



Secret Holonomy and Public Geometry in Mixed-State Quantum Information

Mohamed El Morsalani^{1,*}

¹QWave Consult, Ostfildern, Germany

Abstract

Mixed quantum states exhibit a rich geometric structure from the information geometry of density operators and their purifications. Parallel transport via the Uhlmann connection induces holonomy transformations along closed trajectories of density operators. Although extensively studied in quantum physics, their potential as information-theoretic resources in quantum cryptography remains largely unexplored. This work investigates whether holonomy in the purification bundle can serve as a secrecy resource for mixed-state quantum systems. The key observation is that while a density-operator trajectory describes only the base manifold, the lifted trajectory depends on an additional unitary gauge freedom associated with purification amplitudes. Consequently, distinct lifted trajectories from different gauge choices may generate different holonomy transformations even when the observable density evolution remains identical. We formalize this by proving that holonomy from a closed density-operator trajectory cannot be uniquely reconstructed from base-space observations. Specifically, the

observable trajectory determines holonomy only up to conjugacy in the unitary group. This reveals a structural separation between publicly observable geometric information—namely the density-operator trajectory equipped with Bures quantum information geometry—and hidden bundle-level transformations arising from purification gauge choices. Based on this property, we introduce a minimal geometric encoding primitive where classical symbols correspond to gauge transformations in the purification bundle while the observable density trajectory remains unchanged. We further formalize a base-space-restricted adversarial model, define a distinguishability advantage for message recovery, and analyze potential attacks including tomographic, geometric, and algebraic reconstruction attempts. Explicit single-qubit and multi-qubit examples illustrate how Abelian and non-Abelian holonomy arise in low-dimensional mixed-state systems. These results identify holonomy as a geometric information carrier in mixed-state quantum information and provide structural foundations for future holonomy-based quantum cryptographic protocols.

Keywords: mixed-state quantum cryptography, uhlmann holonomy, quantum information geometry, bures geometry, purification bundle, geometric secrecy.



Submitted: 07 January 2026

Accepted: 10 April 2026

Published: 17 May 2026

Vol. 1, No. 1, 2026.

doi:10.62762/JQC.2026.133798

*Corresponding author:

✉ Mohamed El Morsalani

mohamed.elmorsalani@qwave-consult.eu

Citation

El Morsalani, M. (2026). Secret Holonomy and Public Geometry in Mixed-State Quantum Information. *Journal of Quantum Cryptography*, 1(1), 35–54.



© 2026 by the Author. Published by Institute of Central Computation and Knowledge. This is an open access article under the CC BY license (<https://creativecommons.org/licenses/by/4.0/>).

1 Introduction

Quantum cryptography traditionally relies on operational principles of quantum mechanics such as measurement disturbance, no-cloning, and entanglement correlations. Protocols such as BB84 demonstrate that these physical principles can be exploited to achieve provably secure communication channels.

Beyond operational protocol design, several recent works have explored whether deeper geometric structures of quantum state space can also play a role in cryptographic constructions. In particular, the geometry of Hilbert space and the structure of quantum state manifolds provide a natural language for describing transformations, invariants, and information flow in quantum systems.

One example of this geometric viewpoint appears in the work of Di Cairano [1], where secrecy for pure bipartite quantum states is interpreted through the geometry of entanglement level sets. In that framework, classical information can be associated with the motion of quantum trajectories relative to a foliation of projective Hilbert space defined by an entanglement measure.

While conceptually appealing, such constructions rely strongly on properties specific to pure states. Once mixed quantum states are considered, scalar entanglement measures generally fail to define smooth geometric foliations of the state space. As a consequence, the geometric encoding mechanism based on entanglement level sets becomes unstable in the presence of noise and mixed states.

The present work proposes a different geometric perspective for the mixed-state regime. Instead of relying on scalar entanglement functionals, we consider the bundle geometry associated with purifications of density operators. In this setting, parallel transport defined by the Uhlmann connection [2] induces holonomy transformations along closed trajectories of mixed quantum states.

The key observation is that the density-operator trajectory describes only the base manifold of this bundle structure, while the lifted trajectory in the purification bundle contains additional geometric degrees of freedom. As a result, different bundle lifts of the same density-operator trajectory may generate distinct holonomies even though the observable mixed-state evolution remains identical.

This separation between observable base-space data

and hidden bundle-level transformations suggests a natural geometric secrecy mechanism. Classical information can be associated with gauge choices in the purification bundle while the publicly observable trajectory of density operators remains unchanged.

The main contributions of this paper are the following.

- We introduce a geometric framework for mixed-state quantum information based on the purification bundle and the Uhlmann connection.
- We prove that the holonomy associated with a closed density-operator trajectory cannot be uniquely reconstructed from the base-space trajectory alone.
- We present a minimal geometric encoding primitive illustrating how classical information may be embedded in bundle-level holonomy while leaving the density-operator trajectory unchanged.
- We provide explicit examples for single-qubit and multi-qubit systems demonstrating how the proposed mechanism arises in practice.

This conceptual structure is illustrated in Figure 1.

This paper should therefore be viewed as a pre-protocol geometric framework identifying holonomy as a potential secrecy resource in mixed-state quantum information.

Contributions. The contributions of this work can be separated into two categories.

Conceptual contributions

- Identification of holonomy in the purification bundle as a geometric secrecy resource for mixed-state quantum systems.
- Formal separation between observable base-space information (density-operator trajectories) and hidden bundle-level data (purification gauge choices).
- A geometric reinterpretation of secrecy in terms of non-reconstructibility of holonomy from density-operator trajectories.

Technical contributions

- A formal adversarial model distinguishing public base-space observations from hidden bundle degrees of freedom.

- A proof that the holonomy associated with a closed density-operator trajectory is determined only up to conjugacy in the unitary group.
- A minimal geometric encoding primitive illustrating how classical symbols can be embedded in purification-bundle gauge choices.
- Explicit single-qubit and multi-qubit examples demonstrating Abelian and non-Abelian holonomy effects.
- A security model and indistinguishability definition based on distinguishability advantage.
- An analysis of potential attack surfaces and computational complexity of holonomy evaluation.

Research program perspective. The present work forms part of a broader research program investigating geometric resources for quantum cryptography. The first stage of this program identified discretized holonomy encodings as a geometric primitive for embedding discrete symbols into mixed-state quantum geometry through gauge choices in the purification bundle.

The present paper develops the structural, geometric, and information-theoretic foundations needed to interpret such bundle-level transformations as a secrecy resource.

In parallel work currently in preparation, we investigate how these primitives can be assembled into concrete holonomy-based cryptographic protocols, including key generation mechanisms and communication models based on mixed-state quantum geometry.

Organization of the paper. Section 2 introduces the assumptions and adversarial model. Section 3 reviews related work in geometric phases, quantum information geometry, and geometric approaches to quantum cryptography.

Section 4 explains why entanglement-based foliations fail in the mixed-state regime. Section 5 introduces the purification bundle and the Uhlmann connection.

Section 6 formalizes the distinction between public and secret geometric data. Section 7 establishes the non-reconstructibility theorem for holonomy.

