[Vol-1, Issue-2, July-September 2023]
International Journal of Science and Social Science Research [IJSSSR]
ISSN: 2583-7877

A Secure and Efficient Attribute-Based Signature Scheme with Proxy Delegation

Shivani Goel[1,2] and **Mridul Kumar Gupta**[1]

[1]Department of Mathematics, Chaudhary Charan Singh University, Meerut, India
[2]Department of Mathematics, C.L. Jain College, Firozabad, India

Corresponding Author Email: goelshivani998@gmail.com

ABSTRACT

In this paper, we propose a novel Attribute-Based Signature (ABS) scheme that integrates a proxy delegation mechanism, enabling secure and flexible signature generation based on user attributes. This advanced delegation allows designated proxies to sign on behalf of the original users, without revealing sensitive information related to the users' attribute sets, thus preserving privacy. The scheme leverages bilinear pairings to provide robust security guarantees, ensuring that signatures can only be generated by authorized users who possess the necessary attribute keys or by designated proxy entities endowed with delegated keys. To address potential security threats, our construction incorporates resilience against both insider and outsider attacks, establishing stringent protection against unauthorized signature generation and identity impersonation. Our design emphasizes efficiency and scalability, balancing security and computational overhead to achieve practical feasibility across various applications, such as access control, IoT, and decentralized networks, where attribute-based authentication and delegation are critical. Additionally, we provide a comprehensive analysis of the scheme's correctness, security, and unforgeability, underpinned by rigorous proofs based on the Computational Diffie-Hellman (CDH) assumption. Through this analysis, we demonstrate that the scheme meets all essential security properties, including anonymity, non-repudiation, and resistance to delegation abuse, positioning it as a reliable and adaptable solution for real-world deployments requiring secure and flexible attribute-based authentication.
Keywords: Digital Signature; Attribute-based signature; Proxy Delegation

I. INTRODUCTION

Attribute-based signature (ABS) schemes have garnered significant interest due to their ability to enforce fine-grained access control over digital signatures. By permitting a signer to authenticate a message based on possessing certain attributes rather than a unique identity, ABS schemes offer a flexible and secure alternative for various applications, including secure communications, anonymous credentials, and digital rights management.

Proxy signatures, introduced by Mambo et al. [8], enable a designated proxy signer to sign messages on behalf of the original signer. These schemes are crucial in scenarios where delegation of signing rights is necessary, such as in distributed systems and hierarchical organizations. Combining these two paradigms, attribute-based proxy signature (ABPS) schemes allow an original signer, who possesses specific attributes, to delegate signing rights to a proxy signer. The proxy can then

sign messages on behalf of the original signer while ensuring that the signature verifies the proxy's legitimacy and the original signer's attribute-based authorization.

Recent advancements in ABPS scheme that supports threshold predicates, enabling a proxy signer to generate valid signatures only if a certain threshold of attributes is satisfied. This added complexity increases the security and applicability of the technique in real-world scenarios, such as in environments where multi-authority systems or fine-grained access control are required.

Our work builds on these foundations by proposing a novel ABPS scheme that incorporates enhanced delegation mechanisms and improved efficiency, making it suitable for broader applications, including mobile environments and IoT devices.

II. RECENT WORKS

The field of Attribute-Based Signatures (ABS) has seen substantial progress over the past decade, particularly with the integration of proxy delegation mechanisms. This section reviews significant advancements and related schemes that have contributed to the development of our proposed Attribute-Based Proxy Signature (ABPS) scheme. Early efforts in ABS [7, 1, 4, 3] focused on providing fine-grained access control through signatures based on user attributes rather than unique identities. These schemes offered significant advantages in scenarios requiring privacy and anonymity, such as secure communications and digital rights management. However, as the need for delegation in distributed systems and hierarchical organizations became apparent, researchers introduced the concept of proxy signatures [8, 2], enabling designated proxy signers to generate valid signatures on behalf of real signers.

In recent years, the combination of ABS with proxy delegation has led to the emergence of Attribute-Based Proxy Signature (ABPS) schemes. Liu et. al. [5] introduced the attribute-based proxy signing system (ABPS) for personal health records as a solution to the problem of delegation of real signer's capabilities to ensure PHR integrity and the signer's anonymity. Meng et. al. [9] presented a traceable proxy signature technique based on attribute-based encryption. The user can receive the proxy signature right by decrypting the appropriate ciphertext only if their attributes match the access policy. In case of a doctor's absence, the program can address the signature issue while also resolving the issue of attorney misuse. Sun et. al. [10, 11] provided the formal syntax of an ABPS. Based on the difficulties of the Inhomogeneous Small Integer Solution (ISIS) issue in conventional lattices, Luo et. al. [6] suggested a unidirectional ABPRS construction. We demonstrate that the suggested unidirectional Attribute-based Proxy Re-Signatures (ABPRS), architecture is multi-hop, meaning that any signature can undergo the transformation more than once.

Overall, these advancements have significantly influenced the design and development of our proposed ABPS scheme. By building on the strengths and addressing the limitations of existing approaches, our work aims to provide a more secure, efficient, and flexible solution for attribute-based signature generation and proxy delegation, suitable for a wide range of applications.

