IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received March 1, 2022, accepted March 20, 2022, date of publication March 25, 2022, date of current version April 1, 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3162231

Attribute-Based Blind Signature Scheme Based on Elliptic Curve Cryptography

RUI MA[1] AND LINYUE DU[2]
[1]Xingzhi College, Zhejiang Normal University, Jinhua 321004, China
[2]Personnel Department, Zhejiang Normal University, Jinhua 321004, China

Corresponding author: Linyue Du (duly@zjnu.edu.cn)

ABSTRACT Blind signature is a special digital signature that allows the signer to sign a document without knowing its content. However, in many situations, multiple people need to blindly sign messages. At this time, the traditional blind signature can no longer satisfy the application requirements. To solve this problem, attribute-based cryptography has been combined with the blind signature. The concept of the attribute-based blind signature is generated. At present, all attribute-based blind signature schemes require the support of bilinear pairing technology, which involves several complex pairing and exponential operations in the signature and verification processes, and the computational efficiency is not high. In this paper, we present an attribute-based blind signature scheme based on elliptic curve cryptography (ECC), and the security of new scheme is proved under the intractability of elliptic curve discrete logarithm problem (ECDLP). Our scheme is a key policy attribute-based signature (KP-ABS). The new scheme uses linear secret sharing scheme (LSSS) matrix technology that does not require recursive operation to achieve more flexible and fine-grained access control. In addition, the scheme is based on Elliptic Curve Cryptography (ECC) using scalar multiplication on an elliptic curve instead of a bilinear pairing operation. Our scheme has significant advantages in terms of computational efficiency and storage compared with existing attribute-based blind signature schemes.

INDEX TERMS Attribute-based, blind signature, elliptic curve cryptography (ECC), elliptic curve discrete logarithm problem (ECDLP), key policy attribute-based signature, LSSS matrix.

I. INTRODUCTION

In 1982, Chaum first proposed the blind signature [1], which is a digital signature that can protect user privacy. Blind signature enables the signer to sign the document without knowing the content of the signed document. In addition, the signer cannot match the signature obtained by the message owner unblinded to the blind signature with the message signed by him/herself. Therefore, blind signatures are widely used on many occasions that require anonymity and authentication, such as electronic cash, electronic auctions, electronic voting and other places. Since then, blind signatures have attracted considerable research attention. Various blind signature schemes have been proposed. These blind signature schemes are often one-to-one; that is, one person blindly signs the message and one person verifies the validity of the blind signature. However, in many situations, multiple people who meet certain attributes or access structures must blindly sign messages. Obviously, a traditional blind signature can no longer satisfy the application requirements. To solve this problem, attribute-based cryptography and blind signatures are combined to produce the concept of the attribute-based blind signature.

Attribute-based cryptography can realize fine-grained access control, and has become a very active topic in the development of cryptography in recent years because of its broad application prospects. Attribute-based signature (ABS) extends identity-based signatures. Signers are defined as a set of attributes or access structures in attribute-based signature schemes. When the signer satisfies the corresponding attributes or access structures, the signer can use a private key to sign the message. The verifier only knows that the signer satisfies the corresponding attribute or access structure but does not know the identity information of the signer. Attribute-based signatures can be classified into signature policy attribute-based signatures (SP-ABS) and key policy

The associate editor coordinating the review of this manuscript and approving it for publication was Shuai Liu.

attribute-based signatures (KP-ABS) according to access policy. In SP-ABS, the key generation algorithm needs to input a set of signer attributes, and the signature algorithm is completed by the access structures and the private key. KP-ABS requires the key generation algorithm to input access structures, and the signature algorithm is completed by the attribute set and private key.

On the one hand, attribute-based blind signature has the characteristics of blind signature, and on the other hand, it can also implement fine-grained access control, allowing signers that satisfy certain attributes or access structures to blindly sign messages. However, existing attribute-based blind signature schemes are all supported by bilinear pairings, which involve several complex pairing and exponential operations in the process of signature and verification, resulting in low computational efficiency [2].

In addition, current attribute-based blind signature schemes are based on the access tree structure. The access tree structure can represent flexible access control policies. However, because the access structure is represented as a tree, recursion is required to perform operations. When the recursion depth reaches a certain level, the running time space of the program is affected to a certain extent. The linear secret sharing scheme (LSSS) access structure solves this problem well. LSSS uses the linear recombination property of the linear secret-sharing scheme to reconstruct secrets without recursive operation, which is more efficient, and the expressivity of LSSS and the access tree structure is equivalent.

Based on the above background, we propose an attribute-based blind signature scheme based on elliptic-curve cryptography. The new scheme uses scalar multiplication on an elliptic curve instead of a bilinear pairing operation, which reduces the overhead of signature and verification and solves the problem that recursion is required to the access tree structure.

