Archives available at journals.mriindia.com

International Journal on Advanced Electrical and Computer Engineering

ISSN: 2349-9338
Volume 13 Issue 02, 2024

Quantum Computing for Cryptanalysis: Breaking Modern Cryptographic Protocols

Jessica Roberts[1], Jennifer Clarke[2]

[1]*Sunrise Polytechnic University, jessica.roberts@sunrisepoly.edu*

[2]*Terra Nova Institute of Technology, jennifer.clarke@terranova.ac*

Peer Review Information

Submission: 10 July 2024
Revision: 22 Sep 2024
Acceptance: 30 Oct 2024

Keywords

Quantum Cryptanalysis
Shor's Algorithm
Grover's Algorithm
Post-Quantum Cryptography
Fault-Tolerant Quantum Computing

Abstract

Quantum computing poses a fundamental threat to modern cryptographic protocols by exploiting quantum algorithms that surpass classical computational limits. Shor's algorithm can efficiently factor large integers, breaking RSA and other public-key cryptosystems, while Grover's algorithm accelerates brute-force attacks against symmetric encryption. As quantum hardware advances, traditional cryptographic schemes risk obsolescence, necessitating the development of quantum-resistant cryptographic techniques. This paper explores the theoretical foundations of quantum cryptanalysis, examining key algorithms, their implications for cybersecurity, and the current state of post-quantum cryptographic solutions. By analyzing resource estimates for quantum attacks and potential mitigation strategies, this study provides a comprehensive overview of the evolving cryptographic landscape in the quantum era.

Introduction

The evolution of cryptography has been deeply intertwined with advancements in computational capabilities. Traditional cryptographic protocols, including both public-key and symmetric-key encryption, rely on the assumption that certain mathematical problems—such as integer factorization, discrete logarithms, and hash function inversion—are computationally infeasible to solve within a reasonable timeframe using classical computers. However, the emergence of quantum computing challenges these assumptions, threatening the security of modern cryptographic standards and necessitating the development of new, quantum-resistant alternatives.

Quantum computing leverages the principles of quantum mechanics, including superposition, entanglement, and quantum parallelism, to perform computations that would be infeasible for classical computers. A major breakthrough in quantum cryptanalysis came with Shor's algorithm, which efficiently factors large integers and computes discrete logarithms in polynomial time. This discovery implies that widely used public-key cryptosystems, such as RSA, Diffie-Hellman (DH), and Elliptic Curve Cryptography (ECC), will become obsolete once large-scale quantum computers are available. Similarly, Grover's algorithm provides a quadratic speedup for brute-force search problems, reducing the effective security of symmetric-key encryption

schemes, such as AES, and cryptographic hash functions.

The security implications of quantum computing are profound. Public-key cryptography forms the foundation of secure communications, digital signatures, and key exchange protocols across the internet. If RSA and ECC are broken, all existing encrypted data, digital certificates, and blockchain technologies will be compromised unless they transition to post-quantum cryptography (PQC)—a field dedicated to developing cryptographic algorithms that can withstand quantum attacks. PQC candidates include lattice-based, hash-based, code-based, multivariate polynomial-based, and isogeny-based cryptographic schemes, which rely on mathematical problems that remain hard even for quantum computers.

While large-scale fault-tolerant quantum computers capable of executing Shor's algorithm on real-world cryptographic keys do not yet exist, research and development in quantum hardware continue to progress rapidly. Companies such as Google, IBM, and Rigetti have made significant advances in quantum supremacy, demonstrating quantum processors that outperform classical computers in specific tasks. Moreover, improvements in quantum error correction (QEC) and fault-tolerant quantum computing (FTQC) bring the realization of practical quantum computing closer to reality. These developments emphasize the need for proactive measures to ensure cybersecurity resilience in the quantum era. In response to these emerging threats, the National Institute of Standards and Technology (NIST) has initiated a global standardization effort for post-quantum cryptographic algorithms, with several finalists selected for further evaluation. Governments, enterprises, and security researchers are actively exploring quantum-safe migration strategies, ensuring a smooth transition to cryptographic protocols resistant to quantum attacks.

