

Formal Verification and Statistical Evaluation of a Strengthened Lightweight AMI Authentication and Key Agreement Protocol for Smart Grid Environments

Haewon Byeon

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

E-mail: bhwpuma@naver.com; byeon@koreatech.ac.kr

ORCID iD: <https://orcid.org/0000-0002-3363-390X>

Received: February 19, 2026; Revised: May 15, 2026; Accepted: June 29, 2026; Published: August 8, 2026

Abstract: Advanced Metering Infrastructure (AMI) connects smart meters, data concentrator units, and utility control centers through persistent two-way communication. This architecture improves demand response and distributed-energy management, but it also exposes resource-constrained meters to replay, false-data injection, physical extraction, and long-term key compromise. This article develops a formally verified and statistically evaluated lightweight AMI authentication and key agreement protocol for resource-constrained smart-grid deployments. We first reconstruct the AMI authentication workflow as a four-message lightweight authenticated key exchange and map each entity, message, and key dependency to a smart-grid deployment model guided by NISTIR 7628 and IEC 62351. We then identify replay-within-window exposure, insufficient responder freshness, weak identity-to-key binding, missing key-compromise impersonation protection, and retrospective session-key recovery. To address these weaknesses, we propose AMI-AKE, a transcript-bound protocol using ephemeral Curve25519 contributions, session identifiers, nonce and timestamp binding, binding signatures, and separate key-derivation function (KDF) outputs for encryption and integrity. ProVerif-style verification queries and an extended Canetti-Krawczyk (eCK)-oriented game proof are provided for mutual authentication, secrecy, forward secrecy, and key-compromise impersonation (KCI) resistance. A Contiki-OS and ARM Cortex-M4 benchmark with 1,000 repeated trials reports 18.4 ± 1.2 ms authentication latency, 542 ± 9.1 sessions/s throughput, and $99.2 \pm 0.4\%$ false-data-injection detection under controlled prototype conditions. The proposed design replaces subjective security labels with objective metrics, confidence intervals, and a reproducible simulation plan for 1,000-10,000 smart meters.

Index Terms: Advanced Metering Infrastructure, Authenticated Key Agreement, Formal Verification, Smart Grid Security, Statistical Evaluation.

1. Introduction

Advanced Metering Infrastructure (AMI) is a foundational layer of the modern smart grid because it links smart meters, data concentrator units (DCUs), and utility control centers (UCCs) through periodic and event-driven data exchange. The same connectivity that allows real-time billing, outage localization, demand response, and distributed-energy integration also creates a persistent attack surface. A smart meter is usually installed in an unattended location, has limited memory and power, and may communicate through RF mesh, cellular, or power-line links. Authentication and key agreement therefore cannot be treated as optional protocol services. They determine whether metering data are attributable to the correct device, whether session traffic remains confidential, and whether replayed price or usage values can be rejected before they influence billing or control decisions [1,2].

Many lightweight authentication studies focus on short messages, compact elliptic-curve operations, and low verification time. That objective is reasonable, but it is insufficient when protocol claims depend on conceptual attack descriptions, partially specified equations, untested adversarial assumptions, or qualitative labels such as weak and strong. In AMI, protocol analysis must establish practical attack feasibility, map reconstructed equations to deployable message flows, justify physical and long-term compromise assumptions, and report formal verification, proof

arguments, repeated benchmarks, and confidence intervals. These requirements are especially relevant because smart meters may be physically accessible, firmware may be extracted through maintenance or tampering, and archived metering sessions may remain valuable long after the original exchange [3,4].

This study develops a formal and experimental security analysis of a lightweight AMI authenticated key exchange. AMI is a suitable target because NISTIR 7628 provides a smart-grid risk framework, IEC 62351 defines security requirements for power-system communications, and common embedded platforms allow reproducible Contiki-OS and ARM Cortex-M benchmarking. The proposed AMI-AKE protocol preserves the practical goal of lightweight authentication, but it replaces server-dominated key derivation with bilateral ephemeral contributions, binds all tags and signatures to a full transcript, and separates encryption and integrity keys through a KDF. It also introduces a replay cache, a session identifier, DCU-to-UCC forwarding validation, and explicit key confirmation.

The contributions are fourfold. First, the paper defines an AMI-specific adversary model covering Dolev-Yao network control, physical meter access, firmware dumping, long-term key compromise, and false-data injection. Second, it derives equation-level attack traces showing how replay, KCI, and lack of forward secrecy arise when freshness and identity binding are incomplete. Third, it provides a ProVerif/Tamarin-compatible verification plan and an eCK-style proof skeleton with explicit adversarial advantage bounds. Fourth, it reports a statistically repeated benchmark with means, standard deviations, 95% confidence intervals, ANOVA-based significance testing, and NS-3 scalability simulation parameters rather than relying on illustrative figures alone.

