Attribute-based Blind Signature Scheme based on Elliptic Curve Cryptography

RUI MA\textsuperscript{1}, LINYUE DU\textsuperscript{2}
\textsuperscript{1}Xingzhi College, Zhejiang Normal University, Jinhua 321004, China
\textsuperscript{2}Personnel Department, Zhejiang Normal University, Jinhua 321004, China

Corresponding author: Linyue Du (e-mail: 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 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, Yeh 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.
A probabilistic algorithm outputs the system be an for the signers. Give to as inputs outputs secret key by to , and master key er is organized as follows. In is , is generated for and , in polynomial randomly selects . Challenger and a claimed attribute-based blind signature: A probabilistic algorithm executed by and attribute set . It holds that , master key by input : A probabilistic algorithm that unblinds be , of on the the Public key If a point to obtain , and an access : A probabilistic algorithm that takes are binary and some : [1x6] W Verify PK W M Sign [1x6]Verify PK [1x6] [2x6]Q kG k Z  [2x6]G GF p [2x6]  [2x6]  [2x3]t [2x3]t [2x3]i [2x4]σ [2x4]σ [2x3]m [2x3]k [2x3]k [2x7]Sign W M [2x5]M [2x6] [2x6]Sign PK m SK W [2x6]Sign W M [2x6]MessageBlind M [2x3]MSK [2x3]SK [2x3]SK [2x5]M [2x5]z [2x2]PK [2x2]PK [3x6]y x ax b p a b [6x6]PK SK Gen z [6x6]L [6x6] [6x3]i [7x11]2 3 3 2 [8x4]= Setup,Extand,MessageBlind,Sign,UnBlind,Verify) = Setup,Extand,MessageBlind,Sign,UnBlind,Verify) [8x4] [8x4] [10x3]1 [11x6] [11x6], [11x6], [11x4]( [12x3]0 [13x6]     [13x12]** [14x6]  [14x6]  [15x3]2 [16x6]  [16x6]  [16x6]  [16x4]i i i [16x7], [18x6]  [18x4]SK [19x6]  [23x6]  [23x6]  [23x6]  [24x6]*, [24x6]p [24x6]  [29x6]  [29x6]b [29x6], [31x696]follows. [37x84]time. [37x96]provided, it is difficult to compute the integer [37x108]the base point for order [37x132]element on an elliptic curve defined over a finite - [37x168]operations [28]. Its security is based on the difficulty of the [37x228]are no bilinear pairing and modular exponential [68x123]elliptic curve discrete logarithm problem (ECDLP). [70x11]l et [96x10]This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/ [107x6],[624]attribute-based blind signature scheme constructed using [156x3]blind signature scheme [168x288]is proposed by Neal Koblitz [174x636]our scheme is the first [181x276]Compared with other [202x516]attributes, reducing [229x7],[612]complex [249x452]provides [257x428]based [262x132]field [265x352]and [267x581] [297x617] [297x677]Definition 1 (Attribute-based Blind Signature). [297x707]BASED [304x389]public key [304x430]as inputs returns either valid or invalid. [320x485]and a message [333x747] Setup k [465x747] MSK T [458x351]BASED [489x707]BASED [510x327] ,L  [521x91] 0,1b  [525x231]2t  [537x483] ,Verify PK  [547x333]= Setup,Extand,MessageBlind,Sign,UnBlind,Verify)( [1566x333]= Setup,Extand,MessageBlind,Sign,UnBlind,Verify)( [1120x767]Setup,Extand,MessageBlind,Sign,UnBlind,Verify( ) [1140x260]σ= Setup,Extand,MessageBlind,Sign,UnBlind,Verify)( A security model of an attribute-based blind signature scheme. 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. Compared with other cryptosystems, it not only has the characteristics of a small key size, required storage, and bandwidth resources, but also has great advantages in computational efficiency because there are no bilinear pairing and modular exponential operations [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 $GF(p)$:

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

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 $Q = kG, k \in \mathbb{Z}_p$ 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 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 blinks the message $M$ to obtain $m'$, which is sent to the signer.
- Sign($PK, m', SK, W$): 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 $\sigma'$ on the message $m$.
- Unblind($PK, \sigma'$): A probabilistic algorithm that unblinds signature $\sigma'$ to the final attribute-based blind signature $\sigma$ 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 $\sigma$ as inputs returns either valid or invalid.