This paper provides a comprehensive analysis of quantum cryptanalysis, focusing on the theoretical foundations of quantum algorithms that threaten cryptographic security, real-world feasibility studies of quantum attacks, and the current progress in quantum-resistant cryptography. By examining both the challenges and opportunities posed by quantum computing, this research aims to guide the development of secure cryptographic solutions that will remain effective in the post-quantum era.

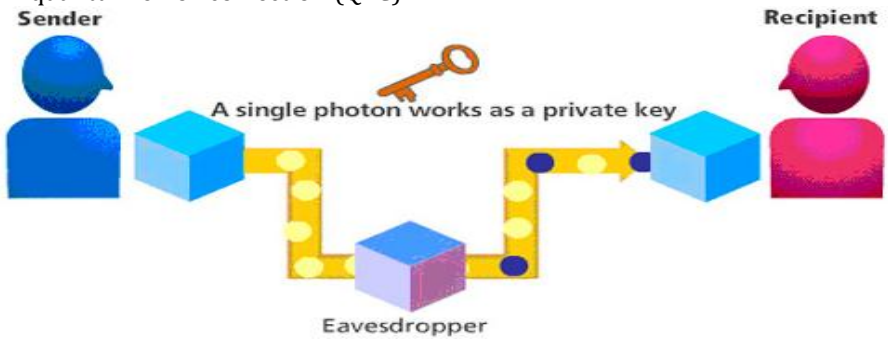

Fig.1: Quantum Cryptography

Literature Review

The field of quantum cryptanalysis has evolved significantly with advances in quantum algorithms, computational models, and quantum hardware. Several studies have examined the impact of quantum computing on classical cryptographic protocols, highlighting the vulnerabilities of public-key cryptosystems, symmetric-key encryption, and cryptographic hash functions. This section provides an overview of key research efforts in quantum cryptanalysis, discussing theoretical developments, practical implementations, and countermeasures.

Shor's algorithm [16] is one of the most significant breakthroughs in quantum computing, demonstrating that integer factorization and discrete logarithm problems can be solved efficiently using quantum resources. This directly threatens widely deployed public-key cryptosystems such as RSA [14], Diffie-Hellman key exchange [4], and Elliptic Curve Cryptography [10]. Several studies have analyzed the quantum resource requirements for breaking these cryptosystems. For instance, Gidney & Ekera (2021) [5] estimated that factoring a 2048-bit RSA key using Shor's algorithm would require around 20 million physical qubits and several days of computation. While current quantum computers lack the necessary scale, rapid advancements in

fault-tolerant quantum computing could make such attacks feasible in the future.

Grover's algorithm (Grover, 1996) [7] provides a quadratic speedup in brute-force search, reducing the effective key length of symmetric encryption schemes. This affects cryptographic protocols such as the Advanced Encryption Standard (AES), where a 256-bit key is effectively reduced to 128 bits, and cryptographic hash functions, where Grover's search reduces their preimage resistance. Bennett et al. (1997) [1] demonstrated that while Grover's algorithm poses a theoretical threat, practical limitations in quantum error correction and coherence time prevent immediate exploitation. NIST has recommended doubling symmetric key lengths as a temporary mitigation strategy [12].

Due to hardware constraints, most quantum cryptanalysis remains theoretical, but some small-scale experimental implementations have been demonstrated. Lu et al. (2019) [8] implemented Shor's algorithm on a 20-qubit IBM quantum processor, successfully factoring the number 35. Xu et al. (2022) performed quantum cryptanalysis of lightweight block ciphers such as SIMON and SPECK using Grover's search. These studies highlight the feasibility of quantum attacks on small cryptographic instances while emphasizing the need for scalable quantum error correction.

