

# TORUS Quantum Security Framework

## A Probabilistic Quantum Authentication Approach

*This work was developed as part of the XPRIZE Quantum Applications initiative and is presented here as a standalone research framework.*

**Author:** Virginie Guignard-Legros

**Affiliation:** ECOSYSTEM VLG World

**Contribution Type:** Applied Quantum Cybersecurity

**License Notice:**

**This document is distributed under the Apache License 2.0.**

### LICENSE NOTICE

This document is distributed under the Apache License 2.0.

This license applies to access, reading, reproduction, and distribution of the document.

However, implementation, deployment, or operational use of the systems described remains subject to the ECOSYSTEM VLG World Governance & Licensing Framework (VLG-WGL).

Any real-world activation requires prior authorization and compliance with the governance framework.

Independent validation may be conducted through authorized certification pathways.

### VERSION HISTORY

#### Version 1 – July 31, 2025

Initial framework definition.

#### Version 2 – August 2, 2025

Addition of “Additional Protection for Applied Cybersecurity Modules” and reinforcement of governance and licensing scope.

#### Version 3 – April 22, 2026

Introduction of structured separation between:

- TORUS 1 (Applied layer)
- TORUS 2 (Interpretative layer)

Clarification of:

- experimental vs conceptual distinction
- probabilistic framing of quantum advantage
- removal of absolute irreproducibility claims

# ABSTRACT

The TORUS Quantum Security Framework introduces a probabilistic approach to authentication based on parameterized quantum circuits and distribution-based verification.

Rather than relying on fixed credentials, TORUS models identity as a statistical signature emerging from repeated quantum circuit executions on NISQ devices. Authentication is performed by comparing observed output distributions to reference distributions using statistical distance metrics.

The framework is structured into two complementary layers:

- TORUS 1 (Applied Layer): an implementable quantum-classical authentication model based on measurable circuit outputs, statistical validation, and reproducible distributional signatures.
- TORUS 2 (Interpretative Layer): a conceptual framework that provides structured representations of quantum transformations, enabling analysis of system behavior in terms of stability, convergence, and transformation dynamics, without introducing new physical claims.

Simulations using Qiskit demonstrate stable and reproducible distributional signatures dependent on circuit structure and parameters. TORUS explores regimes where classical simulation becomes computationally expensive, without asserting absolute classical irreproducibility.

This approach proposes a shift from deterministic identity verification toward probabilistic coherence analysis, opening new directions in post-quantum cybersecurity.

# SUMMARY

<b>TORUS Quantum Security Framework</b>	<b>1</b>
<b>ABSTRACT</b>	<b>2</b>
<b>SUMMARY</b>	<b>3</b>
<b>1. INTRODUCTION</b>	<b>4</b>
<b>2. TORUS 1 - QUANTUM PROBABILISTIC AUTHENTICATION FRAMEWORK</b>	<b>5</b>
2.1 Formal Model	5
2.2 Authentication Protocol	5
2.3 Statistical Distance Metrics	5
2.4 Circuit Design Principles	6
2.5 Noise Considerations	6
2.6 Security Model	6
2.7 Experimental Validation	6
2.8 Classical Benchmarking	7
2.9 Limitations	7
<b>3. TORUS 2 - INTERPRETATIVE FRAMEWORK</b>	<b>7</b>
3.1 Positioning	7
3.2 Conceptual Mapping	7
3.3 Identity as Distributional Coherence	8
3.4 Symbolic Representation (Optional)	8
3.5 Applications	8
3.6 Functional Role of TORUS 2	8
<b>4. CONCLUSION</b>	<b>8</b>
<b>5. AUTHOR</b>	<b>9</b>
<b>6. COPYRIGHT &amp; LICENSING</b>	<b>9</b>

# 1. INTRODUCTION

Contemporary cybersecurity systems rely on deterministic authentication mechanisms such as passwords, cryptographic keys, and multi-factor authentication. These approaches assume computational hardness that may be challenged by quantum computing.

