Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 28 (2025), No. 6, pp. 2371–2382
DOI : 10.47974/JDMSC-2302

An improved attribute-based signature using elliptic curve cryptography

Shivani Goel *
Department of Mathematics
Chaudhary Charan Singh University
Meerut 250004
Uttar Pradesh
India

and

Department of Mathematics
C. L. Jain College
Firozabad 283203
Uttar Pradesh
India

Mridul Kumar Gupta †
Saru Kumari §
Department of Mathematics
Chaudhary Charan Singh University
Meerut 250004
Uttar Pradesh
India

Abstract

The attribute-based signature(ABS) scheme enables users to sign messages based on their attributes while keeping their identities private. ECC provides strong security with smaller key sizes, enhancing the efficiency & practicality of the system. To address the high overhead of traditional ABS schemes, an improved attribute based signature scheme using elliptic curve cryptography along with a default attribute set is proposed. In order to reduce the computational overhead for signing and verification, the technique uses scalar multiplication on elliptic curves, which is computationally lighter than bilinear

* *E-mail:* goelshivani998@gmail.com (Corresponding Author)
† *E-mail:* mkgupta2k2@gmail.com
§ *E-mail:* saryusiirohi@gmail.com

pairing utilised in conventional systems. The scheme's security is demonstrated under the challenging elliptic curve discrete logarithm problem (ECDLP). Additionally, the scheme employs a linear secret sharing scheme (LSSS) access structure, offering stronger access policy expression and higher efficiency compared to simpler access structures. This makes the proposed scheme particularly appropriate for resource-constrained environments, such as cloud end-users. This study leverages advanced mathematical principles, such as number theory and algebraic structures, to develop robust cryptographic algorithms, underscoring the essential role of mathematics in enhancing data security.

Subject Classification: *68Q11.*

Keywords: *Attribute-based signature, Elliptic curve cryptography, LSSS matrix.*

1. Introduction

A digital signature is a cryptographic method for confirming the integrity and veracity of digital communications or documents. It guarantees two things: (a) that a message was created by a original sender (authentication) & (b) that it was not changed in transit. Digital signatures are frequently employed in many different contexts, including email communications, software distribution, financial transactions, & legal contracts, where the authenticity and integrity of information are crucial. Asymmetric cryptography, which uses two keys–a private key & a public key is the foundation of electronic signatures. The signer creates the signature using the private key, & the verifier uses the matching public key to ensure the signature's legitimacy. A strong degree of security is offered by this method, which makes sure that only the owner of the private key may produce a legitimate signature. Attribute-Based Signatures (ABS) [1] represent an another powerful cryptographic tool designed to enhance the flexibility and security of digital signatures. In an ABS scheme, users can sign messages based on specific attributes, such as roles, credentials, or other identifying characteristics, rather than relying solely on their identities. This attribute-centric approach permits for fine-grained control over who can sign and verify messages, making ABS particularly useful in scenarios requiring stringent access control and privacy protection. One of the key benefit of ABS is its capability to provide anonymous authentication. By using attributes to validate signatures, the system ensures that the signer's identity remains hidden, which is crucial in applications where privacy is paramount. For example, in electronic voting systems, whistleblowing platforms, and confidential business transactions, maintaining the anonymity of the participants is essential to protect their privacy and encourage honest communication.

One of the most effective encryption methods is elliptic curve cryptography (ECC) [2] for implementing digital signatures. ECC uses far smaller key sizes than classic techniques like RSA to provide the same degree of security while enabling faster computations and less storage space usage. This makes embedded systems and mobile devices–environments with constrained resources–well suited for ECC. Dhanda, Singh, and Jindal [3] have covered a number of crucial topics related to the application of ECC, including finite fields, curve model and

curve selection, and ECC attacks. Kumari and Kapoor [4] aimed to establish a secure communication framework that enhances confidentiality & data integrity more effectively. Ensuring safe communication between peer-to-peer devices is crucial, because it makes remote access possible in a practical, regulated, and effective way. Utilising cryptographic techniques, validation and authentication are accomplished. Intranet applications connect many systems within a network, with each organization maintaining its own intranet. Their suggested solution incorporates a checksum estimate technique and uses a cryptographic algorithm based on elliptic curve cryptography to produce a safe process. A key is created for further operations when the data is divided into chunks for processing. But most of the traditional ABS schemes [5, 6, 7, 8] are performed using bilinear pairing which requires high computational overhead. In this paper, we present an improved ABS scheme using ECC and the default attribute set. Our scheme aims to reduce the computational and communication overhead typically associated with ABS while maintaining a strong degree of security. By leveraging the properties of ECC along with a default attribute set and employing a robust access structure, our proposed scheme offers a fixed size signature, less verification time, and requires less storage space. It enhances the performance and provides strong protection against unauthorized access and tampering.

