

# Understanding Quantum and Classical Computing Integration

A Look at RSA Encryption and  
Future Cryptography

# Introduction

- Quantum and classical computing are powerful technologies.
  - Quantum computing uses principles of quantum mechanics, while classical computing is based on traditional binary processing.
- We'll explore their combination and impact on security.
  - By understanding both computing types, we can assess their combined potential in enhancing and challenging current security protocols.
- Focus on RSA encryption and future-safe cryptography.
  - RSA is a widely used encryption method that could be vulnerable to quantum attacks, necessitating new cryptographic methods.



# Basics of Classical Computing

**Classical computers use binary bits (0s and 1s).**

- Each bit is a fundamental unit of information, existing in a state of either 0 or 1.

**Perform step-by-step calculations.**

- Classical computers process information sequentially, following specific instructions.

**Widely used for encryption and data security.**

- Algorithms like RSA and AES are implemented on classical computers to protect data.



# Basics of Quantum Computing

**Quantum bits (qubits) can be in many states at once.**

- Unlike classical bits, qubits can represent 0 and 1 simultaneously due to superposition.

**Quantum computers use this to solve complex problems quickly.**

- This ability allows quantum computers to perform multiple calculations at once, exponentially speeding up problem-solving.

**Key idea: quantum superposition and entanglement.**

- Superposition allows qubits to be in multiple states, while entanglement links qubits such that the state of one instantly influences another.

# What is RSA Encryption?



**RSA encrypts data to keep it secure.**

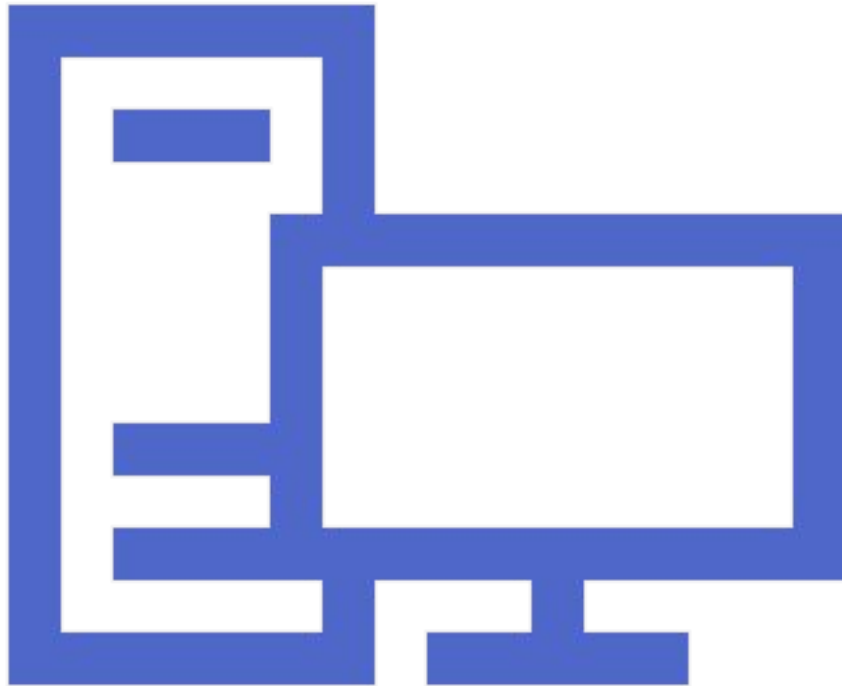
- RSA (Rivest-Shamir-Adleman) is a cryptographic algorithm used to secure sensitive data, particularly in internet communications.

**Relies on the difficulty of factoring large numbers.**

- RSA security is based on the mathematical challenge of decomposing a large number into its prime factors.

**Widely used for internet security.**

- RSA is a cornerstone of secure communications, used in SSL/TLS for secure web browsing, email encryption, and digital signatures.



# Shor's Algorithm

A quantum method to break RSA by factoring large numbers.

