



AMI-SMPA: Secure Authentication for Advanced Metering Infrastructure in Networked Electric-Vehicle Charging Systems

Haewon Byeon ^{*}

Department of Future Technology, Korea University of Technology and Education (KOREA TECH), 31253 Cheonan, South Korea

* Correspondence: Haewon Byeon (bhwpuma@naver.com)

Received: 08-28-2026

Revised: 09-09-2026

Accepted: 09-14-2026

Citation: H. Byeon, “AMI-SMPA: Secure authentication for advanced metering infrastructure in networked electric-vehicle charging systems,” *Mechatron. Intell Transp. Syst.*, vol. 5, no. 4, pp. 272–286, 2026. <https://doi.org/10.56578/mits050401>.



© 2026 by the author(s). Published by Acadlore Publishing Services Limited, Hong Kong. This article is available for free download and can be reused and cited, provided that the original published version is credited, under the CC BY 4.0 license.

Abstract: Networked electric-vehicle (EV) charging increasingly depends on advanced metering infrastructure (AMI) for charging authorization, metered-energy reporting, and demand-response control, making authenticated key establishment a safety-relevant communication requirement. This study reconstructs the security-relevant equations of a recently developed elliptic-curve multi-phase authentication protocol and evaluates whether its claimed properties follow from the specified algebra. Six structural weaknesses are identified: reversible exposure of the infrastructure private-key term, long-term key disclosure through the proposed signature equation, replay susceptibility inside the timestamp window, lack of binding between authentication and ephemeral Diffie-Hellman values, dual session-key definitions, and static-identity linkability. Advanced Metering Infrastructure–Secure Multi-Phase Authentication (AMI-SMPA) is designed with signed credentials, transcript-bound ephemeral elliptic-curve Diffie-Hellman, Hash-based Message Authentication Code (HMAC)-based Extract-and-Expand Key Derivation Function (HKDF), role-separated HMAC key confirmation, Advanced Encryption Standard in Galois/Counter Mode (AES-GCM), rotating aliases, and replay-aware state. The protocol is mapped to the EV, EV supply equipment, charging-station controller, smart meter (SM), data concentrator, and utility control center (UCC); it protects station-meter-to-utility metering and charging-control messages without replacing ISO 15118. In an isolated emulator, all four reconstructed attack conditions succeeded in 1,000/1,000 trials, whereas all corresponding AMI-SMPA checks succeeded in 1,000/1,000 trials. A controlled 1,000-run profile estimated 16.92 ms computation time, 19.35 ms end-to-end latency, 612 bytes/session, 4.35 mJ/session, 99.14% packet-delivery ratio, 98.77% replay detection, 98.76% unauthorized message-modification rejection (UMR), and 97.63% key-compromise containment. A fixed-seed, all-at-once EV charging burst model for 50, 200, and 1,000 charging points yielded 60.36–60.46 completed sessions/s, with queue-inclusive mean completion time rising from 423.69 to 8,279.05 ms. These controlled results support protocol-level feasibility and expose capacity-planning requirements; they do not establish operational-network performance or power-grid stability.

Keywords: Advanced metering infrastructure; Authenticated key exchange; Electric vehicle charging; Electric-vehicle supply equipment; Formal security analysis; Replay protection; Smart meter security

1 Introduction

Advanced metering infrastructure (AMI) is a central communication layer of the modern smart grid because it connects smart meters (SMs), data concentrators, utility head-end systems, and control applications through bidirectional digital networks. National Institute of Standards and Technology (NIST) guidance treats AMI as a cybersecurity-sensitive smart-grid domain and emphasizes risk-based protection across the entire communications path [1]. Early AMI security analysis likewise showed that remote connect/disconnect, metering, and control functions create consequences that cannot be addressed by encryption alone [2]. Broader surveys have subsequently highlighted confidentiality, integrity, availability, authentication, key management, and resilience as interacting requirements rather than independent controls [3].

The security problem is intensified by the fact that SMs are long-lived cyber-physical endpoints. A compromised or weakly authenticated meter can affect billing, demand response, load management, and operational decision-

making, while high-frequency metering data can reveal behavioral information about occupants. McDaniel and McLaughlin [4] identified this coupling of operational security and privacy at an early stage of smart-grid deployment, and Metke and Ekl [5] emphasized scalable public-key and trusted-computing mechanisms for wide-area smart-grid networks. These observations remain relevant because modern AMI increasingly interacts with distributed energy resources and electric-vehicle (EV) charging ecosystems.

A substantial authentication literature has therefore focused on lightweight key establishment for constrained SMs. Garg et al. [6] proposed an elliptic curve cryptography (ECC)-oriented lightweight mutual-authentication scheme for smart metering infrastructure (SMI) with reduced communication and energy overhead. Hasan et al. [7] later presented the lightweight identity-based key-agreement protocol (LIKA), emphasizing computation and communication efficiency in AMI. Hu et al. [8] developed a provably secure ECC-based authentication and key-agreement scheme for AMI and combined formal analysis with a practical Raspberry Pi testbed. Zhang et al. [9] further addressed anonymity and forward secrecy in a lightweight ECC-based smart-grid protocol, while Wang et al. [10] studied provable ECC-based authenticated key agreement in a cloud-edge-end smart-grid architecture.

Recent work also reflects the movement from purely cryptographic protocol design toward deployment-aware security. Parvez et al. [11] combined authentication management and anomaly-oriented packet validation for smart-grid data security. Pei et al. [12] integrated anonymous authentication and blockchain-based aggregation for AMI. Gormus et al. [13] implemented end-to-end object security over a 6TiSCH-oriented AMI architecture and examined reliability under constrained networking. Li et al. [14] proposed a resource-efficient authenticated-key-agreement construction using lightweight authenticated encryption for smart-grid devices. Together, these studies show that contemporary AMI security research increasingly evaluates both security properties and operational cost.

Earlier smart-grid authentication research also established several design principles used in the present study. Fouda et al. [15] demonstrated lightweight message authentication and Diffie-Hellman-based session establishment for smart-grid communications. Nicanfar et al. [16] addressed mutual authentication and key management at smart-grid scale. Tsai and Lo [17] investigated anonymous key distribution, and He et al. [18] reduced the cost of anonymous ECC-based key distribution. Chim et al. [19] used pseudo-identities to reduce linkability in a privacy-preserving authentication scheme, while Efthymiou and Kalogridis [20] showed that high-frequency SM data can expose household behavior unless identity and usage data are carefully separated.

Against this background, the present study focuses on the recently published Secure Multi-Phase Authentication Protocol for Cloud Infrastructure (SMPA-CI) using ECC [21]. The protocol is attractive as an analysis target because it explicitly claims the use of ECC, Elliptic Curve Digital Signature Algorithm (ECDSA)/Elliptic Curve Diffie-Hellman (ECDH)-oriented mechanisms, mutual authentication, replay resistance, impersonation resistance, man-in-the-middle resistance, and low overhead. However, those claims must be evaluated against the actual equations in the registration, login, user-authentication, system-authentication, and secure-key-exchange algorithms. The core research question is therefore whether the specified algebra genuinely provides the security properties associated with the named cryptographic primitives, and, if not, how the multi-phase design can be rebuilt as an authenticated key-exchange protocol for AMI.

The redesign is grounded in standardized cryptographic composition. Digital signatures are aligned with the Digital Signature Standard [22] and approved elliptic-curve domain parameters [23]; pairwise key establishment follows discrete-logarithm guidance that explicitly covers ECDH and key confirmation [24]. Session keys are derived through Hash-based Message Authentication Code (HMAC)-based Extract-and-Expand Key Derivation Function (HKDF) [25], and telemetry protection uses Advanced Encryption Standard in Galois/Counter Mode (AES-GCM) authenticated encryption [26]. The adversarial communication model follows the classical Dolev-Yao abstraction [27], while the computational security discussion draws on the Canetti-Krawczyk authenticated-key-exchange framework [28] and the stronger extended Canetti-Krawczyk (eCK)-style adversary model introduced by LaMacchia et al. [29]. ProVerif is used as the target symbolic specification language because it supports secrecy and correspondence properties for security protocols [30]. Finally, the electric-mobility relevance is framed against ISO 15118-20 vehicle-to-grid communication requirements [31] and the broader EV security and privacy landscape summarized by Brighente et al. [32].

In public EV charging, the electric vehicle–electric vehicle supply equipment (EV–EVSE) exchange, charging-station controller, revenue-grade meter, and utility backend form adjacent but distinct trust domains. A compromise in station-meter-to-utility authentication can alter authorization status, tariff or demand-response instructions, or the integrity and attribution of metered-energy reports even when the EV–EVSE protocol operates correctly. Prior work has characterized charging-station attack surfaces from both grid and station perspectives [33, 34], while authenticated key agreement and privacy-preserving authentication studies have addressed vehicle-to-grid communication [35, 36]. Accordingly, this paper frames Advanced Metering Infrastructure–Secure Multi-Phase Authentication (AMI-SMPA) as a secure communication mechanism for the meter/utility control center (UCC) link supporting networked charging services, not as an independent controller of traffic flow, power flow, or grid stability.