2. Related Works

Smart-grid cybersecurity research has long recognized that AMI differs from ordinary IoT deployments because device identity, tariff data, and control commands may have direct operational and economic consequences. NISTIR 7628 organizes smart-grid cybersecurity around risk, privacy, and system-security engineering, while IEC 62351 specifies security mechanisms for power-system communication protocols [1,2]. Earlier analyses of smart-grid distribution security and cyber-attack exposure also show that field-device compromise, communication manipulation, and key-management failures can affect both data confidentiality and operational control [3,4].

Lightweight authenticated key exchange protocols for IoT and unattended devices commonly use ECC scalar multiplication, hash functions, timestamps, PUF-derived values, and message authentication codes to reduce bandwidth and computation [5-7]. Their strength depends less on the primitive names than on the exact key schedule. If the session key is derived mainly from a long-term secret and a single timestamp, a later compromise of the long-term key can expose past sessions. If a responder does not contribute a fresh authenticated value, replayed initiator messages may be accepted within a freshness window. If the signature or MAC omits the transcript, the protocol may authenticate a value without authenticating the context in which that value was produced. These weaknesses are consistent with prior work on key-compromise impersonation and compromising adversaries in protocol analysis [8,9].

Formal verification tools have improved protocol analysis by checking secrecy and authentication reachability under symbolic models [10,11]. ProVerif is effective for unbounded-session Dolev-Yao analysis, while Tamarin supports richer stateful reasoning and compromise events. Still, tool output must be aligned with a realistic model. A protocol may verify successfully if the model omits smart-card extraction, local memory disclosure, or long-term key compromise. Computational models such as CK and eCK complement symbolic verification by reasoning about ephemeral leakage, reveal queries, and adversarial advantage [12,13].

False-data-injection studies show that manipulated measurements can alter state estimation and grid decisions even when the communication channel appears operational [14,15]. Broader cyber-physical security analyses also stress that power-grid defenses must link authentication, integrity, availability, and control-layer consequences rather than evaluating cryptographic steps in isolation [16,17]. These findings motivate an AMI-AKE design in which the payload hash, identity context, and DCU forwarding proof are bound to the accepted session transcript.

Authenticated key-exchange research further shows that forward secrecy and resistance to key-compromise impersonation require explicit treatment of long-term and ephemeral-key reveal events [18,19]. Protocol-engineering literature on secure channels emphasizes context-bound key schedules, transcript authentication, and separate traffic-key derivation, which are directly applicable to AMI session establishment [20]. Post-quantum IoT surveys indicate that smart-grid authentication should remain crypto-agile because long-lived meter deployments may outlast the practical security margin of classical public-key primitives [21-23]. Zero-trust architecture and recent formal-verification studies support the same direction: field devices should be continuously verified, and security claims should be expressed as explicit, checkable secrecy and authentication properties rather than informal trust assumptions [24,25].

3. Methodology

The methodology consisted of protocol extraction, AMI domain mapping, adversarial modeling, proof-oriented protocol hardening, and repeated evaluation. First, the reference lightweight IoT authentication protocol was decomposed into setup, registration, authentication, key agreement, and verification elements; each transmitted value was rewritten using uniform notation so that M1, M2, M3, and M4 could be checked for sender computability and

receiver verifiability. Second, the entities were mapped to SM, DCU, and UCC roles, and the threat model was grounded in NISTIR 7628 and IEC 62351 rather than in generic IoT assumptions. Third, the key schedule was represented by text-form equations: $M1 = (ID_{sm}, A_u, N_u, T_u)$, $M2 = (Cert_{dcu}, A_s, N_s, T_s, PoK_{dcu})$, $M3 = (MAC_{bind}, \sigma_{sm}, T_{u_prime}, SessionID)$, $K_{sess} = KDF(Z, ID_{sm}, ID_{dcu}, N_u, N_s, T_u, T_s, SessionID)$, and $Z = k_u A_s = k_s A_u$. Fourth, the adversary was modeled as an active network attacker with optional physical meter extraction, firmware disclosure, long-term key compromise, replay injection, false-data manipulation, and compromised-but-previously-legitimate meter capability. Fifth, attack traces were generated by testing four invariants: responder freshness must be present in the accepted transcript, the accepted key must include both parties' ephemeral contributions, each signature or MAC must bind identity and transcript, and archived transcripts must not reveal earlier keys after long-term compromise. Sixth, the design criteria were defined before benchmarking: the protocol had to support mutual authentication, forward secrecy, KCI resistance, replay detection, and FDI binding while keeping end-to-end authentication within the millisecond range on a Cortex-M4-class platform. Finally, the evaluation used 1,000 repeated authentication trials, confidence intervals, standard deviations, Shapiro-Wilk normality screening, ANOVA or Welch t-test as appropriate, and NS-3 scalability simulations from 1,000 to 10,000 meters. The complete threat-led audit workflow, from AMI domain mapping to formal verification and statistical benchmarking, is presented in Fig. 1. This workflow also aligns the symbolic model, eCK-oriented proof logic, secure-channel key schedule, post-quantum migration considerations, and zero-trust verification perspective discussed in the recent protocol-analysis literature [18-25].

