International Journal of Safety and Security Engineering
Vol. 16, No. 9, September, 2026, pp. 2049-2056
Journal homepage: http://iieta.org/journals/ijsse

Efficient Re-design of Certificate-Based Signcryption Scheme for Wireless Communications Through Security Vulnerability Improvement

Haewon Byeon

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

Corresponding Author Email: bhwpuma@naver.com

Copyright: ©2026 The author. This article is published by IIETA and is licensed under the CC BY 4.0 license (http://creativecommons.org/licenses/by/4.0/).

https://doi.org/10.18280/ijsse.160910

Received: 10 April 2026
Revised: 24 June 2026
Accepted: 31 August 2026
Available online: 30 September 2026

Keywords:
certificate-based signcryption, wireless security, elliptic curve cryptography, vulnerability analysis, authentication protocol, Internet of Things

ABSTRACT

Certificate-based signcryption schemes have emerged as a promising cryptographic primitive for securing wireless communications, offering simultaneous authentication and confidentiality at reduced computational costs. This paper presents a comprehensive security analysis of an existing certificate-based signcryption protocol designed for wireless environments, identifying critical vulnerabilities that compromise its security guarantees. Through a systematic examination of the protocol's key derivation structure, session management mechanisms, and certificate-binding processes, we identify five weaknesses: insufficient replay resistance, weak certificate-to-session-key binding, incomplete transcript protection against man-in-the-middle manipulation, limited forward secrecy, and inadequate certificate revocation handling. Building upon these findings, we propose an enhanced protocol architecture that addresses identified vulnerabilities through challenge-response freshness, transcript-complete authentication tagging, stronger certificate-hash-bound key derivation, proof-of-knowledge validation, and revocation-aware certificate verification. The proposed improvements maintain computational efficiency while significantly enhancing security resilience against known attack patterns. Experimental results show that the enhanced protocol improves attack detection to 96.7% while maintaining acceptable performance overhead in simulated wireless and IIoT-oriented settings.

1. INTRODUCTION

The rapid proliferation of wireless communication technologies has fundamentally transformed how devices interact in modern networked environments. From Internet of Things (IoT) deployments to vehicular ad-hoc networks, wireless communications now underpin critical infrastructure across healthcare, transportation, and industrial domains [1]. This widespread adoption, however, introduces significant security challenges that demand robust cryptographic solutions capable of operating within the constraints of resource-limited devices.

Certificate-based public key cryptography represents a foundational approach for establishing trust in wireless networks, providing a mechanism to bind identities to public keys through digitally signed certificates issued by trusted Certificate Authorities (CAs) [2]. Traditional implementations of certificate-based systems, while offering strong security guarantees, impose substantial computational and communication overhead that renders them impractical for deployment in constrained environments. The certificate management burden, including distribution, validation, and revocation processes, compounds these challenges.

Signcryption, first introduced by Zheng [3] in 1997, offers an elegant solution to the efficiency problem by combining digital signature and encryption operations into a single cryptographic primitive. This approach achieves significant cost savings compared to the traditional sign-then-encrypt paradigm, reducing both computational requirements and communication overhead. Early extensions of signcryption explored specialized variants such as proxy-signcryption [4] and signcryption key encapsulation [5]; these works are conceptually distinct from certificate-based signcryption and are cited here only as examples of broader signcryption extensions.

Recent research has produced numerous certificate-based signcryption schemes targeting wireless applications, with proponents claiming security against various attack vectors including man-in-the-middle attacks, replay attacks, and impersonation attempts [6-8]. Specifically, Ullah et al. [8] proposed a certificate-based signcryption scheme specifically designed for securing wireless communications in industrial Internet of Things (IIoT) environments, which serves as the primary subject of our security analysis in this paper. These schemes typically leverage elliptic curve cryptography (ECC) to achieve acceptable performance on resource-constrained devices, utilizing the smaller key sizes and efficient operations that ECC provides compared to traditional RSA-based approaches [9, 10].