The study makes five contributions. First, it reconstructs the security-critical equations of SMPA-CI and

maps them to SM/UCC communication without silently correcting the original algebra. Second, it derives six vulnerabilities and validates four in an isolated emulator. Third, it proposes AMI-SMPA, which replaces reversible key masking with standard signatures, authenticates ephemeral ECDH values in a complete transcript, uses one authoritative HKDF schedule, and adds explicit key confirmation and replay state. Fourth, it defines the AMI-SMPA execution boundary and trust responsibilities across the EV, EVSE, charging-station controller, SM, data concentrator unit (DCU), and UCC. Fifth, it separates functional, calculated, and simulated evidence and adds a fixed-seed charging-point burst scenario to quantify queueing behavior at 50, 200, and 1,000 endpoints.

2 Methodology

2.1 System Model and Advanced Metering Infrastructure Mapping

The extended system model contains an EV, EVSE, a charging-station controller, a revenue-grade SM, a DCU, a UCC, and an adversary. The EV and EVSE remain in the ISO 15118 trust domain. The station controller coordinates connectors, local tariff presentation, and demand-response actions but does not hold the meter's signing key. AMI-SMPA executes between the SM (or its tamper-resistant station security gateway) and the UCC. It protects charging authorization status, metered-energy reports, and utility charging-control messages across the SM-DCU-UCC path. The DCU is a semi-trusted relay that may aggregate routing metadata, rate-limit bursts, and cache replay identifiers but cannot terminate the end-to-end protected payload. The UCC is the trusted authority for credential lifecycle, billing/control processing, policy epochs, and audit; the adversary controls the network but not an uncompromised UCC.

The original SMPA-CI user is mapped to the SM endpoint and the CI to the UCC. A password/token-oriented registration value is interpreted as a managed bootstrap credential issued during manufacturing, commissioning, or utility enrollment. The user key pair becomes the meter long-term signing key pair, and the infrastructure key pair becomes the UCC authentication key pair. The derived application keys protect the station-meter-to-utility metering and charging-control flow. Figure 1 makes this protection boundary explicit and distinguishes it from the EV-EVSE and station-management protocols.

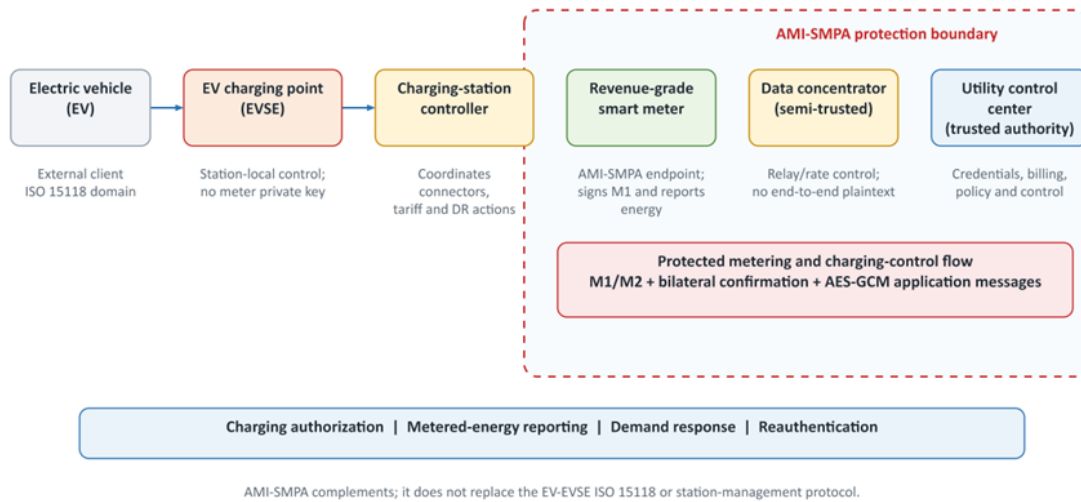


Figure 1. AMI-SMPA protection boundary and trust roles in a networked EV charging system

Note: AMI-SMPA—Advanced Metering Infrastructure–Secure Multi-Phase Authentication; EV—electric vehicle; EVSE—electric vehicle supply equipment; AES-GCM—Advanced Encryption Standard in Galois/Counter Mode; M1/M2—handshake messages.

2.2 Public Electric-Vehicle Charging Use Case

A public charging session begins when the EV and EVSE complete their local association and the station controller requests authorization. The station SM then establishes an AMI-SMPA session with the UCC, which returns authenticated authorization and policy context. During charging, cumulative and interval energy values are sent as AES-GCM-protected metered-energy reports bound to the session identifier (SID), message type, policy epoch, and monotonic sequence number. Utility charging or demand-response instructions follow the reverse protected path and are accepted only after origin, freshness, and policy validation. After a communication or power interruption, the meter discards the prior ephemeral state, generates a new ephemeral scalar, nonce, and SID, and performs full reauthentication before reporting or control resumes.

In this workflow, replay can duplicate an old authorization, energy report, or control instruction; endpoint impersonation can misattribute consumption or cause an unauthorized station action; and disclosure of an endpoint long-term key can enable future impersonation of that endpoint. AMI-SMPA's signed ephemeral transcript, explicit confirmation, and replay state address the first two conditions and contain a single-meter compromise. Forward secrecy is limited to completed sessions whose ephemeral scalars were erased and not revealed: later disclosure of the meter signing key does not reconstruct the past ECDH secret, but compromise during an active session remains outside that guarantee.

2.3 Threat Model and Security Objectives

The network adversary can observe, delay, suppress, duplicate, replay, reorder, and modify messages; initiate concurrent sessions; and impersonate unverified network peers. A device-compromise adversary may obtain the long-term credentials of one SM. For forward-secrecy analysis, disclosure of a long-term key is also considered after completion of a target session. The adversary is not assumed to solve the elliptic-curve discrete logarithm problem, forge a secure signature without the signing key, distinguish HKDF output from pseudorandom keying material under its assumed security properties, or recover AES-GCM plaintext without the corresponding data key.

The required security properties are mutual authentication, session-key secrecy, replay resistance, explicit key confirmation, resistance to transcript substitution and cross-session key confusion, forward secrecy for completed sessions whose ephemeral secrets remain unrevealed, containment of a single-meter compromise, reduced static-identity exposure, and authenticated confidentiality of metering/control messages. Cryptographic integrity is not interpreted as physical truthfulness: a fully compromised meter may generate a semantically false but correctly authenticated reading, which is outside the unauthorized message-modification rejection (UMR) metric evaluated here.

2.4 Exact Protocol Reconstruction

The reconstruction follows the published Algorithm 2–6 equations without replacing nonstandard operations with the standard primitives named in the surrounding prose. Table 1 summarizes the security-relevant equations and their AMI interpretation.

Table 1. Reconstruction of security-relevant SMPA-CI equations and AMI interpretation

Phase	Specified Operation	AMI Interpretation	Security Observation
Registration	$PK_U = SK_U \times F$	Long-term meter public key	Conventional EC public-key relation
Registration	$SIT_U = HAF1(ID_U \parallel PW_U \parallel PK_U) \text{ XOR } PVK_{CI}$	Meter identity token	Infrastructure private-key term appears in a reversible token
Login	$LR_U = HAF1(ID_U \parallel PW_U \parallel PK_U \parallel T) \text{ XOR } SIT_U$	Login authenticator	Timestamp freshness without independent uniqueness state
Login	$SK_{\text{session}} = HAF2(ID_U \parallel T_U \parallel PVK_{CI} \parallel T)$	Login-stage session key	Independent of later ECDH key schedule
User authentication	$DSig_U = HAF1(ID_U \parallel T) \text{ XOR } SK_U$	Meter authentication value	Does not instantiate standard ECDSA signing algebra
System authentication	$DSig_{CI} = HAF1(ID_{CI} \parallel T) \text{ XOR } SK_{CI}$	UCC authentication value	Same reversible structure
Key exchange	$PK_{\text{temp}} = SK_{\text{temp}} \times G ; PK_{CI} \text{ temp} = SK_{CI} \text{ temp} \times G$	Ephemeral ECDH values	Not included in the earlier authenticated transcript
Key exchange	$SK_{\text{session}} = HAF2(\text{Shared})$	ECDH-derived session key	Creates a second session-key definition

Note: SMPA-CI—Secure Multi-Phase Authentication Protocol for Cloud Infrastructure; AMI—advanced metering infrastructure; EC—elliptic curve; ECDH—elliptic curve Diffie–Hellman; ECDSA—elliptic curve digital signature algorithm; UCC—utility control center; CI—cloud infrastructure; PK—public key; SK and PVK—secret/private key; ID—identity; PW—password; SIT—signed identity token; HAF1/HAF2—source-protocol one-way hash functions 1/2; LR—login request; DSig—digital-signature value as named in the source protocol; XOR—exclusive OR; T—timestamp. Subscripts U, CI, temp, and session denote the user, cloud infrastructure, ephemeral value, and session; F and G are EC base points; Shared is the ECDH shared secret; $\parallel$ denotes concatenation.

