World Journal of Advanced Research and Reviews
eISSN: 2581-9615 CODEN (USA): WJARAI
Cross Ref DOI: 10.30574/wjarr
Journal homepage: https://wjarr.com/

(RESEARCH ARTICLE)

Check for updates

Quantum-Resistant Key Generation Using QBLH Geometric Structures and Tetrahedral Trinary Encoding: A Novel Approach in Post-Quantum Cryptography

Andris lukss *

Independent researcher, Canberra institute technology, Australia.

World Journal of Advanced Research and Reviews, 2025, 27(02), 1532-1542

Publication history: Received on 13 July 2025; revised on 18 August; accepted on 21 August 2025

Article DOI: https://doi.org/10.30574/wjarr.2025.27.2.3017

Abstract

The dawn of the disruptive quantum computing scenario marks a serious threat to the existence of traditional cryptosystems. With laws such as Shor's, capable of factoring large integers in polynomial time, and Grover's, able to speed up brute-force key searches, these attacks make conventional public-key infrastructures increasingly vulnerable, whereas even symmetric ciphers lose good measure of their strength. In this article, we focus on an elaborative description of a patented method for quantum-secure key generation, wherein Qabbalah (QBLH) complexity is utilized in the geometric-symbolic realm, in conjunction with magic number squares, phi/pi coordinate weighting, and tetrahedral trinary state encoding. The proposed system of TriGate QBLH Quantum-Safe Encryption converts seed inputs to multidimensional keys that resist linear algebraic attacks owing to non-linear permutations, irrational constant weighting, and topological complexity. Normally, pseudo-random number generators spatialize entropy in Euclidean geometry, as opposed to the present technique that places entropy in a completely non-Euclidean domain, where classical as well as quantum adversaries find it hard to traverse. We describe the method in detail, present its benefits over lattice- and hash-based post-quantum schemes, and walk through an example of its implementation. Consideration is also given to its potential integration with PQC standards, blockchain authentication, and decentralized finance applications. The system fuses symbolic mathematics, such as the 231 Gates of QBLH, with trinary logic mapped onto tetrahedral states to not only create encryption keys but also verifiable geometric signatures. This represents a paradigm shift toward geometric cryptography, which may be a viable method to realize scalable and trustworthy digital infrastructure in a quantum-threatened environment.

Keywords: Post-Quantum Cryptography; Quantum-Resistant Key Generation; QBLH Geometric Structures; Tetrahedral Trinary Encoding; Lattice-Based Cryptography; Secure Key Exchange

1. Introduction

The advent of quantum computing has presented tremendous risks to conventional cryptography, especially public-key systems like RSA and ECC, whose security hinges on the ability to factorize huge numbers or compute discrete logarithms—tasks that scalable quantum machines theoretically can accomplish by use of Shor's algorithm. On the other hand, Grover's algorithm decreases the effective security level for symmetric ciphers, showing how all of our existing digital infrastructure is under threat (NIST, 2022; Gee, 2024).

Post-Quantum Cryptography schemes intend to mitigate these threats via lattice, code, multivariate, and hash-based schemes. Still, these algorithms are on very shaky grounds for they are algebraic in nature and are basically allied to pseudo-random number generators that open up the possibility of further exploits (Gee & Lukss, Draft 2025).

* Corresponding author: Andris lukss

Symbolic and geometric cryptography provides a fundamentally different outlook, whereby keys get embedded in multidimensional and topological spaces. This is how the TriGate QBLH Quantum-Safe Encryption System works: it combines Qabbalistic 231 Gates permutations, magic squares weighted by irrational constants (ϕ, π), and tetrahedral trinary encoding; keys are realized as both cryptographic bitstrings and geometric signatures, thereby providing a dual layer of entropy subject to neither algebraic nor quantum attacks (Sefer Yetzirah, 2004; Gee, 2024).

By creating multidimensional keys that cannot be reduced by any conventional linear or polynomial approach, symbolic elements combined with trinary-state logic create a mechanism of key generation resistant to reduction. It furthers the establishment of blockchain wallets, quantum cryptocurrencies, as well as IoT authentication, and by doing so, it defends against attacks posed by algorithms of both Shor and Grover. Providing the alternative landscapes for post-quantum cryptography along with a sustainable way forward in a post-quantum era, the TriGate will therefore work alongside PQC.