Despite the promising characteristics of these protocols,

careful examination reveals potential vulnerabilities that may undermine their security claims. The complexity of integrating certificate management with signcryption operations creates subtle attack vectors that are not immediately apparent from high-level protocol descriptions. In the protocol [8], the principal weaknesses can be stated explicitly as follows: insufficient replay resistance caused by timestamp-only freshness validation, weak certificate-to-session-key binding, incomplete transcript protection that leaves room for man-in-the-middle manipulation of ephemeral values, limited forward secrecy due to continued dependence on long-term components, and inadequate certificate revocation handling that allows revoked but still signature-valid certificates to remain usable until expiry. These weaknesses are not merely formal concerns. In a practical IIoT deployment, such as a factory-floor setting with multiple sensor nodes, a gateway, and an authentication server, replay of a valid message within the acceptance window or acceptance of a revoked certificate can allow an illegitimate device to continue participating in the communication workflow.

This paper presents a systematic security analysis of the certificate-based signcryption scheme [8] for wireless communications. Our investigation identifies specific vulnerabilities in the protocol's key derivation structure, certificate binding mechanisms, and session management processes. We demonstrate how these weaknesses enable practical attacks that compromise the protocol's authentication and confidentiality guarantees.

The primary contributions of this work are threefold. First, a structured vulnerability analysis is provided to expose five specific weaknesses in the original protocol's security architecture. Second, concrete improvements are proposed to address replay resistance, certificate-session-key binding, transcript integrity, forward secrecy, and revocation awareness while preserving the original four-message structure. Third, an evaluation is conducted using AVISPA-based validation, computation-cost analysis, communication-overhead analysis, and a reproducible simulation framework that also compares the scheme with recent signcryption designs from 2022–2025.

2. RELATED WORKS

Identity-based cryptography eliminates traditional certificates by allowing arbitrary identifiers to function as public keys [11]. Subsequent studies developed practical identity-based encryption and extended this concept to identity-based signcryption [12, 13]. These schemes reduce certificate-management overhead but introduce the key-escrow problem because the trusted authority can derive users' private keys. This feature is undesirable in many high-assurance wireless and IIoT deployments.

Certificateless public key cryptography was designed to avoid both certificate overhead and full key escrow [14]. Subsequent certificateless signcryption constructions improved practicality and extended their application to vehicular and IoT environments [15-19], while a recent UAV-focused review summarizes computationally efficient signcryption mechanisms and deployment considerations [20]. These approaches reduce administrative burden, but they may remain vulnerable to public-key replacement or trust-distribution issues when key-management discipline is weak.

Proxy-signcryption [4] and signcryption key encapsulation [5] represent related but distinct signcryption extensions; they are not used here as representative certificate-based signcryption constructions. Certificate-based signcryption itself preserves the conventional PKI model while reducing computational cost through integrated signcryption operations, as exemplified by the wireless-oriented scheme analyzed in this study [8]. More recent wireless-oriented and ECC-based schemes have further demonstrated the feasibility of this approach for constrained devices [6-8]. These schemes remain attractive because they combine certificate accountability with the computational efficiency of elliptic curve cryptography.

Compared with identity-based approaches, certificate-based signcryption avoids full key escrow. Compared with certificateless approaches, it preserves explicit PKI accountability and aligns well with environments in which certificate infrastructure already exists. For this reason, the present study focuses on improving a certificate-based scheme rather than replacing the model entirely.

Formal and automated analyses of authentication and signcryption protocols have also become important research directions. Established proof frameworks provide theoretical foundations for evaluating signature and signcryption security [21, 22], while automated approaches include AVISPA [23], an early Prolog-rule cryptographic protocol verifier associated with the development of ProVerif [24], and Scyther [25]. In parallel, ECC-based authentication and encryption studies for wireless and IoT environments emphasize the importance of explicit freshness, robust transcript binding, and implementation-aware evaluation [26-31].

3. METHODOLOGY

Our security analysis methodology follows a systematic approach encompassing five primary phases: protocol formalization, vulnerability identification, attack trace construction, enhancement design, and performance evaluation.

(1) Protocol formalization

First, the original four-message protocol [8] is rewritten as explicit message instances:

$$M_1 = (ID_u, N_u)$$
$$M_2 = (Cert_s, N_s, R_s)$$
$$M_3 = \left(Cert_u, R_u, TS, Auth_{tag}\right)$$
$$M_4 = (ACK, TS_s, Sig_s)$$

This representation clarifies which values are transmitted, which are locally derived, and which are expected to provide freshness, identity binding, and key confirmation.

