

PQRD: The Post-Quantum Ratchet, and its Security in a Bounded-Capture Adversary Model

Adrian Neal
Oxford Scientifica

adrian.neal@oxfordscientific.com

September 2026

Abstract. We analyse the security properties of PQRD (the Post-Quantum Ratchet, Transcript-Derived), a software-only, packet-level protocol whose working keys evolve continuously as a function of the traffic itself. The analysis uses a *bounded-capture adversary model*: the relevant resource limit is the completeness of the adversary’s intercept of the wire transcript. This places the model between Maurer’s bounded-storage setting and the channel-advantage tradition of Wyner and Maurer. Within this model, a later compromise of the ML-KEM establishment does not by itself recover the session. Reconstruction also requires a complete capture of the protected transcript, and the adversary’s residual advantage can be bounded by the guessing entropy of its sparsest capture gap over confirmed traffic. Confirmed epochs have a monotone effect: once an epoch has hardened the state, its capture requirement remains part of every subsequent state.

The model is extended to noisy capture, where an intercepted transcript may contain errors as well as gaps. Ratchet-keyed artificial noise and frequency evasion can make a reconstruction error persistent; on frequency-agile channels, a schedule-agnostic full-support recording strategy incurs a storage cost set by spectrum and mission duration. This is a sufficient completeness strategy, not a claimed lower bound on every possible interceptor architecture. Transcript binding also changes the economics of opportunistic collection: partial capture cannot simply be completed after a future break of the establishment mechanism, because any missing confirmed fold input remains missing. A single high-entropy exchange whose non-capture is established provides everlasting security with respect to ML-KEM: after that point, confidentiality of the key chain no longer depends on the computational security of the establishment mechanism. Such an exchange may be supplied out of band or by ordinary protocol traffic sent under conditions in which capture is physically precluded or detection-evident. Post-establishment authentication can also be based on the transcript-derived state. The establishment signature authenticates the initial relationship; later packets are accepted using state derived from that relationship, and concurrent use of duplicated state can be exposed at epoch cadence. The deployed construction is not information-theoretically secure; we identify the reason, and give a universal-hash variant that achieves conditional information-theoretic security in the bounded-storage sense. We conclude with a qualitative structural comparison against widely deployed authenticated-encryption schemes, including the state-rollback and state-continuity obligations introduced by the ratchet itself.

Keywords: post-quantum cryptography · key evolution · ratchet protocols · bounded-storage model · wiretap channel · harvest-now-decrypt-later · continuity authentication · attack surface

1. Introduction

Harvest-now-decrypt-later (HNDL) turns present-day collection into a long-term cryptographic liability. Traffic recorded today may need to remain secret for decades. It is therefore protected only if the cryptography guarding the recording withstands the cryptanalysis of the entire secrecy lifetime of the data, and not only the cryptanalysis of the present. The post-quantum key-establishment mechanisms standardised in 2024, in particular ML-KEM, rest on a single family of structured lattice problems with roughly a decade of concentrated public analysis behind them. The NIST standardisation process itself demonstrated how abruptly confidence in a post-quantum design can fail. A system whose recorded traffic depends solely on one such assumption carries the full longevity risk of that assumption.

PQRD retains an establishment mechanism, but is intended to prevent that mechanism from remaining a single point of failure. Its working keys are evolved by a ratchet into which the protocol folds a digest of the traffic itself, so that the key chain ceases to be a deterministic function of the initially established secret. The informal claim made in the protocol’s engineering documentation is that an adversary who later breaks the establishment mechanism, can reconstruct the key chain if, and only if, its intercept of the session was complete and gap-free.

The purpose of this paper is to put that engineering claim on a precise footing and to separate the guarantees that follow from the model from those that remain deployment assumptions. The main contributions are:

1. **The bounded-capture adversary model** (Section 4): a formal model in which the adversary’s resource bound is the completeness of its capture of the wire transcript, with residual security quantified by the conditional min-entropy of the material it lacks.
2. **The two-track construction** (Section 3): a separation of the ratchet into a gap-tolerant *key track* and a transcript-binding *binding track*, reconciled by confirmed epochs. The separation resolves the tension between loss tolerance and traffic binding, and yields a *monotone hardening* guarantee (Lemma 1).
3. **Security theorems** (Section 5): a bound on the advantage of a KEM-breaking adversary in terms of its sparsest confirmed capture gap (Theorem 1); everlasting security with respect to ML-KEM given one out-of-band entropy injection (Theorem 2); and a proof that the epoch-commit mechanism introduces no leakage class beyond one already present (Proposition 3).
4. **The relation to information-theoretic security** (Section 6): a precise account of why the deployed construction is not ITS, why the underlying claim is nonetheless of the same conditional character as bounded-storage ITS, and a universal-hash variant that achieves conditional ITS under an explicit adversary-erasure assumption.
5. **Manufactured channel advantage** (Section 7): a generalisation of the model to *noisy capture*, in which the adversary’s copy of the transcript carries errors as well as gaps, together with two ratchet-keyed mechanisms, artificial noise and radio frequency evasion, under which a reconstruction error can persist, together with a quantified cost for the schedule-agnostic strategy of recording the full possible hop band; and a proof that a confirmed capture gap prevents later reconstruction past that hardening point under the stated entropy assumptions.
6. **Continuity authentication** (Section 7.5): a proof that, after an authentic establishment, later compromise of the establishment signature scheme does not by itself permit intrusion into the existing relationship. Post-establishment packets are authenticated from transcript-derived state, and concurrent use of duplicated endpoint state produces fork evidence at epoch cadence.

7. **A qualitative structural comparison** (Section 8): an inventory of the principal mathematical and misuse interfaces in AES-256-GCM, AES-256-CTR with HMAC-SHA-256, ChaCha20-Poly1305 and the PQRD data path, explicitly including PQRD’s state-continuity obligations and avoiding a numerical security ranking.

Throughout, ω^- and ω^+ denote the backward and forward compromise bounds (the *bounded compromise horizon*), and the term *resistance to automated cryptanalysis* denotes the property of presenting minimal exploitable structure to machine-assisted analysis.

2. Related Work

Bounded storage. Maurer’s bounded-storage model (BSM) achieves information-theoretic key agreement against an adversary whose storage is bounded below the size of a public randomiser. Cachin and Maurer, and later Aumann, Ding and Rabin, developed *everlasting security*: secrecy that holds even if the adversary’s computational limits fall away entirely after the protocol run, provided the storage bound held during it. Its information-theoretic character comes from the combination of an enforced resource bound, a provable entropy gap, and unconditional extraction. The randomiser is sized so that the storage restriction is a design assumption; the residual uncertainty follows from a counting argument; and universal hashing, under the leftover hash lemma, performs the extraction. These three properties provide the reference point for the comparison with PQRD below.

Channel advantage. Wyner’s wiretap channel and Maurer’s secret-key agreement from correlated randomness establish that genuine information-theoretic secrecy is achievable whenever the legitimate receiver’s channel dominates the eavesdropper’s channel. In Maurer’s satellite scenario this holds even when both channels are noisy and neither party controls the noise. The assumption concerns the adversary’s channel rather than its computation or storage. We show below that PQRD’s capture requirement is a channel-dominance condition, which places the construction in this lineage.

