Spectrum of Engineering Sciences
ISSN (e) 3007-3138 (p) 3007-312X Volume 4, Issue 3, 2026

AERO-SC: PRIVACY-PRESERVING POST-QUANTUM SIGNCRYPTION WITH ERASURE RATCHETING FOR LIGHTWEIGHT INTERNET-OF-DRONES ACCESS

M. Asif[1], Zafar Iqbal[2], Syed Zohaib Hassan[*3], Muhammad Usman Javeed[4]

[1]*Department of Computer Science, University of Sahiwal, Sahiwal 57000, Pakistan*
[2, *3,4]*Department of Computer Science, COMSATS University Islamabad, Sahiwal Campus, Sahiwal 57000, Pakistan*

[1]asifrai60@gmail.com, [2]roy_zafar@cuisahiwal.edu.pk [*3]zohaib@cuisahiwal.edu.pk,
[4]usmanjavveed@gmail.com

DOI: https://doi.org/10.5281/zenodo.21846473

Keywords

Authentication, Internet of Drones, post-quantum cryptography, privacy, ratchet, signcryption, Tamarin.

Article History

Received: 20 January 2026
Accepted: 05 March 2026
Published: 19 March 2026

Corresponding Author: *
Syed Zohaib Hassan

Abstract

Post-quantum drone authentication is expensive if a lattice signature and key encapsulation are repeated on every telemetry packet symmetric-only sessions, however, do not recover after key exposure and usually expose a stable identity to the edge. This article presents AERO-SC, a post-quantum signcryption and erasure-ratchet protocol for Internet-of-Drones (IoD) access. A mission authority pre-authorizes one-use ML-KEM-768 receiver capsules and unlinkable window pseudonyms. A drone signs its real identity, nonce, and payload with ML-DSA-65, then encrypts the signature and identity under the encapsulated secret. A 128-bit per-window HMAC lets an edge reject unauthorised ciphertext before ground-control public-key work compromising this filter cannot forge or decrypt the inner signcryption. The ground-control station (GCS) consumes and erases the receiver secret after one accepted checkpoint, returns a ChaCha20-Poly1305 confirmation, and establishes independent HMAC-SHA-384 chain-key ratchets. Re-anchoring every $R = 256$ packets gives past-packet secrecy after current-chain exposure and healing at the next uncompromised checkpoint the symmetric ratchet alone is not claimed to heal. Scyther 1.3.0 reports all 12 secrecy, agreement, and synchronization claims Ok Tamarin 1.12.0 verifies ten executable checkpoint/ratchet lemmas, including injective acceptance and post-erasure secrecy. An executable Node.js implementation reports median 256-byte checkpoint signcryption/unsigncryption times of 11.369/3.592 ms and steady seal/open times of 0.020/0.020 ms on an Intel Xeon 8573C host. One checkpoint plus 255 telemetry packets averages 319.98 bytes per payload, 15.33× below per-packet checkpointing. A 1,350-run seeded discrete-event study is also reported with raw data and confidence intervals.

I. INTRODUCTION

Internet-of-Drones (IoD) systems connect mobile, physically exposed aircraft to ground-control stations (GCSs), edge relays, and cloud services [1, 2]. Open radio links and high mobility combine impersonation, replay, tracking, capture, and denial-of-service risks [3–6]. An authentication design must therefore answer more than "who holds a key?": what is visible to the relay, what

survives later compromise, and how much public-key work is placed on a flight computer?

Existing IoD authentication ranges from PUF/hash protocols to anonymous classical and lattice-based access control [7–10]. Recent protocols improve privacy, 6G access, swarm operation, and blockchain-assisted management [11–17]. Quantum-safe IoD work uses Ring-LWE, PUFs, dynamic identities, or standardized post-quantum components [18–22]. Nevertheless, repeating a kilobyte-scale KEM ciphertext and a 3309-byte ML-DSA-65 signature per telemetry packet is a poor default. Conversely, a static session key gives no past-message protection after exposure.

Signcryption jointly targets confidentiality and authenticity [23] secure sign-then-encrypt composition is formally studied in [24]. Lattice signcryption is advancing in adjacent IoMT settings [25], but IoD additionally needs relay-side admission, packet-loss handling, pseudonym rotation, receiver-key erasure, and a cheap steady state. These requirements motivate

$$\mathcal{G}_{\mathrm{AERO-SC}} = \{\text{PQ hidden-signature checkpoint}\} \cap \{\text{one-use receiver erasure}\} \cap \{\text{packet ratchet}\}. \quad (1)$$

The contributions are fourfold.

- A complete six-phase IoD protocol combines ML-KEM-768 and ML-DSA-65 in a sign-then-encrypt checkpoint. The civil identity and signature are ciphertext-internal only a rotating PID, capsule identifier, timing, and traffic metadata are exposed.
- Every accepted checkpoint consumes one receiver secret. Independent uplink/downlink HMAC chain keys are then erased forward per packet. This separates *past secrecy* from *healing*: current-chain exposure does not reveal old message keys, while healing occurs only at the next uncompromised PQ checkpoint.
- A per-window edge admission key covers the entire checkpoint ciphertext. The edge can discard unauthorised traffic in 0.0125 ms median before GCS KEM/DSA work edge compromise only removes this DoS filter.
- Executable cryptography, byte-exact accounting, Scyther and Tamarin models, a seeded discrete-event simulator, raw trials, assumptions, and 95% confidence intervals accompany the design. Claims are delimited from sensor truth, RF anonymity, and hardware energy.

II. RELATED WORK AND DESIGN POSITION

Mahmood *et al.* use explicit symbolic phases, adversary arguments, computation counts, communication cost, and network simulation for anonymous edge/IoD access [10–12]. AERO-SCfollows that evaluative flow but changes the security mechanism: the checkpoint uses final NIST KEM/signature standards and the data plane uses an erasure ratchet. PMAP, SAAF-IoD, D2D-MAP, REHAS, and TS-PAID target lightweight mutual authentication using PUF, chaotic, elliptic/hyperelliptic, or symmetric components [7–9, 16, 17]. Their classical security goals remain useful comparators, but they do not provide standardized post-quantum signcryption.

Mishra *et al.*, Nair *et al.*, and Chaudhary–Lee address quantum-safe IoD authorization [18–20]. pqRID focuses on anonymous Remote ID [21] Roodsari–Sarmadi study post-quantum drone-network authentication [22]. Efficient embedded PQ signatures remain implementation-sensitive [26, 27]. Table I records stated design objectives, not a universal ranking. A dash means the objective is not reported in the cited design.