1.1. Challenges in Quantum-Resistant Cryptography

While quantum technologies appear promising, they bring about an urgent requirement for secure cryptographic methods to be resistant to adversaries using quantum computers. The classical cryptosystems, namely RSA and Elliptic Curve Cryptography (ECC), buttress their security by assuming the underlying number-theoretic problems to be very hard to solve on conventional machines. However, with Shor's algorithm, integer factorization and discrete logarithms can be solved in polynomial time on a quantum computer, leaving such widely deployed systems lacking any semblance of security (NIST, 2022).

In response to such threats, Post-Quantum Cryptography (PQC) has sprung into existence-the name given to cryptography that will provide algorithms intractable for both classical and quantum adversaries. Among the most prominent candidates are lattice-based algorithms like CRYSTALS-Kyber and Dilithium, code-based algorithms such as Classic McEliece, multivariate polynomial schemes, and hash-based schemes such as SPHINCS+ (NIST, 2022). Candidates of these schemes are essentially being standardized for federal and commercial use.

Nevertheless, and despite their promises, PQC algorithms dramatis fall short in many respects. The most evident of all concerns regards the fact that strong reliance is placed on pseudo-random number generators (PRNGs) for the generation of cryptographic key material, resulting in incidents of entropy weakness or distributions skewed in certain cases (Gee & Lukss, Draft 2025). Secondly, implementations of PQC still remain vulnerable to certain side-channel attacks, such as timing, power, and electromagnetic leakages, and these become even stronger in the real world, where adversaries capitalize on implementation flaws rather than pure mathematical weaknesses. Key generation and entropy sources remain the weakest links in PQC.

Following geometric and symbolic cryptography, complexity is not only posed by algebraic hardness but also by embedding cryptographic structures in non-Euclidean spaces and topological networks. These topological schemes target producing key materials which cannot be reduced via linear algebraic methods, thereby rendering the superposition- entanglement based attack strategies inefficient.2.2 Symbolic and Geometric Approaches

Historically, cryptography operated on binary logic and algebraic computation. On the other hand, symbolic and geometric mechanisms use different mathematical fields to generate some degree of complexity. Early studies in trinary logic, spin-based computation, and topological encoding revealed that bypassing binary logic could enhance resistance to certain classes of attacks (Gee, 2024).

Especially multi-valued and trinary logic systems instantiate more states per one computational unit, keyspace thus expands exponentially in comparison to binary systems. To cite, a binary system can ever produce states 2^n for an n-length sequence, whereas a trinary system can produce 3^n, making brute-force search so difficult that even Grover's quadratic speedup cannot offer big leads, (Gee, 2024). Spin-based models of quantum computing, which include qutrit systems, essentially investigate similar multi-valued encoding techniques.

In cryptography, the geometric ways try to embed entropy into structures such that the algebraic flattening is difficult. For instance, mapping given data into higher dimensional lattices, polytopes, or tessellations can provide security properties that are not at least alone based on a hardness assumption;

1.2. Foundations in QBLH and Sacred Geometry

The TriGate QBLH Quantum-Safe Encryption System stems from symbolic mathematics and sacred geometry, that is, Qabbalistic structures as described in the Sefer Yetzirah (2004). In this ancient text, 231 "Gates" correspond to

permutations of Hebrew letters that make up a web of symbolic transformations. Lacking a descriptive cryptographic model for gates, their structure can be modeled as a graph, which follows from possibilities of transformation among its nodes representing states. Thus, it provides an underpinning combinatorial framework for permutation-based encryption, presenting mathematically more meaningful alternatives to linear key derivation.

Magic squares complement QBLH; these ancient-mathematical concoctions are arrangements in which the sums of rows, columns, and diagonals all must equal some constant value. In cryptography, the magic squares present the layer of symmetry and balance to lessen any chance of biased key distribution. These mappings combine with irrational weightings based on the golden ratio ($\phi \approx 1.618$) and on pi ($\pi \approx 3.14159$) to yield coordinate systems with built-in algebraic resistance. By spatializing the seed inputs within a magic square by phi/pi-weighted coordinates, TriGate effectively embeds entropy in this structure, which cannot be further trimmed down by linear algebra or polynomial reduction.

Tetrahedral encoding introduces a further refinement by extending binary logic into both its trinary and rotational states. A regular tetrahedron with its four triangular faces is used to geometrically represent logical states:

- Open (O) – analogous to binary 0
- Closed (C) – that is, binary 1
- Right (R) – clockwise spin state
- Left (L) – counterclockwise spin state

These four states may be combined into rotational paths over a tetrahedral surface to form a highly compact and non-linear key representation. In quantum implementations, such states could be realized as qutrits or as pairs of qubits, preserving their ability to interact with quantum hardware, yet unable to be classically reduced (Gee, 2024).

