

Trace-Driven Evaluation of Post-Quantum Authentication for ADS-B Using OpenSky Network Data

Marcos Cabañas Maldonado ^{*,1} Junzi Sun ^{1,2} and Martin Strohmeier ^{3,2}

¹Faculty of Aerospace Engineering, Delft University of Technology, Delft, Netherlands

²OpenSky Network, Burgdorf, Switzerland

³Cyber-Defence Campus, armasuisse Science & Technology, Zurich, Switzerland

*Corresponding author: marcoscabanas@outlook.com

Abstract

ADS-B lacks native cryptographic source authentication, while aviation's long deployment lifetimes motivate quantum-resistant security. This study evaluates digital signatures conveyed through additional, fragmented 1090 MHz Extended Squitter transmissions. A reproducible framework combines day and night Mode S recordings from an OpenSky receiver at TU Delft with real signatures, and modeled processing and transmission queues. Each recording supplies a one-hour target window and a ten-minute authentication follow-up. Across 480 replay cases, ECDSA P-256 provides a classical reference for Falcon-512 and ML-DSA-44. Scenarios vary in message grouping, fragment transmission rate, receiver capacity, and reception assumptions, tracking ordinary reception separately from authentication. Under the no-interference control, with groups of 20 messages and 50 authentication frames/s per aircraft, Falcon authenticates 22.66% of daytime and 24.82% of nighttime targets within ten seconds of their source timestamps; ML-DSA authenticates none within this deadline. Across all tested scenarios using the assumed capture model, neither post-quantum scheme authenticates any target by the 70-minute cutoff because complete authentication material is not recovered. Grouping reduces communication demand and improves ordinary reception, but does not resolve reconstruction failures. SLH-DSA-SHA2-128s is validated on small workloads but excluded from full replay because of its high signature-generation cost and communication requirements. These findings are conditional on recorded timing, computational profiles, and interference assumptions. They identify barriers to comprehensive post-quantum authentication through the evaluated fragmented-signature design and motivate joint design of authentication, transport, and loss recovery.

Keywords: ADS-B; post-quantum cryptography; message authentication; digital signatures; aviation cybersecurity

Abbreviations: 1090ES: 1090 MHz Extended Squitter, ADS-B: Automatic Dependent Surveillance - Broadcast, ECDSA: Elliptic Curve Digital Signature Algorithm, ML-DSA: Module-Lattice-Based Digital Signature Algorithm, PQC: Post-Quantum Cryptography, SLH-DSA: Stateless Hash-Based Digital Signature Algorithm

1. Introduction

Automatic Dependent Surveillance-Broadcast (ADS-B) supports air-traffic surveillance through the periodic broadcast of aircraft identity and state information. However, its widely deployed 1090 MHz Extended Squitter (1090ES) implementation provides no native cryptographic source authentication, leaving receivers unable to establish message authenticity from the broadcast alone [1]. Introducing conventional signatures such as ECDSA could provide authentication, but a sufficiently capable quantum computer could recover their signing keys using Shor's algorithm and generate signatures that pass verification [2]. Aviation's long development, certification, and operational lifetimes make quantum resistance a present design consideration, since an authentication extension introduced today may remain deployed when such attacks become feasible [3]. Standardized post-quantum signatures offer candidate mechanisms, but their security alone does not establish their suitability for

ADS-B [4, 5].

The difficulty is both computational and communicational. Authentication material must share a constrained radio channel with surveillance traffic, while aircraft generate signatures and receivers reconstruct and verify them. Existing proposals explore different combinations of signatures, delayed key disclosure, and alternative transport mechanisms [6]. This paper examines the specific feasibility of conveying digital signatures through additional 1090ES-style transmissions. Ordinary message reception and subsequent authentication are treated separately: surveillance information can arrive before sufficient supporting material is available to establish its authenticity.

This work develops a reproducible evaluation using Mode S recordings from an OpenSky receiver hosted at TU Delft. Real cryptographic signatures are combined with a replay model of message grouping, fragment transmission, processing queues, and assumed interference. ECDSA P-256 provides a classical reference for Falcon-512 and ML-DSA-44 in the completed replay; SLH-DSA-SHA2-128s is additionally examined through implementation validation and analytical screening. The evaluation varies group size, fragment transmission rate, receiver processing capacity, and channel assumptions, measuring ordinary reception, authentication coverage, and authentication delay.

2. Background & Related Work

2.1 ADS-B 1090ES and Authentication Constraints

ADS-B operating on the 1090ES data link transmits identity, position, velocity, and other state information, using 112-bit Mode S Extended Squitter messages. Of these 112 bits, 56 constitute the ME field carrying the ADS-B application data, while the remaining fields are required for message identification, aircraft addressing, and parity/interrogator identification. The ME field is itself allocated according to the ADS-B message type and therefore does not constitute unused capacity available for arbitrary content. Importantly, 1090ES provides no generic fragmentation and reassembly mechanism through which larger objects can be transported across multiple messages [7, 8, 9].

The 1090ES protocol has parity mechanisms to provide error detection and support Mode S addressing functions, but does not establish the authenticity of the transmitter or protect message contents against deliberate modification. The protocol offers no mechanisms for transporting cryptographic credentials, establishing sessions, exchanging keys, or associating large authentication objects with sequences of ADS-B messages. Introducing digital signatures into 1090ES must therefore be treated as a protocol-extension problem rather than as the addition of a security field to an existing message.

ADS-B transmissions are periodic and asynchronous, and share the 1090 MHz channel with other surveillance traffic. Depending on the information being transmitted and the operational state of the aircraft, multiple Extended Squitters may be generated per second. A representative modeling value of up to 6.2 ADS-B transmissions per second per aircraft corresponds to approximately 0.0744% of raw channel airtime per aircraft when an Extended Squitter duration of approximately 120 μ s is considered [10]. ADS-B channel usage increases with aircraft density and is dwarfed by Mode S and other surveillance transmissions on the same frequency. Consequently, any in-band authentication mechanism introduces additional load on an already congested channel.

2.2 Existing ADS-B Authentication Research

The absence of native authentication in ADS-B has motivated research into mechanisms for establishing message integrity and source authenticity. Existing approaches include asymmetric digital signatures, identity-based and certificate-less cryptography, delayed-disclosure symmetric authentication, and physical- or infrastructure-based verification [11]. Despite their different security architectures, these cryptographic proposals face a common challenge: for successful real-world adoption,

authentication must be implemented within the restricted communication capacity of ADS-B while preserving its broadcast operation and compatibility with existing infrastructure.

Several works have investigated asymmetric authentication directly. Baek et al. proposed an identity-based signature scheme that precomputes message-independent operations before a surveillance message becomes available, reducing the computation required to complete its signature afterward [12]. Other approaches have considered hierarchical identity-based signatures with batch verification and certificate-less short signatures, addressing receiver verification workload, key management, and communication overhead [13, 14]. An alternative line of research employs delayed key disclosure to avoid public-key operations on individual ADS-B messages. Prakash et al. proposed authentication through retroactive key publication [15], while other approaches have similarly investigated time-dependent symmetric authentication for the ADS-B broadcast environment.

More recently, the Compatible Authenticated Bandwidth-efficient Broadcast protocol for ADS-B (CABBA) combines TESLA-based authentication with public-key infrastructure and the D8PSK phase overlay capability specified in DO-260C [6]. This allows authentication information to be conveyed without relying exclusively on additional conventional Extended Squitter transmissions. Preliminary software-defined radio experiments demonstrated that the two tested legacy receivers continued to decode ordinary ADS-B information correctly, while a separate traffic-based analysis estimated additional packet transmissions below 6% across the evaluated configurations. These findings are promising for bandwidth-efficient, backward-compatible authentication. However, the evaluated design uses ECDSA for its public-key component and does not assess post-quantum signatures. Consequently, the reported results do not establish the communication overhead or authentication performance of a post-quantum adaptation of CABBA, which would require further evaluation [6].

Other research has considered physical- and infrastructure-based verification, including multilateration, time-difference-of-arrival, ranging, and direction-of-arrival techniques [1, 16]. These approaches independently verify the physical origin or plausibility of a received transmission but do not provide cryptographic message-origin authentication; thus, they are complementary.

