IAES International Journal of Artificial Intelligence (IJ-AI)
Vol. 15, No. 6, December 2026, pp. 5949∼5959
ISSN: 2252-8938, DOI: 10.11591/ijai.v15.i6.pp5949-5959

Elliptic curve certificate scheme with privacy and revocation support for internet of things-based agriculture

Rachid Tahri[1], Abdellah Ouammou[1], Abdellatif Lasbahani[2], Youssef Balouki[3]
[1]Faculty of Sciences and Technologies, Hassan First University, Settat, Morocco
[2]Faculty of Sciences and Technologies, Sultan Moulay Slimane University, Beni Mellal, Morocco
[3]Higher School of Technology, Mohammed V University, Salé, Morocco

Article Info

Article history:

Received Jul 24, 2025
Revised Aug 30, 2026
Accepted Sep 19, 2026

Keywords:

Certificate-based authentication
Certificate revocation
Elliptic curve cryptography
Formal verification
Lightweight authentication
Privacy preservation
Smart agriculture IoT

ABSTRACT

Smart agriculture increasingly relies on interconnected internet of things (IoT) devices and sensors to enhance productivity, monitoring accuracy, and operational efficiency. Despite these benefits, ensuring secure authentication and privacy preservation remains a major challenge due to resource constraints, identity exposure, and inefficient certificate revocation mechanisms. Conventional certificate-based authentication schemes often incur high computational overhead and depend on heavy certificate revocation lists, making them unsuitable for large-scale and low-power agricultural IoT deployments. To address these limitations, this paper proposes a lightweight elliptic curve cryptography (ECC)-based certificate authentication scheme for the internet of agriculture things. The proposed approach preserves user privacy through anonymity and untraceability while employing ephemeral session keys to achieve forward secrecy and resistance against replay, impersonation, eavesdropping, and man-in-the-middle attacks. Furthermore, short-lived certificates are introduced to reduce revocation overhead, with explicit revocation required only in exceptional cases such as key compromise. The proposed scheme is evaluated through comprehensive security and performance analyses, demonstrating improved efficiency in terms of computational and communication costs compared with existing solutions. In addition, formal verification using the Scyther tool confirms that the scheme satisfies essential security properties under a symbolic adversary model. Overall, the proposed method provides a secure, privacy-preserving, and efficient authentication solution suitable for resource-constrained smart agriculture environments.

This is an open access article under the CC BY-SA license.

Corresponding Author:

Rachid Tahri
Faculty of Sciences and Technologies, Hassan First University
Km 3, B.P.: 577 Route de Casablanca, Settat, Morocco
Email: rachid.tahri.tr@gmail.com

1. INTRODUCTION

The widespread adoption of internet of things (IoT) technologies has brought about a significant shift in modern agriculture, giving rise to what is commonly known as precision farming. By deploying networks of connected sensors and intelligent monitoring systems, farmers, and agricultural businesses can now access detailed, real-time data on key variables such as soil composition, crop health, and livestock conditions [1]. This technological transition has also driven considerable economic growth, with industry projections estimating that the agricultural IoT market will surpass USD 34 billion in value by 2030, alongside an annual

deployment of over 12 million IoT devices in farming environments [2], [3].

Outside of purely commercial considerations, agriculture supported by IoT technology makes a tangible contribution to achieving sustainability goals by improving data-driven resource allocation, dynamically adapting to changing environmental conditions, and enhancing operational decision-making frameworks [4]. The integration of machine learning and predictive modeling has further enhanced these abilities, enabling proactive interventions and corrective measures that minimize potential crop losses [5]. Empirical evidence from field deployments suggests that smart farming systems can achieve labor cost reductions of close to 30% whilst simultaneously improving the precision of agricultural operations [6]. Furthermore, IoT-based supply chain tracking has provided unprecedented transparency across all stages of the agricultural value chain, contributing to an estimated 25% reduction in post-harvest losses through improved traceability and optimized logistics [7]. Overall, these developments support flexible, data-driven agricultural approaches capable of meeting the demands of a growing global population.

However, these attractive advantages come with the trade-off that IoT-based agricultural systems operate in environments that are both open and resource-constrained, dealing with sensitive data that requires robust protection against unwanted access and tampering. Certificate-based authentication has emerged as the mechanism of choice for securing communications between agricultural IoT nodes and back-end service providers. However, traditional certificate management methods often reveal device identities through communication patterns and sent certificates, thereby increasing vulnerabilities to privacy breaches and system compromise [8], [9]. To make matters worse, typical agricultural IoT devices have extremely limited computing power and energy capacity, making computationally intensive cryptographic methods, such as Rivest-Shamir-Adleman (RSA)-based authentication—impractical due to their massive resource consumption [10]. Consequently, there is an urgent need for low-weight authentication solutions that simultaneously address privacy preservation, strong revocation, and the minimization of computational overhead.

A lot of research has already looked at how to secure smart farming, IoT, and similar networks. Most of it tries to fix either privacy, speed, or how to cancel certificates. Itoo *et al.* [11] used ECC and biometrics for farm security. They checked their work with Scyther and Burrows-Abadi-Needham (BAN) logic. But mixing biometrics with farm sensors can be hard in real life. Fatima *et al.* [12] built a three-factor method for farm sensor networks. They used the Chinese remainder theorem and fuzzy extractors. It keeps users anonymous, but it does not block denial-of-service (DoS) attacks. Rostampour *et al.* [13] made an ECC protocol for smart grids using physical unclonable functions. It stops replay and impersonation but ignores DoS. Garai *et al.* [14] came up with a certificate method for cars. It blocks replay, DoS, and Sybil attacks, but the certificate overhead is too heavy for small devices.