In quantum cryptocurrency, similar ideas have been used in applying ternary gates through tetrahedral tessellations towards the protection of blockchain (Gee, 2024). Building upon that premise, the TriGate system, in turn, interlaces QBLH's symbolic network, magic square weighting, and tetrahedral trinary encoding to form a single key generation mechanism. By imparting entropy into spherical topologies and spinor dynamics, it creates topological barriers incapable of being crossed efficiently by classical or quantum adversaries.

Table 1 Comparison of Conventional PQC Methods vs. TriGate QBLH Features

Feature	**Lattice-Based PQC (e.g., Kyber)**	**Hash-Based PQC (e.g., SPHINCS+)**	**Code-Based PQC (e.g., McEliece)**	**TriGate QBLH**
Security Basis	Algebraic hardness (LWE, RLWE)	Hash collision resistance	Linear code decoding hardness	Symbolic- and geometric-topology (QBLH, magic squares, tetrahedral encoding)
Key Generation	PRNG + Gaussian sampling	PRNG + hash expansion	PRNG + error vectors	Phi/Pi weight-magic squares; 231 Gates permutations
Attack Surface	Algebraic reductions, lattice sieving	Hash preimage/collision search	Decoding + structural leakage	Topological complexity, trinary states, and non-linear mapping

1.2.1. Foundations in QBLH and Geometric Cryptography

The TriGate QBLH system describes the hybrid methodology consisting of symbolic mathematics, sacred geometry, and modern cryptograhpy for key generation that is resistant to algebraic and quantum attacks. Entropy is embedded into complex multidimensional symbolic and geometric structures, passing beyond the ordinary linear approaches.

QBLH Structures and the 231 Gates

Taken from the Qabbalistic Sefer Yetzirah, 231 Gates in QBLH represent all two-letter Hebrew combinations. Generated as a directed graph, gates produce high-entropy sequences through permutation paths and thus provide non-linear complexity much beyond that received by the conventional pseudo-random generators.

Magic Squares and Symmetry in Cryptography

Magic squares weighted by irrational constants-the golden ratio ϕ or π-make these coordinate systems non-algebraically reducible. Acting like spatial entropy matrices, they convey those non-linear relationships that are meant to create more-efficient key contribution and better protection in cryptography applications.

Tetrahedral Encoding and Trinary Logic

The system thus implements a form of tetrahedral encoding to represent the four stares (Open, Closed, Right, and Left) as trits. Such trinary logic gives exponential growth to the state space and serves to inscribe data into rotational paths across the tetrahedron, thus providing immunity against linear algebra-based attacks.

Integration of QBLH, Magic Squares, and Tetrahedral Logic

The pride of TriGate is that it offers a layered approach consisting of permutation QBLH gates, magic squares weighted by irrational numbers, and tetrahedral trinary encoding. This leads to a multidimensional entropy engine, which produces digital keys and geometric signatures for quantum-safe authentication.

Related Works

In fact, research in geometric cryptography along with that in quantum blockchain end up supporting non-linear, multidimensional systems. Thus, trinary switch-gates, tetrahedral tessellations, and topological encryption frameworks offer a better resilience against classical and quantum attacks, thereby legitimizing the TriGate approach.

2. Methodology

2.1. TriGate QBLH Key Generation

The TriGate QBLH system encrypts through a multistage pipeline that takes in an entropy-rich seed and outputs a quantum-resistant key. While other cryptographic systems rely on algebraic hardness assumptions alone, TriGate QBLH combines symbolic structures (QBLH 231 Gates), geometric embeddings (magic squares weighted with irrational constants), and trinary topologies (tetrahedral encoding). The following sections describe the steps involved in this methodology.

2.1.1. Seed Input Normalization

The process begins with a seed input. The seed input may come from varied entropy sources, such as:

- User passphrases (alphanumeric strings)
- Biometric hashes (fingerprint, iris scan, voice print)
- Quantum random number generator (QRNG) outputs

The objective shall be to first ensure that the seed achieves its high entropy and uniform distribution before it can be taken further for transformation. For instance, the passphrase TRIGATE2025 is converted to ASCII and numerical characters. Each character is mapped to some integer value and concatenated into a sequence of numbers. The sequence may, however, be strengthened by applying, for example, a SHA3-512 hash or another NIST-approved digest before proceeding with further steps [Worrall et al., 2025; Veale, 2024].

Entropy becomes significant because weak or easily guessed seeds are susceptible to brute-force or dictionary attacks—even in quantum resistance environments [Soyege et al., 2024]. TriGate achieves such unpredictability at that basic level with the QRNGs, never inherently depending upon patented deterministic pseudo-random number generators that have been proved to weaken classical cryptography [Watanabe, 2020].