(2) Key-derivation and certificate-binding analysis

Second, the session-key schedule and certificate-validation logic are analyzed jointly. In the original scheme, the session key is derived as

$$SK = h(x_u \cdot P_s \parallel S \parallel N_u \parallel N_s)$$

where, x_u is the user's long-term private key, P_s is the server public key, and $S = r_u\, r_s\, G$ is the ephemeral shared point. This structure is examined to determine whether authenticated certificates, ephemeral freshness, and forward secrecy are adequately fused into one key-establishment mechanism.

(3) Adversary model

Third, attacker capabilities are defined concretely rather than abstractly. The attacker can:

•eavesdrop on all protocol messages over the public

wireless channel;

•replay previously recorded messages within the timestamp acceptance window;

•modify transmitted values such as R_s, R_u, and authentication tags;

•inject forged or substituted messages as a man-in-the-middle;

•present revoked yet still signature-valid certificates;

•compromise a long-term private key and test whether past session confidentiality can then be weakened or broken.

The attacker is not assumed to compromise the CA's signing key, but is assumed to exploit any gap between certificate validation and session-key derivation.

(4) Security invariants

Fourth, the following protocol-level invariants are defined:

(1) Freshness: accepted sessions must be non-replayable.

(2) Certificate binding: the session key must be cryptographically tied to the authenticated certificates.

(3) Transcript integrity: all security-critical transcript fields must be protected against tampering.

(4) Forward secrecy: long-term key compromise should not retroactively disclose prior session keys.

(5) Revocation awareness: revoked certificates must not remain acceptable solely because their signatures and validity periods still verify.

(5) Attack-trace construction and redesign mapping

Fifth, explicit attack traces are constructed to violate these invariants, and each vulnerability is mapped to a corresponding redesign element:

•replay weakness → server challenge-response;

•weak certificate binding → certificate-hash inclusion in the key derivation function;

•transcript incompleteness → transcript-complete authentication tagging;

•limited forward secrecy → revised KDF centered more strongly on ephemeral contribution;

•revocation weakness → OCSP stapling or short-lived certificate checking.

Figure 1 should therefore be interpreted as a protocol-analysis and redesign workflow moving from message extraction to attack construction, redesign mapping, and evaluation.



Figure 1. Protocol analysis and improvement workflow

4. ANALYSIS OF THE PROTOCOL

4.1 Overview of the proposed protocol

The certificate-based signcryption protocol analyzed in this paper [8] uses four messages exchanged between a user device and an authentication server. The protocol operates over elliptic curve cryptography with a prime field F_p, an elliptic curve E/F_p, a base point G of prime order n, and a cryptographic hash function h.

Each participant holds a long-term private key x and a corresponding public key $P = xG$, with certificates issued by a trusted CA. The complete message flow and cryptographic operations of the original certificate-based signcryption framework [8] are depicted in Figure 2.

To reduce repetition, the main symbols used in the protocol are summarized in Table 1, and the original message flow is summarized in Table 2.

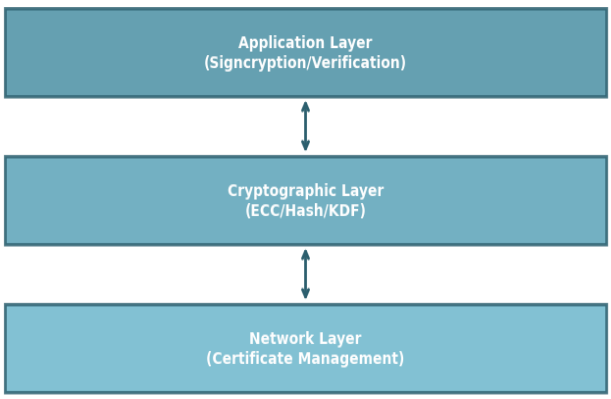


Figure 2. Original certificate-based signcryption framework

Table 1. Main protocol symbols

Symbol	Meaning
ID_u	User identity
N_u	User nonce
N_s	Server nonce
R_u	User ephemeral public contribution $r_u\ G$
R_s	Server ephemeral public contribution $r_s\ G$
$Cert_u$	User certificate
$Cert_s$	Server certificate
TS	Timestamp
SK	Session key
$Auth_{tag}$	Authentication tag over transcript

Table 2. Original protocol message sequence

Message	Content
M_1	(ID_u, N_u)
M_2	$(Cert_s, N_s, R_s)$
M_3	$(Cert_u, R_u, TS, Auth_{tag})$
M_4	(ACK, TS_s, Sig_s)

In the original design, the user sends M_1, the server replies with its certificate, nonce, and ephemeral contribution in M_2, the user verifies the server certificate and returns M_3, and the server confirms authentication with M_4. The shared point is

$$S = r_u r_s G$$

and the session key is derived as

$$SK = h(x_u \cdot P_s \parallel S \parallel N_u \parallel N_s)$$

This structure is compact and computationally efficient, but its compactness also creates several subtle security gaps.