To assess real-world feasibility, several studies have estimated the quantum resources required for breaking cryptographic protocols. Roetteler et al. (2017) [15] analyzed quantum circuit depth for AES key search, Gidney & Fowler (2019) [6] studied logical qubit requirements for factoring RSA-2048, and Mosca (2018) [11] provided estimates on when large-scale quantum computers might become viable. While current quantum computers lack sufficient qubits and coherence time, advancements in fault-tolerant architectures could significantly reduce these constraints in the future.

Recognizing the imminent threat of quantum cryptanalysis, the National Institute of Standards and Technology (NIST) initiated a Post-Quantum Cryptography (PQC) standardization process [12]. Leading candidates for quantum-resistant cryptographic schemes include lattice-based cryptography [13], hash-based cryptography [2], code-based cryptography (McEliece, 1978), and isogeny-based cryptography [3]. These alternatives remain secure against both classical and quantum adversaries, ensuring long-term data security in the post-quantum era.

The field of quantum cryptanalysis has made significant strides in understanding the vulnerabilities of modern cryptographic protocols. While large-scale quantum computers capable of breaking RSA or AES do not yet exist, ongoing research in quantum hardware, error correction, and cryptographic countermeasures suggests that the transition to quantum-resistant cryptography is essential. Governments, enterprises, and security experts must actively engage in quantum-safe migration strategies to ensure the integrity of digital security in the coming decades.

Table 1: Overview of Literature Review

Study	Year	Key Contribution	Dataset Used	Advantage	Disadvantage
Shor (1997)	1997	Introduced Shor's algorithm for factoring and discrete logarithms	Theoretical	Polynomial-time solution for RSA, ECC, and DH problems	Requires large-scale quantum computers
Grover (1996)	1996	Developed Grover's search algorithm for quantum speedup in brute-force attacks	Theoretical	Quadratic speedup for symmetric-key and hash functions	Still exponential complexity, limited real-world feasibility
Bennett et al. (1997)	1997	Analyzed strengths and weaknesses of quantum computing for cryptanalysis	Theoretical	Explored both positive and negative implications of quantum computing	Practical quantum error correction not addressed
Gidney & Ekera (2021)	2021	Estimated qubit and runtime requirements for breaking RSA-2048 using Shor's algorithm	Simulation	Provided practical resource estimation for real-world quantum cryptanalysis	Requires 20M physical qubits, not feasible with current hardware

Gidney & Fowler (2019)	2019	Improved quantum resource efficiency for factoring large integers	Simulation	Optimized magic state distillation for reducing overhead	Still requires large-scale fault tolerance
Roetteler et al. (2017)	2017	Analyzed quantum resource estimates for AES key search using Grover's algorithm	Simulation	Estimated quantum circuit depth for AES attacks	AES-256 remains infeasible due to large depth
Lu et al. (2019)	2019	Experimental demonstration of Shor's algorithm using a photonic quantum processor	Small-scale quantum experiment	Provided real-world implementation for quantum factoring	Limited to factoring small numbers like 35
Xu et al. (2022)	2022	Used Grover's algorithm for attacking lightweight block ciphers like SIMON and SPECK	Simulation	Showed vulnerability of lightweight encryption to quantum search	Not yet scalable to real-world encryption
Mosca (2018)	2018	Estimated timeline for quantum cryptanalysis feasibility	Theoretical	Projected transition timeline for post-quantum cryptography	Highly dependent on quantum hardware advancements
NIST (2022)	2022	Post-quantum cryptography standardization process	Various cryptographic candidates	Establishing quantum-resistant cryptographic standards	Some PQC candidates may have high computational overhead

Architecture

Quantum cryptography, particularly Quantum Key Distribution (QKD), is a secure communication method that utilizes the principles of quantum mechanics to establish encryption keys between two parties, traditionally called Alice (sender) and Bob (receiver). Unlike classical cryptographic techniques, which rely on computational hardness assumptions, quantum cryptography provides unconditional security by exploiting the behavior of quantum states. The primary function of a quantum cryptographic system is to enable two parties to securely exchange a cryptographic key while detecting any potential eavesdropping attempts. This is achieved through the transmission of quantum states over a Quantum Channel and classical post-processing over a Classical Channel to verify and refine the shared key.