2.3 Post-Quantum Authentication and Research Gap

While ADS-B authentication has received considerable attention, its treatment from a post-quantum perspective remains limited. PQC has been investigated more broadly for aeronautical communications, particularly for security-aware future systems such as LDACS [17, 18, 19]. In contrast, little work has examined the integration of post-quantum authentication into the 1090ES environment. Recent ADS-B research continues to investigate new signature constructions, including hierarchical identity-based schemes [20], but has focused primarily on cryptographic security and computational performance rather than the system-level interaction of authentication mechanisms with 1090ES traffic. This leaves a gap between the development and standardization of post-quantum digital signatures and their operational feasibility within ADS-B 1090ES.

In this paper, rather than proposing a new protocol, we address this gap by evaluating how the size and computational characteristics of NIST-standardized and selected post-quantum digital signatures interact with real ADS-B traffic.

3. Evaluation Framework

3.1 Security Objective and Scope

This evaluation addresses message-origin authentication and integrity using post-quantum digital signatures. Confidentiality, jamming resistance, and location verification are out of scope and require complementary mechanisms. The focus is on the system-level feasibility of integrating digital

Table 1. Digital signature schemes and parameter sets considered in the evaluation.

Role	Scheme	Parameter set	PK [B]	Signature [B]
Classical baseline	ECDSA	P-256	65	64
PQC candidate	ML-DSA	ML-DSA-44	1312	2420
PQC candidate	Falcon	Falcon-512	897	Variable (approx. 655)
PQC candidate	SLH-DSA	SLH-DSA-SHA2-128s	32	7856

signatures into ADS-B. The analysis considers the generation, transmission, reconstruction, and verification of authentication material, as well as the resulting communication and computational requirements. Key provisioning, certificate distribution, trust-anchor management, revocation, and the detailed encoding of an eventual protocol extension are outside the scope. A valid association between an aircraft identity and the corresponding verification key is therefore assumed.

The evaluation is restricted to ADS-B over 1090ES. The alternative Universal Access Transceiver (UAT) link operates at 978 MHz and uses different message formats and transmission procedures [21, 22], which are outside the scope of this paper.

3.2 Candidate Signature Selection

The U.S. National Institute of Standards and Technology (NIST) established an international process to evaluate and standardize cryptography resistant to quantum attacks [23]. Selecting algorithms from this process provides comparatively mature candidates subjected to multiple rounds of public evaluation and cryptanalysis. The evaluation, therefore, considers ML-DSA and SLH-DSA, standardized as FIPS 204 and FIPS 205, respectively, and Falcon, selected as the basis for FN-DSA standardization under FIPS 206 [4, 5, 24].

These candidates exhibit different characteristics relevant to ADS-B. ML-DSA is a lattice-based scheme balancing signature size and computational performance, and represents NIST’s principal standardized general-purpose post-quantum signature. Falcon is also lattice-based but produces considerably smaller signatures, making it relevant to bandwidth-constrained communications. SLH-DSA instead relies on hash functions, providing a structurally different alternative with substantially larger signatures. Together, these schemes expose trade-offs between communication requirements, computational performance, and cryptographic construction.

ECDSA P-256 is included as a mature, standardized classical reference. ECDSA with SHA-256 over P-256 has also been specified for authentication within the Aeronautical Telecommunication Network using IPS [25, 26]. P-256 provides approximately 128 bits of security against classical (non-quantum) attacks, corresponding to an estimated attack effort of roughly 2^{128} operations. Its signature occupies 64 bytes when its two components are encoded as fixed-width 256-bit integers. Such a signature, while smaller than its PQC counterparts, already significantly exceeds the capacity of a single ME field. The selected parameter sets and their sizes are summarized in Table 1.

3.3 Authentication Architectures

The evaluation compares *per-message authentication* and *grouped-message authentication*. Both use detached signatures, which are pieces of the information calculated with keys that verify the correctness of the original messages. Both cases assume that the receiver possesses an authenticated public key for the transmitting aircraft.

In *per-message authentication*, each ADS-B message receives its own signature, corresponding to a group size of $k = 1$. Once the message contents are complete, signing can begin. The ordinary ADS-B

message is transmitted without waiting for this computation to finish; its signature is sent separately afterward. The receiver reads the message upon reception, but initially treats it as unauthenticated. Authentication occurs only after the receiver has obtained the complete signature and successfully verified it against the message.

In *grouped-message authentication*, one signature covers $k > 1$ consecutive messages from the same aircraft. The aircraft transmits each ordinary message without waiting for authentication and keeps a copy onboard. Once it has created all k messages, it can generate a signature over their stored copies. Each message belongs to only one group. The signed input also includes metadata identifying the aircraft, the group, and its constituent messages. The signature is transmitted separately. The receiver can read ordinary messages as they arrive, but authenticates the group only after receiving every message in that group and the complete signature, and successfully verifying the signature.

Larger k -groups reduce the number of signatures required per ordinary message, potentially reducing processing and transmission queues. However, they introduce a collection delay and require the receiver to obtain all constituent messages before verifying the group. Increasing k therefore creates a trade-off between reduced authentication workload, collection delay, and sensitivity to lost messages; it does not necessarily increase or decrease total authentication delay.

3.4 Analytical Constraint Screening

We first estimate the minimum communication demand of each signature scheme. For a signature of S_{sig} bits, allocating the 56-bit ME field of each authentication transmission to signature data gives

$$n_{\text{frag,min}} = \left\lceil \frac{S_{\text{sig}}}{56} \right\rceil. \quad (1)$$

This signature-only lower bound excludes association metadata and fragment headers; the implemented transport accounts for both, as described in Section 4.

With one signature per k surveillance messages, the minimum average overhead is $n_{\text{frag,min}}/k$ additional transmissions per message. For an aircraft transmitting at a mean rate $r_{\text{ADS-B}}$, the corresponding normalized authentication airtime demand is

$$C_{\text{auth,min}} = r_{\text{ADS-B}} \frac{n_{\text{frag,min}}}{k} t_{\text{ES}}, \quad t_{\text{ES}} = 120 \text{ } \mu\text{s}. \quad (2)$$

This quantity represents the required transmission time per unit time, excluding ordinary traffic.

4. Trace-Driven Experimental Methodology

This section describes how recorded ADS-B traffic is signed and replayed to evaluate the signature schemes. The experiment measures additional communication and processing requirements, effects on ordinary-message delivery, and the coverage and delay of subsequent authentication.

Ordinary reception and authentication are tracked separately. Signatures over individual messages or per-aircraft groups are fragmented into additional transmissions. The augmented traffic is evaluated under a no-interference control and a capture model, using the common receiver procedure that is described in detail in Figure 5.

4.1 Dataset and Observation Window

For the real-world validation of our assumptions, two decoded Mode S datasets, described in Table 2, were obtained from an OpenSky receiver at the Faculty of Aerospace Engineering, TU Delft, Netherlands, using the pyModeS live-recording command.

Table 2. Characteristics of the TU Delft recordings. Counts and rates refer to the first-hour target interval.

Characteristic	Daytime	Nighttime
Observation date(s)	8 October 2026	8–9 October 2026
First-hour interval, CEST	09:30–10:30	23:00–00:00
Follow-up interval, CEST	10:30–10:40	00:00–00:10
Recorded Mode S frames, all DFs	5,322,199	4,497,009
Target DF17 messages	752,053	651,084
Distinct target ICAO addresses	798	412
Mean recorded Mode S rate, frames/s	1,478.39	1,249.17
Mean target DF17 rate, messages/s	208.90	180.86
Maximum distinct target addresses per 60 s	268	183

The experimental input consists of the Mode S message records and timestamps stored in two .jsonl files. All supplied downlink formats contribute to the recorded channel traffic, while only first-hour DF17 messages are selected for authentication. These files contain frames recovered and exported by the receiver and decoder. Unobserved or undecoded transmissions, and Mode A/C replies omitted by the exporter, are unavailable. Consequently, the replay evaluates additional authentication traffic against the recorded Mode S traffic rather than a complete measurement of physical 1090 MHz channel occupancy. Furthermore, the inspected recording software assigns timestamps using the receiving computer’s clock separately for each incoming network batch. Variable network and processing delays can therefore distort the recorded timing between batches. The original receiver counters are not retained, preventing validation of these inter-batch intervals. Replay treats the supplied timestamps as assumed transmission and message-availability times; interference results are therefore conditional sensitivity estimates rather than measured RF loss probabilities.

