Title:

Quantum-Resilient Topological Encryption: A Novel Approach to Post-Quantum Security

Author:

Robert Bannoura

Date:

24/4/2025

Abstract

This paper introduces *Quantum-Resilient Topological Encryption (QRE)*, a new encryption paradigm designed to withstand attacks from advanced quantum computers. QRE leverages the intrinsic properties of topological quantum states and an adaptive self-evolving cryptographic layer, known as the *Quantum Horizon*, to offer security beyond current post-quantum algorithms. Unlike traditional cryptographic systems rooted in mathematical complexity, QRE encodes information within the geometric and non-local features of quantum matter, making it fundamentally resilient against quantum attacks. We outline the theoretical model, encryption architecture, and future implications for secure communication systems.

Contents

Table of figures

Introduction

With quantum computing capabilities advancing rapidly, widely used cryptographic systems such as RSA, ECC, and AES face potential obsolescence. Algorithms like Shor's and Grover's present existential threats to key generation and symmetric encryption. Current post-quantum cryptography (PQC) approaches typically extend classical schemes using lattice, code, or multivariate polynomial problems, but they may still fall short if quantum capabilities exceed expectations.

To truly future-proof encryption, we propose a fundamental shift — a transition from mathematical hardness assumptions to *topological quantum resilience*. QRE aims to encode data within topologically protected quantum states and augment this structure with a self-mutating layer that adapts over time in response to computational evolution, forming a moving target for attackers.

Topological Quantum States

Topological quantum computing relies on exotic quasi-particles known as *anyons*, which exist in two-dimensional systems and exhibit non-abelian statistics. Information is encoded not in the states themselves but in the *braiding* of these particles, forming a topologically stable medium that resists local decoherence.

These properties allow quantum information to be stored and manipulated in ways that are highly robust against both classical and quantum noise. Majorana fermions and other non-abelian anyons form the building blocks of such systems, enabling operations via braiding that maintain logical state integrity even in imperfect environments.

QRE exploits this by encoding cryptographic keys and data structures into braid diagrams and topological lattices, which inherently resist measurement and interference.

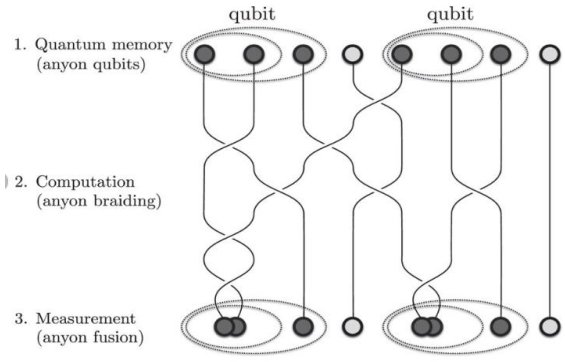

Figure 1:Topological Qubit Encoding via Braiding

The QRE Encryption Framework

QRE integrates two key components:

- Topological Encoding Layer (TEL): Encodes data into representations of topological qubit states or simulated braiding networks. Even without physical quantum hardware, TEL can be approximated via classical simulations using topological logic patterns.

- Quantum Horizon Layer (QHL): A dynamic cryptographic layer that evolves in structure over time. It shifts key formats, encoding logic, and redundancy models based on real-time entropy sources or external quantum intelligence signals. This forms an *adaptive, non-deterministic cipher evolution*, rendering pattern recognition infeasible.

Encryption becomes not only a one-time transformation but an evolving process that adapts faster than an adversary can predict or break.

