IIETA International Information and Engineering Technology Association
Advancing the World of Information and Engineering

Ingénierie des Systèmes d'Information
Vol. 31, No. 7, July, 2026, pp. 2231-2239
Journal homepage: http://iieta.org/journals/isi

Structural Cryptanalysis and Transcript-Bound Redesign of a Multi-Stage Long-Term Evolution Authentication Protocol

Haewon Byeon

Department of Future Technology, Korea University of Technology and Education (KOREATECH), Cheonan-si 31253, Republic of Korea

Corresponding Author Email: bhwpuma@naver.com

https://doi.org/10.18280/isi.310709

Received: 25 March 2026
Revised: 29 May 2026
Accepted: 12 June 2026
Available online: 31 July 2026

Keywords:
authenticated key exchange, CryptoVerif, Long-Term Evolution security, protocol cryptanalysis, reproducible simulation

ABSTRACT

This study presents a structural cryptanalysis of a multi-stage Long-Term Evolution (LTE) authentication proposal and a transcript-bound redesign. We first formalize the adversary, variable domains, security invariants, and two stepwise attack witnesses. The analysis shows that deterministic token generation permits replay when its context repeats; the published Hyperelliptic Curve Cryptography (HECC) acceptance equation does not by itself bind both peers; and the final Poisson-derived transport secret has at most 17.96 bits in a generous 255,000-candidate domain. The redesign uses rotating pseudonyms, short-lived authorization tickets, fresh X25519 contributions, home subscriber server (HSS)-confirmed transcripts, HMAC-based Key Derivation Function (HKDF) key separation, and bidirectional key confirmation. A CryptoVerif model of the core authenticated key exchange proves key agreement, mutual injective agreement, and session-key secrecy under selective long-term compromise, subject to the stated cryptographic assumptions. We also report absolute message sizes and operation counts and release a deterministic event-driven simulation profile. Across 30 runs for each load, the redesign reduces mean latency relative to the analyzed protocol by 15.26–64.99 ms at 200–500 concurrent user equipment (UE) (paired permutation $p < 0.001$), while detecting all injected replays in the modeled 120-s window. The proposal is a workflow-aligned research extension, not a wire-compatible replacement for standardized Evolved Packet System Authentication and Key Agreement (EPS-AKA).

1. INTRODUCTION

Long-Term Evolution (LTE) remains operationally important in mixed-generation mobile infrastructures, including private cellular systems, railway communication, industrial deployments, and machine-type services [1, 2]. Consequently, LTE-derived attachment, handover, and control procedures remain exposed to identity disclosure, replay, false base stations, and key-compromise propagation [3, 4]. Any proposed extension must therefore be assessed as a protocol composition problem rather than as a collection of individually plausible cryptographic components.

Recent work has pursued stronger authentication and re-authentication for heterogeneous 4G/5G access, Long-Term Evolution for Railway (LTE-R), and Elliptic Curve Cryptography (ECC)-assisted LTE Authentication and Key Agreement (AKA) [5-10]. Parallel studies address scalable machine-type authentication, attack screening, and mobility-oriented group handover [11-24]. These mechanisms differ substantially, but they share one engineering requirement: every accepted key must be bound to fresh state, the intended peers, the serving-network context, and an authorization decision.

Auxiliary physical-layer features, Physically Unclonable Functions (PUFs), blockchain trust, and lightweight signcryption can improve device binding or reduce selected costs [25-32]. They cannot replace freshness or authenticated agreement. The target scheme of Sagar and Saidireddy combines a Recurrent Neural Network (RNN) filter, Haversine Distance-Message Authentication Protocol (HD-MAC) tokenization, Bernoulli Distribution-based Pelican Optimization Algorithm (BD-POA)-selected Hyperelliptic Curve Cryptography (HECC) parameters, and a Poisson-derived three-way handshake [33]. Its breadth is attractive, but its interfaces leave several claimed guarantees unsupported.

This revision makes five contributions. First, it enumerates the attacker capabilities and exclusions and defines agreement, secrecy, freshness, and compromise-containment goals. Second, it gives explicit replay and conditional unknown-key-share witnesses and quantifies the Poisson key space. Third, it replaces the ad hoc key schedule with a transcript-bound authenticated key exchange and verifies its core in CryptoVerif. Fourth, it reports absolute byte and operation counts and maps each step to the relevant LTE workflow. Fifth, it supplies a reproducible event-driven simulator with fixed seeds, complete queue parameters, confidence intervals, and paired significance tests.

The term workflow-aligned is used deliberately. The

redesign preserves the order of access request, home-network authorization, challenge, and key confirmation, but its Open Authorization (OAuth) ticket and ephemeral public-key fields are research extensions. It is neither bit-level compatible with existing Non-Access Stratum (NAS) messages nor claimed to be 3rd Generation Partnership Project (3GPP) compliant without standardization and implementation work.

2. RELATED WORKS

LTE and LTE/5G authentication studies have sought lower signaling delay while strengthening mutual authentication and identity protection [5-10]. IoT-enabled LTE and handover protocols further emphasize group state, mobility, and partial trust at the edge [11, 12, 16-24]. Anomaly detection can reduce the traffic reaching expensive verifiers [13-15], but a classifier decision is not evidence of secret possession and should not enter the key schedule.

Physical-layer authentication and PUF-based designs provide complementary evidence [25-29], while wider 5G and blockchain surveys emphasize cross-domain trust [30, 31]. HECC can offer compact operands at a given security level [32], but a scalar-multiplication saving cannot repair a circular acceptance predicate or an unbound transcript. This distinction motivates our separation of payload protection from access authentication.