Bounded retrieval. The bounded-retrieval model (Di Crescenzo, Lipton and Walfish; Dziembowski; Alwen, Dodis and Wichs) bounds the volume of data an adversary can exfiltrate from a compromised machine whose secret storage is made deliberately large. It is the nearest existing relative of the model introduced here, and the distinction is exact: bounded retrieval limits what leaves the defender’s storage, whereas bounded capture limits what the adversary collects from the channel. The bounded resource is an intercept of a transcript in transit rather than a retrieval from a store at rest, and the defender’s corresponding lever is traffic and channel conditions rather than storage size.

Computational ratchets. The Signal double ratchet provides forward secrecy and post-compromise security by combining a Diffie–Hellman ratchet with symmetric key derivation. PQRD addresses channels on which repeated asymmetric exchanges may be unavailable or undesirable, including lossy or one-way tactical links and long-lived managed infrastructure. Its key evolution is bound to the transcript, and its post-establishment analysis includes later failure of the establishment mechanism, which is outside the threat model of the double ratchet. Authentication is also used differently. The double ratchet anchors new sessions to long-term identity keys. PQRD uses the establishment signature when the relationship is created; Section 7.5 analyses subsequent authentication from transcript-derived state and the effect of a later break of the signature scheme.

Forward-secure storage and intrusion resilience. Dziembowski’s forward-secure storage and the broader intrusion-resilience literature share PQRD’s assumption that devices are captured and algorithms known. PQRD’s contribution relative to this line is the use of the transcript as the

binding resource, which is naturally available on a communications link and costs no dedicated bandwidth beyond periodic commits.

3. The Construction

3.1 Setting and notation

Two endpoints communicate in authenticated packets over an unreliable channel. The construction is intended for both contested physical links and long-lived managed infrastructure. In the *contested* setting, the motivating examples are expeditionary and tactical links on which an adversary may jam, degrade or intercept traffic and packet loss is normal. The *infrastructure* setting covers wired or managed links carrying supervisory, metering, financial or telemetry traffic over long service lives; losses may be less frequent, while the secrecy lifetime of recorded traffic can extend for decades. The protocol mechanism is unchanged between these settings. Some terminology below is drawn from the contested case: “mission” corresponds to “session” in an infrastructure deployment, and “pre-mission preparation” to provisioning.

Establishment produces an initial secret S_0 from ML-KEM-1024 shared-secret material authenticated by ML-DSA-87. FIPS 203 specifies a 256-bit shared secret for each ML-KEM encapsulation, including ML-KEM-1024. A deployment profile may combine more than one independent encapsulation through an approved combiner or KDF when additional independent key material or redundancy is required; doing so does not multiply the NIST security category of ML-KEM-1024 or constitute a claim of 512- or 768-bit ML-KEM hardness. H denotes SHA-512, modelled where stated as a random oracle. Each packet p_i denotes the complete authenticated wire unit as transmitted: header, sequence number, ciphertext and MAC tag. $H_\infty(X \mid Y)$ denotes conditional min-entropy. ω^- and ω^+ denote the backward and forward compromise bounds.

3.2 Two tracks

The ratchet is separated into two components with distinct obligations.

The **key track** evolves deterministically from the current *hardened state* as a function of sequence position: given hardened state h_k and sequence number i , both endpoints derive per-packet encryption and authentication keys without reference to the packet contents of the current epoch. The key track is therefore gap-tolerant by construction. A receiver that missed any subset of packets derives the keys for the next packet it receives from (h_k, i) alone, with no recovery traffic. The key track carries all synchronisation; it contributes no HNDL protection beyond that of the establishment mechanism, and none is claimed for it.

The **binding track** is a transcript accumulator. Each endpoint folds into its accumulator every authenticated packet it actually processes, in a keyed fold applied strictly after MAC verification:

$$a_i \leftarrow H(a_{i-1} \parallel p_i)$$

Byte-identical retransmissions (replicas) carrying the same sequence number are folded exactly once. Rejected packets are never folded.

Epoch commitment. Every N packets or T seconds, each endpoint derives a dedicated commit key from current key-track material and transmits the epoch number together with a keyed equality commitment

$$c_e = \text{MAC}_{K_e^{\text{commit}}}(\text{epoch} \parallel e \parallel a_e \parallel \text{context}).$$

The accumulator value a_e itself is never transmitted. A peer computes the expected commitment from its own local accumulator and confirms the epoch only if the commitments agree in both directions. Each endpoint then folds its local accumulator into the hardened state,

$$h_{k+1} \leftarrow H(h_k \parallel a_e) .$$

A lost or mismatched commit defers hardening: the key track continues from the last hardened state, and a later clean epoch can resume the binding process. The commit therefore tests equality without publishing the fold input that a future reconstruction adversary would need to cross a capture gap.

3.3 The fold input is the wire transcript

The fold input is the authenticated ciphertext. The reconstruction adversary considered here breaks the establishment mechanism at a later date and replays the chain until it reaches a capture gap. At that point it knows the pre-gap chain state and the keystream for the missed packet. From its perspective, therefore, the ciphertext and plaintext of the gap are related by a known bijection and have the same guessing entropy.

Using the wire transcript also fixes the representation being folded, so implementations do not have to agree on a reconstructed plaintext encoding. The MAC tag is included in the fold and therefore becomes part of the key chain’s history. It also lets the adversary model in Section 4 be expressed directly in terms of possession of wire bytes. The corresponding engineering constraint is that any FEC, whitening or other radio-layer transformation must be removed below the fold; the fold itself sits at the protocol layer.

3.4 Entropy injection, verified gaps and one-way operation

The construction admits explicit entropy injection: a value r exchanged out of band is folded into the hardened state in the same position as an epoch accumulator. The intended exchange channel is one on which capture is physically precluded. In a contested deployment this can be a direct physical link used during pre-mission preparation; in an infrastructure deployment it can be the bench or staging connection used during commissioning or service. If a link has no return channel and epochs cannot be confirmed, the binding track idles and the key track continues from the state hardened by the injection. This covers, for example, telemetry through a data diode and an airborne one-way downlink. Section 5 gives the resulting security bound.

The same security condition can be obtained without a separate out-of-band interface. Because every authenticated packet enters the binding track, an ordinary packet can supply the missing entropy when its non-capture is established. Fresh locally generated randomness of a designed length may be sent while the link is physically controlled or while interception would be evident, for example during a controlled pre-mission window or across a commissioning bench. This operating case, called *verified-gap* mode, requires no additional packet type and is analysed in Section 5.

Some deployment profiles prohibit pre-provisioned or pre-placed secret material, whether by regulation (for example, current US Department requirements for software-based encryption) or by operator policy in infrastructure procurement. In those profiles the injection interface can be disabled. The rest of the construction is unchanged, and results that do not use injection continue to apply; verified-gap mode remains available under the conditions stated in Section 5.

3.5 Composition from standardised primitives

PQRD introduces no bespoke cryptographic primitive, but its composition and state machine are protocol-specific and are themselves security-relevant. The building blocks are selected from standardised primitive families; that does not make the composition a standardised protocol or remove the need for composition-specific analysis, implementation validation and state-management assurance.

