How Shor's Algorithm Breaks Modern Cryptography

Alwin S.
Universitas Indonesia

Sahira AK
Universitas Gadjah Mada

June 16, 2025

Abstract

The security of our global digital infrastructure—from financial transactions to classified government communications—is predicated on the computational difficulty of a few specific mathematical problems. Public-key cryptosystems, such as RSA and Elliptic Curve Cryptography (ECC), have served as the bedrock of digital trust for decades, assuming that problems like integer factorization and the discrete logarithm are intractable for classical computers. In 1994, Peter Shor introduced a quantum algorithm that fundamentally invalidates this assumption. This paper provides a comprehensive exploration of how Shor's algorithm achieves this feat. We deconstruct the algorithm's mechanics, revealing how it transforms these famously hard problems into a solvable task of period-finding. We demonstrate its direct application to breaking both RSA and ECC, thereby exposing their shared vulnerability to a quantum adversary. Contextualizing this theoretical threat, we examine the current state of quantum hardware development, the immense resources required for a cryptographically relevant attack, and the global effort led by institutions like NIST to standardize a new suite of post-quantum cryptographic algorithms. Finally, we analyze the profound security and ethical implications of this paradigm shift, including the immediate danger of "Harvest Now, Decrypt Later" attacks and the urgent, global imperative to transition to a quantum-resistant cryptographic future.

1 Introduction

The modern world runs on data, and the confidentiality, integrity, and authenticity of that data are guaranteed by a sophisticated architecture of cryptographic protocols. At the heart of this architecture lies public-key cryptography, a revolutionary concept that enables secure communication and digital signatures between parties who have never previously met. This digital trust infrastructure underpins everything from secure e-commerce and private messaging to the command-and-control systems that safeguard national security [1].

The security of these systems is not absolute; it is conditional. It rests upon the presumed computational difficulty of certain mathematical problems. For decades, we have built our digital society on the belief that these problems are too hard to solve in any practical timeframe using the best-known algorithms on the most powerful classical computers.

The advent of quantum computing challenges this foundational belief. A quantum computer is not merely a faster version of a classical computer; it operates on an entirely different set of physical principles, harnessing the counterintuitive phenomena of quantum mechanics—superposition, entanglement, and interference—to process information in ways that have no classical analogue [3].

This paper argues that Peter Shor's 1994 algorithm for integer factorization and discrete logarithms represents a singular, disruptive event in the history of information security [4]. It is not an incremental improvement on existing attacks but a fundamental breakthrough that invalidates the core security assumptions of the most widely

deployed public-key systems.

Classical security relies on problems like integer factorization being in a complexity class that is believed to be outside of P (Polynomial time) and BPP (Bounded-error Probabilistic Polynomial time) [5]. Shor's algorithm demonstrates that these problems are, in fact, in BQP (Bounded-error Quantum Polynomial time) [6]. This implies not just a faster computer but a fundamental shift in what is considered computable in practice.

2 Modern Cryptography: Foundations and Vulnerabilities

The security of modern public-key cryptography relies on the concept of a "trapdoor one-way function." This is a function that is easy to compute in one direction but extremely difficult to reverse unless one possesses a secret piece of information—the trapdoor. The two most dominant families of public-key cryptosystems, RSA and Elliptic Curve Cryptography (ECC), are built on different mathematical problems, yet they share a common structural vulnerability when confronted with a quantum computer.

2.1 The RSA Cryptosystem

Developed in 1977 by Ron Rivest, Adi Shamir, and Leonard Adleman, the RSA algorithm has become the workhorse of public-key encryption. Its security is directly tied to the difficulty of the Integer Factorization Problem (IFP) [7].

The key generation process for RSA is as follows [7]:

1. Choose two large, distinct prime numbers, p and q. These are kept secret.
2. Compute the modulus $N = pq$. This value is part of the public key.
3. Compute Euler's totient function of N, which is $\phi(N) = (p-1)(q-1)$.
4. Choose a public exponent e such that $1 < e < \phi(N)$ and $\gcd(e, \phi(N)) = 1$.
5. Compute the private exponent d as the modular multiplicative inverse of e modulo $\phi(N)$.