Our system interpretation follows the confidentiality, authentication-data distribution, Evolved Packet System Authentication and Key Agreement (EPS-AKA), key-hierarchy, and security-mode concepts in 3GPP TS 33.401 [33]. Formal LTE studies have shown why this level of precision matters: Tsay and Mjolsnes exposed an AKA vulnerability through protocol reasoning [34], and Ben Henda and Norrman [35] demonstrated both the value and the modeling difficulty of formal LTE security analysis. We therefore use computational verification rather than qualitative labels alone. CryptoVerif supplies game-based proofs [36]; Tamarin is a complementary symbolic framework for stateful protocols [37].

Unlike earlier variants that primarily add a mechanism, this paper treats the target protocol as a staged state machine, identifies the exact acceptance relations that fail, and then checks a minimal redesigned core against explicit queries. This positions the work as a reproducible protocol-engineering study rather than a conceptual critique.

3. METHODOLOGY

3.1 Reconstruction and notation

We reconstructed the published messages and equations of Sagar and Saidireddy [38] as a labeled transition system over user equipment (UE), eNodeB, OAuth, MME/serving network (SN), and home subscriber server (HSS). Each transition records the sender, receiver, visible fields, locally held secrets, freshness state, and acceptance event. For the HECC notation, let C be a genus-2 curve over F_p and $J_C(F_p)$ its Jacobian subgroup of prime order q. The divisor d lies in $J_C(F_p)$; Δ_{sen}, Δ_{rec}, ω, and rand lie in Z_q^*; $\Phi_{sen} = \Delta_{sen}d$ and $\Phi_{rec} = \Delta_{rec}d$; ρ maps a divisor to an l-bit string; e, y lie in Z_q; and χ lies in $J_C(F_p)$. These domains remove the ambiguity surrounding Δ_{sen} and Φ_{sen} in the original text.

For each accepted session *sid*, we extracted the dependency chain from κ_A to token T, the HECC tuple, κ_B, the identity check, and κ_{sec}. We then tested whether acceptance remained possible after message replay, context substitution, disclosure of one cached artifact, or disclosure of one long-term credential after session completion. Figure 1 summarizes this analysis-to-redesign workflow.

Figure 1. Evidence-driven workflow from protocol reconstruction to formal and quantitative validation
Note: Output: a workflow-aligned, transcript-bound redesign with explicit assumptions and reproducible evidence.

Table 1. Formal adversary capabilities and boundaries

ID	Capability	Modeled Boundary
A1	Intercept, inject, drop, reorder, and replay any public-channel message.	Authenticated core-link protection is an explicit assumption.
A2	Know algorithms, public parameters, public keys, formats, and old accepted transcripts.	No security by obscurity.
A3	Start concurrent sessions and manipulate timing/retransmissions within clock tolerance.	Fresh nonces remain uniformly generated.
A4	Compromise one eNodeB or OAuth cache and obtain its stored state.	No simultaneous UE-HSS compromise.
A5	Learn one long-term UE or server credential after a completed target session.	Erased ephemeral scalars are not recovered.
A6	Issue adaptive verification queries and reuse a captured authorization artifact.	Primitives are not broken; endpoint malware is outside scope.

Table 2. Formal claims for the redesigned core

Property	CryptoVerif Query/Evidence	Result and Assumptions
Key agreement	$\text{end}_{SN}(...,k) \wedge \text{end}_{UE}(...,k') \Rightarrow k = k'$	Proved.
UE→SN injective agreement	$\text{inj-end}_{SN}(tr, k) \Rightarrow \text{inj-end}_{UE}(tr, k) \vee \text{Corrupt}(UE)$	Proved up to nonce collision and signature terms.
SN→UE injective agreement	$\text{inj-end}_{UE}(tr, k) \Rightarrow \text{inj-begin}_{SN}(tr) \vee \text{Corrupt}(SN)$	Proved up to nonce collision and signature terms.
Session-key secrecy/FS	Secrecy of completed-session key with post-session long-term corruption.	Proved under CDH, EUF-CMA signatures, and collision bounds.
Identity exposure	IMSI absent from public terms; rotating PID only.	Paper-level invariant; radio side channels excluded.

Note: UE: User equipment; SN: Serving network; HSS: Home subscriber server; IMSI: International Mobile Subscriber Identity; PID: Pseudonymous Identifier; FS: Forward Secrecy; HECC: Hyperelliptic Curve Cryptography; EUF-CMA: Existential Unforgeability under Chosen-Message Attack; CDH: Computational Diffie–Hellman.

3.2 Adversary model

The network adversary has Dolev-Yao control and may schedule unbounded concurrent sessions. $K0$ contains all public parameters, public keys, identities intentionally exposed by the protocol, message formats, and previously transmitted traffic. Corrupt(P, t) reveals the current state of one eNodeB or OAuth cache at time t; RevealLT(P, t) reveals one UE-side or server-side long-term credential; and RevealSession(sid, t) reveals a completed session key only for the designated session. The model is summarized in Table 1.

3.3 Security goals and proof method

A session is fresh when its nonce pair has not appeared in the replay cache, its tickets are unexpired, and no party or session disallowed by the property has been revealed. The agreement transcript is tr = (PID, $SNID$, tid, $epoch$, N_u, N_s, X_u, X_s). We require: G1 freshness uniqueness; G2 non-disclosure of International Mobile Subscriber Identity (IMSI) on the public channel; G3 UE-to-SN and SN-to-UE injective agreement on tr; G4 agreement and indistinguishability of SK; G5 forward secrecy after allowed post-session long-term compromise; G6 unknown-key-share resistance through explicit role and peer binding; and G7 containment after a single edge compromise.

The core AKE was encoded in CryptoVerif 2.12 as two replicated roles with fresh nonces and Diffie-Hellman exponents, role-tagged signed transcripts, key derivation, begin/end events, and post-session corruption oracles. Valid HSS authorization and the integrity-protected MME-HSS channel are modeled as preconditions, so the proof covers the cryptographic core rather than the complete OAuth implementation or 3GPP carriage. The tool produced 'All queries proved' for the queries in Table 2.