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.

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

$$\sigma = \langle Setup, Extand, MessageBlind, Sign, Unblind, Verify \rangle$$

for any access policy $(L, \rho)$ and attribute set $W$ that satisfies the access policy $(L, \rho)$, it holds that

$$\text{Verify}(PK, W, M, \text{Sign}) = 1.$$ 2) Definition 2 (Blindness).

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

For $i = 1$ to $t$, $(PK, SK) \leftarrow Gen(1^t, z)$ is generated for randomly chosen $z$. Give to $A$ the Public key $s = \langle PK \rangle_{N}$.

Adversary $A$ is also given access to a signature query. The adversary $A$ sends $(W', M')$ to challenger $C$ and then obtains $\text{Sign}_{SK}(W', M')$.

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

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.

The article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2022.3162231, IEEE Access
The adversary $A$ gives a guess $b'$ of $b$, and succeeds if $b'=b$.

The attribute-based blind signature scheme $\sigma = (\text{Setup}, \text{Extend}, \text{MessageBlind}, \text{Sign}, \text{UnBlind}, \text{Verify})$ achieves blindness; if, for any PPT adversary $A$ and any positive integer number $t \geq 2$, the success probability of $A$ in the above game is negligibly close to $1/2$.

3) Definition 3 (Unforgeability).

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

- **Init**: The adversary $A$ outputs the challenge attribute set $W$ and a message $M'$.
- **Setup**: Challenger $C$ selects the safety parameter $k$ and calculates $(PK, MSK) \leftarrow \text{Setup}(k)$. Then, challenger $C$ sends $PK$ to adversary $A$.
- **Queries**: Adversary $A$ is also given access to a polynomial time query. Challenger $C$ sends the query results to adversary $A$.
- **Private key query**: Adversary $A$ sends access structure $T$ to challenger $C$. If $T(W') \neq 1$, challenger $C$ runs algorithm $	ext{Extract}$ to generate signature key $SK$ and sends it to adversary $A$.
- **Signature query**: Adversary $A$ sends attribute set $W$ and message bit $m$ to challenger $C$. Then challenger $C$ invokes algorithm Sign to generate signature $\sigma$ and sends it to adversary $A$.
- **Forgery**: Adversary $A$ exports forged signature $\sigma'$ of $(M', W')$. Adversary $A$ succeeds if the following three conditions are true:
  - $\text{Verify}(PK, W', M', \sigma') = 1$.
  - The access structure $T$ for any query is satisfied $T(W') \neq 1$.

The scheme is unforgeable if Adversary $A$ 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 $\{1,2,...,n\}$, 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 $z_i \in z_p^*$ and computes $f_{\mu_i} = \alpha G$. 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 $PK = \{p, G, H, h_1, h_2, ..., h_n, P_{\mu_0}\}$ and master secret key $MSK = \{\alpha, z_1, z_2, ..., z_n\}$.

2) Extract.

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

The system parameter generation algorithm constructs a column vector $v = (\alpha, r_2, r_3, ..., r_s)$, where $r_2, r_3, ..., r_s \in z_p^*$ are random. For $i \in \{1,2,...,s\}$, the secret value is $z_i = L_i \cdot v$, and $d_i = z_i + r_i$. Then, it outputs the signature key $SK = \{d_i\}_{i=1}^{s}$.

3) MessageBlind.

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

The message owner selects $x \in z_p^*$ and computes the coordinates of $R' = x^* R$ to obtain $(x_1, y_1)$.

4) Sign.

Assume that the signature attribute set is $W \subseteq U$. 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 $\{a_i \in z_p^*: i \in \bar{\omega}\}$ that can be found in polynomial time, making $\sum_{i \in \bar{\omega}} a_i L_i = (1,0,...,0)$,

where $\bar{\omega} = \{i \in \{1,2,...,s\}: \rho(i) \in W\}$.

Compute $\sigma_i = m' \sum_{i \in \bar{\omega}} d_i a_i + c_i$.

The signer sends $\sigma_i$ to the message owner.

5) Unblind.

