



Access Control in Cloud-Based Computing Environments Using a Novel Quantum Digital Signature Scheme

Manish Kumar Srivastava^a, Pradeep Kumar Singh^a, and Sanjay Kumar Singh^b

^aDepartment of Computer Science and Engineering, MMMUT, Gorakhpur, Uttar Pradesh, India

^bDepartment of Computer Science and Engineering, IIT(BHU), Varanasi, Uttar Pradesh, India

✉ mksghkp@gmail.com; topksingh@gmail.com; sks.cse@iitbhu.ac.in



KEYWORDS ABSTRACT

access control;
cloud-based computing environment;
quantum ice-cream;
quantum cryptography

Access control in cloud-based computing environments is in essence a security mechanism enabling decisions as to which subjects may access which protected resources and under what operations. The rapid emergence of quantum computing threatens the hardness assumptions underlying classical digital signatures and public-key infrastructures. The authors of this work recently proposed a novel quantum ice-cream model to demonstrate the basic concepts of quantum cryptography in a simple and intuitive manner. In this work we present a novel quantum ice-cream digital signature scheme by using our proposed quantum ice-cream model. Our quantum ice-cream digital signature scheme maps two non-commuting measurement bases to the ‘flavor’ and ‘shape’ attributes of the quantum ice-cream model. It achieves information-theoretic security against forgery and repudiation via threshold tests and natively supports signer–verifier–arbiter workflow that is suitable for cloud access control. Although our scheme is presented theoretically, a rigorous mathematical analysis has been carried out using Hoeffding-type inequalities. We also discuss the implementation of our proposed scheme by using weak-coherent BB84-like optics with decoy states. This article demonstrates that our proposed quantum ice-cream digital signature scheme preserves the practicality of memoryless quantum digital signature schemes while aligning with cloud authorization requirements. Furthermore, we draw analogies between the design of our proposed QIDS and robust control theory to provide an interdisciplinary perspective on system stability and security.

Manish Kumar Srivastava, Pradeep Kumar Singh and Sanjay Kumar Singh

Access Control in Cloud-Based Computing Environments Using a Novel Quantum Digital Signature Scheme



1. Introduction

Cloud-based computing environments are now everywhere and proliferating rapidly. With this proliferation of cloud services the issue of cloud security, particularly the problem of ensuring that only authenticated access occurs to sensitive resources has become a paramount concern. Access control is the first line of defense to regulate who (or what) can access which resources under specific conditions. Any access control system serves two main functions: (a) prevention of unauthorized access by malicious or illegitimate users, and (b) restraint of authorized users to only permitted actions on protected resources. The basic mechanism of access control is illustrated in Figure 1.

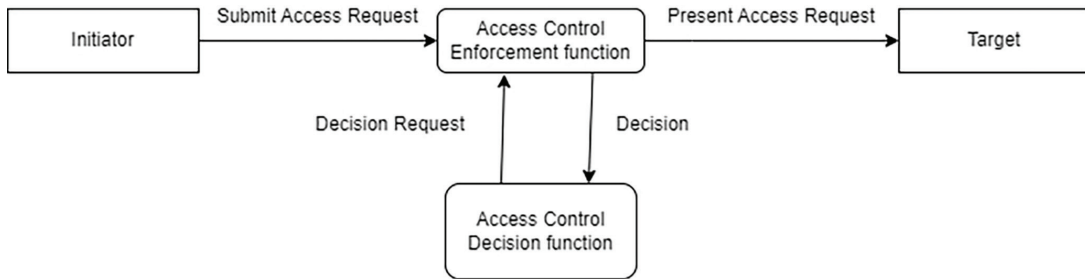


Figure 1. Basic architecture of an access control mechanism in a computing system

Access control has remained a fundamental component of computer security, with a wide range of models proposed over the past several decades (Cai et al., 2019). Early systems introduced discretionary access control (DAC) and mandatory access control (MAC) (Bell & La Padula, 1976). These were later complemented by role-based access control (RBAC), which assigns permissions based on user roles and supports the principle of least privilege in organizational settings (Osborn et al., 2000). With the emergence of cloud and distributed computing environments, cryptographic techniques have increasingly been integrated into access control mechanisms. In such approaches, data are encrypted and access is enforced through controlled distribution of cryptographic keys, as seen in attribute-based encryption, identity-based encryption, and related schemes (El Sibai et al., 2020).

However, the security of widely used cryptographic primitives underlying these mechanisms is based on computational hardness assumptions, such as integer factorization and discrete logarithms. These assumptions may be weakened in the presence of large-scale quantum computers, which can solve such problems efficiently using quantum algorithms such as Shor's algorithm. This raises concerns regarding the long-term security of classical cryptographic access control systems deployed in cloud environments.

To address this challenge, two main directions have been developed: post-quantum cryptography (PQC) and quantum cryptography. PQC focuses on classical algorithms that are believed to resist quantum attacks, while quantum cryptography exploits the principles of quantum mechanics to provide security guarantees that are not solely based on computational assumptions. Quantum key distribution (QKD) is a well-established example of the latter approach.

Recent studies have investigated the integration of quantum cryptographic techniques into access control systems. For example, Qiu et al. (2018) proposed a quantum-based access control model for

cloud computing that employs entanglement and quantum key distribution for authentication and certification. In this model, access is granted after verifying quantum-secured credentials. Although such approaches demonstrate the potential of quantum techniques, they often rely on entanglement and relatively complex quantum operations, which may limit their practical applicability. Furthermore, existing works primarily focus on authentication and key distribution, with comparatively less emphasis on digital signatures and non-repudiation within access control frameworks.

In this paper, we propose a quantum digital signature (QDS)-based approach for cloud access control. Specifically, we introduce the Quantum Ice-Cream Digital Signature (QIDS) protocol, which is designed as a prepare-and-measure scheme suitable for cloud-based environments. The proposed protocol avoids the use of quantum entanglement and complex quantum operations, thereby improving simplicity and potential feasibility of implementation.

The main contributions of this work are as follows. First, we present a consolidated view of classical access control models and cryptographic enforcement techniques, highlighting their limitations in the quantum computing context. Second, we formally describe the proposed QIDS protocol, including system assumptions, notation, and operational steps, and analyze its security in terms of correctness, unforgeability, and non-repudiation under specified conditions. Third, we discuss practical considerations and provide an interpretation of the protocol using control-theoretic concepts such as adaptive thresholding and layered verification.

The remainder of this paper is organized as follows. Section 2 reviews cloud access control models. Section 3 discusses related work, including quantum-based approaches. Section 4 presents the proposed QIDS protocol. Section 5 provides the correctness and security analysis. Section 6 offers a comparative evaluation with existing QDS schemes. Section 7 presents simulation results. Section 8 discusses implementation aspects. Section 9 provides a control-theoretic interpretation of the protocol. Section 10 presents a case study and practical considerations. Section 11 concludes the paper.

2. Cloud Access Control Models

Access control in computing systems ensures that only authorized entities can perform allowed operations on protected resources. Over time, numerous models for access control have been developed. We briefly summarize the major categories relevant to cloud computing.

2.1. Discretionary Access Control

In Discretionary Access Control (DAC), resource owners define access permissions for other users, typically through access control lists. While flexible, DAC may lead to unintended privilege propagation due to user-controlled delegation.