3.4 Reproducible quantitative evaluation

The performance analysis uses a Python 3.12 standard-library discrete-event simulator. It models control-plane queues and declared cryptographic service costs, not radio waveforms or a deployed EPC. Each condition uses seeds 20260801-20260830, one 100-ms burst with one authentication per UE, and 30 independent replications. For every latency mean, we report a nonparametric 95% bootstrap interval (10,000 resamples). Original-versus-redesign differences use a two-sided paired random-sign permutation test with 20,000 permutations. The source script, run-level CSV, summary CSV, and JSON metadata are retained as the reproducibility record.

4. CRYPTANALYSIS OF THE TARGET PROTOCOL

4.1 Reconstructed five-stage protocol

The protocol in reference [38] begins when UE sends a connection request through eNodeB. HSS applies an RNN classifier and issues κ_A if the request is labeled benign. In the code-grant stage, message M and κ_A are recursively split and transformed, after which T = MD5(Transform(M, κ_A, ctr)). In the implicit-grant stage, T and κ_A reach MME, and the BD-POA-HECC process produces (C_{msg}, χ, e). The identity-request stage replaces T with κ_B and only then checks IMSI through HSS. The authentication-grant stage derives κ_{sec} = $e^{(-\mu)}\mu^R/R$. Figure 2 shows the resulting dependency flow.

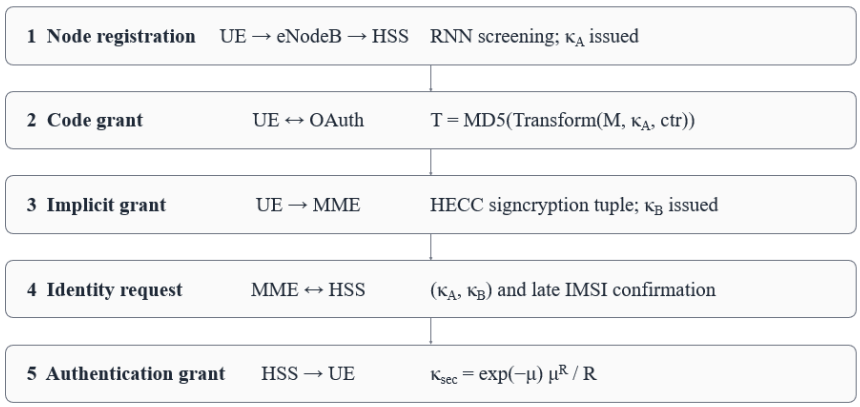

Figure 2. Reconstructed five-stage target protocol and the location of its late identity check

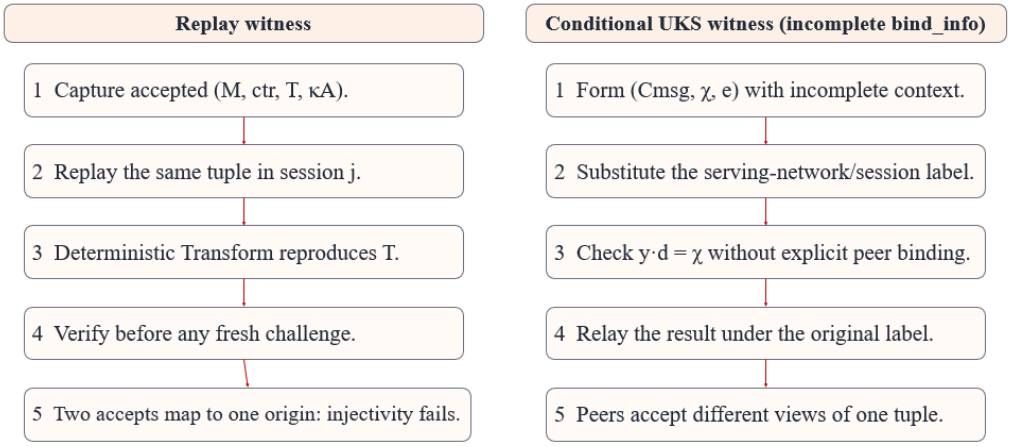

Figure 3. Stepwise replay and conditional unknown-key-share witnesses against the published relations
Note: Conditional witness against the published bind_info; not an attack claim against deployed EPS-AKA.

The published HECC relations can be written as $Y_1 = \rho(\omega d)$, $Y_2 = \rho(\omega \Phi_{rec})$, $C_{msg} = EY_2(M)$, $y = \rho Y_1(M||\text{bind}_{info})$, $e = \omega/(rand + \Delta_{sen})$, and $\chi = yd$. The receiver reconstructs Y_1 from e and long-term terms, recomputes y, and accepts when $yd = \chi$. The variable ω can randomize signcryption, but κ_{sec} contains neither ω nor an independently authenticated ephemeral Diffie-Hellman secret. Thus, our forward-secrecy critique concerns the final transport key, not a claim that the HECC payload operation has no randomness.

4.2 Explicit attack witnesses

Replay witness W_1 is: (1) an adversary records (M, ctr, T, κ_A) from accepted run i; (2) it replays the tuple in run j; (3) unchanged transform inputs reproduce T; (4) the receiver reaches HECC processing before receiving a fresh cryptographic challenge; and (5) two acceptance events map to one originating authorization event. This violates injective agreement whenever the counter/context is reused or accepted from the message rather than verifier state. MD5 and the Haversine-style bit transform do not supply a pseudorandom function (PRF)-based message authentication code (MAC) proof.

Conditional unknown-key-share witness W_2 is:

(1) UE forms (C_{msg}, χ, e) under an underspecified bind_{info};

(2) the adversary substitutes or relays a serving-network/session label;

(3) the receiver recomputes y and checks $\chi = yd$ without an explicit ordered pair of peer identities;

(4) the result is relayed; and

(5) the peers may accept different context views.

