http://dx.doi.org/10.62762/TISC.2026.243476

RESEARCH ARTICLE

Discretized Holonomy as an Encoding Primitive for Quantum Cryptography

Mohamed El Morsalani[1,*]

[1] QWave Consult, Ostfildern, Germany

Abstract

Geometric phases in quantum systems give rise to holonomies associated with cyclic evolution. In mixed-state settings, these holonomies arise from Uhlmann parallel transport on the purification bundle of density operators and depend on the global geometry of density-operator trajectories. In this work we introduce *discretized mixed-state holonomy* as a geometric encoding primitive. The public object is a density-operator trajectory, while the encoded information resides in a finite family of purification gauges associated with the same holonomy conjugacy class. By discretizing the gauge freedom of the purification bundle, continuous mixed-state holonomy is converted into finite alphabets suitable for discrete key spaces. We formalize the resulting primitive through an operational observation model and establish several structural properties. First, the holonomy representative cannot in general be reconstructed from the density-operator trajectory alone. Second, under conjugation-invariant observation channels, different encoded symbols are indistinguishable at the level of base-space observables. Third, discretized holonomy alphabets admit stable decoding under bounded perturbations of the underlying trajectory. The construction is illustrated through explicit qubit realizations based on isospectral mixed-state loops, together with representative-level decoding mechanisms and finite holonomy alphabets. We further discuss symmetry breaking, frame leakage, and limitations arising in realistic implementations. These results isolate a primitive-level geometric encoding mechanism based on mixed-state quantum geometry and provide a structural foundation for future cryptographic constructions involving representative-level holonomy information.

Keywords: mixed-state holonomy, uhlmann holonomy, quantum information geometry, bures geometry, geometric encoding primitive, quantum cryptography.

1 Introduction and Motivation

Quantum cryptography traditionally encodes information through observable physical quantities such as measurement outcomes, correlation statistics, or computationally structured keys. Security is typically derived from measurement disturbance, entropic uncertainty relations, entanglement correlations, or computational hardness assumptions.

These approaches rely on information carriers that are directly accessible at the level of observable statistics. By contrast, the geometric structure of quantum state

Submitted: 27 March 2026
Revised: 28 May 2026
Accepted: 15 June 2026
Published: 18 August 2026

Vol. 2, **No.** 3, 2026.
10.62762/TISC.2026.243476

***Corresponding author:**
✉ Mohamed El Morsalani
mohamed.elmorsalani@qwave-consult.eu

Citation
El Morsalani, M. (2026). Discretized Holonomy as an Encoding Primitive for Quantum Cryptography. *ICCK Transactions on Information Security and Cryptography*, 2(3), 119–135.

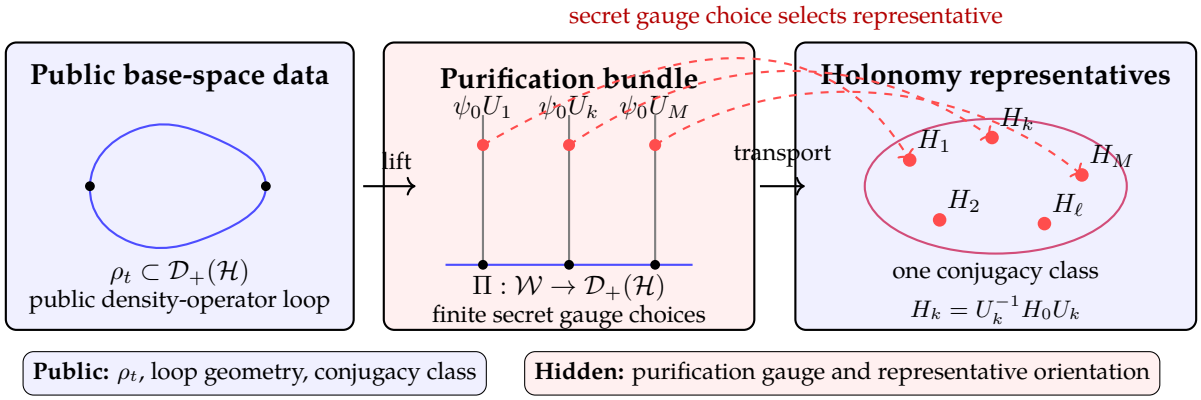

Figure 1. Conceptual structure of the discretized holonomy encoding primitive. A public density-operator loop ρ_t determines a conjugacy class of Uhlmann holonomies. Different purification lifts, selected from a finite set of gauge choices, generate distinct holonomy representatives $H_k = U_k^{-1} H_0 U_k$ within the same conjugacy orbit. The encoded symbol is carried by representative-level orientation rather than by conjugacy-invariant base-space data.

space contains additional global information that is not completely determined by local observables alone. Understanding whether such geometric structure may support cryptographic primitives is therefore a natural conceptual and mathematical question.

A particularly rich geometric framework arises in the theory of mixed quantum states. Density operators admit purifications forming a principal bundle equipped with the Uhlmann connection, and parallel transport in this bundle generates mixed-state holonomy. Unlike ordinary observable quantities, the resulting holonomy contains representative-level gauge structure associated with the purification fiber.

In our previous work [1], we showed that the holonomy associated with a closed density-operator trajectory cannot, in general, be uniquely reconstructed from base-space observations alone. More precisely, the publicly observable density-operator loop determines only the conjugacy class of the holonomy, while the representative within that class depends on the purification gauge. This establishes a structural separation between publicly accessible geometric information and hidden gauge-level data.

The present work develops this observation into a constructive framework. Rather than viewing mixed-state holonomy only as a conceptual geometric secrecy resource, we show how the associated gauge ambiguity can be discretized and organized into finite encoding alphabets.

The central idea is simple, as illustrated schematically in Figure 1. Fix a public density-operator loop together with a finite family of admissible purification gauges. The corresponding Uhlmann holonomies then form a finite set of representatives belonging to the same conjugacy class. Each representative encodes a discrete symbol while the public mixed-state trajectory remains unchanged.

This leads to a primitive-level geometric encoding mechanism: the observable dynamics determine the conjugacy class of the holonomy, whereas the encoded information resides in the representative-level orientation inside that class, as depicted in the rightmost panel of Figure 1.

The objective of this paper is to formalize this construction as a *discretized holonomy encoding primitive*. The paper develops the geometric and operational structure of the primitive, introduces finite holonomy alphabets, and analyzes the corresponding observation and decoding constraints.

Importantly, the present work does not attempt to provide a complete cryptographic protocol or a composable security framework. Instead, we isolate the primitive-level mechanism itself, in the same spirit as early studies of cryptographic primitives prior to full protocol realization.

Contributions. The contributions of the paper are both conceptual and structural.

Geometric encoding framework. We introduce discretized mixed-state holonomy as a geometric encoding primitive in which:

- the public object is a density-operator trajectory,
- the hidden information resides in representative-level gauge structure,
- and discretization of the purification gauge produces finite holonomy alphabets suitable for discrete key spaces.

Operational and security structure. We formalize the primitive-level observation model and establish several structural properties:

- non-reconstructibility of holonomy representatives from base-space data,
- indistinguishability under conjugation-invariant observation channels,
- robustness of discretized holonomy alphabets under bounded perturbations,
- and quantitative leakage bounds under approximate symmetry breaking.