2.5 Vulnerability Derivation

The first vulnerability follows directly from the signed-identity-token equation:

$$\text{SIT_U} = \text{HAF1}(\text{ID_U} \parallel \text{PW_U} \parallel \text{PK_U}) \text{XOR PVK_CI} \quad (1)$$

A registered endpoint knows its own identity, password/bootstrap credential, public key, and issued token. Because exclusive OR (XOR) is reversible, the infrastructure private-key term is algebraically isolated as:

$$\text{PVK_CI} = \text{SIT_U} \text{XOR} \text{HAF1}(\text{ID_U} \parallel \text{PW_U} \parallel \text{PK_U}) \quad (2)$$

The second vulnerability follows from the proposed user-authentication value:

$$\text{DSig_U} = \text{HAF1}(\text{ID_U} \parallel \text{T}) \text{XOR SK_U} \quad (3)$$

The public transcript contains ID_U, T, and DSig_U, allowing the private-key term to be isolated:

$$\text{SK_U} = \text{DSig_U} \text{XOR} \text{HAF1}(\text{ID_U} \parallel \text{T}) \quad (4)$$

The system-authentication equation has the same structure. These observations are algebraic consequences of the protocol definition rather than attacks on ECC itself. They also explain why describing the construction as an ECDSA signature does not automatically provide the EUF-CMA security expected from a standardized signature algorithm.

The third vulnerability concerns replay. The login request includes a timestamp, but the reconstructed Algorithms 3–5 do not include an independent nonce, monotonic sequence number, or replay-cache identifier. If a receiver accepts any message for which $|T_{\text{receive}} - T_{\text{message}}| \leq \Delta t$, then two identical messages can both be fresh during the same acceptance interval. The fourth vulnerability concerns ECDH authentication: the ephemeral public keys are exchanged after identity authentication but are not included in the authenticated transcript. Figure 2 depicts this cryptographic discontinuity.

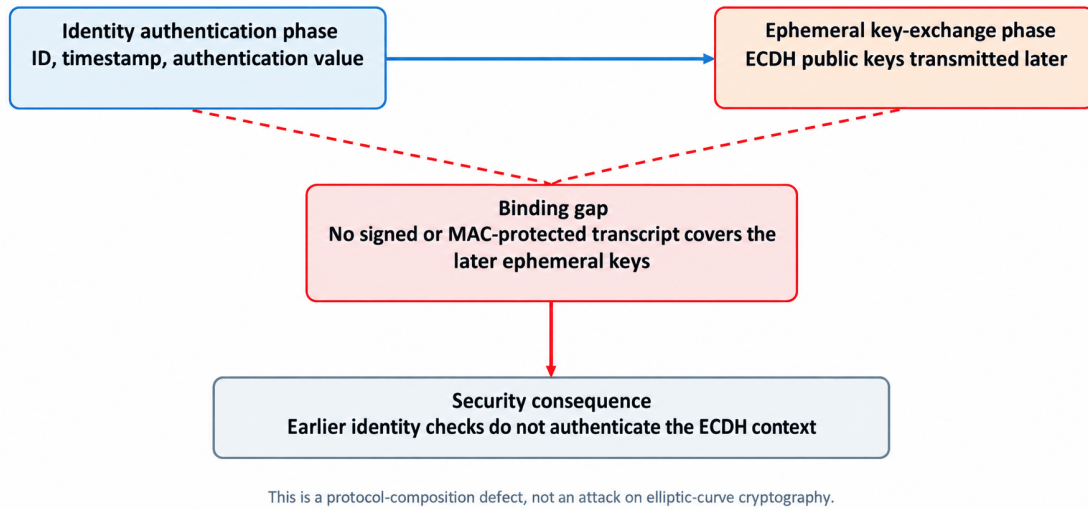


Figure 2. Security discontinuity between identity authentication and the unbound ephemeral key exchange

Note: ID—identity; ECDH—elliptic curve Diffie–Hellman; MAC—message authentication code.

The fifth vulnerability is key-state ambiguity. The login phase defines one session key using identity, token/infrastructure material, and timestamp, while the later key-exchange phase defines another session key from ECDH. The protocol does not specify a unique transition rule that determines which key protects application traffic or when the earlier key is retired. The sixth vulnerability is privacy-related: registration and authentication repeatedly transmit static identity and public-key information, enabling long-term linkability even if later payloads are encrypted. The six vulnerabilities and their AMI consequences are summarized in Table 2.

2.6 Advanced Metering Infrastructure–Secure Multi-Phase Authentication Design

AMI-SMPA preserves the multi-phase organization but replaces the unsafe cryptographic composition. During initialization, the UCC provisions approved EC parameters, a trust root, algorithm identifiers, credential validity,

Table 2. Identified vulnerabilities and their AMI consequences

ID	Vulnerability	Required Capability	Principal AMI Consequence
V1	Infrastructure key embedded in XOR token	One legitimate/compromised endpoint	Utility trust-root exposure
V2	Long-term key recoverable from signature equation	Passive transcript observation	Meter/UCC credential compromise
V3	Timestamp-only replay protection	Capture and resend inside freshness window	Duplicate or stale request acceptance
V4	Unbound ephemeral ECDH values	Network-field modification	Loss of authenticated key agreement
V5	Two session-key definitions	State ambiguity or later key compromise	Key confusion and weakened PFS reasoning
V6	Static identity exposure	Passive traffic correlation	Long-term meter/EV-use linkability

Note: ID—identity; AMI—advanced metering infrastructure; XOR—exclusive OR; UCC—utility control center; ECDH—elliptic curve Diffie–Hellman; PFS—perfect forward secrecy; EV—electric vehicle.

policy epoch, alias-rotation policy, and replay-state rules. Each meter holds a long-term signing key pair (SK_SM, PK_SM); the UCC holds (SK_UCC, PK_UCC). Private keys are never used as reversible masking values. Subscripts SM and UCC identify the SM and UCC; SK_SM and SK_UCC are long-term signing keys, PK_SM and PK_UCC are their public keys, and unindexed SK denotes the session secret.

During controlled registration, the UCC validates the manufacturing/commissioning credential and issues a signed identity token binding the meter identity, public key, device class, expiry, and credential epoch. A rotating alias can be used on the network while the UCC retains the accountability mapping.

$$\text{SIT_SM} = \text{Sign_SK_UCC}(\text{H}(\text{ID_SM} \parallel \text{PK_SM} \parallel \text{Device Class} \parallel \text{Expiry} \parallel \text{Credential Epoch})) \quad (5)$$

For a new session, the meter samples an ephemeral scalar a , a nonce N_SM , and a fresh SID, and computes $A_SM = aG$. Message $M1$ contains the rotating alias, A_SM , N_SM , timestamp, SID, and credential epoch and is signed with the meter long-term signing key. The UCC validates credential state, freshness, alias status, and the meter signature, samples b and N_UCC , computes $B_UCC = bG$, and signs a response $M2$ that covers $M1$ and the UCC ephemeral key. Figure 3 shows the complete message sequence.

Both parties compute $Z = abG$. The complete transcript digest TR covers $M1$, the meter signature, $M2$, and the UCC signature. The authoritative session secret is then derived from the ECDH result and the authenticated context:

$$\text{SK} = \text{HKDF}(Z, \text{TR} \parallel N_SM \parallel N_UCC \parallel \text{SID} \parallel \text{Policy Epoch}) \quad (6)$$

Independent authentication and data keys are derived using HKDF-Expand, the domain-separated expansion step of HKDF [25], rather than a separate key-derivation primitive. The expanded output is split into K_auth and K_data ; L_auth and L_data denote their lengths in bytes:

$$K_auth \parallel K_data = \text{HKDF-Expand}(\text{SK}, \text{“AMI-key-separation”}, L_auth + L_data) \quad (7)$$

Explicit key confirmation is performed before application traffic is accepted:

$$\text{Auth_SM} = \text{HMAC_K_auth}(\text{“SM”} \parallel \text{TR}); \text{Auth_UCC} = \text{HMAC_K_auth}(\text{“UCC”} \parallel \text{TR}) \quad (8)$$

Telemetry and control messages are protected with AES-GCM. Associated data contains SID, sequence number, message type, and policy epoch. The UCC maintains authoritative replay state, while the DCU may maintain a coarse cache and rate-control state. This design binds identity, role, ephemeral key contributions, freshness, policy context, and the application key to one authenticated session transcript. In Eqs. (5)–(8), SIT_SM is the meter credential, Sign_SK_UCC denotes signing with SK_UCC, H is the hash function, TR is the authenticated transcript digest, N_SM/N_UCC are nonces, SID is the session identifier, PolicyEpoch is the current policy version, and Auth_SM/Auth_UCC are role-specific key-confirmation tags; $\parallel$ denotes concatenation.