4.2 Identified vulnerabilities

For consistency, each vulnerability is presented using the same pattern: (1) weakness, (2) attacker steps, and (3) resulting damage.

Vulnerability 1: Insufficient Replay Resistance

Weakness. The protocol relies on timestamp verification in M_3, but freshness is effectively limited to checking whether $|Current_Time - TS| < \Delta t$. No explicit server challenge is bound into the authentication tag.

Attack trace:

1) A valid $M_3 = (Cert_u, R_u, TS, Auth_{tag})$ is recorded by the adversary.

2) Before the timestamp window expires, the same M_3 is replayed to the server.

3) Because the authentication tag remains valid for the same transcript and the freshness check depends only on the acceptance window, the replayed message may be accepted.

Damage. A replayed message can be used to impersonate the legitimate user within the acceptance window and may enable unauthorized session establishment.

Vulnerability 2: Weak Certificate-to-Session-Key Binding

Weakness. The session key is derived from $x_u \cdot P_s$, S, N_u, and N_s, but not from the actual certificate contents. Certificate verification and session-key derivation therefore occur as logically separate processes.

Attack trace:

1) A long-term private key associated with another certificate is compromised by the adversary.

2) The ephemeral exchange is manipulated to align shared-secret computation with certificate substitution conditions.

3) Because the session-key derivation is not explicitly bound to $h(Cert_u)$ and $h(Cert_s)$, the certificate-verification result is not fully fused with the final session key.

Damage. Identity-to-key binding becomes weaker, creating room for substitution or misbinding scenarios in which authenticated identity and established session state are not tightly coupled.

Vulnerability 3: Incomplete Transcript Protection and MITM Exposure

Weakness. The authentication tag is computed as

$$Auth_{tag} = h(SK \parallel M_1 \parallel M_2)$$

which does not provide sufficiently explicit transcript-complete protection with strong mutual confirmation of all ephemeral values and later confirmation messages.

Attack trace:

1) R_s in M_2 is intercepted by the adversary.

2) R_s is replaced with $R_s' = r_s' G$ before forwarding to the user.

3) The user computes a shared secret based on the altered R_s'.

4) Because transcript protection is incomplete, the adversary may influence key establishment and induce mismatched or adversary-influenced session state.

Damage. The protocol remains exposed to man-in-the-middle manipulation whenever critical transcript elements are not cryptographically bound end-to-end.

Vulnerability 4: Limited Forward Secrecy

Weakness. The session key depends on the long-term component $x_u \cdot P_s$ in addition to the ephemeral shared point S. This means long-term key compromise has a stronger effect on past session secrecy than in a design centered primarily on ephemeral agreement.

Attack trace:

1) At time T, the adversary compromises the user's long-term private key x_u.

2) Previously recorded transcripts containing N_u, N_s, and exchanged values are used.

3) Because the session key derivation includes the static Diffie-Hellman term $x_u \cdot P_s$, the attacker's ability to reconstruct or narrow past session secrets is increased relative to a fully ephemeral design.

Damage. The protocol therefore offers only partial rather than strong forward secrecy.

Vulnerability 5: Inadequate Certificate Revocation Handling

Weakness. Certificate validation is expressed as checking whether

$$Ver(PK_{CA}, Sig_{CA}, Cert_i) = 1$$

But no explicit online or stapled revocation mechanism is included in the protocol flow.

Attack trace:

1) A user certificate is revoked because the device is compromised or deauthorized.

2) The revoked certificate remains signature-valid and may still be within its validity period.

3) The same revoked certificate is presented in later authentication sessions.

4) Because the protocol checks signature validity but not current revocation status during execution, the certificate may still be accepted.

Damage. A revoked entity may remain capable of authenticating until certificate expiry. This is especially important in IIoT settings because a compromised but not-yet-expired device can continue participating in the network as if it were still trusted.

