

Securing Corporate Data Exchange: An Efficient Identity-Based Authenticated Signcryption Over Elliptic Curves

Minh Tu Le, Van Nghi Nguyen(✉), Hanh Thi Tran, Minh Thang Vu, and Van Duan Nguyen

Academy of Cryptography Techniques, Hanoi, Vietnam
{nghinv,hanhtt,thangvm,nguyenvanduan}@actvn.edu.vn

Abstract. In this paper, we propose a lightweight signcryption scheme integrating an identity based signature and the Ascon cipher for applications in authentication and data security of enterprise network environments. Our objective is to provide a secure signcryption scheme that combines public key distribution and user authentication with identity information at a reduced implementation cost compared to using PKI system. The proposed scheme is designed for application to the S/MIME protocol to ensure secure email communication in enterprise network environments. We conduct a thorough analysis of the security measures and compare the computational overhead of the proposed scheme with other published works that use PKI system. This will enable us to determine the level of security and efficiency offered by the proposed scheme.

Keywords: Ascon cipher · Elliptic curve · Identity based signature · Signcryption

1 Introduction

Signcryption, a cryptographic technique established by Zheng in 1997 [1], combines the processes of signature and encryption inside a single scheme. In the last 10 years, there have been many publications on signcryption schemes [2–9]. These schemes all include two cryptographic primitives: public key cryptography and a secret key cryptosystem. The public key cryptography used can be on finite fields such as RSA, Elgamal cryptosystem, or elliptic curve cryptosystem. Elliptic curve cryptographic schemes have small key lengths while having the same security as finite field cryptographic schemes based on RSA and Elgamal. Currently, computer networks are used in several aspects of human activity, including employment, education, commerce, and entertainment. Authentication of entities and communication data in computer networks regarding identity and origin is a critical information security concern. In contemporary computer networks, this task is accomplished by cryptographic methods, including digital signatures and digital certificates provided by a Public Key Infrastructure (PKI) from a trusted third party inside the network.

© The Author(s), under exclusive license to Springer Nature Switzerland AG 2027
O. Gervasi et al. (Eds.): ICCSA 2026, LNCS 16767, pp. 3–17, 2027.
https://doi.org/10.1007/978-3-032-30491-9_1

In this paper, the problem we are interested in is the way of exchanging public keys between communicating parties. In [2–4, 6], finite-field signcryption schemes are integrated with a method of distributing public keys directly through a public channel and verification based on identification. Paper [5] propose an elliptic curve signcryption scheme based on the theory of linear pairs, and the distribution and authentication of public keys are also based on user identification. The signcryption schemes of [7, 8] are based on using the PKI system to exchange public keys, and the publication of [9] establishes a trusted management server to be able to distribute and authenticate public keys for the elliptic curve signcryption scheme.

For elliptic curve signcryption schemes, the method of exchanging public keys between communicating parties through identification has only been published in the direction of using cryptography on linear pairs; however, there is no published standard on ensuring security for this type of cryptography. The utilization of the PKI system necessitates both parties involved in communication to acquire digital certificates from this infrastructure, resulting in substantial expenses for deployment and installation. This approach is particularly unsuitable for network environments with a large number of users, as it is impractical to compel ordinary network users or IoT devices to obtain and purchase digital certificates. In this paper, we propose a lightweight signcryption scheme for data security in the enterprise network environments. Our proposed scheme has a different approach that employs an identity-based key generation mechanism for generating user key pair, allowing user to directly exchange public keys with each other. Furthermore, it utilizes identity information and public key for user authentication. The deployment of identity-based key pairs for users reduces dependence on PKI, thereby simplifying deployment, reducing operational costs, and improving system scalability. This approach still helps the proposed signcryption scheme, in addition to ensuring the general security goals of a signcryption scheme such as confidentiality, integrity, origin authentication, data tampering, and non-repudiation. It also ensures user authentication, forward security, internal security, and especially low computational overhead, making it easy to install and deploy. The proposed signcryption scheme is applied to email security, specifically by applying it to the S/MIME protocol to secure end-to-end email communication between two parties. The security properties of the proposed scheme will be analyzed in detail in this paper. We also compare the computational cost and implementation performance with published elliptic curve signcryption schemes using trust centers to distribute public keys, such as [9].

This paper consists of 6 main sections. After the introduction in Sect. 1, we present the theoretical foundations of the signcryption scheme, the identity-based signature scheme, and other cryptographic primitives in Sect. 2. These are the foundations for proposed signcryption scheme for application in the data security of enterprise network environments in Sect. 3. The security properties of the proposed scheme are analyzed in Sect. 4. In Sect. 5, we discuss the computational overhead and performance of the proposed scheme with some other publications. Finally, Sect. 6 concludes the paper.

2 Preliminaries

This section provides the theoretical foundation for the scheme presented in this work. It will cover the definition and characteristics of the signcryption scheme, the identity-based signature scheme and elliptic curve cryptography, as well as the Ascon cipher.