Liang *et al.* [15] worked on healthcare IoT access control. Their method supports forward and backward secrecy, but they did not run formal automated security checks. Zhang *et al.* [16] created a three-factor ECC method for e-health. It gives anonymity and blocks common attacks, but the computation is too heavy for low-power gadgets. Kurt *et al.* [17] proposed a privacy method for connected vehicles. It stops replay and man-in-the-middle (MITM), but not DoS, and lacks formal proofs. Song *et al.* [18] used Merkle trees and bilinear pairings for certificate revocation. It authenticates well, but pairing math is slow and heavy. Höglund *et al.* [19] made a light certificate revocation for tiny IoT nodes using bloom filters and elliptic curve digital signature algorithm (ECDSA). But it leaves the system open to man-in-the-middle attacks. Many studies solve one piece of the puzzle, but few give a complete, light, formally proven, and easily revocable answer for farm IoT. That gap is exactly what our work tries to fill.

To address these challenges, this study present an effective certificate validation framework based on elliptic curve cryptography (ECC), which integrates privacy preservation and support for certificate revocation particularly for smart farming contexts. The proposed scheme eliminates the reliance on traditional certificate revocation list mechanisms by adopting short-term certificates paired with a distributed verification approach, thereby reducing both management and network overheads. This design enables temporary and secure access to shared agricultural resources, facilitating rapid revocation of compromised devices without service interruption. By exploiting the efficiency of ECC, this scheme achieves security guarantees comparable to those provided by the RSA system with significantly lower computational and energy overheads. Overall, the proposed solution seeks to strike an effective balance between security, privacy and performance objectives, making it a good choice for large-scale, resource-constrained IoT-based smart farming systems.

2. PRELIMINARIES

2.1. Certificate-based cryptography

The high society brought certificate-based cryptography to light in 2003. It was meant to solve problems found in both standard public key systems and identity-based encryption [10], [20]. Public key setups suffer from heavy certificate handling, while identity-based methods have key escrow flaws. Certificate-based cryptography uses digital certificates to avoid too much control while still giving solid authentication. In this method, a trusted certificate authority (CA) creates and signs certificates that link an entity to its public key [21]. This gives strong authentication and stays flexible and scalable, which is helpful in low-resource places like farm IoT.

2.2. Elliptic curve cryptography

Paar *et al.* [22] introduced ECC as a public-key system built on elliptic curves over finite fields. A curve E over $\mathbb{F}_p$ is written as (1).

$$y^2 = x^3 + ax + b \tag{1}$$

Where $a, b \in \mathbb{F}_p$, and $4a^3 + 27b^2 \neq 0$ to keep it non-singular. The curve's points, plus a point at infinity, form an Abelian group under addition [23]. This structure allows key generation, signing, and encryption. ECC matches RSA security but with much smaller keys, which is great for limited IoT devices.

2.3. Trapdoor functions

A trapdoor function is simple to compute one way but very resistant to reverse without a secret key [24]. These functions are basic to public-key crypto. For ECC, the trapdoor comes from the elliptic curve discrete log problem, making it robust against attacks.

2.4. Elliptic curve discrete logarithm problem

ECC security relies on the hardness of the elliptic curve discrete logarithm problem (ECDLP). Given points β and γ, the task is to find an integer S so that: $\beta = S \cdot \gamma$, where $S \cdot \gamma$ is scalar multiplication [11]. With the right curve parameters, this is impossible to solve in polynomial time. That hardness is the backbone of our protocol's security.

3. NETWORK MODEL

The proposed system architecture comprises five principal entities: agricultural IoT sensors, a controller, a CA, a service provider, and a certificate revocation manager (CRM). These components work in concert to enable secure, privacy-preserving communication within smart agricultural environments. Agricultural IoT sensors encompass diverse devices deployed throughout farming operations, including instruments for measuring temperature, humidity, soil moisture, and light intensity. These sensors continuously gather environmental data and relay it to proximal controllers. Given their limited computational and energy capacities, sensors delegate security-critical operations and external communications to the controller.

The controller functions as an intermediary bridging IoT sensors and the service provider. Prior to communication initiation, both the controller and service provider must undergo registration with the CA. Upon identity verification, the CA issues time-limited certificates to each entity. The employment of short-lived certificates reduces the risk associated with long-term credential compromise and minimizes dependency on frequent revocation verification.

Following registration, the controller initiates an authentication session with the service provider, presenting its certificate while preserving privacy through pseudo-identity utilization. The authentication procedure incorporates time-dependent verification mechanisms, ensuring resilience against replay and impersonation attacks. Secure communication channels are established exclusively upon successful mutual authentication. Meanwhile, the CRM oversees certificate validity monitoring. In cases where a short-lived certificate is compromised prior to expiration, the revocation manager updates the revocation list and invalidates the affected certificate. This mechanism prevents exploitation of compromised credentials and enhances overall system trustworthiness.