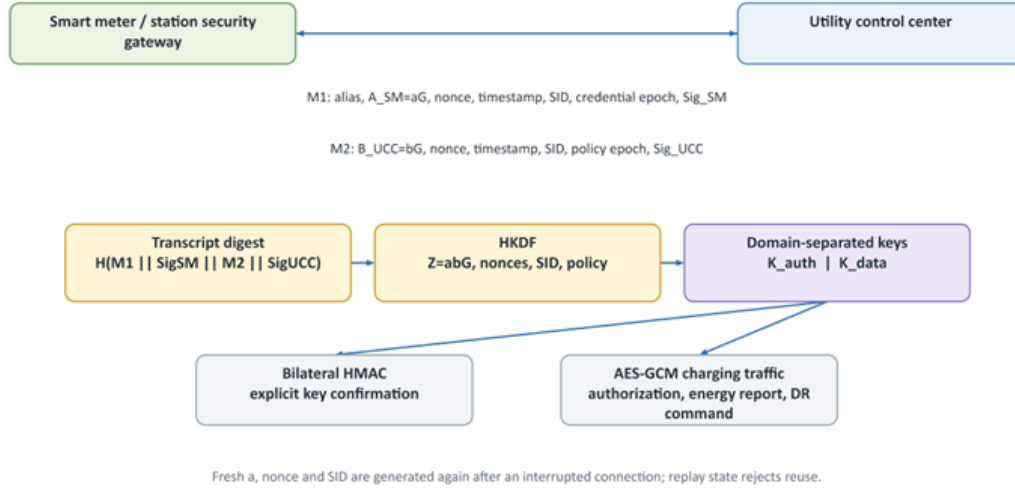


Figure 3. AMI-SMPA key-establishment sequence for metering and charging-control traffic

Note: AMI-SMPA—Advanced Metering Infrastructure—Secure Multi-Phase Authentication; SM—smart meter; UCC—utility control center; SID—session identifier; H—hash function; HKDF—HMAC-based Extract-and-Expand Key Derivation Function; HMAC—hash-based message authentication code; AES-GCM—Advanced Encryption Standard in Galois/Counter Mode; DR—demand response. M1/M2 are handshake messages; Sig_SM/SigSM and Sig_UCC/SigUCC denote the respective signatures; a/b are ephemeral scalars, G is the EC base point, A_{SM}/B_{UCC} are public contributions, Z is the shared secret, and K_{auth}/K_{data} are authentication/data keys; $\parallel$ denotes concatenation.

2.7 Formal Security Argument and Symbolic Specification

The security argument treats a fresh accepted session as one in which the peer long-term signing key is not compromised before authentication completes and the target ephemeral secret is not revealed during the session. Under these conditions, modification of an accepted ephemeral public key, nonce, SID, or policy epoch requires either forging an endpoint signature or presenting a transcript that fails verification. Because the HKDF input includes both the ECDH result and the transcript digest, cross-session substitution of any authenticated field changes the derived session context.

For an eCK-style adversary, the qualitative reduction is expressed as $\text{Adv}_A^{AKE} \leq \text{Adv}_{\text{ECDH}} + \text{Adv}_{\text{SIG}}^{\text{EUF-CMA}} + \text{Adv}_{\text{HKDF}}^{\text{PRF}} + q^2/2^\lambda$, where the terms represent the adversary's advantages against ECDH, the signature scheme, the KDF pseudorandomness assumption, and freshness collisions. The purpose of this bound is not to claim a concrete numerical security level; it identifies the primitive failures an adversary would need in order to distinguish a fresh AMI-SMPA session key.

A ProVerif model is supplied as a reproducibility artifact and defines queries for session-key/data secrecy and injective correspondence between SM/UCC start and accept events. The symbolic model was prepared but was not executed in the environment used to generate the present numerical results because ProVerif was not installed. Accordingly, this paper does not claim a tool-generated “no attack trace” result. The formal claims reported here are the equation-level derivations and the authenticated-key-exchange reduction argument. Figure 4 summarizes the analysis workflow.

2.8 Isolated Emulator and Performance Evaluation

Functional validation was conducted in an isolated protocol emulator using synthetic messages only; no operational utility, production meter, charging station, or public network was targeted. The measured emulator outcomes were the accept/reject or key-recovery counts from 1,000 trials per condition. The reconstructed conditions were recovery of the infrastructure-key term, recovery of the endpoint long-term-key term, replay inside a 30 s freshness window, and substitution of an unauthenticated ephemeral ECDH value. Corresponding AMI-SMPA checks measured rejection of an altered authenticated field, duplicate-session rejection, bilateral key confirmation, and acceptance of legitimate AES-GCM application messages.

A separate controlled simulation estimated resource-constrained behavior. Four profiles were evaluated for 1,000 Monte Carlo runs each: reconstructed SMPA-CI, AMI-SMPA, and two literature-informed synthetic configurations labeled ECC-AKA-1 and ECC-AKA-2. The latter are comparison profiles with greater signature/message overhead; they do not reproduce a named protocol or published hardware testbed. The pseudorandom seed was fixed at 20260828. Thus, the emulator counts are measured within the implemented logic, message size is deterministically calculated from serialization, energy is calculated from simulated operation times and component power, and latency,

throughput, reliability, and security-rate metrics are simulation outputs.

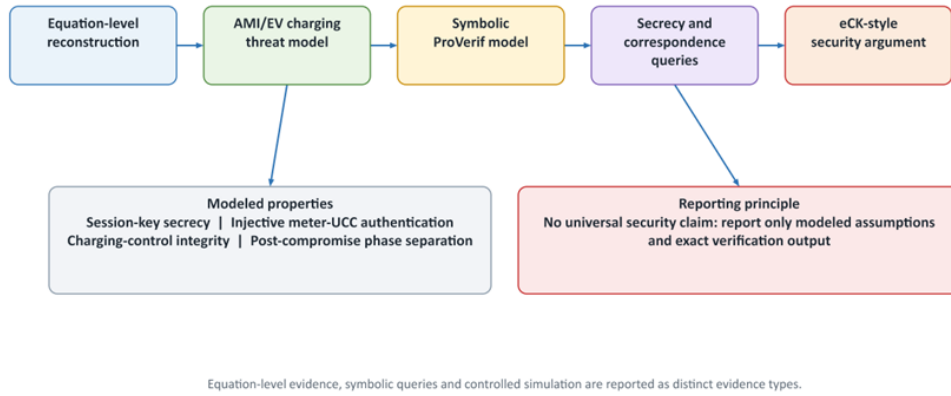


Figure 4. Formal security analysis and reproducibility workflow for the AMI/EV charging mapping

Note: AMI—advanced metering infrastructure; EV—electric vehicle; eCK-style security argument—extended Canetti–Krawczyk-style security argument; UCC—utility control center.

The metrics were authentication computation time, end-to-end latency, communication bytes/session, energy/session, throughput, PDR, replay detection, UMR, and key-compromise containment (KCC). Energy was calculated as $E_{\text{session}} = \sum(P_j t_j)$. Communication cost sums serialized EC points, signatures, nonces, aliases, timestamps, SIDs, policy metadata, and tags (612 bytes for AMI-SMPA). $UMR = 100 \times N_{\text{rejected_unauthorized}}/N_{\text{injected_unauthorized}}$, where unauthorized trials modify or inject protected messages without a valid K_{data} ; it does not assess a semantically false reading signed by a compromised meter. In each KCC trial, one meter key is disclosed and $KCC = 100 \times (1 - N_{\text{affected_uncompromised}}/N_{\text{uncompromised}})$, where affected denotes an uncompromised identity/session that the adversary can successfully impersonate or derive under the modeled compromise rules.