The message owner computes $\sigma = x^* \sigma$, and then outputs the attribute-based blind signature $\sigma$ after blindness removal.

6) Verify.

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

- Calculates $m = H(M)$ and $r = x_0 \mod P$.
- Verifies whether equation $\sigma G - R_i = m (P_{\mu_0} + \sum_{i \in \bar{\omega}} h_i \alpha)$

is valid. If the equation is valid, the attribute-based blind signature $\sigma$ 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 exist the same set $\{\omega_i \in z_\ast, i \in \mathcal{S}\}$ of refactoring constants as the signer in polynomial time, making $\sum_{i=0}^{m} a_i L_i = (1,0,\ldots,0)$, where $\mathcal{S} = \{i \in [1,s] : \rho(i) \in W\}$. According to the properties $\sum_{i=0}^{m} \lambda_i \omega_i = \alpha$ of the LSSS matrix and public key $PK$, the procedure for verifying the signature is as follows:

$\sigma G - R_i = x^1 \sigma G - x^1 R$

\[= x^1 \left( \sum_{i=0}^{m} d_i \omega_i + c_0 \right) G - x^1 c_i G \]

\[= x^1 \left( \sum_{i=0}^{m} d_i \omega_i + c_0 \right) G - x^1 c_i G \]

\[= x^1 \sum_{i=0}^{m} (\lambda_i + z_i) \omega_i G + x^1 c_i G - x^1 c_i G \]

\[= x^1 \sum_{i=0}^{m} (\lambda_i + z_i) \omega_i G \]

\[= x^1 \cdot \sum_{i=0}^{m} (\lambda_i + z_i) \omega_i G \]

\[= \sum_{i=0}^{m} (\lambda_i + z_i) \omega_i G \]

\[= \sum_{i=0}^{m} (\lambda_i \omega_i G + \sum_{i=0}^{m} z_i \omega_i G) \]

\[= \sum_{i=0}^{m} (\lambda_i \omega_i G + \sum_{i=0}^{m} h_i \omega_i) \]

2) Theorem 2 (Blindness).
Our attribute-based blind signature scheme based on elliptic curve cryptography satisfies the blindness.

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

To obtain the content of the message, the adversary $A$ must know the value of $x$ and $r$, that is, to solve $x$ by $R_i = x^1 R$. 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 $A$ that can successfully forge a valid attribute-based blind signature with a non-negligible probability in polynomial time; then, the challenger $C$ can use the algorithm of adversary $A$ to solve an elliptic curve discrete logarithm problem (ECDLP) in polynomial time. The interaction between adversary $A$ and challenger $C$ is as follows.

- **Init**: The attribute set $W$ and a list of message bits $M = \{M_0, M_1, \ldots, M_t\} \in \{0,1\}^t$ to be forged by the adversary $A$ are sent to challenger $C$.

- **Setup**: Taking as $k$ inputs the security parameter, challenger $C$ simulates and generates the public parameters as follows:

Randomly selects $\beta \in z_\ast$, computes $P_{pub} = \beta G$.

For each attribute $i \in W$, computes $h = \gamma_i G$, where $\gamma_i \in z_\ast$ is random select.

For each attribute $i \in U \setminus W$, computes $h = (\gamma_i - v_i) G$, where $\gamma_i, v_i \in z_\ast$ is random select.

Let $H : \{0,1\}^t \rightarrow z_\ast$ be a cryptographic secure hash function. Challenger $C$ sends the public parameter $PK = \{p,G,H,h,h_2,\ldots,h_s,P_{pub}\}$ to the adversary $A$.

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

**Private key query.**
Adversary $A$ sends access structure $T$ to challenger $C$, where $T(W') \neq 1$. Challenger $C$ runs algorithm $Extract$ to generate master secret key $z_i$ as follows:

Let $z_i = \left\{ \gamma_i, \rho(i) \in W' \right\}$, computes $h = z_i G$.

Then Challenger $C$ structures a column vector $\tilde{v} = (x, r_2, r_3, \ldots, r_t)$, where $r_2, r_3, \ldots, r_t \in z_\ast$ are random. For each row $i \in [1,s]$ of LSSS matrix, calculates $\lambda_i = L_i \cdot \tilde{v}$.