Recent Works

Digital signatures, recognized as a fundamental component of public-key cryptography, offer a potential solution for ensuring unforgeability, non-repudiation, and data authentication. The first workable digital signature system was first conceived by Hellman in 1976 [9], and it was formalized in 1978 by Rivest, Shamir, and Adleman [10] using the factoring issue as the basis. Similar to conventional handwritten signatures, an electronic signature offers a mathematical way to check the authenticity of a message, confirming to the recipient that the digital information genuinely comes from the claimed sender. A legitimate digital signature exhibits three crucial properties: integrity, non-repudiation, & authentication. These properties assure the receiver that the data was indeed generated by the person claiming authorship (authentication). An ABS system, which achieves strong unforgeability by linking the signer's key to their attributes, was introduced by Maji, Prabhakaran, and Rosulek [1] in 2008. In 2009 Shahandashti and Safavi-Naini [11] presented another ABS scheme supporting threshold access structures was given. In 2011, Maji, Prabhakaran, and Rosulek [12] developed a general framework for ABS techniques and many bilinear pair-based techniques. Li *et al.* [5] explored a new method for signature signing and offered two effective ABS structures enabling adjustable threshold predicate. They also provided an ABS architecture with several attribute authorities to further undermine the confidence in attribute authority. In 2014, Rao and Dutta [13] proposed a scheme using the LSSS access policy, allowing more flexible fine-grained access control than the threshold access structure. In 2017 Rani and Ali [14] presented a novel ABS scheme using access tree structure, supporting flexible AND and OR access control. A multi-attribute-centric

attribute-based signature criterion for use with electronic health record systems was proposed by Guo *et al.* [15] in 2018 [5]. Hong *et al.* [16] developed a different security mechanism called the combined public-key technique for attribute-based systems (CP-ABES) to manage user access control in Wireless Body Area Networks (WBANs). Their approach integrated encoding & electronic signatures. It employed ciphertext-policy attribute-based encryption to ensure the information confidentiality and access control, and ciphertext-policy ABS to achieve identity authentication. In 2020, Wang *et al.* [17] introduced two efficient pairing-free ciphertext-policy attribute-based techniques, eliminating the mathematical-intensive bilinear pairing operation. Kang *et al.* [18] provided a constant-size attribute-based signature (TFS-ABS) scheme which supports adjustable threshold predicates and is both traceable and forward-secure. When a signer engages in abusive behavior, the suggested technique may be utilized to track the signer's true identity using attribute authority (AA) and lessen the damage caused by key disclosure. Additionally, the proposed technique maintains a fixed signature size that is not affected by the quantity of characteristics. In 2021 Oberko *et al.* [19] provided a detailed survey on ABS schemes. Additionally, the survey provides accurate insights into the design philosophy and several famous algorithms that are developed with concrete. They also looked at ABS's advancements since its founding and its extensions, or other paths. Many efficient attribute based signature schemes [20, 21, 22, 23, 24, 25] came further based on bilinear pairings. But each paring requires high computations. For this reason, we built our signature system using ECC.

Our Contribution

We present an effective attribute-based signature system utilising ECC in this work along with a default attribute set to randomize the user's attribute set, maintaining attribute signer privacy strongly. Its security is grounded in the intractability of the ECDLP. Our method greatly reduces the computational cost for both signature creation and verification by substituting scalar multiplication for the complex bilinear pairing operation on the elliptic curve. Additionally, the use of a monotonic access structure LSSS matrix enhances expressivity and efficiency, eliminating the need for recursive operations to attain fine-grained access control. Furthermore, our technique ensures a constant sign length free of the number of signer's attributes, thereby minimizes communication, computational cost and time.