We further illustrate the construction through explicit qubit realizations and discuss extensions to higher-dimensional non-Abelian holonomy alphabets.

These results provide a mathematical and operational foundation for treating discretized mixed-state holonomy as a geometric encoding primitive for future quantum cryptographic constructions.

Organization of the paper. Section 2 reviews the literature on mixed-state holonomy, geometric phases, quantum reference frames, and quantum cryptography relevant to the present work.

Section 3 specifies the assumptions, observation model, and scope of the primitive-level framework.

Section 4 introduces the geometric preliminaries required for the construction, including density operators, the purification bundle, and Uhlmann parallel transport.

Section 5 develops the discretized holonomy encoding primitive and the associated finite holonomy alphabets.

Section 6 introduces the operational observation model and the representative-level adversarial framework.

Section 7 presents minimal operational realizations, including explicit qubit constructions and representative-level decoding mechanisms.

Section 8 establishes the main structural and primitive-level security results, including non-reconstructibility, indistinguishability under conjugation symmetry, and stability of discretized holonomy alphabets.

Section 9 analyzes symmetry breaking, leakage mechanisms, noise effects, and implementation limitations.

Finally, Section 10 discusses broader implications, future directions, and concluding remarks.

2 Related Work

The present work lies at the intersection of quantum information geometry, geometric phase theory, and quantum cryptography. We briefly review the strands of literature most closely related to the discretized holonomy encoding primitive.

Geometric phases and holonomy. Geometric phases arise when quantum systems undergo cyclic evolution. The adiabatic phase discovered by Berry [2] and its non-Abelian generalization by Wilczek and Zee [3] revealed that cyclic quantum dynamics naturally produce gauge-theoretic structures. More generally, geometric phases may be interpreted as holonomies associated with connections on bundles over parameter spaces. These ideas form the conceptual foundation for treating holonomy as a geometric resource.

Mixed-state geometric phases. For mixed quantum states the appropriate geometric framework was developed by Uhlmann [4, 5], who introduced a notion of parallel transport for density operators and the associated mixed-state holonomy. The geometry of mixed states is closely related to the Bures metric [6], originally introduced as a measure of distinguishability between states in the operator-algebraic setting and subsequently adopted as the natural Riemannian metric on the manifold of density operators. Explicit computational methods for the Bures distance were developed in [7], and its statistical interpretation in terms of quantum Fisher information was established in [8]. The differential-geometric structure of the Bures metric, including its curvature properties, was further analyzed in [9], providing a foundation for understanding the global geometry of density-operator manifolds relevant to holonomy transport. Monotone Riemannian metrics on matrix spaces, of which the Bures metric is a distinguished representative, were systematically classified in [10]. Mixed-state geometric phases have also been investigated experimentally and theoretically in interferometric settings [11, 12]. The geometric structure underlying these phases has been further analyzed from the perspective of quantum information geometry, with particular attention to holonomy and its role in the space of density operators [13].

Holonomic quantum computation. Holonomy has also been explored as a computational resource. Zanardi and Rasetti [14] proposed *holonomic quantum computation*, in which quantum gates are implemented through geometric transport in parameter space. In that setting, holonomy is used operationally to realize robust quantum logic operations. The present work investigates a conceptually different direction: holonomy is not used to implement computation, but rather as a geometric encoding primitive in which information is associated with representative-level gauge structure inside a fixed conjugacy class.

Quantum cryptography and geometric encoding. Quantum cryptography traditionally derives security from measurement disturbance, entanglement correlations, or computational assumptions. Canonical examples include the BB84 protocol [15] and entanglement-based key distribution schemes such as Ekert's protocol [16], whose security properties have been studied extensively [17]. In these approaches the encoded information is directly tied to observable measurement statistics.

The present work explores a complementary direction in which information is associated with geometric structure beyond local observable data. More precisely, the public density-operator trajectory determines only the conjugacy class of the associated holonomy, while the encoded information resides in the representative-level gauge orientation within that class. This differs conceptually from phase-encoding approaches in which the phase itself is directly measured or estimated.

Reference frames and gauge information. The interpretation of purification gauge choices as hidden information is related to the resource-theoretic treatment of quantum reference frames [18, 19]. In that framework the availability of a shared reference frame enables access to otherwise inaccessible relational information. In the discretized holonomy primitive a similar role is played by the gauge orientation within the purification bundle. This viewpoint is also closely connected to the role of conjugation symmetry in determining which features of the holonomy remain operationally observable.

Contribution of the present work. The contribution of this paper is to introduce a *discretized holonomy encoding primitive* that converts continuous mixed-state holonomy into finite alphabets suitable for cryptographic key spaces.

We formalize the encoding mechanism through finite families of holonomy representatives associated with a fixed public density-operator trajectory and establish the structural separation between publicly observable geometric data and hidden gauge-level information.

The paper further establishes structural properties of the primitive, including non-reconstructibility of holonomy representatives from base-space data, stability under bounded perturbations of the trajectory, and the role of conjugation symmetry in protecting representative-level secrecy.

A high-level comparison between the present primitive and established quantum cryptographic frameworks is provided in Table 1, which highlights the distinctive role of purification gauge orientation as a hidden information carrier in the holonomy-based construction.

3 Assumptions and Scope

In order to clearly specify the setting in which the proposed construction operates, we summarize the assumptions and scope of the present work.

State space. We consider density operators

$$\rho \in \mathcal{D}(\mathcal{H}), \tag{1}$$

on a finite-dimensional Hilbert space $\mathcal{H}$. Unless otherwise stated, we restrict attention to *faithful states*, i.e. density operators with full rank. This assumption ensures that the manifold of density operators admits a smooth geometric structure and that the Uhlmann connection and holonomy are well defined. Situations involving rank-deficient states may be treated by restricting the construction to the support of the density operator or through suitable limiting procedures.

Public trajectory. The public data consist of a smooth closed trajectory

$$\gamma : [0, 1] \to \mathcal{D}(\mathcal{H}), \qquad \gamma(0) = \gamma(1), \tag{2}$$

in the manifold of density operators. Operationally, this trajectory may be generated by a known control protocol or reconstructed from observable state-space data. The trajectory therefore represents publicly accessible base-space information.

Purification bundle. Each density operator ρ admits purifications in a larger Hilbert space. These purifications form the fibers of a principal bundle over the state manifold. Parallel transport in this bundle

Table 1. Comparison between standard quantum cryptographic paradigms and the discretized holonomy encoding primitive.

Framework	Carrier of Information	Hidden Structure	Security / Operational Principle
BB84 [15]	Measurement outcomes in non-orthogonal bases	None	Measurement disturbance and uncertainty relations
Ekert protocol [16]	Entanglement correlations	None	Bell nonlocality and entanglement security
Holonomic quantum computation [14]	Geometric phase / holonomy	None	Geometric robustness of quantum gates
Present work	Holonomy representatives associated with a public density-operator loop	Purification gauge orientation inside a conjugacy class	Conjugation ambiguity and representative-level secrecy

with respect to the Uhlmann connection induces a unitary holonomy operator associated with closed density-operator trajectories.