To encrypt a message M, one computes the ciphertext C as:

$$C \equiv M^e \pmod{N}$$

To decrypt the ciphertext C, the recipient uses their private key d:

$$M \equiv C^d \pmod{N}$$

The correctness of this process is guaranteed by Euler's theorem. The security of RSA hinges on the fact that an adversary, knowing only the public key (N, e), cannot feasibly determine the private key d. To compute d, the adversary would need to know $\phi(N)$, which requires factoring N into its prime components p and q. For large N, this is considered classically intractable [8].

2.2 Elliptic Curve Cryptography (ECC)

Introduced independently by Neal Koblitz and Victor Miller in 1985, Elliptic Curve Cryptography (ECC) offers equivalent security to RSA but with significantly smaller key sizes [9]. Its security is based on the Elliptic Curve Discrete Logarithm Problem (ECDLP).

An elliptic curve over a finite field $\mathbb{F}_p$ (where p is a large prime) is the set of points (x, y) that satisfy the equation:

$$y^2 \equiv x^3 + ax + b \pmod{p}$$

along with a special "point at infinity," denoted $\mathcal{O}$. The coefficients a and b are constants from the field $\mathbb{F}_p$ [10].

ECC cryptosystems, such as the Elliptic Curve Diffie-Hellman (ECDH) key exchange, operate as follows [9]:

1. Alice and Bob publicly agree on a curve E and a base point P of large order on that curve.

2. Alice chooses a secret integer k_A (her private key) and computes her public key $Q_A = k_A P$.

3. Bob chooses a secret integer k_B (his private key) and computes his public key $Q_B = k_B P$.

4. They exchange public keys and compute the shared secret $(k_A k_B)P$.

The security of ECC relies on the ECDLP: given the base point P and the public key $Q = kP$, it is computationally infeasible for a classical computer to determine the private key k [11].

2.3 The Quantum Achilles' Heel

Despite their different mathematical underpinnings, the security of both RSA and ECC collapses for the same fundamental reason: the hard problems they rely on can be reduced to a more general problem of period-finding [12].

For RSA, the task of factoring N can be transformed into finding the period of the modular exponentiation function $f(x) = a^x \bmod N$ for a randomly chosen base a. This function is periodic because the set of integers coprime to N forms a finite multiplicative group.

For ECC, solving the ECDLP to find k in $Q = kP$ can be transformed into finding the period of a related two-dimensional function [13].

3 Quantum Computing: A New Computational Paradigm

Quantum computing is not an evolution of classical computing but a revolution. It leverages the laws of quantum mechanics to process information in a fundamentally new way, granting computational power that is unattainable for any classical machine.

3.1 The Qubit: Superposition and Entanglement

The fundamental unit of classical information is the bit, which can be in one of two definite states: 0 or 1. The quantum analogue is the qubit, a two-level quantum system. A qubit can exist in the state $|0\rangle$, the state $|1\rangle$, or, crucially, in a superposition of both states simultaneously [14].

Using the Dirac bra-ket notation, the state of a single qubit $|\psi\rangle$ is described as:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

Here, α and β are complex numbers called probability amplitudes, which satisfy the normalization condition $|\alpha|^2 + |\beta|^2 = 1$ [15].

The second key principle is entanglement, a uniquely quantum correlation. When two or more qubits are entangled, their fates are inextricably linked, regardless of the physical distance separating them [15].

3.2 Quantum Interference: The Engine of Computation

A common misconception is that quantum computers derive their power simply by trying all 2^n possibilities in parallel. The true source of quantum advantage lies in the principle of quantum interference [14].

Quantum algorithms are designed to be a carefully choreographed dance of probability amplitudes:

1. **Initialization**: The quantum register is prepared in a superposition of all possible inputs.

2. **Computation**: A sequence of quantum gates is applied to manipulate both values and phases.

3. **Interference**: A final transformation causes probability amplitudes to interfere.

4. **Measurement**: Through constructive interference, correct answers are amplified while incorrect answers cancel out.

3.3 Computational Complexity and BQP

To formalize the power of quantum computers, complexity theorists have defined the class BQP

(Bounded-error Quantum Polynomial time) [16]. BQP is the class of decision problems that can be solved by a quantum computer in polynomial time with bounded error probability.

The known relationships between complexity classes are [6]:

$$P \subseteq BPP \subseteq BQP \subseteq PSPACE$$

Shor's algorithm provides the strongest evidence that BQP strictly contains BPP, demonstrating that quantum computers possess fundamentally superior computational power.