Component	Role in the construction	Standardised object
Key establishment	produces S_0 (Section 3.1)	ML-KEM-1024, FIPS 203
Establishment authentication	signs the establishment transcript	ML-DSA-87, FIPS 204
Hash primitive H	transcript fold and the idealised random-oracle model	SHA-512, FIPS 180-4
Key derivation and generator profile	derives labelled key-track, keystream and commit material from secret state	SHA-512-based PRF/KDF; SP 800-108 Rev. 1 HMAC-SHA-512 is an approved derivation profile
Per-packet and commit MAC	keyed from separately labelled key-track material	HMAC-SHA-512 under FIPS 198-1 or successor NIST HMAC guidance
Extraction variant (Section 6)	non-deployed ITS boundary case	two-universal hashing; a literature construction, not a standardised object

The proofs in Sections 5 and 7 idealise H as a random oracle. A concrete implementation necessarily replaces that idealisation with a specified hash/PRF/KDF profile. SHA-512 supplies the underlying standardised hash primitive, while labelled secret-key derivations should use an approved keyed construction where compliance requires it; SP 800-108 Rev. 1 provides HMAC- and KMAC-based KDF families. Primitive validation does not validate the PQRD composition: domain separation, state erasure, rollback resistance, commit handling and transcript canonicalisation remain protocol obligations.

Standardisation supplies scrutiny but does not guarantee indefinite security. PQRD therefore states explicitly where later results continue to depend on ML-KEM or ML-DSA and where an independently missing entropy input removes those mechanisms from the reconstruction argument. The two-universal extraction variant in Section 6 remains a non-deployed boundary construction, not a claim that the deployed SHA-512 profile is information-theoretic.

4. The Bounded-Capture Adversary Model

Definition 1 (Transcript and capture set). Let $\mathcal{T} = (p_1, \dots, p_n)$ be the ordered wire transcript of a session. The adversary’s *capture set* $C \subseteq \{1, \dots, n\}$ is the set of indices of packets it possesses in full. Its *gap set* is $G = \{1, \dots, n\} \setminus C$.

Definition 2 (Bounded-capture adversary). A *bounded-capture adversary* $\mathcal{A}$ is given the

complete protocol specification; the public establishment transcript; the packets $\{p_i : i \in C\}$; unbounded computation with respect to the establishment mechanism, so that it may recover S_0 ; and oracle access to the MAC verification behaviour implied by its captured material. It is bounded only in that $G \neq \emptyset$ with respect to the traffic it attacks.

Definition 3 (Gap entropy). The *gap entropy* of epoch e is $\gamma_e = H_\infty(\{p_i : i \in G \cap e\} \mid V)$, where V denotes the adversary’s entire remaining view. The *session gap entropy* over confirmed epochs E is $\gamma = \min_{e \in E} \gamma_e$, the minimum taken over epochs with $G \cap e \neq \emptyset$, since the adversary attacks the sparsest gap.

The model has three important boundaries. Its capture constraint is empirical: a co-located interceptor recording at the antenna, or an adversary operating the transport network, may achieve $C = \{1, \dots, n\}$. Whether the model is appropriate for a deployment therefore depends on the adversary’s collection posture, as discussed in Section 6. Gap entropy is likewise traffic-dependent. Missing a nearly deterministic packet such as a periodic heartbeat contributes little, and the bounds below retain that dependence explicitly. Finally, the binding track contains only packets processed by the receiver and epochs it confirmed. The relevant capture condition is consequently that the adversary obtain at least what the receiver obtained, which is a channel-dominance condition.

Definition 5 (Verified gap). A *verified gap* is a subset $G_v \subseteq G$ whose membership in the gap set is established by observation rather than assumption: either capture of the corresponding packets was physically precluded by the channel conditions under which they were sent, or the channel is *detection-evident*, meaning that any capture attempt produces an observable event with evasion probability at most ε_{det} , and no such event was observed before the material was relied upon. The *verified gap entropy* γ_v is the conditional min-entropy of the content of G_v given the adversary’s remaining view.

Definition 4 (Bounded compromise horizon). A protocol has compromise bounds (ω^-, ω^+) if disclosure of the complete endpoint state at time t exposes plaintext only within the window $(t - \omega^-, t + \omega^+)$, where ω^+ terminates at the next hardening event whose inputs the adversary lacks.

5. Security Analysis

Throughout this section H is modelled as a random oracle and q bounds the adversary’s oracle queries. We separate failure to reconstruct the ratchet state from direct cryptanalysis of the traffic protection. Adv_{TP} denotes the adversary’s independent confidentiality advantage against the traffic-protection primitive when the relevant working key has not been reconstructed, and Adv_{MAC} denotes the corresponding independent post-establishment MAC-forgery advantage. Proof sketches are given with the statements; the omitted detail consists of the corresponding oracle and conditioning expansions.

Lemma 1 (Monotone hardening). Let epochs $e_1 < e_2 < \dots$ be confirmed in order. For any j , reading any traffic keyed after the hardening of e_j requires reconstructing h_j , which requires the accumulator values $a_1, \dots, a_j$ in full. The capture requirement is therefore monotone: each confirmed epoch permanently raises, and never lowers, the completeness of capture required for all subsequent traffic.

Sketch. We have $h_j = H(H(\dots H(h_0 \parallel a_1) \dots) \parallel a_j)$. In the random-oracle model, evaluating the chain requires each a_i as an explicit query input, and each a_i is itself a chained digest requiring every folded packet of epoch i . No later event removes an earlier fold. ■

Theorem 1 (Post-establishment-break reconstruction bound). Let $\mathcal{A}$ be a bounded-capture adversary with session gap entropy γ over confirmed epochs, attacking a packet keyed after the hardening of the gapped epoch. Its advantage in reconstructing the required post-hardening ratchet state is bounded by

$$\text{Adv}_{\text{rec}}(\mathcal{A}) \leq q \cdot 2^{-\gamma} + \varepsilon_H.$$

Consequently its confidentiality advantage through either state reconstruction or an independent attack on the traffic-protection primitive is at most

$$\text{Adv}_{\text{conf}}(\mathcal{A}) \leq q \cdot 2^{-\gamma} + \varepsilon_H + \text{Adv}_{\text{TP}}.$$

Here ε_H collects negligible random-oracle terms. The theorem does not claim that the capture gap is the only conceivable cryptanalytic route to plaintext.

Sketch. By Lemma 1, $\mathcal{A}$ must produce the accumulator of the gapped epoch. Given everything $\mathcal{A}$ holds, including S_0 and hence the pre-gap chain state and keystream, the missing fold inputs retain min-entropy γ by definition. Each candidate for the missing material determines one accumulator query, and a candidate can be confirmed only through MAC verification, so each query identifies the correct value with probability at most $2^{-\gamma}$. The union bound over q queries gives the claim. ■

The strength of Theorem 1 depends directly on the traffic in the gap. A missed high-entropy payload may give a substantial bound, while a single predictable heartbeat may give very little. Payload padding, commit cadence and epoch sizing therefore affect the quantified guarantee and are part of the deployment assumptions.