A. RELATED WORKS

In 1983, Chaum proposed a blind signature scheme based on RSA [3], which can be used in electronic payment systems. In 1992, Okamoto proposed the Schnorr blind signature scheme [4] based on the Schnorr digital signature system. Compared to the previous RSA blind signature scheme, it has higher security and efficiency. In 1994, Camenisch *et al.* [5] presented two blind signature schemes based on a discrete logarithm problem. In 2000, Mohammed *et al.* proposed a blind signature scheme [6] based on an ElGamal digital signature system. In 2003, Chang *et al.* constructed a blind signature scheme [7] by transforming the Schnorr signatures based on elliptic curves. In 2018, Tsaur *et al.* proposed an effective PBS scheme [8] and analyzed the safety of this scheme under the assumption of an elliptic curve discrete logarithm problem (ECDLP). In 2020, Duong *et al.* proposed a post-quantum blind ring signature scheme [9], which was constructed based on multivariate public key cryptography. In 2021, Huang *et al.* proposed an ECDSA-based partially blind signature scheme [10] compatible with the current bitcoin protocol.

Khader proposed an attribute-based group signature scheme in 2007 [11], in which members of the group satisfying certain attributes can sign, and the verifier can judge the true identity of the signer. In 2008, Maji *et al.* proposed an attribute-based signature scheme [12], where the signer's key is associated with its own attributes, and the scheme satisfies strong unforgeability. Subsequently, in 2009, an attribute-based signature scheme [13] that supports threshold access structures was proposed. In 2010, Maji *et al.* [14] proposed a general framework for attribute-based signature schemes, as well as several bilinear pair-based schemes. In 2014, the scheme proposed by Rao *et al.* [15] adopted the LSSS access policy, which can implement fine-grained access control more flexibly than the threshold access structure. In 2015, Kaafarani *et al.* [16] proposed three attribute-based signature schemes, namely DTABS, ABS-UCL, and ABS-HEP. Rani *et al.* [17] proposed a new ABS scheme with an access tree structure in 2017, which supports the flexible access control of AND and OR. In 2018, Guo *et al.* [18] proposed a multi-attribute-centric attribute-based signature scheme and applied it to electronic health-record systems. In 2020, Wang *et al.* proposed two efficient pairing-free ciphertext-policy attribute-based schemes [19] that eliminate the computation intensive bilinear pairing operation. With the development of the Internet of Things, in 2021, Liu *et al.* proposed a fuzzy detection strategy to prejudge the target tracking result [20] and a multi-layer template update mechanism to achieve effective monitoring in a multimedia environment [21]. In 2021, Chen *et al.* proposed the first instance of CL-ME [22] based on bilinear pairing. In 2021, Saju *et al.* analyzed elliptic curve digital signature algorithm (ECDSA) along with the primary operations of elliptic curves [23]. In 2022, the scheme [24] proposed by Liu *et al.* combined the relevant characteristics of human inertial thinking, and the integration of the proposed edge learning method with the IoT can be well applied to the construction of smart cities and future generation systems.

To meet the requirements of electronic voting, electronic auction, electronic payment, and other applications, Deng *et al.* proposed an attribute blind signature scheme based on an access tree structure in cloud storage [25], which combined attribute-based signature technology with a blind signature.

B. OUR CONTRIBUTIONS

Currently, all existing attribute-based blind signature schemes require the support of bilinear pairing technology, which involves several complex pairing and exponential operations in the signature and verification process. This leads to a low computational efficiency [2]. However, scalar multiplication on an elliptic curve is more computationally efficient than modular exponentials and bilinear pairing. Therefore, it is easier to implement in hardware. It can be seen that elliptic curve cryptography (ECC) has great advantages in

encryption and decryption speed, computing efficiency and storage resource occupation [26]. The advantages of this study are as follows.

- In this paper, an attribute-based blind signature scheme based on elliptic curve cryptography (ECC) is proposed. The security of our scheme is based on the intractability of the elliptic curve discrete logarithm problem (ECDLP). To the best of our knowledge, our scheme is the first attribute-based blind signature scheme constructed using elliptic curve cryptography. In this study, the complex bilinear pairing operation is replaced by scalar multiplication on the elliptic curve, reducing the computational overhead of the signature and verification.
- A monotonic access structure LSSS matrix with high expressivity does not require recursive operations to achieve fine-grained access control, which is more efficient.
- The new scheme achieves a fixed signature length independent of the number of signer attributes, reducing communication and computational overhead.

C. ORGANIZATION OF THE PAPER

The remainder of this paper is organized as follows. In Section II, we introduce the relevant knowledge and provide a generic attribute-based blind signature scheme with its security model. In Section III, we present an attribute-based blind signature scheme based on elliptic curve cryptography. In Section IV, the efficiency of the proposed scheme is analyzed. We conclude this paper in Section V.

II. PRELIMINARY

In this section, we introduce elliptic curve cryptography and provide the algorithm definition and security model of attribute-based blind signatures.

A. ELLIPTIC CURVE CRYPTOGRAPHY

Elliptic curve cryptography [27] is proposed by Neal Koblitz and Victor Miller in 1985. Scalar multiplication operations on elliptic curves are computationally faster than modular exponential operations and bilinear pairings, and are easier to implement in hardware. It can be seen that elliptic curve cryptography has many advantages in encryption and decryption speed, computational efficiency, storage and bandwidth resource occupation [28]. Its security is based on the difficulty of the elliptic curve discrete logarithm problem (ECDLP).