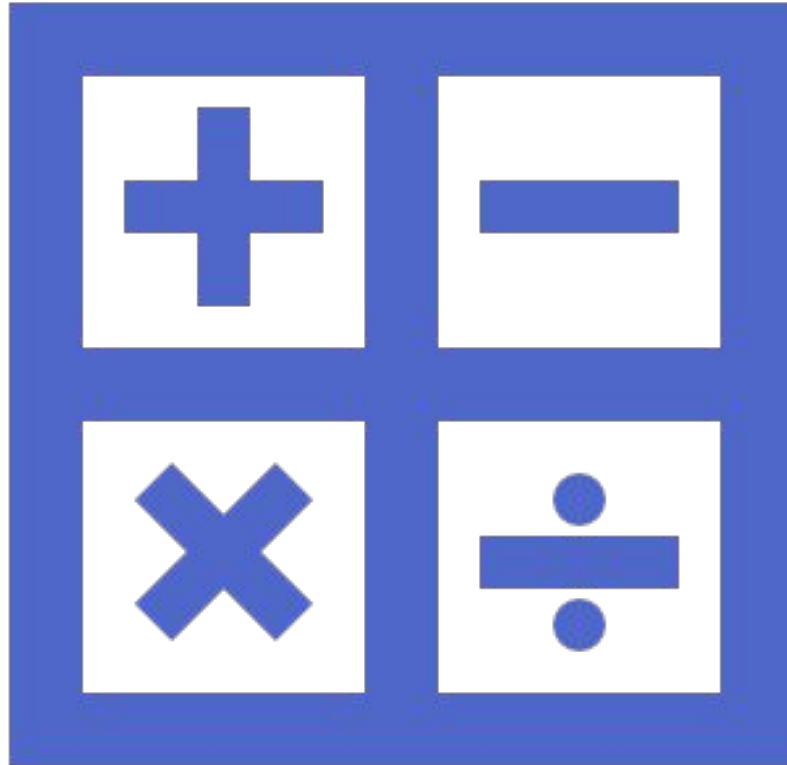
- Shor's algorithm leverages quantum computing to efficiently factor large integers, a task that is infeasible for classical computers.
- Uses quantum properties to solve problems faster than classical methods.
- Utilizes quantum parallelism and entanglement to significantly reduce the time needed to factorize.
- Threatens current encryption methods. If large-scale quantum computers become available, RSA encryption could be broken quickly, compromising data security.





# Why RSA is Vulnerable

- Quantum computers could solve RSA problems quickly.
- Shor's algorithm, running on a sufficiently powerful quantum computer, can factor large integers exponentially faster than the best-known classical algorithms.
- Current encryption relies on classical difficulty.
- Need for new, secure methods as quantum tech advances.
- As quantum computing technology advances, new cryptographic methods that can withstand quantum attacks are necessary to maintain data security.



# Combining Quantum and Classical Computing

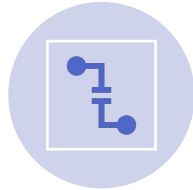
- Use quantum speed for tough problems.
- Quantum computers can handle complex calculations at unprecedented speeds.
- Classical methods to analyze and interpret results.
- Classical computers can process and interpret data generated by quantum computations.
- Stronger together for breaking encryption



# Singular Value Decomposition (SVD) Basics



SVD breaks data into simpler parts.



Singular Value Decomposition is a mathematical technique used to decompose a matrix into its constituent components.



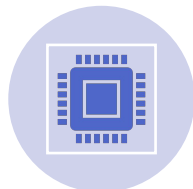
Helps find patterns in encrypted information.