2.2. Mandatory Access Control

Mandatory Access Control (MAC) is a stricter model where access decisions are based on fixed policies determined by a central authority. Users and objects are assigned security labels (e. g., classification levels), and access is allowed only if a user's clearance dominates the object's classification (as in military «secret»/ «top-secret» hierarchies). MAC ensures high assurance isolation but is inflexible for general corporate environments.

2.3. Role-Based Access Control

Role-Based Access Control (RBAC) assigns permissions to roles rather than directly to users. Users acquire permissions through role membership, simplifying administration and supporting least privilege. RBAC is widely used in enterprise and cloud systems.

2.4. Attribute-Based Access Control

Attribute-Based Access Control (ABAC) evaluates access requests based on attributes of users, resources, and context. It enables fine-grained and dynamic policy enforcement, making it suitable for complex cloud environments.

2.5. Encryption-Based Access Control

In cloud settings, cryptographic techniques are used to enforce access control by encrypting data and distributing decryption keys only to authorized users. This approach is particularly relevant when data are stored on untrusted servers.

2.6. Identity-Based Encryption

In Identity-Based Encryption (IBE), a user's identity, or an attribute such as an e-mail address, serves as the public key. A trusted third party called a private key generator generates the corresponding private key for a user by using the master private key.

2.7. Attribute-Based Encryption

Attribute-Based Encryption (ABE) enables fine-grained access by associating policies with ciphertexts and attributes with user keys. Decryption is possible only if the user's attributes satisfy the embedded policy.

2.8. Capability-Based Access Using Encryption

Capability-based access using encryption involves using a cryptographic token, or «capability», that contains both an object's identity and a set of access rights, securing it with an encryption key. These tokens are unforgeable and are used to directly control access to resources, meaning a subject must possess the correct capability to access a resource, making the capability itself the authorization mechanism. Encryption ensures the integrity and authenticity of the capability and allows for fine-grained, secure sharing of access.

2.9. Time-Based or Location-Based Encryption

These approaches incorporate temporal or spatial constraints into encryption, allowing decryption only under specified conditions such as time windows or geographic locations.

These models are often combined in practice. For example, RBAC may be used for coarse-grained control, while encryption provides fine-grained protection. Surveys by Cai et al. (2019) and El Sibai et al. (2020) highlight the growing use of cryptographic approaches in cloud access control.

2.10. Certificate-Based Access Control Process in Cloud

In cloud systems, access control typically involves authentication followed by authorization. In certificate-based mechanisms, a trusted authority issues a digital certificate that encodes user permissions. The user presents this certificate to the cloud service, which verifies its authenticity and checks policy conditions such as validity and allowed operations. If the conditions are satisfied, access is granted, often by providing encrypted data that the user can decrypt using authorized keys. Figure 2 shows the certificate-based access control process pictorially.

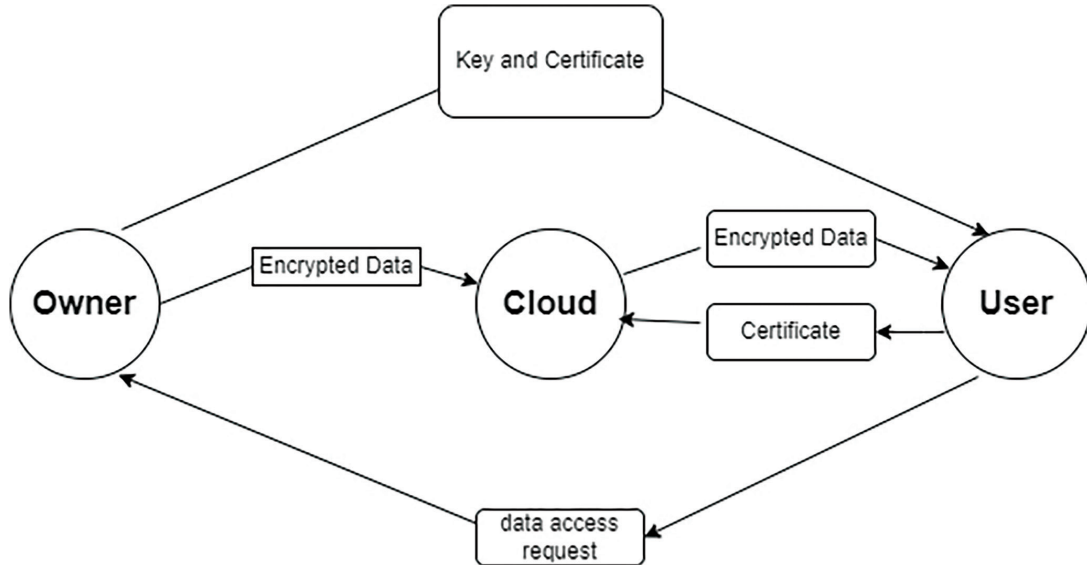


Figure 2. Certificate-based access control workflow in a cloud computing environment

3. Previous Related Work

Classical access control models such as discretionary access control (DAC), mandatory access control (MAC), and role-based access control (RBAC) were originally designed for centralized and enterprise environments (Osborn et al., 2000). While these models remain foundational, they face limitations in cloud settings characterized by dynamic roles, multi-tenant resource sharing, and stronger adversarial assumptions. To address these challenges, cryptographic enforcement mechanisms such as attribute-based, identity-based, and time-based encryption have been introduced (Cai et al., 2019; El Sibai et al., 2020). However, the security of these schemes depends on computational hardness assumptions, including integer factorization and discrete logarithms, which can be efficiently solved using Shor's algorithm on a sufficiently powerful quantum computer. Consequently, widely used classical signature schemes such as RSA and ECDSA may not provide long-term security in the quantum era.

Post-quantum cryptography (PQC) has emerged as a practical response, with lattice-, code-, and hash-based signature schemes such as Dilithium, Falcon, and SPHINCS+ offering resistance against known quantum attacks (Bos et al., 2015; NIST, 2024). These approaches are compatible with existing

infrastructures, including PKI and TLS. However, PQC schemes provide computational security rather than information-theoretic guarantees and may not fully address requirements such as transferability and arbitration in adversarial cloud environments.

Quantum cryptography offers an alternative by leveraging the principles of quantum mechanics. Quantum key distribution (QKD) enables information-theoretically secure key exchange (Bennett & Brassard, 1984), with practical implementations demonstrated using decoy states and satellite links (Lo et al., 2005; Liao et al., 2018). For authentication and integrity, quantum message authentication schemes have also been proposed (Barnum et al., 2002). However, QKD primarily addresses secrecy and does not directly provide digital signatures. This has motivated the development of quantum digital signatures (QDS), which aim to ensure unforgeability, non-repudiation, and transferability.

Early QDS protocols relied on entanglement and multiparty correlations, providing strong security guarantees but requiring complex resources (Dunjko et al., 2014). Subsequent prepare-and-measure approaches, based on BB84-type states and threshold verification, eliminated the need for quantum memory and improved practical feasibility (Wallden et al., 2015). Later extensions explored multi-user and cloud-based scenarios, demonstrating scalability while raising challenges related to device trust and noise resilience (Qiu et al., 2019; Li et al., 2021).

Recent advances have further improved the practicality and robustness of QDS systems. Measurement-device-independent QDS enhances security against detector side-channel attacks (Bian et al., 2024), while continuous-variable QDS reduces signature length and supports high-throughput applications (Zhang et al., 2024). Experimental demonstrations over deployed fiber networks and integrated photonic platforms indicate increasing feasibility of real-world deployment (Chapman et al., 2023; Zhu et al., 2025; Du et al., 2025). Despite this progress, many existing approaches involve complex architectures or focus primarily on physical-layer optimization rather than integration with higher-level access control workflows.

