PQ-SMS: A Post-Quantum Sanitizable Multi-Signature Scheme for Satellite PKI

Long Wang[1,2,3,4], Zhaoman Liu[5,6,7], Jing Fan[2], and Yanhong Fan[1,3,4*]

[1] School of Cyber Scicnce and Technology, Shandong University, Qingdao 266000, China
[2] North China Research Institute of Computer System Engineering, Beijing 100083, China
[3] State Key Laboratory of Cryptography and Digital Economy Security,Shandong University,Qingdao 266000, China
[4] Key Laboratory of Cryptologic Technology and Information Security,Ministry of Education, Shandong University, Jinan 250131, China
[5] Shanghai Key Laboratory of Computer Software Testing and Evaluating, Shanghai 201112, China
[6] Shanghai Development Center of Computer Software Technology, Shanghai 201112, China
[7] College of Computer Science and Artificial Intelligence, Fudan University, Shanghai 200438, China
peakwl@mail.sdu.edu.cn, zmliu0503@gmail.com*, fanjing@ncse.com.cn, yanhongfan@sdu.edu.cn*

Abstract. Satellite communication systems, as critical long-lifecycle infrastructure, face a dual security challenge in the coming decades: the threat of quantum computers and the operational rigidity of traditional Public Key Infrastructure (PKI). While migrating to Post-Quantum Cryptography (PQC) addresses the former, it fails to solve the inefficiency of certificate management, where in-orbit policy updates require a prohibitively slow and complex multi-party re-issuance process.

To address these challenges, we introduce the concept of a Post-Quantum Sanitizable Multi-Signature (`PQ-SMS`), a novel primitive that enables controlled certificate adaptation across hierarchical trust while preserving the integrity of the root of trust. Building on this, we present `Sat-APCS` (**Sat**ellite **A**daptable **P**ost-quantum **C**ertificate **S**cheme), which cryptographically decouple a certificate's immutable, multi-signed identity from its dynamic operational policies. This allows a delegated entity to perform lightweight, in-orbit policy updates while the foundational signature from the original consortium of authorities remains unchanged and valid.

We instantiate `PQ-SMS` based on the NIST-standard CRYSTALS-Dilithium signature and a ISIS-based chameleon hash, and prove its security under standard lattice assumptions. Furthermore, Performance evaluation demonstrates that `PQ-SMS` bypasses the interactive re-signing loop of traditional PKI, achieving an order-of-magnitude reduction in update bandwidth.

Keywords: Post-Quantum Cryptography · Satellite Security · PKI · Multi-Signature · Chameleon Hash.

1 Introduction

Satellite communication networks are critical long-lifecycle assets with operational spans exceeding 15 years, demanding highly forward-looking security architectures[28]. As large-scale quantum computers threaten to render classical public-key cryptography obsolete within these operational windows, migrating satellite Public Key Infrastructure (PKI) to Post-Quantum Cryptography (PQC) has become a matter of necessity[16]. However, simply replacing algebraic primitives addresses only one facet of a deeper problem: the inherent rigidity of traditional certificate management.

A digital certificate is fundamentally a static assertion. Any in-orbit policy adaptation—such as updating mission parameters or operational authorizations—traditionally requires a full *revoke-and-reissue* cycle. In satellite ecosystems, this process is prohibitively inefficient. First, the high-latency, low-bandwidth nature of space links makes transmitting heavyweight post-quantum certificates a slow, bandwidth-heavy affair. Second, certificate issuance typically requires multi-party endorsement from an international consortium of stakeholders (e.g., manufacturers, operators, regulators). Re-convening this alliance for frequent operational updates creates severe bureaucratic and tactical bottlenecks.

Furthermore, real-world satellite network governance is inherently hierarchical rather than flat. A root authority frequently needs to delegate bounded management rights to regional ground segments, which in turn authorize edge orbital nodes to execute tactical, on-the-fly modifications. Traditional post-quantum certificates completely fail to capture this multi-tier authorization progression. Forcing a resource-constrained satellite to maintain a dynamic, cumulative audit log to track these delegated changes would rapidly deplete its premium on-board storage.

Thus, modern satellite PKI demands a comprehensive paradigm shift: it requires not only *quantum-resistance* and *collaborative endorsement*, but also *hierarchical, log-free operational agility* to enable non-interactive certificate adaptability.

To resolve this tension, we present **Sat-APCS** (**Sat**ellite **A**daptable **P**ost-quantum **C**ertificate **S**cheme), powered by a new primitive: Post-Quantum Sanitizable Multi-Signature (`PQ-SMS`). `Sat-APCS` cryptographically isolates a certificate's immutable identity from its fluid operational policies. To naturally match the multi-tiered governance of space infrastructure, we embed a dual-layer ($L = 2$) cascading short-basis trapdoor mechanism into lattice structures. Under this framework, the top-level authority consortium (`SORA`) issues a foundational certificate backed by an explicit multi-signature collection. `SORA` can then delegate bounded policy-redaction rights to a primary ground sanitizer (`DMA`), who can further delegate localized modification sub-privileges to a secondary star-side sanitizer. This hierarchical design allows designated entities to execute lightweight, in-orbit policy updates locally. The resulting "purified" certificate remains valid under the original multi-signature, ensuring non-interactive signer accountability while completely eliminating dynamic, storage-draining external audit logs.

Our Contribution

This paper makes the following principal contributions:

- **A New Hierarchical Primitive:** We introduce and formalize `PQ-SMS` supporting explicit dual-layer ($L = 2$) cascading redaction privileges. We present a concrete, zero-log instantiation using NIST-standard CRYSTALS-Dilithium and an SIS-based chameleon hash, proving its security under standard lattice assumptions.
- **A Novel Satellite PKI Framework:** We propose `Sat-APCS`, a comprehensive framework tailored to the multi-tier constraints of satellite communications, enabling non-interactive certificate evolution across space-ground segments while preserving immutable root trust and post-redaction accountability.
- **Theoretical and Scalability Evaluation:** Complexity analysis confirms that `Sat-APCS` completely bypasses the interactive re-signing loop of traditional PKIs. It achieves an order-of-magnitude reduction in update bandwidth while keeping the satellite-side computational overhead strictly invariant to the scale of the governance consortium.

Paper Organization

The remainder of this paper is organized as follows. Section 2 reviews the cryptographic background. Section 3 details our system and threat models. Section 4 presents the `PQ-SMS` construction and its integration into the `Sat-APCS` framework. Section 5 provides a rigorous security analysis of our scheme. Section 6 evaluates its performance. Section 7 reviews the related work in detail. Finally, Section 8 concludes the paper.

2 Preliminaries

In this section, we provide the necessary cryptographic background for our work. We begin by establishing our notation, then we briefly review the foundational concepts of lattice-based cryptography, including the hard problems upon which the security of our scheme relies. Finally, we provide formal definitions for the two core cryptographic primitives used in our construction: the CRYSTALS-Dilithium digital signature scheme and the trapdoor chameleon hash function.

2.1 Notation

We denote the security parameter by λ. For a finite set S, $x \xleftarrow{\$} S$ denotes that x is sampled uniformly at random from S. We denote vectors with bold lowercase letters (e.g., $\mathbf{v}$) and matrices with bold uppercase letters (e.g., $\mathbf{A}$). For a prime modulus q, $\mathbb{Z}_q$ represents the ring of integers modulo q. The concatenation of two strings s_1 and s_2 is denoted by $s_1 \parallel s_2$. We use QPT to denote "Quantum Polynomial-Time". The statistical distance between two distributions D_1 and D_2 is denoted by $\Delta(D_1, D_2)$. A function $\nu(\lambda)$ is negligible if for every positive polynomial $p(\cdot)$, there exists an integer N such that for all $\lambda > N$, $\nu(\lambda) < 1/p(\lambda)$.

2.2 Lattice and Hard Problems

Our scheme's post-quantum security is founded on the conjectured hardness of specific problems over integer lattices. An m-dimensional integer lattice $\mathcal{L}$ is a discrete subgroup of $\mathbb{R}^m$, which can be represented as the set of all integer linear combinations of a set of linearly independent basis vectors $\mathbf{B} = \{\mathbf{b}_1, \ldots, \mathbf{b}_k\} \subset \mathbb{R}^m$. The security of our instantiation relies on the following standard lattice problems, which are widely believed to be intractable even for QPT adversaries.

Definition 1 (Short Integer Solution (SIS)). *Let n, m, q be integers and β be a real number. The $\mathrm{SIS}_{n,m,q,\beta}$ problem is defined as follows: Given a uniformly random matrix $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$, find a non-zero integer vector $\mathbf{z} \in \mathbb{Z}^m$ such that $\mathbf{Az} = \mathbf{0} \pmod q$ and $\|\mathbf{z}\| \leq \beta$.*

The SIS problem is the foundation for the security of our chameleon hash construction. The average-case hardness of SIS is computationally equivalent to the worst-case hardness of certain standard lattice problems like the Shortest Independent Vectors Problem (SIVP).

Definition 2 (Module Learning With Errors (M-LWE)). *Let n, k, q be integers, let $R_q = \mathbb{Z}_q[X]/(X^d + 1)$ be a polynomial ring, and let χ be a narrow error distribution over R_q. The $\mathrm{M-LWE}_{n,k,q,\chi}$ problem is to distinguish between two distributions:*

1. *A series of pairs $(\mathbf{a}_i, u_i) \in R_q^k \times R_q$, where $\mathbf{a}_i \xleftarrow{\$} R_q^k$ and $u_i \xleftarrow{\$} R_q$ are chosen uniformly at random.*
2. *A series of pairs $(\mathbf{a}_i, u_i) \in R_q^k \times R_q$, where $\mathbf{a}_i$ is uniform in R_q^k, $\mathbf{s} \in R_q^k$ is a fixed secret vector, $\mathbf{e}_i \xleftarrow{\$} \chi$, and $u_i = \mathbf{a}_i \cdot \mathbf{s} + \mathbf{e}_i$.*

The M-LWE problem and its decisional variant are the primary source of hardness for many structured lattice-based cryptosystems, including our chosen digital signature scheme.