Theorem 2 (Everlasting security with respect to the establishment mechanism). Suppose a value r with $H_\infty(r \mid \mathcal{A}'\text{'s view}) \geq \kappa$ is injected out of band into the hardened state at time t_0 . Then for all traffic keyed after t_0 , the bound of Theorem 1 holds with γ replaced by κ , independently of any computational assumption about the establishment mechanism. In particular, it holds against an adversary that recovers S_0 in full and captured the entire wire transcript.

Sketch. The injected r never crosses the intercepted channel, so the adversary's view is independent of it up to its designed entropy κ . Reconstruction of any post- t_0 hardened state requires r as an oracle input, and the argument of Theorem 1 applies with the gap replaced by the injection. ■

Theorem 2 removes the ordinary traffic-capture assumption from the state-reconstruction bound for traffic after the injection. A single early exchange in a controlled environment is sufficient to break the reconstruction path even if the adversary has an otherwise complete recording of the session. This is an everlasting-security argument in the bounded-storage tradition, but the entropy source is deliberately introduced rather than inferred from an imperfect collection process. On a one-way mission, the same condition can be met by ordinary protocol traffic sent over a direct bench link before deployment. Corollary 2.1 then applies without use of a separate injection interface.

Corollary 2.1 (Verified-gap hardening). Let a confirmed epoch contain a verified gap of entropy γ_v . Then for all traffic keyed after the hardening of that epoch, $\text{Adv}_{\text{rec}}(\mathcal{A}) \leq q \cdot 2^{-\gamma_v} + \varepsilon_H$ if capture was physically precluded, and $\text{Adv}_{\text{rec}}(\mathcal{A}) \leq q \cdot 2^{-\gamma_v} + \varepsilon_H + \varepsilon_{\text{det}}$, conditioned on no detection event, if the channel is detection-evident. In particular, if doctrine places a packet of fresh uniform randomness of length κ in the verified gap, the establishment-independent reconstruction guarantee of Theorem 2 is obtained using only in-protocol traffic. Confidentiality retains the additive Adv_{TP} term stated in Theorem 1.

Sketch. Immediate from Theorem 1 with the gap established by observation: the capture assumption

of the bounded-capture model is discharged for G_v rather than assumed, and in the detection-evident case the event that the adversary captured the material without observation has probability at most ε_{det} . ■

The detection-evident case requires the alarm to precede reliance on the new hardened state. If detection can arrive only after traffic has been keyed from that state, the result is attributable compromise rather than confidentiality for the affected traffic. The value of γ_v also comes from the payload itself: a protected but low-entropy packet contributes only that limited entropy. Corollary 2.1 therefore assumes fresh randomness of a designed length, not merely a protected transmission.

Remark (the ceiling). A verified exchange of κ bits cannot provide unconditional protection for more than κ bits of subsequent plaintext; Shannon’s bound applies to every finite-key construction. Beyond that amount, Theorem 2 and Corollary 2.1 remove dependence on the establishment mechanism, while confidentiality still rests computationally on the symmetric primitive. Unconditional protection of an unbounded stream would require fresh entropy in proportion to the traffic, as in the pre-provisioned configurations of Section 3.4.

Proposition 3 (Non-revealing epoch commits add only an equality test). The epoch commit of Section 3.2 transmits no accumulator value. Under the PRF/unforgeability assumption of the commit MAC, a passive recording of the commit exposes only a keyed equality test for a candidate local accumulator. After a later establishment break gives the adversary the pre-gap commit key, the recorded tag can verify a guessed gap fill, but it does not reveal the correct accumulator or reduce the candidate space below the entropy already accounted for in Theorem 1. The same class of candidate verification is available from post-hardening packet authentication.

Sketch. A candidate gap fill determines a candidate accumulator a_e . With the recovered pre-gap commit key, the adversary can compute the expected tag and compare it with the recorded commitment. This is an oracle for equality of the complete candidate; it supplies no partial information about a wrong candidate under the MAC assumption. A correct candidate also determines the post-hardening state and hence the packet-MAC keys, so an equivalent equality test is available from captured post-hardening authentication tags. ■

Proposition 4 (Compromise horizons). Disclosure of complete endpoint state at time t exposes traffic backward only to the preceding hardening event whose accumulator inputs are not recoverable from the disclosed state (bound ω^- , enforced by erasure of pre-hardening state), and forward only to the next hardening event whose inputs the adversary does not capture or, in the injected mode, does not hold (bound ω^+). Both horizons are configuration-controlled through epoch cadence and injection schedule.

6. Relation to Information-Theoretic Security

The comparison with information-theoretic security is best made by separating the capture claim from the extraction mechanism. Requiring a complete recording of every prior confirmed epoch resembles a bounded-storage assumption, but the deployed construction does not meet the bounded-storage standard of information-theoretic security.

Limits of the deployed construction. In a bounded-storage scheme, the storage restriction can be set as a design parameter by making the public randomiser larger than the assumed storage capability. PQRD has no equivalent enforcement mechanism for capture: a co-located interceptor may, in principle, record the whole channel. Its entropy gap is also supplied by the traffic and the

collection process rather than by a counting argument over deliberately sized random material. Finally, the deployed fold uses SHA-512 and is analysed in the random-oracle model, so its extraction step remains computational.

There is nevertheless a precise parallel. Bounded-storage security is unconditional with respect to computation only after accepting a resource assumption about the adversary. Theorem 1 has the same conditional form, with incomplete capture taking the place of limited storage. Its exact capture condition is also a channel condition: the adversary must obtain at least every packet that contributed to each confirmed receiver state. This connects the model directly to the Wyner–Maurer line of work on secrecy from a receiver advantage. Corollary 2.1 strengthens the operational basis for this assumption when a gap can be verified by observation, because the relevant non-capture is then established for the packet concerned. On contested links, receiver loss and interceptor loss also have different consequences: receiver loss merely postpones hardening, whereas a missing interceptor input cannot later be recovered from the transcript.

An information-theoretic extraction variant. Consider replacing the fold of confirmed accumulator material with two-universal hashing, $h_{k+1} = f(h_k, \text{Ext}(a_e\text{-material}))$, where Ext is a two-universal family applied to the concatenated confirmed-epoch material. Assume that each transmitted packet independently fails to enter the adversary’s capture set with probability at least δ , and that the epochs have a designed minimum entropy density. Under this explicit *adversary-erasure assumption*, the leftover hash lemma yields keys statistically close to uniform even against a computationally unbounded adversary. The result is conditional information-theoretic security in the usual bounded-resource sense.

This variant is included to locate the boundary of the construction, not as a deployment recommendation. The SHA-512 random-oracle instantiation is simpler and faster, and uses a conservative deployed primitive. The important point is that the remaining computational dependence comes from the selected extraction mechanism; it is not forced by the ratchet architecture itself.

For the deployed protocol, the resulting claim is therefore narrower than unconditional ITS. Theorem 1 gives a quantified capture-dependent bound; Theorem 2 and Corollary 2.1 remove dependence on ML-KEM after an established high-entropy exchange; and the variant above shows how the same ratchet can be paired with information-theoretic extraction under an explicit channel assumption. A complete intercept with no such exchange remains outside those guarantees.