TABLE I
SCOPED FUNCTIONAL POSITIONING OF AUTHENTICATION DESIGNS

Protocol	Core mechanism	Final NIST PQ pair	Hidden ID and signature	One-use GCS key erasure	Per-packet ratchet	Edge early rejection	Executable formal model
PMAP [7]	PUF/chaotic authentication	–	partial	–	–	–	reported
SAAF-IoD [8]	Chaotic map/symmetric access	–	✓	–	–	–	reported
Mahmood et al. [11]	PUF/classical access control	–	✓	–	–	–	informal
Mishra et al. [18]	Ring-LWE authorization	pre-standard	–	–	–	–	reported
pqRID [21]	PQ anonymous Remote ID	signatures	✓	–	–	–	reported
Roodsari–Sarmadi [22]	Lattice drone-network security	PQ	partial	–	–	–	reported
Xu et al. [25]	Lattice certificateless signcryption (IoMT)	PQ	✓	–	–	–	proof
AERO-SC	ML-KEM/ML-DSA + erasure ratchet	✓	✓	✓	✓	✓	Scyther/Tamarin

III. MODELS, PRIMITIVES, AND GOALS

A. Entities and Adversary

Figure 1 contains a trusted mission authority TA, drone D_i, admission edge E, and GCS G. TA enrolls long-term ML-DSA identities and may be co-located with G. Before a mission, G creates a bounded batch of one-use receiver capsules. The edge is an availability aid, not an authentication endpoint.

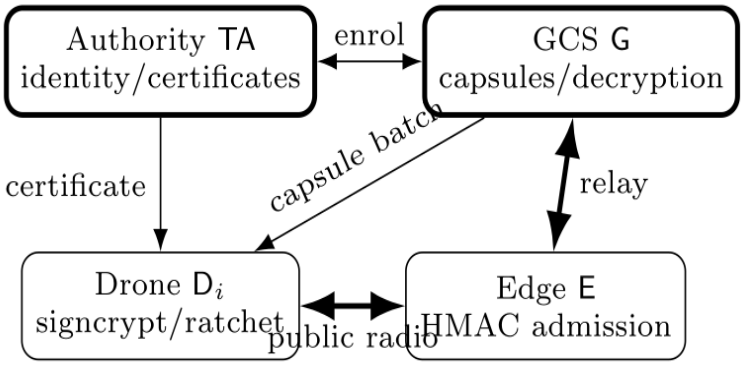

Fig. 1. The edge sees rotating metadata and ciphertext. Its admission secret is neither a signcryption nor a session key.

The adversary $\mathcal{A}$ controls public channels as in Dolev–Yao [28], records traffic indefinitely, reorders/replays/injects packets, and may compromise the edge, a drone signing key, a pre-erasure capsule key, or a current chain key at explicitly modelled times. Trust assumptions are: (A1) TA/G software is honest during an accepted checkpoint (A2) erased keys and plaintext are not recoverable from storage (A3) ML-KEM, ML-DSA, HMAC/HKDF, and AEAD implementations are correct and side-channel resistant and (A4) drone entropy is sound. GCS database compromise, malicious sensors/firmware, RF/visual tracking, jamming, traffic-analysis anonymity, and rollback-resistant erasure hardware are outside the theorem.

B. Primitives, State, and Security Goals

ML-KEM-768 supplies $(pk^K, sk^K) \leftarrow \mathsf{KeyGen}$, $(c_K, z) \leftarrow \mathsf{Encaps}(pk^K)$ and $z \leftarrow \mathsf{Decaps}(sk^K, c_K)$ [29, 30]. ML-DSA-65 supplies $(vk, sk) \leftarrow \mathsf{KeyGen}$, $\sigma \leftarrow \mathsf{Sign}_{sk}(x)$, and $\mathsf{Verify}_{vk}(x, \sigma)$ [31]. HKDF/HMAC-SHA-384, ChaCha20-Poly1305, and canonical fixed-width encodings follow [32, 33] the KEM/DEM separation is consistent with hybrid-encryption guidance [34]. Domain labels and suite identifier S appear in every derivation.

TABLE II
PRINCIPAL SYMBOLS AND PERSISTENT STATE

Symbol	Meaning
i, j, W	drone, capsule index, mission window
$RID_i, PID_{i,j}$	resolvable identity, rotating pseudonym
$(pk_{i,j}^K, sk_{i,j}^K)$	one-use GCS ML-KEM capsule pair
$a_{i,j}, tID_{i,j}$	256-bit admission key, 128-bit lookup ID
h^-, β	public header without tag, 128-bit edge tag
n_D, n_G, sid	256-bit nonces, 128-bit session ID
T, z, RK	signed transcript, KEM secret, ratchet root
$CK_l^{\uparrow}, CK_l^{\downarrow}$	directional chain keys at counter l
R, w_s	re-anchor interval, receive skip window

Goals are (G1) mutual entity authentication and injective GCS acceptance (G2) payload/signature confidentiality and outsider unforgeability (G3) pseudonym unlinkability across independently sampled windows, except timing/traffic inference (G4) replay resistance (G5) past checkpoint secrecy after receiver-key erasure (G6) past telemetry secrecy after current-chain exposure and (G7) healing at the next uncompromised PQ checkpoint. G6 is not post-compromise healing.

IV. THE AERO-SC PROTOCOL

A. Phase I–II: Setup, Enrolment, and Capsule Issue

TA creates (vk_A, sk_A) and certifies each drone ML-DSA key vk_i. The drone proves possession by signing a fresh authority challenge. G retains the binding $(RID_i, vk_i, status)$ the edge never receives RID_i.

For $j \in [0, B-1]$, G computes

$$\begin{aligned} (pk_{i,j}^K, sk_{i,j}^K) &\leftarrow \mathsf{MLKEM768.KG}, \\ PID_{i,j}, tID_{i,j} &\xleftarrow{\$} \{0,1\}^{128}, \quad a_{i,j} \xleftarrow{\$} \{0,1\}^{256}, \\ q_{i,j} &= \mathsf{enc}(i, j, W, PID_{i,j}, pk_{i,j}^K, tID_{i,j}, R, exp), \\ Cap_{i,j} &= \left(q_{i,j}, \mathsf{Sign}_{sk_A}(\mathrm{CAP} \parallel q_{i,j})\right). \end{aligned} \tag{2}$$

It sends $(Cap_{i,j}, a_{i,j})$ to D_i through the enrolment channel and pushes $(tID_{i,j}, PID_{i,j}, W, a_{i,j}, quota, unused)$ to E. G keeps $(sk_{i,j}^K, unused)$. For $B = 8$, only 19.2 kB of ML-KEM secret-key material per drone is online at G batches are replenished under policy. Precomputation preserves erasure but means compromising an unused batch compromises those future capsules.

B. Phase III: Signcrypted Checkpoint and Edge Admission

D_i verifies $Cap_{i,j}$, freshness, and unused local state. Let the 70-byte public header h^- encode $(v, type, W, PID_{i,j}, time, ctr, flags, tID_{i,j})$. The drone samples $n_D \leftarrow \{0,1\}^{256}$, obtains 256-byte payload M, and computes

$$\begin{aligned} (c_K, z) &\leftarrow \mathsf{Encaps}(pk_{i,j}^K), \\ p &= \mathsf{H}(S \parallel h^- \parallel c_K), \\ u &= RID_i \parallel fp(cert_i) \parallel n_D \parallel M, \\ T &= \mathsf{H}(p \parallel \mathsf{H}(u)), \quad \sigma_i \leftarrow \mathsf{Sign}_{sk_i}(T), \\ k_{sc} &= \mathsf{HKDF}(z, \mathsf{H}(S \parallel W), \mathrm{SC} \parallel p), \\ A &= S \parallel h^- \parallel c_K, \\ C &= \mathsf{AEAD}.Enc_{k_{sc}}(N(p), A, u \parallel \sigma_i), \\ \beta &= \mathsf{HMAC}_{a_{i,j}}(S \parallel h^- \parallel c_K \parallel C)[0{:}128]. \end{aligned} \tag{3}$$

It transmits $P_1 = (h^- \parallel \beta, c_K, C)$. The key/nonce depend only on z and public pre-transcript p, so the receiver can decrypt before reconstructing T the signature still binds the complete inner plaintext. This avoids a circular key derivation.