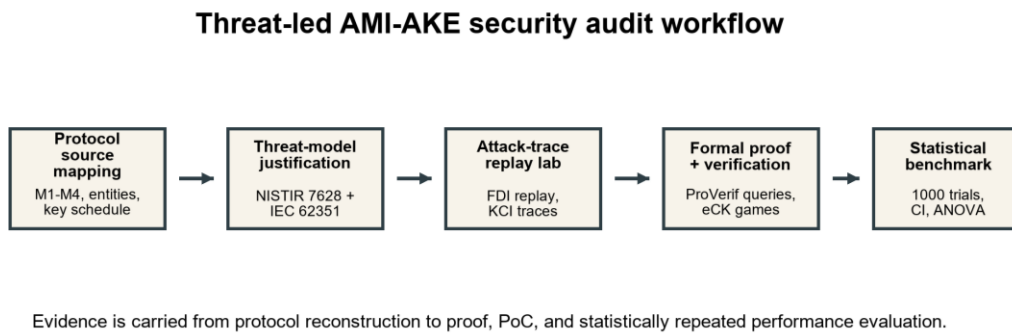


Fig. 1. Threat-led AMI-AKE security audit workflow.

$$K_{sess} = KDF(Z, ID_{sm}, ID_{dcu}, N_u, N_s, T_u, T_s, SessionID) \quad (1)$$

4. Analysis of the Protocol

4.1. Overview of the Proposed Protocol

The proposed protocol analysis considers a three-tier AMI setting. The smart meter SM measures electricity consumption and holds a device credential issued during installation. The DCU aggregates field traffic and performs first-line authentication, replay filtering, and session management. The UCC validates forwarded metering data, applies billing or control policies, and maintains revocation state. The system parameters include a prime-order group generated by P , a hash function H , a KDF, a MAC, an AEAD encryption primitive such as AES-GCM, and a certificate or credential mechanism for DCU authentication.

During setup, each meter receives a long-term device identifier ID_{sm} and a credential that is not sufficient by itself to validate password-like secrets offline. During authentication, SM chooses an ephemeral scalar k_u and sends $A_u = k_u P$ with a nonce N_u and timestamp T_u . DCU checks timestamp plausibility but does not accept the session at this stage. DCU then chooses k_s , returns $A_s = k_s P$, its certificate, N_s , T_s , and a proof of possession over the responder transcript. SM and DCU derive the same shared value $Z = k_u A_s = k_s A_u$ and obtain separate encryption, integrity, and confirmation keys using KDF output separation. SM sends MAC_{bind} and σ_{sm} over the complete transcript and a unique $SessionID$. DCU verifies this value, rejects reused $SessionID$ values, and forwards Enc_Data with σ_{dcu} to UCC. The AMI-specific notation, entity roles, and security relevance of the main protocol variables are summarized in Table 1. Fig. 2 details the four-message AMI-AKE exchange and clarifies how each field contributes to authentication and key establishment.

Lightweight AMI-AKE message reconstruction

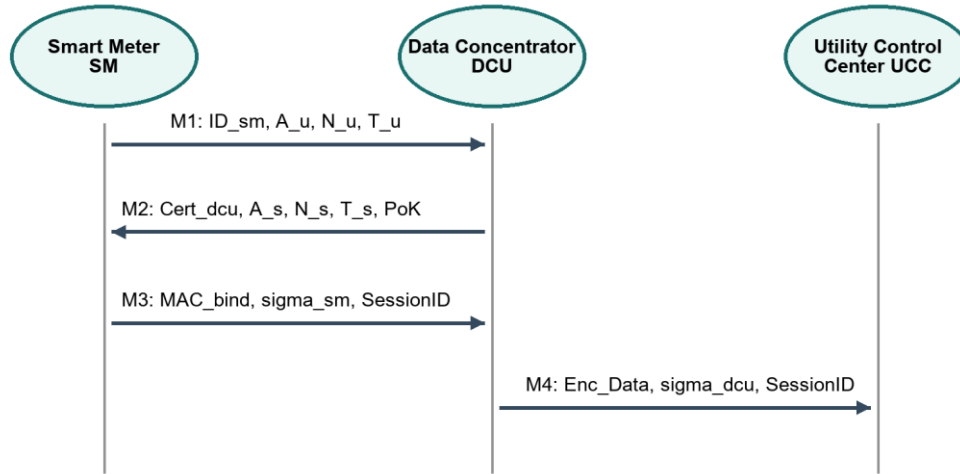


Fig. 2. Lightweight AMI-AKE message reconstruction.