In this context, Srivastava et al. (2025) introduced the Quantum Ice-Cream model, which provides an intuitive abstraction for quantum communication protocols using a flavor–shape analogy. Building on this framework, the present work proposes the Quantum Ice-Cream Digital Signature (QIDS) protocol, a prepare-and-measure QDS scheme tailored for cloud access control. The proposed approach avoids entanglement and quantum memory, emphasizing simplicity, conceptual clarity, and compatibility with existing optical infrastructures. By integrating QDS into the access control process, the QIDS protocol aims to support secure and verifiable authorization in cloud environments under quantum-capable adversarial conditions.

4. Quantum Ice-Cream Digital Signature Protocol

4.1. Assumptions

Before proposing our scheme, we will discuss the underlying assumptions.

A1 (Distribution without storage): Alice prepares L quantum states (or, equivalently, L quantum ice-cream). She distributes them to Bob and Trent through a quantum channel, here termed a Quantum Ice-Cream Channel (QIC) to emphasize its analogy-driven nature. Both Bob and Trent must «consume» (measure) the ice-cream immediately—no freezing (quantum memory) is allowed.

A2 (Noise model): The imperfections of the channel, detectors, and devices are captured by the quantum bit error rate (QBER, Q), which in the QIC metaphor represents the melting rate of the ice-cream. For an honest Alice, the mismatch probability observed by each recipient is at most Q .

A3 (Adversary's guessing bound): Any dishonest party attempting to forge must guess the flavor or shape of a quantum ice-cream without knowing its preparation basis. Their minimum mismatch probability is bounded below by p^* . In ice-cream language: no forger can always guess the correct flavor or shape; at least some melt-induced wrong tastings are unavoidable.

A4 (Exchangeability): Since Alice distributes from the same batch of ice-cream, Bob and Trent's mismatch distributions are symmetric and exchangeable. Statistical fluctuations (such as random melting) are the only source of differences.

Separation condition: Verification threshold s_v and arbitration threshold s_a satisfy $Q < s_v < s_a < p^*$.

4.2. Protocol Description

Distribution Phase: Alice prepares a sequence of L quantum states using two non-commuting bases (flavor/shape). Each state is duplicated and sent to Bob and Trent via the quantum channel (QIC). Upon receipt, Bob and Trent immediately measure in randomly chosen bases (looking or tasting). They record only the classical outcomes.

Messaging Phase: To sign a message m , Alice publishes her preparation basis choices (cone/stick vs. mango/vanilla) for the corresponding sequence. Bob checks his recorded outcomes against Alice's declaration to compute his mismatch rate $\bar{X}$.

Verification Phase:

Bob **accepts** the message if $\bar{X} \leq s_v$.

If Bob forwards the signed message to Trent, Trent computes his mismatch rate and **accepts** if $\bar{Y} \leq s_a$.

Thresholds satisfy $Q < s_v < s_a < p^*$.

Figure 3 illustrates our protocol.

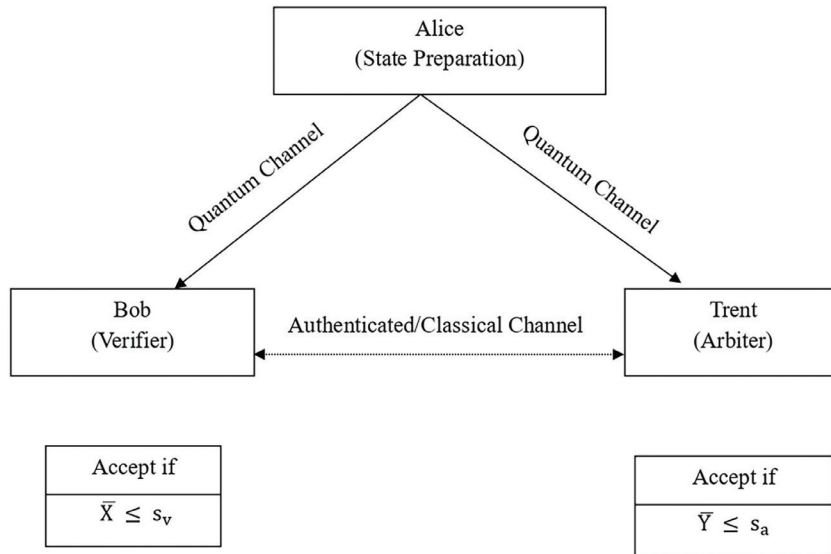


Figure 3. Operational workflow of the proposed Quantum Ice-Cream Digital Signature (QIDS) protocol

5. Correctness & Security Analysis

5.1. Model and Notation

Signature length (number of quantum states per message): $L \in \mathbb{N}$.

For each position $i \in \{1, \dots, L\}$, Alice prepares a state in one of two non-commuting bases (flavor/shape) and sends identical copies to Bob and to Trent.

Each recipient measures immediately on a randomly chosen basis and records a mismatch indicator: $X_i = \mathbf{1} \{\text{Bob's outcome} \neq \text{Alice's declaration at } i\}$, $Y_i = \mathbf{1} \{\text{Trent's outcome} \neq \text{Alice's declaration at } i\}$

Empirical mismatch rates:

$$\bar{X} = \frac{1}{L} \Re_{i=1}^L X_i, \bar{Y} = \frac{1}{L} \Re_{i=1}^L Y_i$$

Thresholds: verification s_v and arbitration s_a satisfy $0 < s_v < s_a < 1$.

Honest noise (QBER): when Alice is honest, each recipient's mismatch probability is at most Q (the «melt rate»).

Adversarial bound: any forger who does not know the correct basis has per-round mismatch probability at least p^* (equivalently, correct-guess probability at most $q^* = 1 - p^*$)

Exchangeability: the distributions of $\{X_i\}$ and $\{Y_i\}$ are i.i.d. with a common mean under the same preparation/noise conditions (Alice cannot skew Bob vs. Trent beyond statistical fluctuation).

Separation condition:

$$Q < s_v < s_a < p^*,$$

ensuring correctness and security margins for honest and dishonest cases.

Decision rules

Bob accepts if $\bar{X} \leq s_v$; Bob rejects if $\bar{X} \geq s_a$.

Trent accepts if $\bar{Y} \leq s_v$; Trent rejects if $\bar{Y} \geq s_a$.

(Intermediate regions can be mapped to «escalate to arbitration»; the analysis below targets the worst-case error events).

Concentration tool (Hoeffding)

If $Z_1, \dots, Z_L$ are i.i.d. Bernoulli with mean μ , then for any $t > 0$:

$$\Pr \left[\frac{1}{L} \Re_{i=1}^L Z_i - \mu \geq t \right] \leq \exp(-2Lt^2), \quad \Pr \left[\mu - \frac{1}{L} \Re_{i=1}^L Z_i \geq t \right] \leq \exp(-2Lt^2).$$

5.2. Correctness (Honest Acceptance)

Claim 1 (Correctness). If Alice is honest and the honest mismatch probability is at most Q , then

$$\Pr [\text{Bob rejects an honest signature}] = \Pr(\bar{X} > s_v) \leq \exp(-2L(s_v - Q)^2),$$

$$\Pr [\text{Trent rejects an honest signature}] = \Pr(\bar{Y} > s_a) \leq \exp(-2L(s_a - Q)^2).$$

Proof. Under honesty, $\mathbb{E}[X_i] \leq Q$ and $\mathbb{E}[Y_i] \leq Q$. Apply Hoeffding with $t = s_v - Q > 0$ and $t = s_a - Q > 0$, respectively.