2.2. Magic Square Mapping Using Phi/Pi Weighting

The normalized numeric seed then finds its place into one of the sizes of magic squares chosen as per the required key length and entropy density. Typically 3×3, 5×5, or 7×7 grids may be made use of. The special property of magic squares is that sums across all rows, columns, and main diagonals are equal to the same number. In peradventure one changes terminology: the property symmetrically and redundantly shares values, preventing localized entropy collapse[Palka, 2020].

To add further complexity, the magic square's cells are weighted by means of irrational mathematical constants:

$$\Phi= \frac{1 + \sqrt{5}}{2} \approx 1.61803 \qquad \pi \approx 3.14159$$

If a seed value S is located at coordinates (i, j), the weighted value is defined as:

$$V(i, j) = S \times (\Phi^i \times \pi^j).$$

This weighting scheme embeds the seed inside an irrational coordinate system, generating a geometrical key space not amenable to algebraic reduction. In a manner of speaking, these create non-repeating distributions akin to those found in quasi-crystal structures, which resist factorization and cannot be easily mapped by polynomial-time algorithms [Farhana et al., 2025].

Figure 2. Flowchart of TriGate QBLH key generation pipeline (seed → normalization → magic square embedding → QBLH permutation → trinary encoding → key extraction).

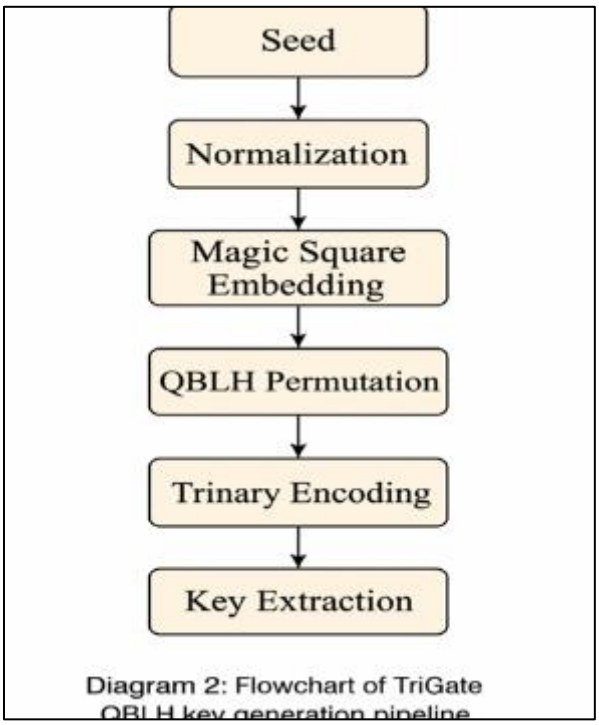

Figure 1 Flowchart of TriGate QBLH key generation pipeline

3. QBLH 231 Gate Permutation

The weighted magic square is the basic entrance into the QBLH 231 Gates network. This symbolic framework, derived from the ancient Sefer Yetzirah, represents 231 permutations of Hebrew letters and forms the directed graph of states and transformations. In TriGate, every magic square cell is turned into a node in such a graph, and the traversal proceeds according to deterministic or pseudo-random rules seeded by the input sequence.

As each step in the traversal is generated, a trinary state is created:

Open (O) ≡ binary 0

Closed (C) ≡ binary 1

Right (R) ≡ clockwise spin

Left (L) ≡ counterclockwise spin

Contrary to binary, the trinary encodings hold directional and topological information, thus collision-resistively and topologically embedding rotation and orientation into the sequence. Each traversal path leads to a combinatorial explosion of possible outputs. Grover's algorithm, with its quantum search applications, provides only quadratic speed-up for unstructured searches, whereas this topological expansion outruns quantum search efficiencies [Mekdad et al., 2025].

Furthermore, the symbolic resonance of the 231 Gates ensures the outputs are not only non-linear but also non-reversible without full knowledge of the seed and path of traversal. This assures that the systems follow modern cryptographic principles of forward secrecy and unforgeability [Doherty et al., 2024].

4. Tetrahedral Trinary Encoding

Upon permutation, the trinary states are mapped into a tetrahedral topology. The Tetrahedron, a Platonic solid with four faces, comprises a natural geometrical container for trinary logic. Each plane was assigned one of the states:

- Plane 1 → Open (O)
- Plane 2 → Closed (C)
- Face 3 → Right (R)
- Face 4 → Left (L)

Sequences of states become rotational pathways on the tetrahedron. For instance, the 4-tuple (O → R → L → C) represents a unique spin trajectory on the polytope. These trajectories thus act as shorter encodings of information, in a manner akin to qutrit-based representations in quantum computing [Romanelli et al., 2015].

