QUANTUM CRYPTANALYSIS OF ELLIPTIC CURVE CRYPTOGRAPHY

Experimental Analysis of Quantum Attack Vectors Against ECC Implementations

By Ibrahim Khamis Ibrahim

Institute for Advanced Cryptographic Research • Department of Computer Science

Date: June 15, 2025 • **Report ID:** QC-ECC-2025-001

ABSTRACT

This research presents a comprehensive experimental analysis of quantum cryptanalytic attacks against elliptic curve cryptography (ECC) implementations. Through systematic testing across multiple elliptic curves with varying field sizes and private key configurations, we evaluate the effectiveness of quantum algorithms in breaking ECC security. Our experimental framework, implemented using the Cirq quantum computing library, demonstrates the current limitations and potential of quantum attacks against modern cryptographic systems. The results provide critical insights into the quantum threat landscape for elliptic curve cryptography and inform post-quantum cryptographic transition strategies.

1. Introduction

Elliptic Curve Cryptography (ECC) has emerged as a cornerstone of modern cryptographic systems, offering robust security with smaller key sizes compared to traditional RSA implementations. However, the advent of quantum computing poses a significant threat to ECC security, as quantum algorithms such as Shor's algorithm can potentially break the elliptic curve discrete logarithm problem (ECDLP) in polynomial time.

This study presents a systematic experimental analysis of quantum attacks against ECC implementations, utilizing state-of-the-art quantum simulation frameworks to evaluate attack effectiveness across various elliptic curve parameters. Our research contributes to the understanding of quantum cryptanalytic capabilities and informs the development of quantum-resistant cryptographic protocols.

2. Theoretical Background

2.1 Elliptic Curve Cryptography

An elliptic curve over a finite field F_p is defined by the Weierstrass equation:

$$y^2 = x^3 + ax + b \ (\mathrm{mod}\ p)$$

where a and b are coefficients in F_p, and the discriminant ? = $-16(4a^3 + 27b^2)$? 0 to ensure the curve is non-singular.

2.2 Quantum Cryptanalytic Approach

The quantum attack methodology employs a modified Shor's algorithm specifically adapted for the elliptic curve discrete logarithm problem. The algorithm utilizes quantum superposition and entanglement to achieve exponential speedup over classical methods, with theoretical complexity $O((\log p)^3)$ compared to the classical O(?p) complexity.

3. Experimental Methodology

3.1 Hardware Configuration

Computational Infrastructure:
- Platform: Windows 11 Professional (Build 10.0.26100)
- Processor: Intel Xeon E5-2697 v4 (28 cores, 2.3 GHz base frequency)
- Memory: 32 GB DDR4 ECC RAM
- Quantum Simulation: Cirq Framework v1.5.0
- Programming Environment: Python 3.12.9

3.2 Experimental Parameters

The experimental design encompasses systematic testing across multiple elliptic curves with varying cryptographic parameters:

- **Field Sizes:** Prime fields F_5, F_7, F_{11}, and F_{13}
- **Curve Configurations:** Four distinct elliptic curves with different coefficient sets
- **Private Key Range:** Systematic testing across cryptographically relevant private key values
- **Quantum Circuit Complexity:** 5-6 qubit implementations with circuit depths ranging from 16-18 gates

4. Experimental Results

4.1 Individual Experiment Analysis

Experiment 1: $y^2 = x^3 + 2x + 3 \pmod{5}$

- **Target Private Key:** 2
- **Quantum Attack Success:** ?
- **Classical Computation Time:** 0.0010 seconds
- **Quantum Computation Time:** 0.0382 seconds
- **Quantum Circuit Specifications:**
  - Qubits Required: 5
  - Circuit Depth: 16 gates
  - Gate Composition: HPowGate: 15, _PauliX: 8, CZPowGate: 8, CCZPowGate: 1, MeasurementGate: 1

Experiment 2: $y^2 = x^3 + 2x + 3 \pmod{5}$

- **Target Private Key:** 3
- **Quantum Attack Success:** ?
- **Classical Computation Time:** 0.0000 seconds
- **Quantum Computation Time:** 0.0371 seconds
- **Quantum Circuit Specifications:**
  - Qubits Required: 5
  - Circuit Depth: 16 gates
  - Gate Composition: HPowGate: 15, _PauliX: 8, CZPowGate: 8, CCZPowGate: 1, MeasurementGate: 1

Experiment 3: $y^2 = x^3 + 2x + 3 \pmod{7}$

- **Target Private Key:** 2
- **Quantum Attack Success:** ?