Outputs the signature key $d_i = \lambda_i + z_i = \left\{ \lambda_i + \gamma_i, \rho(i) \in W' \right\}$.

**Signature query.**
Adversary $A$ sends the attribute set $W$ and message bit $M_0 \in M$ to challenger $C$, 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 $\{\omega_i \in z_\ast, i \in \mathcal{S}\}$ that can be found in polynomial time, making $\sum_{i=0}^{m} a_i L_i = (1,0,\ldots,0)$, where $\mathcal{S} = \{i \in [1,s] : \rho(i) \in W\}$.

Compute $\sigma_i = M_0 \sum_{i=0}^{m} d_i \omega_i + c_0$.

let $c = \sum_{i=0}^{m} c_0$, thus
\[ \sigma_i = M_i \sum_{\alpha} (\lambda_i + \alpha) \epsilon + \epsilon_i \]
\[ = M_i \left( \sum_{\alpha} \lambda_i \alpha + \sum_{\alpha} \alpha \epsilon \right) + \epsilon_i \]
\[ = M_i (\beta + c) + \epsilon_i \]

Finally, Challenger \( \mathcal{C} \) sends \( \sigma_i \) to adversary \( \mathcal{A} \).

- Forgery. Adversary \( \mathcal{A} \) is trained by the inquiry to challenge \( \mathcal{C} \) and outputs a valid signature \( \sigma_i \) of \( W \cdot M \in \mathcal{M} \). By replaying the message, challenger \( \mathcal{C} \) can generate two valid signatures: \( \sigma_i^\prime \) and \( \sigma_i^\prime \), where \( \sigma_i^\prime \) is the valid signature of \( W \cdot M \in \mathcal{M} \). Both of these signatures are valid, so they all satisfy the signature equation:
\[ \sigma_i^\prime = M_i (\beta + c) + \epsilon_i \]
\[ \sigma_i^\prime = M_i (\beta + c) + \epsilon_i \]

(1) minus (2) can get:
\[ \sigma_i - \sigma_i^\prime = (M_i - M_i) \beta + (M_i - M_i) c \]
\[ \beta = (M_i - M_i) \left( [\sigma_i - \sigma_i^\prime] - (M_i - M_i) c \right) \]

Finally, challenger \( \mathcal{C} \) can solve \( \beta \) 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 I 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 \( H-\text{ABPS} \) [29], \( S-\text{ABPS} \) [30], and \( B-\text{ABPS} \) [25] for comparison.

The symbols in table I 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 \( G \), \( T_{\text{exp}} \) represents the time required for modular power operation, \( T_{\text{bp}} \) represents the time required for bilinear pairing, and \( |P| \) represents the number of different attribute sets.

From table I, 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.

### 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.

### REFERENCES

[1] D. Chaum, “Blind signatures for untraceable payments,” in Proc. Crypto’ 82, 1982, pp. 199-203.
[2] X. Chen, W. Susilo, J. Li, “Efficient algorithms for secure outsourcing of bilinear pairings,” Theoretical Computer Science, vol. 562, pp. 112-121, 2015.

[3] D. Chaum, “Blind signatures,” in Crypto/83, 1983, pp. 153-158.

[4] T. Okamoto, “Provable secure and practical identification schemes and corresponding digital signature schemes,” in Crypto ’92, 1992, pp. 31-52.

[5] J. Camenisch, J. Piveteau, M.Stadler, “Blind signatures based on discrete logarithm problem,” in Eurocrypt’ 94, 1994, pp. 428-432.

[6] E. Mohammed, A. E. Emarah, K. E. Shennawy, “A blind signatures scheme based on ElGamal signature,” in IEEE / AFCEA Eurocomm2000 Information Systems for Enhanced Public Safety and Security, 2000, pp.51-53.

[7] Y. S. Yeh, M. H. Chang, “Schnorr blind signature scheme based on the elliptic curves,” Asia Journal of Information Technology, vol. 2, no. 3, pp. 130-134, 2003.

[8] W. Tsaur, J. Tsao, and Y. Tsao, “An efficient and secure ece-based partially blind signature scheme with multiple banks issuing e-cash payment applications,” in Proc. Int. Conf. Enterprise Comput., E-Commerce Services, 2018, pp. 94–100.