4. PROPOSED SCHEME

This section presents the proposed ECC-based certificate authentication scheme with privacy preservation and revocation support for smart agriculture environments. Figure 1 illustrates overall workflow of the proposed system. Additionally, Table 1 summarizes notations used throughout the protocol description.

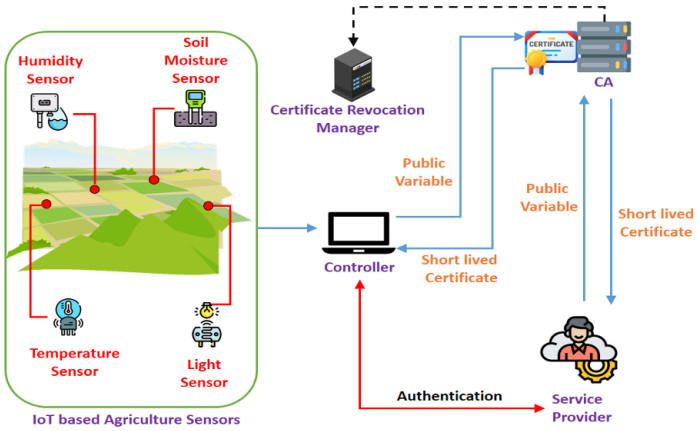

Figure 1. Flow of the proposed authentication scheme

Table 1. Notations and their meanings

Symbol	Meaning
P_{pk}, s	Master public/private key pair of the CA
α_C, α_{SP}	Private keys of the controller and service provider
β_C, β_{SP}	Public keys of the controller and service provider
$\text{Pid}_C, \text{Pid}_{SP}$	Pseudo-identities of the controller and service provider
K_C, K_{SP}	Shared secret values
σ_C, σ_{SP}	Certificate signatures
SK	Session key
N_C, N_{SP}	Nonces of controller and service provider
T	Timestamp
$\text{Cert}_C, \text{Cert}_{SP}$	Certificates issued by the CA

4.1. Setup phase

In this phase, the CA initializes the system parameters as follows:

i) Select an elliptic curve $E(F_p)$ with a generator point G of prime order n.
ii) Choose a master private key $s \in \mathbb{Z}_n$ at random.
iii) Compute the master public key as $P_{pk} = s \cdot G$.
iv) Define three secure and collision-resistant hash functions H_1, H_2, and H_3.
v) Publish the system parameters: $\{E(F_p), G, n, P_{pk}, H_1, H_2, H_3\}$.

4.2. Registration phase

Both the controller and the service provider register with the CA as follows:

i) Each entity selects a private key α_{entity}.
ii) The corresponding public key is computed as $\beta_{entity} = \alpha_{entity} \cdot G$.
iii) A random nonce r_C or r_{SP} is generated.
iv) Pseudo-identities are computed as: $\text{Pid}_C = H_1(ID_C \parallel r_C)$, $\text{Pid}_{SP} = H_1(ID_{SP} \parallel r_{SP})$.
v) The registration message is sent to the CA: $\{ID_C, \beta_C, r_C\}$, $\{ID_{SP}, \beta_{SP}, r_{SP}\}$.

4.3. Certificate generation and issuance

After successful verification, the CA generates certificates as follows:

i) Compute the certificate signatures: $\sigma_C = s \cdot H_1(\text{Pid}_C \parallel \beta_C \parallel T_C)$, $\sigma_{SP} = s \cdot H_1(\text{Pid}_{SP} \parallel \beta_{SP} \parallel T_{SP})$.
ii) Issue short-lived certificates: $\text{Cert}_C = (\text{Pid}_C, \beta_C, T_C, \sigma_C)$, $\text{Cert}_{SP} = (\text{Pid}_{SP}, \beta_{SP}, T_{SP}, \sigma_{SP})$.

4.4. Authentication phase

When the controller initiates authentication with the service provider:

i) Generate a nonce N_C.
ii) Compute the shared secret: $K_C = \alpha_C \cdot \beta_{SP}$.
iii) Construct the authentication message: $\text{Auth}_C = H_2(\text{Pid}_C \parallel \beta_C \parallel T_1 \parallel N_C \parallel K_C \parallel \text{Cert}_C)$.
iv) Send Auth_C to the service provider.

Upon receiving the request, the service provider:

i) Verifies the certificate validity and timestamp.
ii) Checks the certificate signature: $\sigma_C \cdot G \stackrel{?}{=} P_{pk} \cdot H_1(\text{Pid}_C \parallel \beta_C \parallel T_C)$.
iii) Computes the shared secret: $K_{SP} = \alpha_{SP} \cdot \beta_C$.
iv) Validates the authentication message.
v) Generates N_{SP} and timestamp T_2, then responds with: $\text{Auth}_{SP} = H_2(\text{Pid}_{SP} \parallel \beta_{SP} \parallel T_2 \parallel N_{SP} \parallel K_{SP} \parallel \text{Cert}_{SP})$.

Both entities derive the session key as: $SK = H_2(T_1 \parallel T_2 \parallel N_C \parallel N_{SP} \parallel K_C)$.