Secret data. While the base-space trajectory γ is public, the choice of lift of this trajectory in the purification bundle is not uniquely determined. Different admissible lifts may produce different holonomy representatives within the same conjugacy class. In the discretized construction introduced in this paper, a finite subset of admissible gauge choices is selected, and the resulting holonomy representatives form a finite alphabet carrying discrete hidden parameters.

Observation model. Throughout the paper we assume that the observer has access only to the density-operator trajectory or to equivalent base-space information derivable from it. The purification gauge and its associated holonomy representative are not directly observable from the density-operator data alone.

Adversarial model. We adopt an information-theoretic adversarial model at the level of the encoding primitive.

The adversary is assumed to have access to:

- the public density-operator trajectory ρ_t,
- all quantities derivable from ρ_t (e.g. through tomography),
- knowledge of the public loop and discretization scheme.

The adversary does *not* have access to:

- the purification lift ψ_t,
- the initial gauge choice,
- any shared reference frame required to identify holonomy representatives.

The adversary may perform arbitrary classical or quantum post-processing of the accessible data, including repeated estimation of ρ_t under finite precision.

The adversarial objective is to distinguish between two encoded symbols $k \neq \ell$ using only publicly accessible base-space information.

Primitive-level secrecy notion. At the level of the encoding primitive, secrecy is interpreted as indistinguishability under base-space observables.

Definition 3.1 (Geometric secrecy (primitive level))**.** Let K be the finite alphabet and let ρ_t denote the public trajectory. The encoding primitive satisfies geometric secrecy if, for all $k, \ell \in K$ with $k \neq \ell$, the distributions of all observables measurable from the public trajectory are identical under the two encodings.

Equivalently, for any adversary $\mathcal{A}$ operating on base-space data,

$$|\Pr[\mathcal{A}(\rho_t) = k] - \Pr[\mathcal{A}(\rho_t) = \ell]| \leq \varepsilon, \tag{3}$$

for some $\varepsilon \geq 0$ representing negligible distinguishability in the idealized model.

This notion reflects the fact that the density-operator trajectory determines only the conjugacy class of the holonomy, while the representative orientation remains hidden.

Scope of the present work. The goal of the present paper is to isolate and analyze the geometric mechanism underlying discretized holonomy encodings.

The paper does not attempt to provide a complete cryptographic protocol or a composable security proof.

Instead, we focus on the primitive-level structure by which mixed-state holonomy generates discrete encoding alphabets and on the geometric constraints governing their distinguishability, decoding, and robustness.

A more detailed adversarial analysis and quantitative security evaluation, including leakage under approximate symmetry breaking, will be developed in subsequent work.

This abstraction isolates the underlying geometric mechanism independently of any specific communication architecture, in the same spirit as early formulations of cryptographic primitives prior to protocol-level realization.

4 Geometric Preliminaries

This section briefly reviews the geometric ingredients required for the discretized holonomy encoding primitive. The presentation is intentionally self-contained and restricted to the concepts needed later in the paper.

4.1 Density operators

Let $\mathcal{H}$ be a finite-dimensional Hilbert space of dimension d. A quantum state is represented by a density operator

$$\rho \in \mathcal{D}(\mathcal{H}) := \{\rho \in \mathcal{B}(\mathcal{H}) \mid \rho \geq 0,\ \mathrm{Tr}(\rho) = 1\}. \tag{4}$$

We restrict attention to *faithful* states, i.e. density operators of full rank. The set of faithful density operators forms a smooth manifold, denoted

$$\mathcal{D}_+(\mathcal{H}) = \{\rho \in \mathcal{D}(\mathcal{H}) \mid \rho > 0\}. \tag{5}$$

Throughout this paper, the symbol ρ without further qualification shall denote an element of $\mathcal{D}_+(\mathcal{H})$ unless explicitly stated otherwise. The ambient set $\mathcal{D}(\mathcal{H})$ is used only in definitions and limiting arguments.

A *state trajectory* is a smooth map

$$\rho_t : [0, T] \to \mathcal{D}_+(\mathcal{H}), \tag{6}$$

and a *loop* satisfies $\rho_T = \rho_0$.

4.2 Purification bundle

Any density operator ρ admits a purification

$$\rho = \psi\psi^\dagger, \tag{7}$$

where ψ is a linear operator $\psi : \mathcal{H} \to \mathcal{H}_A$ into an auxiliary Hilbert space $\mathcal{H}_A$. Following the standard construction of Uhlmann [4], we take $\mathcal{H}_A \cong \mathcal{H}$, so that ψ is an $n \times n$ matrix and the purification bundle is $\mathcal{W} \cong GL(n, \mathbb{C})$.

The set of amplitudes

$$\mathcal{W} = \left\{\psi \in GL(n, \mathbb{C}) \;\middle|\; \psi\psi^\dagger \in \mathcal{D}_+(\mathcal{H})\right\} \tag{8}$$

forms a principal fiber bundle

$$\Pi : \mathcal{W} \to \mathcal{D}_+(\mathcal{H}), \qquad \Pi(\psi) = \psi\psi^\dagger, \tag{9}$$

with structure group $U(n)$ acting by right multiplication.

The structure group is the unitary group $U(d)$ acting on the right:

$$\psi \mapsto \psi U, \qquad U \in U(d). \tag{10}$$

All amplitudes related by this action correspond to the same density operator. The unitary freedom therefore represents a *gauge degree of freedom* in the purification fiber.

4.3 Uhlmann parallel transport

Uhlmann introduced a canonical notion of parallel transport for amplitudes along a trajectory ρ_t. Given an initial amplitude ψ_0 satisfying

$$\rho_0 = \psi_0\psi_0^\dagger, \tag{11}$$

there exists a unique horizontal lift ψ_t obeying

$$\Pi(\psi_t) = \rho_t. \tag{12}$$

The horizontality condition defining Uhlmann transport can be written as

$$\psi_t^\dagger \dot{\psi}_t = \dot{\psi}_t^\dagger \psi_t. \tag{13}$$

Equation (13) ensures that the lift evolves without introducing unnecessary gauge rotations.

4.4 Mixed-state holonomy

If the base trajectory is a loop,

$$\rho_T = \rho_0, \tag{14}$$

then the horizontal lift satisfies

$$\psi_T = \psi_0 H, \tag{15}$$

for some unitary operator

$$H \in U(d), \tag{16}$$

called the *Uhlmann holonomy* of the loop.

The holonomy depends on the geometric properties of the trajectory ρ_t together with the choice of initial purification gauge.

4.5 Gauge covariance

A key structural property is the covariance of the holonomy under changes of the initial gauge. If the initial amplitude is replaced by

$$\psi_0' = \psi_0 W, \qquad W \in U(d), \tag{17}$$

for an arbitrary gauge transformation W, then the resulting holonomy transforms as

$$H' = W^{-1} H W. \tag{18}$$

Equation (18) shows that the holonomy is defined only up to conjugation by the gauge group. Consequently, the base-space trajectory determines the conjugacy class of the holonomy, while the representative within that class depends on the choice of purification gauge.

Implication for observable data. Equation (18) shows that the holonomy associated with a given density-operator loop is determined only up to conjugation by the gauge group. Consequently, the base-space trajectory fixes the conjugacy class of the holonomy but does not determine its representative uniquely. This structural ambiguity forms the basis of the discretized holonomy encoding primitive introduced in the following sections.