Section 8 introduces a minimal geometric encoding primitive. Section 9 defines the secrecy model and the adversarial distinguishability advantage.

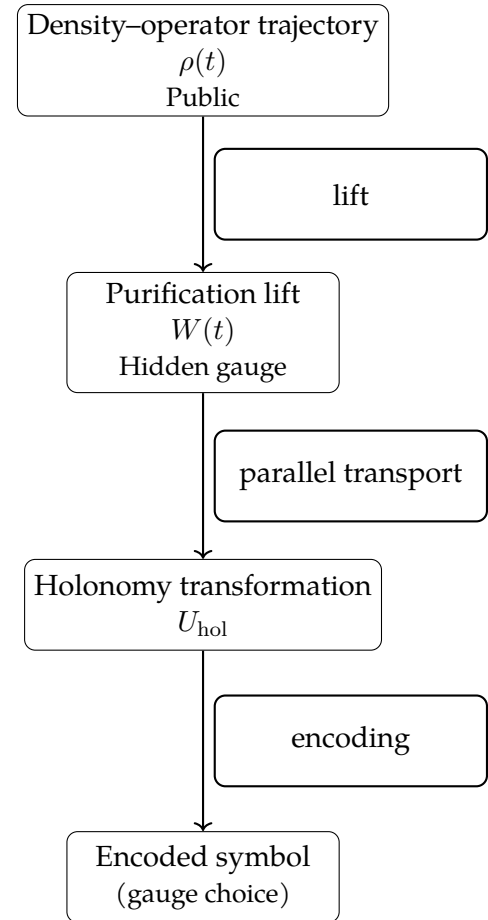


Figure 1. Conceptual structure of geometric secrecy. The observable density-operator trajectory $\rho(t)$ lies on the base manifold of the purification bundle. Different purification lifts $W(t)$ corresponding to different gauge choices generate distinct holonomy transformations even though the observable mixed-state evolution remains identical.

Section 10 analyzes possible attack surfaces, while Section 11 studies the computational complexity of holonomy evaluation.

Section 12 presents explicit single- and multi-qubit examples. Section 13 compares the proposed approach with entanglement-based frameworks.

Finally, Section 14 discusses complexity considerations and Section 15 concludes with open problems and directions for future work.

2 Assumptions and Scope

This section clarifies the assumptions, scope, and adversarial model considered in the present work. The objective of the paper is not to present a complete cryptographic protocol but to formalize a geometric secrecy resource that arises naturally in mixed-state quantum information. To avoid ambiguity, we explicitly distinguish the public data, the secret data,

and the observational capabilities of an adversary.

2.1 Quantum state space

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

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

where $\mathcal{D}(\mathcal{H})$ denotes the set of positive semidefinite operators of unit trace acting on $\mathcal{H}$ [3].

Throughout this work we restrict attention to *faithful density operators*, meaning that ρ is strictly positive and therefore invertible. The set of faithful density operators forms a smooth manifold equipped with natural information-theoretic Riemannian structures, most notably the Bures (quantum Fisher information) metric.

The faithful-state assumption is standard in the differential geometric treatment of quantum state space because it ensures that the manifold structure and associated geometric objects (connections, parallel transport, curvature) are well defined. Rank-deficient states lie on the boundary of the state space and introduce singularities in the information geometry. The extension of the framework to such states is an interesting problem but lies beyond the scope of the present work.

2.2 State trajectories

We consider smooth trajectories of density operators

$$\rho(t), \quad t \in [0, T],$$

in the manifold of faithful states. In particular, we will focus on closed trajectories satisfying

$$\rho(T) = \rho(0),$$

since holonomy is naturally associated with cyclic evolutions.

Such trajectories may arise physically from controlled quantum dynamics combined with noise processes, or from engineered open-system evolutions where the density operator follows a prescribed path in state space.

2.3 Public and secret data

The geometric framework introduced in this paper separates observable data from hidden geometric information.

Public data. The following information is assumed to be publicly accessible:

- the Hilbert space $\mathcal{H}$ and its dimension,
- the density-operator trajectory $\rho(t)$,
- the geometric structure of state space, including the Bures metric,
- the use of the canonical Uhlmann connection for parallel transport.

In principle, the trajectory $\rho(t)$ and its geometric properties can be reconstructed through quantum state tomography and statistical estimation.

Secret data. The hidden information considered in this work resides in the choice of purification lift of the trajectory.

Given a density operator ρ , a purification is an amplitude W satisfying

$$\rho = WW^\dagger.$$

Such amplitudes are defined only up to right multiplication by a unitary operator acting on the ancillary space. This unitary freedom defines a gauge degree of freedom.

The secret information therefore corresponds to a choice of initial purification (equivalently, a gauge choice) within the fiber of the purification bundle.

2.4 Adversarial model

We consider an adversary who has access to the publicly observable data described above. In particular, the adversary may perform:

- full quantum state tomography of the system,
- reconstruction of the density-operator trajectory $\rho(t)$,
- classical post-processing and numerical analysis of the trajectory and its geometric properties.

However, the adversary does not have access to the purification of the state, nor to the ancillary degrees of freedom used to implement the purification. As a result, the adversary can observe the base-space trajectory but not the lifted trajectory in the purification bundle.

2.5 Interpretation of secrecy

The notion of secrecy considered in this paper is geometric rather than directly operational. Informally, secrecy means that distinct purification lifts of the same density–operator trajectory may produce different holonomies, even though the observable mixed–state evolution remains identical.

This notion of secrecy should therefore be understood as *non–reconstructibility of bundle–level geometric information from base–space observations*. The development of full cryptographic protocols exploiting this resource is left for future work.

2.6 Scope of the present work

The goal of the present paper is to identify and formalize a geometric secrecy resource based on holonomy in the purification bundle. We do not claim information–theoretic security guarantees or provide a complete cryptographic protocol.

Instead, the paper establishes the geometric framework, clarifies the separation between public and secret data, and provides illustrative examples showing how identical mixed–state trajectories may encode different hidden geometric information.

The construction should therefore be interpreted as a *pre–protocol cryptographic framework* that identifies a potential resource for geometric encoding in noisy quantum systems.

3 Related Work

The geometric viewpoint adopted in this work draws on several well–established strands of research in quantum information theory, geometric phases, and quantum information geometry. Related geometric and information–theoretic aspects of quantum systems have also been discussed in recent work by the author [4, 5]. In this section we briefly review the most relevant contributions and clarify how the present framework differs from existing approaches.

3.1 Geometric phases and holonomy in quantum mechanics

The idea that geometric effects can encode physically observable information has a long history in quantum mechanics. One of the most prominent examples is the Berry phase [6], which arises when a quantum system undergoes adiabatic cyclic evolution. In such cases the state accumulates a phase determined not by dynamical properties but by the geometry of the parameter space.

More general formulations of geometric phase have since been developed. In particular, Aharonov and Anandan [7] showed that geometric phases arise for arbitrary cyclic quantum evolutions, without the adiabatic assumption. These developments revealed that geometric information associated with closed paths in quantum state space may lead to observable physical effects.

Alternative formulations of geometric phase for mixed states have also been proposed, including the kinematic approach of Tong et al. [8].