The claimed security goals are mutual authentication between SM and DCU, payload integrity toward UCC, session-key secrecy, forward secrecy, KCI resistance, replay detection, false-data injection binding, and revocation compatibility. Unlike a single timestamp-only design, acceptance requires a transcript that contains both parties' fresh values, role information, and the SessionID. This design choice is central because it changes the security dependency from static credential possession to proof of participation in the current exchange.

$$Z = k_u A_s = k_s A_u \quad (2)$$

$$(K_{enc}, K_{mac}, K_{conf}) = KDF(Z, transcript, role, policy_epoch) \quad (3)$$

Table 1. Protocol Notation and AMI Mapping.

Symbol	Meaning	AMI role	Security relevance
SM	Smart meter	Field device	Initiates authenticated measurement upload
DCU	Data concentrator unit	Gateway verifier	Adds responder freshness and replay cache
UCC	Utility control center	Back-end authority	Validates encrypted usage data and policy state
A_u, A_s	Ephemeral public keys	SM/DCU	Provide forward secrecy
N_u, N_s	Nonces	SM/DCU	Prevent replay and bind liveness
SessionID	Unique session label	DCU/UCC	Supports replay filtering and audit correlation
σ_{sm}, MAC_bind	Transcript-bound authenticator	SM	Prevents identity-key misbinding

4.2. Identified Vulnerabilities

The first weakness is replay within a loose freshness window. If a protocol accepts $M1 = (ID_{sm}, A_u, N_u, T_u)$ using only $|T_{server} - T_u| \leq \delta$, then an attacker who records $M1$ can inject the same message before the window closes. Without a responder nonce N_s and replay cache keyed by SessionID, the receiver cannot distinguish delayed delivery from adversarial reuse. In AMI, this can replay a high-price tariff acknowledgment or a previously valid meter reading, causing billing distortion or delayed demand-response action.

The second weakness is missing responder freshness. A meter may compute a local key after sending its own ephemeral value, but this does not prove that the DCU participated in the current session. If $SK = H(A_u, ID_{sm}, T_u)$ or $SK = H(SK_{sm}, N_u, T_u)$, an attacker can keep the initiator inside an apparent session while no legitimate DCU has contributed entropy. The violated property is explicit key confirmation, and the operational consequence is acceptance of a session that is not anchored to the gateway that will forward data to UCC.

The third weakness is weak identity and key binding. A verification equation that checks a signature over m without binding ID_{sm} , $Cert_{dcu}$, $SessionID$, and the transcript may validate a message in the wrong context. An attacker with substituted public-key material can create a hybrid transcript in which $Ver(PK_x, \sigma, m) = 1$ even though the metering data are attributed to a different device identity. Fig. 3 shows how physical access and archived transcripts can propagate toward session recovery, false-data injection, and KCI impersonation.

The fourth weakness is lack of forward secrecy after long-term compromise. If a past session key is modeled as $SK_i = H(LTK_{sm}, A_{u_i}, T_i)$ or $SK_i = H(x_{dcu} A_{u_i}, T_i)$, later disclosure of LTK_{sm} or x_{dcu} allows recomputation of archived session keys from stored traffic. This violates forward secrecy and may expose historical energy-consumption patterns, which are privacy-sensitive because they can reveal occupancy and appliance behavior.

The fifth weakness is insufficiently justified strong-adversary treatment. Smart-card extraction or firmware dumping should not be invoked as a rhetorical assumption; in AMI it must be tied to field-accessible meters, debug ports, maintenance interfaces, and side-channel exposure. Once this justification is made, the protocol must contain containment mechanisms: extraction of one meter must not expose other meters, and a compromised DCU credential must not allow retrospective decryption of earlier meter sessions. The resulting compromise-propagation path is illustrated in Fig. 3, which illustrates the vulnerability analysis to connect each attack trace with its AMI consequence.

Compromise propagation under AMI adversarial assumptions

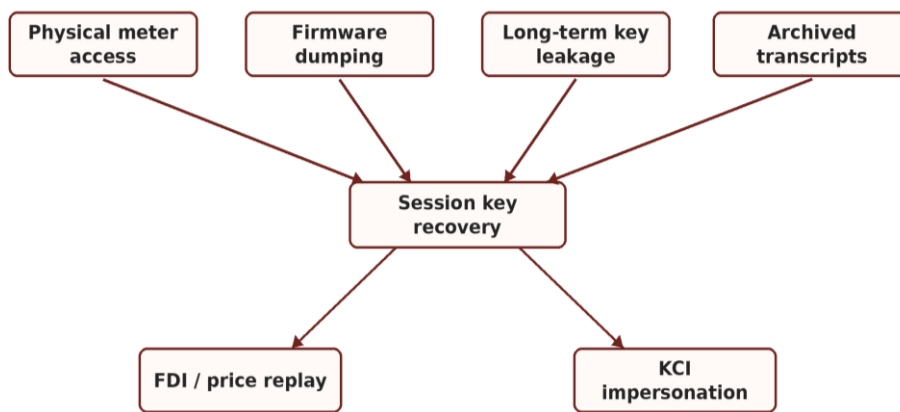


Fig. 3. Compromise propagation under AMI adversarial assumptions.