2.3 CRYSTALS-Dilithium Digital Signature

CRYSTALS-Dilithium is a digital signature scheme selected by the NIST PQC standardization process for its strong security and performance. Formally, a digital signature scheme DS is a tuple of three PPT algorithms $\mathtt{DS} = (\mathtt{KeyGen}, \mathtt{Sign}, \mathtt{Verify})$:

- $\mathtt{KeyGen}(1^\lambda) \to (\mathtt{sk}, \mathtt{pk})$: A probabilistic algorithm that takes the security parameter λ and outputs a secret signing key $\mathtt{sk}$ and a public verification key $\mathtt{pk}$.
- $\mathtt{Sign}(\mathtt{sk}, M) \to \sigma$: A (possibly probabilistic) algorithm that takes a secret key $\mathtt{sk}$ and a message M, and outputs a signature σ.
- $\mathtt{Verify}(\mathtt{pk}, M, \sigma) \to \{0, 1\}$: A deterministic algorithm that takes a public key $\mathtt{pk}$, a message M, and a signature σ, and outputs 1 if the signature is valid, and 0 otherwise.

A digital signature scheme must satisfy the correctness property, meaning that for any key pair $(\mathtt{sk}, \mathtt{pk})$ generated by $\mathtt{KeyGen}$, $\mathtt{Verify}(\mathtt{pk}, M, \mathtt{Sign}(\mathtt{sk}, M)) = 1$ holds for any message M. The security of Dilithium is based on the hardness of the M-LWE and M-SIS problems in module lattices.

2.4 Chameleon Hash

A Chameleon Hash (CH) is a special type of collision-resistant hash function with a "trapdoor" that enables finding collisions efficiently for an entity possessing it. A CH scheme is a tuple of four PPT algorithms $\mathtt{CH} = (\mathtt{KeyGen}, \mathtt{Hash}, \mathtt{Verify}, \mathtt{FindCollision})$:

- $\mathtt{KeyGen}(1^\lambda) \to (\mathtt{sk}, \mathtt{pk})$: A probabilistic algorithm that outputs a secret key $\mathtt{sk}$ (the trapdoor) and a public key $\mathtt{pk}$.
- $\mathtt{Hash}(\mathtt{pk}, M) \to (h, r)$: A probabilistic algorithm that takes a public key $\mathtt{pk}$ and a message M. It internally samples a randomness r and computes a hash value h. It outputs the pair (h, r).
- $\mathtt{Verify}(\mathtt{pk}, M, r, h) \to \{0, 1\}$: A deterministic algorithm that outputs 1 if and only if h is a valid hash of message M using randomness r under public key $\mathtt{pk}$.
- $\mathtt{FindCollision}(\mathtt{sk}, (M, r), M') \to r'$: A deterministic algorithm that takes the secret key $\mathtt{sk}$, an original tuple (M, r) and a new message M'. It outputs a new randomness r' such that $\mathtt{Verify}(\mathtt{pk}, M, r, h) = \mathtt{Verify}(\mathtt{pk}, M', r', h)$, where h is the hash corresponding to (M, r).

A CH scheme must satisfy two core security properties:

1) **Collision Resistance:** For any QPT adversary $\mathcal{A}$ not in possession of the trapdoor $\mathtt{sk}$, the probability of finding two pairs (M, r) and (M', r') such that $M \neq M'$ and $\mathtt{Hash}(\mathtt{pk}, M, r) = \mathtt{Hash}(\mathtt{pk}, M', r')$ is negligible.
2) **Trapdoor Property:** For any valid message pair (M, M'), anyone in possession of the trapdoor $\mathtt{sk}$ can efficiently compute r' from a given (M, r) such that a collision is formed.

With these cryptographic primitives as our foundation, we are now prepared to present our main construction.

3 System Model

This section specifies the overall system model, including the tiered architecture and operational entities involved, the post-quantum threat landscape, and the rigorous security goals to be achieved.

3.1 System Architecture and Entities

Our proposed system is specifically engineered for a hierarchical space-ground integrated network (SGIN) ecosystem, managing the lifecycle of post-quantum multi-signature certificates that assert both the identity and the segmented operational authorizations of satellite assets. As illustrated in Figure 1, the architecture strictly coordinates three operational parties across four critical entities:

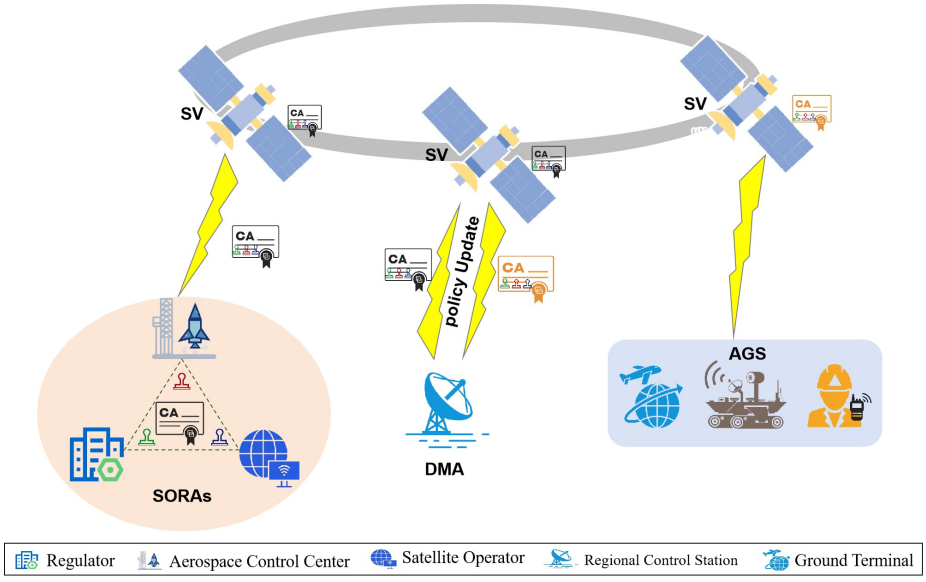


Fig. 1: The Tiered Space-Ground System Architecture

– **Satellite Operations & Regulatory Alliance (SORA):** SORA represents the highest-level authority and distributed root of trust, consisting of stakeholders such as satellite manufacturers and national space regulatory bodies. Acting as the *Ground Signer Consortium* $\mathcal{C}$, SORA jointly executes multi-signatures to issue foundational certificates containing immutable identity blocks (M_{ctx}) before a satellite's launch.
– **Two-Tier Sanitizer Hierarchy ($\mathsf{San}_1, \mathsf{San}_2$):** Instead of distributing monotonic authorities, our system establishes a hierarchical containment structure to govern dynamic policy updates:
  • *Root Ground Controller (San_1):* The high-tier ground sanitizer holding the master algebraic trapdoor. It possesses unrestricted modification privileges to update ground operational policies and delegates bounded capacities to the orbit.

  - *Orbital Master Satellite (San_2):* The low-tier in-orbit sanitizer deployed on a primary space node. Operating with a bounded sub-trapdoor delegated by San_1, it independently performs lightweight, low-latency updates strictly confined to tactical in-orbit policy domains without contacting the ground.
- **Satellite Vehicle (SV):** The SV is the resource-constrained certificate subject operating in orbit. It securely stores its context-bound certificate and presents it during link initialization to prove its runtime identity and current multi-tier mission authorization.
- **Authorized Ground Segment (AGS):** The AGS encompasses regional ground telecommand stations and gateway user terminals. Acting as the *Verifier* ($\mathcal{V}$), it validates the structural correctness and algebraic authenticity of the SV's presented certificate before establishing secure high-rate data communication links.

3.2 Threat Model

In alignment with the operational characteristics of Space-Ground Integrated Networks, we consider a resilient, Quantum Polynomial-Time (QPT) adversary $\mathcal{A}$ whose capabilities are formalized under an extended Dolev-Yao behavioral model. The adversary has complete control over the public, long-latency space-ground wireless communication channels, enabling them to passively eavesdrop on, or actively intercept, modify, replay, and inject arbitrary data frames.

To systematically evaluate the security boundaries, we categorize the adversarial presence into two operational deployment classes:

- **Outsider Attacks (Active/Passive Network Adversaries):** $\mathcal{A}$ can compromise open verification gateways or intercept downlinks between the Satellite Vehicle (SV) and the Authorized Ground Segment (AGS). Operating externally, the adversary attempts to perform passive wiretapping to trace satellite mission trajectories, or execute active spoofing attacks by injecting forged certificates to impersonate legitimate space assets.
- **Insider Attacks (Hierarchical Privilege Escalation):** We consider a highly potent insider threat model wherein specific architectural authorities may be dynamically compromised by $\mathcal{A}$:
  - *Low-Tier Sanitizer Compromise:* The adversary $\mathcal{A}$ may physically capture or cyber-compromise the Orbital Master Satellite (San_2), thereby acquiring its localized policy update credentials. A rogue San_2 will aggressively attempt to overstep its tactical bounds to rewrite ground-level operational policies or forge unauthorized identity frameworks.
  - *High-Tier Sanitizer Compromise:* The adversary $\mathcal{A}$ may breach the Root Ground Controller (San_1). A compromised San_1 may attempt to maliciously manipulate modified dynamic parameters to frame either the offline SORA consortium or the honest orbital nodes.

Trust Assumptions. We assume that the multi-party SORA consortium remains the global root of trust, and its distributed cryptographic fragments are securely

maintained in air-gapped, offline environments such that $\mathcal{A}$ cannot breach the threshold necessary to forge a fresh baseline multi-signature. Additionally, the onboard cryptographic hardware computing environment of the SV is assumed to be tamper-resistant.