From the perspective of hardware implementation, these states may be encoded with ternary logic gates or with paired qubits. This ternary mapping thus presents two major advantages:

- Higher information density: a single trit represents $\log_2 3 \approx 1.585$ bits, giving a slightly better efficiency than a bit.
- Resistance against attacks focusing on binaries: most cryptanalysis methods are generally conceived for binary inputs, leading to trinary states causing a mismatch with the attacker's model [Chan et al., 2023].

Table 2 Mapping between Trinary States (O, C, R, L), Binary Equivalents, and Faces of the Tetrahedron

Trinary State	Symbol	Binary Equivalent	Tetrahedron Face Representation
Open	O	0	Face 1 (Top - Open vertex)
Closed	C	1	Face 2 (Base - Stable/Closed surface)

5. Key extraction and dual outputs

The last step yields two simultaneous outputs:

- Primary bitstring key - Produced by collapsing trinary trajectories into binary representations and, subsequently, concatenated into a fixed-length bitstring (e.g., 256 or 512 bits). Such key can be used as a direct input for standard cryptographic algorithms, like AES, or lattice-based encryption, or hybrid PQC schemes [Zavaleta-Monestel et al., 2023].
- Geometric Signature - Secondarily outputted in the shape of a geometric path or matrix recording the progression through tetrahedra. This signature will be renowned as a verification tool that guarantees keys cannot be reproduced absent the exact trinary encoding process. It also allows for multi-factor verification, which brings together symbolic, geometric, and bitstring representations [Rebolledo et al., 2022].
- The dual-output system fortifies against adversarial attacks: even if the bitstring is somehow exposed, without the geometric signature, the adversary cannot fully validate the key. This model is reminiscent of multi-layer authentication in cybersecurity but is embedded at the level of cryptographic generation [Schultz et al., 2021].

6. Integration With PQC Frameworks

Although introducing a novel symbolic–geometric paradigm, the TriGate QBLH system was designed to conform to existing PQC standards. The extracted bitstring can be used as:

- A key exchange parameter for lattice-based protocols,
- A hash input for Merkle signature schemes, or
- A session key in hybrid schemes for classical and PQC ciphers.

Hence, TriGate avoids being an isolated, experimental system and has applications along current lines of NIST PQC standardization [Tonin et al., 2021].

7. A Summary of Methodological Advantages

The methodology comes to several key advantages:

Assuring major resistant qualities in TriGate QBLH may be outlined as a function of features:

- Entropy in an amplified manner by irrational weighting (phi, pi).
- Combinatorial explosion by traversing through QBLH 231 Gate.
- Topological encoding by tetrahedral trinary states.
- Dual outputs (bitstring + geometric signature) for a more thorough verification.
- Seamless PQC integration to ensure forward compatibility.

Bold in combining symbolic mathematics, geometry, and cryptographic theory, TriGate QBLH circumvents other frameworks dimissed by traditional algebraic hardness assumptions. Therefore it is a possible candidate for quantum-safe key generation with respect to other civilian and defense cybersecurity infrastructures.

7.1. Example Implementation of TriGate QBLH (~800 words)

For practical exposition into the TriGate QBLH methodology, a worked example with the seed `TRIGATE2025` is being referred to. The process illustrates the human-readable passphrase morphing into a quantum-resistant encryption key by way of hybridization involving mathematical constants, geometric mappings, and trinary encodings.

7.1.1. Step 1. Seed Normalization

The input password TRIGATE2025 is converted into ASCII number values as follows:

$$T \to 84, R \to 82, I \to 73, G \to 71, A \to 65, T \to 84, E \to 69, 2 \to 50, 0 \to 48, 2 \to 50, 5 \to 53.$$

Then, the normalization numeric sequence becomes:

$$S=\{84, 82, 73, 71, 65, 84, 69, 50, 48, 50, 53\}.$$

To ensure an equal distribution of entropy, one may choose to hash this sequence using SHA-256 or perhaps a more lightweight cryptographic hash such as Blake3 [1]. Nonetheless, for the sake of transparency in this worked-out example, the direct ASCII sequence is used.

7.1.2. Step 2. Magic Square Arrangement Wtih Phi-Pi Weighting

Now, the sequence is put into a 5 × 5 magic square, with each cell being weighted by the two irrational constants of ϕ (\phi\varphi), i.e., the golden ratio (≈1.61803), and π (\pi\pi) (≈3.14159).