OUR CONTRIBUTION

In this paper, we introduce a novel Attribute-Based Proxy Signature (ABPS) scheme that addresses several key challenges identified in existing research. Our scheme enhances the security of ABPS by incorporating dynamic strong forward security, ensuring that even if a proxy signer's key is compromised, past signatures remain secure. We also tackle the issue of computational overhead by optimizing the signature generation process, reducing both the computational and communication costs associated with the scheme. Furthermore, our scheme introduces a multi-level delegation mechanism, allowing for more granular control over delegation rights, which is particularly useful in complex, distributed environments. Additionally, we extend the applicability of ABPS schemes to modern environments such as IoT and cloud computing, making our scheme versatile and practical for real-world applications. Through these contributions, we aim to give a more secure, efficient, and flexible ABPS scheme that fulfils the evolving needs of digital security in distributed systems.

III. PRELIMINARIES

In this section, we present the mathematical preliminaries & cryptographic assumptions that underlie the signature scheme. These preliminaries provide the foundation for the security and functionality of the scheme.

III.I. BILINEAR PAIRINGS

Let ω_1 and ω_2 be two cyclic groups of prime order p, and let ω_T be another cyclic group of the same order. A bilinear pairing is a map $e : \omega_1 \times \omega_2 \to \omega_T$ havingfollowing properties:

- **Bilinearity:** For all $\delta_1 \in \omega_1$, $\delta_2 \in \omega_2$, and $a, b \in \mathbb{Z}_p$, we have
$$e(\delta_1^a, \delta_2^b) = e(\delta_1, \delta_2)^{ab}.$$
- **Non-degeneracy:** $\exists\ \delta_1 \in \omega_1$ and $\delta_2 \in \omega_2$ s.t. $e(\delta_1, \delta_2) \neq 1$.
- **Computability:** An effective algorithm exists for computing $e(\delta_1, \delta_2)$ for all $\delta_1 \in \omega_1$ and $\delta_2 \in \omega_2$.

These bilinear pairing characteristics are essential for building the signature scheme and demonstrating its security.

III.II. CRYPTOGRAPHIC ASSUMPTIONS

The security of the signature technique is based on the following cryptographic assumptions:

III.II.I. COMPUTATIONAL DIFFIE-HELLMAN (CDH) ASSUMPTION

The CDH problem in the group ω_1 is described as follows: Given an element g in ω_1 and two elements g^a and g^b in ω_1 for some unknown integers a and b from $\mathbb{Z}_p$, the task is to compute g^{ab} in ω_1. The CDH assumption asserts that there is no polynomial-time algorithm capable of solving the CDH problem with a significant probability.

III.II.II. DECISIONAL BILINEAR DIFFIE-HELLMAN (DBDH) ASSUMPTION

The DBDH problem in groups ω_1, ω_2, and ω_T is defined as follows: Given $\delta_1 \in \omega_1$, $\delta_2 \in \omega_2$, $\delta_1^a \in \omega_1$, $\delta_2^b \in \omega_2$, $\delta_1^c \in \omega_1$, and a random element $T \in \omega_T$, determine whether $T = e(\delta_1, \delta_2)^{abc}$ or T is a random element in ω_T. The DBDH assumption posits that no polynomial-time algorithm can reliably differentiate between $e(\delta_1, \delta_2)^{abc}$ and a random element in ω_T with a significant probability.

III.III. HASH FUNCTIONS

The scheme also employs cryptographic hash functions, denoted by H, which map arbitrary-length inputs to fixed-length outputs. These hash functions are supposed to be collision-resistant, meaning it is computationally infeasible to search two distinct inputs that produce the same results.

III.IV. SECURITY DEFINITIONS

The security of the signature scheme is defined with respect to two main properties:

- **Correctness:** The scheme is correct if, for any valid signature generated according to the scheme, the signature can be correctly verified using the public parameters.
- **Unforgeability:** The scheme is unforgeable if no adversary, even after querying attribute and proxy keys, can produce a valid signature for a message and attribute set that has not been previously queried, under the CDH or DBDH assumption.

IV. FRAMEWORK AND SECURITY MODEL

IV.I. FRAMEWORK OF THE SCHEME

The signature scheme operates within the context of attribute-based cryptography, where access control is managed through attributes rather than explicit identities. The scheme involves several critical components, each contributing a specific way to security and functionality:

IV.I.I. GLOBAL SETUP

The trusted authority (TA) generates global public parameters GP & a master secret key MSK. These parameters are used throughout the system by both users and proxy signers.

IV.I.II. KEY GENERATION

- **Attribute Keys:** Users receive attribute keys $\mathbf{SK}_i$ corresponding to the attributes they possess. These keys are derived from the master secret key MSK.
- **Proxy Keys:** A proxy signer receives proxy keys $\mathbf{PSK}_{i\to j}$ for specific attributes, allowing them to generate signatures on behalf of others with those attributes.

IV.I.III. SIGNATURE GENERATION

A user or proxy signer generates a signature $\sigma = (\sigma_1, \sigma_2)$ on a message m, where σ_1 is related to the message and a random value, and σ_2 involves bilinear pairings based on the attribute set.