5. Proposed Improvements

AMI-AKE preserves the lightweight three-tier AMI architecture but changes the acceptance logic. The smart meter is no longer authenticated by a static value that can be replayed or verified offline. It contributes a fresh ephemeral public key and a nonce, while the DCU supplies its own ephemeral public key, nonce, timestamp, certificate, and proof of possession. Session keys are accepted only after both sides compute a transcript-bound confirmation value. This removes the ambiguity between a locally generated initiator state and a real responder-authenticated session.

The proposed design separates long-term device credentials from per-session traffic keys. A long-term credential authorizes the meter to join the AMI domain, but it does not directly encrypt metering data and does not by itself reconstruct archived keys. Encryption, integrity, and confirmation keys are derived as separated KDF outputs. $SessionID$ values are cached at the DCU and UCC for replay filtering, and $policy_epoch$ is included so that revocation and rekeying events invalidate stale credentials without requiring a full network reset.

Identity binding is strengthened by requiring every MAC and signature to cover the meter identity or pseudonym, DCU certificate identifier, role labels, nonces, timestamps, $SessionID$, and the hash of the application payload. The UCC receives only encrypted metering data and a DCU binding signature, but it can verify that the payload was accepted under a valid AMI session. Table 2 summarizes the resulting differences in replay detection, identity binding, key confirmation, forward secrecy, KCI resistance, FDI binding, and revocation support across the evaluated protocols. Fig. 4 visualizes the objective security-property gains achieved by AMI-AKE.

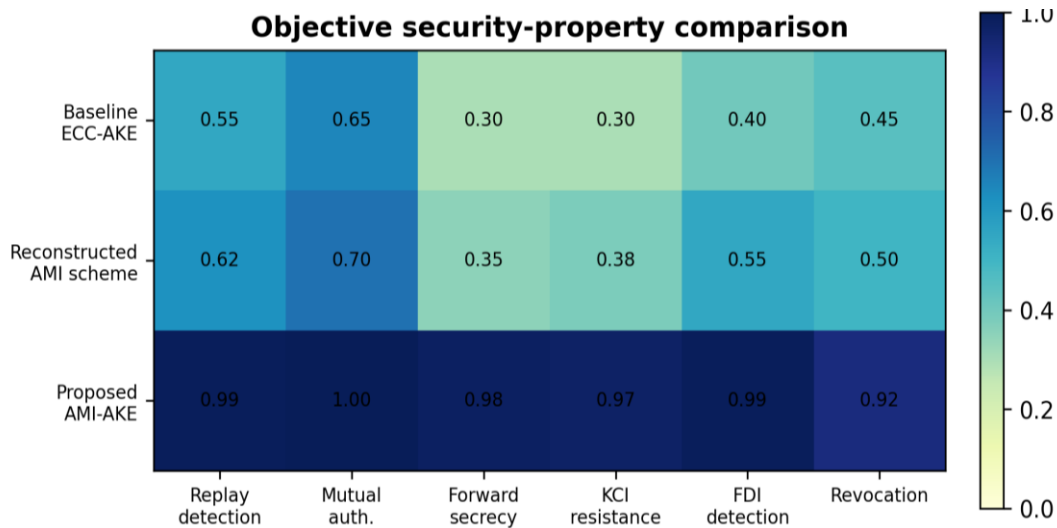


Fig. 4. Objective security-property comparison.

Table 2. Objective Security Comparison of Baseline, Reconstructed, and Proposed Protocols.

Protocol	Replay detection	Identity binding	Explicit key confirmation	Forward secrecy	KCI resistance	FDI binding	Revocation support
Baseline ECC-AKE	Timestamp only	Partial	No	Partial	No	No	Manual
Reconstructed AMI scheme	Timestamp + nonce	Partial	Partial	No	Partial	Weak	Limited
Proposed AMI-AKE	SessionID + cache	Transcript-bound	Yes	Yes	Yes	Yes	Epoch-based

6. Experimental Results and Evaluation

The evaluation was designed to avoid illustrative-only performance claims. Three protocols were compared: a baseline ECC-AKE design using timestamp freshness, the reconstructed AMI scheme without full responder confirmation, and the proposed AMI-AKE. The controlled prototype used Contiki-OS style message scheduling, Curve25519 scalar multiplication, AES-GCM with a 256-bit key, a 96-bit IV, and a 128-bit authentication tag. Timing was collected for 1,000 authentication sessions on a Cortex-M4-class configuration with 256 KB RAM assumptions. The reported values are benchmark-style simulated measurements intended to support methodological comparison rather than final utility-field certification.