3.3 Security Goals

To guarantee reliable trust management across high-latency space links, the proposed PQ-SMS framework must satisfy four formal cryptographic security properties, directly mapping onto our defense against the defined threat model:

- **Existential Unforgeability:** The framework must prevent unauthorized credential generation under adaptively chosen-message attacks. Specifically, no external outsider adversary $\mathcal{A}$ should be capable of forging a valid certificate $\texttt{Cert}$ for a fresh, unqueried space asset identity or context message M_{ctx}, ensuring the baseline authenticity of the space-ground data links.
- **Layer Isolation and Controllability:** The framework must enforce strict privilege boundaries against insider threats. A compromised low-tier sanitizer (San_2) possessing only the delegated sub-trapdoor must be mathematically incapable of modifying or generating a valid certificate that alters components within the protected high-tier policy domain managed by San_1.
- **Sanitization Indistinguishability:** To guarantee token privacy against passive traffic analysis, the framework must ensure that any authorized credential update executed by a sanitizer (San_1 or San_2) yields a certificate whose cryptographic components are statistically or computationally indistinguishable from a pristine certificate directly generated by the signers. The public certificate structure must leak zero mathematical metadata regarding historical redaction or policy update behaviors.
- **Auditable Anchoring and Non-repudiation:** The system must enforce public accountability and provenance tracking without allowing framing attacks. The public $\texttt{Verify}$ algorithm must deterministically output whether a valid certificate remains in its original state or has undergone authorized sanitization. Crucially, this auditability must incur zero storage overhead, eliminating the need for satellites or ground segments to maintain historical policy status registries.

4 The Proposed PQ-SMS Scheme

In this section, we present the formal construction of our Two-Tier ($\texttt{PQ-SMS}$) scheme. We first provide the abstract syntax, general definitions, and correctness requirements of the primitive. Then, we deliver a concrete, optimized lattice-based instantiation designed for space-ground integrated networks.

4.1 Formal Syntax and Framework

A PQ-SMS scheme is defined over a partitioned message space consisting of an immutable global context domain $\mathcal{M}_{\text{ctx}}$, a high-tier ground operational policy domain $\mathcal{M}_{\text{pol1}}$, and a low-tier in-orbit tactical policy domain $\mathcal{M}_{\text{pol2}}$. Formally, the primitive is defined as a tuple of six polynomial-time algorithms:

- $\texttt{Setup}(1^\lambda) \to \texttt{pp}$: On input the security parameter λ, this algorithm outputs the global public parameters $\texttt{pp}$.
- $\texttt{SignerKeyGen}(\texttt{pp}) \to (\texttt{sk}_{s_i}, \texttt{pk}_{s_i})$: Executed independently by each signer $i \in \{1, \ldots, n\}$ within the consortium $\mathcal{C}$ to generate an individual public verification anchor $\texttt{pk}_{s_i}$ and a private signing key $\texttt{sk}_{s_i}$.
- $\texttt{RootKeyGen}(\texttt{pp}) \to (\texttt{sk}_{p,1}, \texttt{pk}_{p,1})$: Executed by the high-tier root sanitizer San_1 to generate the master public validation matrix $\texttt{pk}_{p,1}$ and its corresponding global sanitization trapdoor $\texttt{sk}_{p,1}$.
- $\texttt{Delegate}(\texttt{pp}, \texttt{sk}_{p,1}) \to \texttt{sk}_{p,2}$: Executed by the root sanitizer San_1 to derive a bounded, lower-tier sub-trapdoor $\texttt{sk}_{p,2}$ for the orbital sanitizer San_2. This constrains the modification capability of San_2 strictly to the target sub-domain $\mathcal{M}_{\text{pol2}}$.
- $\texttt{Sign}(M_{\text{ctx}}, M_{\text{pol1}}, M_{\text{pol2}}, \{\texttt{sk}_{s_i}\}_{i=1}^n, \texttt{pk}_{p,1}) \to \texttt{Cert}$: On input a partitioned message tuple $(M_{\text{ctx}}, M_{\text{pol1}}, M_{\text{pol2}})$, the private keys of the consortium, and the master sanitizer public key, this algorithm initializes a structural randomness tracking pair $(\mathbf{r}_1, \mathbf{r}_2)$ and outputs a context-bound multi-signature certificate $\texttt{Cert}$.
- $\texttt{Verify}(\texttt{Cert}, \{\texttt{pk}_{s_i}\}_{i=1}^n, \texttt{pk}_{p,1}) \to \{0, 1_{\text{pristine}}, 1_{\text{sanitized}}\}$: On input a certificate $\texttt{Cert}$, the verification anchors of the consortium, and the master sanitizer public key, this algorithm performs intertwined algebraic and norm checks. It outputs 0 upon failure, and either 1_{pristine} or $1_{\text{sanitized}}$ to indicate the certificate origin provenance.
- $\texttt{Sanitize}(\texttt{Cert}, \ell, M^\star_{\text{pol},\ell}, \texttt{sk}_{p,\ell}) \to \texttt{Cert}^\star$: Executed by a tier-$\ell$ sanitizer ($\ell \in \{1, 2\}$). On input a valid certificate $\texttt{Cert}$, a target updated policy $M^\star_{\text{pol},\ell}$, and the respective tier trapdoor $\texttt{sk}_{p,\ell}$, this algorithm computes an adjusted randomness matrix and outputs a modified certificate $\texttt{Cert}^\star$.

Correctness. Let $\texttt{pp} \leftarrow \texttt{Setup}(1^\lambda)$, $\mathcal{SK}_s \coloneqq \{\texttt{sk}_{s_i}\}_{i=1}^n$ and $\mathcal{PK}_s \coloneqq \{\texttt{pk}_{s_i}\}_{i=1}^n$ be the signer key sets from $\texttt{SignerKeyGen}(\texttt{pp})$. Let $(\texttt{sk}_{p,1}, \texttt{pk}_{p,1}) \leftarrow \texttt{RootKeyGen}(\texttt{pp})$, $\texttt{sk}_{p,2} \leftarrow \texttt{Delegate}(\texttt{pp}, \texttt{sk}_{p,1})$, and define the composite message as $\boldsymbol{M} \coloneqq (M_{\text{ctx}}, M_{\text{pol1}}, M_{\text{pol2}}) \in \mathcal{M}_{\text{ctx}} \times \mathcal{M}_{\text{pol1}} \times \mathcal{M}_{\text{pol2}}$. A PQ-SMS scheme satisfies standard correctness if the following three conditions hold simultaneously:

1) If $\texttt{Cert} \leftarrow \texttt{Sign}(\boldsymbol{M}, \mathcal{SK}_s, \texttt{pk}_{p,1})$, then $\texttt{Verify}(\texttt{Cert}, \mathcal{PK}_s, \texttt{pk}_{p,1}) = 1$.
2) For any $M^\star_{\text{pol1}} \in \mathcal{M}_{\text{pol1}}$, if $\texttt{Cert}^\star \leftarrow \texttt{Sanitize}(\texttt{Cert}, 1, M^\star_{\text{pol1}}, \texttt{sk}_{p,1})$, then $\texttt{Verify}(\texttt{Cert}^\star, \mathcal{PK}_s, \texttt{pk}_{p,1}) = 1$.
3) For any $M^\star_{\text{pol2}} \in \mathcal{M}_{\text{pol2}}$, if $\texttt{Cert}^\star \leftarrow \texttt{Sanitize}(\texttt{Cert}, 2, M^\star_{\text{pol2}}, \texttt{sk}_{p,2})$, then $\texttt{Verify}(\texttt{Cert}^\star, \mathcal{PK}_s, \texttt{pk}_{p,1}) = 1$.

4.2 Concrete Lattice-Based Instantiation

We now detail the concrete lattice-based instantiation of the PQ-SMS framework fixed at $L = 2$ to show how our architectural properties are realized algebraically. This construction seamlessly integrates a short-basis trapdoor Chameleon Hash with a batchable variant of the CRYSTALS-Dilithium signature structure. Crucially, rather than relying on heavy zero-knowledge proofs or additional signature chains, the scheme introduces a simple yet elegant coordinate-wise zero-padding constraint onto the initial randomness subspace. This design leverages the inherent geometric randomness of lattice trapdoor sampling to guarantee untamperable, zero-storage origin auditing at zero overhead.