Quantum systems introduce inherent probabilistic behavior, noise sensitivity, and circuit-dependent dynamics that are not captured by classical security models.

The TORUS Quantum Security Framework proposes a shift from deterministic authentication toward probabilistic verification based on quantum circuit distributions.

Identity is no longer treated as a fixed credential but as a statistical pattern emerging from repeated quantum executions.

The framework is structured into:

- TORUS 1: applied implementation layer
- TORUS 2: interpretative conceptual layer

## 2. TORUS 1 - QUANTUM PROBABILISTIC AUTHENTICATION FRAMEWORK

### 2.1 Formal Model

Authentication is defined as a distribution-based verification process derived from parameterized quantum circuits.

Let  $C(k, \theta)$  be a quantum circuit where:

- $k$  = discrete circuit structure (gate sequence)
- $\theta$  = continuous parameters (rotation angles, phase shifts)

The circuit is executed  $N$  times, producing measurement outcomes:

$$X = \{x_1, x_2, \dots, x_N\}$$

From this, an empirical distribution  $P_{\text{obs}}$  is constructed.

A reference distribution  $P_{\text{ref}}$  is generated during enrollment.

Authentication is based on:

$$D(P_{\text{obs}}, P_{\text{ref}}) < \epsilon$$

where  $D$  is a statistical distance function and  $\epsilon$  a threshold.

### 2.2 Authentication Protocol

Enrollment:

1. Define circuit  $C(k, \theta)$
2. Execute  $N$  shots
3. Store  $P_{\text{ref}}$

Verification:

1. Execute same circuit
2. Compute  $P_{\text{obs}}$
3. Compare distributions
4. Accept if within threshold  $\epsilon$

### 2.3 Statistical Distance Metrics

Possible metrics include:

- Kullback–Leibler divergence
- Jensen–Shannon divergence (preferred in NISQ)
- Total variation distance
- Quantum fidelity (state-based models)

## 2.4 Circuit Design Principles

Key elements:

- Superposition (Hadamard)
- Phase encoding (S, T, RZ)
- Parametric rotations (RX, RZ)
- Entanglement (CNOT, CCX)
- Controlled circuit depth (NISQ constraints)

These elements define a probabilistic signature space.

## 2.5 Noise Considerations

Noise is treated as a contributing factor, not only an error source.

- Enhances distribution variability
- Must remain within stable bounds
- Requires calibration for reproducibility

Noise increases signature richness but does not guarantee security alone.

## 2.6 Security Model

Threat models include:

- Classical simulation attacks
- Statistical learning attacks
- Replay attacks

Security relies on:

- circuit dependency
- distribution complexity
- sensitivity to parameter variations

TORUS security is probabilistic, not absolute.

### Additional Considerations:

The probabilistic nature of TORUS introduces inherent resistance to static credential attacks, as identity is not represented by a fixed value but by a distributional pattern.

Attackers must reproduce not only outputs but the full statistical structure of circuit-dependent distributions, which becomes increasingly complex as circuit depth and parameterization increase.

This shifts the attack surface from deterministic key extraction to high-dimensional probabilistic replication.

## 2.7 Experimental Validation

Simulations using Qiskit demonstrate:

- stable distribution patterns
- reproducible probabilistic signatures
- sensitivity to circuit configuration

Parameters:

- backend: QASM simulator
- shots: 1024

Findings:

- distributions are consistent per circuit
- distinct circuits produce separable signatures

## 2.8 Classical Benchmarking

Classical systems can approximate small circuits but:

- struggle with full distribution matching
- scale poorly with circuit complexity
- cannot efficiently reproduce interference patterns

TORUS does not claim absolute irreproducibility, but computational inefficiency in classical regimes.

## 2.9 Limitations

- NISQ hardware constraints
- noise variability
- lack of formal cryptographic proofs
- scalability not fully validated
- simulator vs hardware gap

# 3. TORUS 2 - INTERPRETATIVE FRAMEWORK

## 3.1 Positioning

TORUS 2 is a conceptual layer that does not introduce physical claims.