Structure of the Paper

The rest of our article is structured in the following order: Section 3 comprised of some basic concepts required in our article. Section 4 comprised of the framework & security model of our proposed signature technique. Our scheme's construction is covered in Section 5. Section 6 proves the correctness & urforgeability of the scheme. Section 7 provides the key findings of the technique and lasts with the references.

3. Preliminaries

3.1 *Elliptic curve cryptography*

Elliptic Curve Cryptography (ECC) [2], defined over a finite field GF(q), depends on the characteristics of elliptic curves, which are mathematical curves described by a specific equation $z^2 = y^3 + ay + b(modq)$ where $4a^3 + 27b^2 \neq 0$. Both a public key & a private key are owned by each user in ECC. The number that is created at random is the private key, while the public key is derived from a point on the elliptic curve. For message encryption, The sender determines a point on the curve by using the public key of the recipient & then performs a number of mathematical procedures. to encode the information. After that, the recipient uses their private key to decode it and retrieves the original content.

3.2 *Linear secret Sharing Scheme*

Let $R_1, R_2, \ldots, R_n$ represent a set of participants, S_T be an $s \times t$ matrix, & $\phi: \{1,2,\ldots,s\} \rightarrow R$ is a mapping that associates a member of the set with each row of the matrix. The following two algorithms describe the linear secret sharing scheme access structure, in accordance with the concept of a linear secret sharing scheme:

Distribute: Given the input matrix S_T with s rows and t columns, the mapping function ϕ, and the secret value $\beta \in Z_p^*$, select random values $\beta_2, \ldots, \beta_t \in Z_p^*$. Form the vector $v = (\beta, \beta_2, \ldots, \beta_t)$, which results in the s shared values $\{\lambda_j = S_{T_j} \cdot v\}_{j\in[1,s]}$ corresponding to the attribute $\phi(j)$, where S_{T_j} denotes the j-th row vector of the matrix S_T.

Reconstruct: Given the input matrix S_T with s rows and t columns, the function ϕ, & the collection of valid attributes $A \in R$, use the Gaussian elimination method to find the collection of reconstruction constants $\{w_j\}$ for $j \in J$ in polynomial time. This set satisfies the equation $\sum_{j\in J} S_{T_j} w_j = (1,0,\ldots,0)$, meaning $\sum_{j\in J} \lambda_j w_j = \beta$. Then, outputs $\{w_j\}$ for $j \in J$, where $J = \{j \in [1,s]: \phi(j) \in W\}$.

3.3 *Elliptic curve discrete logarithm problem (ECDLP)*

The security of the proposed scheme is based on the ECDLP assumption. Choose two points on the elliptic curve, P and K, where $K = r \cdot P$ & r is an integer. Given the points P & $r \cdot P$, it is mathematically challenging to ascertain the value of r.

4. Framework and Security model

4.1 *Framework of our system*

ABS technique using ECC comprises of the following four algorithms:

Setup: The attribute authority AA uses the security parameter as input when executing this procedure. It provides public parameters & master secret key.

KeyGen: This algorithm is also executeed by AA, which uses public parameters, master secret key, access structure & the attribute set of the user as input & results the signing key for the users.

Sign: This method is run by the user, who then uses the message as input and the signing key & to generate the signature.

Verify: This algorithm is executed by the verifier, which uses signature & public key as the input. This results in the validity of the signature.

4.2 *System model*

As illustrated in Figure 1, our system has four distinct entities: the attribute authority, the data owner, the data user, & the data service provider. The attribute authority generates the public parameters and signing keys for the users whose attribute sets meet the predicate. The attribute authority uploads the public parameters to the lagre server, which is known to be the data service provider. Attribute authority gives the signing keys to the claimed users. The signer/ user then creates the signature on the information using his signing key and uploads the signature along with the information to the server. The data user or we say the verifier picks the information along with the signature and the public key of the user from the server. Verifier checks the authenticity of the signer by verifying the signature using his public key.