For mixed quantum states the situation is more subtle. Uhlmann introduced a notion of parallel transport and holonomy for density operators by lifting mixed states to purifications in an enlarged Hilbert space [2]. In this framework the geometric phase becomes a matrix–valued quantity known as the Uhlmann holonomy, which depends on the lifted trajectory in the purification bundle and generally takes values in the unitary group.

Subsequent work has explored related geometric structures for mixed states, including interferometric geometric phases and other operational formulations [9]. These developments demonstrate that holonomy and parallel transport play a fundamental role in the geometric description of mixed–state quantum systems.

Recent work has also investigated holonomy structures within the broader framework of quantum information geometry; see for example Andersson [10].

3.2 Quantum information geometry

The geometric framework used in this paper relies on the differential geometry of quantum state space. The manifold of density operators admits a natural family of monotone Riemannian metrics introduced by Petz [11]. Among these metrics, the Bures metric occupies a distinguished position because of its operational interpretation in quantum state discrimination. The geometric properties of the Bures metric and its curvature structure have been studied extensively in the literature; see, for example, Dittmann [12].

The Bures metric is closely related to the quantum Fisher information metric, coinciding with it up to a constant factor. This metric quantifies the statistical distinguishability of nearby quantum states and plays a central role in quantum parameter estimation. The relation between statistical distance and the geometry of quantum states was studied extensively

by Braunstein and Caves [13], building on earlier work in quantum detection theory [14].

More broadly, these constructions belong to the framework of information geometry, where statistical models are endowed with Riemannian and affine geometric structures. The information–geometric viewpoint adopted here is closely related to the general theory developed by Amari and Nagaoka [15].

These geometric structures provide a natural Riemannian framework in which density–operator trajectories can be analyzed independently of any specific physical implementation.

3.3 Geometric viewpoints in quantum cryptography

Quantum cryptography is traditionally formulated using operational tools from quantum information theory, with security proofs based on measurement disturbance, entropic uncertainty relations, and related principles. The earliest and most prominent example is the BB84 protocol [16], which established the possibility of secure key distribution based on quantum mechanics.

More recently, geometric perspectives have been proposed to reinterpret cryptographic processes in terms of structures on quantum state space. In particular, Di Cairano [1] introduced a geometric framework in which secrecy for pure bipartite states can be described using entanglement foliations of projective Hilbert space. In that picture, classical information can be encoded in the motion of quantum trajectories relative to hidden entanglement level sets.

While conceptually appealing, the foliation–based construction relies crucially on properties specific to pure states. Once mixed states are considered, scalar entanglement measures typically fail to define smooth foliations of state space, making the geometric encoding mechanism unstable in realistic noisy environments.

3.4 Position of the present work

The framework developed in this paper builds on these geometric ideas but proposes a different mechanism for encoding secrecy in the mixed–state regime. Rather than relying on scalar entanglement functionals, we identify holonomy in the purification bundle as the relevant geometric invariant.

In this setting the publicly observable data consist of the trajectory of density operators equipped with

the Bures geometry, while secrecy is associated with hidden gauge choices in the purification bundle. This shift from scalar foliations to bundle–level holonomy provides a geometric structure that remains well defined even in the presence of noise and mixed states.

The present work therefore aims to clarify how holonomy can serve as a geometric secrecy resource in mixed–state quantum information and how this perspective extends earlier geometric interpretations of quantum cryptography.

4 Why Entanglement Foliations Fail for Mixed States

The geometric encoding mechanism proposed for pure quantum states in [1] relies on the existence of a smooth scalar functional whose level sets define a regular foliation of the underlying state space. For pure bipartite states, such functionals arise naturally from entanglement measures. For example, the von Neumann entropy of the reduced density operator defines a smooth function on projective Hilbert space (away from measure–zero singularities), and its level sets determine hypersurfaces of constant entanglement.

In this setting, geometric motion of a quantum trajectory relative to these hypersurfaces can be used to encode classical information. In particular, a trajectory may move upward, downward, or tangentially with respect to the entanglement foliation, providing a geometric interpretation of secrecy in terms of hidden level–set structure.

While this picture is mathematically elegant, it relies critically on properties specific to pure states. Once mixed quantum states are considered, the foliation structure ceases to exist in a stable and well–defined form.

4.1 Mixed–state entanglement measures

Unlike the pure–state case, mixed–state entanglement does not admit a canonical scalar measure with smooth geometric properties. Most physically meaningful entanglement measures for mixed states are defined through convex–roof constructions [17]. Such measures are typically highly nonlocal and generically non–smooth functions of the density operator.

As a consequence, their level sets do not form smooth hypersurfaces in state space. Gradients may fail to exist or may vary discontinuously across large regions of the state space. This lack of regularity prevents

the construction of a well-defined geometric foliation based on entanglement level sets.

4.2 Instability near the separability boundary

The difficulties become particularly pronounced near the boundary between separable and entangled mixed states. In this region many entanglement measures develop non-analytic behavior due to the convex-roof optimization involved in their definition. Small perturbations of the density operator may lead to abrupt changes in the value or gradient of the entanglement measure.

From a geometric perspective, this behavior reflects the fact that the space of mixed states possesses a structure fundamentally different from that of projective Hilbert space. The boundary between separable and entangled states acts as a singular locus where scalar entanglement measures fail to provide a smooth geometric organization of the state space.

4.3 Information-geometric viewpoint

The geometry of mixed-state quantum systems is more naturally described using information-theoretic metrics defined directly on the manifold of density operators. Among these, the Bures metric plays a distinguished role because of its operational interpretation in quantum state discrimination and parameter estimation [13].

When equipped with the Bures metric, the space of faithful density operators becomes a smooth Riemannian manifold independent of any particular choice of entanglement measure. In this geometric setting, state trajectories are well defined even in the presence of noise and mixed states.

However, this geometry does not arise from the gradient of a scalar entanglement functional. Instead, the natural geometric structures that appear are connections, parallel transport, and holonomy.

4.4 Geometric shift from foliations to holonomy

The breakdown of entanglement foliations for mixed states therefore suggests a conceptual shift. Rather than encoding information through scalar functions on state space, one must consider geometric structures associated with lifted paths in a higher-dimensional bundle.

In the mixed-state setting, density operators admit purifications in an enlarged Hilbert space. These purifications form the fibers of a principal bundle over the manifold of density operators. Parallel transport

in this bundle is governed by the Uhlmann connection [2], which is canonically associated with the Bures geometry.

Holonomy arising from this parallel transport provides a global geometric invariant associated with closed trajectories of density operators. Importantly, this invariant depends on the lifted path in the purification bundle rather than solely on the base-space trajectory.

This observation motivates the central idea of the present work: in the mixed-state regime, secrecy may be associated with hidden gauge choices in the purification bundle, while the observable density-state trajectory remains public.

The following section develops the geometric framework required to formalize this perspective.

5 Geometric Framework

In this section we introduce the geometric structures underlying the framework proposed in this work. The construction relies on the information geometry of density operators, the purification bundle, and the notion of parallel transport induced by the Uhlmann connection.

