

TORUS Quantum Security Framework

Une approche probabiliste de l'authentification quantique

Ce travail a été développé dans le cadre de l'initiative XPRIZE Quantum Applications et est présenté ici comme un cadre de recherche autonome.

Auteur: Virginie Guignard-Legros

Affiliation: ECOSYSTEM VLG World

Contribution Type: Applied Quantum Cybersecurity / Cybersécurité quantique appliquée

Mention de licence :

Ce document est distribué sous licence Apache 2.0.

MENTION DE LICENCE :

Ce document est distribué sous licence Apache 2.0.

Cette licence s'applique à l'accès, à la lecture, à la reproduction et à la distribution du document.

Cependant, la mise en œuvre, le déploiement ou l'usage opérationnel des systèmes décrits restent soumis au cadre de gouvernance et de licences de ECOSYSTEM VLG World (VLG-WGL).

Toute activation dans le monde réel requiert une autorisation préalable ainsi que le respect du cadre de gouvernance.

Une validation indépendante peut être réalisée via des mécanismes de certification autorisés.

HISTORIQUE DES VERSIONS

Version 1 – 31 juillet 2025

Définition initiale du cadre (XPRIZE Quantum Applications).

Version 2 – 2 août 2025

Ajout de la section « Additional Protection for Applied Cybersecurity Modules » et renforcement du périmètre de gouvernance et de licence.

Version 3 – 22 avril 2026

Introduction d'une séparation structurée entre :

TORUS 1 (couche appliquée)

TORUS 2 (couche interprétative)

Clarification de :

- la distinction entre expérimental et conceptuel
- le cadrage probabiliste de l'avantage quantique
- la suppression des affirmations d'irréproductibilité absolue

RESUME

Le TORUS Quantum Security Framework introduit une approche probabiliste de l'authentification fondée sur des circuits quantiques paramétrés et une vérification basée sur des distributions. Plutôt que de reposer sur des identifiants fixes, TORUS modélise l'identité comme une signature statistique émergeant d'exécutions répétées de circuits quantiques sur des dispositifs NISQ. L'authentification est réalisée en comparant les distributions de sortie observées à des distributions de référence à l'aide de métriques de distance statistique.

Le cadre est structuré en deux couches complémentaires :

- TORUS 1 (couche appliquée) : un modèle d'authentification quantique-classique implémentable, fondé sur des sorties mesurables de circuits, une validation statistique et des signatures distributionnelles reproductibles.
- TORUS 2 (couche interprétative) : un cadre conceptuel permettant de représenter et d'analyser les transformations quantiques en termes de stabilité, de convergence et de dynamique de transformation, sans introduire de nouvelles hypothèses physiques.

Des simulations réalisées avec Qiskit démontrent l'existence de signatures distributionnelles stables et reproductibles, dépendantes de la structure et des paramètres des circuits. TORUS explore des régimes dans lesquels la simulation classique devient coûteuse, sans affirmer une irréductibilité absolue.

Cette approche propose un passage d'une vérification déterministe de l'identité à une analyse de cohérence probabiliste, ouvrant de nouvelles perspectives en cybersécurité post-quantique.

ABSTRACT (english)

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

TORUS Quantum Security Framework	1
RESUME	2
SUMMARY	3
1. INTRODUCTION	4
2. TORUS 1 - CADRE D'AUTHENTIFICATION QUANTIQUE PROBABILISTE	5
2.1 Modèle formel	5
2.2 Protocole d'authentification	5
2.3 Métriques de distance statistique	5
2.4 Principes de conception des circuits	6
2.5 Considérations sur le bruit	6
2.6 Modèle de sécurité	6
2.7 Validation expérimentale	7
2.8 Benchmarking classique	7
2.9 Limitations	7
3. TORUS 2 - CADRE INTERPRÉTATIF	7
3.1 Positionnement	7
3.2 Cartographie conceptuelle	7
3.3 Identité comme cohérence distributionnelle	8
3.4 Représentation symbolique (optionnelle)	8
3.6 Rôle fonctionnel de TORUS 2	8
4. CONCLUSION	8
5. AUTEUR	9
6. COPYRIGHT & LICENCES	9

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 - CADRE D'AUTHENTIFICATION QUANTIQUE PROBABILISTE

2.1 Modèle formel

L'authentification est définie comme un processus de vérification basé sur des distributions, dérivé de circuits quantiques paramétrés.