5 Stage I: Discretized Holonomy as an Encoding Primitive

5.1 Goal and scope (pre-protocol)

The goal of this section is to construct a cryptographic *encoding primitive* based on mixed-state geometric holonomy. The primitive transforms the continuous, non-Abelian Uhlmann holonomy associated with a public density-operator trajectory into a *finite alphabet* suitable for discrete key spaces.

Importantly, this stage is intentionally *pre-protocol*. We do not propose a full cryptographic protocol, nor do we claim composable security. Instead, we isolate a structural primitive that later protocol constructions may build upon.

The guiding principle is the following separation:

Public geometry, secret gauge.

The public data consist of the density-operator trajectory, its induced information geometry, and the associated conjugacy class of the holonomy.

The encoded information resides in the choice of purification lift within the fiber of the purification bundle. Different gauge choices correspond to different holonomy representatives within the same conjugacy class. Thus the observable mixed-state dynamics remain identical, while the realized holonomy representative encodes the secret.

5.2 Geometric setup: purification bundle and Uhlmann transport

Let $\mathcal{S}$ denote the manifold of faithful (full-rank) density operators on an n-dimensional Hilbert space $\mathcal{H}$. Consider the purification bundle

$$\Pi : \mathcal{W} \to \mathcal{S}, \qquad \Pi(\psi) = \psi\psi^{\dagger}. \tag{19}$$

The unitary group $U(n)$ acts on the fibers via the right action

$$\psi \mapsto \psi U, \qquad U \in U(n), \tag{20}$$

which represents the gauge freedom of purifications.

Equipping the bundle with the canonical Uhlmann (Bures) connection defines a notion of parallel transport for amplitudes. Given a trajectory ρ_t and an initial amplitude $\psi_0 \in \Pi^{-1}(\rho_0)$, there exists a unique horizontal lift ψ_t satisfying

$$\Pi(\psi_t) = \rho_t. \tag{21}$$

If the base trajectory is a loop ($\rho_T = \rho_0$), the endpoint satisfies

$$\psi_T = \psi_0 H_U(\rho; \psi_0), \tag{22}$$

where $H_U(\rho; \psi_0) \in U(n)$ is the Uhlmann holonomy.

A fundamental structural property is gauge covariance. If the initial amplitude is replaced by

$$\psi_0' = \psi_0 V, \qquad V \in U(n), \tag{23}$$

then the holonomy transforms as

$$H_U(\rho; \psi_0 V) = V^{-1} H_U(\rho; \psi_0) V. \tag{24}$$

Equation (24) implies that a fixed public trajectory determines the conjugacy class of the holonomy, but not its representative. The representative orientation depends on the initial gauge choice.

5.3 The discretization problem

The gauge group $U(n)$ is continuous and therefore unsuitable as a cryptographic key space. The central task of Stage I is therefore:

Discretization task. Select a finite subset

$$\mathsf{K} \subset U(n)$$

and restrict secrets to initial lifts of the form

$$\psi_0^{(k)} = \psi_0 U_k, \qquad U_k \in \mathsf{K}.$$

The symbol k represents the encoded key.

For a fixed public loop ρ_t, the resulting holonomies are

$$H_k = H_U(\rho; \psi_0 U_k) = U_k^{-1} H_0 U_k, \qquad H_0 := H_U(\rho; \psi_0). \tag{25}$$

Thus the primitive produces a finite family

$$\{H_k\}_{k \in \mathsf{K}},$$

all belonging to the same conjugacy class but differing as representatives. The key index therefore labels representatives within a fixed conjugacy orbit rather than distinct spectral classes.

5.4 Observation model

We assume that the density-operator trajectory ρ_t is publicly observable. Operationally, such trajectories may be reconstructed from measurement statistics through quantum state tomography or derived from the known control protocol generating the evolution.

An observer therefore has access to the base-space evolution ρ_t and to quantities derived from the resulting holonomy that depend only on its conjugacy class. However, the purification gauge defining the initial lift is not determined by the density-operator trajectory alone.

The encoding primitive therefore exploits the separation between base-space observables and fiber-level gauge information.

5.5 Practical discretization strategies

We outline three natural ways to construct finite alphabets K.

Strategy A: commuting alphabet (Abelian discretization). Choose a maximal torus

$$T^n \subset U(n)$$

and select a finite subset

$$\mathsf{K} \subset T^n \cong U(1)^n.$$

Since all elements commute, the resulting holonomies share a common eigenbasis, and decoding reduces to phase relations.

Strategy B: finite non-Abelian subgroup. Choose a finite subgroup

$$\mathsf{K} \leq U(n)$$

such as a Clifford-type group.

The orbit $\{H_k\}$ then explores a non-commutative conjugacy orbit, producing a genuinely non-Abelian holonomy alphabet.

Strategy C: reference-frame discretization. Because conjugation preserves spectral invariants, an adversary observing only class functions of H_k cannot distinguish keys. If legitimate parties share a *gauge reference frame*, they can access the representative orientation itself.

These strategies illustrate different trade-offs between algebraic structure, decoding complexity, and robustness to symmetry-breaking effects.

5.6 Encoding primitive

Definition 5.1 (Discretized holonomy encoding primitive)**.** Fix a public loop ρ_t in the state manifold $\mathcal{S}$, a public Uhlmann connection, and a reference amplitude ψ_0.

Let

$$\mathsf{K} = \{U_k\}_{k=1}^{M} \subset U(n)$$

be a finite key alphabet. To encode a symbol k, Alice selects the secret lift

$$\psi_0^{(k)} = \psi_0 U_k$$

and performs the same public loop ρ_t.

The resulting holonomy representative is

$$H_k = U_k^{-1} H_0 U_k,$$

as defined in Eq. (25).

The observable mixed-state trajectory ρ_t is identical for all keys.

5.7 Decoding requirement

Because the holonomies differ only by conjugation, any class function f on $U(n)$ satisfies

$$f(H_k) = f(H_0). \tag{26}$$

Consequently, class-level information (such as spectrum or trace) cannot reveal the key. Successful decoding therefore requires access to representative-level information beyond conjugacy-invariant data.

> **Decoding requirement.** Recovering the symbol k requires access to the holonomy representative, not merely its conjugacy class.

5.8 Minimal qubit example

For $n = 2$, consider mixed states

$$\rho_t = \frac{1}{2}\left(I + r\,\mathbf{n}(t)\cdot\sigma\right), \qquad 0 < r < 1, \tag{27}$$

where $\mathbf{n}(t)$ traces a latitude loop on the Bloch sphere.

The corresponding Uhlmann holonomy

$$H_0 \in U(2)$$

is non-trivial and reduces to the Berry phase in the pure-state limit [2].

Choosing a finite family

$$\mathsf{K} = \{I, \sigma_x, \sigma_y, \sigma_z\} \subset U(2)$$

generates a discrete set of conjugated holonomy representatives.

An observer restricted to conjugacy-invariant quantities cannot distinguish these representatives, whereas parties possessing additional reference-frame information may access their relative orientation.

5.9 Stage-I deliverables

Stage I therefore establishes the primitive-level structure of discretized holonomy encodings: finite holonomy alphabets, gauge-covariant representative encoding, and the separation between publicly observable geometry and hidden gauge information.

The following section develops the main structural properties of the primitive, including non-reconstructibility and robustness under perturbations.