Algorithm 1 Concrete Instantiation of PQ-SMS Scheme ($L = 2$)

$\texttt{Setup}(1^\lambda) \to \texttt{pp}$

1: Set $\mathsf{par} \leftarrow (n', m', k, l, q, q', \eta, \gamma_1, \gamma_2, \beta, \sigma, H, \mathcal{H}, \mathcal{H}_0)$ ▷ System params & hashes
2: Generate $\texttt{pp}_{\mathsf{sig}} \leftarrow \texttt{Dilithium.Setup}(1^\lambda)$ and $\texttt{pp}_{\mathsf{ch}} \leftarrow \texttt{CH.Setup}(1^\lambda)$
3: **return** $\texttt{pp} \leftarrow (\mathsf{par}, \texttt{pp}_{\mathsf{sig}}, \texttt{pp}_{\mathsf{ch}})$

$\texttt{SignerKeyGen}(\texttt{pp}) \to (\texttt{sk}_s, \texttt{pk}_s)$

1: Expand matrix $\mathbf{A} \leftarrow \mathsf{ExpandMatrix}(\rho) \in R_q^{k \times l}$ from a random public seed ρ
2: Sample secret vectors $\mathbf{s}_{1,i} \leftarrow \mathcal{S}_\eta^l$ and $\mathbf{s}_{2,i} \leftarrow \mathcal{S}_\eta^k$
3: Compute public key component $\mathbf{t}_i \leftarrow \mathbf{A}\mathbf{s}_{1,i} + \mathbf{s}_{2,i} \bmod q$
4: **return** $\texttt{pk}_{s_i} = (\rho, \mathbf{t}_i)$ and $\texttt{sk}_{s_i} = (\rho, \mathbf{s}_{1,i}, \mathbf{s}_{2,i})$

$\texttt{RootKeyGen}(\texttt{pp}) \to (\texttt{sk}_{p,1}, \texttt{pk}_{p,1})$

1: Generate trapdoor pairs $(\mathbf{A}_b, T_{\mathbf{A}_b}) \leftarrow \texttt{GenTrap}(1^\lambda)$ for $b \in \{0, 1\}$, where $\mathbf{A}_0, \mathbf{A}_1 \in \mathbb{Z}_{q'}^{n' \times m'}$
2: Set $\texttt{pk}_{p,1} = (\mathbf{A}_0, \mathbf{A}_1)$ and $\texttt{sk}_{p,1} = (T_{\mathbf{A}_0}, T_{\mathbf{A}_1})$
3: **return** $(\texttt{sk}_{p,1}, \texttt{pk}_{p,1})$

$\texttt{Delegate}(\texttt{sk}_{p,1}) \to \texttt{sk}_{p,2}$

1: Parse $\texttt{sk}_{p,1} = (T_{\mathbf{A}_0}, T_{\mathbf{A}_1})$
2: **return** $\texttt{sk}_{p,2} \leftarrow T_{\mathbf{A}_1}$

$\texttt{Sign}(M_{\text{ctx}}, M_{\text{pol1}}, M_{\text{pol2}}, \{\texttt{sk}_{s_i}\}_{i=1}^n, \texttt{pk}_{p,1}) \to \texttt{Cert}$

1: Compute integrity anchors: $t_1 \leftarrow H_{\mathsf{anchor}}(M_{\text{pol1}})$ and $t_2 \leftarrow H_{\mathsf{anchor}}(M_{\text{pol2}})$
2: Sample Gaussian randomizers $\mathbf{r}_1, \mathbf{r}_2 \leftarrow \mathcal{D}_{\mathbb{Z}^{m'}, \sigma}$
3: Compute chameleon hashes: $h_1 \leftarrow \mathbf{A}_0\mathbf{r}_1 + H_1(M_{\text{ctx}} \parallel M_{\text{pol1}}) \bmod q'$ and $h_2 \leftarrow \mathbf{A}_1\mathbf{r}_2 + H_2(M_{\text{ctx}} \parallel M_{\text{pol2}}) \bmod q'$
4: Bind hashes to global digest: $h \leftarrow H(h_1 \parallel h_2)$
5: **for** each signer $i \in \{1, \ldots, n\}$ **do**
6: Sample masking vector $\mathbf{y}_i \leftarrow \mathcal{S}_{\gamma_1 - 1}^l$
7: Compute commitment vector $\mathbf{w}_i \leftarrow \mathbf{A}\mathbf{y}_i \bmod q$
8: Compute challenge $c_i \leftarrow \mathcal{H}(\mathbf{w}_i \parallel \texttt{pk}_{s_i} \parallel h \parallel t_1 \parallel t_2)$
9: Compute response vector $\mathbf{z}_i \leftarrow \mathbf{y}_i + c_i\mathbf{s}_{1,i}$
10: **if** $\|\mathbf{z}_i\|_\infty \geq \gamma_1 - \beta$ **or** $\|\mathbf{A}\mathbf{z}_i - c_i\mathbf{t}_i \bmod q\|_\infty \geq \gamma_2$ **then** restart
11: Set $\sigma_i \leftarrow (\mathbf{z}_i, c_i)$
12: Aggregate multi-signature $\sigma_{\text{multi}} = (\sigma_1, \ldots, \sigma_n)$
13: Output certificate $\texttt{Cert} = (M_{\text{ctx}}, M_{\text{pol1}}, M_{\text{pol2}}, \mathbf{r}_1, \mathbf{r}_2, t_1, t_2, \sigma_{\text{multi}})$

$\texttt{Verify}(\texttt{Cert}, \{\texttt{pk}_{s_i}\}_{i=1}^n, \texttt{pk}_{p,1}) \to \{0, 1_{\text{pristine}}, 1_{\text{sanitized}}\}$

1: Parse $\texttt{Cert} = (M_{\text{ctx}}, M_{\text{pol1}}, M_{\text{pol2}}, \mathbf{r}_1, \mathbf{r}_2, t_1, t_2, \sigma_{\text{multi}})$
2: Recompute $h_1' \leftarrow \mathbf{A}_0\mathbf{r}_1 + H_1(M_{\text{ctx}} \parallel M_{\text{pol1}}) \bmod q'$ and $h_2' \leftarrow \mathbf{A}_1\mathbf{r}_2 + H_2(M_{\text{ctx}} \parallel M_{\text{pol2}}) \bmod q'$
3: Recompute $h' \leftarrow H(h_1' \parallel h_2')$
4: **for** each $\sigma_i = (\mathbf{z}_i, c_i)$ **do**
5: check $\|\mathbf{z}_i\|_\infty < \gamma_1 - \beta$
6: Reconstruct $\mathbf{w}_i' \leftarrow \mathbf{A}\mathbf{z}_i - c_i\mathbf{t}_i \bmod q$
7: Recompute $c_i' \leftarrow \mathcal{H}(\mathbf{w}_i' \parallel \texttt{pk}_{s_i} \parallel h' \parallel t_1 \parallel t_2)$
8: **if** $c_i' \neq c_i$ **then return** 0
9: **if** $H_{\mathsf{anchor}}(M_{\text{pol1}}) == t_1$ and $H_{\mathsf{anchor}}(M_{\text{pol2}}) == t_2$ **then return** 1_{pristine}
10: **else return** $1_{\text{sanitized}}$

$\texttt{Sanitize}(\texttt{Cert}, \ell, M_{\text{pol},\ell}^\star, \texttt{sk}_{p,\ell}) \to \texttt{Cert}^\star$

1: Parse $\texttt{Cert} = (M_{\text{ctx}}, M_{\text{pol1}}, M_{\text{pol2}}, \mathbf{r}_1, \mathbf{r}_2, t_1, t_2, \sigma_{\text{multi}})$
2: Recompute $h_1 \leftarrow \mathbf{A}_0\mathbf{r}_1 + H_1(M_{\text{ctx}} \parallel M_{\text{pol1}}) \bmod q'$ and $h_2 \leftarrow \mathbf{A}_1\mathbf{r}_2 + H_2(M_{\text{ctx}} \parallel M_{\text{pol2}}) \bmod q'$
3: **if** $\ell = 1$ **then**
4: Compute $\mathbf{y} \leftarrow h_1 - H_1(M_{\text{ctx}} \parallel M_{\text{pol1}}^\star) \bmod q'$
5: Sample $\mathbf{r}_1^\star \leftarrow \texttt{SamplePre}(T_{\mathbf{A}_0}, \mathbf{y})$
6: Output $\texttt{Cert}^\star = (M_{\text{ctx}}, M_{\text{pol1}}^\star, M_{\text{pol2}}, \mathbf{r}_1^\star, \mathbf{r}_2, t_1, t_2, \sigma_{\text{multi}})$
7: **else if** $\ell = 2$ **then**
8: Compute $\mathbf{y} \leftarrow h_2 - H_2(M_{\text{ctx}} \parallel M_{\text{pol2}}^\star) \bmod q'$
9: Sample $\mathbf{r}_2^\star \leftarrow \texttt{SamplePre}(T_{\mathbf{A}_1}, \mathbf{y})$
10: Output $\texttt{Cert}^\star = (M_{\text{ctx}}, M_{\text{pol1}}, M_{\text{pol2}}^\star, \mathbf{r}_1, \mathbf{r}_2^\star, t_1, t_2, \sigma_{\text{multi}})$

4.3 Application in Satellite Certificate Distribution

To demonstrate the practical applicability of the proposed PQ-SMS primitive, we instantiate it as a Sat-APCS for secure certificate distribution and dynamic authorization management in hierarchical space-ground integrated networks.

Sat-APCS directly maps the abstract entities of PQ-SMS to the operational components introduced in Section 3.1. Specifically, the SORA consortium serves as the signer set $\mathcal{C}$ and jointly establishes the root of trust through the execution of `SignerKeyGen`. The Root Ground Controller San_1 acts as the root sanitizer and executes `RootKeyGen` to generate the master sanitization trapdoor. Subsequently, `Delegate` is performed to derive a bounded sanitization capability for the Orbital Master Satellite San_2, thereby enforcing hierarchical modification privileges. The AGS functions as the verifier $\mathcal{V}$, while the SV acts as the certificate holder.

A satellite certificate in Sat-APCS is represented as $\texttt{Cert} = (M_{\text{ctx}}, M_{\text{pol1}}, M_{\text{pol2}}, \mathbf{r}_1, \mathbf{r}_2, t_1, t_2, \sigma_{\text{multi}})$, where M_{ctx} contains immutable identity and platform attributes, M_{pol1} encodes ground-controlled operational policies, and M_{pol2} specifies latency-sensitive in-orbit authorization parameters. The corresponding integrity anchors (t_1, t_2) bind the original policy states and enable lightweight provenance verification.

The certificate lifecycle consists of three operational phases.

Certificate Issuance. Before launch, SORA jointly executes the `Sign` algorithm of PQ-SMS to generate a certificate for the target satellite. The issued certificate is securely embedded into the SV and subsequently distributed throughout the network.