2.1 Signcryption Scheme

A typical signcryption scheme consists of four algorithms: Setup (SU), Key generation (KG), Signcryption (SC) and Unsingcryption (USC). In which the SU algorithm declares the domain parameters of the cryptographic primitives used in the signcryption scheme, KG is the algorithm for generating key pairs for participating users, SC is the algorithm for encrypting data and signing probabilistically, and USC is the algorithm for verifying digital signatures and decrypting data. Any signcryption scheme must provide two properties: efficiency, and security.

- Efficiency: The computational and communication overhead of a signcryption scheme should be less than the best alternative of a signature then encryption scheme using similar functionalities.
- Security: Any signcryption scheme must achieve four main security properties: confidentiality, unforgeability, integrity, and non-repudiation. In addition, some signcryption schemes also provide additional security properties such as public verifiability and forward secrecy of message confidentiality.

2.2 Identity-Based Signature

The identity-based signature (IBS) was first introduced by Adi Shamir in 1984 [11], with the objective of reducing reliance on PKI and digital certificates, thereby simplifying deployment and reducing operational costs. In [11], the user's public key can be derived from their identity information, such as the email address, phone number, personal identifier, or IP address. The corresponding secret key is issued by a trusted Key Generation Center (KGC). An IBS scheme typically consists of the following main processes:

a) Key Generation Process
This process takes as input a secret parameter λ (a positive integer). The output is a master key pair (m_{pk}, m_{sk}), where m_{pk} is master public key and m_{sk} is master secret key. The key generation process is performed by the KGC.

b) Key Extraction Process
This process takes as input the user's identity id and the master key pair (m_{pk}, m_{sk}). . The output is a key pair (pk_{id}, sk_{id}), where pk_{id} is user's public key and sk_{id} is user's secret key. The key extraction process is performed by the KGC.

c) Signing Process
This process takes as input the message m and the signer's secret key sk_{id}. The output is a digital signature s. The signing process is performed by the signer.

d) Verification Process
This process takes as input the message m, the digital signature s and the signer's public key pk_{id}. The output is a message about whether the signature is valid or invalid. The verification process is performed by the verifier.

2.3 Elliptic Curves

a) Elliptic Curves in Weierstrass Form
An elliptic curve over the finite field F_p is defined as the set of points $(x, y) \in F_p$ that satisfy the following equation:

$$y^2 \equiv x^3 + ax + bmodp \tag{1}$$

where $a, b \epsilon F_p$ and $4a^3 + 27b^2 modp \neq 0$. The elliptic curve is denoted by $E_p(a, b)$. The point O is the infinity point on the elliptic curve $E_p(a, b)$. Equation (1) defines the elliptic curve in Weierstrass form.

b) Point Addition in Weierstrass Form
Given $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ are two points on $E_p(a, b)$. The rules for point addition on $E_p(a, b)$ are defined as follows:

1) $P_1 + O = O + P_1 = P_1$.
2) If $x_1 = x_2$ and $y_1 = -y_2 modp$ (i.e. $P_1 = -P_2$), then $P_1 + P_2 = O$.
3) If $P_1 \neq -P_2$ then $P_1 + P_2 = P_3 = (x_3, y_3)$:

$$x_3 = \left(\lambda^2 - x_1 - x_2\right) modp.$$

$$y_3 = (\lambda(x_1 - x_3) - y_1) modp.$$

where:

$$\lambda = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1} incaseofP \neq Q \\ \frac{3{x_1}^2 + a}{2y_1} incaseofP = Q \end{cases}$$

c) Scalar Multiplication in Weierstrass Form

$$Q_1 = t \cdot P_1 = P_1 + P_1 + P_1 + \cdots + P_1(ttimes), \text{ where } t < p.$$

2.4 Ascon-128 Cipher

Ascon cipher was chosen by US National Institute of Standards and Technology (NIST) for future standardization of the lightweight cryptography in 2023.

The ciphers are parameterizable by the key length k (up to 128 bits), "rate" (block size) r, and two numbers of rounds n_1, n_2. All algorithms support authenticated encryption with plaintext P and additional authenticated data A (that remains unencrypted). The encryption input also includes a public nonce N, the output - authentication tag T, size of the ciphertext C is the same as that of P. The decryption uses N, A, C, and T as inputs and produces either P or signals verification failure if the message has been altered. Nonce and tag have the same size as the key K (k bits).

3 Proposed an Efficient and Secure Identity-Based Authenticated Signcryption Scheme Over Elliptic Curve Applied in Enterprise Network Environment

In this section, we first analyze the enterprise network model and then propose a signcryption technique designed for data security in this specific network model, specifically applying it to the S/MIME protocol. Subsequently, we evaluate the correctness of the proposed scheme.