It provides interpretative structures for understanding quantum circuit behavior.

## 3.2 Conceptual Mapping

- phase rotation → vortex-like transformation
- interference → bifurcation dynamics
- convergence → stability pattern

These are metaphors for system behavior, not physical assertions.

### 3.3 Identity as Distributional Coherence

Identity is defined as:

a stable probabilistic distribution across repeated executions.

- stable distribution = valid identity
- divergence = mismatch or transformation

### 3.4 Symbolic Representation (Optional)

- $|0\rangle \rightarrow$  Plumbum (Pb)
- $|1\rangle \rightarrow$  Aurum (Au)
- $|X\rangle \rightarrow$  convergence state

These are conceptual labels only.

### 3.5 Applications

- quantum hardware authentication
- secure access systems
- hardware fingerprinting
- high-trust verification environments

### 3.6 Functional Role of TORUS 2

While TORUS 2 does not introduce new physical models, it plays a functional role in the framework by:

- providing interpretative tools to analyze probabilistic behaviors observed in TORUS 1
- supporting system design through conceptual mapping of transformation dynamics
- enabling reasoning about stability, convergence, and sensitivity in distribution-based authentication systems

TORUS 2 acts as a bridge between measurable quantum outputs and higher-level system understanding, supporting both research exploration and architectural design decisions.

## 4. CONCLUSION

TORUS introduces a probabilistic authentication framework based on quantum circuit distributions, shifting identity verification from deterministic credentials to statistical coherence analysis.

By combining an implementable quantum-classical layer (TORUS 1) with an interpretative framework (TORUS 2), the system provides both operational mechanisms and conceptual tools for understanding distribution-based security models.

Rather than claiming absolute quantum advantage, TORUS explores practical regimes where probabilistic structures, circuit dependency, and distributional complexity create new forms of security challenges for classical systems.

This approach opens a pathway toward adaptive, distribution-based cybersecurity systems aligned with the constraints and opportunities of NISQ-era quantum technologies.



## 5. AUTHOR

Author:

Virginie Guignard Legros  
ECOSYSTEM VLG World — Framework Architecture & Conceptual Design

Acknowledgements:

The author acknowledges Mamadou Niambele for continuous support throughout the development of this work.

Scientific Review:

Bruno Prévost, THALES  
Vice President, IS/IT Group Chief Technology Officer (CTO)  
Vice President Artificial Intelligence  
Digital Transformation · Cybersecurity · Sovereignty · Quantum · Space  
Collective Intelligence & Organizational Transformation  
- Quantum Review & Technical Feedback

## 6. COPYRIGHT & LICENSING

### Copyright & Ownership

All concepts, frameworks, systems, architectures, processes, and associated materials presented within the TORUS Quantum Security Framework are the intellectual property of Virginie Guignard Legros, developed within ECOSYSTEM VLG World.

Authorship must remain explicitly attributed and preserved in all contexts of access, citation, and reference.

Ownership of the underlying structures, transformation logics, and system architectures remains fully defined and protected.

### Licensing Regime

This document is published under the Apache License 2.0, which governs:

- access
- reading
- reproduction
- distribution

This license applies strictly to the document as a readable and shareable resource.

## Scope Limitation

The Apache License does not extend to:

- implementation of the systems described
- deployment of associated architectures
- operational use of processes or transformation logics

Access to this document does not grant any rights for real-world activation.

## Governance & Activation

The Governance & Licensing Framework is implemented through the VLG World Governance License (VLG-WGL).

All implementation, deployment, or operational use of systems, architectures, or processes described in this document is governed by this framework.

**Any real-world activation requires:**

- prior authorization
- validation within the 3Q™ framework
- registration within the Active Blue system

## Controlled Use

Depending on context, certain uses may fall under the Controlled Collaborative License (VLG-CCL), particularly for:

- research
- experimentation
- evaluation

Such use does not grant rights for independent deployment or commercialization.

## Principle

Access to knowledge is open.

Ownership remains defined.

Activation is governed.

Independent validation may be conducted through authorized certification pathways.