-is-aes-encryption/

Riverlane. (n.d.). Quantum Error Correction: The Grand Challenge. Riverlane. https://www.riverlane.com/quantum-error-correction

Schneider, J., & Smalley, I. (2023, December 1). What Is Quantum Cryptography? *IBM*. https://www.ibm.com/topics/quantum-cryptography

Schneider, J., & Smalley, I. (2024, August 5). What Is Quantum Computing? *IBM*. https://www.ibm.com/topics/quantum-computing

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

Smith-Goodson, P. (2019, November 24). Quantum Volume: A Yardstick to Measure the Performance of Quantum Computers. *Forbes*. https://www.forbes.com/sites/moorinsights/2019/11/23/quantum-volume-a-yardstick-to-measure-the-power-of-quantum-computers/

Swayne, M. (2022, May 20). Atom Computing Researchers Keep Qubits in Coherence for Record Time. *The Quantum Insider*. https://thequantuminsider.com/2022/05/20/atom-computing-researchers-keep-qubits-in-coherence-for-record-time/

Tutorialspoint.com. (2019). Advanced Encryption Standard. *Tutorialspoint*. https://www.tutorialspoint.com/cryptography/advanced_encryption_standard.htm

Wikipedia Contributors. (2019, November 18). Elliptic-Curve Cryptography. *Wikipedia; Wikimedia Foundation*. https://en.wikipedia.org/wiki/Elliptic-curve_cryptography