This is a witness against the published equations if bind_{info} omits the peer identities and fresh session identifier; it is not presented as an exploit against deployed 3GPP EPS-AKA. The two stepwise attack traces are summarized in Figure 3.

4.3 Forward secrecy, compromise propagation, and key entropy

After disclosure of Δ_{sen} or Δ_{rec}, an attacker can revisit stored (e, χ, C_{msg}) values and recompute relations that depend on those long-term terms. More importantly, the final κ_{sec} is not derived from an erased ephemeral shared secret. Consequently, the protocol does not establish that past transport keys remain indistinguishable after long-term disclosure. Closely related κ_A, T, and κ_B values also cross UE, OAuth, MME, and HSS without a clean session boundary, allowing one cached compromise to influence later stages.

The Poisson expression is quantitatively unsuitable as a cryptographic key. Even granting μ the grid {0.01, 0.02, ..., 10.00} and R the set {1, ..., 255}, there are only 1000 × 255 = 255,000 candidate input pairs, so $H_\infty(\kappa_{sec}) \le \log_2(255{,}000) = 17.96$ bits before accounting for output collisions. If μ is known or estimable, the upper bound is $\log_2(255) = 7.99$ bits; if both μ and R are transcript-derived, their conditional entropy is zero. All bounds are far below a 128-bit security target.

5. TRANSCRIPT-BOUND REDESIGN

5.1 Credentials and design rules

The redesign uses a rotating 128-bit pseudonym PID, a 128-bit transaction identifier tid, 128-bit nonces, and ephemeral X25519 shares $X_u = x_uG$ and $X_s = x_sG$ [39]. HSS issues $\tau_H = \text{HMAC}_{KH}(PID||SNID||epoch||exp)$, and OAuth issues $\tau_O = \text{Sign}^{\text{Ed25519}}_{sk_O}(PID||aud||exp||jti)$ [40]. UE and HSS share K_{UH}. The authenticated transcript hash includes ordered role tags, both peer contexts, both tickets' identifiers, the epoch, both nonces, and both ephemeral shares. HMAC-based Key Derivation Function (HKDF)-Extract and HKDF-Expand derive independent traffic and confirmation keys [41].

A replay cache stores (jti, N_u, $H(tr)$) for 120 s; OAuth tickets expire after 60 s; and both ephemeral scalars are erased immediately after bidirectional confirmation. IMSI is used only inside the HSS database lookup. PID rotation limits protocol-level linkability, although traffic analysis and radio fingerprints are outside the claimed identity property.

5.2 Formal protocol pseudocode

Protocol 1 defines the redesigned exchange. concat(·) is an unambiguous length-delimited encoding, H is SHA-256, and all rejection paths terminate before payload processing. The MME-HSS interface is assumed to be integrity-protected as in the operator core; τ_O is verified at MME, τ_H and auth_U at HSS, and σ_H at both MME and UE.

Protocol 1. Transcript-bound five-message authenticated key exchange

Step	Pseudocode
Setup	**Home Subscriber Server (HSS):** $\tau_H \leftarrow \mathrm{HMAC}_{KH}(\mathrm{PID}\|\|\mathrm{SNID}\|\|\mathrm{epoch}\|\|\mathrm{exp})$; **OAuth:** $\tau_O \leftarrow \mathrm{Sign}_{sk_O}^{\mathrm{Ed25519}}(\mathrm{PID}\|\|\mathrm{aud}\|\|\mathrm{exp}\|\|\mathrm{jti})$.
M1 UE→MME	Sample N_u, x_u; $X_u = x_u G$; $\mathrm{auth}_U = \mathrm{HMAC}_{KUH}('U1'\|\|H(\mathrm{PID}, \tau_H, \tau_O, \mathrm{SNID}, N_u, X_u))$; send PID, τ_H, τ_O, SNID, tid, N_u, X_u, auth_U.
M2 MME→HSS	Verify τ_O, expiry, audience, and cache; sample N_s, x_s; $X_s = x_s G$; forward M1 context, N_s, X_s, MME_{ID}, epoch over authenticated core link.
M3 HSS→MME	Verify τ_H, auth_U, SNID, epoch and PID→IMSI mapping; tr←concat(PID, SNID, tid, epoch, N_u, N_s, X_u, X_s); return decision, H(tr), $\sigma_H = \mathrm{Sign}_{skH}('H3'\|\|H(\mathrm{tr}))$.
M4 MME→UE	Verify σ_H; $Z \leftarrow X_u^{x_s}$; SK←HKDF-Expand(HKDF-Extract(0, Z), H(tr)||'LTE-redesign'); send N_s, X_s, epoch, σ_H, $\mathrm{MAC}_{SK}('S\text{-}finish'\|\|H(\mathrm{tr}))$.
M5 UE→MME	Verify σ_H and server finish; derive $Z \leftarrow X_s^{x_u}$ and SK; send $\mathrm{MAC}_{SK}('U\text{-}finish'\|\|H(\mathrm{tr}))$; both sides accept, cache identifiers, and erase x_u, x_s.

Note: HSS: Home Subscriber Server; OAuth: Open Authorization; UE: User equipment; MME: Mobility Management Entity; SNID: Serving Network Identifier; PID: Pseudonymous Identifier; HMAC: Hash-based Message Authentication Code; H: Hash Function; MAC: Message Authentication Code; IMSI: International Mobile Subscriber Identity; HKDF: HMAC-based Key Derivation Function; SK: Session Key; MME-ID: Mobility Management Entity Identifier.