E looks up $tID_{i,j}$, checks window/quota/replay state, recomputes β over the *entire* ciphertext, and forwards only on success. A compromised edge can manufacture β and increase GCS load, but cannot create σ_i, recover z, or decrypt C.

C. Phase IV: GCS Acceptance and Mutual Confirmation

G atomically obtains the unused $sk_{i,j}^K$, decapsulates z, derives k_{sc}, opens C, resolves RID_i, and verifies the certificate, $PID/W/tID$, T, σ_i, timestamp, and counter. Any failure yields one generic error and no state change. On success it commits (PID, W, ctr, T) and atomically changes $unused \mapsto consumed$, erases $sk_{i,j}^K$ and z after deriving the response keys, and samples n_G. It sets

$$\begin{aligned} sid &= \mathsf{H}(T \parallel n_G)[0{:}128], \quad k_{cf} = \mathsf{HKDF}(z, \mathsf{H}(T), \mathrm{CF}), \\ C_G &= \mathsf{AEAD}.Enc_{k_{cf}}(N(T), h_G, n_G), \\ RK &= \mathsf{HKDF}(z, \mathsf{H}(T), \mathrm{ROOT} \parallel n_D \parallel n_G, 64), \end{aligned} \tag{4}$$

where $h_G = (v, type, sid, 0)$ is 22 bytes. $P_2 = (h_G, C_G)$ is 70 bytes. Only the holder of $sk_{i,j}^K$ can make a valid response D_i opens it, checks n_D through the common transcript, derives RK, and erases z and checkpoint plaintext state. Separate labels derive $(CK_0^{\uparrow}, CK_0^{\downarrow})$.

D. Phase V: Erasure Ratchet and Loss Handling

For direction $d \in \{\uparrow, \downarrow\}$ and counter l, the sender computes

$$\begin{aligned} MK_l^d &= \mathsf{HMAC}_{CK_l^d}(\mathrm{MSG} \parallel sid \parallel l)[0{:}256], \\ CK_{l+1}^d &= \mathsf{HMAC}_{CK_l^d}(\mathrm{STEP} \parallel sid \parallel l)[0{:}256], \\ C_l &= \mathsf{AEAD}.Enc_{MK_l^d}(N(sid, l), h_l, M_l), \end{aligned} \tag{5}$$

where $h_l = (v, type, sid, l, time)$ is 30 bytes. After authenticated acceptance, both sides erase MK_l^d and CK_l^d. The receiver maintains a 32-bit replay bitmap and derives at most $w_s = 32$ skipped keys, storing them until the gap closes. Counters behind the replay floor or beyond the skip window are rejected. Retransmission is byte-identical a new plaintext never reuses (sid, l).

E. Phase VI: Re-anchor, Revocation, and Recovery

At $l = R$ (default 256), after a loss threshold, or on policy command, the next unused capsule repeats Phases III–IV and replaces sid, RK, CK. A chain-key compromise at l exposes present/future symmetric traffic while the attacker remains active the next checkpoint heals only if its capsule secret and drone signing key were not compromised. Revocation deletes future GCS capsule secrets and edge records and marks RID_i denied. Recovery requires a protected re-enrolment merely changing PID does not repair a stolen signing key.

F. Normative State Machine and Failure Semantics

Table III makes the accept/reject path implementation-ready. The capsule transition is executed in one database transaction a crash before commit leaves it unused, whereas a crash after commit cannot restore sk^K. State versioning and an anti-rollback counter are therefore part of assumption A2. Five invariants govern every implementation:

$$\begin{aligned} &\text{I1:} && s^{cap}: unused \rightarrow \{consumed, revoked\} \text{ only,} \\ &\text{I2:} && (sid, l, d) \text{ authenticates at most one plaintext,} \\ &\text{I3:} && CK_l, MK_l, z, sk_{i,j}^K \text{ are erased at stated commits,} \\ &\text{I4:} && \text{no unauthenticated input advances a counter,} \\ &\text{I5:} && \text{all public failures are length- and code-uniform.} \end{aligned} \tag{6}$$

I5 limits protocol-oracle leakage but does not assert constant-time hardware. To prevent nonce reuse after power loss, the sender persists $(sid, l, \mathsf{H}(C_l))$ before transmission and either retransmits the stored bytes or abandons the session it never rebuilds C_l with changed M_l.

TABLE III
NORMATIVE PROCESSING RULES FOR ALL PROTOCOL PHASES

Phase	Actor/input	Ordered checks and computation	Committed output/state	Reject action
Setup	TA, G / policy	choose suite S create authority/drone certificates set R, w_s, B, validity and quotas	authenticated configuration version	abort before mission
Capsule issue	G / active RID_i	keygen sample PID, tID, a sign canonical Cap protect drone delivery provision edge lookup	sk^K marked unused edge quota record	discard incomplete tuple
Checkpoint	D_i / unused Cap	verify authority/expiry reserve counter encapsulate form p, T, σ, C, β; persist exact packet	pending (tID, T, z, n_D) and P_1	abandon capsule locally
Admission	E / P_1	strict parse find tID check PID, W, expiry/quota/bitmap constant-time verify β	forward exact P_1 reserve quota	generic drop no GCS work
Acceptance	G / admitted P_1	lock unused capsule decap/open validate binding/cert/signature/time/counter derive P_2, RK	atomically consume erase sk^K, z send P_2	generic error release lock
Ratchet	endpoint / (h_l, C_l)	check sid, direction, replay floor and $l \le floor + w_s$ derive/open update bitmap	erase old MK, CK persist new CK	no counter/key advance
Re-anchor/revoke	G / policy event	select next clean capsule or deny RID_i close old sid delete future records if revoked	fresh PQ root or terminal state	require protected re-enrolment

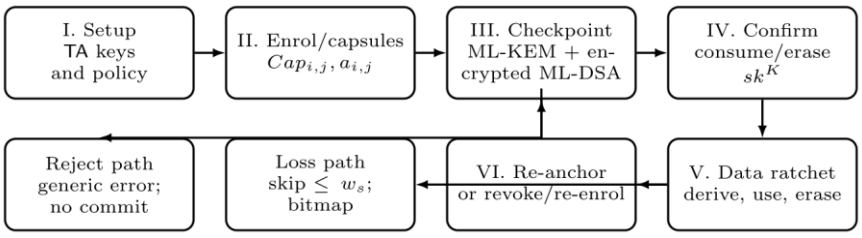

Fig. 2. Complete lifecycle. Only authenticated acceptance advances destructive state; failure and retransmission do not reuse a nonce with different plaintext.