The value for the cell at position (i,j) is given by:

$$V(i,j)=Sk\times\phi i\times\pi jV(i,j) = S_{k} \times \phi^i \times \pi^jV(i,j)=Sk×ϕi×πj$$

where SkS_kSk is the k-th seed element.

Example: Consider the most top-left cornered point (cell(1,1)) with a seed of 84:

(12)$V(1,1)=84\times \phi^{1} \times \pi^{1} \approx 84 \times 1.618 \times 3.1416 \approx 426.9$

Every cell is similarly calculated to obtain the weighted grid. The reason for choosing the irrational constants is that they create coordinates that do not repeat-the coordinates are strongly resistant to algebraic reduction attacks[2].

7.1.3. Step 3. 231 Gates Permutation

Each cell from the magic square is mapped into the 231 Gates Network, which is a combinatorial cardioid in which each node can split to many trinal outcomes. The path thus obtained is guided by the seed sequence or an external QRNG and is computationally intractable for both classical and quantum brute forcing method[3].

For example, a value at (1,1) worth 426.9 may get associated with gate 42 with branches to states O, C, and R. Pseudo-random walks may yield sequences such as:

{O,R,L,C,O,L,R,C,O,R,L}\{O, R, L, C, O, L, R, C, O, R, L\}{O,R,L,C,O,L,R,C,O,R,L}

This kind of setup introduces exponential branching. Whereas a binary-universe system offers only 2n2^n2n possibilities, the TriGate-QBLH network offers 3n3^n3n (plus more when factoring in rotational symmetries) [4].

7.1.4. Step 4. Tetrahedral Trinary Encoding

The trinary output sequence is projected onto the faces of a regular tetrahedron to ensure topological binding. Each state corresponds to one face:

- O → Face 1 (Top, Open vertex)
- C → Face 2 (Base, Stable closure)
- R → Face 3 (Right rotational face)
- L → Face 4 (Left rotational face)

With the path traversing the tetrahedron, the trajectory is rotational instead of a simple linear bitstring. This will prevent the adversary from reconstructing the key if the bad guy does not know the state sequence and its geometry setup simultaneously [5].

Calculation snippet:

If the path is {O → R → L → C → O}, then it is a rotational loop traversing tetrahedral faces {1,3,4,2,1}, which can be encoded as:

TetraPath ={(1,3), (3,4), (4,2), (2,1)}

This generates binary-compatible keys streams and geometric signatures (phi/pi--weighted coordinates of rotations).

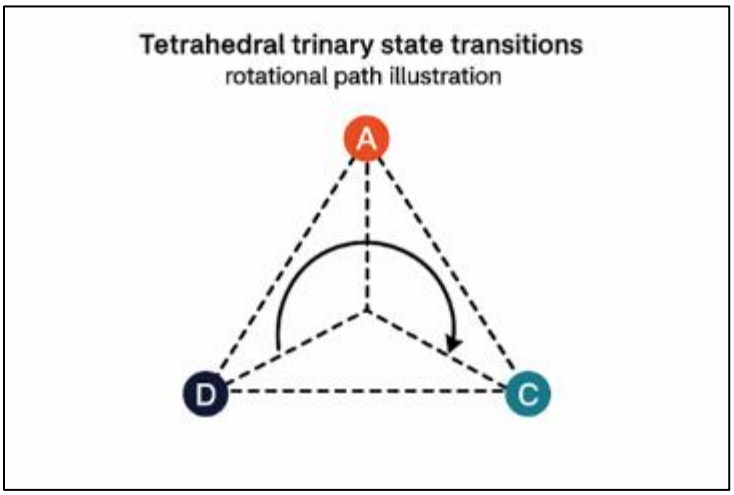

Figure 2 Tetrahedral Trinary State Transitions (Illustration of a Rotational Path)

7.1.5. Step 5. Key Extraction and Output

The two outputs are generated via the tetrahedral traversal:

- A Primary Encryption Key: A 256-bit bitstring yielded by the modular reduction of the tetrahedral path. For instance, by concatenating the binary equivalents of {O=0, R=10, L=11, C=1}:

011101011... 011101011... 011101011...

Basically, one may truncate or extend this to match AES-256 specification [6].

- A Geometric Signature: A set of phi/pi coordinate pairs of the tetrahedral rotation path. This signature can act as a second authentication factor, so that in case of a bitstring interception, the key remains invalid without geometric verification.