4 Shor's Algorithm: Theory and Mechanism

Peter Shor's 1994 algorithm is a masterpiece of interdisciplinary thinking, elegantly weaving together classical number theory with quantum computation. The algorithm's genius lies in its hybrid structure: it uses a classical computer to frame the problem while delegating the classically intractable subroutine of period-finding to a quantum computer.

4.1 The Classical Reduction: From Factoring to Order-Finding

The first part of Shor's algorithm is purely classical and reduces the problem of factoring a large integer N to the problem of finding the order of a randomly chosen integer modulo N [17].

The order of an integer a modulo N is the smallest positive integer r such that $a^r \equiv 1 \pmod{N}$. The reduction proceeds as follows:

1. Choose a random integer a such that $1 < a < N$.
2. Compute $\gcd(a, N)$ using the Euclidean algorithm. If $\gcd(a, N) \neq 1$, we have found a factor.
3. Find the order r of a modulo N (quantum step).
4. If r is odd, return to step 1.
5. If r is even, compute $x = a^{r/2}$.
6. If $x \equiv -1 \pmod{N}$, return to step 1.
7. Otherwise, compute $\gcd(x - 1, N)$ and $\gcd(x + 1, N)$ to find factors.

4.2 The Quantum Core: Period-Finding Subroutine

The heart of Shor's algorithm is the quantum subroutine that finds the period r of the function $f(x) = a^x \bmod N$. This is achieved using two quantum registers and proceeds in three main stages:

State Preparation and Modular Exponentiation: The input register is initialized to an equal superposition:

$$\frac{1}{\sqrt{Q}} \sum_{x=0}^{Q-1} |x\rangle|0\rangle$$

A quantum oracle for modular exponentiation is applied:

$$U_{a,N} : |x\rangle|0\rangle \mapsto |x\rangle|a^x \bmod N\rangle$$

Quantum Fourier Transform: After measuring the output register, the input register collapses into a periodic superposition. The Quantum Fourier Transform (QFT) is then applied [18]:

$$\mathrm{QFT}|j\rangle = \frac{1}{\sqrt{Q}} \sum_{k=0}^{Q-1} e^{2\pi i jk/Q} |k\rangle$$

Measurement and Classical Post-Processing: The input register is measured, yielding an integer c that is close to a multiple of Q/r. The continued fractions algorithm is used to extract the period r.

4.3 Complexity Analysis

The power of Shor's algorithm lies in its dramatic reduction in computational complexity compared to classical algorithms:

4.4 Complexity Analysis

The power of Shor's algorithm lies in its dramatic reduction in computational complexity compared to classical algorithms:

Problem	Classical	Quantum
Integer Factorization	$\exp(O(n^{1/3}(\log n)^{2/3}))$	$O(n^3)$
DLP (mod prime)	$\exp(O((\log p)^{1/3}(\log\log p)^{2/3}))$	$O((\log p)^3)$
ECDLP	$O(\sqrt{n})$	$O((\log n)^3)$

Table 1: Time Complexity Comparison: Classical vs. Quantum

This exponential speedup makes Shor's algorithm a civilization-level threat to modern cryptography.

5 Breaking RSA and ECC: Shor in Action

Having deconstructed the general mechanism of Shor's algorithm, we now examine its specific application against RSA and ECC.

5.1 Case Study 1: Factoring an RSA Modulus

Consider factoring $N = 21$. We choose $a = 2$ and examine $f(x) = 2^x \bmod 21$:

$$\begin{aligned} f(0) &= 1 \\ f(1) &= 2 \\ f(2) &= 4 \\ f(3) &= 8 \\ f(4) &= 16 \\ f(5) &= 11 \\ f(6) &= 1 \end{aligned}$$

The period is $r = 6$. Since r is even, we compute $x = 2^{6/2} = 8$. Since $8 \not\equiv -1 \pmod{21}$, we find:

$$\begin{aligned} \gcd(8-1, 21) &= \gcd(7, 21) = 7 \\ \gcd(8+1, 21) &= \gcd(9, 21) = 3 \end{aligned}$$

We have successfully factored $21 = 3 \times 7$.