5.1 Density operators and the Bures geometry

Let $\mathcal{H}$ be a complex Hilbert space of finite dimension d . Denote by

$$\mathcal{D}(\mathcal{H})$$

the set of density operators on $\mathcal{H}$,

$$\mathcal{D}(\mathcal{H}) = \{\rho \in \mathcal{B}(\mathcal{H}) : \rho \geq 0, \quad \text{Tr}(\rho) = 1\}.$$

We restrict attention to the subset of *faithful* density operators

$$\mathcal{D}^+(\mathcal{H}) = \{\rho \in \mathcal{D}(\mathcal{H}) : \rho > 0\},$$

which forms a smooth manifold of real dimension $d^2 - 1$.

The tangent space at a point $\rho \in \mathcal{D}^+(\mathcal{H})$ can be identified with the vector space

$$T_\rho \mathcal{D}^+(\mathcal{H}) = \{X \in \mathcal{B}(\mathcal{H}) : X = X^\dagger, \quad \text{Tr}(X) = 0\}.$$

Among the family of monotone Riemannian metrics on $\mathcal{D}^+(\mathcal{H})$ introduced by Petz [11], the Bures metric [18] plays a distinguished role.

Given a smooth curve $\rho(t)$ in the manifold of faithful states, the tangent vector

$$\dot{\rho} = \frac{d\rho}{dt}$$

admits an associated symmetric logarithmic derivative (SLD) $L_{\dot{\rho}}$ defined implicitly by

$$\dot{\rho} = \frac{1}{2} (\rho L_{\dot{\rho}} + L_{\dot{\rho}} \rho). \quad (1)$$

The quantum Fisher information metric is then defined as

$$g_{\text{QFI}}(\dot{\rho}, \dot{\rho}) = \frac{1}{2} \text{Tr} (\rho L_{\dot{\rho}}^2), \quad (2)$$

which coincides (up to a constant factor) with the Bures metric [13].

The pair

$$(\mathcal{D}^+(\mathcal{H}), g_{\text{Bures}})$$

therefore defines a Riemannian manifold whose geometric properties are determined entirely by the observable density operators.

5.2 Purification bundle

Mixed quantum states admit purifications in an enlarged Hilbert space. Let

$$\mathcal{H}_A = \mathcal{H}, \quad \mathcal{H}_B = \mathcal{H}$$

and consider the composite Hilbert space

$$\mathcal{H}_A \otimes \mathcal{H}_B.$$

Definition 5.1 (Purification). A purification of a density operator ρ is a vector $|\Psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$ satisfying

$$\rho = \text{Tr}_B (|\Psi\rangle\langle\Psi|). \quad (3)$$

An equivalent formulation uses amplitudes.

Let

$$W \in \mathcal{B}(\mathcal{H})$$

be an operator satisfying

$$\rho = WW^\dagger. \quad (4)$$

Such an operator W is called an *amplitude* of ρ .

Amplitudes are not unique. If

$$U \in U(d)$$

is a unitary operator, then

$$W \mapsto WU \quad (5)$$

produces another amplitude representing the same density operator.

Proposition 5.2. *The set of amplitudes of ρ forms a fiber isomorphic to the unitary group $U(d)$.*

Consequently, the collection of all amplitudes defines a principal fiber bundle

$$\pi : \mathcal{P} \rightarrow \mathcal{D}^+(\mathcal{H}),$$

called the *purification bundle*, where

$$\pi(W) = WW^\dagger.$$

The base space consists of density operators, while the fibers correspond to unitary gauge transformations.

5.3 Uhlmann connection

To compare purifications along a trajectory in the base manifold, one must specify a notion of parallel transport.

Let $\rho(t)$ be a smooth curve in $\mathcal{D}^+(\mathcal{H})$ and let $W(t)$ be a lift of this curve in the purification bundle,

$$\rho(t) = W(t)W(t)^\dagger.$$

The Uhlmann connection is defined by the horizontality condition

$$W^\dagger \dot{W} = \dot{W}^\dagger W. \quad (6)$$

Equivalently,

$$W^\dagger \dot{W} \text{ is Hermitian.} \quad (7)$$

This condition ensures that the lifted path minimizes the Hilbert–Schmidt distance between neighboring purifications.

Proposition 5.3. *Given a base-space trajectory $\rho(t)$ and an initial amplitude $W(0)$, there exists a unique horizontal lift satisfying the Uhlmann parallel transport condition.*

Thus the Uhlmann connection defines a canonical notion of parallel transport in the purification bundle that depends only on the Bures geometry of the base manifold.

5.4 Holonomy

Consider a closed trajectory

$$\rho(0) = \rho(T)$$

in the manifold of density operators.

Let $W(t)$ denote the horizontal lift of this trajectory starting from an initial amplitude $W(0)$.

In general the final amplitude satisfies

$$W(T) = W(0) U_{\text{hol}}, \quad (8)$$

where

$$U_{\text{hol}} \in U(d)$$

is a unitary operator known as the *Uhlmann holonomy*.

The holonomy depends on the entire lifted path and therefore represents a global geometric invariant associated with the closed trajectory $\rho(t)$.

Importantly, the base-space density operator remains unchanged,

$$W(T)W(T)^\dagger = W(0)W(0)^\dagger = \rho(0),$$

so the holonomy cannot be inferred from the density operator alone.

This separation between observable base-space dynamics and hidden bundle-level transformations forms the geometric basis of the secrecy mechanism studied in this paper.

6 Public vs Secret Data and Adversarial Model

The geometric framework introduced in the previous section naturally separates observable information from hidden geometric data. In this section we formalize this distinction and describe the adversarial model considered in the present work.

6.1 Public geometric data

Let

$$\rho(t), \quad t \in [0, T],$$

be a smooth trajectory in the manifold of faithful density operators $\mathcal{D}^+(\mathcal{H})$.

The following information is assumed to be publicly accessible:

1. the Hilbert space $\mathcal{H}$ and its dimension d ,
2. the density-operator trajectory $\rho(t)$,
3. the information-geometric structure of the state space, including the Bures metric,
4. the use of the canonical Uhlmann connection for parallel transport.

In principle, the trajectory $\rho(t)$ can be reconstructed through quantum state tomography and classical post-processing. An observer may therefore determine geometric quantities such as distances, curvature properties, or the Bures length of the path.

We refer to this information collectively as the *public base-space data*.

6.2 Hidden bundle data

While the base-space trajectory $\rho(t)$ is observable, the lifted trajectory in the purification bundle depends on an additional choice of gauge.

Let

$$W(t)$$

be a horizontal lift satisfying

$$\rho(t) = W(t)W(t)^\dagger.$$

The initial amplitude

$$W(0)$$

is not uniquely determined by the density operator $\rho(0)$. If

$$U \in U(d)$$

is a unitary operator, then

$$W(0) \longrightarrow W(0)U$$

defines another valid initial amplitude representing the same density operator.

This unitary freedom corresponds to the gauge symmetry of the purification bundle.

Definition 6.1 (Secret gauge choice). The secret information considered in this work is the choice of the initial purification gauge

$$U_{\text{key}} \in U(d),$$

which determines the lifted trajectory in the purification bundle.

Different gauge choices lead to different lifted trajectories and may produce distinct holonomies, even when the observable density–operator trajectory is identical.