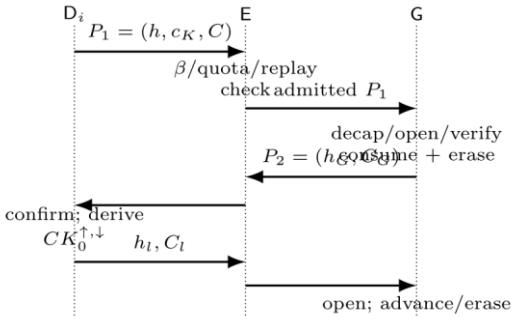

Fig. 3. Checkpoint, confirmation, and steady telemetry message flow.

V. DESIGN RATIONALE AND PROTOCOL CORRECTNESS

The outer admission tag and inner signcryption serve different trust boundaries. Placing an ML-DSA signature outside encryption would let any observer test a public key and link checkpoints. Giving the edge an AEAD or KEM secret would make relay compromise a confidentiality failure. Instead, β is deliberately disposable and per capsule: it proves only that a packet belongs to the edge's current admission set. The GCS makes the security decision from the decrypted identity, authority certificate, transcript signature, one-use capsule state, and freshness fields. Because β covers C as well as c_K, an uncompromised edge rejects ciphertext corruption without asking the GCS to decapsulate it.

TABLE IV
DESIGN DECISIONS AND AVOIDED FAILURE MODES

Alternative	Attractive property	Reason not selected
Static GCS KEM key	simple directory	later key theft opens all recorded checkpoints
Public checkpoint signature	direct edge verification	signature/key linkability; identity-binding exposure
Edge holds z or k_{sc}	strong content filter	relay compromise reveals/forges session
PQ on every payload	fresh public-key evidence	4905 B and 15.032 ms per 256-B payload here
Symmetric-only session	cheapest steady path	no independent root after chain compromise
Global admission key	minimal provisioning	one edge-key leak admits all drones/windows

Correctness proposition: if D_i, E, and G follow Phases I–V, use the same canonical capsule/header, and no packet is modified, then (i) G accepts P_1 once, (ii) D_i accepts P_2, and (iii) both derive equal directional chain keys and equal message keys for every common counter.

Argument: ML-KEM correctness gives the same z at D_i and G. Both compute identical h^-, p, A, k_{sc}, so AEAD correctness recovers the exact $u \parallel \sigma_i$ and reconstructs the same T. Certificate and ML-DSA correctness make signature verification succeed. Equal (z, T, n_D, n_G) gives equal RK in (4); labelled splitting gives equal $CK_0^{\uparrow,\downarrow}$. Induction on l in (5) gives equal (MK_l, CK_{l+1}). Capsule linearity proves the "once" condition. If packet l is lost, both states resynchronize because the receiver derives the same bounded sequence up to w_s and commits only after AEAD verification. Correctness therefore depends on canonical encoding, atomic state, and nonce persistence as well as primitive correctness.

Parameter choice is operational. w_s bounds memory and adversarial hash work during reordering R bounds the nominal time until an independent root B bounds disconnected operation and future-capsule exposure. A mission profile should jointly select (R, w_s, B) from traffic rate, maximum reordering, contact schedule, and acceptable compromise window. These values are signed in Cap so a radio attacker cannot silently weaken them.

VI. WIRE PROFILE AND IMPLEMENTATION RULES

Table V is the normative v1 serialization used by the executable benchmark. Every integer is unsigned network byte order every variable-length external object is rejected because v1 has fixed lengths. W is a random 128-bit window identifier, not wall-clock text. The 64-bit time is mission-relative microseconds under an authenticated mission epoch. The checkpoint counter is 64 bits because it also supports reconnect attempts the telemetry counter is 32 bits and forces re-anchor before wrap. $fp(cert_i) = \mathsf{H}(cert_i)[0{:}256]$ indexes the GCS certificate database but is encrypted in C.

TABLE V

BYTE-EXACT AERO-SC V1 WIRE PROFILE FOR A 256-BYTE APPLICATION PAYLOAD

Object	Offset	Length (B)	Fields	Visibility	Cryptographic binding
Checkpoint P_1	0	70	version/type (2), W (16), PID (16), time (8), counter (8), flags (4), tID (16)	public	pre-transcript p; AEAD AAD; edge HMAC
	70	16	$\beta = \mathrm{HMAC}_{a\_i,j}(S \parallel h^- \parallel c_K \parallel C)[0{:}128]$	public	complete checkpoint admission
	86	1088	ML-KEM-768 ciphertext c_K	public	p, AEAD AAD, HMAC
	1174	3661	AEAD ciphertext of 80-B fixed inner, 256-B payload, 3309-B signature; 16-B tag	opaque	ChaCha20-Poly1305 + inner ML-DSA
Confirmation P_2	0	22	version/type (2), sid (16), counter (4)	public	AEAD AAD
	22	48	encrypted n_G (32) and AEAD tag (16)	opaque	k_{cf} from checkpoint secret

Object	Offset	Length (B)	Fields	Visibility	Cryptographic binding
Telemetry P_l	0	30	version/type (2), sid (16), counter (4), time (8)	public	AEAD AAD and deterministic nonce input
	30	272	encrypted payload (256) and AEAD tag (16)	opaque	one-use MK_l^d

A. Canonical Parsing and Transcript Reconstruction

The receiver never obtains p or T as an unauthenticated extra field. It reconstructs p from the exact received (S, h^-, c_K), derives k_{sc} after decapsulation, opens C, and only then reconstructs T from p and the recovered u. This rule prevents both the circular derivation identified in naive signcryption composition and a transcript-substitution field. The encoded suite S includes protocol version, KEM, signature, hash, KDF, AEAD, field lengths, and direction. Unknown versions or non-canonical encodings fail before a capsule is locked.

The deterministic AEAD nonces $N(p)$ and $N(sid, l, d)$ are safe only under uniqueness. For checkpoints, ML-KEM encapsulation randomness changes c_K and hence p, while a capsule is consumed once. For telemetry, sid is fresh per accepted checkpoint and each (l, d) is unique. Implementations must not substitute a shorter random nonce without persisting it. Direction d is included in the domain separation even though the v1 header type already distinguishes uplink/downlink, providing defense in depth against reflection.

B. Concurrency, Quotas, and Error Surfaces

An edge record is updated by compare-and-swap on $(tID, quota, bitmap)$ so two relay workers cannot forward a nominally one-use checkpoint concurrently. This edge action is only load shedding: the GCS separately locks $cap.state$ before decapsulation and makes acceptance linearizable. A losing concurrent request receives the same public failure as an invalid signature. The GCS may cache a short negative result for duplicate ciphertext hashes, but a positive cache must never recreate an erased response key unless the exact encrypted P_2 was persisted for byte-identical retransmission.