5.3 Security argument

Freshness follows because an accepted transcript contains independently sampled N_u and N_s and a unique *tid*, and the cache rejects a repeated (*jti*, N_u, $H(tr)$). Injective agreement follows from the ordered, role-tagged $H(tr)$, HSS signature, and two direction-specific finish MACs: replaying a finish value under a different peer, epoch, nonce, or share changes $H(tr)$. Unknown-key-share substitution therefore requires either a signature/MAC forgery or a transcript collision.

For key secrecy, the public transcript reveals only X_u and X_s; computing Z after x_u and x_s are erased reduces to CDH in the modeled group. Later disclosure of K_{UH}, K_H, sk_O, or sk_H enables at most future impersonation within the corresponding trust domain; it does not reconstruct Z from an old transcript. A single compromised eNodeB learns only public signaling, and a compromised OAuth cache learns authorization metadata but neither K_{UH} nor an ephemeral scalar. These claims match the proved core queries in Table 2.

5.4 Long-Term Evolution workflow mapping and Hyperelliptic Curve Cryptography scope

HECC is retained only as an optional payload-confidentiality profile when compact genus-2 divisors are an implementation requirement. It does not determine admission, replay state, or the transport key. For a 128-bit target, our explicit profile uses a genus-2 Jacobian over an approximately 128-bit prime field with subgroup order $q \approx 2^{256}$; a compressed divisor is approximately 33 bytes (about 64 bytes uncompressed). The core design instead uses the widely analyzed X25519/Ed25519/HKDF profile [39-41]. Table 3 maps the redesigned messages to the corresponding workflow concepts and clauses in 3GPP TS 33.401.

Table 3. Workflow mapping to 3GPP TS 33.401

Redesign	Long-Term Evolution (LTE) Concept	Relevant Clause	Compatibility Status
PID in M1	User identity confidentiality/temporary identity	5.1.1; 6.1.3	Concept aligned; encoding is new.
M2/M3	Serving-network request and HSS authentication data	6.1.2	Core workflow aligned; ticket fields are extensions.
M1–M4	EPS AKA challenge/response and key hierarchy	6.1.1; 6.2	Function aligned; X25519/HKDF are non-standard.
M4/M5	Security-mode/key-confirmation transition	7.2.4	Additional explicit confirmation messages.
τ_O	Application authorization	Not specified	Non-3GPP application-layer extension.

Note: 3GPP: 3rd Generation Partnership Project; TS: Technical Specification; PID: Pseudonymous Identifier; HSS: Home Subscriber Server; EPS: Evolved Packet System; AKA: Authentication and Key Agreement; HMAC: Hash-based Message Authentication Code; HKDF: HMAC-based Key Derivation Function.

6. QUANTITATIVE EVALUATION

6.1 Computation and communication cost

Counts in Table 4 are derived from the published equations and Protocol 1, not from cross-platform timing. In the original signcryption, the sender evaluates ωd, $\omega \Phi_{\mathrm{rec}}$, and yd (three HECC scalar multiplications); the receiver evaluates the two-to-three reconstruction/verification multiplications, giving five-to-six per session. The redesign evaluates one public share and one shared secret at each endpoint (four X25519 scalar multiplications total), three Ed25519 verifications, and eight hash/MAC/KDF calls in the declared profile.

Table 5 reports application/control payload encoding only; it excludes IP, SCTP, S1AP, and NAS headers because the redesign has not been assigned standardized information elements. For the redesign, M1–M5 contain 304, 352, 112, 152, and 40 bytes, respectively. The 960-byte total includes a 256-byte protected request and length-delimited field labels/padding. The target size is an explicit simulation profile because Sagar and Saidireddy [38] did not fully specify a byte-level wire format.

6.2 Simulation configuration

The Python 3.12 discrete-event simulator represents eNodeB, MME, HSS, and OAuth as first-come, first-served resource queues. For each protocol and load of 100-500 UEs, one authentication per UE arrives uniformly within a 100-ms burst, and 30 independent replications use fixed seeds

20260801-20260830. Each protocol step incurs its declared service cost plus lognormal jitter, while inter-node transmission uses path-specific lognormal delays. Replay attempts constitute 10% of sessions, and single-node compromise is evaluated with 500 forgery trials over a 30-s exposure. Table 6 reports the complete topology, queue, delay, replay-window, cache, compromise, timeout, and statistical parameters.

Run-level outputs include completion latency, timeout status, replay detection, and compromise-containment outcomes. Mean latency is summarized with 95% nonparametric bootstrap confidence intervals (10,000 resamples), and paired target-versus-redesign differences are assessed using a two-sided random-sign permutation test (20,000 permutations). The simulator models declared control-plane queues and service costs rather than radio propagation or a deployed Evolved Packet Core.

6.3 Results

At 100 UEs, the redesign costs 3.83 ms more than the target protocol because the queues are lightly loaded and explicit key confirmation dominates. From 200 to 500 UEs, early replay rejection and lower MME service burden reduce mean latency by 15.26-64.99 ms. Every paired difference is significant at $p < 0.001$ in the random-sign test. Confidence intervals in Table 7 represent between-run uncertainty, not uncertainty in real LTE deployment.

Across loads, modeled replay detection averaged 66.7% for the reference profile, 23.0% for the target, and 100% for the redesign. Corresponding compromise containment was approximately 98.0%, 36.0%, and 100%. The reference profile is a queueing baseline, not a claim that standardized EPS-AKA has only 66.7% replay resistance. The target values arise from its declared short stale-token window and compromise-acceptance profile. Figure 4 makes these model-scoped comparisons explicit.

Figure 5 shows the nonlinear queueing penalty of the target protocol. The redesign is not universally faster: its light-load overhead is visible. Its advantage emerges when MME-bound HECC work and late replay rejection accumulate. Authentication success remained 1.0 in all simulated conditions because every benign completion remained below the 750-ms timeout.