4.5. Certificate revocation phase

4.5.1. Revocation initiation

Although short-lived certificates limit how long a stolen credential can be used, a certificate may still be compromised before it expires, for example through key leakage or the physical capture of a controller deployed in the field. When this happens, the CA notifies the CRM, which updates the revocation list as $\text{CRL} \leftarrow \text{CRL} \cup \{\text{Pid}_C, \text{Pid}_{SP}\}$. Because only pseudo-identities are added to the CRL, revocation can be carried out without disclosing the real identities ID_C or ID_{SP}, so entity privacy is preserved during this phase as well. The CRL only needs to keep these entries until the corresponding certificates reach their expiration time T_C or T_{SP}, after which they become invalid anyway, so the list stays small and is cheap for resource-constrained devices to check.

4.5.2. Revocation check

During authentication, both entities verify certificate validity:

i) The service provider checks $\text{Pid}_C \notin \text{CRL}$.
ii) The controller checks $\text{Pid}_{SP} \notin \text{CRL}$.

If a revoked identity is detected, the authentication session is immediately aborted.

4.5.3. Correctness proof

The correctness of the proposed protocol is demonstrated as follows:

i) Shared secret correctness: $K_C = \alpha_C \cdot \beta_{SP} = \alpha_C \cdot \alpha_{SP} \cdot G = \alpha_{SP} \cdot \beta_C = K_{SP}$.
ii) Certificate verification correctness: $\sigma_C \cdot G = s \cdot H(\text{Pid}_C \parallel \beta_C \parallel T_C) \cdot G = P_{\text{pk}} \cdot H(\text{Pid}_C \parallel \beta_C \parallel T_C)$.

Hence, the correctness of the proposed scheme is ensured.

5. PERFORMANCE ANALYSIS

This section evaluates the proposed authentication scheme in terms of computational cost and communication overhead. The results are compared with several recent state-of-the-art schemes. This comparison demonstrates the efficiency and suitability of the proposed solution for resource-constrained smart agriculture environments.

5.1. Computational cost

Computational cost refers to the execution time required to perform cryptographic operations during protocol execution. This analysis compare the computational cost of the proposed scheme with existing approaches [11], [13], [16], [18]. Only computationally intensive operations are considered, while lightweight operations (e.g., hash functions and exclusive OR (XOR) operations) are neglected due to their negligible impact on the overall cost. The cryptographic operations considered are:

– Bilinear pairing operation ($\varphi\beta$),
– Bilinear pairing multiplication ($\varphi\beta\mathcal{M}$),
– Elliptic curve point multiplication ($\varepsilon cp\mathcal{M}$).

The execution time of these operations is derived from the experimental evaluation reported in [25]. The experiments were conducted using an Intel(R) Core i7-8565U processor operating at 2.4 GHz with 4 GB of RAM and running Ubuntu 18.04.5 long-term support (LTS) as the operating system. Table 2 reports the execution time of the considered cryptographic operations. Based on these values, the total computational cost of each scheme is calculated and summarized in Table 3. The comparative results are further illustrated in Figure 2.

The results clearly indicate that the proposed scheme achieves the lowest computational cost among all compared methods. This improvement is primarily due to the exclusive use of elliptic curve point multiplication operations. The avoidance of expensive bilinear pairing computations makes the scheme well-suited for low-power IoT-based agriculture devices.

Table 2. Time consumed by cryptographic operations in milliseconds

Operation	$\varphi\beta$	$\varphi\beta\mathcal{M}$	$\varepsilon cp\mathcal{M}$
Time (ms)	5.175	2.146	2.063

Table 3. Computational cost comparison

Scheme	Operations	Total cost (ms)
[11]	$4T_{\varepsilon cp\mathcal{M}}$	8.2
[13]	$6T_{\varepsilon cp\mathcal{M}}$	12.3
[16]	$5T_{\varepsilon cp\mathcal{M}}$	10.3
[18]	$2T_{\varphi\beta} + 2T_{\varphi\beta\mathcal{M}}$	14.64
Proposed scheme	$3T_{\varepsilon cp\mathcal{M}}$	6.1

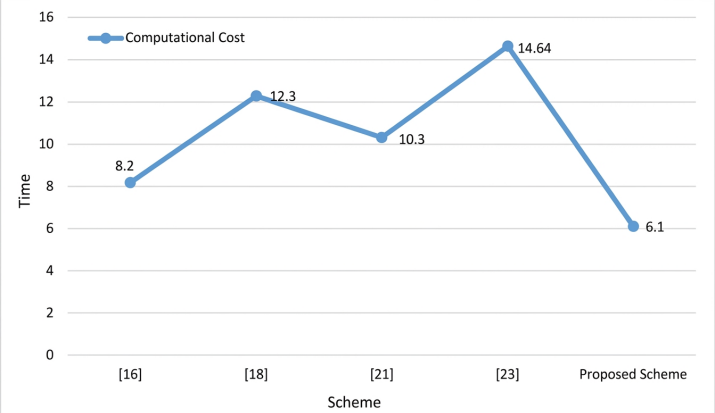

Figure 2. Computational cost comparison

5.2. Communication overhead

Communication overhead represents the total number of extra bits exchanged during protocol execution. Minimizing communication overhead is critical for bandwidth-constrained and energy-limited IoT environments. In this subsection, the communication overhead of the proposed scheme is compared with existing schemes [11], [13], [16], [18]. For a fair comparison, the size of an elliptic curve point is assumed to be 160 bits, while bilinear pairing-based group elements are considered significantly larger. The communication overhead of each scheme is calculated based on the number of transmitted elliptic curve points or group elements. The results are presented in Table 4 and illustrated in Figure 3.