Corollary 1 (Overall honest accept). By a union bound,

$$\Pr [\text{any honest reject}] \leq \exp(-2L(s_v - Q)^2) + \exp(-2L(s_a - Q)^2).$$

Thus, the honest signature is accepted by both with probability at least

$$1 - \exp(-2L(s_v - Q)^2) - \exp(-2L(s_a - Q)^2)$$

Unforgeability (Forgery)

Consider a dishonest recipient who attempts to produce a valid declaration for a message not signed by Alice. By assumption, each trial yields a mismatch with probability at least p^* . The adversary succeeds against Trent only if $\bar{Y} \leq s_a$.

Claim 2 (Unforgeability). For any forging strategy,

$$\Pr [\text{successful forgery}] = \Pr (\bar{Y} \leq s_a) \leq \exp(-2L(p^* - s_a)^2).$$

Proof. Under forging, $\mathbb{E}[Y_i] \geq p^*$. Set $t = p^* - s_a > 0$. By Hoeffding,

$$\Pr (\bar{Y} \leq s_a) = \Pr (p^* - \bar{Y} \geq t) \leq \exp(-2Lt^2).$$

5.3. Non-Repudiation (Repudiation)

Repudiation is the event that Alice makes Bob accept while Trent rejects (or vice versa). With exchangeability, Bob and Trent's mismatch indicators are i.i.d. Bernoulli with a common (unknown) mean μ (bounded by Q when Alice is honest). The worst case for splitting decisions is when μ lies between s_v and s_a .

We bound

$$\Pr(\bar{X} \leq s_v \text{ and } \bar{Y} \geq s_a) \leq \max_{\mu \in [0,1]} \Pr_{\mu}(\bar{X} \leq s_v) \cdot \Pr_{\mu}(\bar{Y} \geq s_a),$$

since $\bar{X}$ and $\bar{Y}$ are independent given μ .

For any fixed μ ,

$$\Pr_{\mu}(\bar{X} \leq s_v) \leq \exp(-2L(\mu - s_v)_+^2), \Pr_{\mu}(\bar{Y} \geq s_a) \leq \exp(-2L(s_a - \mu)_+^2).$$

The product is maximized at $\mu^* = \frac{s_v + s_a}{2}$, yielding symmetric tails:

$$(\mu^* - s_v) = (s_a - \mu^*) = \frac{s_a - s_v}{2}$$

Hence,

Claim 3 (non-repudiation)

$$\Pr(\bar{X} \leq s_v, \bar{Y} \geq s_a) \leq \exp\left(-2L\left(\frac{s_a - s_v}{2}\right)^2\right) \exp\left(-2L\left(\frac{s_a - s_v}{2}\right)^2\right) = \exp\left(-L(s_a - s_v)^2\right).$$

By symmetry the reverse split (Bob rejects, Trent accepts) has the same bound, so

$$\Pr[\text{repudiation}] \leq 2 \exp(-L(s_a - s_v)^2).$$

5.4. Robustness (Honest Abort)

Sometimes one reports the «honest abort» probability: the chance an honest signature is rejected at verification. From Claim 1:

$$\Pr[\text{honest abort at Bob}] \leq \exp(-2L(s_v - Q)^2).$$

This decays exponentially when the verification margin $s_v - Q$ is positive.

Finite-Size Accounting and Composable Error

Define three failure probabilities:

$$\begin{aligned}\varepsilon_{\text{cor}} &= \exp(-2L(s_v - Q)^2) + \exp(-2L(s_a - Q)^2), \\ \varepsilon_{\text{forg}} &= \exp(-2L(p^* - s_a)^2), \\ \varepsilon_{\text{rep}} &= 2 \exp(-L(s_a - s_v)^2).\end{aligned}$$

Under a standard (union-bound) composition,

$$\varepsilon_{\text{tot}} \leq \varepsilon_{\text{cor}} + \varepsilon_{\text{forg}} + \varepsilon_{\text{rep}}.$$

Given a target ε_{tot} (e.g., 10^{-12}), one can pick (L, s_v, s_a) satisfying the separation $Q < s_v < s_a < p^*$ and drive each term below $\varepsilon_{\text{tot}}/3$.

5.5. Parameter Synthesis (Worked Example)

Let

$$Q = 0.02, s_v = 0.05, s_a = 0.08, p^* = 0.12, L = 10,000.$$

Then

$$\begin{aligned}\varepsilon_{\text{cor}} &\leq e^{-2L(0.03)^2} + e^{-2L(0.06)^2} = e^{-18} + e^{-72} \approx 1.5 \times 10^{-8} + 5 \times 10^{-32}, \\ \varepsilon_{\text{forg}} &\leq e^{-2L(0.04)^2} = e^{-32} \approx 1.3 \times 10^{-14}, \\ \varepsilon_{\text{rep}} &\leq 2 e^{-L(0.03)^2} = 2 e^{-9} \approx 2.4 \times 10^{-4}.\end{aligned}$$

Repudiation dominates here; increasing $s_a - s_v$ or L fixes it. For instance, with $s_v = 0.045$, $s_a = 0.085$, $L = 20,000$:

$$\varepsilon_{\text{rep}} \leq 2 e^{-20,000(0.04)^2} = 2 e^{-32} \approx 2.6 \times 10^{-14} \text{ All three errors become } < 10^{-12} \text{ with modest retuning.}$$

6. Comparative Analysis

In this section, we compare our proposed quantum digital signature scheme with some recent schemes proposed in the literature. In the last few years, Quantum Digital Signature (QDS) protocols have diversified significantly, each pushing the limits of experimental security and scalability. MDI-QDS removes detector side-channels but requires complex relay setups, while CV-QDS provides resilience against coherent attacks with high throughput over short metro-scale distances. Entanglement-based QDS has achieved real-world multi-node demonstrations but remains resource intensive. Chip-integrated QDS has achieved a 200 km demonstration, highlighting miniaturization and scalability. Arbitrated QDS relaxed perfect channel assumptions but is at an early stage.