Normality was evaluated using the Shapiro-Wilk test. Computation time, end-to-end latency, and throughput met the parametric criterion and were compared using one-way analysis of variance (ANOVA). Energy and PDR were compared using Kruskal-Wallis tests, as were replay detection, UMR, and KCC because of bounded/ceiling effects. Pairwise AMI-SMPA versus SMPA-CI comparisons used Welch’s t -test for normally distributed metrics and Mann-Whitney U tests otherwise. Cohen’s d and rank-biserial correlation were reported for pairwise comparisons; ANOVA used eta-squared (η^2), and Kruskal-Wallis tests used H-based eta-squared, $\eta^2_H = (H - k + 1)/(N - k)$, where H is the test statistic, $k = 4$ profiles, and $N = 4,000$ observations.

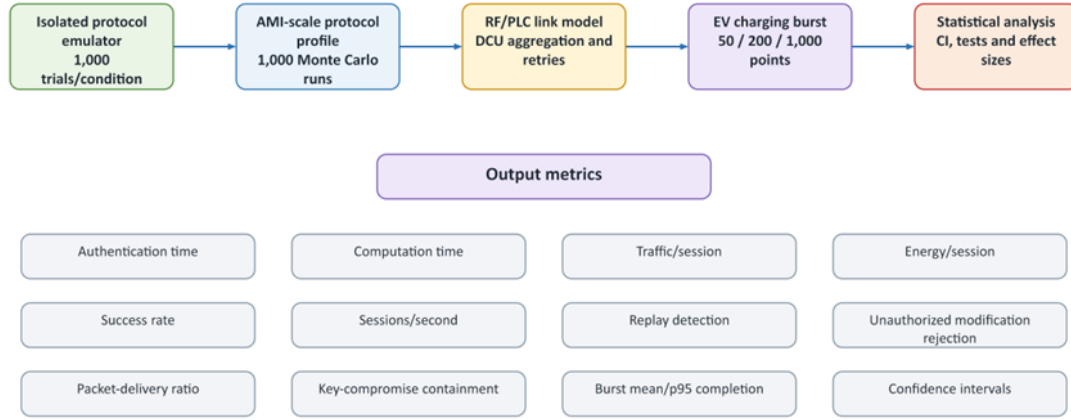
A second fixed-seed event-driven scenario examined simultaneous EV charging reauthentication. All 50, 200, or 1,000 charging points released one request at $t = 0$ to a single first-come-first-served verification worker. Service time followed a lower-bounded normal distribution with mean $1000/61 = 16.39$ ms and SD 0.91 ms; a non-bottleneck 2.43 ms network delay, 0.9914 per-attempt success probability, one retry, and 612 bytes/attempt were applied. Each size was repeated 1,000 times with seed 20260828. Queue-inclusive mean and p95 completion time, ultimate success, completed sessions/s, and traffic/session including retries were recorded. This is a worst-case authentication-queue stress model, not a traffic-flow or power-flow simulation. Figure 5 summarizes the experimental evaluation framework and EV charging burst scenario.

3 Results

3.1 Equation-Level Security Findings

The reconstruction produced six security findings summarized in Table 2. V1 and V2 are deterministic algebraic disclosures: the relevant long-term key terms can be isolated from values that are intentionally available to a registered endpoint or transmitted in the authentication transcript. V3 follows from the absence of a uniqueness state inside the timestamp acceptance interval. V4 follows from the fact that the later ephemeral public values are not covered by the earlier authentication transcript. V5 is a state-machine defect caused by the existence of two independently defined session keys, and V6 is a privacy inconsistency caused by repeated static identity exposure.

These findings do not depend on breaking ECC, reversing a cryptographic hash, or predicting a random nonce. They arise from protocol composition. Consequently, increasing the elliptic-curve key size alone would not correct them. The redesign must instead change how private keys, signatures, ephemeral public values, freshness information, and session-key derivation are connected. Table 3 compares the corresponding security properties of SMPA-CI and AMI-SMPA.



Measured emulator outcomes, deterministic serialization costs, calculated energy, and simulated performance are reported separately.

Figure 5. Experimental evaluation framework including the EV charging burst scenario

Note: AMI—advanced metering infrastructure; EV—electric vehicle; RF—radio frequency; PLC—power-line communication; DCU—data concentrator unit; CI—confidence interval; p95—95th percentile.

Table 3. Security-property comparison between reconstructed SMPA-CI and AMI-SMPA

Security Property	Reconstructed SMPA-CI	AMI-SMPA
Standard signature construction	No	Yes; standardized signature primitive
Infrastructure private-key isolation	No	Yes; private key never masked into endpoint token
Ephemeral-key authentication	No explicit binding	Signed transcript covers both ephemeral contributions
Session-key uniqueness	Two definitions	Single HKDF schedule
Explicit key confirmation	Not specified	Bilateral HMAC confirmation
Replay protection	Timestamp only	Nonce + SID + sequence state
Forward-secrecy-oriented establishment	Ambiguous	Ephemeral ECDH with long-term authentication
Key separation	Not specified	Independent K_auth and K_data
Authenticated data encryption	Not integrated	AES-GCM
Static identity minimization	No	Rotating alias supported

Note: SMPA-CI—Secure Multi-Phase Authentication Protocol for Cloud Infrastructure; AMI-SMPA—Advanced Metering Infrastructure—Secure Multi-Phase Authentication; HKDF—HMAC-based Extract-and-Expand Key Derivation Function; HMAC—hash-based message authentication code; SID—session identifier; ECDH—elliptic curve Diffie–Hellman; AES-GCM—Advanced Encryption Standard in Galois/Counter Mode; K_auth/K_data—authentication/data keys.

3.2 Isolated Proof-of-Concept Validation

All four reconstructed attack conditions succeeded in every injected trial. Specifically, the infrastructure key term was recovered from the token equation in 1,000/1,000 runs, the meter long-term key term was recovered from the proposed signature equation in 1,000/1,000 runs, a captured login request was accepted when replayed inside the configured freshness window in 1,000/1,000 runs, and the unauthenticated ECDH substitution condition was reproduced in 1,000/1,000 runs. These 100% rates reflect deterministic protocol equations and emulator acceptance logic rather than probabilistic cryptanalysis.

The corresponding AMI-SMPA mitigation mechanisms were validated through 1,000 independent functional trials per condition. Modification of either authenticated ephemeral-key contribution caused verification to fail in 1,000/1,000 trials. Reuse of a consumed session-initiation tuple was rejected in 1,000/1,000 trials. The SM and UCC derived identical keying material and verified bilateral role-separated HMAC values in all trials. Legitimate AES-GCM traffic generated with K_data was authenticated and decrypted in 1,000/1,000 trials, whereas an incorrect key or modified authenticated input was rejected. These are functional logic checks, not empirical proofs of cryptographic security; Table 4 summarizes the evidence.

Table 4. Isolated emulator validation results

Validation Item	Trials	Observed Result	Interpretation
SIT-based infrastructure-key recovery	1,000	1,000 successful (100%)	Deterministic disclosure in reconstructed equation
DSig-based user-key recovery	1,000	1,000 successful (100%)	Deterministic disclosure in reconstructed equation
Replay inside 30 s freshness window	1,000	1,000 accepted (100%)	Timestamp alone did not provide uniqueness
Unauthenticated ECDH substitution condition	1,000	1,000 reproduced (100%)	Ephemeral values were not transcript-bound
AMI-SMPA altered ephemeral field rejection	1,000	1,000 rejected (100%)	Signed transcript detected modification
AMI-SMPA duplicate session rejection	1,000	1,000 rejected (100%)	Replay cache enforced session uniqueness
AMI-SMPA bilateral key confirmation	1,000	1,000 valid (100%)	Peers derived matching authenticated context
AMI-SMPA AES-GCM legitimate telemetry	1,000	1,000 valid (100%)	Peer-derived data key protected payload

Note: SIT—signed identity token; DSig—digital-signature value as named in the reconstructed protocol; ECDH—elliptic curve Diffie–Hellman; AMI-SMPA—Advanced Metering Infrastructure–Secure Multi-Phase Authentication; AES-GCM—Advanced Encryption Standard in Galois/Counter Mode.

3.3 Simulation-Based Performance Results

Table 5 reports the 1,000-run controlled simulation profile. Reconstructed SMPA-CI had the lowest authentication computation time (10.77 ± 0.89 ms), as expected from its comparatively lightweight but insecure composition. AMI-SMPA required 16.92 ± 0.91 ms, an increase of 6.15 ms (57.1%) relative to SMPA-CI. Nevertheless, AMI-SMPA remained below the predefined 20 ms design target and was faster than ECC-AKA-1 (18.65 ± 0.91 ms) and ECC-AKA-2 (20.33 ± 0.91 ms). The 20 ms computation/latency and 5 mJ/session energy targets are study-selected engineering reference values, not requirements specified by ISO 15118 or another cited standard.

End-to-end authentication latency followed the same ordering. SMPA-CI required 14.59 ± 1.32 ms, whereas AMI-SMPA required 19.35 ± 1.35 ms (95% CI: 19.27–19.43 ms). The two reference profiles required 22.18 ± 1.30 and 24.03 ± 1.32 ms. Thus, the strengthened transcript authentication and explicit key confirmation added latency but did not push the modeled AMI-SMPA session beyond the 20 ms target.