Each replay starts with empty queues. Messages in $[0, 3600)$ s form the target cohort, followed by 600 s during which their outstanding signing, transmission, and verification work may complete. Recorded background traffic continues throughout this period, but later messages do not create or complete target groups. The common observation cutoff is therefore 4,200 s.

4.2 Cryptographic Implementations

ECDSA P-256 uses the Python package cryptography version 50.0.1, its OpenSSL 4.0.2 backend, the SECP256R1 curve, and SHA-256¹. The post-quantum implementations use liboqs-python version 0.16.0.1, imported as oqs, linked to native liboqs version 0.16.0². The selected liboqs mechanisms are Falcon-512, ML-DSA-44, and SLH_DSA_PURE_SHA2_128S. Actual Falcon signature lengths are retained.

ECDSA signatures are converted from the library’s DER encoding to a fixed-width $r \parallel s$ representation, with 32 big-endian bytes per integer, and converted back for verification. Post-quantum signatures retain the bytes returned by liboqs. The repository’s historical identifier FN-DSA-512 selects Falcon-512; it does not denote a finalized FN-DSA implementation, as it has not yet been standardized by NIST.

Each aircraft receives an independently generated key pair within each signed workload. For ordered original messages $m_1, \dots, m_k$, the signed input is

$$M = C \parallel m_1 \parallel \dots \parallel m_k, \quad \sigma = \text{Sign}(sk, M), \quad (3)$$

¹<https://cryptography.io/en/latest/hazmat/primitives/asymmetric/ec/>

²<https://github.com/open-quantum-safe/liboqs-python>

where $\parallel$ denotes byte concatenation. The serialized context C identifies the aircraft, algorithm, session, group sequence, source-time interval, message count, key fingerprint, and ordered message tags. The signature covers the complete original message bytes, not merely their association tags.

Every generated signature is verified with its public key before being accepted into the signed workload. Implementation checks also require rejection of modified messages. Public keys, encoded authentication objects, implementation versions, and checksums are retained in reusable artifacts. During replay, verification is performed over the input reconstructed from received material, rather than treating reception as evidence of cryptographic validity.

4.3 Authentication Generation and Transmission

For each aircraft, consecutive first-hour target messages form non-overlapping groups with $k \in \{1, 5, 10, 20\}$. A group enters the signing queue once all k messages are available; ordinary messages remain eligible for transmission at their trace timestamps.

For a signature of s bytes, the authentication stream contains $56 + 8k + s$ bytes, including association metadata and length fields. The illustrative transport reserves four of the seven ME-field bytes for the group sequence and fragment index, leaving three bytes of stream data per frame. Its authentication-frame requirement is

$$F(k, s) = \left\lceil \frac{56 + 8k + s}{3} \right\rceil. \quad (4)$$

This excludes the original ADS-B messages. Communication characterization also considers the optimistic signature-only bound $\lceil s/7 \rceil$, which omits metadata and fragment headers and does not represent a second implemented transport.

Each authentication frame occupies 120 μ s. Recorded short and long Mode S frames are assigned durations of 64 μ s and 120 μ s, respectively. Authentication fragments are paced at a maximum of

$$r \in \{10, 50, 100\} \text{ frames/s/aircraft,}$$

shared across an aircraft's groups. These rates are sensitivity settings, not measured channel capacities or authorized operational transmission rates.

One simulated radio per aircraft schedules target messages and authentication fragments. Ordinary messages take priority over queued fragments; a fragment already transmitting finishes before another frame starts. Other recorded traffic retains its supplied timing as background interference. The scheduler, therefore, does not represent complete transponder arbitration across every Mode S message type.

The receiver retains ordinary messages and authentication fragments separately. Verification requires every fragment and all original messages belonging to the signed group, with unambiguous association. Successful verification authenticates those messages retrospectively. Public keys are assumed provisioned. Credential distribution, retransmission, and error correction are excluded, and the hypothetical transport has no allocated operational ADS-B message type.

4.4 Computational Model

ECDSA uses published P256-Cortex-M4 measurements on a Nordic Semiconductor nRF52840 microcontroller (Arm Cortex-M4, 64 MHz): 5.9 ms per signature and 15.3 ms per verification [27]. Post-quantum reference times are derived from pqm4 cycle counts at 24 MHz [28]. ML-DSA-44 uses approximately 164.30 ms for signing and 59.23 ms for verification. Falcon uses a provisional FN-DSA implementation as a timing proxy, giving approximately 936.24 ms and 16.54 ms, respectively.

SLH-DSA uses SPHINCS+-SHA2-128s-simple as a lineage proxy, giving approximately 319.06 s for signing and 311.32 ms for verification.

Each algorithm uses fixed signing and verification times, without modeling how individual operations vary or how long they might take in the worst case. The timings come from different hardware and software; those for Falcon and SLH-DSA use related implementations rather than the liboqs code. ECDSA timings exclude message hashing and generation of the signing nonce, while the post-quantum benchmarks use 59-byte messages. Processing times are not adjusted for longer signed inputs. These values therefore describe assumed computing capacities, not the measured performance of a particular aircraft or ground receiver.

Each aircraft signs one complete group at a time, with other completed groups waiting in order of readiness. At the receiver, a shared queue collects verification jobs from all aircraft. The primary configuration checks one signature at a time using the algorithm-specific reference duration. A four-worker configuration checks up to four different signatures simultaneously, without shortening individual verification times. A separate configuration checks signatures sequentially but assumes only 1 ms per verification for every algorithm, corresponding to a capacity of 1,000 signatures/s. This analyst-selected value tests whether substantially faster verification improves authentication; it is not a measured hardware benchmark. Both sensitivity configurations change receiver verification only, leaving aircraft signing and transmission settings unchanged.

Offline multiprocessing used to prepare signatures does not change the simulated worker counts. Queues have no finite capacity limits. Energy use, total memory requirements, and contention with other avionics applications are outside the model.

4.5 Replay Scenarios and Channel Assumptions

Two reception models are compared: one assumes that overlapping transmissions cause no losses, while the other allows added authentication traffic to interfere with reception.

The *no-interference control* assumes that the receiver successfully receives every frame completed before the observation cutoff, even when transmissions overlap. Group formation, signing, fragment transmission, and verification still take time, and their queues remain active. Authentication can therefore be delayed or unfinished even when reception is perfect.

The *capture model* evaluates losses introduced by adding authentication transmissions. Since the original recording contains successfully decoded frames, overlaps between those frames cause no modeled losses, even after simulated scheduling shifts. Added authentication frames can interfere with ordinary messages and with other authentication frames. For an isolated overlapping pair involving an authentication frame, either frame has an equal chance of being received. These random choices are repeated using five seeds.

The scenario template in Table 3 combines these reception models with grouping size, authentication transmission rate, and receiver capacity. It contains 80 cases per algorithm and recording, with identical settings for daytime and nighttime. Every scenario family includes $k \in \{1, 5, 10, 20\}$. Receiver-capacity sensitivity is evaluated only under the no-interference control at 50 authentication frames/s per aircraft.

Without received-power information, the capture model assigns each frame a seeded random priority. For overlaps involving authentication traffic, a frame is rejected if a directly overlapping competitor has higher priority. Decisions depend on direct overlaps, so a chain of overlapping frames can have multiple surviving frames. Rejected frames still contribute interference; no interference cancellation is modeled.

Table 3. Replay scenario template per algorithm and recording. Each row includes $k \in \{1, 5, 10, 20\}$. Reference workers use algorithm-specific verification times. Authentication rates apply per aircraft.

Scenario family	Channel	Rate (frames/s)	Receiver	Seeds	Cases
Processing and pacing	No interference	10, 50, 100	1 reference worker	1	12
Added interference	Capture	10, 50, 100	1 reference worker	1–5	60
Parallel receiver	No interference	50	4 reference workers	1	4
Faster receiver	No interference	50	1 assumed 1 ms worker	1	4
Total per algorithm and recording					80

Capture scenarios are repeated with seeds 1 to 5. Each seed produces repeatable random priorities. All runs use the same recorded traffic and cached signatures; only the capture priorities change. Results report the mean and observed minimum-maximum range across these runs, rather than a confidence interval. Each no-interference configuration is deterministic and runs once. No independent random losses or additional timing jitter are introduced.

Interference between aircraft can cause reception loss but does not make aircraft wait for the shared channel to become free. To isolate losses caused by authentication traffic, reception is also evaluated with authentication frames removed while keeping ordinary-message transmission times unchanged. Received power, propagation geometry, and reception through multiple receivers are not modeled.