6.3 Adversarial capabilities

We consider an adversary who has access to all publicly observable data associated with the density–operator trajectory.

In particular, the adversary may perform:

- full quantum state tomography of the system,
- reconstruction of the trajectory $\rho(t)$,
- numerical computation of geometric quantities derived from the Bures metric,
- classical post–processing of the observed trajectory.

However, the adversary does not have access to the purification of the state, nor to the ancillary degrees of freedom used to implement the purification. As a consequence, the adversary observes only the base–space trajectory in $\mathcal{D}^+(\mathcal{H})$.

6.4 Geometric notion of secrecy

The secrecy mechanism proposed in this work relies on the fact that bundle–level geometric information cannot in general be reconstructed from base–space observations.

Informally, secrecy arises when two different lifted trajectories

$$W_1(t), \quad W_2(t)$$

project to the same density–operator trajectory

$$\rho(t)$$

but accumulate different holonomies.

The following section formalizes this statement.

7 Non–Reconstructibility of Holonomy

We now formalize the central geometric property underlying the secrecy mechanism proposed in this work.

Theorem 7.1 (Gauge non–reconstructibility). *Let*

$$\rho(t), \quad t \in [0, T],$$

be a closed trajectory in the manifold of faithful density operators such that

$$\rho(T) = \rho(0).$$

Let

$$W_1(t), \quad W_2(t)$$

be two horizontal lifts of this trajectory satisfying

$$W_2(0) = W_1(0)U,$$

for some unitary operator

$$U \in U(d).$$

Then the corresponding holonomies satisfy

$$U_{\text{hol}}^{(2)} = U^{-1}U_{\text{hol}}^{(1)}U.$$

Consequently, knowledge of the density–operator trajectory $\rho(t)$ determines the holonomy only up to conjugation in $U(d)$.

In particular, the exact holonomy cannot be uniquely reconstructed from base–space data alone.

Proof. Let $W_1(t)$ denote a horizontal lift of the trajectory $\rho(t)$ with initial amplitude $W_1(0)$.

Define

$$W_2(t) = W_1(t)U.$$

Since right multiplication by a constant unitary does not affect the horizontality condition, $W_2(t)$ is also a horizontal lift of the same base–space trajectory.

For the first lift we have

$$W_1(T) = W_1(0)U_{\text{hol}}^{(1)}.$$

For the second lift we obtain

$$W_2(T) = W_1(T)U = W_1(0)U_{\text{hol}}^{(1)}U.$$

On the other hand,

$$W_2(T) = W_2(0)U_{\text{hol}}^{(2)} = W_1(0)U U_{\text{hol}}^{(2)}.$$

Equating the two expressions yields

$$U_{\text{hol}}^{(2)} = U^{-1}U_{\text{hol}}^{(1)}U.$$

The theorem shows that the observable density–operator trajectory determines at most the conjugacy class of the holonomy in the unitary group. The precise bundle–level transformation depends on the initial gauge choice, which is not accessible through state–space observations.

This gauge ambiguity forms the geometric basis of the secrecy mechanism discussed in the remainder of the paper.

8 Minimal Encoding Primitive

The geometric framework developed in the previous sections suggests a natural mechanism for encoding classical information using holonomy in the purification bundle. In this section we introduce a minimal encoding primitive illustrating how hidden geometric information can be associated with observable mixed–state trajectories.

The goal of this construction is not to define a complete cryptographic protocol, but rather to demonstrate how holonomy can act as an information–bearing resource in a mixed–state setting.

8.1 Message space

Let

$$\mathcal{M} = \{1, \dots, K\}$$

denote a finite message space.

Each message $m \in \mathcal{M}$ will be associated with a distinct unitary element

$$U_m \in U(d),$$

which determines a gauge transformation in the purification bundle.

The collection

$$\mathcal{U} = \{U_1, \dots, U_K\} \subset U(d)$$

therefore defines the geometric encoding alphabet.

8.2 Public trajectory

Let

$$\rho(t), \quad t \in [0, T],$$

□

be a fixed closed trajectory in the manifold of faithful density operators satisfying

$$\rho(T) = \rho(0).$$

This trajectory is assumed to be publicly known and can in principle be reconstructed through tomography.

The geometric data observable to an external observer therefore consist entirely of the density–operator path $\rho(t)$ equipped with the Bures geometry introduced in Section 5.

8.3 Encoding

Let $W(t)$ denote a horizontal lift of $\rho(t)$ with initial amplitude $W(0)$.

To encode a message $m \in \mathcal{M}$ the sender modifies the initial purification according to

$$W_m(0) = W(0)U_m.$$

The lifted trajectory then evolves according to the Uhlmann parallel transport condition.

Since right multiplication by a constant unitary does not affect the projection onto the density–operator manifold, the resulting density trajectory remains unchanged:

$$\rho_m(t) = W_m(t)W_m(t)^\dagger = \rho(t).$$

Thus all encoded messages generate the same publicly observable mixed–state evolution.

8.4 Resulting holonomy

Let

$$U_{\text{hol}}$$

denote the holonomy associated with the reference lift $W(t)$.

For the encoded trajectory the resulting holonomy becomes

$$U_{\text{hol}}^{(m)} = U_m^{-1}U_{\text{hol}}U_m.$$

Thus the encoded message determines the conjugacy class of the holonomy transformation.

Importantly, this transformation acts entirely in the fiber of the purification bundle and does not modify the observable density–state trajectory.

8.5 Decoding

If the receiver has access to the purification degrees of freedom or to an interferometric measurement sensitive to the holonomy, the encoded unitary transformation can be recovered.

In contrast, an observer limited to the base–space trajectory $\rho(t)$ cannot distinguish between different encoded messages.

8.6 Interpretation

The encoding mechanism described above illustrates how classical information may be stored in bundle–level geometric degrees of freedom while leaving the observable mixed–state evolution unchanged.

The secrecy of the encoded information therefore relies on the non–reconstructibility of holonomy from density–operator trajectories established in Section 7.

This construction should be interpreted as a minimal geometric encoding primitive rather than a complete cryptographic protocol. Designing full communication protocols based on this principle is an interesting direction for future work.

9 Security Model and Secrecy Definition

The geometric encoding primitive introduced in the previous section naturally raises the question of how secrecy should be formalized within the present framework. Since the construction is based on bundle geometry rather than on standard quantum communication protocols, the security notion must first be defined at the level of observable information.

9.1 Observable information

Let

$$\rho(t), \quad t \in [0, T]$$

be the publicly observable trajectory of density operators in the manifold of faithful states $\mathcal{D}^+(H)$.

An external observer is assumed to have access to

- the Hilbert space H and its dimension d ,
- the complete density–operator trajectory $\rho(t)$,
- the Bures / quantum Fisher information geometry,
- the use of the canonical Uhlmann connection.

Through quantum state tomography and classical post–processing, the adversary may therefore reconstruct the full base–space trajectory

$$\Gamma_{\text{base}} := \{\rho(t)\}_{t \in [0, T]}.$$

However, the adversary does not have access to the purification degrees of freedom associated with the bundle projection

$$\pi : W \rightarrow \mathcal{D}^+(H), \quad \pi(\psi) = \psi\psi^\dagger.$$

Consequently, only the base-space trajectory is observable, while the lifted trajectory in the purification bundle

$$\psi(t)$$

remains hidden.