Soit $C(k, \theta)$ un circuit quantique où :

k = structure discrète du circuit (séquence de portes)

θ = paramètres continus (angles de rotation, déphasages)

Le circuit est exécuté N fois, produisant des résultats de mesure :

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

À partir de cela, une distribution empirique P_{obs} est construite.

Une distribution de référence P_{ref} est générée lors de l'enrôlement.

L'authentification repose sur :

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

où D est une fonction de distance statistique et ϵ un seuil.

2.2 Protocole d'authentification

Enrôlement :

1. Définir le circuit $C(k, \theta)$
2. Exécuter N tirs (shots)
3. Stocker P_{ref}

Vérification :

1. Exécuter le même circuit
2. Calculer P_{obs}
3. Comparer les distributions
4. Accepter si inférieur au seuil ϵ

2.3 Métriques de distance statistique

Les métriques possibles incluent :

- Divergence de Kullback–Leibler
- Divergence de Jensen–Shannon (préférée en NISQ)
- Distance de variation totale
- Fidélité quantique (modèles basés sur les états)

2.4 Principes de conception des circuits

Éléments clés :

- Superposition (Hadamard)
- Encodage de phase (S, T, RZ)
- Rotations paramétriques (RX, RZ)
- Intrication (CNOT, CCX)
- Profondeur de circuit contrôlée (contraintes NISQ)

Ces éléments définissent un espace de signature probabiliste.

2.5 Considérations sur le bruit

Le bruit est considéré comme un facteur contributif, et non uniquement comme une source d'erreur.

- Augmente la variabilité des distributions
- Doit rester dans des limites stables
- Nécessite une calibration pour assurer la reproductibilité

Le bruit enrichit la signature mais ne garantit pas à lui seul la sécurité.

2.6 Modèle de sécurité

Les modèles de menace incluent :

- Attaques par simulation classique
- Attaques par apprentissage statistique
- Attaques par rejeu

La sécurité repose sur :

- la dépendance au circuit
- la complexité des distributions
- la sensibilité aux variations des paramètres

La sécurité de TORUS est probabiliste, et non absolue.

Considérations complémentaires :

La nature probabiliste de TORUS introduit une résistance intrinsèque aux attaques basées sur des identifiants statiques, dans la mesure où l'identité n'est pas représentée par une valeur fixe mais par un motif distributionnel.

Un attaquant doit reproduire non seulement les sorties, mais l'ensemble de la structure statistique des distributions dépendantes du circuit, ce qui devient de plus en plus complexe à mesure que la profondeur des circuits et leur paramétrisation augmentent.

Cela déplace la surface d'attaque d'une extraction déterministe de clé vers une reproduction probabiliste dans un espace de grande dimension.

2.7 Validation expérimentale

Des simulations utilisant Qiskit démontrent :

- des motifs de distribution stables
- des signatures probabilistes reproductibles
- une sensibilité à la configuration des circuits

Paramètres :

- backend : simulateur QASM
- shots : 1024

Résultats :

- les distributions sont cohérentes pour un même circuit
- des circuits distincts produisent des signatures séparables

2.8 Benchmarking classique

Les systèmes classiques peuvent approximer de petits circuits mais :

- éprouvent des difficultés à reproduire l'ensemble des distributions
- passent difficilement à l'échelle avec la complexité des circuits
- ne peuvent pas reproduire efficacement les motifs d'interférence

TORUS ne revendique pas une irréproductibilité absolue, mais une inefficacité computationnelle dans les régimes classiques.

2.9 Limitations

- Contraintes du matériel NISQ
- Variabilité du bruit
- Absence de preuves cryptographiques formelles
- Scalabilité non entièrement validée
- Écart entre simulateur et matériel réel

3. TORUS 2 - CADRE INTERPRÉTATIF

3.1 Positionnement

TORUS 2 est une couche conceptuelle qui n'introduit pas de nouvelles hypothèses physiques.

Elle fournit des structures d'interprétation pour comprendre le comportement des circuits quantiques.

3.2 Cartographie conceptuelle

- rotation de phase → transformation de type vortex
- interférence → dynamique de bifurcation
- convergence → motif de stabilité

Ces éléments constituent des métaphores du comportement du système, et non des affirmations physiques.

3.3 Identité comme cohérence distributionnelle

L'identité est définie comme :

une distribution probabiliste stable à travers des exécutions répétées.