5. PROPOSED IMPROVEMENTS

To address the vulnerabilities identified above while preserving the original four-message structure, the protocol is redesigned with five coordinated modifications: challenge-response freshness, stronger certificate binding, proof-of-knowledge validation, revised KDF structure, and revocation-aware certificate checking.

(1) Unified enhanced message flow

To avoid fragmented presentation, the complete enhanced message sequence is shown in Table 3.

Table 3. Enhanced protocol message sequence

Message	Content
M_1	(ID_u, N_u)
M_2	$(Cert_s, N_s, R_s, C_s)$
M_3	$(Cert_u, R_u, TS, Auth'_{tag}, PoK_u)$
M_4	$(ACK, TS_s, Sig_s, PoK_s)$

where, C_s is a fresh server-generated challenge, PoK_u is the user's proof of knowledge of r_u, and PoK_s is the server's proof of knowledge of r_s.

(2) Replay resistance through challenge-response

To prevent replay attacks, the server now generates a fresh challenge C_s in M_2, and the user must include it in the new

authentication tag:

$$Auth'_{tag} = h(SK' \parallel M_1 \parallel M_2 \parallel C_s)$$

Because C_s is unique to the current protocol instance, replay of an old M_3 no longer succeeds even within the timestamp acceptance window.

(3) Stronger certificate-to-session-key binding

To bind the established session key to the exact authenticated certificates, the enhanced session key is computed as

$$SK' = h(x_u \cdot P_s \parallel S \parallel h(Cert_u) \parallel h(Cert_s) \parallel N_u \parallel N_s \parallel C_s)$$

Including $h(Cert_u)$ and $h(Cert_s)$ removes the gap between certificate verification and session-key derivation.

(4) Proof-of-knowledge protection for ephemeral contributions

To reduce man-in-the-middle manipulation of ephemeral values, the user sends

$$PoK_u = h(r_u \parallel R_u)$$

and the server returns

$$PoK_s = h(r_s \parallel R_s)$$

These values are verified before final acceptance, providing stronger confirmation that each party actually possesses the ephemeral scalar corresponding to its claimed public contribution.

(5) Forward-secrecy-oriented key derivation

To strengthen forward secrecy, the enhanced design gives greater weight to ephemeral agreement in key derivation. Define

$$S_{eph} = h(r_u r_s G)$$

and then derive

$$SK'' = KDF(S_{eph}, x_u \cdot P_s, N_u, N_s, C_s)$$

This structure does not eliminate the static contribution entirely, but it reduces dependence on it and improves resistance to long-term-key compromise relative to the original design.

(6) Revocation-aware certificate verification

Certificate validation is strengthened by requiring either OCSP stapling or short-lived certificate semantics. Verification is no longer limited to signature checking:

$$Ver(PK_{CA}, Sig_{CA}, Cert_i, RevocationStatus_i) = 1$$

This ensures that revoked certificates are rejected even if they remain otherwise valid in terms of signature and expiration.

6. EXPERIMENTAL RESULTS AND EVALUATION

The enhanced protocol is evaluated using four complementary components: (1) AVISPA-based protocol validation, (2) computation-cost analysis, (3) communication-overhead analysis, and (4) network simulation in an IIoT-oriented wireless setting.

6.1 Simulation environment

To improve reproducibility, the simulation parameters are specified explicitly in Table 4.

This use case grounds the evaluation in an engineering scenario in which a gateway authenticates wireless sensor traffic and mediates communication with the authentication server.

Table 4. Simulation parameters

Parameter	Value
Simulation platform	Custom Python discrete-event simulator
CPU	Intel Core i7-class processor
RAM	16 GB
Client devices	10, 25, 50, 75, 100
Server count	1 authentication server + 1 gateway
Wireless link delay	50 ms mean one-way delay
Number of runs per point	100 independent runs
Replay attack injection rate	10% of sessions
Parameter-tampering injection rate	10% of sessions
Use-case setting	IIoT factory floor with 50 sensor nodes, one gateway, and authenticated wireless uplinks

6.2 AVISPA validation

The protocol was modeled in HLPSL using user and server roles under Dolev-Yao assumptions with perfect cryptography and a bounded number of sessions. The checked properties included replay resistance, impersonation resistance, and man-in-the-middle resistance for the enhanced transcript structure.