4.6 Evaluation Metrics

For a target message, let t_0 denote its source trace time, t_{rx} its successful reception time, and t_{auth} its successful authentication time. Authentication delay is measured from both origins:

$$\begin{aligned} D_{source} &= t_{auth} - t_0, \\ D_{reception} &= t_{auth} - t_{rx}. \end{aligned} \quad (5)$$

Deadline coverage is evaluated at $d \in \{1, 5, 10, 30, 60, 300, 600\}$ s. Source-relative coverage uses all first-hour targets. Reception-relative coverage uses successfully received targets whose complete deadline interval is observable before the cutoff. Eligible and excluded counts accompany these measurements.

Authentication-added transmission delay is measured against the same aircraft radio carrying ordinary messages only:

$$\Delta_{tx,i} = t_{tx,i}^{auth} - t_{tx,i}^{ordinary-only}. \quad (6)$$

This separates authentication contention from ordinary radio queueing already implied by the trace. Since sensor-generation times are unavailable, it does not measure absolute onboard sensor-to-transmission latency.

Communication metrics distinguish total required authentication frames from frames actually transmitted during the observation period. Offered airtime sums frame durations and may exceed elapsed time when transmissions overlap; it is not measured spectrum occupancy.

5. Results

The completed replay comprises 480 cases across ECDSA P-256, Falcon-512, and ML-DSA-44, using 5,678,094 cryptographically verified signatures across the two recordings and four grouping configura-

rations. SLH-DSA was validated on smaller workloads and assessed through the screening described below.

5.1 SLH-DSA Screening and Exclusion from Full Replay

SLH-DSA-SHA2-128s was implemented and successfully validated on small workloads. Its complete workload across both recordings and the four alternative grouping configurations would require 1,892,698 signatures. The full signing-and-replay matrix was omitted because of its high offline generation cost and the unfavorable communication requirements identified below.

A preliminary runtime diagnostic³ used three serial samples per algorithm and grouping configuration on representative inputs. SLH-DSA median signing and verification times were approximately 442–444 ms and 0.45–0.46 ms, respectively. Applying each algorithm’s measured medians to the 1,892,698 signatures required across both recordings and all four grouping configurations projects 233.27 h for sequential SLH-DSA signing and one verification per signature, compared with 1.82 h for Falcon-512 and 8.68 min for ML-DSA-44. Under ideal parallel execution using four processes, these estimates become 58.32 h, 27.27 min, and 2.17 min, respectively. These are preliminary workload projections, not measured end-to-end runtimes; they exclude key generation, file handling, repeated validation, replay, and parallelization overhead.

The communication requirement provides independent evidence for screening. A 7,856-byte signature [5] requires at least $\lceil 7856/7 \rceil = 1123$ additional frames, even when all seven available payload bytes carry signature data. At the fastest evaluated rate of 100 frames/s, fragment transmission alone requires at least 11.22 s. Thus, even optimistic delivery cannot meet the study’s ten-second authentication threshold before adding signing, group formation, queues, verification, or losses.

At the largest evaluated group size, $k = 20$, signature-only airtime totals 5,016.85 s for daytime and 4,362.45 s for nighttime. Both exceed the complete 4,200 s observation horizon, before ordinary traffic or authentication metadata is included. All required signature frames therefore cannot be serialized without overlap within the evaluated time budget. Figure 1 compares these requirements with the other algorithms.

The declared SPHINCS+-SHA2-128s-simple reference proxy [28], implying approximately 319 s per signature at 24 MHz, introduces an additional processing constraint. It is a conditional estimate rather than a measurement of standardized SLH-DSA on aircraft hardware.

These findings support screening out this parameter set as a practical candidate for timely, comprehensive in-band authentication within the investigated grouping and transport design. No full-window SLH-DSA reception percentage, authentication coverage, or replay latency is claimed. The conclusion does not extend to every SLH-DSA parameter set, processor, or alternative communication architecture.

5.2 Baseline Recorded Mode S Traffic Characteristics

The daytime target hour contains 5,322,199 recorded Mode S frames, including 752,053 target DF17 messages from 798 distinct aircraft addresses. The nighttime hour contains 4,497,009 frames, including 651,084 targets from 412 addresses. Figure 2 shows cumulative frame counts by downlink format. All recorded formats contribute to background traffic, while only first-hour DF17 messages are signing targets. The unauthenticated baseline introduces no signature traffic and provides no cryptographic message authentication. Recorded messages are accepted as successfully received by construction, since the input consists of messages already observed by the receiver. This does not imply that every original real-world transmission was received.

³Performed using an ARM64 Mac with eight logical CPUs and 16 GiB RAM, running macOS 26.4, Python 3.13.3, and

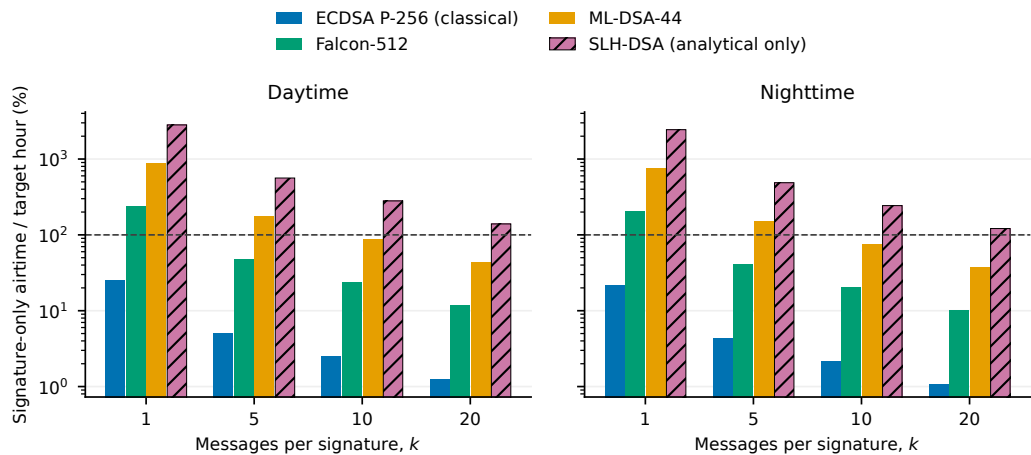


Figure 1. Optimistic signature-only airtime relative to the one-hour target window. ECDSA is the classical reference; SLH-DSA is analytical only. The vertical axis is logarithmic. Ordinary traffic and protocol metadata are excluded. The dashed line represents one hour of aggregate airtime, not an operational capacity threshold.

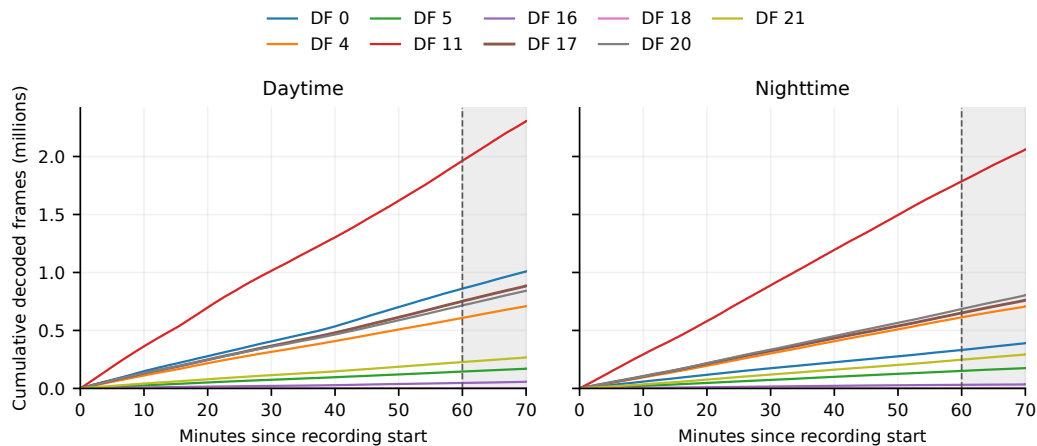


Figure 2. Cumulative recorded Mode S frames by downlink format, with matched daytime and nighttime axes. The dashed line ends target selection at 60 minutes; the shaded region supplies background traffic during authentication follow-up. Counts represent exported decoded frames, rather than every physical transmission on 1090 MHz.