Table 4. Communication overhead comparison

Scheme	Communication overhead	Total (bits)
[11]	$13\|E\|$	2,080
[13]	$12\|E\|$	1,920
[16]	$11\|E\|$	1,760
[18]	$8\|G\|$	8,192
Proposed scheme	$10\|E\|$	1,600

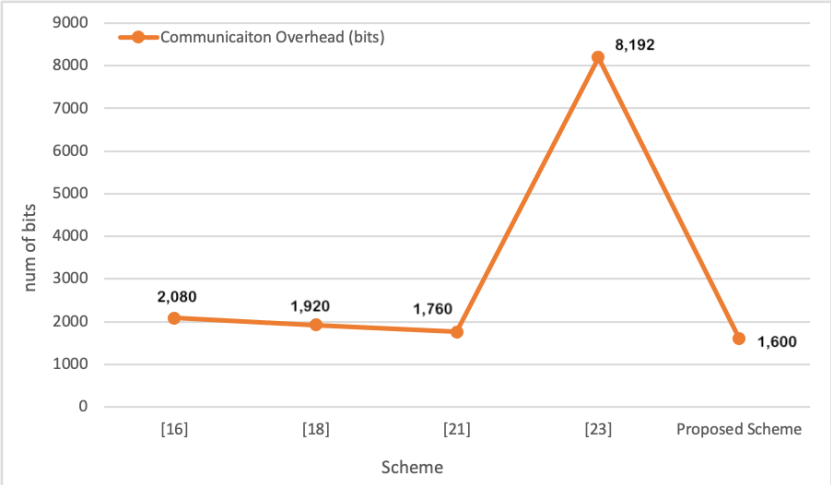

Figure 3. Communication overhead comparison

As shown in the results, the proposed scheme achieves the lowest communication overhead among elliptic curve-based schemes. It also significantly outperforms bilinear pairing-based approaches. This reduction in transmitted data directly contributes to lower energy consumption and improved scalability in smart agriculture IoT deployments.

6. INFORMAL SECURITY ANALYSIS

The security of the proposed scheme against various attacks is analyzed as follows:

i) Mutual authentication: both sides prove who they are. The controller and the service provider check each others certificates, which come from a trusted CA. They also both make the same shared secret, so they know the other party holds the right private key.

ii) Anonymity: not at any time send real IDs. Only pseudo-identities go over the network. To find a real identity, an attacker has to solve ECDLP. That is too hard, so privacy holds.

iii) Integrity: the hash functions tie all the parts of a message together. Change one bit, and the receiver sees the hash is wrong and drops the message.

iv) Forward secrecy: every session uses fresh nonces, timestamps, and a new shared secret. So even if an attacker steals a long-term key later, they cannot read old sessions.

v) Replay attack resistance: fresh nonces and timestamps make old messages stale. Replaying a captured packet just gets rejected.

vi) Resilience to certificate misuse: the proposed certificates die quickly. Even if one gets stolen, it is only useful for a very short time, so there is almost no window to abuse it.

vii) Certificate revocation support: if a certificate gets stolen early, the CRM flags it and kills the pseudo-identity instantly. That locks the bad device out of next sessions.

viii) MiTM attack resistance: a middleman cannot change messages because they do not have the private keys. Without the shared secret, any tampering is caught.

ix) Impersonation attack resistance: forging a valid certificate requires solving ECDLP. That is impossible, so fake identities do not work.

x) DoS attack mitigation: the proposed scheme is fast and cheap. An attacker cannot easily burn up the device's central processing unit (CPU). Also, bad devices are revoked fast, so they can't keep flooding the network.

xi) Sybil attack resistance: every pseudo-identity is signed by the CA. An attacker cannot create endless fake identities without getting caught.

xii) Session hijacking resistance: session keys only function for one session. Once that session ends, the key is expired.

xiii) Eavesdropping resistance: without the shared secret, an attacker cannot read the messages. Decrypting is as hard as solving ECDLP.

7. SCYTHER SIMULATION

This study used Scyther to formally prove proposed protocol is defended. Scyther is a well-known tool that look at security protocols against the Dolev-Yao attacker model [26]. It looks at every possible path an attacker could take. This study wrote proposed protocol in a special language called SPDL. This study ran checks for standard security claims. All of them came back "OK". This means no attacks were found in the bounded sessions. The results are shown in Figure 4.

i) Secrecy: the confidentiality properties have been defined to ensure that sensitive information — specifically the session key $SK = H_2(T_1 \| T_2 \| N_{SP} \| N_C \| K_C)$ and the certificates (Cert_C, Cert_{SP}) — remain confidential throughout the protocol's execution. The result of the verification assures that these values are not revealed to attackers as part of the symbolic model analysis, showing the system's resistance to eavesdropping attacks.

ii) Aliveness: the claim of 'Aliveness' means that every participating entity successfully completes the process of invoking the protocol with the intended communication partner. This prevents a scenario in which an adversary deceives one of the parties into believing that the invocation has been successful, thereby diminishing attempts at 'denial-of-service' attacks based on session disruption.

iii) Non-injective synchronization (Ni-synch): Ni-synch claims validate correct message ordering and new preservation. This guarantee that protocol messages are arrived in the intended sequence and correspond to the same session instance, providing essential protection against replay attacks.

iv) Non-injective agreement (Ni-agree): Ni-agree claims confirm that both communicating entities reach consensus on critical protocol parameters, including nonces, session keys, and certificates. This agreement guarantees strong mutual authentication and prevents impersonation attacks.

v) Weak agreement (weak-agree): furthermore, the claims made by 'weak agreement' show that the connected parties ultimately agree on the existence of a protocol session, even if not all inputs are explicitly confirmed. This demonstrates the robustness of the system to attacks by a 'man-in-the-middle'.

vi) Commit claims: the compliance claims ensure both entities can prove that a session with the intended party has been fully completed, which helps to validate the verification process.