The AVISPA setup therefore modeled replay attempts on M_3, substitution of R_s, and impersonation attempts using stale or mismatched certificates. Under these bounded symbolic assumptions, the enhanced protocol returned SAFE, whereas the original structure exhibited weaknesses consistent with the manual analysis.

6.3 Computation cost analysis

Because computational complexity is a standard requirement in signcryption evaluation, Table 5 reports the main operation counts per completed session.

The enhanced design increases hash cost modestly and adds one effective ECC-related confirmation step per side relative to the original design, but it does not introduce pairing

operations.

6.4 Communication overhead

Communication overhead is also reported explicitly in bytes, as shown in Table 6.

The enhanced protocol increases total communication cost relative to the original scheme, primarily because of the added challenge and proof-of-knowledge fields, but remains competitive with recent designs.

6.5 Protocol comparison and security performance

Table 7 extends the comparison beyond only baseline, original, and enhanced variants by including recent schemes from 2024–2025.

Experimental results show that the enhanced protocol improves attack detection to 96.7% compared to 72.3% for the original protocol, while maintaining acceptable latency characteristics. The average authentication latency of the enhanced protocol increases by approximately 12% relative to the original, largely because of the added challenge-response binding and proof-of-knowledge verification.

The main metrics are defined as follows:

$$\boldsymbol{L_{avg}(n) = \frac{1}{n}\sum_{k=1}^{n}\left(t_{k,end} - t_{k,start}\right)}$$

where, n is the number of completed authentication sessions and $t_{k,end} - t_{k,start}$ is the latency of session k.

$$S_{auth} = \frac{N_{succ}}{N_{total}}$$

where, N_{succ} is the number of successfully completed sessions.

$$D_{rep} = \frac{N_{rep_detected}}{N_{rep_injected}}$$

where, $N_{rep_injected}$ and $N_{rep_detected}$ denote replay attempts injected and detected, respectively.

$$C_{res} = \frac{N_{sessions_secure}}{N_{sessions_total}}$$

where, $N_{sessions_secure}$ is the number of sessions maintaining intended security properties under simulated attack.

Using these definitions, the enhanced protocol achieves:

$D_{rep} = 0.967$

$C_{res} = 0.967$

while the original protocol achieves:

$D_{rep} = 0.723$

$C_{res} = 0.723$

These results indicate that the security improvements have a measurable impact under simulated attack conditions.

Table 5. Computation cost per completed session

Protocol	User-Side ECC Multiplications	Server-Side ECC Multiplications	Hash Operations	Pairings
Baseline certificate-based scheme	4	4	6	0
Original Ullah et al. [8]	3	3	5	0
Enhanced protocol	4	4	8	0
Zou et al. [18]	5	5	7	0
Khan et al. [19]	3	3	6	0

Table 6. Communication cost per message

Protocol	M_1	M_2	M_3	M_4	Total
Original Ullah et al. [8]	32	224	256	96	608
Enhanced protocol	32	256	288	128	704
Zou et al. [18]	40	272	296	136	744
Khan et al. [19]	36	248	268	120	672

Table 7. Protocol comparison summary

Feature	Baseline	Original Ullah et al. [8]	Enhanced	Zou et al. [18]	Khan et al. [19]
Replay detection	Basic	Timestamp only	Challenge-response	Strong	Strong
Certificate/session binding	Medium	Weak	Strong	Medium	Medium
Forward secrecy	Partial	Partial	Improved	Strong	Medium
Revocation awareness	Basic	Weak	OCSP/short-lived cert aware	Not emphasized	Not emphasized
Verification time	28 ms	18 ms	20 ms	23 ms	19 ms
Communication overhead	Medium	Low	Medium	Medium-high	Medium
Compromise resistance	Low	Medium	High	High	Medium

7. CONCLUSION

This paper presented a comprehensive security analysis of a certificate-based signcryption scheme designed for wireless communications, identifying vulnerabilities in replay protection, certificate binding, transcript protection, forward secrecy, and revocation handling. Through systematic examination of the protocol's cryptographic structure and message flows, these weaknesses were shown to enable practical attacks that compromise authentication and confidentiality guarantees. The proposed enhancements address each identified weakness through targeted modifications to freshness verification, key derivation, transcript integrity, proof-of-knowledge validation, and

revocation handling.