Rate limits are layered: per tID at the edge, per source/radio association as an operational control, and per PID/RID at the GCS after authenticated resolution. The outer 128-bit HMAC is selected for a low false-accept probability and constant packet size it is not counted as 256-bit post-quantum authentication because it is not the final authenticator. The inner ML-DSA-65 signature is the accountable evidence retained with T under the mission audit policy. Retaining T, σ_i does not require retaining z, sk^K, M, or RID_i in an online session table.

C. Reproduction Boundary

The accompanying package pins library versions, includes the package lockfile, records CPU/runtime/iteration counts, and emits raw rather than only averaged crypto trials. Scyther commands save bounded XML/text and unbounded text Tamarin commands save complete proof transcripts and tool versions. The simulator reads the benchmark JSON rather than copying timing constants and emits every seed and assumption. Re-running on another host is expected to change time, not byte counts, formal lemmas, or deterministic simulation output when the benchmark input is held fixed. This separation lets reviewers distinguish cryptographic correctness, host performance, and network-model sensitivity.

VII. SECURITY ANALYSIS

A. Reduction-Oriented Argument

Let q_s, q_r, q_p bound signcryption, replay, and pseudonym observations. Under ML-KEM IND-CCA, ML-DSA EUF-CMA, HMAC PRF, and AEAD IND-CCA/INT-CTXT security, standard

game hops replace z and KDF outputs by random values, then reduce a new accepted transcript to a signature/AEAD forgery. The sign-then-encrypt order hides RID_i and σ_i and follows the generic secure-composition rationale of An–Dodis–Rabin [24]. For efficient adversary $\mathcal{A}$,

$$\begin{aligned}\mathrm{Adv}^{\mathrm{auth}}_{\mathrm{AERO-SC}}(\mathcal{A}) &\le q_s \mathrm{Adv}^{\mathrm{euf}}_{\mathrm{DSA}} + \mathrm{Adv}^{\mathrm{int}}_{\mathrm{AE}} \\ &\quad + \mathrm{Adv}_{\mathrm{PRF}} + q_r 2^{-128}, \\ \mathrm{Adv}^{\mathrm{priv}}_{\mathrm{AERO-SC}}(\mathcal{A}) &\le \mathrm{Adv}^{\mathrm{cca}}_{\mathrm{KEM}} + \mathrm{Adv}^{\mathrm{ind}}_{\mathrm{AE}} \\ &\quad + \mathrm{Adv}_{\mathrm{PRF}} + q_p^2 2^{-129}.\end{aligned} \tag{7}$$

The last privacy term is the collision probability of independent 128-bit PIDs metadata linkage remains possible. Capsule linearity and atomic commit give at most one GCS acceptance per tID. After an honest checkpoint, later disclosure of sk_i or the current chain cannot recover z from c_K once $sk^K_{i,j}$ is erased. Hence past-checkpoint confidentiality reduces to ML-KEM/AEAD security plus assumption A2. From (5), CK_{l+1} does not yield CK_l or MK_l in the PRF model, giving past-packet secrecy. It does not stop an attacker holding CK_l from following future steps only an independent KEM re-anchor heals. This distinction follows the wider ratchet-security literature [35].

Attack consequences are explicit: edge compromise bypasses admission but not signcryption pre-erasure capsule compromise reveals that checkpoint drone signing-key compromise enables impersonation until revocation current-chain compromise reveals present/future ratchet traffic until re-anchor GCS compromise defeats identity privacy rollback defeats erasure and jamming remains possible.

TABLE VI
SECURITY MECHANISM AND RESIDUAL RISK

Threat	Enforced mechanism	Residual/condition
Replay	linear capsule; sid/l bitmap	state rollback breaks guarantee
Drone spoof	encrypted ML-DSA transcript	stolen sk_i until revocation
GCS spoof	KEM-secret confirmation	pre-erasure sk^K exposure
MITM/change	AEAD AAD + inner signature	denial remains possible
Edge compromise	no z, RID, CK at edge	admission filter can be bypassed
Tracking	fresh random PID per capsule	timing, RF and location remain
Past-key search	consume/erase sk^K and CK_l	assumes real non-rollback erasure
Chain exposure	one-way symmetric step	no healing until clean re-anchor
Drone capture	per-drone keys/capsules	captured drone can lie for itself

B. Scyther and Tamarin Verification

Scyther 1.3.0 models D_i/G with the network/edge under Dolev–Yao control [36]. Its 8-run bounded and unbounded searches report all 12 Commit, Secret, Niagree, and Nisynch claims *Ok* the unbounded report gives proofs of correctness. Tamarin 1.12.0/Maude 3.2.1 uses two compositional theories [37]: the checkpoint theory consumes a linear receiver state, while the ratchet theory reveals CK_1 after packet 1. Table VII lists machine-generated summaries. The tools idealize KEM, signatures, hashes, and AEAD they do not prove lattice hardness, constant-time code, erasure hardware, or radio availability.

TABLE VII
MACHINE-CHECKED FORMAL RESULTS

Model	Result	Claims/lemmas
Scyther bounded (8 runs)	12/12 Ok	secrecy, commit, non-injective agreement/synchronization
Scyther unbounded	12/12 Ok	proof of correctness in emitted report
Tamarin checkpoint	6/6 verified	executable; auth.; injectivity; key/ID/payload secrecy
Tamarin ratchet	4/4 verified	executable; auth.; replay; past secrecy after CK_1 reveal

VIII. PERFORMANCE AND LIGHTWEIGHTNESS

A. Computation, Communication, Storage, and Energy

The executable benchmark uses @noble/post-quantum 0.6.1, @noble/ciphers 2.2.0, Node.js v24, 1000 PQ trials, 5000 symmetric trials, 200 composite trials, and 20 warm-ups on one visible Intel Xeon Platinum 8573C host. Table VIII gives medians; raw CSV includes mean, standard deviation, p95, min, and max. These timings characterize this software/host only and are not an Arduino, Raspberry Pi, flight controller, or joule measurement.

TABLE VIII
MEASURED CRYPTOGRAPHIC COST (MEDIAN)

Operation	Trials	Time (ms)
ML-KEM-768 keygen / encaps / decaps	1000	0.674 / 0.795 / 1.064
ML-DSA-65 sign / verify	1000	9.994 / 2.373
Edge HMAC admission	5000	0.01254
Checkpoint signcrypt / unsigncrypt	200	11.369 / 3.592
GCS confirmation round trip	200	0.0716
Ratchet seal / open, 256 B	5000	0.0202 / 0.0203

For one 256-byte application payload, the checkpoint is

$$L_{cp} = 86 + 1088 + (80 + 256 + 3309 + 16) = 4835 \text{ B}. \quad (8)$$

The confirmation is 70 B and telemetry is $30 + 256 + 16 = 302$ B. Thus

$$\bar{L}_R = \frac{4905 + (R-1)302}{R}, \quad \bar{L}_{256} = 319.98 \text{ B}, \quad (9)$$

and per-packet checkpointing is $4905/319.98 = 15.33\times$ larger. The corresponding host median compute is $\bar{C}_R = [15.032 + (R-1)0.04047]/R$ ms across both endpoints, giving 151.8× amortization at $R = 256$. This is not a same-platform numerical comparison against cited protocols Table I is functional, while Table X exposes AERO-SC's own operation counts and storage.