3.1 Application of the S/MIME Protocol for Data Security in Enterprise Network Model

Consider the common enterprise network architecture shown in Fig. 1, which consists of an internal network (LAN), servers (Email and Authentication), a Certificate Authority (CA), switch devices (S1, S2), a router with an integrated firewall, and the Internet. The Authentication Server (AS) will possess a digital certificate that includes both a public key and a private key. This certificate will be issued by a trusted third-party CA and transmitted through a secure channel. For the users to access the Email Server and utilize email services, it is necessary to perform authentication with the AS.

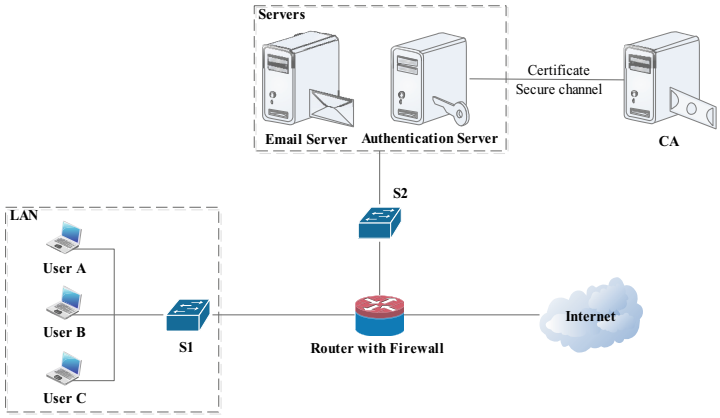

Fig. 1. Enterprise network model

In modern enterprise environments, email serves as a primary communication channel for information exchange among users and departments. Through email systems, various critical data are transmitted, including sensitive information such as financial records, employee and customer personal data, business documents, and contracts,… The exchange of such sensitive information via email necessitates the implementation of appropriate security mechanisms to protect data during transmission. In this context, cryptographic techniques, including encryption and digital signatures are employed to ensure the fundamental security properties of the information: confidentiality, integrity, authentication, and non-repudiation. In a typical enterprise network model, as shown in

Fig. 1, achieving end-to-end email security between users A and C requires the application of the S/MIME protocol. S/MIME provides security mechanism for email messages by combining digital signatures and encryption. This security mechanism is illustrated in Figs. 2 and 3.

In a typical enterprise network model, as shown in Fig. 1, achieving end-to-end email security between users A and C requires the application of the S/MIME protocol. S/MIME provides security mechanism for email by combining digital signatures and encryption. This security mechanism is illustrated in Figs. 2 and 3.

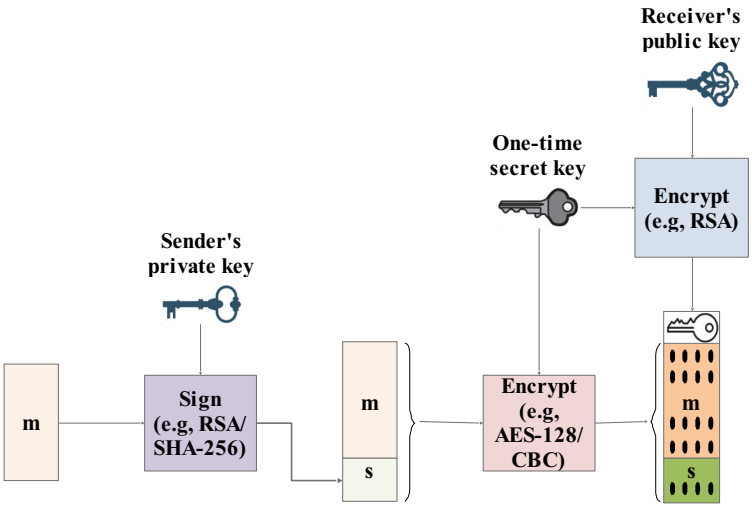

Fig. 2. S/MIME signcryption process

Figure 2 illustrates the signcryption process in the S/MIME protocol. This process consists of the following steps:

1) The Sender creates a message *m*.
2) The Sender uses RSA/ SHA-256 with their private key to generate a digital signature *s* for *m* and then *s* is attached to *m*.
3) The Sender generates a one-time secret key.
4) The message *m* and signature *s* are encrypted as a single block with AES-128/CBC using the one-time secret key.
5) The one-time secret key is encrypted with RSA using the Receiver's public key and the result is appended to the ciphertext of *m* and *s*.

Figure 3 illustrates the unsigncryption process in the S/MIME protocol. This process consists of the following steps:

1) The Receiver uses RSA with its private key to decrypt and recover the one-time secret key.
2) The one-time secret key is used to decrypt and recover the *m* and *s*.
3) The Receiver uses RSA/ SHA-256 with the Sender's public key to verify digital signature *s*. If the signature *s* is valid, the message *m* is accepted.