6 Operational Observation and Adversarial Model

The discretized holonomy encoding primitive relies on a separation between publicly observable geometric information and hidden representative-level gauge structure. This section clarifies the operational meaning of that separation and introduces the corresponding adversarial observation model.

6.1 Conjugacy-level versus representative-level observables

Let

$$H_k \in U(n)$$

denote the holonomy representative associated with the encoded symbol k. Under a gauge transformation

$$H_k \mapsto V H_k V^\dagger, \qquad V \in U(n),$$

all conjugacy-invariant quantities remain unchanged. In particular,

$$\mathrm{spec}(H_k) = \mathrm{spec}(V H_k V^\dagger), \tag{28}$$

and therefore

$$\mathrm{Tr}(H_k) = \mathrm{Tr}(V H_k V^\dagger). \tag{29}$$

Consequently, observables depending only on the conjugacy class of the holonomy cannot distinguish different encoded symbols.

The encoding primitive instead stores information at the level of holonomy representatives. Operationally, decoding therefore requires access to representative-level observables that are sensitive to the orientation of the holonomy within its conjugacy orbit.

6.2 Reference frames and representative access

The ability to distinguish holonomy representatives depends on the availability of a compatible reference frame or equivalent calibration information.

If two parties share a common representative-level reference, they may distinguish holonomies that differ by orientation inside the same conjugacy class. Without such information, conjugate representatives become operationally indistinguishable.

This situation is closely related to the role of reference frames in quantum information theory, where relational data may become inaccessible in the absence of a shared frame.

The discretized holonomy primitive therefore separates:

- publicly observable geometric data,
- representative-level gauge information,
- and frame-dependent decoding information.

6.3 Representative-level observables

To illustrate the distinction operationally, consider the qubit holonomy representatives

$$H_k = \exp\!\left(-\frac{\imath}{2}\Omega_U\,\hat{n}_k\cdot\vec{\sigma}\right), \tag{30}$$

introduced later in Section 7.

Although all representatives share the same eigenvalues, their action on test states depends

on the orientation $\hat{n}_k$. For example, expectation values of the form

$$\langle\psi|H_k|\psi\rangle \tag{31}$$

may distinguish different symbols once a representative-level frame is fixed.

Representative-level decoding therefore depends not only on the geometric loop itself, but also on the operational ability to compare orientations inside the holonomy orbit.

6.4 Adversarial observation model

We consider an information-theoretic adversarial model at the level of the encoding primitive.

The adversary is assumed to have access to:

- the public density-operator trajectory ρ_t,
- all conjugacy-invariant quantities derivable from the holonomy,
- the public discretization scheme and loop geometry.

The adversary is not assumed to possess:

- the purification lift,
- the initial gauge choice,
- or the representative-level reference frame required to distinguish holonomy orientations.

Under this observation model, the public trajectory determines the conjugacy class of the holonomy but does not uniquely fix its representative.

6.5 Idealized symmetry assumption

The primitive-level secrecy mechanism relies on an idealized conjugation symmetry: observations accessible to the adversary depend only on conjugacy-invariant properties of the holonomy.

Under exact conjugation invariance,

$$\mathsf{P}_{H_k} = \mathsf{P}_{H_\ell}, \qquad k, \ell \in \mathsf{K}, \tag{32}$$

where P_{H_k} denotes the adversarial observation distribution associated with the symbol k.

Consequently, no adversary restricted to conjugacy-level observables can distinguish the encoded symbols.

Departures from exact symmetry, including frame leakage, calibration asymmetries, and implementation imperfections, will be discussed in Section 9.

7 Minimal Operational Primitive

This section develops a minimal operational realization of the discretized holonomy encoding primitive in the setting of isospectral mixed-state loops.

The purpose is not to propose a complete communication protocol, but rather to demonstrate explicitly how finite holonomy alphabets arise from representative-level geometric structure.

7.1 Isospectral mixed-state loops

Let ρ_0 be a density operator on a finite-dimensional Hilbert space $\mathcal{H}$ with fixed spectrum

$$\mathrm{spec}(\rho_0) = \{p_1, \ldots, p_d\}, \qquad p_i > 0, \quad \sum_i p_i = 1.$$

The associated isospectral manifold is the unitary orbit

$$\mathcal{S}_p = \left\{ U\rho_0 U^\dagger \;\middle|\; U \in U(\mathcal{H}) \right\}. \tag{33}$$

All states in $\mathcal{S}_p$ share the same eigenvalues and therefore the same degree of mixedness. Motion on $\mathcal{S}_p$ modifies only the eigenbasis structure of the state.

Closed loops

$$\rho_t \subset \mathcal{S}_p$$

generate mixed-state holonomies through Uhlmann parallel transport. The resulting holonomy depends on the geometry of the loop together with the representative-level gauge choice.

7.2 Finite holonomy alphabets

Fix a public loop ρ_t and a reference holonomy

$$H_0 \in U(n).$$

Let

$$\mathsf{K} = \{U_k\}_{k=1}^{M} \subset U(n)$$

be a finite family of gauge transformations.

The corresponding holonomy representatives are

$$H_k = U_k^{-1} H_0 U_k. \tag{34}$$

All representatives belong to the same conjugacy class and therefore share identical spectral invariants. The encoded information is carried not by the spectrum of the holonomy, but by its representative orientation inside the conjugacy orbit.

7.3 Minimal encoding and decoding procedure

The primitive operates as follows.

Encoding step. Alice selects a symbol

$$k \in \mathsf{K}$$

and prepares the corresponding purification lift

$$\psi_0^{(k)} = \psi_0 U_k.$$

She then executes the public loop ρ_t. The resulting holonomy representative is

$$H_k = U_k^{-1} H_0 U_k.$$

Public information. The density-operator trajectory ρ_t, its induced geometry, and all conjugacy-invariant quantities remain identical for all symbols.

Decoding step. A receiver possessing representative-level reference information may distinguish the representatives H_k through suitable observables sensitive to orientation inside the conjugacy orbit.

An observer restricted to conjugacy-invariant quantities cannot distinguish the encoded symbols.

7.4 Explicit qubit realization

Any faithful qubit state may be written in Bloch form

$$\rho(\vec{r}) = \frac{1}{2}\left(I + \vec{r}\cdot\vec{\sigma}\right), \qquad 0 < \|\vec{r}\| < 1, \tag{35}$$

where

$$\vec{\sigma} = (\sigma_x, \sigma_y, \sigma_z).$$

Fixing the eigenvalues of ρ is equivalent to fixing the Bloch radius

$$r = \|\vec{r}\|.$$

The isospectral manifold is therefore the sphere of directions at fixed radius.

We choose the reference state

$$\rho_0 = \frac{1}{2}(I + r\sigma_z)$$

and consider the latitude loop

$$\hat{u}(t) = (\sin\theta\cos 2\pi t,\ \sin\theta\sin 2\pi t,\ \cos\theta), \qquad t \in [0,1]. \tag{36}$$

... For the latitude loop defined above, the resulting Uhlmann holonomy may be written as

$$H = \exp\left(-\frac{\imath}{2}\Omega_U(r,\theta)\,\hat{n}\cdot\vec{\sigma}\right), \tag{37}$$

where the rotation axis $\hat{n}$ is given by the fixed symmetry axis of the latitude loop,

$$\hat{n} = (0,0,1)^T, \tag{38}$$

and $\Omega_U(r,\theta)$ is the Uhlmann phase defined in Eq. (39). Thus $\hat{n}$ is independent of t and coincides with the axis about which the Bloch vector $\hat{u}(t)$ precesses.

$$\Omega_U(r,\theta) = 2\pi\left(1 - \frac{\cos\theta}{\sqrt{1 - r^2\sin^2\theta}}\right). \tag{39}$$

In the pure-state limit $r \to 1$, this reduces to the Berry solid angle.