Elliptic curves defined over a finite-field $GF(p)$ are binary cubic equations with both variables and coefficients over a finite-field $GF(p)$:

$$y^2 = x^3 + ax + b \,(\mathrm{mod} p)\,, 4a^3 + 27b^2 \neq 0$$

It is difficult to calculate the discrete logarithm of an element on an elliptic curve defined over a finite-field $GF(p)$ when a base point is given. In other words, let G be the base point for order p. If a point $Q = kG, k \in Z_p$ is provided, it is difficult to compute the integer k in polynomial time.

B. A GENERIC DEFINITIONS OF ATTRIBUTE-BASED BLIND SIGNATURE

Definition 1 (Attribute-based Blind Signature): An attribute-based blind signature consists of a set of PPT algorithms $(Setup, Extand, MessageBlind, Sign, UnBlind, Verify)$ that generates keys for users, blinds a message, signs a message, unblinds a signature, and verifies the signature:

- $Setup\,(k)$: A probabilistic algorithm outputs the system parameters, public key PK, and master key MSK by input security parameter k.
- $Extract\,(PK, MSK, T)$: A probabilistic algorithm that takes the public key PK, master key MSK, and an access structure T as inputs outputs secret key SK for the signers.
- $MessageBlind\,(M)$: A probabilistic algorithm executed by the message owner blinds the message M to obtain m', which is sent to the signer.
- $Sign\left(PK, m', SK, W\right)$: A probabilistic algorithm that takes as inputs the private key SK of the signers and the public key PK and a message m', which is blinded by the message owner, produces an attribute-based blind signature σ' on the message m'.
- $UnBlind\left(PK, \sigma'\right)$: A probabilistic algorithm that unblinds signature σ' to the final attribute-based blind signature σ by the message owner using the public key PK and some private information of the owner.
- $Verify\,(PK, \sigma)$: A deterministic algorithm that takes the public key PK and a claimed attribute-based blind signature σ as inputs returns either valid or invalid.

C. A SECURITY MODEL OF AN ATTRIBUTE-BASED BLIND SIGNATURE SCHEME

1) CORRECTNESS

The correctness requirement of an attribute-based blind signature scheme is that, if the scheme

$$\sigma = (Setup, Extand, MessageBlind, Sign, UnBlind, Verify)$$

for any access policy (L, ρ) and attribute set W that satisfies the access policy (L, ρ). It holds that

$$Verify\,(PK, W, M, Sign) = 1.$$

2) DEFINITION 2 (BLINDNESS)

Let $\sigma = (Setup, Extand, MessageBlind, Sign, UnBlind, Verify)$ be an attribute-based blind signature scheme for any PPT adversary $\mathcal{A}$, any positive integer number $t \geq 2$, and consider the following game:

For $i = 1$ to t, $(PK_i, SK_i) \leftarrow Gen\left(1^l, z_i\right)$ is generated for randomly chosen z_i. Give to $\mathcal{A}$ the Public key $S \overset{def}{=} \{(PK_i)\}_{i=1}^{t}$.

Adversary $\mathcal{A}$ is also given access to a signature query. The adversary $\mathcal{A}$ sends (W^*, M^*) to challenger $\mathcal{C}$ and then obtains $Sign_{SK_i^*}\,(W^*, M^*)$.

The adversary $\mathcal{A}$ submits two plaintexts, M_0 and M_1, of equal length to challenger $\mathcal{C}$. Challenger $\mathcal{C}$ randomly selects $b \in \{0, 1\}$ generates signature $Sign(W, M_b)$ and sends it to adversary $\mathcal{A}$.

The adversary $\mathcal{A}$ gives a guess b' of b, and succeeds if $b' = b$.

The attribute-based blind signature scheme $\sigma = (Setup, Extand, MessageBlind, Sign, UnBlind, Verify)$ achieves blindness; if, for any PPT adversary $\mathcal{A}$ and any positive integer number $t \geq 2$, the success probability of $\mathcal{A}$ in the above game is negligibly close to1/2.

3) DEFINITION 3 (UNFORGEABILITY)

An attribute-based blind signature scheme $\sigma = (Setup, Extand, MessageBlind, Sign, UnBlind, Verify)$ is unforgeable under selective attribute sets and message attacks can be defined as the following polynomial time game between adversary $\mathcal{A}$ and challenger $\mathcal{C}$:

- *Init* : The adversary $\mathcal{A}$ outputs the challenge attribute set W^* and a message M^*.
- *Setup* : Challenger $\mathcal{C}$ selects the safety parameter k and calculates $(PK, MSK) \leftarrow Setup(k)$. Then, challenger $\mathcal{C}$ sends PK to adversary $\mathcal{A}$.
- *Queries* : Adversary $\mathcal{A}$ is also given access to a polynomial time query. Challenger $\mathcal{C}$ sends the query results to adversary $\mathcal{A}$.

a: PRIVATE KEY QUERY

Adversary $\mathcal{A}$ sends access structure T to challenger $\mathcal{C}$. If $T(W^*) \neq 1$, challenger $\mathcal{C}$ runs algorithm *Extract* to generate signature key SK and sends it to adversary $\mathcal{A}$.

b: SIGNATURE QUERY

Adversary $\mathcal{A}$ sends attribute set W and message bit M to challenger $\mathcal{C}$. Then challenger $\mathcal{C}$ invokes algorithm *Sign* to generate signature σ and sends it to adversary $\mathcal{A}$.