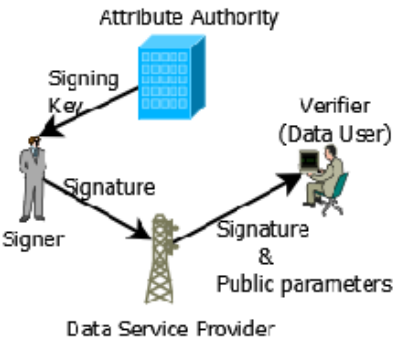

Figure 1
System architecture

4.3 *Security model*

4.3.1 Definition: Correctness

An ABS scheme must be accurate if the condition Verify $(PK, \varphi, \mathcal{M}, Sign) = 1$ is met for every access policy (M, ϕ) and attribute set φ that complies with this policy.

4.3.2 Definition: Unforgeability

The following polynomial-time game between adversary $\mathcal{A}$ & challenger $\mathcal{C}$ defines an ABS scheme as being unforgeable to message attacks and under the selective attribute conditions:

- The message $\mathcal{M}^*$ and the challenge attribute set φ^* are produced by the adversary $\mathcal{A}$.
- After choosing the security parameter k, Challenger $\mathcal{C}$ computes $(PK, MSK) \leftarrow \text{Setup}(k)$. After that, $\mathcal{C}$ sends PK to $\mathcal{A}$.
- It is permitted for the adversary $\mathcal{A}$ to pose polynomial-time enquiries, and challenger $\mathcal{C}$ forwards the outputs of these queries to $\mathcal{A}$.
- The challenger $\mathcal{C}$ receives the access structure Γ^* from the adversary $\mathcal{A}$. If $\Gamma^*(\varphi^*) \neq 1$, challenger $\mathcal{C}$ performs the Extract algorithm to create the signing key SK & transmits it to $\mathcal{A}$.
- Challenger $\mathcal{C}$ receives the attribute set φ^* and message bit $\mathcal{M}$ from adversary $\mathcal{A}$. After that, $\mathcal{C}$ uses the Sign algorithm to create the signature θ^*, which it subsequently delivers to adversary $\mathcal{A}$.
- Adversary $\mathcal{A}$ produces a forged signature θ^* for $(\mathcal{M}^*, \varphi^*)$. If the following three requirements are met then the adversary $\mathcal{A}$ wins:

$$\text{Verify}\,(PK, \varphi^*, \mathcal{M}^*, \theta^*) = 1$$

$\mathcal{A}$ does not request the signature for $(\mathcal{M}^*, \varphi^*)$. For any query, the access structure Γ^* is satisfied such that $\Gamma^*(\varphi^*) \neq 1$. The system is considered unforgeable if $\mathcal{A}$ is unable to win in the above game having a non-negligible probability within polynomial time.

5. Construction of the scheme

The following is how our signature technique is put together:

5.1 *Setup*

Consider $GF(k)$ as a finite field with order k, & let E be an elliptic curve over $GF(k)$. Define P as an element within E having a large prime order q. The point P creates a cyclic subgroup of E, making the ECDLP infeasible within this subgroup. $V = \{1,2,\ldots,l\}$ is represented as the collection of attributes in the system, with j being an individual attribute from this set. Moreover, Assume $\mathcal{F}: \{0,1\}^* \rightarrow Z_q^*$ represents a cryptographically safe hash function. Define a default attribute set $\mu = \{l+1, l+2, \ldots, 2l-1\}$ s.t. $|\mu| = l-1$. During the system parameter generation, an element $\beta \in Z_q^*$ is randomly selected, and $P_{pub} = \beta P$ is calculated. For each attribute $j \in V \cup \mu$, select a random element $y_j \in Z_q^*$, & calculate

$$x_j = y_j P \tag{1}$$

Hence, the output is the public key $PK = \{q, P, \mathcal{F}, x_1, x_2, \ldots, x_{2l-1}, Ppub\}$ & the master secret key $MSK = \{\beta, y_1, y_2, \ldots, y_{2l-1}\}$.

5.2 *KeyGen*

Suppose (M, ϕ) represents the access structure Γ. To create shares, a matrix M with s rows & r columns is utilised. To associate each j with a party, row j is labelled with the function ϕ_j for each s rows & r columns is

utilised. To each $j \in \{1,2,\ldots,s\}$, row j. Now, make a column vector $\vec{\alpha} = (\beta, t_2, t_3, \ldots, t_r)$, where $t_2, t_3, \ldots, t_r$ are randomly chosen elements in Z_q^*. For each j in the range $[1, s]$, the secret value is calculated as $\delta_j = \vec{M_j} \cdot \vec{\alpha}$, and C_j is computed as $\delta_j + y_j$.
i.e.

$$C_j = \delta_j + y_j \tag{2}$$

The algorithm then produces the signing key $SK = \{C_j\}$ for $j \in [1, s]$.