- **Classical Computation Time:** 0.0000 seconds
- **Quantum Computation Time:** 0.0366 seconds
- **Quantum Circuit Specifications:**
    - Qubits Required: 5
    - Circuit Depth: 16 gates
    - Gate Composition: HPowGate: 15, _PauliX: 8, CZPowGate: 8, CCZPowGate: 1, MeasurementGate: 1

Experiment 4: $y^2 = x^3 + 2x + 3 \pmod 7$

- **Target Private Key:** 3
- **Quantum Attack Success:** ?
- **Classical Computation Time:** 0.0000 seconds
- **Quantum Computation Time:** 0.0370 seconds
- **Quantum Circuit Specifications:**
    - Qubits Required: 5
    - Circuit Depth: 16 gates
    - Gate Composition: HPowGate: 15, _PauliX: 8, CZPowGate: 8, CCZPowGate: 1, MeasurementGate: 1

Experiment 5: $y^2 = x^3 + 2x + 3 \pmod 7$

- **Target Private Key:** 4
- **Quantum Attack Success:** ?
- **Classical Computation Time:** 0.0000 seconds
- **Quantum Computation Time:** 0.0430 seconds
- **Quantum Circuit Specifications:**
    - Qubits Required: 5
    - Circuit Depth: 16 gates
    - Gate Composition: HPowGate: 15, _PauliX: 8, CZPowGate: 8, CCZPowGate: 1, MeasurementGate: 1

Experiment 6: $y^2 = x^3 + 1x + 6 \pmod{11}$

- **Target Private Key:** 3
- **Quantum Attack Success:** ?
- **Classical Computation Time:** 0.0000 seconds
- **Quantum Computation Time:** 0.0451 seconds
- **Quantum Circuit Specifications:**
    - Qubits Required: 6
    - Circuit Depth: 18 gates
    - Gate Composition: HPowGate: 20, _PauliX: 10, CZPowGate: 10, CCZPowGate: 1, MeasurementGate: 1

Experiment 7: $y^2 = x^3 + 1x + 6 \pmod{11}$

- **Target Private Key:** 5
- **Quantum Attack Success:** ?
- **Classical Computation Time:** 0.0000 seconds
- **Quantum Computation Time:** 0.0450 seconds
- **Quantum Circuit Specifications:**
    - Qubits Required: 6
    - Circuit Depth: 18 gates
    - Gate Composition: HPowGate: 20, _PauliX: 10, CZPowGate: 10, CCZPowGate: 1, MeasurementGate: 1

Experiment 8: $y^2 = x^3 + 1x + 6 \pmod{11}$

- **Target Private Key:** 7
- **Quantum Attack Success:** ?
- **Classical Computation Time:** 0.0000 seconds
- **Quantum Computation Time:** 0.0440 seconds
- **Quantum Circuit Specifications:**
    - Qubits Required: 6
    - Circuit Depth: 18 gates

    - Gate Composition: HPowGate: 20, _PauliX: 10, CZPowGate: 10, CCZPowGate: 1, MeasurementGate: 1

Experiment 9: $y^2 = x^3 + 4x + 4$ (mod 13)

- **Target Private Key:** 2
- **Quantum Attack Success:** ?
- **Classical Computation Time:** 0.0009 seconds
- **Quantum Computation Time:** 0.0490 seconds
- **Quantum Circuit Specifications:**
    - Qubits Required: 6
    - Circuit Depth: 18 gates
    - Gate Composition: HPowGate: 20, _PauliX: 10, CZPowGate: 10, CCZPowGate: 1, MeasurementGate: 1

Experiment 10: $y^2 = x^3 + 4x + 4$ (mod 13)

- **Target Private Key:** 6
- **Quantum Attack Success:** ?
- **Classical Computation Time:** 0.0000 seconds
- **Quantum Computation Time:** 0.0450 seconds
- **Quantum Circuit Specifications:**
    - Qubits Required: 6
    - Circuit Depth: 18 gates
    - Gate Composition: HPowGate: 20, _PauliX: 10, CZPowGate: 10, CCZPowGate: 1, MeasurementGate: 1