- *Forgery* : Adversary $\mathcal{A}$ exports forged signature σ^* of (M^*, W^*). Adversary $\mathcal{A}$ succeeds if the following three conditions are true:

$$Verify\left(PK, W^*, M^*, \sigma^*\right) = 1.$$

Adversary $\mathcal{A}$ does not ask the signature of (M^*, W^*).

The access structure T for any query is satisfied $T(W^*) \neq 1$.

The scheme is unforgeable if adversary $\mathcal{A}$ cannot succeed in the above game with a nonnegligible probability in polynomial time.

III. AN ATTRIBUTE-BASED BLIND SIGNATURE SCHEME BASED ON ELLIPTIC CURVE CRYPTOGRAPHY

At present, most attribute-based blind signatures are supported by bilinear pairing operations whose computational efficiency is not high. This section presents an attribute-based blind signature scheme based on elliptic curve cryptography without a bilinear pairing operation, and its security analysis.

A. OUR CONSTRUCTION

1) SETUP

Let $GF(q)$ be a finite field of order q, E be an elliptic curve defined over $GF(q)$ and G be an element of a large prime order p in E. Point G generates a cyclic subgroup of E, in which the elliptic curve discrete logarithm problem (ECDLP) is intractable. Suppose the set of attributes in the system is $U = \{1, 2, \ldots n\}$, and i is one of these attributes. In addition, let $H : \{0, 1\}^* \rightarrow z_p^*$ be a cryptographic secure-hash function. The system parameter generation algorithm randomly selects an element $\alpha \in z_p^*$, and computes $P_{pub} = \alpha G$. Choose an element $z_i \in z_p^*$ at random for each attribute i in the system and compute $h_i = z_i G$. The system parameter generation algorithm outputs the public key $PK = \{p, G, H, h_1, h_2, \ldots, h_n, P_{pub}\}$ and master secret key $MSK = \{\alpha, z_1, z_2, \ldots, z_n\}$.

2) EXTRACT

Assume that the access structure T is (L, ρ). The matrix L with s rows and t columns is designed to generate the shares. For $i \in \{1, 2, \ldots, s\}$, each row i is labeled by the function ρ_i to associate it with one of the parties.

The system parameter generation algorithm constructs a column vector $\vec{v} = (\alpha, r_2, r_3, \ldots r_t)$, where $r_2, r_3, \ldots, r_t \in z_p^*$ are random. For $i \in [1, s]$, the secret value is $\lambda_i = \vec{L_i} \cdot \vec{v}$, and $d_i = \lambda_i + z_i$. Then, it outputs the signature key $SK = \{d_i\}_{i \in [1,s]}$.

3) MESSAGEBLIND

The signer selects $c_0 \in z_p^*$ and computes $R = c_0 G$, then sends R to the message owner.

The message owner selects $x \in z_p^*$ and computes the coordinates of $R_1 = x^{-1} R$ to obtain (x_0, y_0). Then calculates $r = x_0 \bmod p, m = H(M)$, and $m' = xrm$. The message owner sends the blinded message m' to the signer and sends R_1 and its coordinate (x_0, y_0) to the verifier.

4) SIGN

Assume that the signature attribute set is $W \subset U$. To obtain an attribute-based blind signature on a message m', the signer acts as follows:

If the attributes of the signer satisfy the access structure T, there must exist a constant set $\left\{\omega_i \in z_p^*, i \in \bar{\omega}\right\}$ that can be found in polynomial time, making

$$\sum_{i \in \bar{\omega}} \omega_i L_i = (1, 0, \ldots, 0),$$

where $\bar{\omega} = \{i \in [1, s] : \rho(i) \in W\}$.

Compute $\sigma_1 = m' \sum_{i \in \bar{\omega}} d_i \omega_i + c_0$.

The signer sends σ_1 to the message owner.

5) UNBLIND

The message owner computes $\sigma = x^{-1} \sigma_1$ and then outputs the attribute-based blind signature σ after blindness removal.

6) VERIFY

To verify the attribute-based blind signature σ for message M and public information PK, the verifier performs the following steps.

- Calculates $m = H(M)$ and $r = x_0 \bmod p$.
- Verifies whether equation

$$\sigma G - R_1 = mr\left(P_{pub} + \sum_{i\in\bar{\omega}} h_i\omega_i\right)$$

is valid. If the equation is valid, the attribute-based blind signature σ is accepted; otherwise, it is not accepted.