7. Manufactured Channel Advantage: the Noisy-Capture Model

Section 4 treats capture at packet granularity: a packet is either present in the adversary’s transcript or absent. A physical interception system usually produces something less clean. It demodulates under a link budget and stores a reconstruction that may retain residual errors even after its best current or future processing of the recorded signal. The noisy-capture model below includes those errors. It also lets us examine two mechanisms that deliberately worsen the interceptor’s reconstruction while leaving the legitimate receiver’s protocol state intact. Neither mechanism helps against an adversary that already possesses an exact post-demodulation copy; that boundary is considered in Section 7.4.

7.1 The noisy-capture adversary

Definition 6 (Noisy-capture adversary). A *noisy-capture adversary* is a bounded-capture adversary (Definition 2) whose possession of the transcript is mediated by an error process: for each

i in its capture set C it holds $\tilde{p}_i = p_i \oplus e_i$ for an error pattern e_i , and for $i \in G$ it holds nothing. The *effective gap entropy* of epoch e is $\hat{\gamma}_e = H_\infty(\{p_i : i \in e\} \mid \tilde{V})$, where $\tilde{V}$ is the adversary's entire view including its corrupted copies. The bounded-capture model is the special case $e_i = 0$ for all $i \in C$.

Only errors in material the reconstruction adversary cannot recompute contribute to $\hat{\gamma}_e$. The adversary considered here knows S_0 and therefore the keystream, so canonical protocol fields and predictable payload can often be reconstructed from context. Errors in fresh locally generated random fields cannot: there is no side information from which to repair them.

The ratchet also removes the locality normally exploited by error correction. A wrong bit in any folded packet changes a_e , then h_{k+1} , and hence every later key. Nor does the verifier provide a useful measure of proximity to the right answer. Proposition 3 leaves only the MAC result, which accepts when the whole candidate state is correct. The interceptor therefore has to resolve the joint error pattern for the epoch. The legitimate receiver is in a different position because transport FEC is applied locally below the fold, before authenticated packets enter the binding track.

Theorem 3 (Noisy-capture bound). Let doctrine place designated fields of fresh, locally generated uniform randomness totalling m bits in the packets of confirmed epoch e , and let a noisy-capture adversary's residual errors strike those field bits as independent Bernoulli(δ) events, independent of its remaining view. Then

$$\hat{\gamma}_e \geq m \log_2 \frac{1}{1-\delta} \approx 1.44 m \delta \quad (\delta \text{ small}),$$

and the bound of Theorem 1 holds with $\hat{\gamma}_e$ in place of γ_e for all traffic keyed after the hardening of e .

Sketch. Recovering the fold inputs of e from the corrupted copies entails identifying the error pattern restricted to the designated fields; the pattern is distributed Bernoulli(δ) ^{m} and independent of the remaining view by hypothesis, so its most probable value has probability $(1 - \delta)^m$ and its conditional min-entropy is $m \log_2(1 - \delta)^{-1}$. Guessing the true packets given the corrupted copies is at least as hard as guessing the pattern, whence the bound on $\hat{\gamma}_e$; Theorem 1's oracle-counting argument uses only the entropy hypothesis and is otherwise unchanged. ■

The independence assumption is part of the channel model. Correlated burst errors reduce the bound toward the entropy of the burst process, and any link-budget estimate of δ must allow conservatively for the adversary's processing gain, including future processing of stored raw signal. Even a residual error rate that is operationally small can matter substantially to reconstruction. For example, a rate of 10^{-4} across 10^6 designed field bits in an epoch gives $\hat{\gamma}_e \approx 144$ bits, despite an intercepted copy that would ordinarily be described as nearly complete.

7.2 Ratchet-keyed artificial noise

The defender need not wait for the channel to supply the error process. Let the endpoints derive, from current key-track material under a dedicated derivation label, a per-epoch *noise key*, and let the transmitter superimpose on its emission a pseudorandom artificial-noise waveform generated from that key. The legitimate receiver, holding the chain, regenerates and cancels the waveform before demodulation; its residual error rate is unchanged, and the fold input (the post-verification wire bytes) is untouched, preserving the layering of Section 3.3. An interceptor without the chain state demodulates beneath an elevated noise floor engineered, through ordinary link-budget design, to leave a residual rate $\delta' > 0$ in its stored copy. Unlike thermal noise, however, this component is reproducible only with the noise key. Additional processing of the recording does not reveal that

key; it is derived from the hardened state being protected.

The protocol proof does not establish that a real interceptor will have a particular residual rate δ' . That is a physical-layer assumption which must be supported by link-budget analysis, receiver models and, for a deployment claim, measurement against the relevant class of interceptor. The cryptographic result below is conditional on the residual error model once established.

Corollary 3.1 (Single-slip permanence). Run the protocol under ratchet-keyed noise with interceptor residual rate δ' when uncanceled, and doctrine placing m designed field bits per epoch. If a reconstruction adversary's candidate for the hardened state at epoch e is incorrect, whether through a gap, an unresolved error or a wrong guess, then its stored copies of every subsequent epoch are effectively corrupted at rate at least δ' on the designated fields, so $\hat{\gamma}_{e'} \geq 1.44 m \delta'$ for all $e' > e$, and by Lemma 1 the deficit is permanent for the reconstruction route: $\text{Adv}_{\text{rec}} \leq q \cdot 2^{-1.44 m \delta'} + \varepsilon_H$ for all later traffic. Direct attacks on the traffic-protection primitive retain the separate term of Theorem 1.

Sketch. Cancellation of epoch e' 's waveform requires the epoch's noise key, a random-oracle output on a preimage containing the hardened state the adversary lacks; absent the correct query, the waveform is uniform to it, and its copy retains the uncanceled error process. The theorem above applies per epoch, and monotone hardening (Lemma 1) makes each epoch's requirement permanent. ■

The effect is cumulative for the interceptor. An error in epoch e can prevent recovery of the hardened state needed to cancel the noise in epoch $e+1$, which in turn leaves further residual errors. The legitimate receiver does not follow this path: cancellation and FEC occur before authenticated packets are folded, and packet loss can defer hardening without desynchronising the key track. Once the interceptor has failed to reconstruct a hardened epoch exactly, later designed-randomness packets are evaluated against that unresolved state.

7.3 Ratchet-keyed frequency evasion and the cost of complete capture

Artificial noise operates on packets that the adversary has captured. Frequency agility can instead prevent a dwell from being captured at all. If the interceptor fails to follow a hop, the packets in that dwell enter the gap set G of Definition 1 and the original bounded-capture model already applies. When the interceptor can scan only part of the hopset, hopset breadth, dwell timing and cadence determine the probability of such gaps. With the designed-randomness doctrine of Section 5, a missed dwell then contributes its payload entropy to the bound of Theorem 1. Existing battlefield waveforms already provide frequency agility, so this mechanism can be integrated with that physical-layer behaviour.

Conventional hopping normally depends on pre-placed transmission-security fill, which some deployment profiles considered in Section 3.4 are intended to avoid. The hop schedule can instead be derived from key-track material under a dedicated derivation label. In that case no separate fill is required, and the emitter's spectral position becomes a function of the ratchet state. A later adversary replaying the chain against stored recordings must therefore recover the relevant state before it can derive the corresponding dehopping schedule.