Communication overhead increased from 356 bytes/session for SMPA-CI to 612 bytes/session for AMI-SMPA because the strengthened exchange carries authenticated ephemeral material, nonces, a SID, signatures, and explicit confirmation values. Even with this additional 256-byte cost, AMI-SMPA remained below ECC-AKA-1 (688 bytes) and ECC-AKA-2 (736 bytes). The increase is therefore a bounded cost of converting a loosely connected multi-phase flow into a transcript-bound authenticated key exchange.

Energy consumption showed the same security-performance trade-off. AMI-SMPA consumed 4.35 ± 0.32 mJ/session (95% CI: 4.33–4.37 mJ), compared with 2.91 ± 0.33 mJ for SMPA-CI. The modeled value remained below the 5 mJ/session design target and below ECC-AKA-1 (4.96 ± 0.31 mJ) and ECC-AKA-2 (5.47 ± 0.33 mJ). AMI-SMPA throughput was 61.00 ± 3.00 sessions/s versus 85.04 ± 3.08 sessions/s for SMPA-CI, but exceeded both reference profiles (55.48 ± 2.89 and 51.36 ± 3.06 sessions/s).

Reliability did not deteriorate under the larger handshake. AMI-SMPA achieved a mean PDR of $99.14 \pm 0.22\%$ (95% CI: 99.13–99.15%), compared with $98.80 \pm 0.22\%$ for SMPA-CI, $98.74 \pm 0.23\%$ for ECC-AKA-1, and $98.45 \pm 0.22\%$ for ECC-AKA-2. The improvement in the simulation profile reflects the assumed replay/state handling and bounded retransmission behavior rather than a claim that cryptography itself increases physical-layer reliability.

The largest gains were observed in security-oriented metrics. SMPA-CI detected $71.46 \pm 1.80\%$ of injected replay events, whereas AMI-SMPA achieved $98.77 \pm 0.81\%$; ECC-AKA-1 and ECC-AKA-2 achieved $96.34 \pm 1.65\%$ and $94.01 \pm 1.79\%$. UMR reached $98.76 \pm 0.81\%$ for AMI-SMPA, compared with $84.77 \pm 1.43\%$ for SMPA-CI. As defined in Section 2.8, this metric covers only modification/injection without a valid data key and not a physically false measurement produced by a fully compromised meter.

Key-compromise containment showed the strongest separation. The reconstructed SMPA-CI profile retained only $17.89 \pm 2.44\%$ containment after endpoint-key exposure because the reconstructed token/signature equations permit trust propagation beyond a single meter. AMI-SMPA reached $97.63 \pm 1.49\%$, compared with $94.39 \pm 2.38\%$ for ECC-AKA-1 and $91.24 \pm 2.43\%$ for ECC-AKA-2. This result is consistent with endpoint-specific long-term

credentials and ephemeral session establishment that do not embed a UCC master private key into a meter-accessible token.

Table 5. Controlled simulation-based performance and security results

Metric	SMPA-CI	AMI-SMPA	ECC-AKA-1	ECC-AKA-2
Authentication computation time (ms)	10.77 ± 0.89	16.92 ± 0.91	18.65 ± 0.91	20.33 ± 0.91
End-to-end latency (ms)	14.59 ± 1.32	19.35 ± 1.35	22.18 ± 1.30	24.03 ± 1.32
Communication cost (bytes/session)	356	612	688	736
Energy/session (mJ)	2.91 ± 0.33	4.35 ± 0.32	4.96 ± 0.31	5.47 ± 0.33
Throughput (sessions/s)	85.04 ± 3.08	61.00 ± 3.00	55.48 ± 2.89	51.36 ± 3.06
Packet-delivery ratio (%)	98.80 ± 0.22	99.14 ± 0.22	98.74 ± 0.23	98.45 ± 0.22
Replay detection (%)	71.46 ± 1.80	98.77 ± 0.81	96.34 ± 1.65	94.01 ± 1.79
UMR (%)	84.77 ± 1.43	98.76 ± 0.81	97.10 ± 1.27	95.60 ± 1.44
Key-compromise containment (%)	17.89 ± 2.44	97.63 ± 1.49	94.39 ± 2.38	91.24 ± 2.43

Note: SMPA-CI—Secure Multi-Phase Authentication Protocol for Cloud Infrastructure; AMI-SMPA—Advanced Metering Infrastructure—Secure Multi-Phase Authentication; ECC-AKA-1/ECC-AKA-2—elliptic curve cryptography-based authenticated key-agreement synthetic profiles 1/2; SD—standard deviation; UMR—unauthorized message-modification rejection. Values are mean ± SD from 1,000 controlled simulation runs per protocol profile. Communication cost is deterministic for the modeled serialized message format. ECC-AKA-1 and ECC-AKA-2 are literature-informed synthetic reference profiles and are not direct reproductions of a specific published hardware testbed. Replay detection, UMR, and key-compromise containment are empirical outputs of the simulation settings in Section 2.8, not intrinsic cryptographic success probabilities or security guarantees.

3.4 Electric-Vehicle Charging Burst Scenario

Table 6 reports the all-at-once charging-point scenario. Throughput remained close to the configured single-worker service capacity (60.36–60.46 sessions/s), and one permitted retry raised ultimate success above 99.99%. Queue-inclusive mean completion time increased from 423.69 ms for 50 points to 1,664.87 ms for 200 and 8,279.05 ms for 1,000; the corresponding mean p95 values were 787.96, 3,145.55, and 15,712.80 ms. Traffic including retries remained 616.92–617.43 bytes/session.

The near-constant service rate shows that cryptographic processing is stable, whereas completion time scales with the queue when every endpoint reconnects simultaneously. This result supports DCU/UCC admission control, staggered reconnect timers, or parallel verification workers for large charging sites. It does not demonstrate operational charging-network performance.

Table 6. Fixed-seed simultaneous EV charging authentication-burst results

Charging Points	Mean Completion (ms)	Mean p95 (ms)	Success (%)	Sessions/s	Traffic/Session (B)
50	423.69	787.96	99.9940	60.36	616.92
200	1,664.87	3,145.55	99.9945	60.42	617.43
1,000	8,279.05	15,712.80	99.9923	60.46	617.30

Note: EV—electric vehicle. Mean values across 1,000 replications per size; all requests arrive at $t = 0$. Completion time includes first-come-first-served (FCFS) queueing, service, and the modeled network delay. Traffic/session includes retries.

3.5 Statistical Analysis

The Shapiro-Wilk test supported normality for computation time, latency, and throughput in all four protocol groups ($p > 0.05$). One-way ANOVA therefore showed significant between-profile differences for authentication computation time ($F = 21,238.14$, $p < 0.001$, $\eta^2 = 0.941$), end-to-end latency ($F = 9,656.73$, $p < 0.001$, $\eta^2 = 0.879$), and throughput ($F = 25,103.81$, $p < 0.001$, $\eta^2 = 0.950$).

Energy consumption and PDR had at least one group that failed the normality criterion, so Kruskal-Wallis tests were used. Significant differences were observed for energy ($H = 3,423.91$, $p < 0.001$, H -based η -squared (η_H^2) = 0.856) and PDR ($H = 2,200.41$, $p < 0.001$, $\eta_H^2 = 0.550$). Replay detection, UMR, and KCC also differed significantly ($H = 3,360.32$, 3, 203.59, and 3,287.16; all $p < 0.001$), with η_H^2 values of 0.840, 0.801, and 0.822.

Pairwise AMI-SMPA versus SMPA-CI comparisons confirmed statistically distinguishable costs and security outcomes. Welch tests yielded Cohen's $d = 6.83$ for computation time and $d = 3.57$ for latency (both $p < 0.001$); energy also differed substantially (Mann-Whitney $U = 999,342$, $p < 0.001$; rank-biserial correlation = 0.999). Replay detection, UMR, and KCC favored AMI-SMPA with rank-biserial correlations of approximately 1.00 in the simulated profile.

4 Discussion

4.1 Interpretation of the Security Findings

The principal result is that protocol security cannot be inferred from the names of the primitives cited in a design. SMPA-CI is described using ECC, ECDSA, and ECDH terminology, yet the published equations use reversible XOR masking for values that are described as signatures or identity tokens. The resulting disclosures are therefore composition failures, not failures of ECC. This distinction is important for peer review and implementation because simply replacing curve parameters or increasing key size would leave V1 and V2 unchanged.