B. SECURITY ANALYSIS

In this section, we analyze the security properties of the proposed attribute-based blind signature scheme based on elliptic curve cryptography. Security properties include correctness, blindness, and unforgeability.

1) THEOREM 1 (CORRECTNESS)

The attribute-based blind signature scheme based on elliptic curve cryptography proposed by us satisfies the correctness.

Proof: When the attributes W of the signer satisfy the access structure T, there must can find the same set $\left\{\omega_i \in z_p^*, i \in \bar{\omega}\right\}$ of refactoring constants as the signer in polynomial time, making $\sum_{i\in\bar{\omega}} \omega_i L_i = (1, 0, \ldots, 0)$, where $\bar{\omega} = \{i \in [1, s] : \rho(i) \in W\}$. According to the properties $\sum_{i\in\bar{\omega}} \lambda_i\omega_i = \alpha$ of the LSSS matrix and public key PK, the procedure for verifying the signature is as follows:

$$\begin{aligned}
\sigma G - R_1 &= x^{-1}\sigma_1 G - x^{-1}R \\
&= x^{-1}\left(m'\sum_{i\in\bar{\omega}} d_i\omega_i + c_0\right)G - x^{-1}c_0 G \\
&= x^{-1}\left(m'\sum_{i\in\bar{\omega}} d_i\omega_i G + c_0 G\right) - x^{-1}c_0 G \\
&= x^{-1}m'\sum_{i\in\bar{\omega}} (\lambda_i + z_i)\,\omega_i G + x^{-1}c_0 G - x^{-1}c_0 G \\
&= x^{-1}m'\sum_{i\in\bar{\omega}} (\lambda_i + z_i)\,\omega_i G \\
&= x^{-1}\cdot xrm\sum_{i\in\bar{\omega}} (\lambda_i + z_i)\,\omega_i G \\
&= rm\sum_{i\in\bar{\omega}} (\lambda_i + z_i)\,\omega_i G \\
&= rm\left(\sum_{i\in\bar{\omega}} \lambda_i\omega_i G + \sum_{i\in\bar{\omega}} z_i\omega_i G\right) \\
&= rm\left(P_{pub} + \sum_{i\in\bar{\omega}} h_i\omega_i\right)
\end{aligned}$$

2) THEOREM 2 (BLINDNESS)

Our attribute-based blind signature scheme based on elliptic curve cryptography satisfies the blindness.

Proof: The adversary $\mathcal{A}$ submits two equal-length messages M_0 and M_1 to the challenger $\mathcal{C}$. Subsequently, the challenger $\mathcal{C}$ flips a fair binary coin $b \in \{0, 1\}$ at random and calculates $m = H(M_b)$, which is blinded by calculating $m' = xrm$. Then, outputs the attribute-based blind signature σ with respect to M_b and sends σ to the adversary $\mathcal{A}$.

To obtain the content of the message, the adversary $\mathcal{A}$ must know the value of x and r, that is, to solve x by $R_1 = x^{-1}R$. This is an elliptic curve discrete logarithm problem (ECDLP). Therefore, the probability that the adversary can determine the real message should not be greater than $1/2$. Thus, our attribute-based blind signature scheme based on elliptic curve cryptography in this study satisfies blindness.

3) THEOREM 3 (UNFORGEABILITY)

Under the assumption that the ECDLP is difficult, our attribute-based blind signature scheme based on elliptic curve cryptography is unforgeable.

Proof: Suppose there is an adversary $\mathcal{A}$ that can successfully forge a valid attribute-based blind signature with a non-negligible probability in polynomial time; then, the challenger $\mathcal{C}$ can use the algorithm of adversary $\mathcal{A}$ to solve an elliptic curve discrete logarithm problem (ECDLP) in polynomial time. The interaction between adversary $\mathcal{A}$ and challenger $\mathcal{C}$ is as follows.

- *Init*. The attribute set W^* and a list of message bits $M = \left\{M_0, M_1, \ldots, M_f\right\} \in \{0, 1\}^*$ to be forged by the adversary $\mathcal{A}$ are sent to challenger $\mathcal{C}$.
- *Setup*. Taking as k inputs the security parameter, challenger $\mathcal{C}$ simulates and generates the public parameters as follows:

Randomly selects $\beta \in z_p^*$, computes $P_{pub} = \beta G$.

For each attribute $i \in W^*$ computes $h_i = \gamma_i G$, where $\gamma_i \in z_p^*$ is random select.

For each attribute $i \in U\backslash W^*$ computes $h_i = (\gamma_i - \nu_i)\,G$, where $\gamma_i, \nu_i \in z_p^*$ is random select.

Let $H : \{0, 1\}^* \to z_p^*$ be a cryptographic secure-hash function. Challenger $\mathcal{C}$ sends the public parameter $PK = \left\{p, G, H, h_1, h_2, \ldots, h_n, P_{pub}\right\}$ to the adversary $\mathcal{A}$.