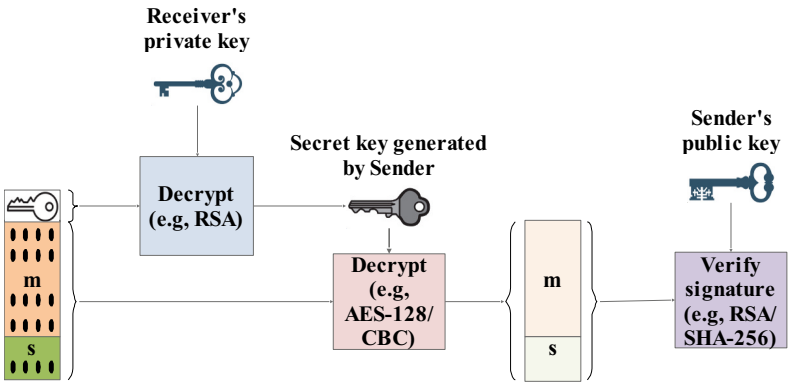

Fig. 3. S/MIME unsigncryption process

In the email security model using S/MIME, each user must possess a public/ private key pair to perform digital signature and email encryption functions. In practice, to ensure the authenticity and reliability of private keys, users typically obtain digital certificates from a trusted third-party CA or deploy an internal PKI to manage and distribute certificates. However, this approach leads to several limitations, including complex deployment and management processes, high operational costs, and limited scalability as the number of users increases.

Therefore, this paper proposes an identity-based authenticated signcryption scheme that reduces reliance on digital certificates and PKI. The scheme is designed for application to the S/MIME protocol in enterprise network environments, offering low cost and ease of deployment, while preserving the essential security properties of email: authentication, confidentiality, integrity, and non-repudiation. The proposed scheme focuses on two main components: a user key generation mechanism based on identity information and a signcryption scheme integrating identity-based authentication.

3.2 Proposed Identity-Based Key Generation Mechanism in Enterprise Network

Firstly, we propose a method for generating a user's key pair based on identity information in the enterprise network system.

Figure 4 illustrates the user key generation process based on identity information. Specifically, the user first sends their identity (ID) to the AS. The server then generates and issues an identity-based key pair to the user over a secure communication channel. In this process, the key pair (mpk, msk) is used as input parameters, where mpk denotes the master public key and msk denotes the master secret key. This master key pair (mpk, msk) is issued by a trusted third-party CA and distributed to the AS via a digital certificate. The certificate is transmitted over a secure channel and this master key pair is owned by the AS. The identity-based key generation mechanism is presented in Fig. 5.

The key generation mechanism utilizes an elliptic curve $E_p(a, b)$ with base point G and degree n as domain parameters. Additionally, a secure hash function H is employed.

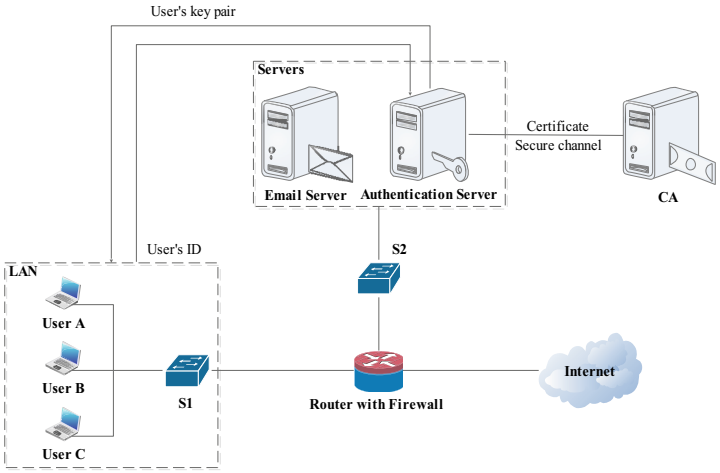

Fig. 4. Key generation process based on user's identity

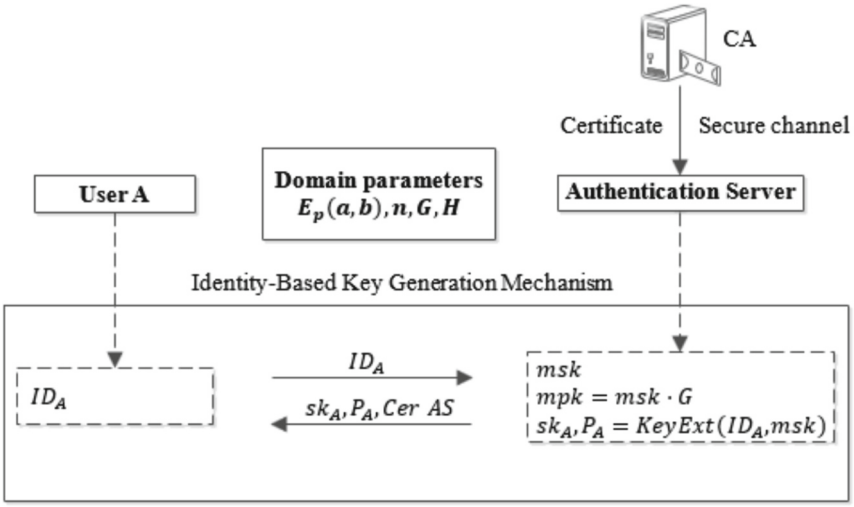

Fig. 5. Identity-based key generation mechanism

First, user A sends its identity ID_A to the AS. Then, the AS generates a key pair for A using the Key Extraction Algorithm.