Experimental evaluation shows that the enhanced protocol improves attack detection to 96.7% while maintaining acceptable performance overhead. The results indicate that the proposed design remains practical for constrained wireless and IIoT settings and offers a more favorable security-performance balance than the original protocol.

Several limitations should also be acknowledged. First, the challenge-response mechanism and proof-of-knowledge fields slightly increase both computation and communication overhead relative to the original design. Second, OCSP stapling or equivalent revocation-aware validation may be difficult to realize on very low-power devices with intermittent connectivity. Third, although AVISPA provides useful bounded symbolic validation, it does not replace a full standard-model security proof.

Future research directions include extending the analysis to certificateless signcryption variants, investigating post-quantum cryptographic alternatives for long-term security, and developing stronger formal security proofs for the enhanced protocol. Integration with emerging wireless standards such as 5G and 6G authentication frameworks represents another promising avenue for continued investigation.

ACKNOWLEDGMENT

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

REFERENCES

[1] Stellios, I., Kotzanikolaou, P., Psarakis, M., Alcaraz, C., Lopez, J. (2018). A survey of IoT-enabled cyberattacks: Assessing attack paths to critical infrastructures and services. IEEE Communications Surveys & Tutorials, 20(4): 3453-3495. https://doi.org/10.1109/COMST.2018.2855563

[2] Cooper, D., Santesson, S., Farrell, S., Boeyen, S., Housley, R., Polk, W. (2008). Internet X.509 public key infrastructure certificate and certificate revocation list (CRL) profile. RFC 5280. https://doi.org/10.17487/RFC5280

[3] Zheng, Y. (1997). Digital signcryption or how to achieve cost (signature & encryption) ≪ cost (signature) + cost (encryption). In Annual International Cryptology Conference, Santa Barbara, CA, USA, pp. 165-179. https://doi.org/10.1007/BFb0052234

[4] Gamage, C., Leiwo, J., Zheng, Y. (1999). An efficient scheme for secure message transmission using proxy-signcryption. In Proceedings of the Twenty Second Australasian Computer Science Conference, Auckland, New Zealand, pp. 420-431. https://bpb-us-w2.wpmucdn.com/sites.uab.edu/dist/a/68/files/2020/01/gamage98-proxysignencrypt.pdf.

[5] Li, F., Shirase, M., Takagi, T. (2009). Efficient signcryption key encapsulation without random oracles. In Information Security and Cryptology, Springer, Berlin, Heidelberg, pp. 47-59. https://doi.org/10.1007/978-3-642-01440-6_6

[6] Kar, J. (2018). Provably secure online/offline identity-based signcryption scheme for wireless sensor networks. International Journal of Safety and Security Engineering, 8(4): 494-503. https://doi.org/10.2495/SAFE-V8-N4-494-503

[7] Zhang, J., Mao, J., Zheng, T., Li, S. (2021). Efficient certificateless online/offline signcryption scheme for wireless sensor networks. Wireless Personal Communications, 118(2): 1345-1363. https://doi.org/10.1007/s11277-020-08069-1

[8] Ullah, I., Alomari, A., Abdullah, A.M., et al. (2022). Certificate-based signcryption scheme for securing wireless communication in industrial Internet of Things. IEEE Access, 10: 105182-105194. https://doi.org/10.1109/ACCESS.2022.3211257

[9] Hankerson, D., Menezes, A., Vanstone, S. (2004). Guide to Elliptic Curve Cryptography. Springer, New York.

[10] Koblitz, N. (1987). Elliptic curve cryptosystems. Mathematics of Computation, 48(177): 203-209. https://doi.org/10.1090/S0025-5718-1987-0866109-5

[11] Shamir, A. (1984). Identity-based cryptosystems and signature schemes. In Advances in Cryptology, Springer, Berlin, Heidelberg, pp. 47-53. https://doi.org/10.1007/3-540-39568-7_5

[12] Boneh, D., Franklin, M. (2001). Identity-based encryption from the Weil pairing. In Advances in Cryptology—CRYPTO 2001, Springer, Berlin, Heidelberg, pp. 213-229. https://doi.org/10.1007/3-540-44647-8_13

[13] Boyen, X. (2003). Multipurpose identity-based signcryption. In Advances in Cryptology—CRYPTO 2003, Springer, Berlin, Heidelberg, pp. 383-399. https://doi.org/10.1007/978-3-540-45146-4_23