5.2 Case Study 2: Solving the ECDLP

The attack on ECC uses a generalization of Shor's algorithm. We define a function:

$$f(x_1, x_2) = x_1 P + x_2 Q$$

This function is periodic with period vector (r_1, r_2) such that:

$$r_1 P + r_2 Q = \mathcal{O}$$

Substituting $Q = kP$:

$$r_1 + r_2 k \equiv 0 \pmod{n}$$

From this, we solve for the secret key:

$$k \equiv -r_1 \cdot r_2^{-1} \pmod{n}$$

5.3 A Unified Vulnerability: The Hidden Subgroup Problem

Both RSA and ECC vulnerabilities stem from the fact that both problems are instances of the Abelian Hidden Subgroup Problem (HSP) [12]. Shor's algorithm is essentially an efficient quantum algorithm for solving the HSP for any finite abelian group.

6 State of Quantum Hardware

The theoretical threat posed by Shor's algorithm depends on the development of large-scale, fault-tolerant quantum computers.

6.1 The NISQ Era and its Challenges

We are currently in the Noisy Intermediate-Scale Quantum (NISQ) era [19]. Today's quantum processors face challenges including:

- **Decoherence**: Loss of quantum properties due to environmental interactions
- **Gate Errors**: Imperfect quantum operations that accumulate over time
- **Connectivity**: Limited qubit interactions requiring complex routing

6.2 Hardware Progress and Roadmaps

Major technology companies are pursuing different approaches:
IBM: Targeting fault-tolerant system "Starling" by 2029 with 200 logical qubits capable of 100 million operations [20].
Google: Demonstrated quantum supremacy with Sycamore and major progress in error correction with Willow chip [21].

6.3 Resource Estimates for Breaking RSA-2048

Source	Logical Qubits	Physical Qubits	Runtime
Beauregard (2003)	4,099	$\sim$4 Million	Days-Weeks
Gidney & Ekerå (2021)	$\sim$20,000	$\sim$20 Million	8 hours
Gidney (2025)	N/A	$<$ 1 Million	$<$ 1 week

Table 2: Resource Estimates to Break RSA-2048

Recent algorithmic improvements have reduced estimated requirements by 20x, suggesting timelines may be shorter than anticipated [22].

7 Post-Quantum Cryptography

The inevitability of cryptographically relevant quantum computers has catalyzed development of Post-Quantum Cryptography (PQC) [23].

7.1 NIST PQC Standardization Process

NIST initiated a public competition in 2016 to standardize quantum-resistant algorithms [24]. In 2024, NIST published the first three official standards [25]:

- **FIPS 203 (ML-KEM)**: Key-Encapsulation Mechanism based on CRYSTALS-KYBER
- **FIPS 204 (ML-DSA)**: Digital Signature Algorithm based on CRYSTALS-Dilithium
- **FIPS 205 (SLH-DSA)**: Hash-based signature scheme SPHINCS+

In 2025, NIST selected HQC (Hamming Quasi-Cyclic) as an additional code-based KEM [26].

7.2 Leading PQC Algorithm Families

Lattice-Based Cryptography: Most promising family, based on problems like Learning With Errors (LWE) [27].

Code-Based Cryptography: Based on error-correcting codes, offering strong security but large key sizes [28].

Hash-Based Signatures: Security relies solely on hash function collision-resistance [29].

7.3 Migration Challenges

Transitioning to PQC faces several challenges [30]:

- **Performance and Size**: Larger keys and signatures
- **Implementation Complexity**: Complete cryptographic inventory required
- **Crypto-Agility**: Need for systems that can easily switch algorithms

8 Future Outlook and Ethical Implications

The development of cryptographically relevant quantum computers poses profound ethical and security challenges.

8.1 The "Harvest Now, Decrypt Later" Threat

The most immediate danger is the "Harvest Now, Decrypt Later" (HNDL) attack strategy [31]. Adversaries are already intercepting and storing encrypted data, waiting for quantum computers to decrypt it. This makes PQC migration urgent for any long-lived sensitive data.

8.2 National Security and the Quantum Arms Race

The quantum threat has triggered a global arms race [2]. The US has established national policy through NSM-10, mandating government-wide PQC transition by 2035 [32].