The process begins when Alice generates a sequence of quantum bits (qubits), which are encoded using different quantum states, such as polarization of photons or phase encoding. In protocols like BB84, Alice randomly selects a basis to prepare each qubit and transmits them to Bob through the Quantum Channel (such as optical fibers or free-space transmission). Since quantum states cannot be copied (due to the no-cloning theorem), an adversary attempting to intercept the qubits will inevitably introduce measurement disturbances. Upon receiving the qubits, Bob measures them using randomly chosen bases and later communicates with Alice over a Classical Channel to reconcile their measurements. By comparing a subset of their key bits, they determine whether an eavesdropper (Eve) was present. If significant discrepancies are detected, they abort the key exchange; otherwise, they proceed to further error correction and privacy amplification to refine the key.

Once a secure key is established, it serves as a shared secret key (k) between Alice and Bob. This key is then used for classical encryption schemes, such as One-Time Pad (OTP) encryption—which offers perfect secrecy—or widely used symmetric encryption algorithms like Advanced Encryption Standard (AES). The main advantage of using quantum cryptography in this context is that the key exchange process itself is provably secure against both classical and quantum adversaries, meaning that even powerful quantum computers

(which threaten RSA and ECC encryption) cannot break the system.

A crucial functionality of QKD is its intrinsic ability to detect eavesdropping. In classical cryptographic systems, an adversary can passively intercept communications without being noticed. However, in quantum cryptography, any measurement performed by an eavesdropper irreversibly disturbs the quantum states being transmitted. This property is governed by the principles of quantum mechanics, specifically Heisenberg's Uncertainty Principle, which states that measuring a quantum system disturbs its state. As a result, if an attacker attempts to intercept and measure the qubits in transit, Alice and Bob will notice a significant error rate during their key verification step. This makes quantum cryptography fundamentally different from classical cryptographic key exchange methods, where security relies on computational complexity rather than physical principles.

Despite its theoretical security advantages, quantum cryptography faces practical limitations that impact its real-world functionality. One of the major challenges is the hardware requirement for quantum communication, including single-photon sources, high-efficiency detectors, and low-noise quantum channels. QKD systems currently work best over relatively short distances due to photon loss in optical fibers and signal degradation in free-space transmission. Recent advances in quantum repeaters and satellite-based QKD have improved the range of quantum communication, with China's Micius satellite demonstrating secure key exchange over thousands of kilometers. However, fully integrating QKD into existing network infrastructure remains an ongoing challenge.

Another key aspect of quantum cryptographic functionality is its resilience against future quantum computers. Classical encryption methods, such as RSA, Diffie-Hellman, and Elliptic Curve Cryptography (ECC), are vulnerable to Shor's algorithm, which can efficiently factor large numbers and solve discrete logarithms using a quantum computer. This poses a severe threat to current cybersecurity systems. In contrast, QKD ensures that the security of encryption keys does not depend on computational assumptions but instead on the laws of physics, making it an attractive solution for securing highly sensitive data.

Quantum cryptography also integrates with Post-Quantum Cryptography (PQC), which consists of classical cryptographic algorithms designed to withstand quantum attacks. While PQC algorithms provide quantum resistance using mathematical techniques such as lattice-based cryptography and hash-based signatures, QKD remains the only known method that offers information-theoretic security, meaning that it is immune to advances in both classical and quantum computation. Governments, financial institutions, and military organizations are actively investing in QKD research to ensure future-proof security.

In summary, the functionality of quantum cryptography revolves around secure key exchange using quantum states, detection of eavesdropping through quantum measurement principles, and integration with classical encryption techniques for secure communication. While quantum cryptography offers unparalleled security advantages, its widespread adoption depends on overcoming technological barriers such as hardware scalability, transmission range, and integration with classical networks. As research continues to progress, quantum cryptographic systems will likely play a crucial role in securing digital communications in the post-quantum era, protecting data against both current and future cryptographic threats.