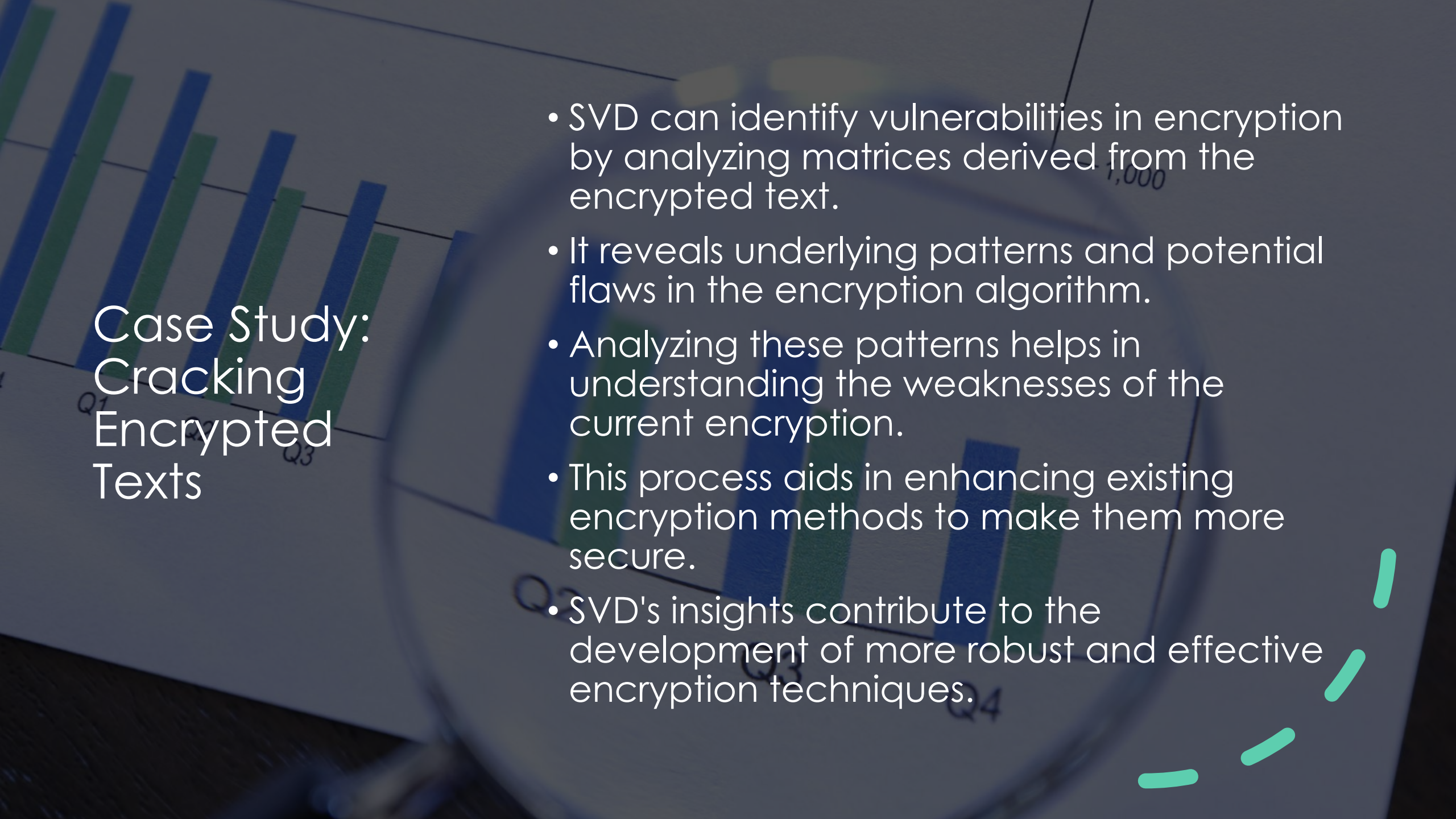
By breaking down data, SVD can identify underlying patterns that may not be obvious.



Useful in classical cryptanalysis.




SVD is a powerful tool in analyzing and improving cryptographic systems by finding weaknesses in encryption algorithms.



## Case Study: Cracking Encrypted Texts

- SVD can identify vulnerabilities in encryption by analyzing matrices derived from the encrypted text.
- It reveals underlying patterns and potential flaws in the encryption algorithm.
- Analyzing these patterns helps in understanding the weaknesses of the current encryption.
- This process aids in enhancing existing encryption methods to make them more secure.
- SVD's insights contribute to the development of more robust and effective encryption techniques.



- 
- Some encryption keys are inherently weaker than others, compromising security.
  - SVD can be used to identify these weak encryption keys by analyzing the encryption data.
  - By detecting weak keys, SVD ensures that only strong, secure keys are utilized.



## Identifying Weak Keys



# Post-Quantum Cryptography

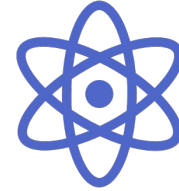
- Future encryption algorithms must be designed to resist attacks from quantum computers.
- Ongoing research focuses on developing new cryptographic methods to ensure security.
- These new methods aim to protect data against the advanced capabilities of quantum computing.
- Ensuring robust data protection in the quantum era is a critical objective for cybersecurity.