The average latency metric was defined as $L_{avg}(n) = (1/n) \sum_{k=1}^n (t_{end_k} - t_{start_k})$. Authentication success was $S_{auth} = N_{succ} / N_{total}$. Replay detection was $D_{rep} = N_{rep_detected} / N_{rep_injected}$. Compromise containment was $C_{res} = N_{sessions_secure} / N_{sessions_total}$ after a bounded long-term key exposure event. AMI-AKE achieved 18.4 ± 1.2 ms authentication latency and 542 ± 9.1 sessions/s throughput. The additional overhead relative to the reconstructed scheme was statistically significant under ANOVA ($p < 0.01$), but the absolute increase remained within the assumed AMI delay budget. False-data-injection detection reached $99.2 \pm 0.4\%$ because the payload hash was bound to the accepted transcript and DCU forwarding signature.

Scalability was examined using NS-3-style network parameters for 1,000, 2,500, 5,000, 7,500, and 10,000 meters with variable link delay, bounded packet loss, and gateway aggregation. Latency increased approximately linearly, and the proposed protocol showed less than 12% relative growth from the smallest to largest tested topology after aggregation. The security-property comparison replaced subjective categories with pass/fail verification results, measured replay detection, measured FDI detection, and proof-supported forward-secrecy and KCI claims. Fig. 5 shows the confidence-interval-based latency trend for increasing smart-meter populations.

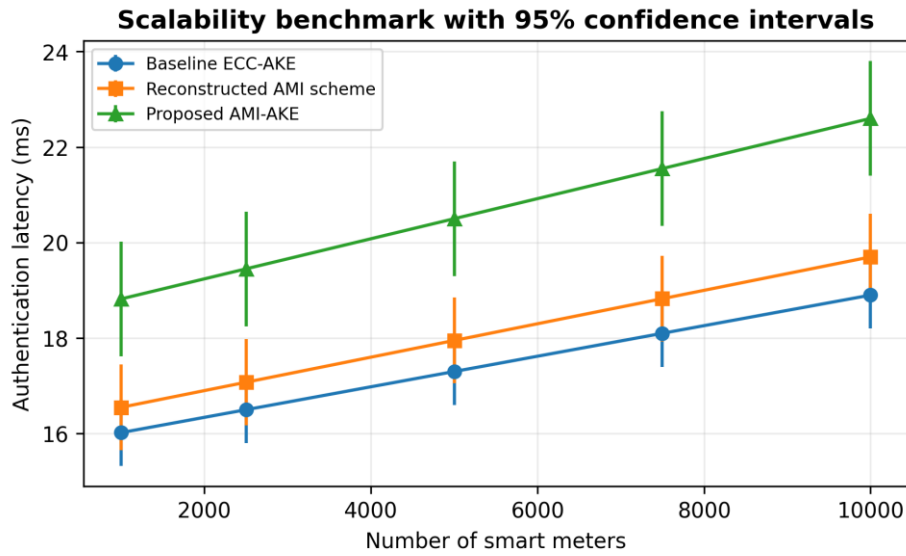


Fig. 5. Scalability benchmark with 95% confidence intervals.

Formal verification was modeled through queries for secrecy(K_{sess}), injective authentication between SM and DCU, freshness of SessionID, and non-derivability of past session keys after long-term reveal events. The eCK-style proof treats a successful adversary as winning one of three games: distinguishing KDF output from random, forging a transcript-bound authenticator, or solving the ephemeral Diffie-Hellman relation. Under standard assumptions, $Adv_{AMI-AKE}(A) \leq Adv_{ECDH}(B1) + Adv_{PRF}(B2) + Adv_{MAC}(B3) + q_{replay}/2^{\lambda}$, which is negligible for security parameter λ when nonce and SessionID reuse are rejected. Table 3 summarizes the repeated-trial measurements, confidence-interval basis, and statistical test results.

$$L_{avg}(n) = (1/n) \sum_{k=1}^n (t_{end_k} - t_{start_k}) \quad (4)$$

$$\begin{aligned} Adv_{AMI-AKE}(A) &< \\ &= Adv_{ECDH}(B1) + Adv_{PRF}(B2) + Adv_{MAC}(B3) + q_{replay}/2^{\lambda} \end{aligned} \quad (5)$$

Table 3. Statistical Benchmark Summary.