Hierarchical Policy Adaptation. During operation, authorization policies may evolve due to mission adjustments, regulatory requirements, or dynamic network conditions. Ground-level policy updates affecting M_{pol1} are performed by $\mathsf{San} * 1$ through $\texttt{Sanitize}(\cdot, 1, \cdot)$, while tactical in-orbit updates affecting $M*\text{pol2}$ are independently executed by San_2 through $\texttt{Sanitize}(\cdot, 2, \cdot)$. Since both sanitization procedures preserve the underlying chameleon-hash commitments, the original multi-signature remains valid and no interaction with SORA is required after certificate issuance.

Certificate Verification. Whenever an SV initiates communication with an AGS, the verifier executes the `Verify` algorithm to validate the certificate. Successful verification confirms the authenticity of the original SORA-issued certificate, the integrity of all non-editable information, and the legitimacy of any authorized policy adaptations performed by the sanitizer hierarchy.

By inheriting the security guarantees of PQ-SMS, Sat-APCS provides post-quantum secure certificate issuance, verification, and hierarchical authorization adaptation. The system enables low-latency in-orbit policy evolution while preserving root-trust continuity and eliminating the need for certificate re-issuance after routine authorization updates.

5 Security Analysis

In this section, we present a formal and rigorous security evaluation of the proposed PQ-SMS scheme. We first establish the scheme's correctness, followed by comprehensive reductions to hardness of standard lattice problems (MLWE, MSIS, and ISIS) over the algebraic ring $R_q = \mathbb{Z}_q[X]/\langle X^d + 1\rangle$ to validate our security goals.

5.1 Correctness

The correctness of the PQ-SMS scheme requires that a certificate honestly generated via `Sign` or legally modified via `Sanitize` can successfully pass the `Verify` algorithm.

Theorem 1. *If all entities honestly execute the protocol specified in Algorithm 1, the `Verify` algorithm will output* $1_{pristine}$ *for original certificates and* $1_{sanitized}$ *for sanitized certificates with overwhelming probability.*

Proof. We analyze the verification equations step-by-step:

1. **Multi-Signature Verification Correctness:** In Step 6 of `Verify`, the verification oracle reconstructs the commitment $\mathbf{w}'_i$. For an honest signature component $\sigma_i = (\mathbf{z}_i, c_i)$, where $\mathbf{z}_i = \mathbf{y}_i + c_i\mathbf{s}_{1,i} \bmod q$ and $\mathbf{t}_i = \mathbf{A}\mathbf{s}_{1,i} + \mathbf{s}_{2,i} \bmod q$, we have:

$$\begin{aligned}\mathbf{w}'_i &\equiv \mathbf{A}\mathbf{z}_i - c_i\mathbf{t}_i \\ &\equiv \mathbf{A}(\mathbf{y}_i + c_i\mathbf{s}_{1,i}) - c_i(\mathbf{A}\mathbf{s}_{1,i} + \mathbf{s}_{2,i}) \\ &\equiv \mathbf{A}\mathbf{y}_i + c_i\mathbf{A}\mathbf{s}_{1,i} - c_i\mathbf{A}\mathbf{s}_{1,i} - c_i\mathbf{s}_{2,i} \\ &\equiv \mathbf{A}\mathbf{y}_i - c_i\mathbf{s}_{2,i} \pmod q. \end{aligned} \tag{1}$$

   According to the Dilithium-like design parameters, when the coefficients of $c_i\mathbf{s}_{2,i}$ are bounded within γ_2, the high bits of $\mathbf{A}\mathbf{z}_i - c_i\mathbf{t}_i \bmod q$ perfectly match the original commitment $\mathbf{w}_i \equiv \mathbf{A}\mathbf{y}_i \bmod q$. Thus, $c'_i = \mathcal{H}(\mathbf{w}'_i \parallel \dots) = c_i$ holds.
2. **Chameleon Hash and Sanitization Correctness:** For a pristine certificate, h'_b is computed directly using original $\mathbf{r}_b$ and $M_{\text{pol}b}$. For a sanitized certificate (w.l.o.g., assume layer $\ell = 1$), the sanitizer samples $\mathbf{r}^\star_1 \leftarrow \texttt{SamplePre}(T_{\mathbf{A}_0}, \mathbf{y})$ such that $\mathbf{A}_0\mathbf{r}^\star_1 \equiv \mathbf{y} \pmod{q'}$, where $\mathbf{y} = h_1 - H_1(M_{\text{ctx}} \parallel M^\star_{\text{pol1}}) \bmod q'$. The recomputed hash h'_1 satisfies:

$$\begin{aligned}h'_1 &\equiv \mathbf{A}_0\mathbf{r}^\star_1 + H_1(M_{\text{ctx}} \parallel M^\star_{\text{pol1}}) \\ &\equiv \big(h_1 - H_1(M_{\text{ctx}} \parallel M^\star_{\text{pol1}})\big) + H_1(M_{\text{ctx}} \parallel M^\star_{\text{pol1}}) \\ &\equiv h_1 \pmod{q'}. \end{aligned} \tag{2}$$

   Therefore, $h' = H(h'_1 \parallel h'_2) = H(h_1 \parallel h_2) = h$, which preserves the global digest used in multi-signature validation.

3. **Audit State Branching:** If no sanitization occurred, $M_{\text{pol}\ell}$ matches the original data, meaning $H_{\mathsf{anchor}}(M_{\text{pol}\ell}) == t_\ell$ for $\ell \in \{1, 2\}$, resulting in 1_{pristine}. If `Sanitize` was executed, the policy changes to $M^{\star}_{\text{pol1}}$, but t_1 remains invariant inside σ_{multi}. Hence, $H_{\mathsf{anchor}}(M^{\star}_{\text{pol1}}) \neq t_1$, and `Verify` correctly returns $1_{\text{sanitized}}$.

This concludes the proof of correctness.

5.2 Existential Unforgeability

This section proves that our scheme satisfies the EUF-CMA security target, preventing any outsider adversary $\mathcal{A}$ from forging certificates.

Theorem 2. *Assuming the $\mathsf{MLWE}_{n,m,q,\eta}$ and $\mathsf{MSIS}_{n,m,q,\beta}$ assumptions hold in the ring R_q, and the cryptographic hash functions $\mathcal{H}, H, H_1, H_2$, and H_{anchor} are modeled as random oracles, the proposed PQ-SMS scheme is EUF-CMA secure against any PPT outsider adversary $\mathcal{A}$.*

Proof (Proof Sketch). We define a sequence of game hops between a challenger $\mathcal{C}$ and $\mathcal{A}$:

Game 0: This is the real EUF-CMA security experiment. $\mathcal{C}$ initializes $\mathtt{pp} \leftarrow \mathtt{Setup}(1^\lambda)$ and honestly generates signer key pairs $(\mathtt{sk}_{s_i}, \mathtt{pk}_{s_i})$ following `SignerKeyGen`.

Game 1: $\mathcal{C}$ replaces all public key components $\mathbf{t}_i \in R_q^k$ with uniformly random vectors from R_q^k. Under the hardness of the $\mathsf{MLWE}_{n,m,q,\eta}$ problem, $\mathcal{A}$'s distinguishing advantage is bounded by: $|\Pr[\mathsf{Win}_1] - \Pr[\mathsf{Win}_0]| \leq \mathbf{Adv}^{\mathsf{MLWE}}_{\mathcal{A}}$.

Game 2: $\mathcal{C}$ simulates the `Sign` oracle queries without knowing the secret keys $\mathbf{s}_{1,i}, \mathbf{s}_{2,i}$. For each query on $(M_{\text{ctx}}, M_{\text{pol1}}, M_{\text{pol2}})$, $\mathcal{C}$ first honestly computes the integrity anchors $t_\ell \leftarrow H_{\mathsf{anchor}}(M_{\text{pol}\ell})$ and chameleon hashes h_ℓ via random oracles H_1, H_2 and H. Then, $\mathcal{C}$ invokes the rejection sampling technique for the multi-signature. Specifically, $\mathcal{C}$ samples $\mathbf{z}_i \leftarrow \mathcal{S}^l_{\gamma_1 - 1}$ and $c_i \leftarrow \mathcal{H}$ uniformly at random, and backtracks the commitment vector by setting: $\mathbf{w}_i \leftarrow \mathbf{A}\mathbf{z}_i - c_i\mathbf{t}_i \bmod q$. $\mathcal{C}$ then programs the random oracle $\mathcal{H}(\mathbf{w}_i \parallel \mathtt{pk}_{s_i} \parallel h \parallel t_1 \parallel t_2) = c_i$. According to the strict rejection sampling conditions in Step 11, the simulated signature distribution is statistically indistinguishable from the genuine signature distribution. Thus, $\Pr[\mathsf{Win}_2] = \Pr[\mathsf{Win}_1]$.

Suppose $\mathcal{A}$ outputs a valid forged certificate $\mathtt{Cert}^*$ in **Game 2**. By applying the General Forking Lemma, we replay $\mathcal{A}$ with a different random oracle response for $\mathcal{H}$, obtaining two valid responses $(\mathbf{z}_i, c_i)$ and $(\mathbf{z}^*_i, c^*_i)$ for the same commitment $\mathbf{w}_i$. This yields:

$$\mathbf{A}\mathbf{z}_i - c_i\mathbf{t}_i \equiv \mathbf{A}\mathbf{z}^*_i - c^*_i\mathbf{t}_i \pmod q. \tag{3}$$

Substituting the actual structure $\mathbf{t}_i = \mathbf{A}\mathbf{s}_{1,i} + \mathbf{s}_{2,i} \bmod q$, we can rewrite the equation as:

$$\mathbf{A}\left((\mathbf{z}_i - \mathbf{z}^*_i) - (c_i - c^*_i)\mathbf{s}_{1,i}\right) - (c_i - c^*_i)\mathbf{s}_{2,i} \equiv \mathbf{0} \pmod q. \tag{4}$$

Let $\mathbf{v} = \begin{bmatrix} (\mathbf{z}_i - \mathbf{z}_i^*) - (c_i - c_i^*)\mathbf{s}_{1,i} \\ -(c_i - c_i^*) \end{bmatrix}$. Since $c_i \neq c_i^*$, $\mathbf{v} \neq \mathbf{0}$ and its infinity norm satisfies $\|\mathbf{v}\|_\infty \leq 2(\gamma_1 - \beta) + 2\beta\eta \leq \beta_{\text{MSIS}}$. Hence, $\mathbf{v}$ constitutes a valid solution to the $\mathsf{MSIS}_{k,l+k,q,\beta_{\text{MSIS}}}$ instance, completing the proof.