Key Extraction Algorithm

This algorithm takes as input parameters the identity ID_A and the mater key pair (mpk, msk). The output parameter is the A's key pair (P_A, sk_A), where P_A denotes the public key and sk_A denotes the secret key. This algorithm works as follows:

1) Randomly generate an integer *nonce* such that $0 < nonce < n$
2) Compute $l_A = H(msk \| ID_A \| nonce) mod n$

3) Compute $F_A = l_A \cdot G$ and set $p_A \equiv x_{F_A} modn$, where x_{F_A} is the x coordinate of point F_A. If $p_A = 0$, go back to step 1
4) Compute $t_A = H(mpk \| ID_A) modn$. If $t_A = 0$ then set $t_A = 1$
5) Compute $sk_A \equiv (p_A \cdot msk + l_A \cdot t_A) modn$. If $sk_A = 0$, go back to step 1
6) Compute $P_A = sk_A \cdot G$

The AS transmits the identity-based key pair (P_A, sk_A), the point F_A and the digital certificate *CerAS* to user A via a secure communication channel. The process of issuing identity-based key pairs for other users in the enterprise network model is similar to that for user A described above.

Public Key Verification Process
In the proposed approach, it is not necessary to deploy a PKI infrastructure to authenticate the public key P_A of user A. Instead, the validity of P_A can be verified through the following steps:

1) A sends the parameters ID_A, P_A, F_A to the verifier
2) The AS transmits the master public key mpk to the verifier. The verifier can then authenticate the validity of mpk through a PKI
3) Verifier computes $p_A \equiv x_{F_A} modn$, where x_{F_A} is the x coordinate of point F_A
4) Verifier computes $t_A = H(mpk \| ID_A) modn$. If $t_A = 0$ then set $t_A = 1$
5) Verifier checks the equation $P_A = p_A \cdot mpk + t_A \cdot F_A$. If it is satisfied, then P_A is valid. Otherwise, P_A is invalid.

Under this approach, the public key of user A is verified by the verifier using A's identity information and the master public key of the AS.

3.3 Operation of the Proposed Signcryption Scheme

Assume that two users A and C in the enterprise network model shown in Fig. 1 who intend to perform signcryption and exchange electronic documents. Initially, each user must possess an identity-based key pair. These key pairs are generated and issued by the Authentication Server; with A receiving (P_A, sk_A) and C receiving (P_C, sk_C). The identity-based key generation process is detailed in Sect. 3.2. In this scenario, the IB-SCECC signcryption scheme is employed.

The proposed signcryption scheme (IB-SCECC) utilizes an elliptic curve $E_p(a, b)$ with base point G and degree n. Furthermore, the Ascon cipher and the secure hash function H are employed. The IB-SCECC scheme consists of two main processes: the signcryption process and the unsigncryption process.

a) Signcryption Process
This process is performed by A. Additionally, A also receives the parameters ID_C, P_C and F_C from C, which enable A to verify the validity of C's public key P_C. The public key verification process is detailed in Sect. 3.2.

Using the key pair (P_A, sk_A), A executes the signcryption process. Specifically, A first generates a signature (r, s) for the message m and attaches (r, s) to m. Then, A computes a session key K and employs it to encrypt the plaintext pt consisting of m

and (r, s) using the Ascon cipher. Finally, A obtains the ciphertext ct and transmits it to C along with ID_A, ts and the point I. The signcryption process is described in detail in Fig. 6.