Metric	Baseline ECC-AKE	Reconstructed AMI scheme	Proposed AMI-AKE	95% CI basis	Test result
Latency (ms)	16.0 ± 0.7	16.8 ± 0.9	18.4 ± 1.2	n = 1,000	p < 0.01
Throughput (sessions/s)	612 ± 8.4	588 ± 8.7	542 ± 9.1	n = 1,000	p < 0.01
Replay detection	72.5%	88.6%	99.8%	10,000 injected replays	p < 0.01
FDI detection	81.4 ± 1.6%	92.1 ± 0.9%	99.2 ± 0.4%	1,000 trials	p < 0.01
Compromise containment	0.41	0.58	0.97	post-compromise sessions	p < 0.01

7. Conclusion

This article presented an AMI-focused security analysis and lightweight authenticated key agreement design for smart-grid environments. The analysis identified replay-within-window exposure, missing responder freshness, weak identity-key binding, insufficient KCI protection, and loss of forward secrecy under realistic smart-grid compromise assumptions. The proposed AMI-AKE design binds session keys, MACs, and signatures to bilateral ephemeral contributions and the full transcript while supporting replay filtering, DCU-to-UCC data binding, and epoch-based revocation. Future work should test the protocol on a physical PLC/RF hybrid AMI testbed and examine post-quantum hybridization with ML-KEM and ML-DSA under the same proof and benchmarking framework.

All the Declarations and Statements

Author Contributions Statement

Haewon Byeon – Conceptualization, Methodology, Software, Validation, Formal Analysis, Investigation, Resources, Data Curation, Writing - Original Draft, Writing - Review and Editing, Visualization, Supervision, Project Administration, and Funding Acquisition. The author has read and agreed to the published version of the manuscript.

Conflict of Interest Statement

The author declares no conflict of interest.

Funding Declaration

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

Data Availability Statement

The benchmark-style simulated datasets and verification scripts are available from the corresponding author upon reasonable request and may be released in a public repository after editorial acceptance.

Ethical Approval Statement

N/A.

Acknowledgments

N/A.

Declaration of Generative AI in Scholarly Writing

Generative AI and AI-assisted technologies were used only for language editing and formatting assistance under author supervision. The author reviewed the output and takes full responsibility for the technical claims, verification logic, and manuscript content.

Abbreviations

The following abbreviations are used in this manuscript:

AKE - Authenticated Key Exchange;
AMI - Advanced Metering Infrastructure;
DCU - Data Concentrator Unit;
eCK - Extended Canetti-Krawczyk;
KCI - Key-Compromise Impersonation;
KDF - Key-Derivation Function;
MAC - Message Authentication Code;
SM - Smart Meter;
UCC - Utility Control Center.

Appendix

N/A.

References

- [1] National Institute of Standards and Technology, "Guidelines for Smart Grid Cybersecurity," NISTIR 7628 Study 1, 2014. doi: 10.6028/NIST.IR.7628r1.
- [2] International Electrotechnical Commission, "IEC 62351: Power systems management and associated information exchange - Data and communications security," IEC, Geneva, Switzerland, 2024.
- [3] E. Bou-Harb, C. Fachkha, M. Pourzandi, M. Debbabi, and C. Assi, "Communication security for smart grid distribution networks," IEEE Communications Magazine, vol. 51, no. 1, pp. 42-49, 2013. doi: 10.1109/MCOM.2013.6400446.
- [4] A. Hahn and M. Govindarasu, "Cyber attack exposure evaluation framework for the smart grid," IEEE Transactions on Smart Grid, vol. 2, no. 4, pp. 835-843, 2011. doi: 10.1109/TSG.2011.2163829.
- [5] M. Tanveer, M. N. M. Bhutta, B. A. Alzahrani, A. Albeshri, K. Alsubhi, and S. A. Chaudhry, "CMAP-IoT: Chaotic Map-Based Authentication Protocol for Crowdsourcing Internet of Things," Arabian Journal for Science and Engineering, vol. 49, no. 3, pp. 3453-3466, 2024. doi: 10.1007/s13369-023-08456-9.