5.3 *Sign*

Suppose the signature attribute set be $\varphi \subset V$. If the signer's attributes meet the access structure Γ, a set of constants $\{\gamma_j \in Z_q^*, j \in \bar{\gamma}\}$ must be present that can be determined in polynomial time, such that:

$$\Sigma_{j\in\bar{\gamma}} \gamma_j M_j = (1,0,\ldots,0) \tag{3}$$

where $\bar{\gamma} = \{j \in [1, s]: \phi(j) \in W \cup \mu\}$. The signer then finds the signature on the message $\mathcal{M}$ as

$$\theta = \mathcal{F}(\mathcal{M})\Sigma_{j\in\bar{\gamma}} C_j \gamma_j \tag{4}$$

Finally, the signer gives this signature θ to the message owner or the verifier.

5.4 *Verify*

After receiving the signature, verifier uses the following equation to verify the signature's legitimacy.

$$\theta \cdot P = \mathcal{F}(\mathcal{M})(P_{pub} + \Sigma_{j\in\bar{\gamma}} x_j \gamma_j) \tag{5}$$

If the equation is satisfied then the verifier returns 1, otherwise 0.

6. Security Analysis

6.1 *Correctness Proof*

To verify the equation 5.

$$\begin{aligned} \theta \cdot P &= (\mathcal{F}(\mathcal{M})\Sigma_{j\in\bar{\gamma}} C_j \gamma_j) \cdot P && \text{(Using 2)} \\ &= \mathcal{F}(\mathcal{M})\Sigma_{j\in\bar{\gamma}} (\delta_j + y_j)\gamma_j \cdot P \\ &= \mathcal{F}(\mathcal{M})(\Sigma_{j\in\bar{\gamma}} \delta_j \gamma_j \cdot P + \Sigma_{j\in\bar{\gamma}} y_j \gamma_j \cdot P) \end{aligned}$$

(Using reconstruction property of the LSSS and eq 1)

$$\begin{aligned} &= \mathcal{F}(\mathcal{M})(\beta \cdot P + \Sigma_{j\in\bar{\gamma}} x_j \gamma_j) \\ &= \mathcal{F}(\mathcal{M})(P_{pub} + \Sigma_{j\in\bar{\gamma}} x_j \gamma_j) \end{aligned}$$

Hence, correctness of the equation is verified.

6.2 *Unforgeability*

Theorem: The suggested signature protocol is resistant to forgery due to the difficulty of ECDLP.

Proof: Firstly, the attribute set φ^* and and message blocks $\mathcal{M}^* = \{\mathcal{M}_0^*, \mathcal{M}_1^*, \ldots, \mathcal{M}_f^*\}$, which the adversary $\mathcal{A}$ intends to forge, are sent to the challenger $\mathcal{C}$. Using these attributes, $\mathcal{C}$ creates the public parameters in the following way:

$\mathcal{C}$ pics $\beta^* \in Z_{q^*}$ randomly & finds $P_{pub} = \beta^* \cdot P$. Then, for every attribute in the attribute set the Challenger $\mathcal{C}$ computes $x_j^* = y_j^* \cdot P$, where $y_j^* \in Z_{q^*}$ is randomly choosen. $\mathcal{C}$ uses a hashing function $\mathcal{F}: \{0,1\}^* \to Z_q^*$. Finally, $\mathcal{C}$ gives the list of public parameters $PK = \{q, P, \mathcal{F}, x_1^*, x_2^*, \ldots, x_{2l-1}^*\}$ to the adversary $\mathcal{A}$.

To create the signing key, $\mathcal{C}$ makes a column vector $\vec{v} = (\beta^*, d_2, d_3, \ldots, d_r)$ where $d_2, d_3, \ldots, d_r \in Z_q^*$ are randomly choosen. Then, computes $\Delta_j = L_j \cdot \vec{v}$ & generates the signing key $sk_j = \Delta_j + y_j^*$.