TABLE IX
RE-ANCHOR TRADEOFF FROM EXACT SIZES/HOST MEDIANS

R	B/payload	wire gain	ms/payload	compute gain
1	4905.00	1.00 ×	15.0322	1.00 ×
64	373.92	13.12 ×	0.2747	54.72 ×
128	337.96	14.51 ×	0.1576	95.39 ×

R	B/payload	wire gain	ms/payload	compute gain
256	319.98	15.33 ×	0.0990	151.79 ×
512	310.99	15.77 ×	0.0698	215.51 ×

Larger R reduces cost but lengthens compromise exposure and healing delay: at 4 packets/s, the scheduled clean re-anchor is at most $R/4$ seconds away. R must therefore be a risk policy, not a fixed claim of optimality.

TABLE X
PER-ROLE COMPUTATION, COMMUNICATION, AND STORAGE ACCOUNTING

Phase/entity	Dominant computation	Radio object	Persistent secret state	Failure/erasure rule
Issue, GCS (offline)	$B(1T_{Kg}) + B$ random admission keys	protected capsule batch	$B \times 2400$ B KEM SK	delete unused batch on revocation
Checkpoint, drone	$1T_{Ke} + 1T_S + 1T_{AE} + 1T_H$	4835 B	4032 B DSA SK + capsules	erase z, k_{sc} after confirm
Admission, edge	$1T_H$ plus lookup/quota/bitmap	forwards checkpoint	≈ 84 B/capsule	invalid tag: no GCS forwarding
Acceptance, GCS	$1T_{Kd} + 1T_V + 1T_{AD} + 1T_H$	70 B confirmation	1952 B drone VK + capsule SK	atomic consume; erase sk^K, z
Steady packet, each end	$2T_H + 1T_{AE/AD}$	302 B	two 32-B chain keys + replay state	advance only on authentic packet
R=256 amortized	one checkpoint + 255 steady packets	319.98 B/payload	$B = 8$: 19.2 kB GCS KEM SK/drone	next clean capsule heals chain exposure

For radio power P_t, bitrate b, and retry count r_x, a transparent energy model is

$$E_{tx} = P_t \frac{8Lr_x}{b}, \qquad E_{cpu} = V \sum_o I_o\, t_o. \tag{10}$$

Without measured airborne V, I_o, AERO-SCdoes not convert host timing into joules. Equation (10) and exact L, t_o allow a board-specific audit.

B. Seeded Discrete-Event Study

A reproducible Python transaction-level simulator was used rather than labelling synthetic output as OMNeT++. It reads measured crypto medians and exact sizes, models one FCFS 6-Mb/s link plus one FCFS GCS crypto server, 4 packets/s/drone, 256-byte payloads, independent PER ∈ {1,5,10}%, up to three retransmissions, 2-ms one-way propagation, uniform 0–15-slot backoff (9 μs), random initial re-anchor phase, and 250-ms timely deadline. Fleet size is 10–100 every point uses 30 deterministic seeds, 5-s warm-up, and 60-s measurement: $3 \times 5 \times 3 \times 30 = 1350$ runs.

Figure 4 shows PER=5%. Table XI reports the 100-drone point. AERO-R256 uses 20.8% mean radio occupancy and retains 99.9994% timely delivery the per-packet PQ baseline eventually transmits 99.9997% but misses the 250-ms deadline because both link and GCS queues saturate. Model radio energy uses 1.4-W transmit/0.9-W receive power and is not flight-hardware energy.

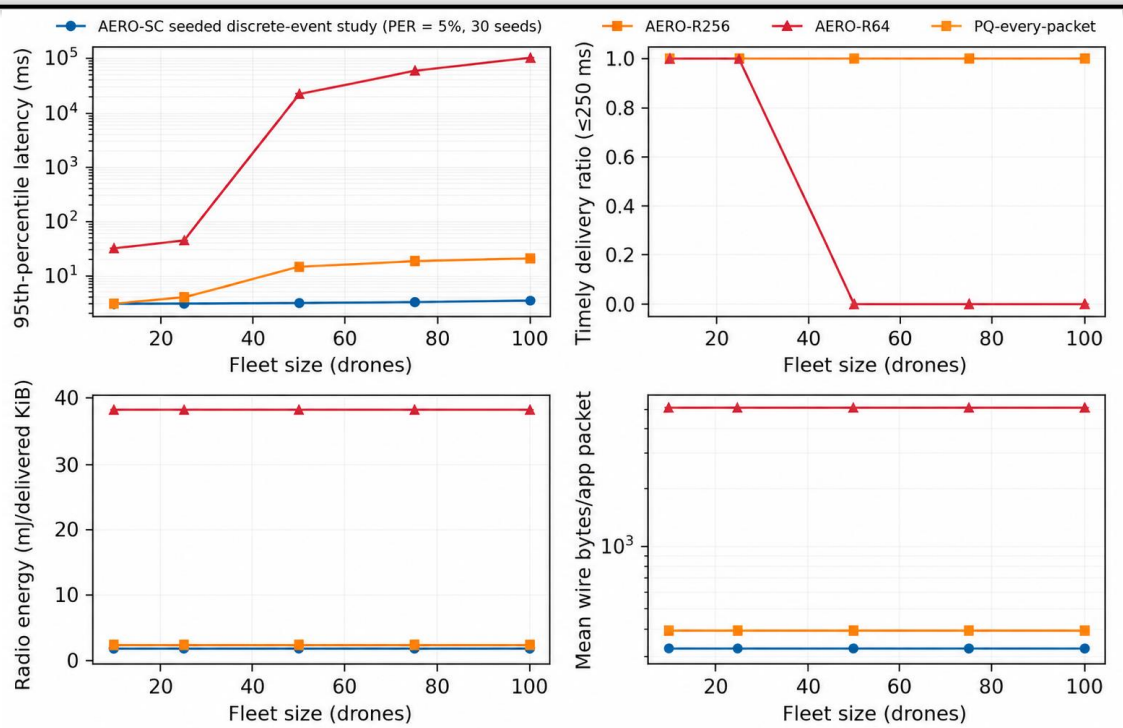

Fig. 4. Seeded transaction-level study at PER=5%; error bars are 95% confidence intervals across 30 seeds. Log scales are used for latency and wire bytes.

TABLE XI
100 DRONES, PER=5%, 30 SEEDS (MEAN ± 95% CI HALF-WIDTH)

Profile	p95 latency (ms)	timely ratio	mJ/KiB
AERO-R256	3.35 ± 0.04	0.999994 ± 0.000005	2.513 ± 0.002
AERO-R64	20.51 ± 0.15	0.999994 ± 0.000005	2.939 ± 0.005
PQ every packet	110536.5 ± 73.6	0	38.339 ± 0.017

At 100 drones, AERO-R256's p95 latency changes from 3.17 to 3.35 and 3.60 ms as PER rises from 1% to 5% and 10% timely ratios are 1.000000, 0.999994, and 0.999897. Mean model radio energy grows from 2.411 to 2.513 and 2.650 mJ/delivered KiB because of retries. The simulator's expected eventual delivery for four independent attempts is $1 - \mathrm{PER}^4$, and the raw output agrees within sampling error this sanity check does not validate a physical-layer error model. A synchronized-launch stress option and correlated fading remain future extensions.