7.5 Axis discretization and representative encoding

A finite alphabet is obtained by restricting the rotation axis to a finite set.

Let

$$\mathsf{K} = \{1,2,3\}, \qquad \hat{n}_1 = \hat{x}, \quad \hat{n}_2 = \hat{y}, \quad \hat{n}_3 = \hat{z}.$$

The corresponding holonomy representatives are

$$H_k = \exp\left(-\frac{\imath}{2}\Omega_U(r,\theta)\,\hat{n}_k\cdot\vec{\sigma}\right). \tag{40}$$

All representatives satisfy

$$\mathrm{spec}(H_k) = \left\{e^{-\imath\Omega_U/2}, e^{+\imath\Omega_U/2}\right\}, \tag{41}$$

and therefore share identical conjugacy invariants.

The encoded symbol is carried by the representative orientation $\hat{n}_k$ rather than by spectral data.

7.6 Representative-level decoding

Once a representative-level reference frame is fixed, simple observables can distinguish the symbols.

For example, using the test state

$$|0\rangle,$$

one obtains

$$\langle 0|H_z|0\rangle = e^{-\imath\Omega_U/2}, \tag{42}$$

whereas

$$\langle 0|H_x|0\rangle = \cos(\Omega_U/2). \tag{43}$$

Different probe states similarly distinguish the remaining axis orientations.

This demonstrates explicitly that the symbols become operationally distinguishable once representative-level orientation information is accessible.

Table 2. Summary of the principal structural and primitive-level security properties established in this work.

Property	Statement	Reference
Non-reconstructibility	Holonomy representatives cannot be uniquely reconstructed from base-space data alone	Theorem 4.1
Primitive-level geometric secrecy	Conjugation-invariant observations induce identical laws for all encoded symbols	Theorem 4.3
Vanishing distinguishing advantage	Adversaries restricted to conjugation-invariant observations have zero distinguishing advantage	Proposition 4.4
Stability under perturbations	Discretized holonomy alphabets remain decodable under bounded trajectory perturbations	Theorem 4.5
Representative-level decoding requirement	Successful decoding requires access to information beyond conjugacy-invariant observables	Proposition 4.4
Leakage under approximate symmetry breaking	Statistical leakage is controlled by the invariance defect parameter η	Proposition 5.1

7.7 Higher-dimensional extension

The same construction extends naturally to higher-dimensional systems.

For a qutrit state

$$\rho_0 = \mathrm{diag}(p_1, p_2, p_3),$$

closed isospectral loops generate holonomies in the stabilizer subgroup

$$U_\lambda = \{V \in U(3) \mid [V, \rho_0] = 0\}.$$

Restricting the gauge choices to a finite subset

$$\mathsf{K} \subset U(3)$$

produces finite holonomy alphabets in direct analogy with the qubit construction.

In higher dimensions, the resulting alphabets may exhibit genuinely non-Abelian representative structure.

8 Main Structural and Security Results

This section establishes the principal structural and primitive-level security properties of discretized holonomy encodings. The main results are summarized in Table 2 for quick reference.

The results formalize three central features of the construction:

- non-reconstructibility of holonomy representatives from base-space data,
- indistinguishability under conjugation-invariant observation,
- and robustness of finite holonomy alphabets under bounded perturbations.

8.1 Non-reconstructibility of holonomy representatives

The encoding primitive relies on the separation between base-space observables and representative-level gauge structure.

Theorem 8.1 (Non-reconstructibility from base-space data)**.** *Let ρ_t be a closed trajectory in the manifold $\mathcal{S}$ of faithful density operators and let*

$$H_U(\rho; \psi_0)$$

denote the associated Uhlmann holonomy.

Assume that the observer has access only to the density-operator trajectory ρ_t and quantities derivable from it.

Then the holonomy representative cannot be uniquely determined from the base-space data alone. In particular, for every $W \in U(n)$,

$$H_U(\rho; \psi_0 W) = W^{-1} H_U(\rho; \psi_0) W, \tag{44}$$

while the induced density-operator trajectory remains unchanged.

Proof. The statement follows directly from the gauge covariance property of Uhlmann holonomy established in Eq. (24).

Replacing the initial purification amplitude by

$$\psi_0 V$$

changes the holonomy by conjugation while preserving the projected trajectory ρ_t.

Therefore the density-operator loop determines only the conjugacy class of the holonomy and not its representative. □

Interpretation. Theorem 8.1 shows that representative-level information is not recoverable from publicly observable geometric data alone. The primitive therefore separates:

- public geometric evolution,
- and hidden gauge-level orientation information.

8.2 Primitive-level geometric secrecy

We now formalize the primitive-level secrecy mechanism.

Let

$$\mathsf{K} = \{U_k\}_{k=1}^{M} \subset U(n)$$

be a finite holonomy alphabet and let

$$H_k = U_k^{-1} H_0 U_k$$

denote the corresponding representatives.

For each encoded symbol k, let

$$\mathsf{P}_{H_k}$$

denote the probability distribution induced by the adversarial observation process.

Definition 8.2 (Conjugation-invariant observation channel)**.** An adversarial observation channel is called *conjugation invariant* if

$$\mathsf{P}_{VHV^\dagger} = \mathsf{P}_H, \qquad \forall H \in U(n), \quad \forall V \in U(n). \tag{45}$$

Under this symmetry assumption, all representatives inside the same conjugacy class produce identical observation laws.

Theorem 8.3 (Primitive-level geometric secrecy)**.** *Assume that the adversarial observation channel satisfies the conjugation-invariance condition (45).*

Then for all encoded symbols

$$k, \ell \in \mathsf{K},$$

the corresponding observation laws satisfy

$$\mathsf{P}_{H_k} = \mathsf{P}_{H_\ell}. \tag{46}$$

Consequently, no adversary restricted to conjugacy-invariant observations can distinguish between encoded symbols.

Proof. All representatives satisfy

$$H_k = U_k^{-1} H_0 U_k.$$

By conjugation invariance of the observation channel,

$$\mathsf{P}_{H_k} = \mathsf{P}_{H_0}$$

for all k. Hence all observation laws coincide. □

Interpretation. The secrecy mechanism does not rely on computational hardness assumptions. Instead, it follows from the inability of conjugation-invariant observations to access representative-level orientation information.

8.3 Indistinguishability advantage

The previous theorem immediately implies a primitive-level indistinguishability property.

Proposition 8.4 (Vanishing distinguishing advantage)**.** *Let $\mathcal{A}$ be any adversary operating on conjugation-invariant observations.*

Under the assumptions of Theorem 8.3, the distinguishing advantage

$$\mathrm{Adv}(\mathcal{A})$$

between any two symbols $k \neq \ell$ satisfies

$$\mathrm{Adv}(\mathcal{A}) = 0. \tag{47}$$

Proof. Since the induced observation laws coincide, the adversary receives statistically identical data under both encodings. Therefore the optimal distinguishing advantage vanishes. □

8.4 Stability of discretized holonomy alphabets

We now establish robustness under bounded perturbations of the public trajectory.