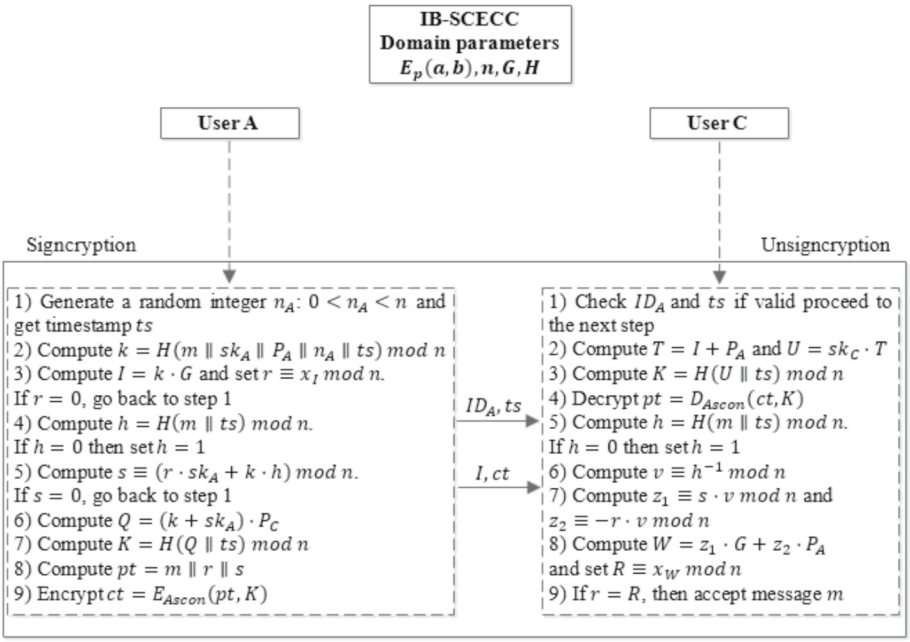

Fig. 6. IB-SCECC signcryption scheme

b) Unsigncryption Process

This process is performed by C. Additionally, C also receives the parameters ID_A, P_A and F_A from A, which enable C to verify the validity of A's public key P_A. The public key verification process is detailed in Sect. 3.2.

User C first verifies the validity of ID_A and ts. Next, C computes a session key K and employs it to decrypt the ciphertext ct using the Ascon cipher to recover the plaintext pt, which includes m and (r, s). Finally, C verifies the validity of the signature (r, s) associated with m. The message is accepted if the signature is valid, otherwise, it is rejected. The unsigncryption process is described in detail in Fig. 6.

3.4 Correctness of the Proposed Signcryption Scheme

For the proposed signcryption scheme, correctness is guaranteed when the following two conditions are satisfied:

- The secret session key computed on both communicating parties is the same.
- The digital signature for message m is valid.

The Correctness of the Session Key Calculated on Both Communicating Sides
To ensure the correctness of the scheme, the session keys computed by both communicating parties must be proven to be the same, i.e., $K = H(Q\|ts)modn = H(U\|ts)modn$. Consider $K = H(Q\|ts)modn$ is calculated at user A side, $K = H(U\|ts)modn$ is calculated at user C side. We only need to show that $Q = U$.

Specifically, $Q = (k + sk_A) \cdot P_C = k \cdot P_C + sk_A \cdot P_C = k \cdot P_C + sk_A \cdot sk_C \cdot G$. On the other hand, $U = sk_C \cdot T = sk_C \cdot I + sk_C \cdot P_A = k \cdot P_C + sk_A \cdot sk_C \cdot G$.

Therefore, we have $Q = U$, that is the session key calculated at both communication sides is the same.

The Correctness of the Signature Verification
User C accepts the message m only if the digital signature is valid i.e., if it can verify that the values r and R are equal. Since $r \equiv x_I modn$ and $R \equiv x_W modn$, we only need to show that the point I equals point W.

Specifically, $I = k \cdot G$. On the other hand, $W = z_1 \cdot G + z_2 \cdot P_A = G \cdot (s \cdot v - r \cdot v \cdot sk_A) = G \cdot ((r \cdot sk_A + k \cdot h) \cdot v - r \cdot sk_A \cdot v) = G \cdot (r \cdot sk_A \cdot v + k \cdot h \cdot v - r \cdot sk_A \cdot v) = G \cdot (k \cdot h \cdot h^{-1}) = k \cdot G$.

So, we have $I = W$ and $r = R$ ensures that C can verify the correctness of user A's signature.

Therefore, our signcryption scheme is correct.

4 Security Analysis

The proposed signcryption scheme employs an Identity-based key generation mechanism to generate a key pair for users and the Ascon cipher for encryption, so the security properties provided by the scheme include user authentication, confidentiality, unforgeability, integrity and non-repudiation, forward security, and internal security. Now, we will examine each of these properties thoroughly.

User Authentication: User C can always authenticate user A by using the Public Key Verification Process with the identity information and public key received from A as inputs. If A's public key is invalid, C terminates the unsigncryption process and discards the ciphertext. On the other hand, A can also authenticate C.

Confidentiality: The proposed scheme provides confidentiality for two objects: the plaintext and the session key. The confidentiality of the plaintext is ensured by the Ascon symmetric encryption algorithm. Currently, there is no theoretically effective attack that can completely break the Ascon cipher [10]. The session key is calculated based on hashing and point multiplication on secp256r1. Therefore, session key secrecy is based on ECDLP, and since secp256r1 is used, solving this ECDLP problem in polynomial time is infeasible when using the domain parameter secp256r1 with modulo p and order n of ~ 256 bits.