Our Quantum Ice-Cream Digital Signature (QIDS) protocol complements these advances by offering a prepare-and-measure discrete-variable scheme that is simple, threshold-based, and fully compatible with current DV-QKD technology. While other QDS families focus on hardware scaling, throughput, or entanglement distribution, QIDS contributes a unique pedagogical dimension. The Quantum Ice-Cream Channel analogy translates cryptographic thresholds and noise tolerance into intuitive concepts (flavors, shapes, melting), making QIDS both rigorous and accessible. This positions

Table 1. Comparison with Some Recent QDS Schemes

Protocol / Architecture	Security Model	Experimental Status	Distance / Scale	Signature Rate	Hardware Complexity	Remarks vs. QIDS
MDI-QDS (Bian et al., 2024)	Info-theoretic; MDI, detector side-channel free	Lab demo (asynchronous relay)	50–100 km	Moderate (multi-bit)	High (interference + synchronization)	Strong security, but complex; QIDS simpler and pedagogical
CV-QDS (Zhang et al., 2024)	Info-theoretic; coherent-attack resilience, finite-size	Proof-of-concept (Gaussian modulation)	<50 km metro	High throughput (Mb/s)	Moderate (homodyne/heterodyne)	Optimized for throughput; QIDS is Discrete Variable and easier
Entanglement-based QDS (Chapman et al., 2023)	Info-theoretic; entangled multiparty correlations	Campus fiber demos	~50 km	Low–Moderate	High (entangled photon sources)	Elegant, but resource-heavy; QIDS avoids entanglement
Arbitrated QDS (Zhu et al., 2025)	Relaxes perfect channel assumptions; arbiter-based	Early prototypes	Small scale	Variable	Low–Moderate	Similar to QIDS arbitration; QIDS adds ice-cream analogy
Chip-integrated QDS (Du et al., 2025)	Info-theoretic; decoy-state + hashing	Field demo over 200 km fiber	200 km	~0.04 sig/s for 1 Mb	Low–Moderate	Hardware efficient; QIDS can adapt to chips
Our QIDS (2025)	Info-theoretic; prepare-and-measure, threshold-based	Theoretical + simulations	50–200 km (with decoys)	Comparable to Wallden QDS	Low (Discrete Variable optics, threshold detectors)	Combines rigorous security with quantum ice-cream pedagogy

QIDS as a complementary contribution—simpler than entanglement or CV schemes, pedagogically powerful, and theoretically secure.

7. Simulation Results

To validate the theoretical bounds of the Quantum Ice-Cream Digital Signature (QIDS) protocol, we simulated the correctness, forgery, and repudiation error probabilities under varying system parameters. The results highlight the protocol’s exponential security scaling and its robustness against channel noise.

The parameters used are shown in Table 2 and the resulting graphs are shown in Figures 4, 5 and 6.

Table 2. Parameter Table

Parameter	Meaning	Value(s) used in plots
L	Signature length (number of quantum states / ice-cream)	1000 – 20,000 (step 1000)
Q	Quantum Bit Error Rate (QBER) = melting rate in QIC analogy	0.02 (baseline); 0.005 – 0.05 (sweep)
s_v	Verification threshold	0.05
s_a	Authentication / arbitration threshold	0.08
p^*	Minimum mismatch probability (forging bound)	0.12
$s_a - s_v$	Threshold separation parameter	0.01 – 0.10 (for repudiation sweep)

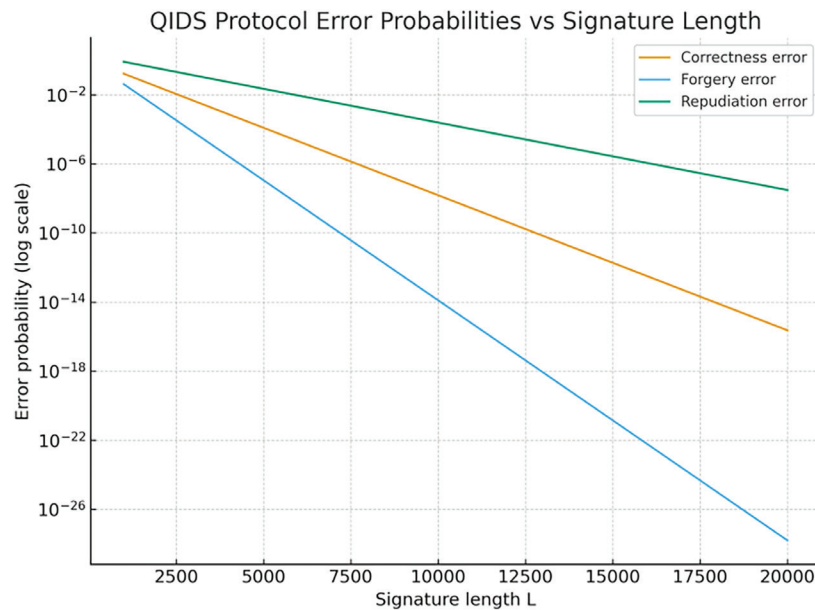


Figure 4. Error probabilities versus signature length in the QIDS protocol

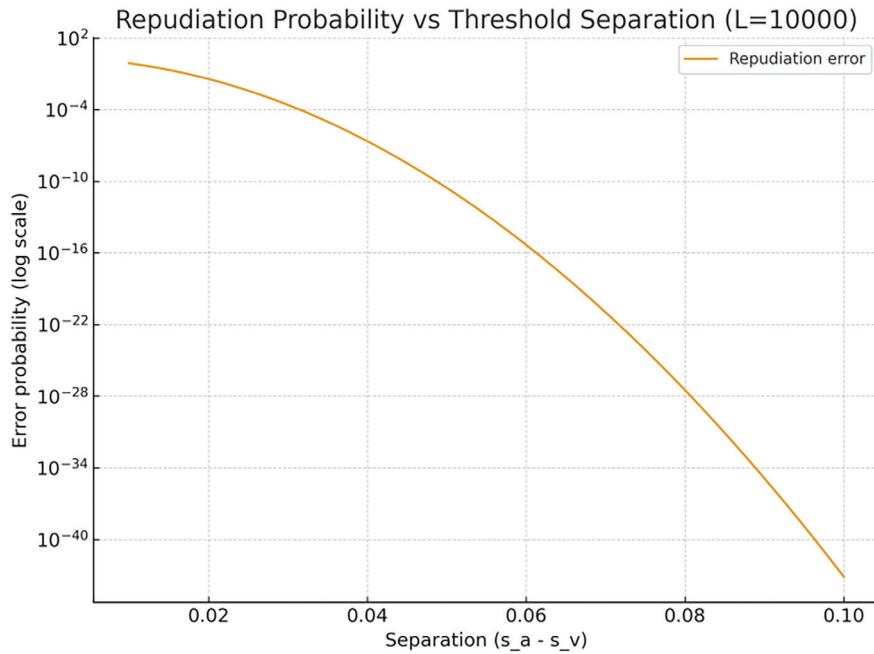


Figure 5. Repudiation error as a function of threshold separation

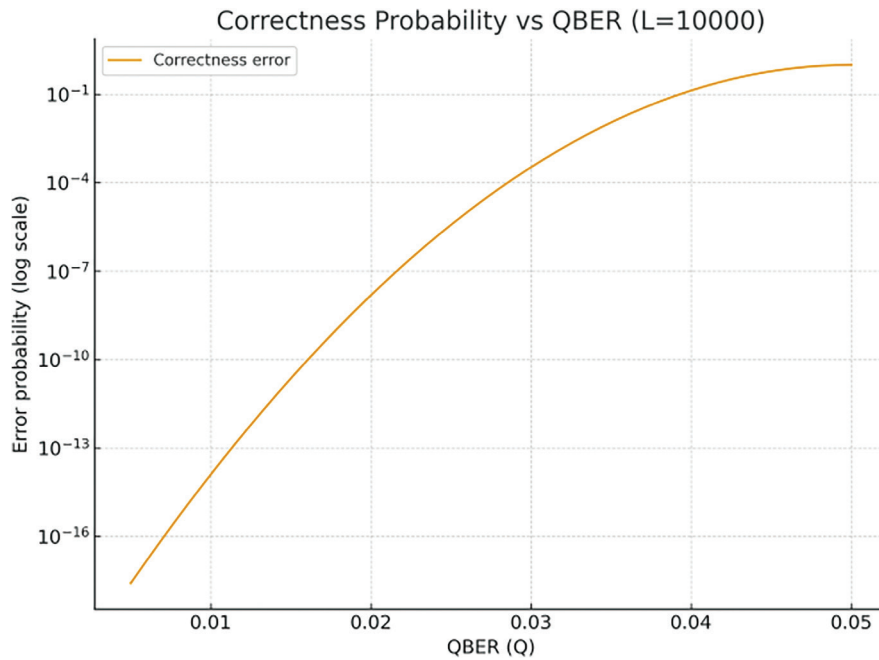


Figure 6. Correctness error as a function of quantum bit error rate (QBER)

8. Implementation Details

8.1. Physical Layer Requirements

The QIDS protocol is a prepare-and-measure scheme realizable using discrete-variable (DV) quantum optics platforms similar to BB84 QKD. The sender prepares weak coherent pulses (WCPs) in randomly chosen polarization or phase encodings, while recipients use threshold single-photon detectors (SPDs). The absence of entanglement and quantum memory significantly simplifies implementation.