Experiment 11: $y^2 = x^3 + 4x + 4$ (mod 13)

- **Target Private Key:** 8
- **Quantum Attack Success:** ?
- **Classical Computation Time:** 0.0010 seconds

- **Quantum Computation Time:** 0.0450 seconds
- **Quantum Circuit Specifications:**
  - Qubits Required: 6
  - Circuit Depth: 18 gates
  - Gate Composition: HPowGate: 20, _PauliX: 10, CZPowGate: 10, CCZPowGate: 1, MeasurementGate: 1

4.2 Aggregate Performance Metrics

11

Total Experiments

9.09%

Quantum Success Rate

100%

Classical Success Rate

42.3ms

Avg Quantum Time

4.3 Detailed Statistical Analysis

Curve Family	Field Size	Experiments	Success Rate	Avg Quantum Time (ms)	Avg Circuit Qubits	Avg Circuit Depth
$y^2 = x^3 + 2x + 3$	F_5	2	50.0%	37.65	5	16
$y^2 = x^3 + 2x + 3$	F_7	3	0.0%	38.87	5	16
$y^2 = x^3 + 1x + 6$	F_{11}	3	0.0%	44.70	6	18
$y^2 = x^3 + 4x + 4$	F_{13}	3	0.0%	46.33	6	18

5. Analysis and Discussion

5.1 Quantum Algorithm Performance

The experimental results reveal significant insights into the current state of quantum cryptanalytic capabilities against ECC implementations. The overall quantum success rate of 9.09% (1 out of 11 experiments) demonstrates the nascent nature of practical quantum attacks against elliptic curve cryptography, even in controlled simulation environments.

5.2 Scalability Analysis

The relationship between field size and attack complexity is clearly demonstrated in our results. As the prime field size increases from F_5 to F_{13}, we observe:

- Increased quantum computation time (37.65ms to 46.33ms average)
- Higher qubit requirements (5 to 6 qubits)
- Greater circuit depth complexity (16 to 18 gates)
- Decreased success probability (50% to 0% for larger fields)

5.3 Circuit Architecture Analysis

The quantum circuit implementations demonstrate sophisticated gate architectures, utilizing Hadamard gates for superposition creation, Pauli-X gates for bit manipulation, controlled-Z gates for entanglement generation, and Toffoli gates (CCZ) for complex logical operations. The measurement gates provide the final state collapse necessary for result extraction.

5.4 Performance Comparison

The classical vs. quantum performance comparison reveals interesting dynamics. While classical methods maintain 100% success rates with sub-millisecond execution times, quantum approaches require significantly more computational resources (average 42.3ms) with substantially lower success rates. This disparity highlights the current limitations of quantum computing hardware and algorithm implementations.

6. Implications for Cryptographic Security

These experimental results provide crucial insights for the cryptographic community regarding the timeline and nature of the quantum threat to ECC. The low success rates observed in our experiments suggest that:

- Current quantum computing capabilities are insufficient for practical ECC attacks
- Significant advances in quantum error correction and gate fidelity are required

- The transition to post-quantum cryptography, while urgent, may have a longer timeline than initially anticipated
- Hybrid classical-quantum attacks may represent a more immediate threat vector

7. Conclusions and Future Work

This comprehensive experimental study provides empirical evidence for the current state of quantum cryptanalytic attacks against elliptic curve cryptography. Our findings demonstrate that while quantum algorithms possess theoretical advantages over classical methods, practical implementations face significant challenges in terms of success rates and computational overhead.

The 9.09% success rate observed across 11 systematic experiments indicates that quantum threats to ECC, while theoretically sound, remain practically limited by current quantum computing capabilities. However, the exponential improvement trajectory of quantum technologies suggests that this landscape will evolve rapidly.

Future Research Directions:

- Investigation of quantum error correction impacts on cryptanalytic success rates
- Analysis of hybrid classical-quantum attack methodologies
- Exploration of quantum attacks against larger field sizes (F_p where $p > 100$)
- Development of quantum-resistant ECC variants
- Real quantum hardware validation of simulation results