These results confirm that the proposed scheme satisfies the targeted security properties and is formally verified to be secure with respect to authentication, secrecy, synchronization, and agreement guarantees.

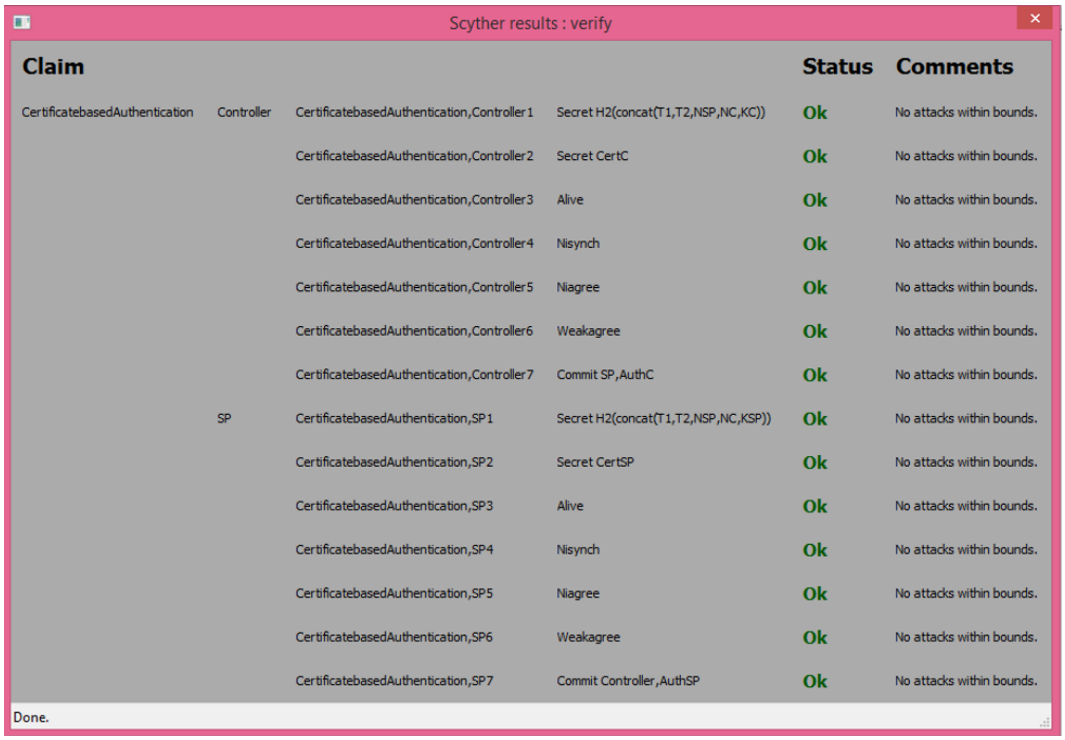

Figure 4. Scyther simulation results showing successful verification of all security claims

8. CONCLUSION

Agriculture remains a fundamental sector of the global economy, directly influencing food security, employment, and sustainable development. While IoT technologies enable smart agriculture through continuous monitoring and intelligent decision-making, they also introduce substantial security and privacy concerns due to device resource limitations and extensive network connectivity. To overcome these challenges, this paper has introduced an ECC-based certificate authentication scheme for IoT-enabled smart agriculture. The proposed framework delivers mutual authentication, privacy preservation, and efficient certificate revocation through short-lived certificates, reducing communication overhead and revocation latency. User privacy is maintained via pseudo-identities, while ephemeral session keys and fresh nonces ensure forward secrecy and resistance against replay, impersonation, and man-in-the-middle attacks. Performance evaluations demonstrate that the proposed scheme outperforms existing approaches in computational efficiency and communication overhead, making it suitable for resource-constrained agricultural IoT devices. Informal security analysis confirms the protocol's robustness, and formal verification using Scyther validates key security properties including secrecy, authentication, synchronization, and agreement. Overall, the proposed scheme constitutes a secure, efficient, and privacy-preserving authentication solution for smart agriculture systems, offering a practical foundation for future large-scale IoT-based agricultural deployments.

FUNDING INFORMATION

This research received no specific grant from any funding agency.

AUTHOR CONTRIBUTIONS STATEMENT

This journal uses the Contributor Roles Taxonomy (CRediT) to recognize individual author contributions, reduce authorship disputes, and facilitate collaboration.