Corollary 3.2 (Single-slip permanence, spectral form). Under ratchet-keyed hopping, if a reconstruction adversary's candidate for the hardened state at epoch e is incorrect, then it cannot generate the dehopping schedule for any $e' > e$; unless it recorded the full band, each subsequent dwell escapes its collection with at least the probability of its uncovered scan fraction, the corresponding

packets enter G , and by Theorem 1 and Lemma 1 the capture deficit, with its designed entropy, is permanent.

Sketch. The epoch’s hop schedule is a random-oracle output on a preimage containing the hardened state the adversary lacks; absent the correct query the schedule is uniform to it, and the adversary is reduced to the pre-break interceptor’s position, an energy search over the band with whatever coverage its receivers afford. The permanence is Lemma 1. ■

A collector can avoid hop-selection uncertainty by recording the whole band as raw signal at sufficient fidelity for the entire session and retaining it for later processing. This is the most direct schedule-agnostic strategy, but it is not the only conceivable interception architecture.

Proposition 5 (Cost of full-support schedule-agnostic recording). Against ratchet-keyed hopping over possible spectral support B , a collector that guarantees completeness by recording that full support at demodulation fidelity for duration T incurs storage proportional to $B \cdot T$ per receiver position. The proposition is a cost statement about this sufficient collection strategy, not a lower bound on every receiver: real-time energy detection, channelisation, compressive acquisition or other signal-processing methods may reduce the amount retained if they can identify useful emissions without knowing the cryptographic hop schedule.

Sketch. Full-support recording retains every dwell irrespective of the unknown schedule, so its storage scales with sampled support and duration. Any strategy that stores less must make an additional receiver-model assumption about its ability to locate or preserve the occupied signal in real time. ■

The engineering point is therefore conditional. Increasing hopset breadth and mission duration increases the cost of the simple full-support strategy and may raise the cost of alternative collectors, but the protocol proof does not establish a universal storage lower bound. If a particular interceptor model cannot maintain complete collection, the resulting gaps fall under Theorem 1; if it can, hopping alone supplies no cryptographic advantage.

A sufficiently resourced collector may still record the required bandwidth for a priority target; wideband recording is an established collection technique. Its copy is then governed by whatever wideband residual error rate remains, so Theorem 3 and ratchet-keyed noise may still be relevant. These mechanisms address different parts of the problem: frequency evasion raises the cost of complete collection, artificial noise affects the quality of what is collected, designed padding supplies entropy when a gap or error occurs, and Theorem 2 remains available for targets against which no collection bound can safely be assumed.

7.4 From opportunistic to mandatory capture

Sections 7.1–7.3 concern the cost and quality of complete interception. Monotone hardening also changes the value of partial interception, which is particularly relevant to harvest-now-decrypt-later collection.

Against a scheme whose session keys are determined by the establishment, a partial recording may retain independent future value: after the establishment mechanism is broken, the adversary can decrypt the portion it actually stored. Ratchet binding removes that independence across confirmed hardening points.

Proposition 7 (A confirmed gap breaks later state reconstruction). Let a correspondent pair harden at confirmed epochs $e_1 < e_2 < \dots$. A bounded-capture adversary whose capture set

omits any packet folded into a confirmed epoch e_j has, for all traffic keyed after the hardening of e_j , only the state-reconstruction advantage of Theorem 1 evaluated at the gap entropy of its omission; plaintext recovered from earlier, fully captured epochs does not supply the missing fold input. An opportunistic collector that accepts gaps therefore does not preserve the ratchet-state reconstruction path beyond its first relevant uncaptured confirmed epoch. This proposition does not exclude an independent attack on the traffic-protection primitive, represented by Adv_{TP} in Theorem 1.

Sketch. Reading post- e_j traffic requires h_j , which by Lemma 1 requires every folded packet of e_j as an accumulator input; decrypted plaintext of other epochs is not such an input, and a missing fold input retains its gap entropy by the argument of Theorem 1. Fragments of a chained relationship therefore do not compose into access past the gap. ■

Proposition 7 changes the collection requirement after the first confirmed hardening point. A partial recording still yields whatever plaintext was captured before a gap, but it no longer preserves access to later traffic. For HNLD this matters because the usual collection strategy assumes that value can be decided later. Here, an omitted accumulator input has already left the wire by the time the establishment mechanism is broken, and later decryption of surrounding traffic does not recreate it.

For an adversary relying on later establishment recovery and ratchet replay, the required fold inputs must therefore be captured while the traffic is being collected and retained across the relevant hardening history. If an adversary does not yet know whether a correspondent pair will become valuable later, preserving that option requires continuous gap-free collection before that value is known.

Observation (conditional effect of collection-time identity dispersal). Suppose a deployment uses proxies or other mechanisms that, for the adversary class being analysed, prevent reliable collection-time identification of the flows belonging to a target correspondent pair. This assumption must include the metadata available to that adversary, including timing, volume and endpoint correlation; the ratchet does not itself provide traffic-analysis anonymity. Under that assumption, Proposition 7 means that preserving future decryptability selectively requires the collector either to discover another valid selector or to retain a sufficiently large superset of candidate flows continuously. If sustained retention of that superset is infeasible and a relevant confirmed gap results, Theorem 1 applies at the entropy of that gap.

This observation is deliberately conditional on the external anonymity or dispersal mechanism. It does not constrain a collector that can correlate the target despite the proxies, nor one that records the entire network continuously. Against a complete recorder the additional guarantee, when available, comes from the independently missing entropy of Theorem 2 or Corollary 2.1, not from identity uncertainty.

7.5 Requirement conversion for authentication

Section 7.4 concerns confidentiality. Post-establishment authentication depends on the ratchet state for the same underlying reason: after the relationship is established, traffic authentication no longer invokes the establishment signature.

ML-DSA-87 authenticates establishment (Section 3.1). Protocols that authenticate each new session against long-term credentials require those credentials to remain unforgeable while new sessions are accepted. PQRD uses the signature when the relationship is created. Subsequent packets are authenticated by a MAC keyed from key-track material (Section 3.2), which is derived from hardened

state. We use *continuity authentication* for this post-establishment reliance on transcript-derived state.

Proposition 8 (Authentication exposure is bounded to establishment). Let a relationship be established under an ML-DSA-87-authenticated establishment and harden at confirmed epochs. Let $\mathcal{A}$ be a bounded-capture adversary that, at any time after establishment, additionally acquires an unrestricted forging capability for the establishment signature scheme, and whose capture omits material of some confirmed epoch with gap entropy γ . Then $\mathcal{A}$ produces a packet that either endpoint accepts as a continuation of the relationship, keyed after the hardening of that epoch, through ratchet-state reconstruction with advantage at most $q \cdot 2^{-\gamma} + \varepsilon_H$. Including an independent attack on the post-establishment MAC, the total continuation-forgery advantage is at most $q \cdot 2^{-\gamma} + \varepsilon_H + \text{Adv}_{\text{MAC}}$. For an existing relationship, a later signature-forging capability does not otherwise increase this bound.