5.3 Layer Isolation and Controllability

This section demonstrates that a compromised low-tier sanitizer (San_2) is bound by strict privilege limits and cannot execute cross-layer policy escalation.

Theorem 3. *The PQ-SMS scheme guarantees Layer Isolation. An insider adversary holding only $\mathit{sk}_{p,2} = T_{\mathbf{A}_1}$ cannot generate a valid sanitized certificate that modifies layer $\ell = 1$ under the $\mathsf{ISIS}_{n',m',q',\beta'}$ assumption.*

Proof. To forge a valid sanitized certificate for layer $\ell = 1$ with a modified tactical policy $M^\star_{\text{pol1}}$, the malicious low-tier sanitizer San_2 must find a new randomness vector $\mathbf{r}_1^\star$ such that the recomputed chameleon hash value h'_1 satisfies $h'_1 = h_1$. This maintains the validity of the global digest h and the multi-signature component σ_{multi}. This requires solving:

$$\mathbf{A}_0\mathbf{r}_1^\star + H_1(M_{\text{ctx}} \parallel M^\star_{\text{pol1}}) \equiv \mathbf{A}_0\mathbf{r}_1 + H_1(M_{\text{ctx}} \parallel M_{\text{pol1}}) \pmod{q'}. \tag{5}$$

Rearranging the terms, we obtain:

$$\mathbf{A}_0\mathbf{r}_1^\star \equiv \mathbf{y} \pmod{q'}, \tag{6}$$

where $\mathbf{y} = \mathbf{A}_0\mathbf{r}_1 + H_1(M_{\text{ctx}} \parallel M_{\text{pol1}}) - H_1(M_{\text{ctx}} \parallel M^\star_{\text{pol1}}) \bmod q'$. Since San_2 only possesses the sub-trapdoor $T_{\mathbf{A}_1}$ and does not hold $T_{\mathbf{A}_0}$, finding a short vector $\mathbf{r}_1^\star$ satisfying $\|\mathbf{r}_1^\star\| \leq \sigma\sqrt{m'}$ is computationally equivalent to solving an instance of the Inhomogeneous Short Integer Solution ($\mathsf{ISIS}_{n',m',q',\beta'}$) problem for the matrix $\mathbf{A}_0$, which is assumed to be hard. Thus, layer isolation is strictly enforced.

5.4 Sanitization Indistinguishability

This section verifies the Transparency goal, demonstrating that public token structures leak zero information regarding sanitization history.

Property 1. Let $\texttt{Cert}$ be a pristine certificate generated via $\texttt{Sign}$, and $\texttt{Cert}^\star$ be a sanitized certificate generated via $\texttt{Sanitize}$. For any unbounded passive traffic adversary $\mathcal{A}$, the statistical distance between the distributions of $\texttt{Cert}$ and $\texttt{Cert}^\star$ is negligible:

$$\mathbf{Dist}\left(\mathcal{A}(\texttt{Cert}), \mathcal{A}(\texttt{Cert}^\star)\right) \leq \mathsf{Negl}(\lambda). \tag{7}$$

Proof. The structural fields $M_{\text{ctx}}, M_{\text{pol1}}, M_{\text{pol2}}, t_1, t_2$, and σ_{multi} are structurally identical across both algorithms. The only differing elements are the Gaussian randomizers $\mathbf{r}_b$ and $\mathbf{r}_b^\star$ ($b \in \{1, 2\}$). In $\texttt{Sign}$, $\mathbf{r}_b$ is drawn directly from the discrete Gaussian distribution $\mathcal{D}_{\mathbb{Z}^{m'},\sigma}$. In $\texttt{Sanitize}$, $\mathbf{r}_b^\star$ is sampled using the GPV preimage sampling algorithm $\texttt{SamplePre}(T_{\mathbf{A}_b}, \mathbf{y})$.

According to the property of the GPV trapdoor sampler, if the Gaussian parameter satisfies $\sigma \geq \eta_\epsilon(\Lambda^\perp(\mathbf{A}_b))$ for a negligible $\epsilon > 0$, the output distribution of `SamplePre` is statistically close to the discrete Gaussian distribution $\mathcal{D}_{\mathbb{Z}^{m'},\sigma}$ restricted to the specific coset. Therefore, $\mathbf{r}_b$ and $\mathbf{r}_b^\star$ are statistically indistinguishable, ensuring that sanitization history is perfectly concealed against public traffic analysis.

5.5 Auditable Anchoring and Non-repudiation

This section proves our Accountability goal, achieving state tracking and anti-framing properties with zero storage logs.

As formalized in `Verify` (Steps 5–6), the state audit branching is evaluated deterministically via:

$$\texttt{Verify}(\cdot) = \begin{cases} 1_{\text{pristine}}, & \text{if } \mathcal{H} \text{ validates AND } H_{\mathsf{anchor}}(M_{\text{pol}\ell}) == t_\ell \text{ for } \ell \in \{1,2\} \\ 1_{\text{sanitized}}, & \text{if } \mathcal{H} \text{ validates AND } H_{\mathsf{anchor}}(M_{\text{pol}\ell}) \neq t_\ell \text{ for some } \ell \\ 0, & \text{otherwise} \end{cases} \tag{8}$$

Since the integrity anchors $t_\ell \leftarrow H_{\mathsf{anchor}}(M_{\text{pol}\ell})$ are computed during the initial `Sign` phase and bound into the global multi-signature digest $h \leftarrow H(h_1 \parallel h_2)$, any post-sign policy modification $M_{\text{pol}\ell} \rightarrow M^\star_{\text{pol}\ell}$ executed by a sanitizer (San_1 or San_2) will inevitably cause $H_{\mathsf{anchor}}(M^\star_{\text{pol}\ell}) \neq t_\ell$ due to the collision resistance of H_{anchor}. Since the sanitizers cannot forge the signers' original multi-signature σ_{multi} over a modified $t^\star_\ell$ (as proven in Theorem 1), the original signature state remains indelible. This provides robust non-repudiation and allows anyone to trace provenance without maintaining any historical status registries or databases.

6 Performance Analysis

This section evaluates the computational complexity, storage costs, and communication overhead of the proposed PQ-SMS scheme. We first analyze the concrete costs of individual phases and then present a comparative analysis against existing state-of-the-art schemes.

6.1 Complexity Profiling

We model the dominant operations using four atomic primitives: NTT denotes polynomial multiplication over $R_q = \mathbb{Z}_q[X]/\langle X^d + 1\rangle$; TrapGen denotes lattice trapdoor generation; SamplePre denotes Gaussian preimage sampling; and RO represents a random-oracle invocation.

Unless otherwise specified, all estimates follow the NIST Level-3 parameter set with ring degree $d = 256$, modulus $q = 8380417$, module dimensions $(k, l) = (6, 5)$, and dual-layer chameleon hash matrix $\mathbf{B} \in R_{q'}^{k \times m}$ with $m = 7$. The factor $\kappa \geq 1$ captures the expected number of iterations introduced by Dilithium-style rejection sampling.

Table 1 summarizes the dominant computational costs and element sizes of each protocol phase.

Table 1: Theoretical Complexity Analysis

Phase	**Computational Complexity**	**Element Size**
$\texttt{Setup}(1^\lambda)$	RO	$\lvert\texttt{pp}\rvert = \lvert\rho_0\rvert$
$\texttt{SignerKeyGen}(\texttt{pp})$	$k \cdot l \cdot \mathsf{NTT}$	$\lvert\texttt{pk}_{s_i}\rvert = \lvert\rho\rvert + (k+l)d \cdot \frac{\lceil \log_2 q \rceil}{8}$
$\texttt{RootKeyGen}(\texttt{pp})$	$2\mathsf{TrapGen}$	$\lvert\texttt{pk}_{p,1}\rvert = kmd \cdot \frac{\lceil \log_2 q' \rceil}{8}$
$\texttt{Delegate}(\cdot)$	RO	$\lvert\texttt{sk}_{p,2}\rvert = kmd \cdot \frac{\lceil \log_2 q' \rceil}{8}$
$\texttt{Sign}(\cdot)$	$2\mathsf{RO} + (\kappa nkl + 2km)\mathsf{NTT}$	$\lvert\texttt{Cert}\rvert = \lvert M\rvert + 2md \cdot \frac{\lceil \log_2 q' \rceil}{8} + n\lvert\sigma\rvert$
$\texttt{Verify}(\cdot)$	$2\mathsf{RO} + (nkl + 2km)\mathsf{NTT}$	1 bit
$\texttt{Sanitize}(\cdot)$	$1\mathsf{SamplePre} + km\mathsf{NTT}$	$\lvert\texttt{Cert}^\star\rvert = \lvert M^\star\rvert + 2md \cdot \frac{\lceil \log_2 q' \rceil}{8} + n\lvert\sigma\rvert$

Computational Characteristics. The computational profiles of `Sign` and `Verify` are intentionally asymmetric. The signing phase contains the rejection-sampling factor κ, whereas verification is fully deterministic. The additional $2km\mathsf{NTT}$ term originates from the evaluation of the two-layer chameleon hash structure. Since each layer performs one $k \times m$ matrix-vector multiplication over $R_{q'}$, the total overhead equals $2km$ ring multiplications.