$\mathcal{A}$ sends the message block $\mathcal{M}_0 \in \mathcal{M}$ & the attribute set φ^* to the challenger $\mathcal{C}$. $\mathcal{C}$ then puts the signature on the message block. If the attribute set φ^* meets the access structure Γ^* then in polynomial time, $\mathcal{C}$ can search the constants $\{\gamma_j \in Z_q^*, j \in \bar{\gamma}\}$ and produces $\Sigma_{j\in\bar{\gamma}}\gamma_j M_j = (1,0,\ldots,0)$, where $\bar{\gamma} = \{j \in [1,s]: \phi(j) \in \varphi^* \cup \mu^*\}$. Compute

$$\begin{aligned}\theta^* &= \mathcal{M}_0 \Sigma_{\bar{\gamma}} sk_j \gamma_j, k = \Sigma_{\bar{\gamma}} y_j^* \gamma_j \\ &= \mathcal{M}_0 \Sigma_{\bar{\gamma}} (\Delta_j + y_j^*)\gamma_j \\ &= \mathcal{M}_0 (\Sigma_{\bar{\gamma}} \Delta_j \gamma_j + \Sigma_{\bar{\gamma}} y_j^* \gamma_j) \\ &= \mathcal{M}_0 (\beta^* + k)\end{aligned}$$

The challenger $\mathcal{C}$ then givess this signature to the adversary $\mathcal{A}$. To forge the signature, $\mathcal{A}$ requires to obtain β^*. However, finding β^* is difficult due to the hardness of ECDLP assumption. Therefore, the signature of our proposed technique is unforgeable.

7. Conclusion

In this research article, we offer an improved attribute-based signature scheme utilizing elliptic curve cryptography & a default attribute set. By leveraging the strengths of ECC, we achieve robust security with significantly smaller key sizes, enhancing both the efficiency & practicality of the system. This approach is computationally lighter than the bilinear pairing technique typically used in traditional ABS techniques. Thereby, our signature technique decreases the computational overhead for both signing & verification processes, as this method is based on scalar multiplication on elliptic curves. It provides significant benefits in the randomization of attribute set, as it confuses with the default attribute set. It features fast signature speed, less verification time, and less storage space. Furthermore, our scheme employs LSSS access structure, which provides a more expressive and efficient access policy compared to simpler structures like the "And" gate or access tree. This advancement not only strengthens access control but also enhances the overall computational efficiency. The combination of these innovations makes our proposed ABS scheme especially well-suited for conditions with limited resources, including those

encountered by cloud end-users. Our result shows that the suggested technique provides a viable and effective solution for safe & efficient ABS in such settings. Our goal for further research is to enhance performance and investigate the security trade-offs between bilinear pairing and scalar multiplication.

Acknowledgement:

This work is supported by the grant from the State Government of Uttar Pradesh, India sanctioned under Government order no.-47/2021/606/sattar-4-2021-4(56)/2020 dated 30/03/2021.

Conflict of interest:

There are no conflicts of interest for the authors.

References

[1] H. Maji, M. Prabhakaran, and M. Rosulek, "Attribute based signatures: Achieving attribute privacy and collusion-resistance. 2008," EPRINT http://eprint. iacr. org/2008/328 (2008).

[2] N. Koblitz, "Elliptic curve cryptosystems," *Mathematics of computation*, vol. 48, no. 177, pp. 203–209 (1987).

[3] S. S. Dhanda, B. Singh, and P. Jindal, "Demystifying elliptic curve cryptography: Curve selection, implementation and countermeasures to attacks," *Journal of Interdisciplinary Mathematics*, vol. 23, no. 2, pp. 463–470 (2020).

[4] A. Kumari and V. Kapoor, "Competing secure text encryption in intranet using elliptic curve cryptography," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 23, no. 2, pp. 631–641 (2020).

[5] J. Li, M. H. Au, W. Susilo, D. Xie, and K. Ren, "Attribute-based signature and its applications," in Proceedings of the 5th ACM symposium on information, computer and communications security, pp. 60–69 (2010).