Theorem 8.5 (Stability of discretized holonomy alphabets)**.** *Let*

$$\{H_k\}_{k \in \mathsf{K}}$$

be the discretized holonomy alphabet associated with a public loop ρ_t.

Assume that the realized trajectory $\tilde{\rho}_t$ satisfies

$$\|\tilde{\rho}_t - \rho_t\| \leq \varepsilon \tag{48}$$

for all t.

Assume furthermore that the holonomy map is Lipschitz continuous in the following sense: there exists a constant

$C > 0$, depending only on the reference loop ρ_t and the alphabet K, such that

$$\|H_k(\tilde{\rho}) - H_k(\rho)\|_{\mathrm{HS}} \le C\|\tilde{\rho} - \rho\|_\infty, \tag{49}$$

where $\|\tilde{\rho} - \rho\|_\infty := \max_t \|\tilde{\rho}_t - \rho_t\|_1$.

Let $\|\cdot\|$ denote any unitarily invariant norm on $M_n(\mathbb{C})$, for instance the Hilbert–Schmidt norm. Define the minimum alphabet separation as

$$\Delta := \min_{k \neq \ell} \|H_k - H_\ell\|. \tag{50}$$

Since all norms on finite-dimensional spaces are equivalent, the qualitative stability condition $C\varepsilon < \Delta/2$ is independent of the particular norm choice up to a constant factor.

If

$$C\varepsilon < \frac{\Delta}{2}, \tag{51}$$

then nearest-neighbor decoding uniquely recovers the encoded symbol.

Proof. Under the perturbation assumptions, each representative moves within a ball of radius $C\varepsilon$.

Condition (51) ensures that these neighborhoods remain disjoint. Therefore no perturbed representative can cross into the decoding region of another symbol. □

Operational interpretation. Theorem 8.5 shows that discretized holonomy alphabets admit robust decoding under sufficiently small implementation errors. The separation parameter Δ therefore acts as a geometric decoding margin.

8.5 Representative-level decoding condition

The preceding results imply a fundamental operational constraint.

Proposition 8.6 (Representative-level decoding requirement)**.** *Any decoding strategy capable of recovering the encoded symbol must access information beyond conjugacy-invariant observables.*

Proof. Conjugacy-invariant observations depend only on the spectrum and conjugacy class of the holonomy.

Since all representatives in the alphabet belong to the same conjugacy class, such observations are identical for all encoded symbols.

Therefore successful decoding requires access to representative-level orientation information. □

9 Noise, Symmetry Breaking, and Limitations

The secrecy mechanism developed in the previous sections relies on an idealized conjugation symmetry. Realistic implementations may violate this symmetry through reference-frame leakage, calibration asymmetries, finite precision effects, or environmental coupling.

This section discusses the resulting limitations and the effect of approximate symmetry breaking on primitive-level security.

9.1 Approximate conjugation symmetry

In realistic settings, the adversarial observation process may fail to be exactly conjugation invariant.

We model this through an *invariance defect* parameter

$$\eta \ge 0,$$

measuring the deviation from exact symmetry.

Formally, we assume that the observation distributions satisfy

$$d_{\mathrm{TV}}(\mathsf{P}_{VHV^\dagger}, \mathsf{P}_H) \le \eta, \tag{52}$$

for all $H \in U(n)$ and all $V \in U(n)$, where d_{TV} denotes total variation distance.

The idealized secrecy model corresponds to the case

$$\eta = 0.$$

9.2 Leakage induced by symmetry breaking

When $\eta > 0$, encoded symbols need no longer induce identical observation laws. In particular, representative-level asymmetries may become partially observable through calibration bias, laboratory frame information, anisotropic control noise, hardware-dependent couplings, or environmental leakage channels. The resulting statistical distinguishability is controlled by the magnitude of the symmetry defect.

Proposition 9.1 (Leakage bound under approximate symmetry)**.** *Assume that the adversarial observation channel satisfies the approximate symmetry condition (52).*

Then for any two encoded symbols $k, \ell \in \mathsf{K}$,

$$d_{\mathrm{TV}}(\mathsf{P}_{H_k}, \mathsf{P}_{H_\ell}) \le \eta. \tag{53}$$

Proof. Since all representatives belong to the same conjugacy orbit,

$$H_\ell = V H_k V^\dagger$$

for some unitary V.

Applying the approximate symmetry assumption yields the result directly. □

Interpretation. Equation (53) shows that secrecy degrades continuously with symmetry breaking. The invariance defect η therefore acts as a primitive-level leakage parameter.

9.3 Frame leakage and calibration asymmetry

The most important source of symmetry breaking is typically representative-level frame information. If the adversary gains access to shared calibration data, orientation references, representative-level tomography, or hardware alignment information, then conjugate representatives may become operationally distinguishable. The secrecy mechanism therefore depends critically on the extent to which representative-level orientation information remains hidden.

9.4 Finite precision and tomography

Realistic observation processes involve finite-sample estimation and imperfect tomography.

Although conjugacy invariants remain identical in the idealized model, estimation procedures may introduce small asymmetries that correlate with representative-level structure.

Such effects are implementation dependent and may accumulate under repeated observations.

9.5 Noise and perturbed loops

Control imperfections may perturb the realized density-operator trajectory away from the intended loop.

The stability theorem (Theorem 8.5) shows that decoding remains robust provided that the perturbation magnitude remains below the geometric decoding margin determined by the alphabet separation.

Beyond this regime, different representatives may become operationally indistinguishable or decoding errors may occur.

9.6 Scalability considerations

The discretized holonomy primitive extends naturally to higher-dimensional systems, but several practical constraints arise, including increasing control complexity for high-dimensional loops, representative-level frame synchronization, growth of non-Abelian conjugacy structure, and decoding complexity for large alphabets. While the geometric construction itself is dimension independent, realistic implementations become progressively more demanding in higher dimensions.

9.7 Scope limitations

The present work develops a primitive-level geometric encoding framework. It does not provide a composable cryptographic security proof, a fault-tolerant implementation architecture, a full quantum communication protocol, or a hardware-level security analysis. Instead, the objective is to isolate and formalize the underlying geometric secrecy mechanism associated with mixed-state holonomy and representative-level gauge structure.

10 Discussion and Outlook

The results of this paper identify discretized mixed-state holonomy as a geometric resource capable of carrying discrete information at the representative level of the purification bundle.

The central mechanism is the separation between publicly observable base-space geometry and hidden gauge-level orientation information. While the density-operator trajectory determines the conjugacy class of the associated holonomy, the representative within that class depends on the purification gauge and therefore remains inaccessible to purely conjugacy-invariant observations.

The paper developed this idea at the level of a geometric encoding primitive. Rather than proposing a complete cryptographic protocol, the objective was to isolate the structural mechanism by which mixed-state holonomy generates finite symbolic alphabets while preserving the observable density-operator dynamics.

The analysis established several primitive-level properties:

- non-reconstructibility of holonomy representatives from base-space data,
- indistinguishability under conjugation-invariant observation channels,
- robustness of discretized holonomy alphabets under bounded perturbations,
- and the role of representative-level reference information in operational decoding.