9.2 Adversarial capabilities

We consider an adversary $\mathcal{A}$ with the following capabilities:

1. full quantum state tomography of the system,
2. unlimited classical computation,
3. numerical reconstruction of geometric quantities derived from the Bures metric.

However, the adversary does not have access to the ancillary system used for purification and therefore cannot observe the lifted trajectory in the purification bundle.

Formally, the adversary receives the public data

$$\mathcal{O} = \Gamma_{\text{base}}.$$

9.3 Encoding map

Let

$$M = \{1, \dots, K\}$$

denote a finite message space.

Each message $m \in M$ corresponds to a gauge element

$$U_m \in U(d)$$

which modifies the initial purification

$$\psi_m(0) = \psi(0)U_m.$$

Under Uhlmann parallel transport the lifted trajectory generates the holonomy

$$U_{\text{hol}}^{(m)} = U_m^{-1}U_{\text{hol}}U_m.$$

The publicly observable trajectory remains

$$\rho_m(t) = \rho(t).$$

9.4 Geometric secrecy

The secrecy of the encoding relies on the fact that the holonomy transformation cannot be uniquely reconstructed from base-space observations.

Let

$$\mathcal{H}(\rho(t))$$

denote the holonomy determined by a closed trajectory of density operators.

From Theorem 7.1 we know that the observable trajectory determines only the conjugacy class

$$[U_{\text{hol}}] = \{V^{-1}U_{\text{hol}}V \mid V \in U(d)\}.$$

The specific representative

$$U_{\text{hol}}$$

depends on the secret gauge choice and is therefore not observable from $\rho(t)$ alone.

9.5 Distinguishability advantage

Let $\mathcal{A}$ be an adversary attempting to infer the encoded message m from the observable trajectory Γ_{base} .

The adversary outputs a guess $\hat{m}$.

Following the standard indistinguishability framework used in modern cryptography [19, 20], the distinguishing advantage of the adversary is defined as

$$\text{Adv}_{\mathcal{A}} = \left| \Pr[\hat{m} = m] - \frac{1}{|M|} \right|.$$

The quantity $\frac{1}{|M|}$ corresponds to the success probability of random guessing in the absence of any information about the encoded message.

A scheme achieves *perfect geometric secrecy* if

$$\text{Adv}_{\mathcal{A}} = 0$$

for every adversary $\mathcal{A}$ observing the density-operator trajectory.

In the present framework this condition holds whenever the observable density-operator trajectory $\rho(t)$ is independent of the encoded message.

9.6 Perfect geometric secrecy

The encoding primitive satisfies *perfect geometric secrecy* if for every adversary $\mathcal{A}$

$$\text{Adv}_{\mathcal{A}} = 0.$$

This condition holds whenever the observable trajectory $\rho(t)$ is independent of the encoded message.

$$\rho_m(t) = \rho(t) \quad \forall m \in M. \quad (9)$$

In this case the adversary's observations provide no information about the chosen gauge element.

9.7 Interpretation

The secrecy notion considered here differs from traditional information-theoretic security.

Instead of relying on measurement disturbance or entropic uncertainty, secrecy arises from a geometric non-reconstructibility property: bundle-level holonomy cannot be determined from base-space data.

This geometric separation between observable and hidden structures forms the conceptual foundation for holonomy-based cryptographic constructions.

10 Attack Surfaces and Security Considerations

The geometric secrecy mechanism proposed in this work relies on the separation between observable base-space data and hidden bundle-level information. In this section we analyze potential attack strategies available to an adversary and explain why these attacks cannot recover the secret gauge information.

10.1 Tomographic reconstruction attacks

The most natural attack strategy is full quantum state tomography of the system.

Given sufficiently many copies of the quantum state, an adversary may reconstruct the density-operator trajectory

$$\rho(t), \quad t \in [0, T].$$

This reconstruction provides complete knowledge of the base-space trajectory in the manifold of density operators.

However, tomography determines only the density operators themselves and does not reveal the purification amplitudes satisfying

$$\rho(t) = W(t)W(t)^\dagger.$$

Since amplitudes are defined only up to right multiplication by a unitary element

$$W(t) \rightarrow W(t)U,$$

the reconstructed trajectory does not uniquely determine the lifted path in the purification bundle.

Consequently, tomography cannot recover the holonomy representative associated with the secret gauge choice.

10.2 Geometric reconstruction attacks

An adversary might attempt to infer the holonomy from geometric properties of the trajectory such as

- Bures length of the path,
- curvature of the density-operator manifold,
- fidelity relations between nearby states.

All such quantities are functions of the base-space trajectory and are therefore gauge-invariant.

Since the holonomy representative depends on the choice of lift in the purification bundle, these geometric observables determine at most the conjugacy class of the holonomy but not the specific unitary transformation associated with the secret gauge.

10.3 Algebraic reconstruction attacks

Another possible strategy is to exploit algebraic properties of the density operators along the trajectory.

For instance, an adversary may compute the spectral decomposition

$$\rho(t) = \sum_i \lambda_i(t) |e_i(t)\rangle \langle e_i(t)|$$

and attempt to track the evolution of eigenvectors.

However, the purification bundle introduces an additional unitary gauge freedom acting on the ancillary system.

This gauge freedom implies that distinct lifted trajectories may correspond to the same family of density operators.

Therefore, algebraic analysis of eigenvalues and eigenvectors does not determine the secret holonomy transformation.

10.4 Structural attacks on the encoding

The encoding primitive associates messages $m \in M$ with gauge elements

$$U_m \in U(d).$$

An adversary observing only the density-operator trajectory obtains no information about the chosen gauge element because the observable states satisfy

$$\rho_m(t) = \rho(t)$$

for all m .

Thus the message space is information-theoretically hidden from any adversary restricted to base-space observations.

10.5 Noise robustness

An advantage of the geometric framework is that the observable trajectory is defined directly at the level of density operators.

Noise and decoherence modify the trajectory $\rho(t)$ but do not eliminate the gauge freedom in the purification bundle.

As a result, the geometric separation between base-space information and bundle-level holonomy persists even in noisy mixed-state settings.

11 Computational Complexity of Holonomy Computation

The geometric encoding mechanism introduced in this work relies on the computation of holonomy associated with a closed trajectory of density operators in the purification bundle. In this section we briefly analyze the computational cost of evaluating this quantity and its scaling with system dimension.

11.1 Parallel transport computation

Let

$$\rho(t), \quad t \in [0, T]$$

be a smooth trajectory of density operators in the manifold of faithful states.

The horizontal lift of this trajectory satisfies the Uhlmann parallel transport condition

$$W^\dagger \dot{W} = \dot{W}^\dagger W.$$

In practice, computing the lifted trajectory requires integrating the associated differential equation along the path.

If the trajectory is discretized into N time steps, the transport operator can be approximated as a time-ordered product

$$\Gamma \approx \prod_{k=1}^N \exp(-A_k \Delta t),$$

where A_k denotes the connection form evaluated at the k -th step.