8.3 Retroactive Decryption and Societal Trust

The prospect of retroactive decryption threatens long-term digital privacy, potentially undermining trust in digital systems [33]. This could have chilling effects on digital communication and commerce.

9 Conclusion

Shor's algorithm stands as a landmark achievement demonstrating how quantum computing can upend established security principles. By exploiting hidden periodic structures in RSA and ECC, it transforms intractable problems into solvable puzzles for quantum computers.

This breakthrough presents a dual challenge: engineering fault-tolerant quantum computers and migrating global digital infrastructure to post-quantum standards. We are living in a unique moment where a theoretical algorithm has preemptively rendered deployed security technologies obsolete, forcing a global migration driven by the silent threat of "Harvest Now, Decrypt Later" attacks.

The race between quantum code-breakers and post-quantum code-makers will shape the landscape of digital security for generations to come. The outcome will determine whether we enter an era of unprecedented surveillance capability or successfully transition to a quantum-resistant cryptographic future.

References

[1] Post-Quantum Cryptography, Explained - Booz Allen, accessed June 16, 2025, https://www.boozallen.com/insights/ai-research/post-quantum-cryptography-explained.html

[2] Quantum Computing Threat to Cryptography - Just Security, accessed June 16, 2025, https://www.justsecurity.org/113733/quantum-computing-crytopography/

[3] Physical Principles Underpinning Quantum Computing - EE Times Europe, accessed June 16, 2025

[4] Shor, P. W. (1994). Algorithms for quantum computation: discrete logarithms and factoring. In Proceedings of the 35th Annual Symposium on Foundations of Computer Science (pp. 124–134). IEEE.

[5] Computational hardness assumption - Wikipedia, accessed June 16, 2025

[6] Quantum complexity theory - Wikipedia, accessed June 16, 2025

[7] The Mathematical Cryptography of the RSA Cryptosystem, accessed June 16, 2025

[8] Integer factorization - Wikipedia, accessed June 16, 2025

[9] Understanding Elliptic Curve Cryptography (ECC) - Encryption Consulting, accessed June 16, 2025

[10] Elliptic Curve Cryptography - Basic Math - EmbeddedRelated.com, accessed June 16, 2025

[11] Discrete Logarithms on Elliptic Curves - Rose-Hulman Scholar, accessed June 16, 2025

[12] Shor's algorithm - Wikipedia, accessed June 16, 2025

[13] Shor's discrete logarithm quantum algorithm for elliptic curves, arXiv preprint quant-ph/0301141

[14] What Is Quantum Computing? — IBM, accessed June 16, 2025

[15] Superposition and entanglement - Quantum Inspire, accessed June 16, 2025

[16] BQP - Wikipedia, accessed June 16, 2025

[17] Shor's factoring algorithm — Quantiki, accessed June 16, 2025

[18] Quantum Fourier transform - Wikipedia, accessed June 16, 2025

[19] Making Quantum Error Correction practical - Q-CTRL, accessed June 16, 2025

[20] IBM Sets the Course to Build World's First Large-Scale, Fault-Tolerant Quantum Computer, accessed June 16, 2025

[21] Meet Willow, our state-of-the-art quantum chip - Google Blog, accessed June 16, 2025

[22] Google Researcher Lowers Quantum Bar to Crack RSA Encryption, accessed June 16, 2025

[23] Post-quantum cryptography - BSI, accessed June 16, 2025

[24] Post-Quantum Cryptography Standardization - NIST, accessed June 16, 2025

[25] Post-Quantum Cryptography — CSRC - NIST, accessed June 16, 2025

[26] NIST advances post-quantum cryptography standardization, selects HQC algorithm, accessed June 16, 2025

[27] Prepping for post-quantum: a beginner's guide to lattice cryptography, accessed June 16, 2025

[28] What is Code-based Cryptography? - Utimaco, accessed June 16, 2025

[29] What is Hash-based Cryptography? - Utimaco, accessed June 16, 2025

[30] PostQuantum Migration Challenges — Technology Innovation Institute, accessed June 16, 2025

[31] Harvest now, decrypt later: Why today's encrypted data isn't safe, accessed June 16, 2025

[32] US Allied Militaries Must Prepare for the Quantum Threat - RAND, accessed June 16, 2025

[33] Quantum computing may create ethical risks for businesses - Deloitte, accessed June 16, 2025