# Creating Quantum-Resistant Encryption



Develop encryption methods that are resistant to attacks from quantum computers



Combine the strengths of classical and quantum computing to enhance security.



Ensure that data security is robust and future-proof against quantum advancements.



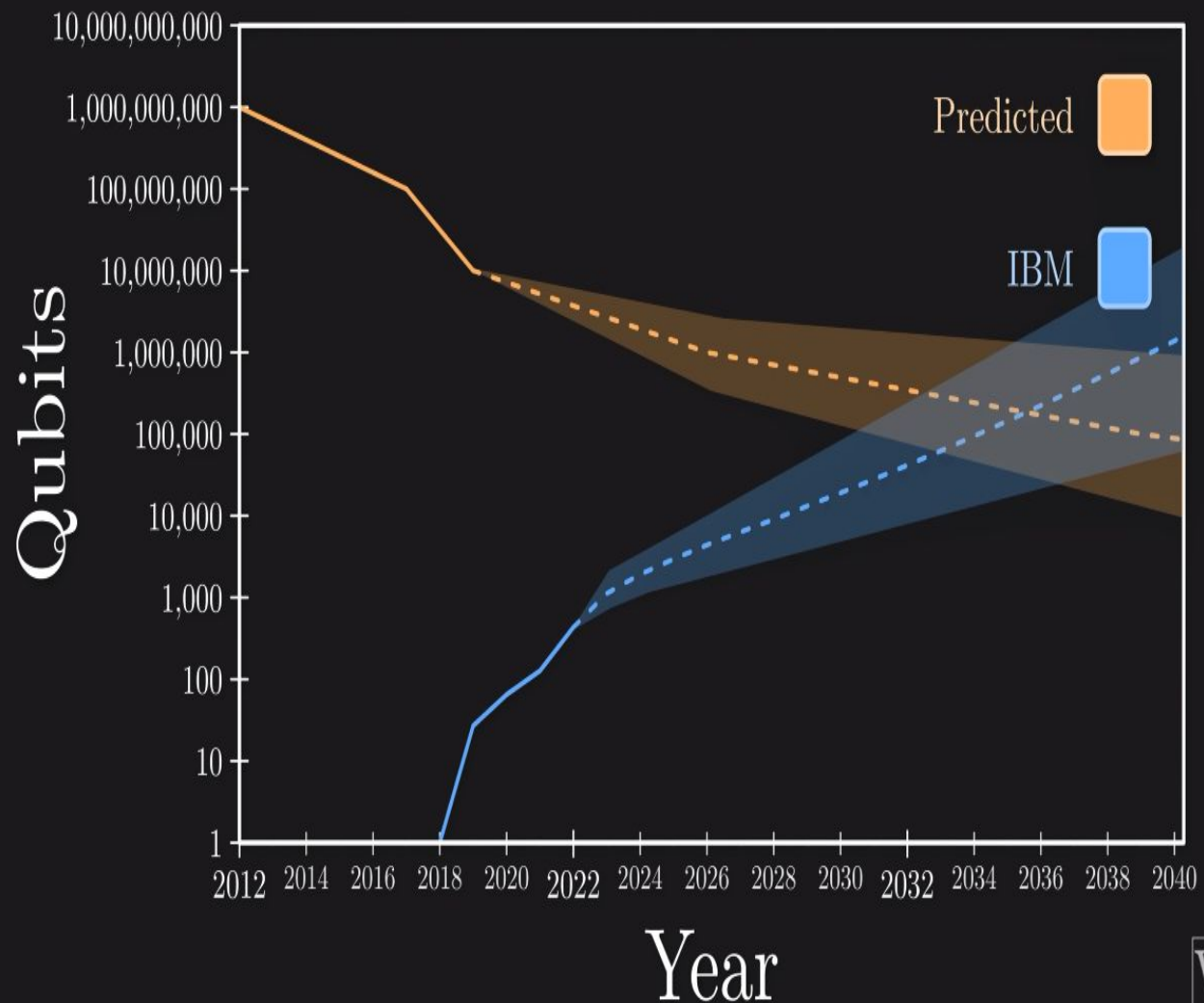
Aim to protect sensitive information from potential quantum-based threats.