Table 4. Absolute cryptographic operation counts per successful session

Profile	Asymmetric Operations	Hash/MAC/KDF	Symmetric
Reference LTE-style	0 public-key operations in the simulator profile	12	2 block-cipher calls
Target protocol	5-6 HECC scalar multiplications	7	1 encryption + 1 decryption
Redesign	4 X25519 scalar multiplications + 3 Ed25519 verifications	8	AEAD available after key confirmation

Note: LTE: Long-Term Evolution; KDF: Key Derivation Function; MAC: Message Authentication Code; HECC: Hyperelliptic Curve Cryptography; AEAD: Authenticated Encryption with Associated Data.

Table 5. Absolute communication burden

Profile	Message Payloads (bytes)	Total (bytes)	Access Side (bytes)
Reference Long-Term Evolution (LTE)-style	profile total	608	320
Target protocol	reconstructed profile	896	432
Redesign	304 + 352 + 112 + 152 + 40	960	496

Table 6. Reproducible event-driven simulation parameters

Parameter	Value	Generation/Model
Topology	500 UE, 20 eNodeB, 4 MME, 1 HSS, 1 OAuth	Logical control-plane resources
Load	100, 200, 300, 400, 500 UE	One authentication per UE in a uniform 100-ms burst
Replications	30 per protocol-load pair	Seeds 20260801-20260830
Workers	eNB 40; MME 8; HSS 4; OAuth 4	FCFS queues
Network delay	path means 3.0-6.5 ms	Lognormal jitter $\sigma = 0.22$
Service delay	step means 0.15-3.60 ms	Lognormal jitter $\sigma = 0.15$; DB cost included at HSS
Replay	10%; delay U(0,45 s)	Window: reference 30 s, target 10 s, redesign 120 s
Tokens/cache	redesign expiry 60 s; cache 100,000	No eviction at evaluated load
Compromise	T = 30 s; 500 forgery trials	Single eNodeB/OAuth-side state exposure
Timeout/statistics	750 ms; bootstrap B = 10,000; permutation B = 20,000	95% CI; paired two-sided test

Note: UE: User equipment; eNodeB: evolved NodeB; MME: Mobility Management Entity; HSS: Home Subscriber Server; OAuth: Open Authorization; FCFS: First-Come, First-Served; DB: Database; CI: Confidence Interval; T: compromise duration.

Table 7. Mean authentication latency over 30 independent runs

User Equipment	Reference (ms)	Target (ms)	Redesign (ms; 95% Confidence Interval)	Δ Target-Redesign	*p*
100	21.27	29.88	33.71 [33.61, 33.81]	−3.83	<.001
200	21.28	49.46	34.20 [34.12, 34.28]	+15.26	<.001
300	21.43	100.26	51.01 [50.16, 51.88]	+49.24	<.001
400	22.97	144.72	85.88 [84.99, 86.76]	+58.84	<.001
500	33.18	188.04	123.05 [122.15, 123.97]	+64.99	<.001

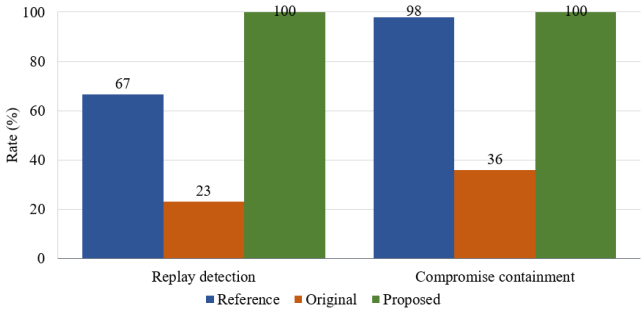

Figure 4. Measured replay detection and single-node compromise containment in the declared simulator
Note: Thirty seeded runs at each of five loads; rates are averaged over loads.

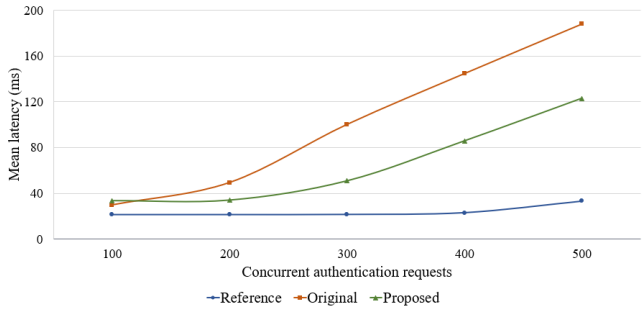

Figure 5. Measured mean authentication latency versus concurrent user equipment (UE) load
Note: Error bars show 95% bootstrap intervals. Thirty-run means; 95% intervals and paired tests are reported in Table 7.

6.4 Threats to validity and deployment implications

Internal validity depends on the declared service-time profile; operation counts and latency are therefore reported separately. Construct validity is limited because compromise containment is a protocol-level forgery outcome, not a measure of endpoint recovery. External validity is limited by the absence of radio, EPC, and operator testbed measurements. The fixed seeds, run-level outputs, and complete parameter file make the results reproducible but do not transform the simulator into a deployment benchmark.

Formal validity is likewise scoped. CryptoVerif establishes the core AKE claims under its CDH, signature, and collision assumptions; it does not verify an OAuth implementation, HSS database authorization, denial of service, radio linkability, or standards conformance. A deployable version would require new NAS information elements, downgrade protection, inter-MME state transfer, key-erasure assurance, and 3GPP review.

7. CONCLUSIONS

The target protocol's principal weakness is compositional: deterministic token logic, an underspecified HECC verification context, late identity validation, and a low-entropy Poisson transport secret do not jointly establish freshness or authenticated key agreement. The revised analysis converts those observations into explicit adversary actions, attack witnesses, variable domains, and numerical bounds.