Sketch. A post-hardening packet is accepted only if its MAC verifies under key-track material derived from hardened state. By Lemma 1, deriving that material requires the folded transcript of every confirmed epoch. A signature forgery supplies none of the missing fold input because signatures do not enter the fold, key track or packet MAC. Theorem 1 therefore gives the guessing bound. Forged credentials can be used to create a fresh establishment, but the resulting relationship starts with fresh state and does not key traffic in the existing chain. ■

Corollary 8.1 (Establishment-suite-independent state-reconstruction term). Under the conditions of Theorem 2 or Corollary 2.1, the ratchet-state reconstruction term in Proposition 8 holds at κ (respectively γ_v) independently of the computational assumptions of ML-KEM-1024 and ML-DSA-87. The total continuation-forgery bound still includes the independent Adv_{MAC} term of Proposition 8.

Sketch. Theorem 2 and Corollary 2.1 grant the adversary S_0 and a complete capture, and bound reconstruction of the hardened state by the entropy of the uncaptured exchange. Proposition 8 reduces continuation forgery to that reconstruction. ■

A complete copy of endpoint state gives the adversary the state that continuity authentication verifies. Proposition 4 therefore governs this case, including the forward compromise horizon ω^+ and eviction by an injection whose inputs the adversary lacks. Concurrent use of the copied state can additionally create a detectable fork in the binding track.

Corollary 8.2 (Fork evidence after divergent use). Suppose complete endpoint state at time t is duplicated. If the genuine endpoint and the holder of the duplicate subsequently accept different packet histories within the same relationship, their binding-track accumulators diverge at the first packet present on only one branch, and the divergence surfaces at the next epoch commitment. The result is conditional on divergent use: a duplicate kept perfectly in lockstep by transparent relaying need not create a fork, and a duplicate used only after the genuine endpoint is suppressed is governed by Proposition 4.

Sketch. Each party folds the authenticated packets it processes (Section 3.2). A packet processed on one branch but not the other enters one accumulator history and not the other. Later folds do not remove the difference, and the next epoch commit exposes the mismatch. ■

Compromise of an ML-DSA-87 signing key permits forged establishments for as long as that credential is accepted. A copied ratchet state presents a different case: if it is used concurrently with the genuine endpoint, the commit mechanism can expose the fork; if the genuine endpoint has been destroyed or silenced, Proposition 4’s endpoint-compromise model applies.

Continuity authentication verifies possession of transcript-derived state, not the identity of the operator holding it. Binding that state to an operator is an endpoint and key-management problem outside this model. The result also assumes an authentic establishment; a forging capability already available at establishment can create a valid relationship. Device identity, platform and firmware signing, and the certification path remain outside the result and retain their own lifetime requirements. Hash-based signatures (FIPS 205, or the stateful schemes of SP 800-208 at fixed roots) provide one conservative option for those trust anchors.

7.6 Position of the mechanisms

Proposition 6 (Transient dominance suffices). In the wiretap tradition (Section 6), the channel-dominance condition must hold for the transmissions whose information-theoretic secrecy is claimed. Under the ratchet, an advantage confined to a single confirmed epoch—for example, elevated interceptor error on designed fields or a verified gap in the sense of Corollary 2.1—becomes an input to every later hardened state by Lemma 1. Later restoration of the adversary’s channel does not remove that missing input.

Sketch. Immediate from Lemma 1: the accumulator of the dominated epoch is a permanent input to every later hardened state, and the theorems of Section 5 quantify the residue. ■

The same mechanisms affect the interpretation of the extraction variant in Section 6. There, the adversary-erasure probability δ is an empirical property of collection. Ratchet-keyed noise or evasion can make the corresponding error or erasure rate partly a property of the transmitted waveform. On channels where that model is appropriate, the resource assumption can therefore be tied to an engineering parameter instead of being inferred solely from observed collection performance.

These mechanisms operate where the adversary must demodulate its own copy of a physical signal: radio, optical free-space, acoustic. An adversary obtaining post-demodulation bytes (a co-located tap on an operated transport network) receives an exact copy, is untouched by noise floor and hopset alike, and against it the construction’s guarantees remain exactly those of Theorem 2 and Corollary 2.1 where a verified exchange exists, and of the establishment mechanism where none does. A genuinely perfect intercept is unaffected by either mechanism. Their purpose is to increase the cost of sustaining such an intercept and to preserve the consequence of a lapse once one occurs. A tactical link may combine ratchet-keyed hopping, ratchet-keyed noise, designed per-packet randomness and a pre-mission verified exchange. In that configuration the full-support collection cost of Proposition 5, the noisy-capture bound of Theorem 3, the gap-entropy bound of Theorem 1 and the everlasting-establishment result of Theorem 2 apply to different parts of the same deployment.

8. Qualitative Structural Comparison

Long secrecy lifetimes make it reasonable to inventory the mathematical and operational interfaces on which a construction depends, but such an inventory is not a security score. A mature primitive with substantial visible structure can be better understood and more trustworthy than a smaller or newer composition. The comparison below therefore avoids counting “interfaces” or “hardness objects” and does not rank the schemes.

AES-256-GCM. The continuing data path contains the AES permutation and key schedule, counter-mode input structure, GHASH’s polynomial authenticator and nonce discipline. These

components are extensively studied and standardised. The main operational misuse condition is nonce reuse under a key, for which the consequences are well characterised.

AES-256-CTR with HMAC-SHA-256. This composition combines the AES permutation and counter discipline with an independently keyed hash-based MAC. Its assurance therefore includes both primitive families, correct nonce/counter management and the encrypt-then-MAC composition and verification order.

ChaCha20-Poly1305. The data path exposes ChaCha’s ARX permutation, Poly1305’s modular authenticator and nonce/counter discipline. As with GCM, nonce reuse is an important operational condition and the construction has a large public analysis literature.

PQRD data path. PQRD replaces a conventional block- or ARX-cipher encryption transform with XOR against generator output derived from evolving secret state. This removes round structure from the XOR operation itself, but it does not remove cryptographic structure from the system: confidentiality continues to depend on the SHA-512-based generator/KDF profile and on the post-establishment MAC. In addition, PQRD introduces a state-continuity obligation that must be counted as a misuse class of its own. Rollback, snapshot restoration or reuse of an old pair (h_k, i) can reproduce previous derivation inputs and may repeat working material. Secure erasure, monotonic sequence/state handling, rollback protection and domain separation are therefore part of the security boundary, not merely implementation conveniences.

Comparison.

Property	AES-256-GCM	AES-CTR+HMAC	ChaCha20-Poly1305	PQRD data path
Primary confidentiality primitive	AES-256	AES-256	ChaCha20	SHA-512-based generator/KDF profile
Authentication	GHASH/GCM tag	HMAC-SHA-256	Poly1305	separately labelled hash-based MAC
Prominent operational state requirement	unique nonce per key	unique counter/nonce per key	unique nonce per key	monotonic ratchet state and sequence; no rollback/replay of old state
Effect of state misuse	nonce reuse can be catastrophic	counter reuse leaks plaintext relations	nonce reuse repeats keystream and authenticator material	old-state restoration may reproduce prior derivation inputs and working material

Property	AES-256-GCM	AES-CTR+HMAC	ChaCha20-Poly1305	PQRD data path
Public structural analysis target	AES rounds/key schedule and GHASH	AES plus SHA-256/HMAC composition	ChaCha ARX and Poly1305	SHA-512-based derivation/generator plus ratchet composition

The engineering motivation for PQRD is therefore modest: concentrate the continuing data path on a small set of mature primitive families and remove nonce allocation from normal packet processing. The trade is a stronger state-management obligation. Nothing in this section proves that PQRD is cryptographically stronger than AES-GCM, ChaCha20-Poly1305 or another standard construction; it identifies where assurance effort moves when the ratchet design is adopted.