V4 illustrates a second general lesson: successful identity authentication in one phase does not automatically authenticate an ephemeral key sent later. Authenticated key exchange requires a cryptographic binding between the peer identity, role, fresh key contribution, and session context. AMI-SMPA creates this binding by signing M1/M2 and by feeding the authenticated transcript into HKDF. Explicit HMAC confirmation then demonstrates that both peers derived the same context-bound secret before data traffic is accepted.

The replay findings also show why freshness must be treated as a state-management property. Timestamps are useful for rejecting stale traffic, but a valid timestamp cannot prove that a message has not already been processed. The proposed use of nonces, SID values, sequence numbers, and replay cache state converts freshness from a purely temporal check into uniqueness that can be enforced per session.

4.2 Performance-Security Trade-Off

The strengthened protocol is intentionally more expensive than the reconstructed SMPA-CI critical path. AMI-SMPA adds signature verification, authenticated ephemeral key material, HKDF processing, bilateral key confirmation, and authenticated encryption metadata. The 57.1% modeled increase in authentication computation time and 49.5% increase in energy relative to SMPA-CI therefore represent the cost of eliminating deterministic key disclosure and key-exchange ambiguity. The more relevant engineering question is whether that cost remains within the resource envelope of the target meter, not whether it is numerically smaller than an insecure baseline.

In the controlled profile, AMI-SMPA remained below the stated 20 ms single-session latency/computation target and below 5 mJ/session while using less computation, latency, communication, and energy than the two synthetic reference profiles. The simultaneous-arrival scenario adds a system-level qualification: cryptographic service remained approximately 60.4 sessions/s, but queue-inclusive completion rose sharply with 200 and 1,000 charging points. Large sites should therefore combine protocol deployment with parallel verifiers, admission control, or randomized backoff. These are reproducible simulation estimates, not substitutes for embedded measurement or operational-network validation.

4.3 Advanced Metering Infrastructure Privacy and Electric-Mobility Implications

AMI privacy is not solved by payload encryption alone. Static meter identifiers and public keys can remain linkable over long periods, and high-frequency traffic can be correlated with occupancy, appliance use, and charging behavior. Rotating aliases in AMI-SMPA are therefore intended to reduce unnecessary network-level linkability while preserving accountability at the UCC. They are not presented as absolute anonymity because the utility must still resolve the responsible meter for billing, incident response, and regulatory obligations.

The transportation relevance is operational and bounded. ISO 15118-20 governs EV-EVSE communication, whereas AMI-SMPA protects the adjacent station-meter-to-utility authentication path. Charging cybersecurity studies show that compromised stations and coordinated charging actions can affect authorization, billing, privacy, and grid-facing operations [33, 34]. Vehicle-to-grid authentication research similarly emphasizes authenticated key establishment and privacy protection across multi-party charging relationships [35, 36]. AMI-SMPA contributes signed meter/UCC identity binding, replay-resistant energy reporting, authenticated demand-response instructions, post-interruption reauthentication, and endpoint compromise containment. It neither replaces ISO 15118 nor, by itself, establishes power-system stability. Recent connected-vehicle research also examines AI-based anomaly detection and threat analysis [37], offering a complementary monitoring layer to authenticated protocol exchanges.

4.4 Limitations

This study has six limitations. First, the vulnerability analysis applies to the published SMPA-CI equations; an implementation that substitutes standard ECDSA/ECDH would be a different protocol. Second, the PoC is an isolated logical emulator rather than a complete utility/charging stack. Third, Table 5 values are controlled

simulations, not direct MCU or secure-element power measurements. Fourth, the supplied ProVerif model was not executed in the manuscript environment, so no automated “no attack trace” claim is made. Fifth, UMR cannot detect a physically false value generated and authenticated by a compromised meter. Sixth, the EV-burst scenario uses a simplified single-worker FCFS queue, homogeneous endpoints, fixed service assumptions, and no mobility, station-management, traffic-flow, or power-flow model. Consequently, neither operational-network performance nor grid-stability improvement can be inferred.

Future work should port the meter path to representative embedded hardware, execute the symbolic model independently, assess credential revocation and alias resynchronization, and validate multi-worker DCU/UCC scaling under measured public-charging traffic. Field-oriented evaluation should preserve trust-domain separation among the meter, utility back end, EVSE, station controller, and charging-service provider and should report network, workload, and power-system outcomes separately.

5 Conclusions

This study reconstructed a recently developed elliptic-curve multi-phase authentication protocol and evaluated its suitability for the AMI path supporting networked EV charging. Six structural weaknesses were identified: infrastructure private-key exposure, long-term key disclosure, replay within a timestamp window, unbound ephemeral ECDH values, dual session-key definitions, and static-identity linkability. Four conditions were reproduced deterministically in an isolated emulator.

AMI-SMPA replaces reversible private-key masking with signed credentials, binds both ephemeral contributions to the transcript, derives one HKDF session secret, separates authentication/data keys, confirms the key bilaterally, and protects messages with AES-GCM and replay state. The controlled profile produced 16.92 ms computation, 19.35 ms end-to-end latency, 612 bytes/session, 4.35 mJ/session, 99.14% PDR, 98.77% replay detection, 98.76% UMR, and 97.63% KCC. In the worst-case simultaneous burst, one verification worker sustained about 60.4 sessions/s; queue-inclusive mean completion rose from 423.69 ms at 50 charging points to 8,279.05 ms at 1,000 points.

The results support AMI-SMPA as a protocol-level secure communication mechanism for charging authorization, metered-energy reporting, demand-response control, and post-interruption reauthentication under the stated assumptions. They also show that burst capacity must be engineered separately from single-session cryptographic cost. Because all evidence derives from an isolated emulator and controlled simulations, the study makes no claim of operational deployment performance or improved power-grid stability.

Data Availability

The reconstructed equations, isolated-emulator configuration, fixed-seed simulation procedures (seed 20260828), EV charging burst parameters, statistical settings, and symbolic ProVerif specification are available from the corresponding author upon reasonable request. No operational utility or charging-system data were used.

Conflicts of Interest

The author declares no conflicts of interest.

Declaration on the Use of Generative AI and AI-assisted Technologies

Generative AI and AI-assisted technologies were used for language refinement, formatting support, and manuscript organization. The author reviewed and verified the protocol equations, statistical results, references, technical interpretations, and final conclusions and remains fully responsible for the content of the manuscript.

References

- [1] V. Y. Pillitteri and T. L. Brewer, “Guidelines for Smart Grid Cybersecurity,” 2014, National Institute of Standards and Technology, NISTIR 7628 Revision 1. <https://doi.org/10.6028/NIST.IR.7628r1>
- [2] F. M. Cleveland, “Cyber security issues for advanced metering infrastructure (AMI),” in *2008 IEEE Power and Energy Society General Meeting—Conversion and Delivery of Electrical Energy in the 21st Century*, Pittsburgh, PA, USA, 2008, pp. 1–5. <https://doi.org/10.1109/PES.2008.4596535>
- [3] Y. Yan, Y. Qian, H. Sharif, and D. Tipper, “A survey on cyber security for smart grid communications,” *IEEE Commun. Surv. Tutor.*, vol. 14, no. 4, pp. 998–1010, 2012. <https://doi.org/10.1109/SURV.2012.010912.00035>
- [4] P. McDaniel and S. McLaughlin, “Security and privacy challenges in the smart grid,” *IEEE Secur. Privacy*, vol. 7, no. 3, pp. 75–77, 2009. <https://doi.org/10.1109/MSP.2009.76>
- [5] A. R. Metke and R. L. Ekl, “Security technology for smart grid networks,” *IEEE Trans. Smart Grid*, vol. 1, no. 1, pp. 99–107, 2010. <https://doi.org/10.1109/TSG.2010.2046347>
- [6] S. Garg, K. Kaur, G. Kaddoum, J. J. P. C. Rodrigues, and M. Guizani, “Secure and lightweight authentication scheme for smart metering infrastructure in smart grid,” *IEEE Trans. Ind. Inform.*, vol. 16, no. 5, pp. 3548–3557, 2020. <https://doi.org/10.1109/TII.2019.2944880>