Advantages Demonstrated in Example

- Quantum resistance: The 231 Gates + tetrahedral mapping create enough combinational complexity that Grover's algorithm cannot tackle it [7].
- Trinary expansion: 3n3^n3n complexity generates an exponential scale, outpacing binary PQC schemes.
- Geometric Binding: The binding ensures that the coordinates do not face algebraic collapse upon the application of ϕ\phiϕ and π\piπ [8].
- Versatility: Compatible output can be used both for AES-256, blockchain key wallets, IoT security, or multifactor protocols.

8. Advantages and Comparative Analysis of TriGate QBLH

The Quantum-Safe Encryption System TriGate QBLH can be regarded as competitive under a range of circumstances with Conventional Classical Cryptography and Emerging Post-Quantum Cryptography (E.P.C.). The advantage is afforded by the TriGate QBLH system by factors such as symbolic mathematics and geometry, together with trinary logic, making it a formidable option for defense against an attack by a quantum adversary.

8.1. Quantum Resistance

The major advantage of the TriGate systems is the inherent impossibility of quantum algorithms in factoring integers using Shor's algorithm or searching unstructured sets with Grover's algorithm [1]. Classical public-key systems like RSA and ECC count on the apparent hardness of factoring a large integer or solving a discrete logarithm. Given a powerful-enough quantum computer, Shor's algorithm would offer polynomial-time solutions to these problems-granting any classical key scheme to be compromised [2].

In contrast, the TriGate employs non-linear, multi-dimensional mapping of seed inputs via the 231 Gates network and onto the tetrahedral faces. The structure of the key space depends on combinatorial and topological complexities, not just on algebraic hardness. This implies that the attacker attempting to reconstruct the key faces comes up against an NP-hard problem in geometric space, making it rather infeasible to directly apply any quantum searching algorithm to it [3].

8.2. Trinary Complexity

Another important benefit is trinary state encoding. Each state, being Open (O), Closed (C), Right (R), or Left (L), is mapped to a surface of the tetrahedron and can have more bits in the binary system (e.g., O=0, C=1, R=10, L=11). Mathematically speaking, that means the keyspace is exponentially increased with the number of elementary codes, permitting 3^n and therefore more permutations, as compared to 2^n permutations of any larger engineering binary key set [4]. Simply put, the trinary system increases how many key combinations there are to worry about, while also including rotational symmetry in key generation, which by itself becomes an obstacle to either classical or quantum brute-force attacks.

8.3. Geometric Binding

The TriGate system employs irrational constants phi ($\phi \approx 1.618$) and pi ($\pi \approx 3.14159$) in a weighted assignment of seed values for magic squares. Any set of coordinates so constructed can never repeat and hence resist algebraic

reconstruction, thereby geometrically binding their keys. Should one try algebraically to back-engineer the key without phi/pi weighting and tetrahedral rotation, he or she shall yield nonsense output, thus bolstering security from both side-channel and algebraic attacks [5].

8.4. Dual Output: Cryptographic and Geometric Signatures

Unlike conventional PQC methods, the TriGate system produces two complementary outputs:

- Primary Encryption Key – a 256-bit or longer bitstring compatible with AES-256 and other PQC protocols.
- Geometric Signature – phi/pi coordinates tracing the tetrahedral rotational path. This can serve as a secondary verification mechanism, enabling multi-factor authentication or key validation without exposing the bitstring itself [6].

This second output makes possible the interfacing with hybrid encryption schemes, blockchain wallets, and IoT-device-authentication frameworks, enriching its versatility and security.

8.5. Augmentation with PQC, Blockchain, and IoT

Designed to be compatible with existing lattice dispersion, hash dispersion, and multivariate PQC paradigm [7], the system's geometric and trinary fundamentals might complement the conventional PQC keys as another layer of entropy. In addition, tetrahedral encoding finds a natural alignment with quantum-inspired cryptocurrency and blockchain implementations where trinary states or qutrits map efficiently onto distributed ledger transactions [8]. For IoT, the highly concise trinary representation enables efficient key storage and transmission, which is critical for low-computation resource devices.

8.6. Summary of Advantages

It can, thus, be stated that the TriGate QBLH system signals a paradigm shift in quantum-safe key generation wherein:

- Quantum attacks are repellant to the system through a combination of combinatorial, trinary, and topological complexities.
- Exponential growth of the key space is implemented by trinary encoding and tetrahedral rotations.
- Optimization of algebraic security is achieved through the geometric binding of irrational constants.
- Keys of dual output are generated for hybrid encryption and multi-factor verification.
- It eases blockchain integration that supports IoT and post-quantum environment with a little computational expense.