## Collaborative Efforts

- Quantum and classical computing experts are working together to enhance encryption methods.
- Sharing knowledge between these fields leads to improved security solutions.
- Collaborative efforts result in the development of more robust encryption techniques.
- Joint initiatives between experts strengthen overall data protection.





## IBM's Research on Quantum Computing and its Potential to Break Encryption

- **IBM's Quantum Computing Research and its Impact on Encryption:**
  - IBM is a leader in quantum computing research and development.
  - They have made significant strides in developing quantum processors and quantum computing poses a threat to current encryption methods, including RSA and other public-key cryptographic algorithms.
  - IBM's quantum computers, like those built on their IBM Q network, are capable of executing algorithms like Shor's algorithm.

# Initiatives: NIST's Post-Quantum Cryptography Standardization Project



**NIST Leadership:** NIST is spearheading the effort to create encryption standards that can withstand the power of quantum computers, which threaten current cryptographic methods.



**Project Launch:** The Post-Quantum Cryptography Standardization Project was launched in 2016, aiming to find and evaluate algorithms capable of resisting quantum attacks.



**Candidate Algorithms:** The project received 82 candidate algorithms from researchers worldwide, highlighting a broad international effort to tackle this challenge.

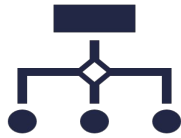


**Evaluation Process:** These algorithms are being subjected to a rigorous multi-round evaluation process, testing them for security, efficiency, and practicality.



**Current Focus:** The evaluation has now narrowed down the initial pool to a select group of finalists that have shown the most promise in meeting the stringent criteria set by NIST.

# Progress: Current Status and Selected Algorithms



**Final Round:** The project is in its final evaluation phase, focusing intensely on the security and performance of the candidate algorithms to ensure they can provide robust protection against quantum attacks.



## Selected Algorithms:

### Lattice-Based:

- **CRYSTALS-Kyber:** Strong security and efficiency for encryption.
- **CRYSTALS-DILITHIUM:** Secure and efficient digital signatures.

### Code-Based:

- **Classic McEliece:** Resilient against classical and quantum attacks.

### Multivariate Polynomial:

- **Rainbow:** Unique approach solving multivariate quadratic equations.



**Future Standards:** NIST plans to finalize and release the first set of quantum-resistant cryptographic standards by 2025, setting the foundation for secure communications in the quantum era.





# Summary of Key Points

- **Key Takeaways:**

1. **Urgency of Quantum-Proof Encryption:** Quantum computing poses a substantial threat to current cryptographic methods, necessitating the development of quantum-resistant encryption.
2. **Power of Hybrid Cryptanalysis:** Leveraging both quantum and classical computing strengths enhances cryptanalytic capabilities, crucial for robust security solutions.
3. **NIST's Leadership in Standards:** NIST plays a pivotal role in standardizing post-quantum cryptographic algorithms, ensuring global readiness against quantum threats.

# Conclusion

- **Importance of Quantum-Proof Encryption:** Quantum computing challenges RSA and ECC, underscoring the need for resilient encryption solutions.
- **Call to Action for Collaboration:** Joint efforts among researchers, institutions, and standards bodies are crucial for developing robust encryption standards.
- **Timeline for Implementation:** Initial quantum-resistant cryptographic standards are expected by 2025, enhancing global cybersecurity preparedness.

# References

- • **Citing Key Sources and Research Papers:**
- • [1] Shor, P.W. “Algorithms for quantum computation: Discrete logarithms and factoring.” Proceedings 35th Annual Symposium on Foundations of Computer Science. IEEE, 1994.
- • [2] Rivest, R.L., Shamir, A., Adleman, L. “A method for obtaining digital signatures and public-key cryptosystems.” Communications of the ACM 21.2 (1978): 120-126.
- • [3] Nielsen, M.A., Chuang, I.L. “Quantum Computation and Quantum Information.” Cambridge University Press, 2010.



Q&A





The background is a vibrant, abstract digital scene. It features a dark blue to black gradient, overlaid with numerous glowing light trails in shades of red, orange, and yellow. These trails curve and sweep across the frame, creating a sense of motion and energy. Scattered throughout the scene are various binary digits (0s and 1s) in different colors (white, blue, yellow) and sizes, some appearing to float or move. The overall aesthetic is futuristic and high-tech, typical of digital art or a presentation about technology.

THANK YOU