Name of Author	C	M	So	Va	Fo	I	R	D	O	E	Vi	Su	P	Fu
Rachid Tahri	✓	✓	✓			✓			✓	✓	✓	✓	✓	✓
Abdellah Ouammou	✓				✓				✓	✓		✓	✓	
Abdellatif Lasbahani		✓	✓		✓					✓	✓			
Youssef Balouki	✓						✓	✓		✓		✓		

C : **C**onceptualization
M : **M**ethodology
So : **So**ftware
Va : **Va**lidation
Fo : **Fo**rmal Analysis
I : **I**nvestigation
R : **R**esources
D : **D**ata Curation
O : Writing - **O**riginal Draft
E : Writing - Review & **E**diting
Vi : **Vi**sualization
Su : **Su**pervision
P : **P**roject Administration
Fu : **Fu**nding Acquisition

CONFLICT OF INTEREST STATEMENT

The authors declare no conflict of interest.

INFORMED CONSENT

This section is not applicable. This study did not involve human participants, human data, or any personally identifiable information. All data used were either publicly available, fully anonymized, or derived from non-human sources, and therefore no informed consent was required from individuals.

ETHICAL APPROVAL

This section is not applicable. This research did not involve human subjects, human biological materials, or experimental procedures on animals. The work was conducted solely on computational models, publicly available datasets, or non-sensitive data that did not require intervention with living organisms. Therefore, ethical approval from an institutional review board or animal ethics committee was not necessary for this study.

DATA AVAILABILITY

Data availability is not applicable to this paper as no new data were created or analyzed in this study.

REFERENCES

[1] V. P. Kour and S. Arora, "Recent developments of the internet of things in agriculture: a survey," *IEEE Access*, vol. 8, pp. 129924–129957, 2020, doi: 10.1109/ACCESS.2020.3009298.

[2] K. H. Chai, M. M. F. Azizi, S. Romeli, and H. Y. Lau, "A deployment of IoT sensors in the revolution of agriculture," *RA Journal of Applied Research*, vol. 9, no. 6, Jun. 2023, doi: 10.47191/rajar/v9i6.01.

[3] S. Al-Sarawi, M. Anbar, R. Abdullah, and A. B. Al Hawari, "Internet of things market analysis forecasts, 2020–2030," in *2020 Fourth World Conference on Smart Trends in Systems, Security and Sustainability (WorldS4)*, Jul. 2020, pp. 449–453, doi: 10.1109/WorldS450073.2020.9210375.

[4] V. Kumar, K. V. Sharma, N. Kedam, A. Patel, T. R. Kate, and U. Rathnayake, "A comprehensive review on smart and sustainable agriculture using IoT technologies," *Smart Agricultural Technology*, vol. 8, Aug. 2024, doi: 10.1016/j.atech.2024.100487.

[5] R. Chataut, A. Phoummalayvane, and R. Akl, "Unleashing the power of IoT: a comprehensive review of IoT applications and future prospects in healthcare, agriculture, smart homes, smart cities, and Industry 4.0," *Sensors*, vol. 23, no. 16, Aug. 2023, doi: 10.3390/s23167194.

[6] N. M. Priya, "IoT and machine learning based precision agriculture through the integration of wireless sensor networks," *Journal of Electrical Systems*, vol. 20, no. 4s, pp. 2292–2299, Apr. 2024, doi: 10.52783/jes.2399.

[7] T. Chang, T. Watteyne, K. Pister, and Q. Wang, "Adaptive synchronization in multi-hop TSCH networks," *Computer Networks*, vol. 76, pp. 165–176, Jan. 2015, doi: 10.1016/j.comnet.2014.11.003.

[8] J. Xie, X. Tan, and L. Tan, "CR-BA: public key infrastructure certificate revocation scheme based on blockchain and accumulator," *Security and Communication Networks*, vol. 2022, pp. 1–15, Jul. 2022, doi: 10.1155/2022/2069195.

[9] V. A. Thakor, M. A. Razzaque, and M. R. A. Khandaker, "Lightweight cryptography algorithms for resource-constrained IoT devices: a review, comparison and research opportunities," *IEEE Access*, vol. 9, pp. 28177–28193, Jan. 2021, doi: 10.1109/ACCESS.2021.3052867.

[10] C. Gentry, "Certificate-based encryption and the certificate revocation problem," in *Advances in Cryptology—EUROCRYPT 2003*, Berlin, Heidelberg: Springer, 2003, pp. 272–293, doi: 10.1007/3-540-39200-9_17.

[11] S. Itoo, A. A. Khan, M. Ahmad, and M. J. Idrisi, "A secure and privacy-preserving lightweight authentication and key exchange algorithm for smart agriculture monitoring system," *IEEE Access*, vol. 11, pp. 56875–56890, Jun. 2023, doi: 10.1109/ACCESS.2023.3280542.

[12] M. N. Fatima, M. S. Obaidat, K. Mahmood, S. Shamshad, M. A. Saleem, and M. F. Ayub, "Privacy-preserving three-factor authentication protocol for wireless sensor networks deployed in agricultural field," *ACM Transactions on Sensor Networks*, Jul. 2023, doi: 10.1145/3607142.

[13] S. Rostampour *et al.*, "Using a privacy-enhanced authentication process to secure IoT-based smart grid infrastructures," *The Journal of Supercomputing*, vol. 80, no. 2, pp. 1668–1693, Jan. 2024, doi: 10.1007/s11227-023-05535-2.