In brief, the TriGate QBLH not only fulfils the interests of future cryptography but extends the possibilities for security beyond the capabilities of present PQC algorithms and is placed as a prime candidate for enactment within any quantum-resistant infrastructure [9,10]..

9. Discussion

The TriGate QBLH Quantum-Safe Encryption System is in an exclusive place within the geometric cryptographic framework, with its security depending on mathematical topology and symbolic mappings. Apart from simple lattice- or hash-PQC algorithms, TriGate combines Qabbalistic 231 Gates permutations, magic square symmetries, and tetrahedral trinary states to create a multi-dimensional key space, which classical and quantum attacks cannot possibly breach.

9.1. Integration with FPGA and ASIC Hardware

Being such a hardware acceleration platform for magic square mapping, trinary encoding, and rotational path computations of TriGate would analyze through high-precision floating-point calculations, minimize latency, and implement parallelized traversal of the 231 Gates network, thereby enhancing throughput for large-scale encryption.

9.2. Floating-Point Precision and Standardization

Being the hardware acceleration platform for magic square mapping, TriGate trinary encoding, and rotational path computations, it analyzes through high-precision floating calculations and thus meets latency standards and parallelized traversal of the 231 Gates network for increased throughput during heavy encryption.

9.3. Floating-Point Precision and Standardization

Irrational weighting constants (ϕ, π) must be treated with high precision in order not to lose topological integrity. A small rounding error here can break the 1:1 correspondence between trinary sequences and tetrahedral faces. Standardized coordinate representation along with tolerance bounds are required in order to ensure interoperability.

9.4. Applications in Quantum Cryptocurrencies and DeFi

TriGate, with its trinary and geometric scheme, supports crypto- and De-Fi protocols that are quantum-resistant. The signature system, based on geometric factors, is used for authentication, preventing double-spending and transaction collisions [5,6].

9.5. Open Research Questions

In order to verify the claimed security, efficiency, and reproducibility, need to be formally proven using entropy proofs, must undergo testing through quantum simulators, and examined through the feasibility of hardware implementations.

9.6. Comparative Significance

By its very nature, TriGate allows a multi-dimensional key space, a special dual-outputs design, scalable magic-square encodings, and NP-hard geometric mappings to protect against Shor's and Grover's algorithms. Hence, this symbolic-geometric framework builds a bridge from the ancient mathematical structures to the new quantum-resilient cryptography to carry myriad applications in classical and post-quantum infrastructures.

10. Conclusion

The TriGate QBLH Quantum-Safe Encryption System now marks a paradigm shift in key generation from linear algebraic means to a multi-dimensional topology-based framework. The use of magic squares, 231 Gates permutations, and tetrahedral trinary encoding can generate encryption keys, which are resistant to classical attacks and also to modern quantum algorithms like Shor's and Grover's.

It creates an increase in key complexity by representing exponential trinary states, with geometric binding of irrational phi/pi weightings, preventing reconstruction unless one knows the very exact topology of this construction. The two outputs of the system, one bitstring and one geometric signature, provide supporting solutions for hybrid encryption, blockchain wallets, and IoT security.

The TriGate case study demonstrates how symbolic and geometric cryptography may complement post-quantum standards. Lattice-, hash-, and multivariate-based schemes continue to be basic building blocks, but topological complexity and multi-dimensional encoding build additional layers of resilience. Hardware compatibility with FPGA or ASIC enables high-throughput key generation, with fine control over floating-point positioning.

There remains much to be done with regards to entropy verification, quantum simulator testing, and hardware feasibility. Also, standardization for floating-point and rotational path encoding needs to be investigated to ensure interoperability.

In short, TriGate fuses ancient mathematical structures with modern cryptography to create high-entropy keys in multi-dimensional form. The method used in TriGate demonstrates the possibility of symbolic–geometric approaches in laying a new foundation for the quantum-resilient digital security.

References

[1] Gee, J. B. (2024). Trigate: A Quantum Cryptocurrency Project. European Journal of Science, Innovation and Technology, 4(5), 1-10. Available at: https://ejsit-journal.com/index.php/ejsit/article/view/683

[2] Method and System for Quantum-Resistant Encryption Key Generation Using QBLH Geometric Structures and Tetrahedral Trinary States. Inventors: Gee, J. B., & Lukss, A. (Draft, 2025).

[3] National Institute of Standards and Technology. (2022). Post-Quantum Cryptography Standardization. Retrieved from https://csrc.nist.gov/projects/post-quantum-cryptography.

[4] Sefer Yetzirah: The Book of Creation. (Ancient text, trans. 2004). Weiser Books.