The redesign separates authorization from key establishment and binds a rotating pseudonym, serving-network identifier, transaction identifier, epoch, nonces, and ephemeral shares into one confirmed transcript. Its core satisfies the stated CryptoVerif queries, and its absolute costs and simulation behavior are reported without normalized qualitative labels. The design should be viewed as a formally supported, workflow-aligned research extension whose next step is implementation in a standards-aware LTE testbed.

ACKNOWLEDGMENT

This research was supported by the Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (NRF-RS-2023-00237287; 2026S1A5A01004224).

REFERENCES

[1] Alam, M.J., Hossain, M.R., Azad, S., Chugh, R. (2023). An overview of LTE/LTE-A heterogeneous networks for 5G and beyond. Transactions on Emerging Telecommunications Technologies, 34(8): e4806. https://doi.org/10.1002/ett.4806

[2] Vaezi, M., Azari, A., Khosravirad, S.R., et al. (2022). Cellular, wide-area, and non-terrestrial IoT: A survey on 5G advances and the road toward 6G. IEEE Communications Surveys and Tutorials, 24(2): 1117-1174. https://doi.org/10.1109/COMST.2022.3151028

[3] Khan, R., Kumar, P., Jayakody, D.N.K., Liyanage, M. (2020). A survey on security and privacy of 5G technologies: Potential solutions, recent advancements, and future directions. IEEE Communications Surveys and Tutorials, 22(1): 196-248. https://doi.org/10.1109/COMST.2019.2933899

[4] Ferrag, M.A., Maglaras, L., Argyriou, A., Kosmanos, D., Janicke, H. (2018). Security for 4G and 5G cellular networks: A survey of existing authentication and privacy-preserving schemes. Journal of Network and Computer Applications, 101: 55-82. https://doi.org/10.1016/j.jnca.2017.10.017

[5] Alezabi, K.A., Hashim, F., Hashim, S.J., Ali, B.M., Jamalipour, A. (2020). Efficient authentication and re-authentication protocols for 4G/5G heterogeneous networks. EURASIP Journal on Wireless Communications and Networking, 2020(1): 105. https://doi.org/10.1186/s13638-020-01702-8

[6] Panda, P.K., Chattopadhyay, S. (2020). An improved authentication and security scheme for LTE/LTE-A networks. Journal of Ambient Intelligence and Humanized Computing, 11(5): 2163-2185. https://doi.org/10.1007/s12652-019-01248-8

[7] Wang, Y., Zhang, W.F., Wang, X.M., Guo, W., Khan, M.K., Fan, P.Z. (2022). Improving the security of LTE-R for high-speed railway: From the access authentication view. IEEE Transactions on Intelligent Transportation Systems, 23(2): 1332-1346. https://doi.org/10.1109/TITS.2020.3024684

[8] Lu, X.F., Yang, F., Zou, L.W., Lio, P., Hui, P. (2023). An LTE authentication and key agreement protocol based on the ECC self-certified public key. IEEE/ACM Transactions on Networking, 31(3): 1101-1116. https://doi.org/10.1109/TNET.2022.3207360

[9] Fei, T., Wang, W.Y. (2023). The vulnerability and enhancement of AKA protocol for mobile authentication