5.3 Communication Overhead and Offered Airtime

The classical ECDSA reference uses 64-byte signatures, compared with approximately 655 bytes for Falcon and 2,420 bytes for ML-DSA. Including the implemented headers and association metadata, per-message authentication requires 43 additional frames for ECDSA, approximately 240 for Falcon, and 828 for ML-DSA.

Grouping reduces the number of signatures, although the information identifying the messages within each group increases. At $k = 20$, the corresponding requirements are 94, approximately 291, and 879 authentication frames per group. These are additional frames; ordinary ADS-B messages

are transmitted separately.

At this group size, required daytime authentication airtime is equivalent to 11.66% of the target hour for the classical reference, compared with 36.07% for Falcon and 109.08% for ML-DSA. Nighttime requirements are 10.14%, 31.37%, and 94.85%, respectively. The post-quantum alternatives therefore retain a substantial communication cost relative to conventional signed authentication.

These requirements include every complete signing group, including work unfinished at the cutoff. They exceed the optimistic bounds in Figure 1 because the implemented transport carries metadata and fragment headers. Summed airtime measures offered demand, not physical channel occupancy or packet loss. Low transmitted authentication traffic can consequently reflect an unfinished queue rather than a small required workload.

5.4 Authentication Latency

Figure 3 compares authentication timeliness under the no-interference control. It asks how promptly authentication could complete if reception losses were removed while retaining processing and transmission constraints.

At matched settings of $k = 20$ and 50 authentication frames/s, 73.31% of daytime targets authenticate within ten seconds using ECDSA, compared with 22.66% using Falcon and zero using ML-DSA. The corresponding nighttime fractions are 78.43%, 24.82%, and zero. Longer deadlines substantially improve coverage. Falcon reaches 98.75% daytime and 98.88% nighttime coverage within 600 seconds, approximately matching the classical reference at this grouping size. ML-DSA reaches 66.40% and 55.15%, respectively. High eventual coverage therefore does not necessarily imply timely authentication.

These deadlines begin at each message’s recorded source timestamp. A message authenticated by the common 70-minute cutoff can still miss its individual 600-second deadline. Consequently, final-cutoff coverage and deadline coverage answer different questions.

Ordinary transmission remains independent of signing. Across the evaluated configurations, authentication adds at most approximately 0.12 ms to ordinary transmission, and fewer than 1.2% of targets experience a positive additional delay. Ordinary messages have priority once any authentication frame already in flight finishes. These values quantify additional modeled delay, rather than absolute onboard sensor-to-transmission latency.

5.5 Authentication Reconstruction and Success

Table 4 reports ordinary reception and subsequent authentication under the capture model. Both percentages use all target messages as their denominator, and authenticated messages are a subset of received messages. Unlike Figure 3, the table includes modeled reception losses and counts authentication completed by the common 70-minute cutoff.

Grouping improves ordinary reception by reducing additional traffic. For daytime $k = 20$, reception reaches 89.23% with the classical reference, 71.55% with Falcon, and 46.87% with ML-DSA. However, none of these configurations authenticate a target message by the cutoff.

The failure counters identify incomplete reconstruction as the principal bottleneck. Even for the smaller classical signatures, daytime ECDSA at $k = 5$ receives approximately 5.49 million authentication fragments but reconstructs only 25 complete authentication signatures out of 150,103, averaged across five runs. Only six groups also have all required ordinary-message inputs available, authenticating 30 messages, or 0.00399% of the target population.

This explains why improved reception may or may not produce improved authentication. Larger

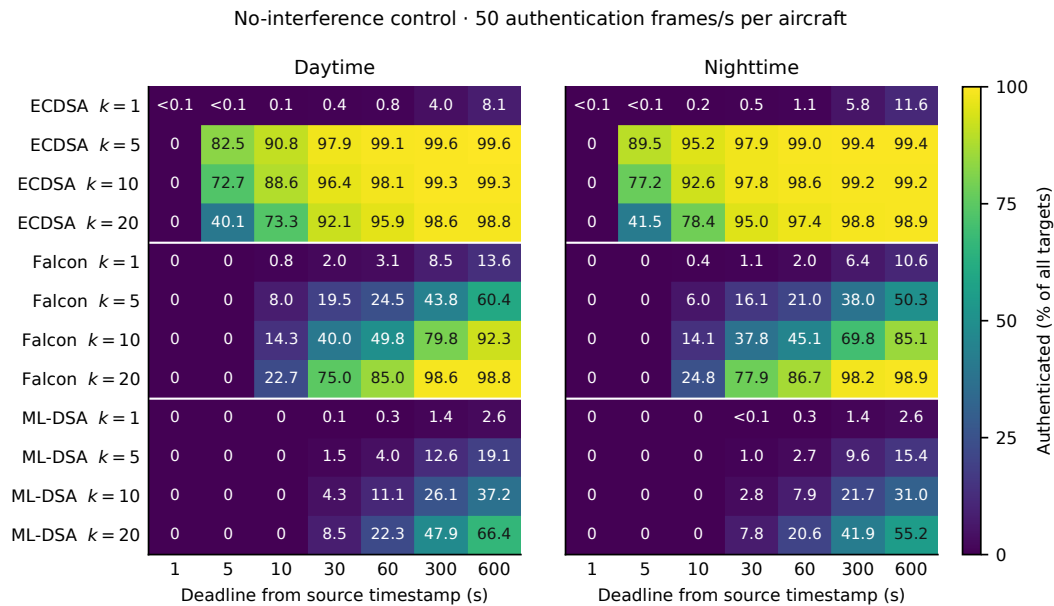


Figure 3. Percentage of all targets authenticated within each source-relative deadline under the no-interference control, at 50 authentication frames/s per aircraft and one reference verification worker. ECDSA supplies the classical comparison. Exact zeros are distinguished from positive values below 0.1%. The figure suppresses reception losses but retains processing and transmission constraints; it does not report final-cutoff coverage.

groups require fewer authentication frames per ordinary message, but each group requires a larger complete authentication object and all of its constituent messages. For example, ECDSA at $k = 20$ requires all 94 authentication fragments and all 20 ordinary messages. In these runs, reduced traffic did not compensate for the complete-group reconstruction requirement.

The larger post-quantum authentication objects encounter the same limitation. Across every tested capture configuration and seed, Falcon and ML-DSA produce no complete received authentication object and consequently authenticate no target messages. These are delivery and reconstruction failures, rather than invalid cryptographic signatures. The evaluated transport provides neither retransmission nor erasure coding.

5.6 Verification Workload

Figure 4 compares receiver capacity across the classical reference and both post-quantum algorithms. Under ideal reception, $k = 1$, and 50 authentication frames/s, increasing the receiver from one to four reference workers raises daytime ECDSA coverage from 36.49% to 93.47%. Falcon increases from 31.55% to 35.91%, while ML-DSA increases from 9.30% to 13.87%. Nighttime improvements for the post-quantum schemes are smaller still.

An assumed 1 ms verification worker produces approximately the same coverage as four reference workers. Remaining signing and transmission work therefore limits coverage even after additional verification capacity is available. Under capture, missing authentication material presents a further limitation that faster verification cannot resolve.

5.7 Sensitivity Analysis

Table 4. Ordinary reception and authentication at 50 authentication frames/s per aircraft, under the capture model with one reference verification worker. Signed results are means across five seeds, expressed as percentages of all first-hour targets. Authentication is measured at the 70-minute cutoff. The unsigned row is the conditioned baseline. Authentication is a subset of reception; zeros denote no authenticated messages, rather than rounded small values.