- [7] M. M. Hasan, N. A. M. Ariffin, and N. F. M. Sani, "LIKA: Lightweight identity based key agreement protocol for secure data transmission in advanced metering infrastructure of smart grid," *Energies*, vol. 15, no. 21, p. 8106, 2022. <https://doi.org/10.3390/en15218106>
- [8] S. Hu, Y. Chen, Y. Zheng, B. Xing, Y. Li, L. Zhang, and L. Chen, "Provably secure ECC-based authentication and key agreement scheme for advanced metering infrastructure in the smart grid," *IEEE Trans. Ind. Inform.*, vol. 19, no. 4, pp. 5985–5994, 2023. <https://doi.org/10.1109/TII.2022.3191319>
- [9] Y. Zhang, J. Chen, S. Wang, K. Ma, and S. Hu, "Lightweight anonymous authentication and key agreement protocol for a smart grid," *Energies*, vol. 17, no. 18, p. 4550, 2024. <https://doi.org/10.3390/en17184550>
- [10] C. Wang, P. Huo, M. Ma, T. Zhou, and Y. Zhang, "A provable secure and lightweight ECC-based authenticated key agreement scheme for edge computing infrastructure in smart grid," *Computing*, vol. 105, pp. 2511–2537, 2023. <https://doi.org/10.1007/s00607-023-01188-4>
- [11] I. Parvez, M. Aghili, H. Riggs, A. Sundararajan, A. I. Sarwat, and A. K. Srivastava, "A novel authentication management for the data security of smart grid," *IEEE Open Access J. Power Energy*, vol. 11, pp. 218–230, 2024. <https://doi.org/10.1109/OAJPE.2024.3393971>
- [12] T. Pei, Z. Hou, J. Zhou, C. Xiao, and J. Zou, "Blockchain-based anonymous authentication and data aggregation for advanced metering infrastructure in smart grid," *Int. J. Crit. Infrastruct. Prot.*, vol. 46, p. 100702, 2024. <https://doi.org/10.1016/j.ijcip.2024.100702>
- [13] S. Gormus, H. Aydin, B. Aydin, and I. H. Dereli, "Towards reliable and secure metering: Implementing OSCORE over 6TiSCH for smart grid advanced metering infrastructure systems," *Sustain. Energy Grids Netw.*, vol. 43, p. 101892, 2025. <https://doi.org/10.1016/j.segan.2025.101892>
- [14] S. Li, H. Guo, H. Song, Y. Wu, J. Liu, and Y. Han, "A resource-efficient authentication and key agreement protocol for smart grid," *Cybersecurity*, vol. 9, p. 50, 2026. <https://doi.org/10.1186/s42400-025-00411-3>
- [15] M. M. Fouda, Z. M. Fadlullah, N. Kato, R. Lu, and X. S. Shen, "A lightweight message authentication scheme for smart grid communications," *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 675–685, 2011. <https://doi.org/10.1109/TSG.2011.2160661>
- [16] H. Nicanfar, P. Jokar, K. Beznosov, and V. C. M. Leung, "Efficient authentication and key management mechanisms for smart grid communications," *IEEE Syst. J.*, vol. 8, no. 2, pp. 629–640, 2014. <https://doi.org/10.1109/JSYST.2013.2260942>
- [17] J.-L. Tsai and N.-W. Lo, "Secure anonymous key distribution scheme for smart grid," *IEEE Trans. Smart Grid*, vol. 7, no. 2, pp. 906–914, 2016. <https://doi.org/10.1109/TSG.2015.2440658>
- [18] D. He, H. Wang, M. K. Khan, and L. Wang, "Lightweight anonymous key distribution scheme for smart grid using elliptic curve cryptography," *IET Commun.*, vol. 10, no. 14, pp. 1795–1802, 2016. <https://doi.org/10.1049/iet-com.2016.0091>
- [19] T. W. Chim, S. M. Yiu, L. C. K. Hui, and V. O. K. Li, "PASS: Privacy-preserving authentication scheme for smart grid network," in *2011 IEEE International Conference on Smart Grid Communications (SmartGridComm)*, Brussels, Belgium, 2011, pp. 196–201. <https://doi.org/10.1109/SmartGridComm.2011.6102316>
- [20] C. Efthymiou and G. Kalogridis, "Smart grid privacy via anonymization of smart metering data," in *2010 First IEEE International Conference on Smart Grid Communications*, Gaithersburg, MD, USA, 2010, pp. 238–243. <https://doi.org/10.1109/SMARTGRID.2010.5622050>
- [21] R. Sivasankar and M. Marikkannan, "A secure multi phase authentication protocol for cloud infrastructure using elliptic curve cryptography," *Sci. Rep.*, vol. 15, p. 41205, 2025. <https://doi.org/10.1038/s41598-025-25117-x>
- [22] National Institute of Standards and Technology, "Digital Signature Standard (DSS)," 2023, FIPS PUB 186-5. <https://doi.org/10.6028/NIST.FIPS.186-5>
- [23] L. Chen, D. Moody, K. Randall, A. Regenscheid, and A. Robinson, "Recommendations for Discrete Logarithm-based Cryptography: Elliptic Curve Domain Parameters," 2023, NIST SP 800-186. <https://doi.org/10.6028/NIST.SP.800-186>
- [24] E. Barker, L. Chen, A. Roginsky, A. Vassilev, and R. Davis, "Recommendation for Pair-Wise Key-Establishment Schemes Using Discrete Logarithm Cryptography," 2018, NIST SP 800-56A Revision 3. <https://doi.org/10.6028/NIST.SP.800-56Ar3>
- [25] H. Krawczyk and P. Eronen, "HMAC-based Extract-and-Expand Key Derivation Function (HKDF)," 2010, IETF, RFC 5869. <https://doi.org/10.17487/RFC5869>
- [26] M. Dworkin, "Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC," 2007, NIST SP 800-38D. <https://doi.org/10.6028/NIST.SP.800-38D>
- [27] D. Dolev and A. C. Yao, "On the security of public key protocols," *IEEE Trans. Inf. Theory*, vol. 29, no. 2, pp. 198–208, 1983. <https://doi.org/10.1109/TIT.1983.1056650>
- [28] R. Canetti and H. Krawczyk, "Analysis of key-exchange protocols and their use for building secure channels,"

- in *Advances in Cryptology–EUROCRYPT 2001*, ser. Lecture Notes in Computer Science, vol. 2045. Berlin, Heidelberg: Springer, 2001, pp. 453–474. https://doi.org/10.1007/3-540-44987-6_28
- [29] B. A. LaMacchia, K. Lauter, and A. Mityagin, “Stronger security of authenticated key exchange,” in *Provable Security. ProvSec 2007*, ser. Lecture Notes in Computer Science, vol. 4784. Berlin, Heidelberg: Springer, 2007, pp. 1–16. https://doi.org/10.1007/978-3-540-75670-5_1
 - [30] B. Blanchet, “Modeling and verifying security protocols with the applied pi calculus and ProVerif,” *Found. Trends Privacy Secur.*, vol. 1, no. 1–2, pp. 1–135, 2016. <https://doi.org/10.1561/33000000004>
 - [31] International Organization for Standardization, “ISO 15118-20:2022, Road vehicles–Vehicle to grid communication interface–Part 20: 2nd generation network layer and application layer requirements,” 2022, ISO 15118-20:2022. <https://www.iso.org/standard/77845.html>
 - [32] A. Brighente, M. Conti, D. Donadel, R. Poovendran, F. Turrin, and J. Zhou, “Electric vehicles security and privacy: Challenges, solutions, and future needs,” *ACM Trans. Cyber-Phys. Syst.*, vol. 10, no. 3, pp. 1–27, 2026, art. 34. <https://doi.org/10.1145/3801968>
 - [33] S. Acharya, Y. Dvorkin, H. Pandzic, and R. Karri, “Cybersecurity of smart electric vehicle charging: A power grid perspective,” *IEEE Access*, vol. 8, pp. 214 434–214 453, 2020. <https://doi.org/10.1109/ACCESS.2020.3041074>
 - [34] Z. Pourmirza and S. Walker, “Electric vehicle charging station: Cyber security challenges and perspective,” in *2021 IEEE 9th International Conference on Smart Energy Grid Engineering (SEGE)*, Oshawa, ON, Canada, 2021, pp. 111–116. <https://doi.org/10.1109/SEGE52446.2021.9535052>
 - [35] V. Sureshkumar, P. Chinnaraj, P. Saravanan, R. Amin, and J. J. P. C. Rodrigues, “Authenticated key agreement protocol for secure communication establishment in vehicle-to-grid environment with FPGA implementation,” *IEEE Trans. Veh. Technol.*, vol. 71, no. 4, pp. 3470–3479, 2022. <https://doi.org/10.1109/TVT.2022.3146409>
 - [36] Y. Liang, Y. Liu, X. Zhang, and G. Liu, “Physically secure and privacy-preserving charging authentication framework with data aggregation in vehicle-to-grid networks,” *IEEE Trans. Intell. Transp. Syst.*, vol. 25, no. 11, pp. 18 831–18 846, 2024. <https://doi.org/10.1109/TITS.2024.3443171>
 - [37] R. Arslan, T. Özseven, M. M. Aydın, and Y. Çelik, “Cybersecurity in intelligent transportation systems: A comparative study on AI-based anomaly detection and threat analysis,” *Mechatron. Intell. Transp. Syst.*, vol. 5, no. 1, pp. 11–30, 2026. <https://doi.org/10.56578/mits050102>