[6] A.-J. Ge, C.-G. Ma, and Z.-F. Zhang, "Attribute-based signature scheme with constant size signature in the standard model," *IET Information Security*, vol. 6, no. 2, pp. 47–54 (2012).

[7] Y. Ren and T. Jiang, "Verifiable outsourced attribute-based signature scheme," *Multimedia Tools and Applications*, vol. 77, pp. 18 105–18 115 (2018).

[8] Q. Tao, X. Cui, and A. Iftekhar, "A novel lightweight decentralized attributebased signature scheme for social co-governance," *Information Sciences*, vol. 654, p. 119839 (2024).

[9] M. Hellman, "New directions in cryptography," *IEEE transactions on Information Theory*, vol. 22, no. 6, pp. 644–654 (1976).

[10] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Communications of the ACM*, vol. 21, no. 2, pp. 120–126 (1978).

[11] S. F. Shahandashti and R. Safavi-Naini, "Threshold attribute-based signatures and their application to anonymous credential systems," in Progress in Cryptology–AFRICACRYPT 2009: Second International Conference on Cryptology in Africa, Gammarth, Tunisia, June 21-25, 2009. Proceedings 2. Springer, pp. 198–216 (2009).

[12] H. K. Maji, M. Prabhakaran, and M. Rosulek, "Attribute-based signatures," in Cryptographers' track at the RSA conference. Springer, pp. 376–392 (2011).

[13] Y. S. Rao and R. Dutta, "Expressive bandwidth-efficient attribute based signature and signcryption in standard model," in Australasian Conference on Information Security and Privacy. Springer, pp. 209–225 (2014).

[14] S. Rani and S. T. Ali, "Expressive key-policy attribute-based constant-size signature," in 2017 ISEA Asia Security and Privacy (ISEASP). *IEEE*, pp. 1–4 (2017).

[15] 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. 11 676–11 686 (2018).

[16] J. Hong, B. Liu, Q. Sun, and F. Li, "A combined public-key scheme in the case of attribute-based for wireless body area networks," *Wireless Networks*, vol. 25, pp. 845–859 (2019).

[17] Y. Wang, B. Chen, L. Li, Q. Ma, H. Li, and D. He, "Efficient and secure ciphertext-policy attribute-based encryption without pairing for cloudassisted smart grid," *IEEE Access*, vol. 8, pp. 40 704–40 713 (2020).

[18] Z. Kang, J. Li, J. Shen, J. Han, Y. Zuo, and Y. Zhang, "Tfs-abs: Traceable and forward-secure attribute-based signature scheme with constant-size," *IEEE Transactions on Knowledge and Data Engineering*, vol. 35, no. 9, pp. 9514–9530 (2023).

[19] P. S. K. Oberko, V.-H. K. S. Obeng, H. Xiong, and S. Kumari, "A survey on attribute-based signatures," *Journal of Systems Architecture,* vol. 124, p. 102396 (2022).

[20] Q. Xue, Z. Lu, and T. Zhang, "Attribute-based proxy signature scheme with dynamic strong forward security," *International Journal of Sensor Networks*, vol. 44, no. 4, pp. 214–225 (2024).

[21] B. Chen, T. Xiang, X. Li, M. Zhang, and D. He, "Efficient attribute-based signature with collusion resistance for internet of vehicles," *IEEE Transactions on Vehicular Technology*, vol. 72, no. 6, pp. 7844–7856 (2023).

[22] O. Blazy, L. Brouilhet, E. Conchon, and M. Klingler, "Anonymous attributebased designated verifier signature," *Journal of Ambient Intelligence and Humanized Computing,* vol. 14, no. 10, pp. 1–11 (2023).

[23] Q. Su, R. Zhang, R. Xue, Y. Sun, and S. Gao, "Distributed attribute-based signature with attribute dynamic update for smart grid," *IEEE Transactions on Industrial Informatics*, vol. 19, no. 9, pp. 9424–9435 (2022).

[24] J. Zhang and J. Chen, "Efficient traceable attribute-based signature with update-free revocation for blockchain," *The Computer Journal,* vol. 66, no. 4, pp. 842–865 (2023).

[25] K. Gu, K.Wang, and L. Yang, "Traceable attribute-based signature," *Journal of Information Security and Applications*, vol. 49, p. 102400 (2019).

Received August, 2024