11.2 Matrix operation cost

For a Hilbert space of dimension d , each step of the transport computation involves matrix operations of dimension $d \times d$.

Typical operations include

- matrix multiplication,
- matrix square roots,
- spectral decomposition.

The computational cost of these operations scales as

$$O(d^3)$$

using standard linear algebra algorithms.

Consequently, the total cost of computing the holonomy along a discretized trajectory scales approximately as

$$O(Nd^3).$$

11.3 Scalability

For low-dimensional systems such as qubits and small multi-qubit systems, the computational overhead remains modest. In higher-dimensional systems, however, the cost grows polynomially with system size.

Importantly, this computational cost affects only the legitimate participants performing the holonomy evaluation. An adversary restricted

to observing the density-operator trajectory cannot reconstruct the bundle-level transformation regardless of computational power, due to the gauge non-reconstructibility property established in Section 7.

11.4 Implications for protocol design

Future holonomy-based cryptographic protocols may benefit from restricting the encoding alphabet to finite subgroups of the unitary group, such as

$$\mathbb{Z}_n \subset U(d),$$

which would reduce the complexity of decoding and simplify the implementation of geometric encoding schemes.

A detailed complexity analysis of concrete protocol implementations will be addressed in future work.

12 Illustrative Examples

In this section we illustrate the geometric encoding mechanism introduced in Section 8 through two explicit examples. The first example considers a single-qubit mixed-state trajectory, while the second example demonstrates how non-Abelian holonomy arises in higher-dimensional systems.

12.1 Single-qubit mixed-state loop

Consider a single qubit with Hilbert space

$$\mathcal{H} = \mathbb{C}^2.$$

Every density operator can be written in Bloch form

$$\rho = \frac{1}{2} (I + \vec{r} \cdot \vec{\sigma}), \quad (10)$$

where

$$\vec{r} \in \mathbb{R}^3, \quad |\vec{r}| < 1,$$

and

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

denotes the vector of Pauli matrices.

Consider the closed trajectory

$$\vec{r}(t) = r \begin{pmatrix} \sin \theta \cos \phi(t) \\ \sin \theta \sin \phi(t) \\ \cos \theta \end{pmatrix}, \quad (11)$$

where

$$\phi(t) = \frac{2\pi t}{T}, \quad t \in [0, T].$$

This trajectory corresponds to a circle of constant latitude on the Bloch sphere with radius r .

The corresponding density-operator path is

$$\rho(t) = \frac{1}{2} (I + r \sin \theta (\cos \phi(t) \sigma_x + \sin \phi(t) \sigma_y) + r \cos \theta \sigma_z). \quad (12)$$

A purification of $\rho(t)$ can be written using the amplitude

$$W(t) = \sqrt{\rho(t)}. \quad (13)$$

The Uhlmann holonomy associated with this loop can be computed explicitly [2]. One finds

$$U_{\text{hol}} = \exp \left(-i \frac{\Omega}{2} \sigma_z \right), \quad (14)$$

where Ω denotes the solid angle enclosed by the trajectory on the Bloch sphere.

Thus the holonomy acts as a phase rotation around the z -axis.

If the initial purification is modified according to

$$W(0) \rightarrow W(0)U_m, \quad (15)$$

the resulting holonomy becomes

$$U_{\text{hol}}^{(m)} = U_m^{-1} U_{\text{hol}} U_m. \quad (16)$$

The observable density trajectory $\rho(t)$ remains unchanged.

12.2 Two-qubit example and non-Abelian holonomy

We now consider a two-qubit system

$$\mathcal{H} = \mathbb{C}^2 \otimes \mathbb{C}^2.$$

Let

$$\rho(t) = \sum_{i=1}^4 \lambda_i(t) |e_i(t)\rangle \langle e_i(t)| \quad (17)$$

be a spectral decomposition of a density operator trajectory, where

$$\lambda_i(t) > 0, \quad \sum_i \lambda_i(t) = 1.$$

Assume that the eigenvectors evolve according to

$$|e_i(t)\rangle = V(t) |e_i(0)\rangle, \quad (18)$$

with

$$V(t) \in SU(4).$$

The density trajectory then becomes

$$\rho(t) = V(t) \rho(0) V(t)^\dagger. \quad (19)$$

A purification amplitude can be written as

$$W(t) = \sqrt{\rho(t)} V(t). \quad (20)$$

In this higher-dimensional setting the Uhlmann holonomy is a general unitary matrix

$$U_{\text{hol}} \in U(4).$$

Because the unitary group is non-Abelian for dimension $d > 1$, the holonomy transformations do not commute in general.

For two loops γ_1 and γ_2 in the density-operator manifold one may obtain

$$U_{\text{hol}}(\gamma_1) U_{\text{hol}}(\gamma_2) \neq U_{\text{hol}}(\gamma_2) U_{\text{hol}}(\gamma_1). \quad (21)$$

This non-commutativity reflects the non-Abelian structure of the Uhlmann connection.

Consequently, geometric encodings based on holonomy in higher dimensions naturally possess a richer algebraic structure than the single-qubit case.

12.3 Implications for geometric encoding

The examples above illustrate two key properties of the proposed framework:

1. identical density-operator trajectories may correspond to distinct bundle-level transformations,
2. in higher-dimensional systems the resulting holonomies form a non-Abelian unitary group.

These properties suggest that geometric encodings based on holonomy may support richer algebraic structures than scalar geometric phases.

13 Operational Comparison with Entanglement-Based Frameworks

The geometric encoding mechanism introduced in this work differs substantially from entanglement-based approaches traditionally used in quantum cryptography. In particular, the secrecy resource is not a scalar functional on state space but a bundle-level geometric invariant.

In this section we briefly compare the two viewpoints.

13.1 Conceptual differences

Entanglement-based cryptographic frameworks typically rely on scalar entanglement measures defined on bipartite quantum states. These quantities act as monotonic resources under local operations and classical communication (LOCC) and can therefore serve as indicators of cryptographic capability.

In contrast, the framework developed here relies on geometric structures associated with parallel transport in the purification bundle. The relevant invariant is the holonomy transformation generated by closed density-operator trajectories.

The Table 1 summarizes the main conceptual differences.

13.2 Operational perspective

In entanglement-based constructions, secrecy is typically associated with correlations between subsystems that cannot be reproduced by classical shared randomness.

In the holonomy-based framework proposed here, secrecy arises from the inability of an observer

Table 1. Conceptual comparison between entanglement-based and holonomy-based geometric frameworks for mixed-state quantum cryptography.

Feature	Entanglement based	Holonomy based
Resource type	Scalar functional	Bundle holonomy
Underlying geometry	Level sets in state space	Parallel transport in bundle
Typical invariant	Entanglement entropy	Uhlmann holonomy
Dependence on noise	Often unstable	Naturally defined for mixed states
Algebraic structure	Scalar quantity	Unitary group element
Information carrier	Position relative to level sets	Gauge degree of freedom

restricted to base-space information to reconstruct bundle-level geometric transformations.

This difference reflects a shift from a *state-based resource* (entanglement) to a *path-dependent geometric resource* (holonomy).