Four non-orthogonal states are used, corresponding to two «flavors» (e.g., horizontal/vertical or phase $0/\pi$) and two «shapes» (diagonal/anti-diagonal or phase $\pi/2, 3\pi/2$). These are transmitted over optical fiber or free-space quantum channels subject to noise and attenuation. Recipients measure immediately in randomly chosen bases and store classical outcomes.

8.2. Classical post-processing

After transmission, Alice reveals preparation bases. Bob and Trent compute mismatch rates X and Y by comparison with recorded outcomes. Acceptance is determined via thresholds s_v and s_a , while Trent performs arbitration using a looser threshold to ensure non-repudiation.

8.3. Experimental Feasibility

QIDS aligns with existing QKD technology. Telecom fibers support distances up to ~200 km with decoy states, and free-space links extend this further. Threshold detectors with efficiency $\eta > 0.6$ and dark-count probability $p_{dark} \approx 10^{-6}$ are sufficient. Time-bin or polarization encoding may be used for synchronization. Simulations indicate that signature lengths $L \geq 10^4$ achieve correctness and repudiation error probabilities below 10^{-6} .

9. Control-Theoretic Interpretation of the QIDS Protocol

In this section, we provide a formal control-theoretic interpretation of the Quantum Ice-Cream Digital Signature (QIDS) protocol. Unlike heuristic or adaptive control designs, QIDS does not introduce learning-based or tunable controllers. Instead, its information-theoretic security guarantees naturally correspond to well-established notions in modern nonlinear and robust control, including finite-time stability, robustness margins, and output-feedback consensus. The purpose of this section is therefore interpretive rather than algorithmic: to show that QIDS already satisfies properties analogous to those sought in advanced control systems, without requiring adaptation or online optimization.

9.1. Formal System-Level Mapping

The QIDS protocol can be modeled as a **discrete-time stochastic decision system** operating under bounded uncertainty.

- **System state:** The empirical mismatch rate

$$\hat{p}_L = \frac{1}{L} \Re_{i=1}^L X_i$$

where $X_i \in \{0,1\}$ denotes a mismatch event.

- **Disturbances:**

Channel noise, detector imperfections, and adversarial guessing are modeled as bounded disturbances characterized by honest noise rate p_h and forging bound p^*

- **Decision regions:** Verification and arbitration thresholds (τ_v, τ_a) define invariant regions:

$$p_h < \tau_v < \tau_a < p^*$$

- **Control objective:** Ensure convergence of $\hat{p}_L$ into an acceptance region in finite time (signature length L) with exponentially small error probability.

This structure aligns with nonlinear systems analyzed in robust and finite-time control, where convergence is guaranteed under bounded disturbances without parameter adaptation.

9.2. Information-Theoretic Security as Finite-Time Stability

The Hoeffding-type bounds derived in Section 5 show that, for honest participants,

$$\Pr[\hat{p}_L \geq \tau_v] \leq e^{-2L(\tau_v - p_h)^2}.$$

This result admits a direct finite-time stability interpretation:

- The mismatch process converges to the acceptance region $\hat{p}_L < \tau_v$ after a finite number of steps L .
- The convergence probability approaches unity exponentially fast.
- The parameter L plays the role of finite convergence time, while the failure probability corresponds to residual instability probability.

This mirrors finite-time and fixed-time stability results in nonlinear control, where system states reach an invariant set within a bounded time regardless of initial conditions (e.g., fixed-time synchronization in fractional-order chaotic systems) (Boukroune et al., 2025).

Unlike classical control systems where convergence is established via Lyapunov functions, QIDS achieves finite-time stability through information concentration, yielding mathematically stronger guarantees under adversarial uncertainty.

9.3. Robustness Margins and Threshold Separation

The threshold separation condition

$$p_h < \tau_v < \tau_a < p^*$$

defines an explicit robustness margin, analogous to gain or phase margins in robust control.

- As long as the disturbance magnitude (QBER) remains within this margin, correctness and non-repudiation are preserved.
- Increasing the separation $\tau_a - \tau_v$ improves repudiation resistance, analogous to enlarging invariant sets in robust nonlinear systems.

This parallels robustness analysis in nonlinear optimal control and autonomous systems, where stability is maintained despite bounded modeling uncertainty (Yang & Zhou, 2019; Rigatos et al., 2020).

Importantly, these margins are designed offline and do not require adaptive tuning, which distinguishes QIDS from neural or adaptive controllers.

9.4. Arbitration as Output-Feedback Consensus

In QIDS, Bob and Trent make decisions solely from observed mismatch statistics, without access to the underlying quantum states. Arbitration therefore operates as an output-feedback consensus mechanism:

- Each verifier observes only output measurements.
- Agreement is enforced through asymmetric thresholds rather than shared internal states.
- Exchangeability ensures symmetric disturbance statistics.

This mirrors output-feedback synchronization in uncertain nonlinear systems, where consensus is achieved despite partial observability. However, unlike control systems that rely on observer design, QIDS guarantees consensus through statistical symmetry and threshold separation (Zhang et al., 2021).

9.5. Why Adaptive or Learning-Based Control Is Not Required

Recent control literature emphasizes adaptive fuzzy control, neural adaptive control, and backstepping methods to cope with uncertainty. While these frameworks are conceptually related, QIDS does not employ adaptation (Xu et al., 2025; Zirkohi et al., 2022; Zouari et al., 2013; Zouari & Chen, 2023).

Key distinctions:

- Adaptive fuzzy control adjusts parameters online; QIDS uses fixed thresholds.
- Neural adaptive controllers require training or excitation conditions; QIDS relies on concentration inequalities.
- Backstepping designs hierarchical stabilizers; QIDS achieves layered verification through static decision rules.

Introducing adaptive thresholds would require new security proofs and may undermine non-repudiation. Therefore, QIDS deliberately avoids adaptation, achieving finite-time robustness without learning, which is a stronger and more conservative guarantee.

10. Cloud Access-Control Case Study and Practical Constraints

To clarify the practical implications of the Quantum Ice-Cream Digital Signature (QIDS) protocol, we present a concrete cloud access-control scenario and analyze communication cost, latency, scalability, and robustness trade-offs relative to post-quantum and memoryless quantum signature schemes.

10.1. Case Study: Role-Based Access Control (RBAC) in a Multi-Tenant Cloud

Consider a cloud storage provider supporting multi-tenant enterprise environments. Access to sensitive resources is governed by Role-Based Access Control (RBAC), where:

- A data owner assigns roles (e.g., «Finance Manager», «Research Admin»).
- Users request access tokens asserting role membership.
- The cloud verifies authorization before granting data access.