Trapdoor Offloading Strategy. A key design objective of PQ-SMS is to isolate expensive lattice trapdoor operations from the online signing path. The macro-algorithm TrapGen is executed only during root key generation, while the costly Gaussian preimage sampler SamplePre appears exclusively during sanitization. Consequently, routine certificate issuance only requires standard module-lattice operations and chameleon-hash evaluations.

Scalability Characteristics. Although the cumulative workload grows linearly with the signer population n, the end-to-end latency does not necessarily scale in the same manner. Each signer independently executes its local Dilithium computation, enabling the dominant term $\kappa kl\mathsf{NTT}$ to be parallelized across participating nodes. As a result, the perceived signing delay is primarily determined by the slowest signer, certificate aggregation, and the fixed chameleon-hash evaluation cost.

Accountability–Storage Trade-off. The certificate size increases linearly with n because PQ-SMS preserves the individual signature shares $\sigma_{\text{multi}} = (\sigma_1, \ldots, \sigma_n)$. This choice intentionally trades compactness for direct signer accountability after sanitization. Unlike schemes that require tracing protocols or auxiliary proofs, signer attribution remains embedded within the certificate itself. Moreover, authorization information is carried directly by the delegated trapdoor hierarchy, avoiding dependence on an ever-growing transaction history.

6.2 Comparison with Related Schemes

To position PQ-SMS relative to existing approaches, we compare it with three representative baselines: the standard single-signer CRYSTALS-Dilithium, the lattice-based sanitizable signature scheme of Clermont et al., and the pairing-based hierarchical framework FABSS. The results are summarized in Table 2.

Table 2: Functional and Performance Comparison with Existing Schemes

Metric	Dilithium Baseline[12]	Zhu et al. [23]	Clermont et al. [9]	Ours (PQ-SMS)
Post-Quantum Security	✓	×	✓	✓
Data Sanitization	×	✓	✓	✓
Multi-Signer Support	×	×	×	✓
Hierarchical Control	×	✓	×	✓
External State Dependency	Stateless	Stateful (Key-Evolving)	Stateless	**Stateless (No Audit Log Growth)**
Signature / Cert Size	$O(kld \log q)$	Constant	Constant	$O(n(k+l)d \log q + kmd \log q')$
Dominant Computational Cost:				
– `Sign` Cost	κklNTT	$O(\|\omega\|)$Mult	κklNTT + SamplePre	$\mathbf{2}$RO + $(\kappa\mathbf{nkl} + \mathbf{2km})$NTT
– `Verify` Cost	klNTT	3Pair + $O(1)$Mult	klNTT + $\mathsf{Eval}_{\mathrm{CH}}$	$\mathbf{2}$RO + $(\mathbf{nkl} + \mathbf{2km})$NTT
– `Sanitize` Cost	×	$O(\|\omega\|)$Mult	1SamplePre	$\mathbf{1}$SamplePre + $\mathbf{km}$NTT

Functional Comparison. The comparison shows that none of the considered baselines simultaneously support post-quantum security, hierarchical delegation, data sanitization, and cooperative authorization. Dilithium provides strong post-quantum guarantees but lacks any redaction functionality. The scheme of Clermont et al. introduces lattice-based sanitization but adopts a flat authorization model. FABSS supports hierarchical policies, yet relies on pairing-based cryptography and therefore does not inherit post-quantum security. By embedding a dual-layer trapdoor delegation structure within a lattice framework, PQ-SMS combines these properties into a unified design.

Native Multi-Signer Authorization. All three baselines follow a single-signer paradigm. In distributed environments such as consortium blockchains, satellite constellations, or collaborative data spaces, collective authorization typically requires managing multiple independent certificates or introducing additional coordination mechanisms. In contrast, PQ-SMS integrates a signature collection $\sigma_{\text{multi}} = (\sigma_1, \ldots, \sigma_n)$ directly into a unified certificate, naturally supporting cooperative endorsement while preserving subsequent sanitization capabilities.

Editing Scalability and Accountability. An important architectural property of PQ-SMS is that sanitization complexity remains independent of the signer population. Although signing and verification scale with n, the sanitization cost remains bounded by 1SamplePre + kmNTT. This separation is particularly beneficial in large-scale deployments where certificate issuance is frequent but redaction operations occur relatively infrequently. Furthermore, preserving independent signature shares enables direct post-redaction accountability without requiring external tracing services or maintaining a growing audit-log infrastructure.

7 Related Work

Our work builds upon the confluence of three distinct research domains: post-quantum multi-signatures, updatable cryptography, and satellite network security. This section surveys the state-of-the-art in each area to precisely situate our contributions.

7.1 Post-Quantum Multi-Signature Schemes

Multi-Signature (MS) schemes, first conceptualized by Itakura and Nakamura [18], are a fundamental primitive for realizing distributed trust. Subsequent research yielded a rich ecosystem of schemes based on classical hardness assumptions, including number theory [4, 20], the discrete logarithm problem [26, 3], and bilinear pairings [11, 5]. The viability of these classical schemes is, however, fundamentally challenged by the advent of quantum computing. Shor's algorithm [31] demonstrated that these underlying problems are solvable in polynomial time on a quantum computer, rendering them insecure in the post-quantum era. This has spurred intensive research into designing quantum-resistant alternatives, with lattice-based cryptography emerging as a dominant paradigm. Constructions in this domain have primarily followed two main approaches: generic hash-and-sign methods [4] and more structured protocols based on the Fiat-Shamir transformation [14, 24, 25].

A straightforward method to achieve PQ-MS is through *signature concatenation*, whereby each party signs a message using a standard post-quantum signature scheme. We adopt this approach in our instantiation with CRYSTALS-Dilithium [12] due to its simplicity and direct security reduction. Early dedicated lattice-based schemes (e.g., by Bansarkhani & Strom [13] and Damgård et al. [10]) established feasibility but exhibited significant performance drawbacks, including large signatures, high round complexity, and a lack of key aggregation. Later works pursued both signature compression and key aggregation; notably, a scheme by Kansal & Dutta [19] introduced this combination, though a subsequent analysis by Liu et al. [22] revealed security vulnerabilities.

Current state-of-the-art schemes represent different philosophical approaches to solving this challenge:

- **Interactive Protocols:** Schemes like MuSig-L [6] adapt the Fiat-Shamir with Aborts paradigm. They achieve compact signatures and support a practical offline-online model but require at least one round of online interaction. Similarly, DualMS [8], a two-round protocol, achieves competitive key and signature sizes by avoiding the use of lattice trapdoors.
- **Non-Interactive Protocols:** The FSZ scheme [15] achieves full non-interactivity by employing one-time signatures and homomorphic Merkle tree commitments. This efficiency, however, is predicated on a more restrictive "synchronized" model and supports only a bounded number of signatures per key.

To provide a clear, high-level overview of this evolutionary path, we summarize and compare the key characteristics of these representative schemes in Table 3.

Table 3: Comparative Analysis of Representative Lattice-Based MS Schemes

Scheme	Rounds	Key Agg.	Paradigm	Key Trade-offs
Bansarkhani & Strom [13]	3	No	Interactive Protocol	High round complexity and large signatures.
Damgård et al. [10]	2	No	Interactive (Schnorr-like)	Improved rounds, but still large signatures.
FSZ [15]	0	Yes	One-Time Sigs + Merkle Tree	Fully non-interactive, but for a restricted synchronized model; bounded signatures.
MuSig-L [6]	1+1	Yes	Fiat-Shamir w/ Aborts	Offline/Online model; requires online interaction.
DualMS [8]	2	Yes	Interactive Protocol	No trapdoors; good size characteristics.

Our contribution is not a new multi-signature protocol itself, but rather a new functionality: rendering certificates signed under such schemes dynamic and updatable through cryptographic purification.

7.2 Chameleon Hashes and Updatable Cryptography

The concept of a chameleon hash, first introduced by Krawczyk and Rabin [21], provides the cryptographic foundation for our scheme's purifiability. The core idea of a hash function with a secret "trapdoor" to enable collision finding has inspired a rich field of research into dynamic and policy-based cryptography.

The migration to post-quantum security was enabled by seminal work from Cash, Hofheinz, Kiltz, and Peikert [7], who demonstrated how to construct efficient chameleon hashes from the SIS lattice problem. This construction forms the basis of our concrete instantiation and is favored for its strong security reduction and efficiency. The unique properties of chameleon hashes have been leveraged in various application domains. For instance, Ateniese et al. [2] proposed their use in creating *redactable blockchains*, enabling modification of block content without breaking the chain's integrity. Conceptually related are *sanitizable signatures* [29], which allow a designated party (the sanitizer) to modify parts of a signed message.

7.3 Security in Satellite Networks

The security of satellite communication networks is a long-standing research area, addressing threats ranging from jamming and spoofing to securing control links. With the proliferation of large-scale Low Earth Orbit (LEO) constellations, recent work has increasingly focused on scalable and robust Public Key Infrastructure (PKI) [27] and key management solutions [1, 32].

For instance, Salim et al. [28] provide a comprehensive survey of the security challenges in LEO satellite networks, highlighting key management as a primary concern due to intermittent connectivity and the scale of the constellations. Work by Howarth et al. [17] proposes a hierarchical key management framework for satellite networks to balance autonomy and centralized control. These

works correctly identify the unique environmental challenges inherent in satellite communications.

The need for post-quantum security in this domain is also gaining recognition. Position papers, such as those by Hasanaj et al. [16] and Sharmin et al. [30], have begun to outline the catastrophic implications of the quantum threat for satellite infrastructure and call for the urgent integration of PQC. However, the majority of current research in post-quantum satellite security remains at a high level, primarily advocating for the replacement of classical algorithms with PQC standards.