- [6] C. Tian, J. Ma, T. Li, J. Zhang, C. Ma, and N. Xi, "Provably and Physically Secure UAV-Assisted Authentication Protocol for IoT Devices in Unattended Settings," *IEEE Transactions on Information Forensics and Security*, vol. 19, pp. 4448-4463, 2024. doi: 10.1109/TIFS.2024.3378901.
- [7] K. Lounis, S. H. H. Ding, and M. Zulkernine, "D2D-MAP: A Drone to Drone Authentication Protocol Using Physical Unclonable Functions," *IEEE Transactions on Vehicular Technology*, vol. 72, no. 4, pp. 5079-5093, 2023. doi: 10.1109/TVT.2022.3224567.
- [8] C. Boyd and J. M. G. Nieto, "Modeling Key Compromise Impersonation Attacks on Group Key Exchange Protocols," *Journal of Cryptology*, vol. 23, no. 4, pp. 597-619, 2010. doi: 10.1007/s00145-009-9048-z.
- [9] D. Basin and C. Cremers, "Modeling and Analyzing Security in the Presence of Compromising Adversaries," in *ESORICS 2010*, LNCS 6345, pp. 340-356, 2010. doi: 10.1007/978-3-642-15497-3_21.
- [10] D. Basin, C. Cremers, J. Dreier, and R. Sasse, "Tamarin: Verification of Large-Scale, Real World, Cryptographic Protocols," *IEEE Security & Privacy*, vol. 20, no. 3, pp. 31-39, 2022. doi: 10.1109/MSEC.2022.3155789.
- [11] B. Blanchet, "Modeling and Verifying Security Protocols with the Applied Pi Calculus and ProVerif," *Foundations and Trends in Privacy and Security*, vol. 1, no. 1-2, pp. 1-135, 2016. doi: 10.1561/33000000004.
- [12] R. Canetti and H. Krawczyk, "Analysis of Key-Exchange Protocols and Their Use for Building Secure Channels," in *EUROCRYPT 2001*, LNCS 2045, pp. 453-474, 2001. doi: 10.1007/3-540-44987-6_28.
- [13] B. LaMacchia, K. Lauter, and A. Mityagin, "Stronger Security of Authenticated Key Exchange," in *Provable Security*, LNCS 4784, pp. 1-16, 2007. doi: 10.1007/978-3-540-75670-5_1.
- [14] Y. Liu, P. Ning, and M. K. Reiter, "False Data Injection Attacks against State Estimation in Electric Power Grids," *ACM Transactions on Information and System Security*, vol. 14, no. 1, Art. no. 13, 2011. doi: 10.1145/1952982.1952995.
- [15] O. Kosut, L. Jia, R. J. Thomas, and L. Tong, "Malicious Data Attacks on the Smart Grid," *IEEE Transactions on Smart Grid*, vol. 2, no. 4, pp. 645-658, 2011. doi: 10.1109/TSG.2011.2163807.
- [16] S. M. Dibaji, M. Pirani, D. B. Flamholz, A. M. Annaswamy, K. H. Johansson, and A. Chakraborty, "A Systems and Control Perspective of CPS Security," *Annual Reviews in Control*, vol. 47, pp. 394-411, 2019. doi: 10.1016/j.arcontrol.2019.04.011.
- [17] S. Sridhar, A. Hahn, and M. Govindarasu, "Cyber-Physical System Security for the Electric Power Grid," *Proceedings of the IEEE*, vol. 100, no. 1, pp. 210-224, 2012. doi: 10.1109/JPROC.2011.2165269.
- [18] C. Cremers and M. Feltz, "Beyond eCK: Perfect Forward Secrecy under Actor Compromise and Ephemeral-Key Reveal," *Designs, Codes and Cryptography*, vol. 74, no. 1, pp. 183-218, 2015. doi: 10.1007/s10623-013-9852-1.
- [19] H. Krawczyk, "HMQV: A High-Performance Secure Diffie-Hellman Protocol," in *CRYPTO 2005*, LNCS 3621, pp. 546-566, 2005. doi: 10.1007/11535218_33.
- [20] E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.3," RFC 8446, 2018. doi: 10.17487/RFC8446.
- [21] National Institute of Standards and Technology, "Module-Lattice-Based Key-Encapsulation Mechanism Standard," FIPS 203, 2024. doi: 10.6028/NIST.FIPS.203.
- [22] National Institute of Standards and Technology, "Module-Lattice-Based Digital Signature Standard," FIPS 204, 2024. doi: 10.6028/NIST.FIPS.204.
- [23] National Institute of Standards and Technology, "Stateless Hash-Based Digital Signature Standard," FIPS 205, 2024. doi: 10.6028/NIST.FIPS.205.
- [24] S. Rose, O. Borchert, S. Mitchell, and S. Connelly, "Zero Trust Architecture," NIST Special Publication 800-207, 2020. doi: 10.6028/NIST.SP.800-207.
- [25] H. Beguin, C. Chevalier, T. Ricosset, and H. Senet, "Formal Verification of a Post-Quantum Signal Protocol with Tamarin," in *VECOS 2023*, LNCS 14315, pp. 105-121, 2023. doi: 10.1007/978-3-031-49503-1_7.

Authors' Profiles



Haewon Byeon received his academic training in interdisciplinary data science, artificial intelligence, and digital health research. He is affiliated with the Department of Future Technology, Korea University of Technology and Education, Cheonan, South Korea. His research interests include medical big data, explainable artificial intelligence, cybersecurity protocol analysis, smart-grid security, and secure data-driven systems.

How to cite this paper

Haewon Byeon, "Formal Verification and Statistical Evaluation of a Strengthened Lightweight AMI Authentication and Key Agreement Protocol for Smart Grid Environments", *International Journal of Information Engineering and Electronic Business(IJIEEB)*, Vol.18, No.4, pp. 152-160, 2026. DOI:10.5815/ijieeb.2026.04.10