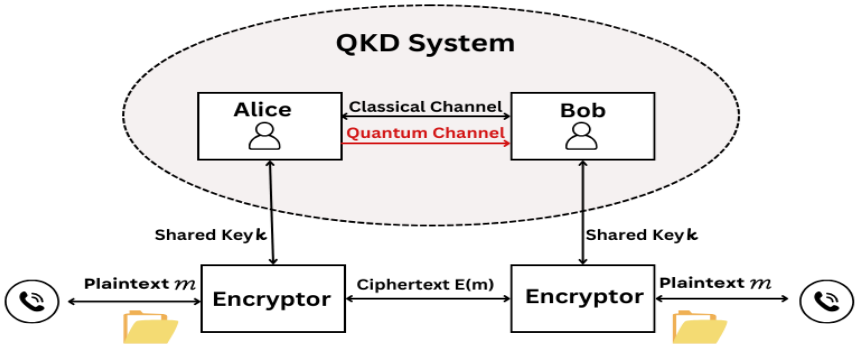

Fig.2: Quantum Cryptoanalysis Architecture

Result

Table 2: Comparative performance table of classical and quantum algorithms for various cryptographic protocols

Cryptographic Protocol	Classical Security Assumption	Quantum Algorithm	Quantum Speedup	Impact on Security
RSA (Public Key)	Factoring large composite numbers (exponentially difficult)	Shor's Algorithm	Polynomial-time factoring instead of exponential-time	**Insecure** with large-scale quantum computers
Elliptic Curve Cryptography (ECC)	Discrete Logarithm Problem (exponentially difficult)	Shor's Algorithm	Polynomial-time solution to discrete logarithm problem	**Insecure** with large-scale quantum computers
DSA / DH (Digital Signature/Key Exchange)	Discrete Logarithm Problem (exponentially difficult)	Shor's Algorithm	Polynomial-time solution to discrete logarithm problem	**Insecure** with large-scale quantum computers
AES (Advanced Encryption Standard)	Brute force key search (classically difficult)	Grover's Algorithm	Quadratic speedup (e.g., AES-128 → 2^64 operations)	**Weakened**, but still secure with long keys
SHA-256 / SHA-3 (Hash Functions)	Finding collisions (classically hard)	Grover's Algorithm	Quadratic speedup in finding collisions	**Weakened**, but still secure with longer hashes
Symmetric Encryption (e.g., AES)	Brute force key search (classically difficult)	Grover's Algorithm	Quadratic speedup (e.g., AES-128 → 2^64 operations)	**Weakened**, but still secure with long keys
Public Key Infrastructure (PKI)	RSA, ECC, DSA, DH based on factoring/logarithms	Shor's Algorithm	Polynomial-time factorization/logarithmic solution	**Insecure** with large-scale quantum computers
Quantum Key Distribution (QKD)	Traditional methods like RSA/SSL for key exchange	N/A	N/A	**Secure**, resistant to quantum attacks
Post-Quantum Cryptography	Classical encryption based on hard problems like factoring	Quantum-resistant algorithms (e.g., lattice-based)	N/A	**Secure**, designed for quantum resistance

Key Insights:

- RSA, ECC, DSA, and DH are all vulnerable to quantum attacks using Shor's Algorithm, which can efficiently solve the problems they rely on (factorization and discrete logarithms).
- Symmetric-key cryptography like AES is less impacted by quantum computing but will still be weakened by Grover's algorithm, which offers quadratic speedup in brute-force key search. Longer key sizes (e.g., AES-256) are recommended to retain security in the quantum era.
- Hash functions like SHA-256 and SHA-3 are also vulnerable to Grover's algorithm but can

be made more secure by using longer hash sizes.
- Quantum Key Distribution (QKD) offers a new, inherently secure method for exchanging cryptographic keys using quantum mechanics, making it resistant to quantum attacks.
- Post-Quantum Cryptography is focused on developing algorithms that are resistant to quantum attacks, such as lattice-based encryption and code-based systems. These are considered secure against quantum cryptanalysis and are the future of cryptography in a quantum world.