Algorithm	k	Daytime		Nighttime	
		Received (%)	Authenticated (%)	Received (%)	Authenticated (%)
Unsigned ADS-B	–	100	0	100	0
ECDSA P-256 (classical)	1	46.23	0.01364	53.89	0.05053
	5	77.29	0.00399	79.89	0.02058
	10	85.04	0.00133	86.88	0.00307
	20	89.23	0	90.55	0
Falcon-512	1	29.81	0	37.71	0
	5	43.40	0	50.93	0
	10	57.42	0	61.75	0
	20	71.55	0	74.68	0
ML-DSA-44	1	22.68	0	33.76	0
	5	30.59	0	39.22	0
	10	35.50	0	44.06	0
	20	46.87	0	52.63	0

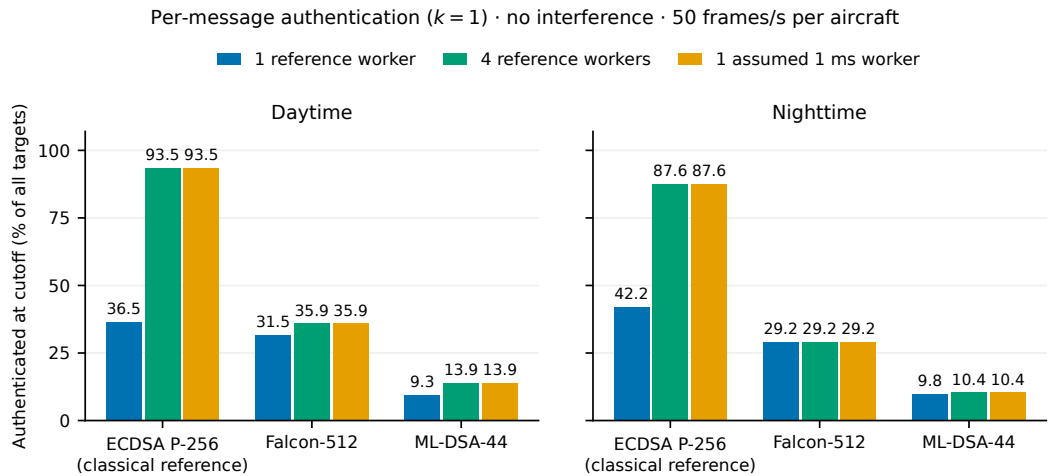


Figure 4. Receiver-capacity sensitivity for per-message authentication ($k = 1$), under the no-interference control at 50 authentication frames/s per aircraft. Bars show the percentage of all targets authenticated by the 70-minute cutoff. ECDSA is the classical reference. Reference-worker speeds are algorithm-specific; the 1 ms verification time is hypothetical.

5.7.1 Grouping and Signing Capacity

Grouping reduces signing frequency and communication demand while increasing the wait for a complete group. Among messages in complete $k = 20$ groups, the 95th-percentile formation wait is 36.69 s in daytime and 23.26 s at night. A further 7,493 daytime and 3,644 nighttime messages remain in incomplete final groups and receive no signature at the cutoff.

439

440

441

442

443

Under the configured Falcon signing proxy of approximately 936.24 ms per group, per-message signing leaves 64,087 daytime and 99,763 nighttime groups unfinished at the signing stage at the cutoff. At $k = 20$, neither window retains unfinished signing groups. Grouping can therefore remove a computational bottleneck without resolving the separate reconstruction failures observed under capture.

5.7.2 Authentication Transmission Rate

Increasing transmission rate can improve ideal-reception coverage while reducing ordinary reception under capture. For daytime ML-DSA at $k = 20$, raising the rate from 10 to 100 frames/s increases no-interference authentication coverage from 36.86% to 98.68%. Under capture, ordinary reception falls from 73.09% to 41.84%, while authentication coverage remains zero.

Faster fragment transmission therefore trades reduced transmission backlog against additional shared-channel interference. Its benefit depends on which stage limits successful authentication.

5.7.3 Traffic Window and Capture Variability

The nighttime window provides higher ordinary reception in the compared configurations. At $k = 20$ and 50 frames/s, Falcon reception increases from 71.55% in daytime to 74.68% at night; ML-DSA increases from 46.87% to 52.63%. Authentication nevertheless remains zero under capture for both schemes. Lower aggregate traffic also does not guarantee smaller processing queues, because workload timing and its distribution across aircraft differ.

The five seeds retain identical messages and signed workloads, changing only the random priorities used to resolve capture conflicts. For daytime ML-DSA at $k = 20$ and 100 frames/s, ordinary reception ranges from 41.80% to 41.87%. This range describes variation across those assignments, rather than a confidence interval for operational reception or variability across recording days.

6. Discussion

The results show that timely ADS-B authentication requires valid signatures, delivery of the supporting material, reconstruction of the signed input, and successful verification. Under the evaluated assumptions, communication and processing constraints substantially limit authentication coverage.

6.1 Limits of Authentication

Separating ordinary reception from authentication preserves the availability of surveillance information while its authenticity remains unresolved. This is useful for compatibility with existing ADS-B operation, but introduces an interval during which received information remains unverified. Authentication completed after an operational decision cannot retrospectively protect that decision. Consequently, high eventual authentication coverage does not necessarily imply effective protection for time-sensitive surveillance. An operational receiver would require explicit policies for provisional use, authentication expiry, and the treatment of missing or rejected authentication material.

Cryptographic authentication also has a narrower scope than surveillance correctness. A valid signature binds message contents to a provisioned credential; it does not independently establish that the reported position is correct or that the underlying navigation source is trustworthy. Incorrect data produced by a legitimate transmitter can still carry a valid signature.

The scenarios defined in subsection 4.5 identify bottlenecks rather than establish rigorous upper and lower bounds on operational performance. Actual reception depends on received power, decoder behavior, and unrecorded interference that the capture model does not reproduce. Moreover, an

ideal reception can increase verification queues, so it does not necessarily maximize authentication coverage within every deadline.

6.2 Algorithm and Architecture Trade-offs

The classical reference demonstrates that fragmentation and incomplete reconstruction constrain signed ADS-B even before the additional overhead of post-quantum signatures is introduced. Falcon and ML-DSA impose different burdens: Falcon requires fewer transmissions, whereas ML-DSA offers faster signing under the selected timing profiles but produces larger signatures. Their suitability, therefore, depends on the combined processing and communication requirements rather than on signature size or isolated execution time alone.

Grouping reduces signature demand but introduces collection delay and, in the evaluated design, dependence on receiving every constituent message and authentication fragment. This dependency is specific to the reconstruction procedure, rather than an unavoidable property of grouped authentication. Alternative message representations or loss-recovery mechanisms could improve robustness, but their additional communication and processing costs would require evaluation.

The timing profiles represent assumed resources rather than measured performance on aircraft and receivers. Optimized implementations and hardware acceleration could shorten processing times, while competing workloads could reduce available capacity. Sustainable operation requires each aircraft's signer to keep pace with group formation and the receiver to keep pace with the aggregate arrival of reconstructable groups, with sufficient headroom for bursts and timing variability.

Faster signing can also expose a communication bottleneck by making more authentication traffic available for transmission, potentially increasing interference with ordinary messages. Hardware improvements, therefore, require evaluation through the complete replay rather than proportional reductions in the reported authentication delays.

The SLH-DSA screening identifies a further constraint that faster hardware cannot remove: its signature bytes still have to be transmitted. Together with the processing requirements under the selected proxy, this supports screening out SLH-DSA-SHA2-128s for timely, comprehensive authentication within the investigated transport and grouping range. This conclusion does not extend to every SLH-DSA parameter set or alternative communication architecture.

6.3 Future CNS Evolution

The findings favor treating authentication as a requirement of the communication, navigation, and surveillance architecture, with an explicit allocation of bandwidth, processing capacity, and trust-management resources. Adding independently fragmented public-key signatures to existing broadcasts places a large burden on a channel that must continue carrying the underlying surveillance traffic.

One research direction is to use post-quantum signatures less frequently to authenticate longer-lived key material, while using compact authenticators for individual messages. Delayed-disclosure broadcast schemes such as TESLA provide a relevant architectural example, although they introduce their own timing and trust requirements⁴. Their suitability would depend on secure initialization, clock assumptions, loss tolerance, and acceptable authentication delay. Such an approach would require a new evaluation and is not validated by the present results.

Another direction is to carry authentication material over a complementary link with greater provision for security traffic. EUROCONTROL describes LDACS as a wideband aeronautical communication system with reservation-based access and ongoing investigation of surveillance applica-

⁴<https://www.rfc-editor.org/rfc/rfc4082.html>

tions⁵. This motivates examining authentication alongside future link design. Any complementary architecture would also need to address coverage, airborne reception, interoperability, credential distribution, and continued operation when the additional link is unavailable.

6.4 Limitations

The empirical scope is limited to two recordings from one receiver. They support a comparison between the observed daytime and nighttime workloads, but do not establish general behavior across airports, receiver locations, traffic conditions, or seasons. Only exported decoded Mode S frames are available, and the timestamp uncertainty described in the Methodology directly affects the inferred overlap patterns. Exact RF failure percentages are therefore less robust than workload counts and signature-size-based communication requirements.