Together, these results suggest that mixed-state geometric structure may serve as an information resource complementary to standard measurement-based encoding mechanisms in quantum information theory.

Toward protocol-level constructions. The primitive developed here naturally suggests several protocol-level extensions.

A minimal communication scenario would involve:

- a sender selecting a symbol $k \in \mathsf{K}$,
- preparation of the corresponding purification lift,
- execution of a public density-operator loop,
- and a receiver possessing representative-level reference information allowing discrimination between holonomy representatives.

In such a setting, secrecy would rely on the inability of an adversary without access to the representative-level frame to distinguish between conjugate holonomy representatives.

Formalizing these constructions in terms of explicit communication models, key-generation procedures, and composable security definitions remains an important direction for future work.

Symmetry breaking and realistic implementations. The secrecy mechanism developed in this paper is exact only under idealized conjugation symmetry.

Realistic implementations may introduce leakage through frame information, calibration asymmetries, finite precision, or environmental coupling. Understanding how such effects modify representative-level distinguishability constitutes an essential step toward practical realizations of geometric holonomy encodings.

Higher-dimensional holonomy alphabets. While the qubit construction illustrates the primitive in its simplest setting, higher-dimensional systems allow substantially richer non-Abelian holonomy structure.

Exploring the geometry, decoding properties, and robustness of high-dimensional holonomy alphabets remains an open direction, particularly in relation to non-commutative representative structure and scalable geometric encoding schemes.

Computational aspects. The evaluation of mixed-state holonomy requires parallel transport in the space of density operators and generally involves matrix differential equations. The computational complexity therefore increases with the dimension of the Hilbert space.

Similarly, representative-level reconstruction and tomography become progressively more demanding in higher dimensions, which may impose practical limitations on large-scale implementations of the primitive.

Geometric resources in quantum information. More broadly, the present work suggests that geometric structures associated with purification bundles and mixed-state holonomy may provide new information-theoretic resources beyond measurement statistics and entanglement correlations alone.

Understanding the role of such geometric resources in cryptography, communication, and quantum information processing may therefore open new directions at the interface of quantum information geometry and quantum cryptography.

Data Availability Statement

Data will be made available on request.

Funding

This work was supported without any funding.

Conflicts of Interest

Mohamed El Morsalani is affiliated with the QWave Consult, Ostfildern, Germany. The author declares that this affiliation had no influence on the study design, data collection, analysis, interpretation, or the decision to publish, and that no other competing interests exist.

AI Use Statement

The author declares that ChatGPT-5 was used for language editing and translation of the manuscript. The author has carefully reviewed, revised, and verified the AI-assisted output and takes full responsibility for the content of the manuscript.

Ethical Approval and Consent to Participate

Not applicable.

References

[1] El Morsalani, M. (2026). Secret Holonomy and Public Geometry in Mixed-State Quantum Information. *Journal of Quantum Cryptography, 1*(1), 3-54. [CrossRef]

[2] Berry, M. V. (1984). Quantal phase factors accompanying adiabatic changes. *Proceedings of the Royal Society of London. Series A, Mathematical and Physical Sciences, 392*(1802), 45-57. [CrossRef]

[3] Wilczek, F., & Zee, A. (1984). Appearance of gauge structure in simple dynamical systems. *Physical Review Letters, 52*(24), 2111-2114. [CrossRef]

[4] Uhlmann, A. (1986). Parallel transport and "quantum holonomy" along density operators. *Reports on Mathematical Physics, 24*(2), 229-240. [CrossRef]

[5] Uhlmann, A. (1992). The metric of Bures and the geometric phase. In R. Gielerak, J. Lukierski, & Z. Popowicz (Eds.), *Quantum Groups and Related Topics*, pp. 267-274. Springer. [CrossRef]

[6] Bures, D. (1969). An extension of Kakutani's theorem on infinite product measures to the tensor product of semifinite w*-algebras. *Transactions of the American Mathematical Society, 135*, 199-212. [CrossRef]

[7] Hübner, M. (1992). Explicit computation of the Bures distance for density matrices. *Physics Letters A, 163*(4), 239-242. [CrossRef]

[8] Braunstein, S. L., & Caves, C. M. (1994). Statistical distance and the geometry of quantum states. *Physical Review Letters, 72*(22), 3439-3443. [CrossRef]

[9] Dittmann, J. (1999). The scalar curvature of the Bures metric on the space of density matrices. *Journal of Geometry and Physics, 31*(1), 16-24. [CrossRef]

[10] Petz, D. (1996). Monotone metrics on matrix spaces. *Linear Algebra and its Applications, 244*, 81-96. [CrossRef]

[11] Du, J., Zou, P., Shi, M., Kwek, L. C., Pan, J. W., Oh, C. H., … & Ericsson, M. (2003). Observation of geometric phases for mixed states using NMR interferometry. *Physical Review Letters, 91*(10), 100403. [CrossRef]

[12] Sjöqvist, E., Pati, A. K., Ekert, A., Anandan, J. S., Ericsson, M., Oi, D. K., & Vedral, V. (2000). Geometric phases for mixed states in interferometry. *Physical Review Letters, 85*(14), 2845-2848. [CrossRef]

[13] Andersson, O. (2019). Holonomy in quantum information geometry. *arXiv preprint arXiv:1910.08140*. [CrossRef]

[14] Zanardi, P., & Rasetti, M. (1999). Holonomic quantum computation. *Physics Letters A, 264*(2-3), 94-99. [CrossRef]

[15] Bennett, C. H., & Brassard, G. (1984/2014). Quantum cryptography: Public key distribution and coin tossing. Originally presented at *IEEE International Conference on Computers, Systems and Signal Processing*, Bangalore, India, pp. 175-179 (1984); reprinted in *Theoretical Computer Science, 560*, 7-11 (2014). [CrossRef]

[16] Ekert, A. K. (1991). Quantum cryptography based on Bell's theorem. *Physical Review Letters, 67*(6), 661-663. [CrossRef]

[17] Scarani, V., Bechmann-Pasquinucci, H., Cerf, N. J., Dušek, M., Lütkenhaus, N., & Peev, M. (2009). The security of practical quantum key distribution. *Reviews of Modern Physics, 81*(3), 1301-1350. [CrossRef]

[18] Bartlett, S. D., Rudolph, T., & Spekkens, R. W. (2007). Reference frames, superselection rules, and quantum information. *Reviews of Modern Physics, 79*(2), 555-609. [CrossRef]

[19] Gour, G., & Spekkens, R. W. (2008). The resource theory of quantum reference frames: manipulations and monotones. *New Journal of Physics, 10*(3), 033023. [CrossRef]

Mohamed El Morsalani is a quantum technologies consultant and researcher at QWave Consult, Ostfildern, Germany. He holds a PhD in mathematics and has over two decades of professional experience at the intersection of quantitative finance, risk analysis, and advanced technologies. His current research focuses on quantum cryptography, post-quantum cryptography, and the geometric foundations of quantum information, including mixed-state geometry and holonomy-based secrecy frameworks. He is also active in advisory and educational activities related to quantum technologies and quantum-safe security. (Email: mohamed.elmorsalani@qwave-consult.eu)