9. Limitations

The results are subject to several limitations. Theorems 1 and 2 and Propositions 3 and 4 use the random-oracle model; SHA-512 is an instantiation of that model and inherits the usual qualification. The gap entropy γ is traffic-dependent, so Theorem 1 may give a weak bound when the missing material is predictable. Padding, cadence and epoch sizing are therefore security-relevant deployment choices.

The bounded-capture assumption itself is empirical. A co-located interceptor, or an adversary operating the transport, may obtain a complete copy. Where a verified exchange exists, Theorem 2 or Corollary 2.1 provides the applicable post-establishment guarantee; without such an exchange the protocol still depends on the computational security of the establishment mechanism. Deployments must also evaluate the correct channel condition: the adversary needs to obtain at least the packets that contributed to the receiver’s confirmed state, not necessarily every packet transmitted.

Side channels, implementation faults and key management are outside the scope of the analysis, as they are for the comparison schemes. The data path admits a favourable constant-time implementation, but that is an engineering property rather than a theorem. State rollback, snapshot restoration, erasure failure and sequence reuse are also security-relevant misuse conditions for PQRD and must be addressed by the implementation and platform. The manufactured-advantage mechanisms of Section 7 apply only when the adversary must demodulate its own copy of a physical signal. They do not affect an adversary that obtains exact post-demodulation bytes from an operated network.

The collection arguments in Section 7 are model-dependent. Proposition 5 quantifies the cost of full-support recording as one sufficient schedule-agnostic strategy; it is not a universal lower bound on interceptor storage. The identity-dispersal observation likewise assumes that timing, volume and other metadata do not restore a collection-time selector. Against an adversary capable of complete sustained recording, the relevant additional protection is the independent entropy of Theorem 2, not uncertainty about capture, spectrum or identity.

Section 7.5 is limited to post-establishment authentication. It verifies possession of transcript-derived state, not the identity of the operator, and a complete endpoint-state compromise remains governed

by Proposition 4. The result assumes that establishment was authentic. A signature-forging capability already available at that event can create a valid relationship, and trust anchors above the establishment signature retain their own lifetime requirements.

10. Conclusion

This analysis gives a quantified form to PQRD’s central operational claim. If an adversary later defeats the establishment mechanism, recovery of post-hardening traffic still depends on reconstructing the confirmed transcript history. Theorem 1 bounds the resulting advantage by the entropy of the sparsest relevant capture gap, and Lemma 1 shows that a confirmed hardening event remains part of every later state.

Proposition 8 gives a separate result for post-establishment authentication. Once a relationship has been established authentically, a later break of ML-DSA-87 does not by itself authenticate packets in the existing chain; the adversary must possess the ratchet state required for the packet MAC. Corollary 8.2 describes the fork evidence produced when a copied endpoint state is used concurrently with the genuine endpoint.

A different guarantee applies after a high-entropy exchange whose non-capture is established. Whether supplied through an injection or by ordinary protocol traffic sent under physically controlled or detection-evident conditions, that exchange removes ML-KEM from the later confidentiality argument. This does not make the deployed protocol information-theoretically secure: its general capture bound is empirical, its gap entropy depends on traffic, and its fold uses a computational extractor. The universal-hash variant in Section 6 shows that conditional information-theoretic extraction can instead be obtained when an explicit channel-erasure assumption is accepted.

The structural comparison makes a narrower engineering point. PQRD removes per-packet nonce allocation and round structure from the XOR operation, but it does not eliminate misuse risk: rollback resistance, monotonic state, erasure and domain separation become explicit parts of the security boundary. Whether this trade is advantageous in a deployment depends on the soundness of the underlying primitives, the quality of state management and the accuracy of the collection model used for that deployment.

References

1. C. E. Shannon. Communication theory of secrecy systems. *Bell System Technical Journal*, 28(4):656–715, 1949.
2. A. D. Wyner. The wire-tap channel. *Bell System Technical Journal*, 54(8):1355–1387, 1975.
3. U. Maurer. Conditionally-perfect secrecy and a provably-secure randomized cipher. *Journal of Cryptology*, 5(1):53–66, 1992.
4. U. Maurer. Secret key agreement by public discussion from common information. *IEEE Transactions on Information Theory*, 39(3):733–742, 1993.
5. C. Cachin and U. Maurer. Unconditional security against memory-bounded adversaries. *CRYPTO 1997*.
6. Y. Aumann, Y. Z. Ding, and M. O. Rabin. Everlasting security in the bounded storage model. *IEEE Transactions on Information Theory*, 48(6):1668–1680, 2002.
7. S. Dziembowski. On forward-secure storage. *CRYPTO 2006*.

8. J. Håstad, R. Impagliazzo, L. Levin, and M. Luby. A pseudorandom generator from any one-way function. *SIAM Journal on Computing*, 28(4):1364–1396, 1999.
9. K. Cohn-Gordon, C. Cremers, B. Dowling, L. Garratt, and D. Stebila. A formal security analysis of the Signal messaging protocol. *EuroS&P 2017*.
10. A. Biryukov and D. Khovratovich. Related-key cryptanalysis of the full AES-192 and AES-256. *ASIACRYPT 2009*.
11. NIST. FIPS 203: Module-Lattice-Based Key-Encapsulation Mechanism Standard. 2024.
12. NIST. FIPS 204: Module-Lattice-Based Digital Signature Standard. 2024.
13. NIST. FIPS 205: Stateless Hash-Based Digital Signature Standard. 2024.
14. NIST. FIPS 180-4: Secure Hash Standard. 2015.
15. NIST. FIPS 198-1: The Keyed-Hash Message Authentication Code (HMAC). 2008.
16. NIST. SP 800-208: Recommendation for Stateful Hash-Based Signature Schemes. 2020.
17. NIST. SP 800-38D: Galois/Counter Mode (GCM) and GMAC. 2007.
18. Y. Nir and A. Langley. ChaCha20 and Poly1305 for IETF Protocols. RFC 8439, 2018.
19. G. Di Crescenzo, R. Lipton, and S. Walfish. Perfectly secure password protocols in the bounded retrieval model. *TCC 2006*.
20. S. Dziembowski. Intrusion-resilience via the bounded-storage model. *TCC 2006*.
21. J. Alwen, Y. Dodis, and D. Wichs. Leakage-resilient public-key cryptography in the bounded-retrieval model. *CRYPTO 2009*.
22. S. Dey. Advancing the idea of probabilistic neutral bits: first key recovery attack on 7.5 round ChaCha. *IEEE Transactions on Information Theory*, 2024.
23. Z. Zhang, M. Li, L. Gao, and M. Wang. Collision attacks on SHA-256 up to 37 steps with improved trail search. Cryptology ePrint Archive, Paper 2026/232.
24. Y. Li, F. Liu, and G. Wang. The first practical collision for 31-step SHA-256. *ASIACRYPT 2024*.
25. NIST. SP 800-108 Rev. 1 (updated 2024): Recommendation for Key Derivation Using Pseudorandom Functions. 2024.