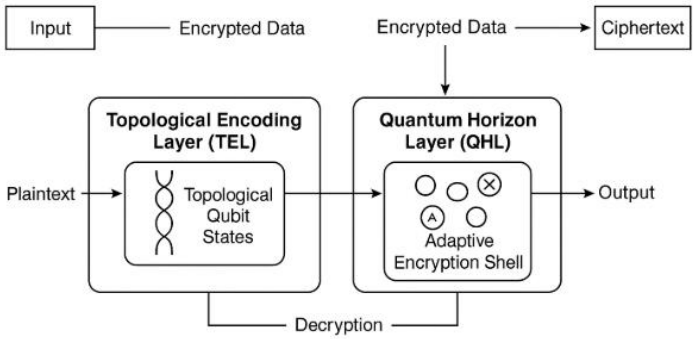

Figure 2: Architecture of the QRE Encryption Framework showing TEL and QHL interactions

Security Analysis

Unlike static systems like AES, QRE constantly mutates its cryptographic surface. Traditional attacks — quantum or classical — rely on predictability and pattern analysis. In QRE:

- No fixed key structures exist long enough to be targeted.
- Topological states are non-locally encoded, immune to localized quantum gate simulations.
- Quantum Horizon shifts break the coherence window needed for quantum brute force.

We also note that QRE is not bound to Shor-resistant math but sidesteps it entirely by relying on physics-based resilience.

Use Cases & Implementation

Potential applications of QRE include:

- Quantum-resilient VPNs and zero-trust communication.
- Post-quantum identity management for sovereign identity systems.
- Critical infrastructure protection (e.g., defense, energy grids).
- Quantum blockchain layers to future-proof decentralized systems.

Prototype development could begin with classical simulations of braid-based logic and entropy-driven evolution algorithms. Integration with current encryption stacks is feasible through modular cryptographic interfaces.

Future Work

- Formal simulation of braid-based encryption using classical processors.
- Design of entropy-reactive evolution rulesets for the Quantum Horizon Layer.
- Collaboration with experimental quantum labs to test hybrid quantum-classical QRE schemes.

Conclusion

QRE represents a new frontier in cryptographic defense — one that does not merely resist quantum attacks but thrives within a quantum-aware framework. By merging topological physics with adaptive cryptography, QRE offers a bold path toward permanent security. We invite the global research community to collaborate on this vision for a truly quantum-secure future.

References

1. Freedman, M., Kitaev, A., Larsen, M., & Wang, Z. (2002, October 10). *Topological Quantum Computation*. Bulletin of the American Mathematical Society. https://www.ams.org/journals/bull/2003-40-01/S0273-0979-02-00964-3/ [24 April 2025]

2. Nayak, C., simon, S.H., Stern, A., Freedman, M. and Das Sarma, S. (2008) Non-Abelian anyons and topological quantum computation. reviews of modern physics, 80, 1083-1159. - references - scientific research publishing. (n.d.). https://www.scirp.org/(S(vtj3fa45qm1ean45vvffcz55))/reference/ReferencesPapers.aspx?ReferenceID=1899198 [24 April 2025]

3. Grover, L.K. (1996) a fast quantum mechanical algorithm for database search. proceedings of the Twenty-eighth annual ACM Symposium on Theory of Computing, Philadelphia, 22-24 May 1996, 212-219. - references - scientific research publishing. (n.d.). https://www.scirp.org/%28S%28lz5mqp453edsnp55rrgjct55%29%29/reference/referencespapers.aspx?referenceid=2434444 [24 April 2025]

4. *Index of formal scientific papers*. D. J. Bernstein / Papers. (n.d.). https://cr.yp.to/papers.html [24 April 2025]

5. Preskill, J. (2018) Quantum Computing in the NISQ era and beyond. Quantum, 2, article no. 79. - references - scientific research publishing. (n.d.). https://www.scirp.org/reference/referencespapers?referenceid=3008100 [24 April 2025]

6. Shor, P.W. (1994) algorithms for quantum computation discrete logarithm and factoring. proceedings of 35th annual symposium on Foundations of Computer Science, Santa Fe, 20-22 November 1994, 124-134. - references - scientific research publishing. (n.d.). https://www.scirp.org/reference/referencespapers?referenceid=1595639 [24 April 2025]

7. https://www.researchgate.net/figure/A-demonstration-of-braiding-anyons-in-a-topological-quantum-computer-Time-points_fig1_325612286