In classical systems, digital certificates signed by a trusted authority are used to assert these roles. Under the QIDS framework, the workflow becomes:

- **Role Assertion:** The data owner (Alice) signs a role-assertion message using QIDS.
- **Verification:** The cloud service (Bob) verifies the signature using mismatch statistics and threshold testing.
- **Dispute Resolution:** If disagreement arises (e.g., a tenant disputes access denial), an arbiter (Trent) verifies using the arbitration threshold.

This structure preserves the logical architecture of certificate-based access control but replaces computational security with information-theoretic guarantees.

10.2. Communication and Latency Analysis

Signature Length and Verification Time

Let L denote the signature length (number of quantum states per message).

- Quantum transmission requires $O(L)$ time.
- Classical verification requires $O(L)$ comparisons.
- No iterative optimization or key search is required.

Thus, total verification complexity is linear in signature length.

Unlike adaptive control schemes, no online parameter tuning is performed, so latency remains deterministic once L is chosen.

10.3. Comparison with Post-Quantum Signatures

Property	PQC (e.g., Dilithium)	QIDS
Security Basis	Computational	Physical / Information-Theoretic
Verification Cost	Polynomial in key size	Linear in L
Long-Term Security	Depends on hardness	Independent of computation
Arbitration	Not inherent	Native via threshold separation

While PQC offers easier deployability in purely classical systems, QIDS provides stronger guarantees in quantum-secure infrastructures.

10.4. Behavior Under Realistic Noise

Channel imperfections introduce quantum bit error rate (QBER) p_h .

QIDS remains secure as long as:

$$p_h < \tau_v < \tau_a < p^{**}$$

Practical Operating Region

Typical decoy-state discrete-variable quantum systems report QBER values between 1 %–5 % over metropolitan fiber distances.

For example:

- $p_h = 0.02$
- $\tau_v = 0.05$
- $\tau_a = 0.08$

Under these conditions, correctness, forgery, and repudiation probabilities decay exponentially with L .

Thus, QIDS tolerates realistic noise levels without adaptive compensation.

10.5. Key Reuse and Signature Freshness

Unlike QKD-based symmetric systems, QIDS uses fresh quantum state sequences for each signature instance.

Practical constraints include:

- No reuse of quantum signature states.
- Each signed access assertion consumes a new batch of L states.
- Storage is purely classical after measurement.

This design avoids long-term quantum memory but imposes bandwidth requirements proportional to signature frequency.

In typical cloud workflows where access tokens are short-lived and infrequent relative to data transfer volume, this overhead is manageable.

10.6. Verifier Scalability

In large-scale cloud systems:

- Thousands of verification events may occur per second.
- Centralized arbitration may become a bottleneck.

QIDS supports scalable deployment via:

- Parallel verification (mismatch computation is embarrassingly parallel).
- Hierarchical arbitration (regional arbiters).
- Distributed threshold verification before escalation.

Unlike entanglement-based QDS, QIDS does not require multiparty entanglement distribution, simplifying scaling.

10.7. Comparison with Memoryless QDS

Memoryless QDS protocols (e.g., prepare-and-measure schemes similar to BB84-based signatures) share similar physical assumptions. But, QIDS differs in explicit threshold separation design for cloud arbitration, its structured mismatch interpretation aligned with access-control workflows, and its conceptual abstraction facilitating implementation integration.

Thus, QIDS maintains the practicality of memoryless QDS while emphasizing deployment in authorization systems.

10.8. Practical Constraints and Limitations

Despite its advantages, QIDS faces practical constraints, namely:

- Quantum communication infrastructure is required.
- Signature generation incurs bandwidth proportional to L .
- Large-scale adoption depends on quantum network availability.
- Real-time access decisions must account for quantum transmission delay.

These constraints suggest that QIDS is best suited for high-value authorization decisions, inter-datacenter secure authentication and long-term archival access policies requiring quantum resilience.

11. Conclusion

In this work, we introduced the Quantum Ice-Cream Digital Signature (QIDS) protocol, a prepare-and-measure quantum digital signature scheme tailored for cloud access-control environments. The protocol achieves information-theoretic guarantees of correctness, unforgeability, and non-repudiation without relying on computational hardness assumptions, quantum memory, or entanglement.

A central contribution of this work is the rigorous analysis of QIDS using concentration inequalities, demonstrating exponential decay of correctness, forgery, and repudiation probabilities as a function of signature length. These guarantees hold against adversaries with unbounded computational power and are independent of future advances in quantum computing. In contrast to post-quantum cryptographic schemes, which provide computational resilience, QIDS provides security grounded in physical principles.

Beyond its cryptographic properties, we provided a formal control-theoretic interpretation of the protocol. We showed that the signature verification process admits a finite-time stability interpretation, where the signature length plays the role of a convergence horizon, threshold separation defines explicit robustness margins against bounded channel noise and adversarial disturbances, and the arbitration mechanism functions as an output-feedback consensus process, ensuring decision agreement under symmetric uncertainty.

Importantly, unlike adaptive fuzzy, neural, or backstepping control schemes, QIDS does not rely on online learning or parameter tuning. Its guarantees are established through fixed thresholds and information-theoretic bounds, resulting in a conservative and robust design that does not require model estimation or adaptation.

From an applied perspective, QIDS integrates naturally into cloud role-based or attribute-based access-control workflows. Verification latency scales linearly with signature length and is independent of policy complexity. Arbitration supports dispute resolution in multi-tenant environments. The protocol remains secure under realistic quantum bit error rates and can be implemented using discrete-variable quantum optical components similar to BB84-type systems with decoy states.

The broader implication of this work is methodological: quantum cryptographic protocols can be interpreted through the lens of modern nonlinear control without introducing heuristic adaptation. By mapping information-theoretic security to concepts such as finite-time stability and robustness margins, we provide a reusable interdisciplinary framework that bridges cryptography and control theory while preserving mathematical rigor.

Future work may extend this framework in three directions: finite-size composable security analysis under realistic channel fluctuation models, experimental implementation over metropolitan-scale fiber networks using integrated photonic platforms, and the extension of the Quantum Ice-Cream abstraction to additional primitives such as quantum authentication and oblivious transfer.

To summarize, QIDS demonstrates that pedagogical clarity and rigorous security are not mutually exclusive. It provides a theoretically sound, practically implementable, and conceptually transparent quantum digital signature framework suitable for the emerging quantum-secure cloud ecosystem.

Acknowledgment

All the authors thank their affiliating institutions for providing a cordial and supportive work environment to facilitate this work.

Author Contributions

Manish Kumar Srivastava: Conceptualization, Methodology, Writing original draft.

Pradeep Kumar Singh: Supervision, Review and editing of original draft.

Sanjay Kumar Singh: Supervision, Review and editing of original draft.

Funding

This research received no external funding.

Conflict of Interest

All authors declare no conflict of interest.

Ethics Approval

Not applicable.

Consent to Participate

Not applicable.

Data Availability

No datasets were generated or analyzed in this study.