IX. LIMITATIONS AND DEPLOYMENT GUIDANCE

AERO-SC's novelty is the IoD composition and state discipline, not a new lattice primitive. The construction inherits the security and implementation assumptions of ML-KEM, ML-DSA, HKDF/HMAC, and ChaCha20-Poly1305. Formal models use perfect primitives. Receiver erasure requires rollback-resistant storage and must be tested on the target autopilot/GCS. A precomputed capsule batch creates bounded future-key exposure smaller B narrows exposure but increases provisioning. Rotating pseudonyms hide civil identity from the edge but not location, RF fingerprint, timing, or packet size. Edge admission mitigates unauthorised public-key load but a compromised edge or authorised bot can still cause DoS. Cryptography authenticates the reporting drone, not physical sensor truth. Finally, the host benchmark and aggregate simulator must

be followed by constant-time embedded implementation, hardware-in-the-loop radio tests, fault injection, and independent cryptanalysis before safety-critical deployment.

X. CONCLUSION

AERO-SCcombines identity-hiding post-quantum signcryption, one-use receiver erasure, relay-side HMAC admission, authenticated confirmation, and bidirectional packet ratchets. It makes a deliberate cost/security split: expensive standardized PQ operations form sparse checkpoints 302-byte symmetric packets carry the steady stream. Executed Scyther/Tamarin models, byte-exact code, raw benchmarks, and a seeded network study support only the stated symbolic, host, and model claims. The design offers a stronger documented property combination than the compared objectives, but publication acceptance and real-world security require external review and airborne validation.

REFERENCES

Gharibi, M., Boutaba, R., and Waslander, S. L., "Internet of drones," *IEEE Access*, vol. 4, pp. 1148–1162, 2016. doi: 10.1109/ACCESS.2016.2537208.

Abualigah, L., Diabat, A., Sumari, P., and Gandomi, A. H., "Applications, deployments, and integration of internet of drones (IoD): A review," *IEEE Sensors Journal*, vol. 21, no. 22, pp. 25532–25546, 2021. doi: 10.1109/JSEN.2021.3114266.

Yahuza, M., Idris, M. Y. I., Ahmedy, I. B., Wahab, A. W. A., Nandy, T., Noor, N. M., and Bala, A., "Internet of drones security and privacy issues: Taxonomy and open challenges," *IEEE Access*, vol. 9, pp. 57243–57270, 2021. doi: 10.1109/ACCESS.2021.3072030.

Derhab, A., Cheikhrouhou, O., Allouch, A., Koubaa, A., Qureshi, B., Ferrag, M. A., Maglaras, L., and Khan, F. A., "Internet of drones security: Taxonomies, open issues, and future directions," *Vehicular Communications*, vol. 39, p. 100552, 2023. doi: 10.1016/j.vehcom.2022.100552.

Kumar, N. and Chaudhary, A., "Surveying cybersecurity vulnerabilities and countermeasures for enhancing UAV security," *Computer Networks*, vol. 252, p. 110695, 2024. doi: 10.1016/j.comnet.2024.110695.

Oli, A. and Mahalal, E., "UAV security: Attacks, defenses, and open challenges," *IEEE Access*, vol. 13, pp. 215606–215635, 2025. doi: 10.1109/ACCESS.2025.3647023.

Pu, C., Wall, A., Choo, K.-K. R., Ahmed, I., and Lim, S., "A lightweight and privacy-preserving mutual authentication and key agreement protocol for internet of drones environment," *IEEE Internet of Things Journal*, vol. 9, no. 12, pp. 9918–9933, 2022. doi: 10.1109/JIOT.2022.3163367.

Tanveer, M., Alasmary, H., Kumar, N., and Nayak, A., "SAAF-IoD: Secure and anonymous authentication framework for the internet of drones," *IEEE Transactions on Vehicular Technology*, vol. 73, no. 1, pp. 232–244, 2024. doi: 10.1109/TVT.2023.3306813.

Lounis, K., Ding, S. H., and Zulkernine, M., "D2D-MAP: A drone-to-drone authentication protocol using physical unclonable functions," *IEEE Transactions on Vehicular Technology*, vol. 72, no. 4, pp. 5079–5093, 2023. doi: 10.1109/TVT.2022.3224611.

Mahmood, K., Ayub, M. F., Hassan, S. Z., Ghaffar, Z., Lv, Z., and Chaudhry, S. A., "A seamless anonymous authentication protocol for mobile edge computing infrastructure," *Computer Communications*, vol. 186, pp. 12–21, 2022. doi: 10.1016/j.comcom.2022.01.005.

Mahmood, K., Ghaffar, Z., Nautiyal, L., Akram, M. W., Das, A. K., and Alenazi, M. J. F., "A privacy-preserving access control protocol for consumer flying vehicles in smart city applications," *IEEE Internet of Things Journal*, vol. 12, no. 1, pp. 978–985, 2025. doi: 10.1109/JIOT.2024.3471861.

Mahmood, K., Shamshad, S., Anisi, M. H., Brighente, A., Saleem, M. A., and Das, A. K., "A privacy-preserving access control protocol for 6G supported intelligent UAV networks," *Vehicular Communications*, vol. 54, p. 100937, 2025. doi: 10.1016/j.vehcom.2025.100937.

Wazid, M., Mittal, S., Das, A. K., Islam, S. H., Alenazi, M. J. F., and Vasilakos, A. V., "Designing secure blockchain-based authentication and key management mechanism for internet of drones applications," *Journal of Systems Architecture*, vol. 160, p. 103365, 2025. doi: 10.1016/j.sysarc.2025.103365.

Illyass, K., Baig, Z. A., and Syed, N. F., "Robust and lightweighted mutual authentication scheme for drone swarm networks," *Journal of Network and Computer Applications*, vol. 242, p. 104264, 2025. doi: 10.1016/j.jnca.2025.104264.

Dong, W., Wang, X., and Li, J., "A secure lightweight identity authentication and key agreement scheme for internet of drones," *Computer Networks*, vol. 270, p. 111503, 2025. doi: 10.1016/j.comnet.2025.111503.

Pratap, B., Singh, A., and Mehra, P. S., "REHAS: Robust and efficient hyperelliptic curve-based authentication scheme for internet of drones," *Concurrency and Computation: Practice and Experience*, vol. 37, no. 3, p. e8333, 2025. doi: 10.1002/cpe.8333.

"Intelligent Image Gallery System Using Deep Learning for Automated Fruit and Vegetable Classification", IJACET, vol. 1, no. 3, pp. 1–15, Sep. 2025, Accessed: Aug. 06, 2026. [Online]. Available: https://ijacet.com/index.php/IJACET/article/view/20

Mahrukh Jaffar, "ONTOLOGY-BASED SENTIMENT ANALYSIS FOR REAL-TIME PRODUCT REPUTATION MODELING", SES, vol. 3, no. 7, pp. 648–667, Jul. 2025.