Unforgeability: The proposed scheme provides unforgeability for two objects: the identity-based key pair and the digital signature.

The attacker attempts to forge the identity-based key pair of user A by generating the forged parameters $ID_A\prime$, $sk_A\prime$, and $P_A\prime$. However, these parameters cannot be equal to ID_A, sk_A and P_A, since sk_A and P_A are generated by the Authentication Server through

the Key Extraction Algorithm using identity information of A (ID_A) and the master secret key of the Authentication Server (msk) as inputs. As the adversary does not know ID_A or sk_B, it follows that $ID_A\prime \neq ID_A$, $sk_A\prime \neq sk_A$ and $P_A\prime \neq P_A$.

Thus, the forgery of the identity-based key pair is not possible in the proposed signcryption scheme.

The attacker attempts to forge A's signature for message m using the forged parameters $k\prime$, $r\prime$, $h\prime$, $sk_A\prime$, $P_A\prime$. Then the signature $s \equiv (r\prime \cdot sk_A\prime + k\prime \cdot h\prime) mod n$ and $Q = (k\prime + sk_A\prime) \cdot P_B$ leads to $r\prime \neq R$. Furthermore, the session key $K = H(Q \| ts) mod n$ computed by attacker is different from the session key $K = H(sk_C \cdot (I + P_A) \| ts) mod n$ computed by user C. Thus, the decryption process is unsuccessful.

Therefore, signature forgery is infeasible in the proposed signcryption scheme.

Integrity and Non-repudiation: The message m is guaranteed to be intact and non-repudiable by the proposed signcryption scheme because it uses the digital signature algorithm incorporating the secure hash function.

Forward Security: The session key of the proposed signcryption scheme will be unique for each communication session because it depends on the plaintext, the key pair of user A, the public key of user C, the timestamp at the time of signing, and a randomly generated nonce value during the Signcryption process. This leads to the fact that if the session key or private key sk_A at time ts_2 is leaked, the attacker cannot find the session key at time ts_1.

Internal Security: Internal security is known in two cases: one is that an attacker knowing the user A's secret key cannot recover the message m from the ciphertext, and two is that an attacker knowing the user C's secret key cannot forge the previously received ciphertext.

In the proposed signcryption scheme, if the attacker knows the secret key sk_A, recovering m from the ciphertext ct requires knowing the session key K. However, the session key K is generated by the SHA-256 hash function of point Q, and Q is calculated from the generated value k, which depends on the pseudorandom nonce value n_A generated once for the communication session. Therefore, based on the collision resistance of SHA-256 and the one-time use of the nonce, the adversary cannot recover the original message m from the ciphertext ct.

Even if the adversary obtains the C's secret key sk_C, they cannot fabricate the valid ciphertext $ct\prime$ for message $m\prime$, since generating a valid signature for this ciphertext $ct\prime$ requires the sender's secret key sk_A, which is unavailable to the adversary.

Therefore, the proposed signcryption scheme is internally secure.

5 Comparison of Security and Performance Property of the Proposed Scheme with Other Publications

5.1 Comparison of Security Properties

In this section, we compare the security properties of the proposed signcryption scheme with some other methods published in the past 10 years. The compared signcryption schemes must use the same elliptic curve digital signature schemes. The comparison

results in terms of security properties between these schemes and our proposed scheme are described in Table 1. The security properties compared include user authentication (UA), confidentiality (CF), unforgeability (UF), integrity and non-repudiation (IT&NR), forward security (FS), and internal security (IS). All the signcryption systems listed in Table 1 include support for user authentication. However, the authentication mechanism is presented in a different manner here, for example, using the PKI system, using a Management Server (MS), and using Identity and public key (ID&PK). For other properties, there are only two options: "Y" which means provided, or "N," which means not provided. Table 1 demonstrates that our suggested signcryption scheme and Zhang's scheme successfully fulfills all six security characteristics.

Table 1. Comparison of security properties of the signcryption schemes

Scheme	UA	CF	UF	IT&NR	FS	IS
Tsai's scheme [7]	PKI	Y	Y	Y	N	N
Malik's scheme [8]	PKI	Y	Y	Y	N	N
Zhang's scheme [9]	MS	Y	Y	Y	Y	Y
Our scheme	ID&PK	Y	Y	Y	Y	Y

5.2 Performance Comparison and Evaluation

We compare and evaluate the performance of the proposed scheme with other publications according computational overhead. The computational overhead of the schemes will be measured by the number of calculations such as Point Multiplication (PM), Point Addition (PA), Modular Multiplication (MM), Modular Addition (MA), Hash Function (H), Inversion Operation (IO), Encryption (EN), and Decryption (DE) with specific measured data in Table 2.