- *Queries*. Adversary $\mathcal{A}$ can make a polynomial private key and signature query, and challenger $\mathcal{C}$ returns the query result to adversary $\mathcal{A}$.

a: PRIVATE KEY QUERY

Adversary $\mathcal{A}$ sends access structure T to challenger $\mathcal{C}$, where $T(W^*) \neq 1$. Challenger $\mathcal{C}$ runs algorithm *Extract* to generate master secret key z_i as follows:

$$\text{let } z_i = \begin{cases} \gamma_i, \rho(i) \in W^* \\ \gamma_i - \nu_i, \rho(i) \notin W^* \end{cases}, \text{computes } h_i = z_i G.$$

Then Challenger $\mathcal{C}$ structures a column vector $\vec{v} = (\beta, r_2, r_3, \ldots r_t)$, where $r_2, r_3, \ldots, r_t \in z_p^*$ are random.

For each row $i \in [1, s]$ of LSSS matrix, calculates $\lambda_i = \vec{L}_i \cdot \vec{v}$.

$$\text{Outputs the signature key } d_i = \lambda_i + z_i = \begin{cases} \lambda_i + \gamma_i, & \rho(i) \in W^* \\ \lambda_i + \gamma_i - v_i, & \rho(i) \notin W^* \end{cases}$$

b: SIGNATURE QUERY

Adversary $\mathcal{A}$ sends the attribute set W and message bit $M_0 \in M$ to challenger $\mathcal{C}$, who signs the message M_0 according to the *Sign* steps.

If the attributes set W satisfies the access structure T, then there must exist a constant set $\left\{\omega_i \in z_p^*, i \in \bar{\omega}\right\}$ that can be found in polynomial time, making $\sum_{i\in\bar{\omega}} \omega_i L_i = (1, 0, \ldots, 0)$, where $\bar{\omega} = \{i \in [1, s] : \rho(i) \in W\}$.

Compute $\sigma_1 = M_0 \sum_{i\in\bar{\omega}} d_i\omega_i + c_0$.

let $c = \sum_{i\in\bar{\omega}} z_i\omega_i$, thus

$$\begin{aligned} \sigma_1 &= M_0 \sum_{i\in\bar{\omega}} (\lambda_i + z_i)\,\omega_i + c_0 \\ &= M_0 \left(\sum_{i\in\bar{\omega}} \lambda_i\omega_i + \sum_{i\in\bar{\omega}} z_i\omega_i \right) + c_0 \\ &= M_0\,(\beta + c) + c_0 \end{aligned}$$

Finally, Challenger $\mathcal{C}$ sends σ_1 to adversary $\mathcal{A}$.

- *Forgery*. Adversary $\mathcal{A}$ is trained by the inquiry to challenger $\mathcal{C}$ and outputs a valid signature σ_1^* of W^*, $M_1 \in M$. By replaying the message, challenger $\mathcal{C}$ can generate two valid signatures: σ_1^* and $\sigma_1^{*\prime}$, where $\sigma_1^{*\prime}$ is the valid signature of $W^*, M_2 \in M$. Both of these signatures are valid, so they all satisfy the signature equation:

$$\sigma_1^* = M_1\,(\beta + c) + c_0 \quad (1)$$
$$\sigma_1^{*\prime} = M_2\,(\beta + c) + c_0 \quad (2)$$

(1) minus (2) can get:

$$\sigma_1^* = \sigma_1^{*\prime} = (M_1 - M_2)\,\beta + (M_1 - M_2)\,c$$
$$\beta = (M_1 - M_2)^{-1}\left[\left(\sigma_1^* - \sigma_1^{*\prime}\right) - (M_1 - M_2)\,c\right]$$

Finally, challenger $\mathcal{C}$ can solve a

$$\beta = (M_1 - M_2)^{-1}\left[\left(\sigma_1^* - \sigma_1^{*\prime}\right) - (M_1 - M_2)\,c\right]$$

as a solution for the ECDLP. This means that challenger $\mathcal{C}$ successfully solves the ECDLP, which contradicts the difficulty assumption of the ECDLP. Thus, no adversary $\mathcal{A}$ can successfully forge an attribute-based blind signature with a non-negligible probability in polynomial time.

IV. EFFICIENCY ANALYSIS

In this section, we present an efficiency analysis of our attribute-based blind signature scheme based on elliptic curve cryptography. Table 1 shows the computational overhead comparison among our attribute-based blind signature scheme based on elliptic curve cryptography and other attribute-based signature schemes for the access structure, access policy, sizes of the private key and signature, signature computation, and verification computation. Here, we choose $H - ABPS$[29], $S - ABPS$[30], and $B - ABPS$[25] for comparison.

TABLE 1. Comparision of schemes.

Scheme	Access structure	Access policy	private key sizes $(\lvert G\rvert)$	Signature sizes $(\lvert G\rvert)$	Signature computation $(T_{\exp})$	Verification computation (T_{bp})
$H-ABPS$	access tree	SP	2	$3s+1$	$3s+1$	$3s$
$S-ABPS$	nothing	nothing	$3w+1$	$3w+1$	$6w+5$	$4w$
$B-ABPS$	access tree	SP	w	$2w+1$	$2w$	$\lvert T\rvert$
Our scheme	LSSS matrix	KP	s	1	0	0

The symbols in table 1 are as follows: w represents the number of attributes of signers, s represents the number of attributes of visitors, $|G|$ represents the length of the group G, $T_{\exp}$ represents the time required for modular power operation, T_{bp} represents the time required for bilinear pairing, and $|T|$ represents the number of different attribute sets.