Chaudhry, S. A., Irshad, A., Alzahrani, B. A., Alhindi, A., Shariq, M., and Das, A. K., "TS-PAID: A two-stage PUF-based lightweight authentication protocol for internet of drones," *IEEE Access*, vol. 13, pp. 1458–1469, 2025. doi: 10.1109/ACCESS.2024.3523352.

Mishra, D., Singh, M., Rewal, P., Pursharthi, K., Kumar, N., Barnawi, A., and Rathore, R. S., "Quantum-safe secure and authorized communication protocol for internet of drones," *IEEE Transactions on Vehicular Technology*, vol. 72, no. 12, pp. 16499–16507, 2023. doi: 10.1109/TVT.2023.3292169.

Nair, A. S., Thampi, S. M., and Jafeel, V., "A post-quantum secure PUF based cross-domain authentication mechanism for internet of drones," *Vehicular Communications*, vol. 47, p. 100780, 2024. doi: 10.1016/j.vehcom.2024.100780.

Muhammad Usman Javeed, Hafiza Ayesha Sadiqa, Mahrukh Jaffar, Shafqat Maria Aslam, Muhammad Khadim Hussain, and Zeeshan Raza, "A DEEP LEARNING APPROACH FOR SECURING IOT SYSTEMS WITH CNN-BASED PREDICTION OF WORST-CASE RESPONSE TIME", SES, vol. 3, no. 7, pp. 376–385, Jul. 2025.

Chaudhary, D. and Lee, C.-C., "Anonymous quantum-safe secure and authorized communication protocol under dynamic identities for internet of drones," *Computers & Electrical Engineering*, vol. 120, p. 109774, 2024. doi: 10.1016/j.compeleceng.2024.109774.

Kim, J., Lee, Y., Kang, J.-H., and Seo, S.-H., "pqRID: Compact, anonymous remote identification, and post-quantum authentication for drones," *IEEE Internet of Things Journal*, vol. 13, no. 6, pp. 10939–10953, 2026. doi: 10.1109/JIOT.2025.3650221.

Roodsari, P. D. and Sarmadi, S. B., "Post-quantum authentication and communication security for drone networks," *IEEE Transactions on Dependable and Secure Computing*, vol. 23, no. 2, pp. 3452–3463, 2026. doi: 10.1109/TDSC.2025.3636937.

Zheng, Y., "Digital signcryption or how to achieve cost(signature & encryption) much less than cost(signature) + cost(encryption)," *Advances in cryptology–CRYPTO '97*, vol. 1294, pp. 165–179, 1997. doi: 10.1007/BFb0052235.

"An Evaluation of Machine Learning Classifiers for Nominal Weather Humidity Prediction", IJACET, vol. 1, no. 4, pp. 1–21, Oct. 2025, doi: 10.64796/r3m9r804.

An, J. H., Dodis, Y., and Rabin, T., "On the security of joint signature and encryption," *Advances in cryptology–EUROCRYPT 2002*, vol. 2332, pp. 83–107, 2002. doi: 10.1007/3-540-46035-7_6.

Xu, S., Chen, X., Guo, Y., Yiu, S.-M., Gao, S., and Xiao, B., "Efficient and secure post-quantum certificateless signcryption with linkability for IoMT," *IEEE Transactions on Information Forensics and Security*, vol. 20, pp. 1119–1134, 2025. doi: 10.1109/TIFS.2024.3520007.

Al-Shareeda, M. A., Ghadban, A. A. H., Glass, A. A. H., Hadi, E. M. A., and Almaiah, M. A., "Efficient implementation of post-quantum digital signatures on raspberry pi," *Discover Applied Sciences*, vol. 7, no. 6, 2025. doi: 10.1007/s42452-025-07201-z.

AI-Powered Sentiment Analysis for Social Media Opinion Mining: A Hybrid NLP and Machine Learning Approach", IJACET, vol. 1, no. 5, pp. 1–15, Nov. 2025, doi: 10.64796/7ytc4b98.

Prajapat, S., Gautam, D., Kumar, P., Jangirala, S., Das, A. K., and Sikdar, B., "Secure lattice-based signature scheme for internet of things applications," *IEEE Access*, vol. 13, pp. 75985–75999, 2025. doi: 10.1109/ACCESS.2025.3565200.

Dolev, D. and Yao, A., "On the security of public key protocols," *IEEE Transactions on Information Theory*, vol. 29, no. 2, pp. 198–208, 1983. doi: 10.1109/TIT.1983.1056650.

National Institute of Standards and Technology, *Module-lattice-based key-encapsulation mechanism standard*, 2024. doi: 10.6028/NIST.FIPS.203.

Alagic, G., Barker, E., Chen, L., Moody, D., Robinson, A., Silberg, H., and Waller, N., *Recommendations for key-encapsulation mechanisms*, 2025. doi: 10.6028/NIST.SP.800-227.

M. U. Javeed, "Unveiling Ambivalence in Reviews: Using Sentence-BERT and K-NN for Airline Recommendations", TJ, vol. 30, no. 03, pp. 51-59, Sep. 2025.

National Institute of Standards and Technology, *Module-lattice-based digital signature standard*, 2024. doi: 10.6028/NIST.FIPS.204.

Krawczyk, H. and Eronen, P., *HMAC-based extract-and-expand key derivation function (HKDF)*, 2010. doi: 10.17487/RFC5869.

Nir, Y. and Langley, A., *ChaCha20 and Poly1305 for IETF protocols*, 2018. doi: 10.17487/RFC8439.

Z. Iqbal, S. Z. Hassan, J. Zhao, et al., "MilQAuth: An Improved and Quantum-Resistant Authentication Framework for Quantum Federated Learning in Military Communication Networks", Software: Practice and Experience, vol. 56, no. 6, pp. 709–733, 2026.

Barnes, R., Bhargavan, K., Lipp, B., and Wood, C. A., *Hybrid public key encryption*, 2022. doi: 10.17487/RFC9180.

Cohn-Gordon, K., Cremers, C., Dowling, B., Garratt, L., and Stebila, D., "A formal security analysis of the signal messaging protocol," *Journal of Cryptology*, vol. 33, pp. 1914–1983, 2020. doi: 10.1007/s00145-020-09360-1.

Cremers, C. J. F., "The scyther tool: Verification, falsification, and analysis of security protocols," *Computer aided verification*, vol. 5123, pp. 414–418, 2008. doi: 10.1007/978-3-540-70545-1_38.

Meier, S., Schmidt, B., Cremers, C., and Basin, D., "The TAMARIN prover for the symbolic analysis of security protocols," *Computer aided verification*, vol. 8044, pp. 696–701, 2013. doi: 10.1007/978-3-642-39799-8_48.

Z. Iqbal, S. Z. Hassan, J. Zhao, and S. M. Umme, "Detailed Cryptanalysis of 'Privacy-Preserving Quantum Federated Learning via Gradient Hiding'", SEET–Software Engineering for Emerging Technologies, Communications in Computer and Information Science, vol. 2725, Springer, 2026.