Note that PKI, MS, and Identity are the methods of establishing and registering the signcryption scheme, in which MS is the trusted management server used to distribute session keys. Based on experimental results of calculations on secp256r1 curve and averaged over about 100 runs on the same computer Laptop Dell Precision 3520 Intel Core i7-8750H 2.20GHz processor, 16 GB of RAM, and Windows 11. We give the experimental implementation time of the calculations on secp256r1 as PM = 7.498 ms, PA = 2.760 ms, MM = 1.609 ms, MA = 1.301 ms, H = 1.938 ms, IO = 4.995 ms.

Table 2. Comparison of security properties of the signcryption schemes

Scheme	Method for registration	Signcryption	Unsigncryption
Tsai's scheme [7]	PKI	4PM + 2MM + 1MA + 2H + 1EN	3PM + 3PA + 3MM + 2MA + 1H + 1DE

(*continued*)

Table 2. (*continued*)

Scheme	Method for registration	Signcryption	Unsigncryption
Malik's scheme [8]	PKI	6PM + 1PA + 3MM + 5MA + 2H + 2IO + 1EN	3PM + 2PA + 2MM + 2H + 1IO + 1DE
Zhang's scheme [9]	MS	1PM + 1MM + 1MA + 2H + 1IO + 1EN	2PM + 1PA + 2MM + 2H + 1IO + 1DE
Our scheme	ID	2PM + 2MM + 2MA + 3H + 1EN	3PM + 2PA + 2MM + 2H + 1IO + 1DE

Based on the information shown in Table 2, it is evident that our proposed scheme and Zhang's system have similar computing costs, making them the two schemes with the most favorable computational costs. However, when evaluating the computational overhead of the KU/Registration process, the utilization of a PKI or MS system necessitates a complicated server installation procedure, a multi-step key calculation/checking procedure, and a database for device logins with a secure transmission using TLS. This results in a significant increase in computational overhead when compared to our suggested scheme.

6 Conclusion

In this paper, we have proposed a lightweight identity-based authenticated signcryption scheme (IB-SCECC) over elliptic curves that integrates an efficient identity-based key generation mechanism with the Ascon cipher. The scheme effectively eliminates the heavy reliance on traditional PKI systems by enabling direct public key exchange and verification through users' identity information. Security analysis demonstrates that our proposed scheme fully satisfies essential security requirements including confidentiality, integrity, user authentication, unforgeability, non-repudiation, forward security, and internal security. Performance evaluation shows that the computational overhead of the scheme is competitive and even lower than several existing elliptic curve signcryption schemes while offering much simpler key management. The proposed IB-SCECC scheme is designed to be easily applied to the S/MIME protocol, providing secure end-to-end email communication in enterprise network environments. In future work, we plan to further optimize the implementation and extend the scheme to other network services and IoT devices.

References

1. Zheng, Y.L.: Digital signcryption or how to achieve cost (signature) + cost (encryption). In: CRYPTO 1997. LNCS, vol. 1294, pp. 165–179, Springer, Berlin (1997). https://doi.org/10.1007/BFb0052234

2. Pandit, T., et al.: Attribute-based signcryption: signer privacy, strong unforgeability and IND-CCA2 security. In: ProvSec 2014. LNCS, vol. 8782, pp. 274–290 (2014). https://doi.org/10.1007/978-3-319-12475-9_19
3. Zhang, X., et al.: Revocable identity-based signcryption scheme without random oracles. J. Network Secur. **17**(2), 110–122 (2015)
4. Datta, P., et al.: Compact attribute-based encryption and signcryption for general circuits from multilinear maps. In: INDOCRYPT 2015, LNCS, vol. 9462, pp. 3–24 (2015). https://doi.org/10.1007/978-3-319-26617-6_1
5. Kar, J.: Provably secure identity-based aggregate signcryption scheme in random oracles. Int. J. Network Secur. **17**(5), 580–587 (2015)
6. Yi, M.: Efficient identity-based online and offline signcryption with short ciphertext. Int. J. Inf. Secur. **16**, 299–311 (2017)
7. Tsai, C., Su, P.: An ECC-based blind signcryption scheme for multiple digital documents, security and communication networks. Secur. Commun. Netw. **2017**, 1–14 (2017)
8. Bashir, M.Z.U.: Analysis and improvement of some signcryption schemes based on elliptic curve. Doctor of Philosophy, Department of Mathematics, Capital University of Science and Technology Islamabad, p.159 (2022)
9. Zhang, P., Li, Y., Chi, H.: An elliptic curve signcryption scheme and its application. Wirel. Commun. Mob. Comput. **2022**, 7499836 (2022)
10. Dobraunig, C., et al.: Ascon v1.2: lightweight authenticated encryption and hashing. J. Cryptology **34**(3) (2021)
11. Shamir, A.: Identity based cryptosystems and signature schemes. In: Advances in Cryptology–Crypto' 84, LNCS 196, pp. 47–53, Springer, Berlin, Heidelberg (1984). https://doi.org/10.1007/3-540-39568-7_5