The observation design also favors eventual completion by stopping the creation of new target groups after the first hour while allowing existing work to continue. A continuously operating system would receive new authentication work throughout that period. Final-cutoff coverage should therefore not be interpreted as evidence of steady-state capacity, and unfinished work at the cutoff remains censored rather than demonstrating permanent authentication failure.

Several assumptions affect realism in different directions. Provisioned keys and unconstrained queues omit credential distribution, storage limits, and resource contention, whereas the absence of retransmission or error correction increases sensitivity to missing material. Adding recovery mechanisms would consume further channel capacity. The evaluation also does not measure energy consumption, worst-case execution times, or performance under deliberate interference and authentication-flooding attacks. The selected parameter sets and heterogeneous timing references do not constitute a security-level-matched hardware benchmark.

The next validation steps should therefore combine recordings that preserve receiver timing with measured performance on candidate onboard and ground platforms, followed by receiver experiments that characterize capture and reconstruction under controlled interference. Operational suitability would additionally require application-specific authentication deadlines and a safety assessment of how unverified information is used.

7. Conclusion

This study combined two recorded Mode S traffic windows with real cryptographic signatures to evaluate fragmented authentication over ADS-B 1090ES. ECDSA P-256 provided a classical reference for Falcon-512 and ML-DSA-44, while SLH-DSA-SHA2-128s was assessed through implementation validation and screening.

Even under ideal reception, processing and fragment transmission constrained authentication within the evaluated deadlines. Under the assumed capture model, Falcon and ML-DSA produced no complete received authentication objects and therefore authenticated no target messages by the observation cutoff. Grouping reduced signature demand and improved ordinary reception, but increased the number of inputs required for successful group authentication. Additional verification capacity relieved individual bottlenecks without resolving signing or delivery constraints. SLH-DSA screening identified substantial signature-transmission requirements alongside high offline generation cost and unfavorable embedded processing estimates.

The results therefore do not support the evaluated fragmented-signature retrofit as a practical means of providing comprehensive post-quantum authentication under the investigated conditions. Reception estimates remain conditional on the recording and interference assumptions, and the findings

⁵<https://www.eurocontrol.int/system/l-band-digital-aeronautical-communication-system>

do not establish that other ADS-B authentication architectures are infeasible. Progress requires joint evaluation of authentication, transport, loss recovery, and processing capacity, supported by measurements on candidate airborne and ground hardware and controlled receiver experiments.

References

- [1] M. Strohmeier, V. Lenders, and I. Martinovic. “On the Security of the Automatic Dependent Surveillance-Broadcast Protocol”. In: *IEEE Communications Surveys & Tutorials* 17.2 (2015), pp. 1066–1087. ISSN: 2373-745X. DOI: 10.1109/comst.2014.2365951.
- [2] D. Moody, R. Perlner, A. Regenscheid, A. Robinson, and D. Cooper. *Transition to Post-Quantum Cryptography Standards*. NIST Internal Report 8547 ipd. Initial Public Draft. National Institute of Standards and Technology, Nov. 2024. DOI: 10.6028/NIST.IR.8547.ipd.
- [3] K. Varner, W. Zaeske, S. Friedrich, A. Kaiser, and A. Bowman. “Agile, Post-Quantum Secure Cryptography in Avionics”. In: *CEAS Aeronautical Journal* 17 (2026), pp. 133–163. DOI: 10.1007/s13272-025-00806-5.
- [4] National Institute of Standards and Technology. *Module-Lattice-Based Digital Signature Standard*. FIPS 204. National Institute of Standards and Technology. Gaithersburg (MD, United States), Aug. 2024. DOI: 10.6028/NIST.FIPS.204.
- [5] National Institute of Standards and Technology. *Stateless Hash-Based Digital Signature Standard*. FIPS 205. National Institute of Standards and Technology. Gaithersburg (MD, United States), Aug. 2024. DOI: 10.6028/NIST.FIPS.205.
- [6] M. Ngamboé, X. Niu, B. Joly, S.P. Biegler, P. Berthier, R. Benito, G. Rice, J.M. Fernandez, and G. Nicolescu. “CABBA: Compatible Authenticated Bandwidth-efficient Broadcast Protocol for ADS-B”. In: *International Journal of Critical Infrastructure Protection* 48 (2025), p. 100728. DOI: 10.1016/j.ijcip.2024.100728.
- [7] Radio Technical Commission for Aeronautics. *Minimum Operational Performance Standards for 1090 MHz Extended Squitter Automatic Dependent Surveillance-Broadcast (ADS-B) and Traffic Information Services-Broadcast (TIS-B)*. RTCA DO-260C. RTCA, Inc. Washington D.C. (United States), Dec. 2020.
- [8] International Civil Aviation Organization. *Aeronautical Telecommunications*. 5th ed. Annex 10 to the Convention on International Civil Aviation - Volume IV Surveillance and Collision Avoidance Systems. Montreal (Quebec, Canada), Mar. 2014. ISBN: 978-92-9249-537-4.
- [9] J. Sun. *The 1090 Megahertz Riddle: A Guide to Decoding Mode S and ADS-B Signals*. 2nd ed. TU Delft OPEN Publishing, 2021. ISBN: 978-94-6366-402-8. DOI: 10.34641/mg.11.
- [10] International Telecommunication Union. *Reception of Automatic Dependent Surveillance Broadcast via Satellite and Compatibility Studies With Incumbent Systems in the Frequency Band 1087.7–1092.3 MHz*. Tech. rep. ITU-R M.2413-0. Geneva (Switzerland): International Telecommunication Union, 2017. URL: https://www.itu.int/dms_pub/itu-r/opb/rep/R-REP-M.2413-2017-PDF-E.pdf.
- [11] H. A. Khan, H. Khan, S. Ghafoor, and M. A. Khan. “A Survey on Security of Automatic Dependent Surveillance-Broadcast (ADS-B) Protocol: Challenges, Potential Solutions, and Future Directions”. In: *IEEE Communications Surveys & Tutorials* 27.5 (Oct. 2025), pp. 3199–3226. ISSN: 2373-745X. DOI: 10.1109/comst.2024.3513213.
- [12] J. Baek, Y.-J. Byon, E. Hableel, and M. Al-Qutayri. “Making Air Traffic Surveillance More Reliable: A New Authentication Framework for Automatic Dependent Surveillance-Broadcast (ADS-B) Based on Online/Offline Identity-Based Signature”. In: *Security and Communication Networks* 8 (2015), pp. 740–750. DOI: 10.1002/sec.1021.
- [13] A. Yang, X. Tan, J. Baek, and D.S. Wong. “A New ADS-B Authentication Framework Based on Efficient Hierarchical Identity-Based Signature with Batch Verification”. In: *IEEE Transactions on Services Computing* 10.2 (2017), pp. 165–175. DOI: 10.1109/TSC.2015.2459709.