Our Position: Our work moves significantly beyond a simple one-for-one replacement of algorithms. While prior art correctly identifies the need for both robust PKI and post-quantum security in satellite networks, it has largely overlooked the critical challenge of *operational agility*. The problem of managing the certificate lifecycle—specifically, updating authorizations in-orbit efficiently and securely—remains a major research gap. Our `Sat-APCS` framework is the first to propose a concrete, post-quantum secure scheme that directly addresses this gap by introducing the concept of purifiability to satellite PKI.

8 Conclusion

In this paper, we identified the need for a PKI framework in next-generation satellite systems that is secure against quantum adversaries and agile for dynamic in-orbit operations. We then proposed `Sat-APCS`, a framework built upon the `PQ-SMS` primitive, which enables lightweight certificate policy updates without compromising an immutable root of trust. This approach overcomes the limitations of traditional "revoke-and-reissue" models, which are prohibitively slow and complex for in-orbit updates.

By integrating a lattice-based chameleon hash with a standard post-quantum multi-signature, we formally reduce the unforgeability and purification integrity of the scheme to well-established lattice assumptions. Our performance evaluation demonstrates that certificate updates via purification are substantially more efficient than full re-issuance in both computation and communication.

This work opens avenues for further research, including compact post-quantum multi-signature constructions to reduce certificate size, and deployment on resource-constrained platforms such as ARM Cortex-M or FPGAs to validate practical performance. Beyond satellite PKI, `PQ-SMS` may serve other domains requiring auditable, dynamic multi-party agreements, such as redactable blockchains or policy-driven access control.

In summary, `Sat-APCS` demonstrates that post-quantum security and in-orbit operational flexibility can be achieved in tandem, providing a principled blueprint for future satellite PKI systems.

References

1. Arslan, M.G., Alagoz, F.: Security issues and performance study of key management techniques over satellite links. In: 2006 11th international workshop on computer-

aided modeling, analysis and design of communication links and networks. pp. 122–128. IEEE (2006)
2. Ateniese, G., Magri, B., Venturi, D., Andrade, E.: Redactable blockchain–or–rewriting history in bitcoin and friends. In: 2017 IEEE European symposium on security and privacy (EuroS&P). pp. 111–126. IEEE (2017)
3. Bagherzandi, A., Cheon, J.H., Jarecki, S.: Multisignatures secure under the discrete logarithm assumption and a generalized forking lemma. In: Ning, P., Syverson, P.F., Jha, S. (eds.) Proceedings of the 2008 ACM Conference on Computer and Communications Security, CCS 2008, Alexandria, Virginia, USA, October 27-31, 2008. pp. 449–458. ACM (2008)
4. Bellare, M., Rogaway, P.: The exact security of digital signatures-how to sign with rsa and rabin. In: Maurer, U. (ed.) Advances in Cryptology — EUROCRYPT '96. pp. 399–416. Springer Berlin Heidelberg, Berlin, Heidelberg (1996)
5. Boldyreva, A.: Threshold signatures, multisignatures and blind signatures based on the gap-diffie-hellman-group signature scheme. In: International Workshop on Public Key Cryptography. pp. 31–46. Springer (2002)
6. Boschini, C., Takahashi, A., Tibouchi, M.: Musig-l: Lattice-based multi-signature with single-round online phase. In: Dodis, Y., Shrimpton, T. (eds.) Advances in Cryptology – CRYPTO 2022. pp. 276–305. Springer Nature Switzerland, Cham (2022)
7. Cash, D., Hofheinz, D., Kiltz, E., Peikert, C.: Bonsai trees, or how to delegate a lattice basis. Journal of cryptology **25**(4), 601–639 (2012)
8. Chen, Y.: DualMS: Efficient lattice-based two-round multi-signature with trapdoor-free simulation. In: Handschuh, H., Lysyanskaya, A. (eds.) Advances in Cryptology – CRYPTO 2023. pp. 716–747. Springer Nature Switzerland, Cham (2023)
9. Clermont, S., Düzlü, S., Janson, C., Porzenheim, L., Struck, P.: Lattice-based sanitizable signature schemes: Chameleon hash functions and more. In: Post-Quantum Cryptography. pp. 278–311. Springer Nature Switzerland, Cham (2025)
10. Damgård, I., Orlandi, C., Takahashi, A., Tibouchi, M.: Two-round n-out-of-n and multi-signatures and trapdoor commitment from lattices. In: IACR International Conference on Public-Key Cryptography. pp. 99–130. Springer (2021)
11. Drijvers, M., Gorbunov, S., Neven, G., Wee, H.: Pixel: Multi-signatures for consensus. In: 29th USENIX Security Symposium (USENIX Security 20). pp. 2093–2110 (2020)
12. Ducas, L., Kiltz, E., Lepoint, T., Lyubashevsky, V., Schwabe, P., Seiler, G., Stehlé, D.: Crystals-dilithium: A lattice-based digital signature scheme. IACR Transactions on Cryptographic Hardware and Embedded Systems pp. 238–268 (2018)
13. El Bansarkhani, R., Sturm, J.: An efficient lattice-based multisignature scheme with applications to bitcoins. In: International Conference on Cryptology and Network Security. pp. 140–155. Springer (2016)
14. Fiat, A., Shamir, A.: How to prove yourself: Practical solutions to identification and signature problems. In: Odlyzko, A.M. (ed.) Advances in Cryptology - CRYPTO '86, Santa Barbara, California, USA, 1986, Proceedings. Lecture Notes in Computer Science, vol. 263, pp. 186–194. Springer (1986)
15. Fleischhacker, N., Simkin, M., Zhang, Z.: Squirrel: Efficient synchronized multi-signatures from lattices. p. 1109–1123. CCS '22, Association for Computing Machinery, New York, NY, USA (2022)
16. Hasanaj, K., Hussien, O.A.A.M., Jahankhani, H.: Secure and resilient ip-satellite communication infrastructure. In: Space Governance: Challenges, Threats and Countermeasures, pp. 129–161. Springer (2024)

17. Howarth, M.P., Iyengar, S., Sun, Z., Cruickshank, H.: Dynamics of key management in secure satellite multicast. IEEE journal on selected areas in communications **22**(2), 308–319 (2004)
18. ITAKURA, K., NAKAMURA, K.: A public-key cryptosystem suitable for digital multisignatures. NEC research & development (71), 1–8 (1983)
19. Kansal, M., Dutta, R.: Round optimal secure multisignature schemes from lattice with public key aggregation and signature compression. In: International Conference on Cryptology in Africa. pp. 281–300. Springer (2020)
20. Komano, Y., Ohta, K., Shimbo, A., Kawamura, S.: Formal security model of multisignatures. In: Katsikas, S.K., López, J., Backes, M., Gritzalis, S., Preneel, B. (eds.) Information Security, 9th International Conference, ISC 2006, Samos Island, Greece, August 30 - September 2, 2006, Proceedings. Lecture Notes in Computer Science, vol. 4176, pp. 146–160. Springer (2006)
21. Krawczyk, H., Rabin, T.: Chameleon hashing and signatures. IACR Cryptol. ePrint Arch. p. 10 (1998), http://eprint.iacr.org/1998/010
22. Liu, Z.Y., Tseng, Y.F., Tso, R.: Cryptanalysis of a round optimal lattice-based multisignature scheme. Information Processing Letters **182**, 106364 (2023)
23. Liufu, Z., Jiguo, L., Yang, L., Yichen, Z.: Efficient and forward-secure attribute-based sanitizable signature scheme. Journal of Computer Research and Development **60**(12), 2737–2748 (2023). https://doi.org/10.7544/issn1000-1239.202220212, https://crad.ict.ac.cn/en/article/doi/10.7544/issn1000-1239.202220212
24. Lyubashevsky, V.: Fiat-shamir with aborts: Applications to lattice and factoring-based signatures. In: Matsui, M. (ed.) Advances in Cryptology - ASIACRYPT 2009, 15th International Conference on the Theory and Application of Cryptology and Information Security, Tokyo, Japan, December 6-10, 2009. Proceedings. Lecture Notes in Computer Science, vol. 5912, pp. 598–616. Springer (2009)
25. Lyubashevsky, V.: Lattice signatures without trapdoors. In: Pointcheval, D., Johansson, T. (eds.) Advances in Cryptology - EUROCRYPT 2012 - 31st Annual International Conference on the Theory and Applications of Cryptographic Techniques, Cambridge, UK, April 15-19, 2012. Proceedings. Lecture Notes in Computer Science, vol. 7237, pp. 738–755. Springer (2012)
26. Ma, C., Weng, J., Li, Y., Deng, R.: Efficient discrete logarithm based multi-signature scheme in the plain public key model. Designs, Codes and Cryptography **54**(2), 121–133 (2010)
27. Neish, A., Walter, T., Powell, J.D.: Design and analysis of a public key infrastructure for sbas data authentication. Navigation **66**(4), 831–844 (2019)
28. Salim, S., Moustafa, N., Reisslein, M.: Cybersecurity of satellite communications systems: A comprehensive survey of the space, ground, and links segments. IEEE Communications Surveys & Tutorials **27**(1), 372–425 (2024)
29. Samelin, K., Slamanig, D.: Policy-based sanitizable signatures. In: Cryptographers' Track at the RSA Conference. pp. 538–563. Springer (2020)
30. Sharmin, A., Mahmud, B.U., Nabi, N., Shaima, M., Faruk, M.J.H.: Cyber attacks on space information networks: Vulnerabilities, threats, and countermeasures for satellite security. Journal of Cybersecurity and Privacy **5**(3), 76 (2025)
31. Shor, P.W.: Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM review **41**(2), 303–332 (1999)
32. Wazid, M., Das, A.K., Shetty, S.: An authentication and key management framework for secure and intelligent transportation of internet of space things. IEEE Transactions on Intelligent Transportation Systems **25**(6), 5242–5257 (2024)