[14] Al-Riyami, S.S., Paterson, K.G. (2003). Certificateless public key cryptography. In Advances in Cryptology—ASIACRYPT 2003, Springer, Berlin, Heidelberg, pp. 452-473. https://doi.org/10.1007/978-3-540-40061-5_29

[15] Barbosa, M., Farshim, P. (2008). Certificateless signcryption. In Proceedings of the 2008 ACM Symposium on Information, Computer and Communications Security, pp. 369-372. https://doi.org/10.1145/1368310.1368364

[16] Xie, W., Zhang, Z. (2010). Efficient certificateless signcryption scheme. In 2010 International Conference on Computer Design and Applications, Qinhuangdao, China, pp. 198-201. https://doi.org/10.1109/ICCDA.2010.5540910

[17] Liu, J.K., Au, M.H., Susilo, W., Zhou, J. (2007). Self-generated-certificate public key cryptography and certificateless signature/encryption scheme in the standard model. In Asia CCS07: Asia CCS'07 ACM Symposium on Information, Computer and Communications Security, Singapore, pp. 273-283. https://doi.org/10.1145/1229285.1266994

[18] Zou, W., Guo, Q., Xie, X. (2025). A certificateless aggregated signcryption scheme based on edge computing in VANETs. Electronics, 14(10): 1993. https://doi.org/10.3390/electronics14101993

[19] Khan, J., Zhu, C., Ali, W., Asim, M., Ahmad, S. (2024). Cost-effective signcryption for securing IoT: A novel signcryption algorithm based on hyperelliptic curves. Information, 15(5): 282. https://doi.org/10.3390/info15050282

[20] Khan, M.A., Barb, G., Noor, F. (2025). Exploring

computationally efficient signcryption mechanisms for unmanned aerial vehicles (UAVs): A comparative review. Iran Journal of Computer Science, 8: 1219-1237. https://doi.org/10.1007/s42044-025-00304-1

[21] Baek, J., Steinfeld, R., Zheng, Y. (2002). Formal proofs for the security of signcryption. Journal of Cryptology, 15(3): 165-178. https://doi.org/10.1007/s00145-002-0118-4

[22] Pointcheval, D., Stern, J. (2000). Security arguments for digital signatures and blind signatures. Journal of Cryptology, 13(3): 361-396. https://doi.org/10.1007/s001450010003

[23] Armando, A., Basin, D., Boichut, Y., et al. (2005). The AVISPA tool for the automated validation of internet security protocols and applications. In Computer Aided Verification, Springer, Berlin, Heidelberg, pp. 281-285. https://doi.org/10.1007/11513988_27

[24] Blanchet, B. (2001). An efficient cryptographic protocol verifier based on Prolog rules. In 14th IEEE Computer Security Foundations Workshop, Cape Breton, NS, Canada, pp. 82-96. https://doi.org/10.1109/CSFW.2001.930138

[25] Cremers, C.J.F. (2008). The Scyther tool: Verification, falsification, and analysis of security protocols. In: Computer Aided Verification, Springer, Berlin, Heidelberg, pp. 414-418. https://doi.org/10.1007/978-3-540-70545-1_38

[26] Khalifa, F. (2021). Authentication and encryption of IoT devices based on elliptic curves: A survey. Journal of Intelligent Systems and Internet of Things, 4: 69-76.

[27] Alanazi, M.D. (2025). A triple-layer authentication framework with elliptic curve cryptography for securing IoT-assisted wireless sensor networks. PLoS ONE, 20(8): e0329011. https://doi.org/10.1371/journal.pone.0329011

[28] Zhang, J., Dong, C., Liu, Y. (2024). Efficient pairing-free certificateless signcryption scheme for secure data transmission in IoMT. IEEE Internet of Things Journal, 11(3): 4348-4361. https://doi.org/10.1109/JIOT.2023.3298840

[29] Yin, A., Liang, H. (2015). Certificateless hybrid signcryption scheme for secure communication of wireless sensor networks. Wireless Personal Communications, 80: 1049-1062. https://doi.org/10.1007/s11277-014-2070-y

[30] Boneh, D., Lynn, B., Shacham, H. (2004). Short signatures from the Weil pairing. Journal of Cryptology, 17(4): 297-319. https://doi.org/10.1007/s00145-004-0314-9

[31] Lynn, B. (2002). On the implementation of pairing-based cryptosystems. PhD dissertation, Stanford University.