References

- Barnum, H., Crépeau, C., Gottesman, D., Smith, A., & Tapp, A. (2002). Authentication of quantum messages. In *Proceedings of the 43rd IEEE Symposium on Foundations of Computer Science* (pp. 449–458). IEEE. <https://doi.org/10.1109/SFCS.2002.1181957>
- Bell, D. E., & La Padula, L. J. (1976). *Secure computer system: Unified exposition and multics interpretation* (Technical Report). <https://apps.dtic.mil/sti/citations/ADA023588>
- Bennett, C. H., & Brassard, G. (1984). Quantum cryptography: Public key distribution and coin tossing. In *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing* (pp. 175–179).
- Bian, J. W., Li, B. H., Xie, Y. M., Yin, H. L., & Chen, Z. B. (2024). Asynchronous measurement-device-independent quantum digital signatures. *Physical Review A*, 110(1), 012609. <https://doi.org/10.1103/PhysRevA.110.012609>
- Bos, J., Costello, C., Naehrig, M., & Stebila, D. (2015). Post-quantum key exchange for the TLS protocol from the ring learning with errors problem. In *Proceedings of the IEEE Symposium on Security and Privacy* (pp. 553–570). <https://doi.org/10.1109/SP.2015.28>
- Boulkroune, A., Boubellouta, A., Bouzeriba, A., Zouari, F. (2025). Practical finite-time fuzzy synchronization of chaotic systems with non-integer orders: Two chattering-free approaches. *Journal of Systems Science and Systems Engineering*, 34, 334–359. <https://doi.org/10.1007/s11518-024-5635-7>
- Cai, F., Zhu, N., He, J., Mu, P., Li, W., & Yu, Y. (2019). Survey of access control models and technologies for cloud computing. *Cluster Computing*, 22, 6111–6122. <https://doi.org/10.1007/s10586-018-1850-7>
- Chapman, J. C., Joshi, S. K., Brougham, T., Wadsworth, W. J., Rarity, J. G., & Wallden, P. (2023). Entanglement-based quantum digital signatures over a deployed campus network. <https://arxiv.org/abs/2310.19457>
- Du, Y., Li, B. H., Hua, X., Cao, X. Y., Zhao, Z., Xie, F., Zhang, Z., Yin, H. -L., Xiao, X., & Wei, K. (2025). Chip-integrated quantum signature network over 200 km. *Light: Science & Applications*, 14(1), 108. <https://doi.org/10.1038/s41377-025-01775-4>
- Dunjko, V., Wallden, P., & Andersson, E. (2014). Quantum digital signatures without quantum memory. *Physical Review Letters*, 112(4), 040502. <https://doi.org/10.1103/PhysRevLett.112.040502>
- El Sibai, R., Gemayel, N., Bou Abdo, J., & Demerjian, J. (2020). A survey on access control mechanisms for cloud computing. *Transactions on Emerging Telecommunications Technologies*, 31(2). <https://doi.org/10.1002/ett.3720>

- Li, L., Qiu, D., Mateus, P., & Paunković, N. (2021). Quantum digital signatures in a multi-user network. *Quantum Information Processing*, 20, 200. <https://doi.org/10.1007/s11128-021-03117-5>
- Liao, S. K., Cai, W. Q., Handsteiner, J., Liu, B., Yin, J., Zhang, L., Rauch, D., Fink, M., Ren, J. -G., Liu, W. -Y., Li, Y., Shen, Q., Cao, Y., Li, F. -Z., Wang, J. -F., Huang, Y. -M., Deng, L., Xi, T., Ma, L., ... Pan, J. -W. (2018). Satellite-relayed intercontinental quantum network. *Physical Review Letters*, 120, 030501. <https://doi.org/10.1103/PhysRevLett.120.030501>
- Lo, H. K., Ma, X., & Chen, K. (2005). Decoy state quantum key distribution. *Physical Review Letters*, 94, 230504. <https://doi.org/10.1103/PhysRevLett.94.230504>
- National Institute of Standards and Technology. (2024). *Post-quantum cryptography standardization: Final standards and selected algorithms*. <https://csrc.nist.gov/projects/post-quantum-cryptography>
- Osborn, S., Sandhu, R., & Munawer, Q. (2000). Configuring role-based access control to enforce mandatory and discretionary access control policies. *ACM Transactions on Information and System Security*, 3(2), 85–106. <https://doi.org/10.1145/354876.354878>
- Qiu, D., Li, L., Mateus, P., & Paunković, N. (2019). Quantum digital signatures for classical messages against collective attacks. *Quantum Information Processing*, 18, 255. <https://doi.org/10.1007/s11128-019-2340-8>
- Qiu, L., Sun, X., & Xu, J. (2018). Categorical quantum cryptography for access control in cloud computing. *Soft Computing*, 22(19), 6363–6370. <https://doi.org/10.1007/s00500-017-3087-4>
- Rigatos, G., Siano, P., Zouari, F., Ademi, S. (2020). Nonlinear optimal control of autonomous submarines' diving. *Marine Systems & Ocean Technology*, 15, 57–69. <https://doi.org/10.1007/s40868-019-00070-3>
- Srivastava, M. K., Singh, P. K., & Singh, S. K. (2025). Design of a novel quantum computing primitive to demonstrate quantum cryptography. *Journal of Optics*. <https://doi.org/10.1007/s12596-025-02878-2>
- Wallden, P., Dunjko, V., Kent, A., & Andersson, E. (2015). Quantum digital signatures with quantum-key-distribution components. *Physical Review A*, 91(4), 042304. <https://doi.org/10.1103/PhysRevA.91.042304>
- Xu, Y., Wang, Z., & Liu, Y. (2025). Adaptive fuzzy control for practical fixed-time synchronization of fractional-order chaotic systems. *Journal of Vibration and Control*, 31(2), 210–225. <https://doi.org/10.1177/10775463251320258>
- Yang, X., & Zhou, Y. (2019). Nonlinear optimal control for a gas compressor driven by an induction motor. *International Journal of Control, Automation and Systems*, 17(6), 1350–1360. <https://doi.org/10.1007/s12555-018-0365-2>
- Zhang, H., Li, Y., & Chen, G. (2021). Output-feedback controller-based projective lag synchronization of uncertain chaotic systems in the presence of input nonlinearities. *International Journal of Bifurcation and Chaos*. <https://doi.org/10.1142/S0218127421500897>
- Zhang, S., Zhou, F., Sun, Y., & Zhang, Z. (2024). Continuous-variable quantum digital signatures that can withstand coherent attacks. *Physical Review A*, 110(5), 052613. <https://doi.org/10.1103/PhysRevA.110.052613>
- Zhu, J., Guo, Y., & Wang, X. (2025). A simplified arbitrated quantum signature protocol without perfect quantum channels. *Optics Communications*, 554, 130691. <https://doi.org/10.1016/j.optcom.2025.130691>

- Zirkohi, M. M., Khalilvand, M., & Baleanu, D. (2022). Fractional adaptive backstepping control for a class of uncertain nonlinear systems. *Nonlinear Analysis: Modelling and Control*, 27(1), 1–19. <https://doi.org/10.15388/name.2022.27.25339>
- Zouari, F., & Chen, C. (2023). Robust neural adaptive control for a class of uncertain nonlinear complex dynamical multivariable systems. *Complexity*. <https://doi.org/10.1155/2023/8487326>
- Zouari, F., Saad, K. B., & Benrejeb, M. (2013). Adaptive backstepping control for a single-link flexible robot manipulator driven DC motor. In Proceedings of the International Conference on Control, Decision and Information Technologies (CoDIT) (pp. 864–871). IEEE. <https://doi.org/10.1109/CoDIT.2013.6689686>