From table 1, we can observe that our attribute-based blind signature scheme based on elliptic curve cryptography uses an LSSS matrix that does not require recursive operations but has a flexible access structure to achieve fine-grained access control. The new scheme belongs to the key policy attribute-based signature; therefore, the signer's private key is related to the number of rows of the LSSS matrix.

However, since the result of multiplying the private key by the constant is added during the signature process, a fixed signature length is achieved. In terms of computational complexity, the new scheme is based on an elliptic-curve cryptosystem, replacing the bilinear pairing operation with scalar multiplication on the elliptic curve. Scalar multiplication on an elliptic curve is faster than a modular exponential operation and bilinear pairings in terms of computational efficiency [31]. Therefore, our scheme has significant advantages in terms of the signature speed, verification time, and storage space.

V. CONCLUSION

All existing attribute-based blind signature schemes currently use bilinear pairings, and the computation cost of the pairings is much higher than that of scalar multiplication over the elliptic curve group. In this paper, an attribute-based blind signature scheme based on elliptic curve cryptography without a bilinear pairing operation is proposed, and its security is analyzed. Our scheme realizes the blindness of signature

messages and allows signers with access structure attributes to sign them, which can be used in electronic auctions, electronic voting, and other places. The scheme adopts a key policy and LSSS matrix technology to flexibly realize fine-grained access control and achieves a fixed signature length independent of the number of attributes of the signer. The scheme uses scalar multiplication over an elliptic curve group instead of bilinear pairings, which has great advantages in terms of signature speed, verification time, and storage space.

ACKNOWLEDGMENT

The authors would like to thank the editors and reviewers for their recognition and hard work on this paper.