[14] M. Garai, M. Sliti, M. Mrabet, N. Boudriga, and L. B. Ammar, "Authentication in QoS aware VANET: an approach based on enhanced digital certificates," *IEEE Access*, vol. 12, pp. 124452–124477, 2024, doi: 10.1109/ACCESS.2024.3425053.

[15] X. Liang, Y. Liu, and J. Ning, "An access control scheme with privacy-preserving authentication and flexible revocation for smart healthcare," *IEEE Journal of Biomedical and Health Informatics*, vol. 28, no. 6, pp. 3269–3278, Jun. 2024, doi: 10.1109/JBHI.2024.3391218.

[16] L. Zhang, Y. Zhu, W. Ren, Y. Zhang, and K.-K. R. Choo, "Privacy-preserving fast three-factor authentication and key agreement for IoT-based E-health systems," *IEEE Transactions on Services Computing*, vol. 16, no. 2, pp. 1324–1333, Mar. 2023, doi: 10.1109/TSC.2022.3149940.

[17] G. K.-Kurt, K. N.-Baykal, and E. Ozdemir, "Privacy-preserving authentication scheme for connected autonomous vehicles," *IEEE Transactions on Intelligent Transportation Systems*, vol. 25, no. 6, pp. 4998–5010, Jun. 2024, doi: 10.1109/TITS.2023.3338060.

[18] Y. Song, Y. Zhang, C. Xu, S. Li, A. Yang, and N. Cheng, "Edge-cloud-assisted certificate revocation checking: an efficient solution against irresponsible service providers," *IEEE Internet of Things Journal*, vol. 10, no. 17, pp. 15563–15580, Sep. 2023, doi: 10.1109/JIOT.2023.3264682.

[19] J. Höglund, M. Furuhed, and S. Raza, "Lightweight certificate revocation for low-power IoT with end-to-end security," *Journal of Information Security and Applications*, vol. 73, Mar. 2023, doi: 10.1016/j.jisa.2023.103424.

[20] Y. Li and F. Zhang, "An efficient certificate-based data integrity auditing protocol for cloud-assisted WBANs," *IEEE Internet of Things Journal*, vol. 9, no. 13, pp. 11513–11523, Jul. 2022, doi: 10.1109/JIOT.2021.3130291.

[21] N. Koblitz, "Elliptic curve cryptosystems," *Mathematics of Computation*, vol. 48, no. 177, pp. 203–209, 1987, doi: 10.1090/S0025-5718-1987-0866109-5.

[22] C. Paar, J. Pelzl, and T. Güneysu, "Elliptic curve cryptosystems," in *Understanding Cryptography*, Berlin, Heidelberg: Springer, 2024, pp. 277–298, doi: 10.1007/978-3-662-69007-9_9.

[23] F. Kitagawa, T. Matsuda, and K. Tanaka, "CCA security and trapdoor functions via key-dependent-message security," *Journal of Cryptology*, vol. 35, no. 2, Apr. 2022, doi: 10.1007/s00145-022-09420-8.

[24] D. Hankerson and A. Menezes, "Elliptic curve discrete logarithm problem," in *Encyclopedia of Cryptography and Security*, Boston, Massachusetts : Springer, 2011, pp. 397–400, doi: 10.1007/978-1-4419-5906-5_246.

[25] V. O. Nyangaresi *et al.*, "Message verification protocol based on bilinear pairings and elliptic curves for enhanced security in vehicular ad hoc networks," *Computers, Materials & Continua*, vol. 81, no. 1, pp. 1029–1057, Oct. 2024, doi: 10.32604/cmc.2024.053854.

[26] C. J. F. Cremers, "The Scyther tool: verification, falsification, and analysis of security protocols," in *Computer Aided Verification*, Berlin, Heidelberg: Springer, 2008, pp. 414–418, doi: 10.1007/978-3-540-70545-1_38.

BIOGRAPHIES OF AUTHORS



Dr. Rachid Tahri obtained a master's degree in Networks and Information Systems from the Faculty of Sciences and Techniques, Settat, in 2014, and is currently pursuing a Ph.D. at Hassan First University. His research interests focus on the integration of security within artificial intelligence and machine learning systems. He is the corresponding author of this article. He can be contacted at email: rachid.tahritr@gmail.com.



Dr. Abdellah Ouammou holds a Ph.D. in Applied Mathematics from the Computer, Networks, Mobility and Modeling Laboratory at Hassan First University of Settat, Morocco. He currently serves as a professor at the Ministry of National Education, Preschool and Sports, while being affiliated with the Faculty of Sciences and Techniques of the same university. His academic interests include probability theory, stochastic and discrete optimization, and their applications in cloud computing. He can be contacted at email: a.ouammou@uhp.ac.ma.



Dr. Abdellatif Lasbahani is a professor at Sultan Moulay Slimane University and earned his Ph.D. from Hassan First University. His work focuses on formal methods and artificial intelligence, with an emphasis on modeling complex systems. He actively contributes to research through teaching, publications, and collaborations. He can be contacted at email: abbdellatif.lasbahani@gmail.com.



Dr. Youssef Balouki is a professor at Higher School of Technology, Mohammed V University, Salé, Morocco and earned his Ph.D. from Hassan First University. His work focuses on formal methods and artificial intelligence, with an emphasis on modeling complex systems. He actively contributes to research through teaching, publications, and collaborations. He can be contacted at email: balouki@fst.ac.ma.