[9] D. H. Duong, W. Susilo and H. T. N. Tran, “A multivariate blind ring signature scheme,” The Computer Journal, vol. 63, no. 1, pp. 1194-1202, Jan. 2020, DOI: 10.1093/COMJN1/BXZ128.

[10] H. Huang, Z. Y. Liu, R. Tso, “Partially blind ECDSA scheme and its application to bitcoin”, in 2021 IEEE Conference on Dependable and Secure Computing (DSC), 2021, pp. 1-8.

[11] D. Khader, “Attribute-based group signatures,” IACR Cryptology ePrint Archive, pp. 159-178, 2007.

[12] H. K. Maji, M. Prabhakaran, M. Rosulek, “Attribute-based signatures: achieving attribute-privacy and collusion resistance,” IACR Cryptology ePrint Archive, pp. 328-351, 2008.

[13] S. F. Shahandashti, R. Safavi-Naini, “Threshold attribute-based signatures and their application to anonymous credential systems,” in International Conference on Cryptology in Africa, 2009, pp. 198-216.

[14] H. K. Maji, M. Prabhakaran, M. Rosulek, “Attribute-based signatures,” Lecture Notes in Computer Science, vol. 6558, pp. 376-392, 2010.

[15] Y. S. Rao, R. Dutta, “Expressive bandwidth efficient attribute based signature and signcryption in standard model,” in Proceedings of Australasian Conference on Information Security and Privacy, 2014, pp. 209-225.

[16] A. Kaafarani, “Traceability, linkability and policy hiding in attribute-based signature schemes,” Ph.D. dissertation, University of Bath, UK, 2015.

[17] S. Rani, S. T. Ali, “Expressive key-policy attribute-based constant-size signature,” in Proceedings of 2017 ISEA Asia Security and Privacy (ISEASP), 2017, pp. 1-4.

[18] R. Guo, H. Shi, Q. Zhao, “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, 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 Transactions on Fuzzy Systems, vol. 29, no. 1, pp. 90-102, Jan. 2021, DOI: 10.1109/ TFUZZ. 2020. 3006520.

[21] S. Liu et al., “Human memory update strategy: a multi-layer template update mechanism for remote visual monitoring,” IEEE Transactions on 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 of Things Journal, vol. 8, no. 19, pp. 15010-15023, Oct. 2021, DOI: 10.1109/ JIOT. 2021. 3073008.

[23] N. S. Saju, “Design and execution of highly adaptable elliptic curve cryptographic processor and algorithm on FPGA using Verilog HDL,” in 2021 International Conference on Communication, Control and Information Sciences (ICCISe), 2021, pp. 1-6, DOI: 10.1109/ ICCISC52257. 2021. 9484881.

[24] S. Liu et al., “Human inertial thinking strategy: A novel fuzzy reasoning mechanism for iot-assisted visual monitoring,” IEEE Internet of Things Journal, pp.1-14, 2022, DOI: 10. 1109/ JIOT. 2022. 3142115.

[25] Y. J. Deng, Y. Xian, “Attribute blind signature scheme based on access tree structure in cloud storage,” Journal of Baoji College of Arts and Sciences, Dec. 2020.

[26] D. W. Li, Z. Y. Wang, J. G. Zhao, “Security analysis of elliptic curve cryptosystem,” Computer Technology and Development, vol. 22, no. 4, pp. 227-234, 2012.

[27] N. Koblitz, “Elliptic curve cryptosystems,” Mathematics of Computation, vol. 48, no. 177, pp. 203-209, 1987.
[28] P. S. Barreto, B. Libert, N. Mccullagh, “Efficient and provably-secure identity-based signatures and signcryption from bilinear maps,” in International Conference on the Theory and Application of Cryptology and Information Security, 2005, pp. 515-532.

[29] H. Hong, Z. Sun, Y. Xia, “Achieving secure and fine-grained data authentication in cloud computing using attribute based proxy signature,” in International Conference on Information Science & Control Engineering. IEEE Computer Society, 2017, pp. 130-134.

[30] C. Sun, Y. Guo, Y. Li, “One secure attribute-based proxy signature,” Wireless Personal Communications, 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, Xidian University., Xi’an, China, 2019.