REFERENCES

[1] D. Chaum, "Blind signatures for untraceable payments," in *Proc. Crypto*, 1982, pp. 199–203.
[2] X. Chen, W. Susilo, and J. Li, "Efficient algorithms for secure outsourcing of bilinear pairings," *Theor. Comput. Sci.*, vol. 562, pp. 112–121, Jan. 2015.
[3] D. L. Chaum, "Blind signatures system," in *Proc. Crypto*, 1983, pp. 153–156.
[4] T. Okamoto, "Provable secure and practical identification schemes and corresponding digital signature schemes," in *Proc. Crypto*, 1992, pp. 31–52.
[5] J. Camenisch, J. Piveteau, and M. Stadler, "Blind signatures based on discrete logarithm problem," in *Proc. Eurorypt*, 1994, pp. 428–432.
[6] E. Mohammed, A. E. Emarah, and K. E. Shennawy, "A blind signatures scheme based on ElGamal signature," in *Proc. IEEE/AFCEA Eurocomm Inf. Syst. Enhanced Public Saf. Secur.*, May 2000, pp. 51–53.
[7] M. H. Chang, I. Chen, I. Wu, and Y. S. Yeh, "Schnorr blind signature scheme based on the elliptic curves," *Asian J. Inf. Technol.*, vol. 2, no. 3, pp. 130–134, 2003.
[8] W. J. Tsaur, J. H. Tsao, and Y. H. Tsao, "An efficient and secure ecc-based partially blind signature scheme with multiple banks issuing e-cash payment applications," in *Proc. Int. Conf. e-Learn., e-Bus., Enterprise Inf. Syst., e-Government (EEE)*, 2018, pp. 94–100.
[9] D. H. Duong, W. Susilo, and H. T. N. Tran, "A multivariate blind ring signature scheme," *Comput. J.*, vol. 63, no. 1, pp. 1194–1202, Jan. 2020.
[10] H. Huang, Z. Y. Liu, and R. Tso, "Partially blind ECDSA scheme and its application to bitcoin," in *Proc. IEEE Conf. Dependable Secure Comput. (DSC)*, Feb. 2021, pp. 1–8.
[11] D. Khader, "Attribute-based group signatures," in *Proc. Cryptographers' Track RSA Conf.*, 2011, pp. 376–392.
[12] H. K. Maji, M. Prabhakaran, and M. Rosulek, "Attribute-based signatures: Achieving attribute-privacy and collusion resistance," *IACR Cryptol.*, vol. 730, no. 1, pp. 1–23, 2008.
[13] S. F. Shahandashti and R. Safavi-Naini, "Threshold attribute-based signatures and their application to anonymous credential systems," in *Proc. Int. Conf. Cryptol. Afr.*, 2009, pp. 198–216.
[14] H. K. Maji, M. Prabhakaran, and M. Rosulek, "Attribute-based signatures," in *CT-RSA*, (Lecture Notes in Computer Science), vol. 6558, A. Kiayias, Ed. Berlin, Germany: Springer, 2011, pp. 376–392.
[15] Y. S. Rao and R. Dutta, "Expressive bandwidth efficient attribute based signature and signcryption in standard model," in *Proc. Australas. Conf. Inf. Secur. Privacy*, Jul. 2014, pp. 209–225.
[16] A. E. Kaafarani, "Traceability, linkability and policy hiding in attribute-based signature schemes," Ph.D. dissertation, Dept. Comput. Sci., Univ. Bath, Bath, U.K., 2015.
[17] S. Rani and S. T. Ali, "Expressive key-policy attribute-based constant-size signature," in *Proc. ISEA Asia Secur. Privacy (ISEASP)*, Feb. 2017, pp. 1–4.
[18] R. Guo, H. Shi, Q. Zhao, and D. Zheng, "Secure attribute-based signature scheme with multiple authorities for blockchain in electronic health records systems," *IEEE Access*, vol. 6, pp. 11676–11686, 2018.
[19] Y. Wang, B. Chen, L. Li, Q. Ma, H. Li, and D. He, "Efficient and secure ciphertext-policy attribute-based encryption without pairing for cloud-assisted smart grid," *IEEE Access*, vol. 8, pp. 40704–40713, 2020, doi: 10.1109/ACCESS.2020.2976746.
[20] S. Liu, S. Wang, X. Liu, C.-T. Lin, and Z. Lv, "Fuzzy detection aided real-time and robust visual tracking under complex environments," *IEEE Trans. Fuzzy Syst.*, vol. 29, no. 1, pp. 90–102, Jan. 2021, doi: 10.1109/TFUZZ.2020.3006520.
[21] S. Liu, S. Wang, X. Liu, A. H. Gandomi, M. Daneshmand, K. Muhammad, and V. H. C. D. Albuquerque, "Human memory update strategy: A multi-layer template update mechanism for remote visual monitoring," *IEEE Trans. Multimedia*, vol. 23, pp. 2188–2198, 2021.
[22] B. Chen, T. Xiang, M. Ma, D. He, and X. Liao, "CL-ME: Efficient certificateless matchmaking encryption for Internet of Things," *IEEE Internet Things J.*, vol. 8, no. 19, pp. 15010–15023, Oct. 2021.
[23] N. S. Saju, "Design and execution of highly adaptable elliptic curve cryptographic processor and algorithm on FPGA using Verilog HDL," in *Proc. Int. Conf. Commun., Control Inf. Sci. (ICCISc)*, Jun. 2021, pp. 1–6.
[24] S. Liu, S. Wang, X. Liu, J. Dai, K. Muhammad, A. H. Gandomi, W. Ding, M. Hijji, and V. H. C. de Albuquerque, "Human inertial thinking strategy: A novel fuzzy reasoning mechanism for IoT-assisted visual monitoring," *IEEE Internet Things J.*, early access, Jan. 11, 2022, doi: 10.1109/JIOT.2022.3142115.
[25] Y. J. Deng and Y. Xian, "Attribute blind signature scheme based on access tree structure in cloud storage," *J. Baoji College Arts Sci.*, vol. 40, no. 4, pp. 15–19, Dec. 2020.
[26] D. W. Li, Z. Y. Wang, and J. G. Zhao, "Analysis on security of elliptic curve cryptosystem," *Comput. Technol. Develop.*, vol. 22, no. 4, pp. 227–234, 2012.
[27] N. Koblitz, "Elliptic curve cryptosystems," *Math. Comput.*, vol. 48, no. 177, pp. 203–209, 1987.
[28] P. S. Barreto, B. Libert, and N. Mccullagh, "Efficient and provably-secure identity-based signatures and signcryption from bilinear maps," in *Proc. Int. Conf. Theory Appl. Cryptol. Inf. Secur.*, 2005, pp. 515–532.
[29] H. Hong, Z. Sun, and Y. Xia, "Achieving secure and fine-grained data authentication in cloud computing using attribute based proxy signature," in *Proc. Int. Conf. Inf. Sci. Control Eng. IEEE Comput. Soc.*, Jul. 2017, pp. 130–134.
[30] C. Sun, Y. Guo, and Y. Li, "One secure attribute-based proxy signature," *Wireless Pers. Commun.*, vol. 103, no. 2, pp. 1273–1283, 2018.
[31] S. Ding, "Research on data security and efficient sharing control mechanism in the Internet of Things," Ph.D. dissertation, Dept. Cyber. Eng., Xidian Univ., Xi'an, China, 2019.

RUI MA received the B.S. degree in applied mathematics from Taiyuan Normal University, Taiyuan, China, in 2007, and the M.S. degree in applied mathematics from the Xi'an University of Technology, Xi'an, in 2011. She is currently a Lecturer with the Xingzhi College, Zhejiang Normal University. Her current research interests include cryptography and information security.

LINYUE DU received the B.S. degree in applied mathematics from Taiyuan Normal University, Taiyuan, China, in 2007, and the M.S. degree in applied mathematics from the Xi'an University of Technology, Xi'an, in 2010. He is currently a Lecturer with Zhejiang Normal University. His current research interests include cryptography and information security.