13.3 Advantages of the geometric approach

The geometric perspective offers several potential advantages:

- The framework remains well defined for mixed states and noisy quantum evolutions.
- The encoding space is a unitary group rather than a scalar parameter, allowing richer algebraic structures.
- The mechanism relies on geometric properties of state space rather than on bipartite entanglement structure.

These features suggest that holonomy-based encodings may complement existing quantum cryptographic resources.

14 Complexity and Attack Surfaces

In this section we briefly discuss the computational complexity of the geometric quantities involved in the proposed framework and outline possible attack strategies.

14.1 Computational complexity

The main geometric object appearing in the framework is the Uhlmann holonomy associated with a density-operator trajectory.

Given a discretized trajectory

$$\rho_0, \rho_1, \dots, \rho_n,$$

the computation of the corresponding parallel transport requires evaluating matrix square roots and unitary polar decompositions.

For density operators acting on a Hilbert space of dimension d , these operations typically require

$$O(d^3)$$

time using standard numerical linear algebra algorithms.

Consequently, the complexity of computing the holonomy along a trajectory with n discretization steps scales as

$$O(nd^3).$$

While polynomial in the Hilbert-space dimension, the computational cost may become significant for very large systems.

14.2 Potential attack strategies

Several classes of attacks may be considered against holonomy-based encodings.

Tomographic reconstruction. An adversary may attempt to reconstruct the density-operator trajectory through repeated measurements. However, as established in Theorem 7, the trajectory alone does not determine the holonomy uniquely.

Geometric inference. An attacker might attempt to infer hidden geometric information by analyzing the curvature or metric properties of the trajectory. Such information remains confined to the base manifold and does not reveal the bundle-level gauge choice.

Ancilla leakage. If the adversary obtains access to the purification ancilla, the hidden gauge degrees of freedom may become observable. Protecting the ancillary subsystem is therefore essential for maintaining secrecy.

Noise sensitivity. In realistic implementations noise may perturb the lifted trajectory and modify the resulting holonomy. Studying the robustness of holonomy-based encodings under noisy evolution remains an important direction for future work.

14.3 Summary

The geometric secrecy mechanism proposed in this paper relies on a fundamental separation between observable density-operator dynamics and hidden bundle-level transformations.

While the computation of holonomy is polynomial in system size, recovering the secret gauge choice from base-space observations alone appears fundamentally impossible within the framework described above.

15 Conclusion and Outlook

This work explores a geometric perspective on secrecy in mixed-state quantum information. Instead of relying on scalar entanglement measures, we investigate holonomy arising from parallel transport in the purification bundle of density operators.

The central observation is that density-operator trajectories describe only the base manifold of the purification bundle. Different lifts of the same trajectory may generate distinct bundle-level holonomies, while the observable mixed-state evolution remains identical. This separation between observable and hidden geometric data provides the basis for a potential secrecy mechanism.

We formalized this idea by proving that the holonomy associated with a closed density-operator trajectory cannot be uniquely reconstructed from base-space information alone. We further introduced a minimal encoding primitive illustrating how classical information may be associated with bundle-level gauge choices while leaving the density-state trajectory unchanged.

Several open questions remain for future work. In particular, the development of full cryptographic protocols based on holonomy-based encodings remains an important challenge. Additional directions include the analysis of robustness under realistic noise models, scalability to high-dimensional systems, and experimental implementations using controllable open quantum systems.

More broadly, the framework developed here represents one step in a larger program toward holonomy-based cryptographic constructions.

The first stage of this program identified discretized holonomy encodings as a geometric primitive for embedding discrete symbols into mixed-state quantum geometry through gauge choices in the purification bundle. The present work develops the structural and information-theoretic foundations of secrecy associated with such geometric mechanisms.

Current work in preparation investigates how these primitives can be assembled into full cryptographic protocols, including key generation mechanisms and concrete communication models exploiting holonomy-based encoding.

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 generative AI tools were used in the preparation of this manuscript for drafting, language editing, and translation purposes. Specifically, ChatGPT-5 was utilized to assist with manuscript preparation. The author reviewed and revised the generated content as necessary and takes full responsibility for the final content of the manuscript.

Ethical Approval and Consent to Participate

Not applicable.

References

- [1] Di Cairano, L. (2025). Secret Entanglement, Public Geometry. Quantum Cryptography from a Geometric Perspective. *arXiv preprint arXiv:2511.22984*. [CrossRef]
- [2] Uhlmann, A. (1986). Parallel transport and “quantum holonomy” along density operators. *Reports on Mathematical Physics*, 24(2), 229-240. [CrossRef]

- [3] Nielsen, M. A., & Chuang, I. L. (2010). *Quantum computation and quantum information*. Cambridge university press.
- [4] Sjöqvist, E. (2015). Geometric phases in quantum information. *International Journal of Quantum Chemistry*, 115(19), 1311-1326. [CrossRef]
- [5] El MORSALANI, M. (2024). *Quantum and Post-Quantum Cryptography: Principles, Protocols, and Challenges* [Preprint]. ResearchGate. https://www.researchgate.net/publication/385041521_Quantum_and_Post-Quantum_Cryptography_Principles_Protocols_and_Challenges
- [6] Berry, M. V. (1984). Quantal phase factors accompanying adiabatic changes. *Proceedings of the Royal Society of London. A. Mathematical and Physical Sciences*, 392(1802), 45-57. [CrossRef]
- [7] Aharonov, Y., & Anandan, J. (1987). Phase change during a cyclic quantum evolution. *Physical Review Letters*, 58(16), 1593. [CrossRef]
- [8] Tong, D. M., Sjöqvist, E., Kwek, L. C., & Oh, C. H. (2004). Kinematic approach to the mixed state geometric phase in nonunitary evolution. *Physical review letters*, 93(8), 080405. [CrossRef]
- [9] 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. [CrossRef]
- [10] Andersson, O. (2019). Holonomy in quantum information geometry. *arXiv preprint arXiv:1910.08140*. [arXiv]
- [11] Petz, D. (1996). Monotone metrics on matrix spaces. *Linear algebra and its applications*, 244, 81-96. [CrossRef]
- [12] 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]
- [13] Braunstein, S. L., & Caves, C. M. (1994). Statistical distance and the geometry of quantum states. *Physical Review Letters*, 72(22), 3439. [CrossRef]
- [14] Helstrom, C. W. (1969). Quantum detection and estimation theory. *Journal of statistical physics*, 1(2), 231-252. [CrossRef]
- [15] Amari, S. I., & Nagaoka, H. (2000). *Methods of information geometry* (Vol. 191). American Mathematical Soc.
- [16] Uhlmann, A. (1991). A gauge field governing parallel transport along mixed states. *letters in mathematical physics*, 21(3), 229-236. [CrossRef]
- [17] Vedral, V., & Plenio, M. B. (1998). Entanglement measures and purification procedures. *Physical Review A*, 57(3), 1619. [CrossRef]
- [18] 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]
- [19] Goldreich, O. (2004). *Foundations of cryptography, volume 2*. Cambridge: Cambridge university press.
- [20] Katz, J., & Lindell, Y. (2007). *Introduction to modern cryptography: principles and protocols*. Chapman and hall/CRC. [CrossRef]

Dr. 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)