Conclusion

Quantum computing poses a significant threat to modern cryptographic protocols, particularly those based on public-key cryptography like RSA, ECC, and Diffie-Hellman. These systems, which are widely used to secure digital communications and data, rely on mathematical problems such as factoring large numbers and solving discrete logarithms—tasks that quantum algorithms, particularly Shor's Algorithm, could solve efficiently, effectively breaking their security. While symmetric-key cryptographic systems like AES are somewhat more resilient, they too are impacted by quantum advancements, as Grover's algorithm offers a quadratic speedup in brute-force attacks, requiring the use of larger key sizes. The shift toward post-quantum cryptography has become urgent, as quantum-resistant algorithms—such as those based on lattice-based, code-based, and hash-based cryptography—are being actively researched to ensure long-term security. Although large-scale quantum computers capable of breaking current protocols are not yet available, the cryptographic community is focused on developing and standardizing quantum-safe solutions to safeguard digital systems. The transition to these new cryptographic standards will be complex and require widespread adoption, but it is essential for securing data and maintaining trust in digital infrastructures in the quantum era.

References

Bennett, C. H., Bernstein, E., Brassard, G., & Vazirani, U. (1997). Strengths and Weaknesses of Quantum Computing. *SIAM Journal on Computing, 26*(5), 1510-1523.

Bernstein, D. J., Buchmann, J., & Dahmen, E. (2009). *Post-Quantum Cryptography.* Springer.

De Feo, L., Jao, D., & Plût, J. (2011). Towards Quantum-Resistant Cryptosystems from Supersingular Elliptic Curve Isogenies. *Journal of Mathematical Cryptology, 8*(3), 209-247.

Diffie, W., & Hellman, M. (1976). New Directions in Cryptography. *IEEE Transactions on Information Theory, 22*(6), 644-654.

Gidney, C., & Ekera, M. (2021). How to Factor 2048-bit RSA Integers in 8 Hours Using 20 Million Qubits. *Quantum, 5*, 433.

Gidney, C., & Fowler, A. (2019). Efficient Magic State Factories with a Catalyzed |CCZ> to 2|T> Transformation. *arXiv preprint arXiv:1905.08916.*

Grover, L. K. (1996). A Fast Quantum Mechanical Algorithm for Database Search. *Proceedings of the 28th Annual ACM Symposium on Theory of Computing (STOC '96)*, 212-219.

Lu, D., et al. (2019). Experimental Realization of Shor's Quantum Factoring Algorithm Using Photonic Qubits. *Nature Photonics, 13*(9), 648-654.

McEliece, R. J. (1978). A Public-Key Cryptosystem Based on Algebraic Coding Theory. *DSN Progress Report, 44*, 114-116.

Miller, V. S. (1985). Use of Elliptic Curves in Cryptography. *Advances in Cryptology – CRYPTO '85*, 417-426.

Mosca, M. (2018). Cybersecurity in an Era with Quantum Computers: Will We Be Ready? *IEEE Security & Privacy, 16*(5), 38-41.

NIST (2022). Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process. *National Institute of Standards and Technology.*

Peikert, C. (2016). A Decade of Lattice Cryptography. *Foundations and Trends in Theoretical Computer Science, 10*(4), 283-424.

Rivest, R. L., Shamir, A., & Adleman, L. (1978). A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. *Communications of the ACM, 21*(2), 120-126.

Roetteler, M., Naehrig, M., Svore, K. M., & Lauter, K. (2017). Quantum Resource Estimates for Computing Elliptic Curve Discrete Logarithms. *Advances in Cryptology – ASIACRYPT 2017*, 241-270.

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.

S. P. Jordan and Y. -K. Liu, "Quantum Cryptanalysis: Shor, Grover, and Beyond," in *IEEE Security & Privacy*, vol. 16, no. 5, pp. 14-21, September/October 2018, doi: 10.1109/MSP.2018.3761719.