- [14] Z. Wu, A. Guo, M. Yue, and L. Liu. “An ADS-B Message Authentication Method Based on Certificateless Short Signature”. In: *IEEE Transactions on Aerospace and Electronic Systems* 56.3 (2020), pp. 1742–1753. DOI: 10.1109/TAES.2019.2933957.
- [15] P. Prakash, A. Abdelhadi, and M. Pan. *Secure Authentication of ADS-B Aircraft Communications Using Retroactive Key Publication*. 2019. DOI: 10.48550/arXiv.1907.04909. arXiv: 1907.04909 [eess.SP].
- [16] S. Rudys, J. Aleksandravicius, R. Aleksiejunas, A. Konovaltsev, C. Zhu, and L. Greda. “Physical Layer Protection for ADS-B Against Spoofing and Jamming”. In: *International Journal of Critical Infrastructure Protection* 38 (2022), p. 100555. DOI: 10.1016/j.ijcip.2022.100555.
- [17] N. Mäurer, T. Gräupl, and C. Schmitt. *L-Band Digital Aeronautical Communications System (LDACS)*. RFC 9372. Internet Engineering Task Force, Mar. 2023. DOI: 10.17487/RFC9372. URL: <https://www.rfc-editor.org/rfc/rfc9372.html>.
- [18] N. Mäurer and A. Bilzhaue. “A Cybersecurity Architecture for the L-band Digital Aeronautical Communications System (LDACS)”. In: *2018 IEEE/AIAA 37th Digital Avionics Systems Conference (DASC)*. IEEE. Sept. 2018, pp. 1–10. DOI: 10.1109/DASC.2018.8569878.
- [19] M. Tiepelt, C. Martin, and N. Mäurer. “Post-Quantum Ready Key Agreement for Aviation”. In: *IACR Communications in Cryptology* 1.1 (2024), p. 17. DOI: 10.62056/aebn2isfg.
- [20] Q. Yu. “Fully Secure and Hierarchical Identity Based Signature for Automatic Dependent Surveillance Broadcast Systems”. In: *Scientific Reports* 15.1 (2025), p. 20532. DOI: 10.1038/s41598-025-05337-x.
- [21] Radio Technical Commission for Aeronautics. *Minimum Operational Performance Standards (MOPS) for Universal Access Transceiver (UAT) Automatic Dependent Surveillance-Broadcast (ADS-B)*. RTCA DO-282C. Issued 23 June 2022. RTCA, Inc. Washington D.C. (United States), June 2022.
- [22] Federal Aviation Administration. *Universal Access Transceiver (UAT) Automatic Dependent Surveillance Broadcast (ADS-B) Equipment Operating on the Radio Frequency of 978 Megahertz (MHz)*. TSO-C154d. Federal Aviation Administration. Washington D.C. (United States), Mar. 2023. URL: <https://www.faa.gov/sites/faa.gov/files/2022-11/TSO-C154d.pdf>.
- [23] National Institute of Standards and Technology. *Post-Quantum Cryptography: PQC Standardization Process*. 2026. URL: <https://csrc.nist.gov/pqc-standardization> (visited on 09/21/2026).
- [24] P.A. Fouque, J. Hoffstein, P. Kirchner, V. Lyubashevsky, T. Pornin, T. Prest, T. Ricosset, G. Seiler, W. Whyte, and Z. Zhang. *FALCON: Fast-Fourier Lattice-Based Compact Signatures over NTRU*. Tech. rep. Specification v1.2. National Institute of Standards and Technology, 2020. URL: <https://falcon-sign.info/falcon.pdf> (visited on 09/17/2026).
- [25] National Institute of Standards and Technology. *Digital Signature Standard (DSS)*. Federal Information Processing Standards Publication FIPS 186-5. National Institute of Standards and Technology, 2023. DOI: 10.6028/NIST.FIPS.186-5.
- [26] International Civil Aviation Organization. *Manual on the Aeronautical Telecommunication Network (ATN) Using Internet Protocol Suite (IPS) Standards and Protocols*. ICAO Doc 9896-AN/469. Montréal, Canada: International Civil Aviation Organization, 2026.
- [27] E. Lenngren. *P256-Cortex-M4: P-256 ECDSA/ECDH for Cortex-M4 and Cortex-M33*. GitHub repository. Revision ecd3ec2222fc. Accessed: 6 October 2026. URL: <https://github.com/Emill/P256-Cortex-M4/blob/ecd3ec2222fc9e18b6b44c86bb7183971a2041fc/README.md>.
- [28] M. Kannwischer. *pqm4: Speed Evaluation*. GitHub repository, benchmarks.md. Accessed: 6 October 2026. URL: <https://github.com/mupq/pqm4/blob/90bfb630e53603b4e273a131cd09a025e51540a5/benchmarks.md>.

Acknowledgements

This work is partially supported by the PostQat project, funded by the European Union’s Horizon Europe research and innovation program through the SESAR Joint Undertaking under grant no. 101286435. Views and opinions expressed are those of the authors only and do not necessarily reflect those of the European Union or SESAR3 Joint Undertaking. Neither the European Union nor SESAR3 Joint Undertaking can be held responsible for them.

Author Contributions

- Marcos Cabañas Maldonado: Conceptualization, Methodology, Software, Validation, Formal analysis, Investigation, Resources, Data curation, Writing (original draft), Writing (review & editing), Visualization.
- Junzi Sun: Conceptualization, Investigation, Resources, Data curation, Writing (review & editing), Supervision, Project administration.
- Martin Strohmeier: Conceptualization, Investigation, Resources, Writing (review & editing), Supervision, Project administration.

Open Data Statement

The daytime and nighttime Mode S recordings, prepared traces, signed message workloads, numerical results, and generated figures are archived on Zenodo at <https://doi.org/10.5281/zenodo.23652076>. The deposit includes provenance metadata and checksums for verifying file integrity. Recordings and generated experimental artifacts are released under the Creative Commons Attribution 4.0 International license (CC BY 4.0).

Reproducibility Statement

The Python implementation, experiment configurations, dependency specifications, automated tests, and figure-generation scripts are provided under the MIT licence at <https://github.com/marcoscabanass/opensky-pqc-eval>. An exact software snapshot is also preserved in the Zenodo deposit. Numerical CSV and JSON outputs provide the underlying data for the simulation results and tables.

The repository README provides step-by-step commands for obtaining the matching code and data, installing dependencies, running the experiment, generating figures, and comparing results against the archived reference. Two workflows are documented: replaying the original saved signatures to reproduce the reported simulation, or repeating the complete procedure from the raw recordings, including signature generation. Fresh signatures introduce cryptographic randomness and may change Falcon signature lengths and consequently the numerical results.

Appendix 1. Supplementary Figures

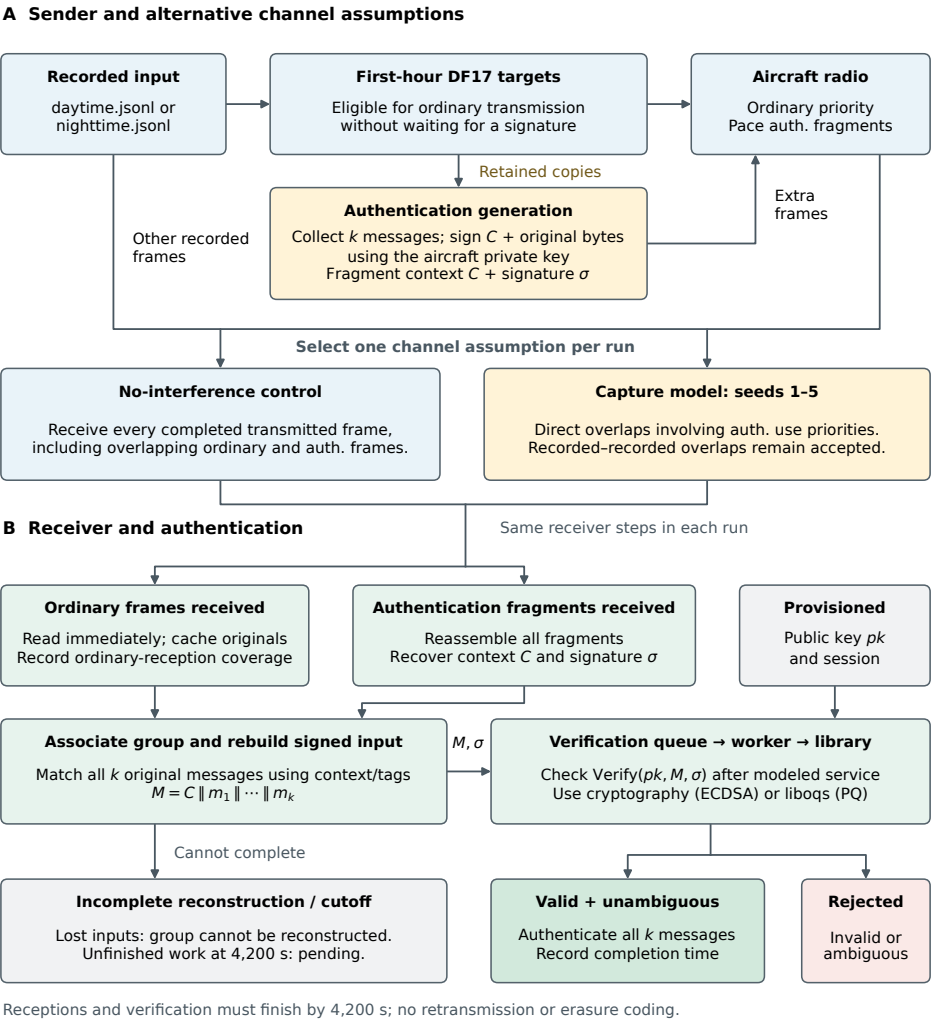


Figure 5. Experimental workflow with alternative channel assumptions (A) and a common receiver procedure (B). Authentication requires complete, unambiguous reconstruction and successful signature verification. Incomplete material and work pending at the cutoff are distinguished from rejection.