in LTE/5G networks. Computer Networks, 228: 109685. https://doi.org/10.1016/j.comnet.2023.109685
[10] Chen, Y., Chang, T., Liu, W. (2023). Improved SRP algorithm and bidirectional heterogeneous LTE-R authentication key. IET Communications, 17(11): 1300-1309. https://doi.org/10.1049/cmu2.12624
[11] Krishna Jyothi, K., Chaudhari, S. (2022). A secure cluster-based authentication and key management protocol for machine-type communication in the LTE network. International Journal of Computers and Applications, 44(12): 1150-1160. https://doi.org/10.1080/1206212X.2019.1693000
[12] Krishna Jyothi, K., Chaudhari, S. (2020). A novel blockchain-based cluster head authentication protocol for machine-type communication in LTE network: Statistical analysis on attack detection. Journal of King Saud University-Computer and Information Sciences, 34(6): 3713-3721. https://doi.org/10.1016/j.jksuci.2020.08.014
[13] Jyothi, K.K., Chaudhari, S. (2020). Optimized neural network model for attack detection in LTE network. Computers and Electrical Engineering, 88: 106879. https://doi.org/10.1016/j.compeleceng.2020.106879
[14] Liu, G., Yan, Z., Feng, W., Jing, X.Y., Chen, Y.X., Atiquzzaman, M. (2021). SeDID: An SGX-enabled decentralized intrusion detection framework for network trust evaluation. Information Fusion, 70: 100-114. https://doi.org/10.1016/j.inffus.2021.01.003
[15] Rao, A.S.V., Roy, P.K., Amgoth, T., Bhattacharya, A. (2024). A deep learning-based authentication protocol for IoT-enabled LTE systems. Future Generation Computer Systems, 154: 451-464. https://doi.org/10.1016/j.future.2024.01.014
[16] Divakaran, J., Chakrapani, A., Srihari, K. (2023). Fuzzy logic based handover authentication in 5G telecommunication heterogeneous networks. Computer Systems Science and Engineering, 46(1): 1141-1152. https://doi.org/10.32604/csse.2023.028050
[17] Sodhro, A.H., Awad, A.I., van de Beek, J., Nikolakopoulos, G. (2022). Intelligent authentication of 5G healthcare devices: A survey. Internet of Things, 20: 100610. https://doi.org/10.1016/j.iot.2022.100610
[18] Xu, S., Yang, S., Zhang, K.F. (2023). Formal analysis of SA-TEK 3-way handshake protocols. Journal of Shanghai Jiaotong University (Science), 28(6): 753-762. https://doi.org/10.1007/s12204-021-2340-2
[19] Saxena, N., Grijalva, S., Chaudhari, N.S. (2016). Authentication protocol for an IoT-enabled LTE network. ACM Transactions on Internet Technology, 16(4): 1-20. https://doi.org/10.1145/2981547
[20] Cao, J., Li, H., Ma, M., Li, F.H. (2018). UPPGHA: Uniform privacy preservation group handover authentication mechanism for mMTC in LTE-A networks. Security and Communication Networks, 2018: 6854612. https://doi.org/10.1155/2018/6854612
[21] Gupta, S., Parne, B.L., Chaudhari, N.S. (2021). ISAG: IoT-enabled and secrecy aware group-based handover scheme for e-health services in M2M communication network. Future Generation Computer Systems, 125: 168-187. https://doi.org/10.1016/j.future.2021.06.038
[22] Roy, P.K., Sahu, P., Bhattacharya, A. (2022). FastHand: A fast handover authentication protocol for densely deployed small-cell networks. Journal of Network and Computer Applications, 206: 103435. https://doi.org/10.1016/j.jnca.2022.103435
[23] Mobarhan, M.A., Salamah, M. (2022). REPS-AKA3: A secure authentication and re-authentication protocol for LTE networks. Journal of Network and Computer Applications, 201: 103345. https://doi.org/10.1016/j.jnca.2022.103345
[24] Mobarhan, M.A., Salamah, M. (2023). REPS-AKA5: A robust group-based authentication protocol for IoT applications in LTE system. Internet of Things, 22: 100700. https://doi.org/10.1016/j.iot.2023.100700
[25] Bai, L., Zhu, L., Liu, J.W., Choi, J.H., Zhang, W. (2020). Physical layer authentication in wireless communication networks: A survey. Journal of Communications and Information Networks, 5(3): 237-264. https://doi.org/10.23919/JCIN.2020.9200889
[26] Xie, N., Li, Z.Y., Tan, H.J. (2021). A survey of physical-layer authentication in wireless communications. IEEE Communications Surveys and Tutorials, 23(1): 282-310. https://doi.org/10.1109/COMST.2020.3042188
[27] Braeken, A. (2018). PUF based authentication protocol for IoT. Symmetry, 10(8): 352. https://doi.org/10.3390/sym10080352
[28] Lee, S.W., Safkhani, M., Le, Q., et al. (2023). Designing secure PUF-based authentication protocols for constrained environments. Scientific Reports, 13(1): 21702. https://doi.org/10.1038/s41598-023-48464-z
[29] Zerrouki, F., Ouchani, S., Bouarfa, H. (2023). T2S-MAKEP and T2T-MAKEP: A PUF-based mutual authentication and key exchange protocol for IoT devices. Internet of Things, 24: 100953. https://doi.org/10.1016/j.iot.2023.100953
[30] Salahdine, F., Han, T., Zhang, N. (2023). Security in 5G and beyond recent advances and future challenges. Security and Privacy, 6(1): e271. https://doi.org/10.1002/spy2.271
[31] Asif, M., Aziz, Z., Bin Ahmad, M., Khalid, A., Waris, H. A., Gilani, A. (2022). Blockchain-based authentication and trust management mechanism for smart cities. Sensors, 22(7): 2604. https://doi.org/10.3390/s22072604
[32] Ullah, S., Zheng, J.B., Hussain, M.T., Din, N., Ullah, F., Farooq, M.U. (2022). A perspective trend of hyperelliptic curve cryptosystem for lighted weighted environments. Journal of Information Security and Applications, 70: 103346. https://doi.org/10.1016/j.jisa.2022.103346
[33] 3rd Generation Partnership Project (3GPP). (2020). 3GPP TS 33.401 V16.4.0: 3GPP System Architecture Evolution (SAE); Security Architecture. ETSI Technical Specification, 2020, pp. 1-173. https://www.etsi.org/deliver/etsi_ts/133400_133499/133401/16.04.00_60/ts_133401v160400p.pdf.
[34] Tsay, J.K., Mjølsnes, S.F. (2012). A vulnerability in UMTS and LTE authentication and key agreement protocols. Computer Network Security, 65-76. https://doi.org/10.1007/978-3-642-33704-8_6
[35] Ben Henda, N., Norrman, K. (2014). Formal analysis of security procedures in LTE: A feasibility study. In Research in Attacks, Intrusions and Defenses. RAID 2014. Lecture Notes in Computer Science, pp. 341-361. https://doi.org/10.1007/978-3-319-11379-1_17
[36] Blanchet, B. (2008). A computationally sound mechanized prover for security protocols. IEEE Transactions on Dependable and Secure Computing, 5(4): 193-207. https://doi.org/10.1109/TDSC.2007.1005

[37] Basin, D., Cremers, C., Dreier, J., Sasse, R. (2017). Symbolically analyzing security protocols using Tamarin. ACM SIGLOG News, 4(4): 19-30. https://doi.org/10.1145/3157831.3157835

[38] Sagar, D., Saidireddy, M. (2024). A novel secured authentication model for LTE network system using BD-POA-HECC, HD-MAC, and PD-3WHP techniques. Expert Systems with Applications, 258: 124967. https://doi.org/10.1016/j.eswa.2024.124967

[39] Bernstein, D.J. (2006). Curve25519: New Diffie-Hellman speed records. In Public Key Cryptography-PKC 2006, pp. 207-228. https://doi.org/10.1007/11745853_14

[40] Bernstein, D.J., Duif, N., Lange, T., Schwabe, P., Yang, B.Y. (2012). High-speed high-security signatures. Journal of Cryptographic Engineering, 2(2): 77-89. https://doi.org/10.1007/s13389-012-0027-1

[41] Krawczyk, H. (2010). Cryptographic extraction and key derivation: The HKDF scheme. In Advances in Cryptology-CRYPTO 2010, pp. 631-648. https://doi.org/10.1007/978-3-642-14623-7_34