- distribution stable = identité valide
- divergence = incohérence ou transformation

3.4 Représentation symbolique (optionnelle)

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

Ces éléments constituent uniquement des labels conceptuels.

3.5 Applications

- authentification de matériel quantique
- systèmes d'accès sécurisés
- empreinte matérielle (hardware fingerprinting)
- environnements de vérification à haute confiance

3.6 Rôle fonctionnel de TORUS 2

Bien que TORUS 2 n'introduise pas de nouveaux modèles physiques, il joue un rôle fonctionnel dans le cadre en :

- fournissant des outils d'interprétation pour analyser les comportements probabilistes observés dans TORUS 1
- soutenant la conception des systèmes via une cartographie conceptuelle des dynamiques de transformation
- permettant de raisonner en termes de stabilité, de convergence et de sensibilité dans les systèmes d'authentification basés sur des distributions

TORUS 2 agit comme un pont entre les sorties quantiques mesurables et une compréhension de niveau supérieur du système, au service à la fois de la recherche et de la conception architecturale.

4. CONCLUSION

TORUS propose un cadre d'authentification probabiliste fondé sur les distributions issues de circuits quantiques, en remplaçant les identifiants déterministes par une analyse de cohérence statistique. En combinant une couche implémentable (TORUS 1) et un cadre interprétatif (TORUS 2), le système offre à la fois des mécanismes opérationnels et des outils de compréhension des modèles de sécurité basés sur des distributions.

Sans revendiquer d'avantage quantique absolu, TORUS explore des régimes dans lesquels la complexité probabiliste, la dépendance aux circuits et la structure des distributions introduisent de nouveaux défis pour les systèmes classiques.

Cette approche ouvre une voie vers des systèmes de cybersécurité adaptatifs, fondés sur des distributions, en cohérence avec les contraintes et les opportunités de l'ère NISQ.

5. AUTEUR

Auteur :

Virginie Guignard Legros
ECOSYSTEM VLG World — Architecture du cadre & conception conceptuelle

Remerciements :

L'auteure remercie Mamadou Niamele pour son soutien continu tout au long du développement de ce travail.

Relecture scientifique :

Bruno Prévost, THALES
Vice-président, Directeur technique (CTO) du groupe IS/IT
Vice-président Intelligence Artificielle
Transformation digitale · Cybersécurité · Souveraineté · Quantique · Spatial
Intelligence collective & transformation organisationnelle
– Revue quantique & retours techniques

6. COPYRIGHT & LICENCES

Droits d'auteur et propriété

L'ensemble des concepts, cadres, systèmes, architectures, processus et matériaux associés présentés dans le TORUS Quantum Security Framework constitue la propriété intellectuelle de Virginie Guignard Legros, développée au sein de ECOSYSTEM VLG World.

L'attribution de l'auteur doit être explicitement maintenue et préservée dans tous les contextes d'accès, de citation et de référence.

La propriété des structures sous-jacentes, des logiques de transformation et des architectures systèmes demeure pleinement définie et protégée.

Régime de licence

Ce document est publié sous licence Apache 2.0, qui régit :

- l'accès
- la lecture
- la reproduction
- la distribution

Cette licence s'applique strictement au document en tant que ressource lisible et partageable.

Limitation du périmètre

La licence Apache ne s'étend pas à :

- la mise en œuvre des systèmes décrits
- le déploiement des architectures associées
- l'usage opérationnel des processus ou des logiques de transformation

L'accès à ce document ne confère aucun droit d'activation dans le monde réel.

Gouvernance et activation

Le cadre de gouvernance et de licences est mis en œuvre à travers la VLG World Governance License (VLG-WGL).

Toute mise en œuvre, tout déploiement ou tout usage opérationnel des systèmes, architectures ou processus décrits dans ce document est régi par ce cadre.

Toute activation dans le monde réel requiert :

- une autorisation préalable
- une validation dans le cadre du système 3Q™
- un enregistrement dans le système Active Blue

Usage contrôlé

Selon le contexte, certains usages peuvent relever de la Controlled Collaborative License (VLG-CCL), notamment pour :

- la recherche
- l'expérimentation
- l'évaluation

Ces usages ne confèrent aucun droit de déploiement indépendant ni de commercialisation.

Principe

L'accès à la connaissance est ouvert.

La propriété demeure définie.

L'activation est gouvernée.

Une validation indépendante peut être réalisée via des mécanismes de certification autorisés.