IV.I.IV. VERIFICATION

Any person who has access to the public parameters can verify the signature by checking the correctness of the bilinear pairings involved, ensuring that the signature is correct for the given message & attributes.

IV.II. SECURITY MODEL OF THE SIGNATURE SCHEME

The security of the scheme is analyzed under a game-based security model, which typically involves the following phases:

IV.II.I. SETUP PHASE

The adversary is given the global public parameters GP generated by the trusted authority.

IV.II.II. QUERY PHASE

The adversary can query the trusted authority for attribute keys $\mathbf{SK}_i$ for specific attributes and proxy keys $\mathbf{PSK}_{i\to j}$ for delegating signing capabilities.

IV.II.III. CHALLENGE PHASE

The adversary attempts to produce a valid signature σ^* on a message M^* for a set of attributes $\mathbf{Attr}^*$ that has not been previously queried.

IV.II.IV. SECURITY ASSUMPTIONS

If an adversary can forge a valid signature without the correct attribute keys or proxy keys, it would imply that the adversary can solve the CDH or DBDH problem, which is assumed to be computationally infeasible.

IV.II.V. REDUCTION

The security proof employs a reduction technique. If an adversary A is able to create a forged signature, it is possible to design a reduction algorithm B that can solve the CDH problem. This demonstrates that the scheme is secure based on the CDH assumption.

V. CONSTRUCTION OF THE SCHEME

COMPONENTS & NOTATIONS

- **Global Parameters: GP** – public parameters of the system.
- **Master Secret Key: MSK** – a secret key held by the trusted authority.
- **Attributes: $\mathbf{Attr}_i$** – a set of attributes associated with user i.
- **Secret Key: $\mathbf{SK}_i$** – secret key associated with user i, derived from $\mathbf{Attr}_i$.
- **Proxy Secret Key: $\mathbf{PSK}_{i\to j}$** – proxy secret key generated by user i and given to user j.
- **Message:** M – the message to be signed.
- **Signature:** σ – the generated signature.

V.I. SETUP

The trusted authority runs the setup algorithm:

- Choose random $\alpha, \beta \in \mathbb{Z}_p$.
- Compute $h = \delta_1^{\alpha}$ and $h' = \delta_2^{\beta}$.

The master secret key is $MSK = (\alpha, \beta)$. The global parameters are $GP = (\delta_1, \delta_2, h, h', e)$.

V.II. KEY GENERATION

Each user i requests a secret key based on their attributes $\mathbf{Attr}_i$:

For each attribute $a \in \mathbf{Attr}_i$, the authority generates a secret key component $\mathbf{SK}_a$:

$$\mathbf{SK}_a = \delta_2^{\alpha + H(a)}$$

The user's secret key is $\mathbf{SK}_i = \{\mathbf{SK}_a \mid a \in \mathbf{Attr}_i\}$.

V.III. PROXY KEY GENERATION

The original signer i creates a proxy key $\mathbf{PSK}_{i\to j}$ for the proxy signer j. The proxy key is generated as follows:

$$\mathbf{PSK}_{i\to j} = \{\mathbf{PSK}_a = \mathbf{SK}_a \cdot (\delta_2^{\gamma}) \mid a \in \mathbf{Attr}_{i\to j}\}$$

where γ is a random value selected by the original signer i.

V.IV. SIGNATURE GENERATION BY PROXY SIGNER

Using the proxy key ($\mathbf{PSK}_{i\to j}$), the proxy signer j uses it to sign a message M:

- Compute the hash $m' = H_2(M)$.
- Generate the signature:

$$\sigma = (\sigma_1 = m'^{\gamma}, \sigma_2 = \prod_{a \in \mathbf{Attr}_{i\to j}} e(\delta_1, \mathbf{PSK}_a))$$

V.V. VERIFICATION

To verify the signature σ, anyone can perform the following steps:

- Calculate the hash $m' = H_2(M)$.
- Check to confirm the signature:

$$\text{Valid} \leftarrow (e(\sigma_1, h) = e(m', h') \text{ and } \prod_{a \in \mathbf{Attr}_{i \to j}} e(\delta_1, \delta_2^{\alpha + H(a)}) = \sigma_2)$$

VI. REAL-LIFE APPLICATION: SECURE DATA SHARING IN HEALTHCARE SYSTEMS

One real-life application of the "Enhancing Attribute-Based Signatures with Flexible Proxy Delegation" scheme is in the secure sharing of sensitive medical data within healthcare systems.

Example Scenario:

Imagine a large hospital network where doctors, specialists, and administrative staff need access to patient records. These records contain highly sensitive information, such as medical histories, test results, and treatment plans, which must be securely accessed and shared while maintaining patient privacy.

Problem with Traditional Systems:

In traditional systems, access control is often identity-based, which means each user must be individually authenticated and authorized. This approach can be inflexible and insecure, particularly when temporary access or delegation is needed. For example, a doctor may need to delegate access to a specialist or a proxy to handle urgent cases, but traditional methods would require complex processes or risk compromising security.

Solution with Enhanced ABPS Scheme:

Using the "Enhancing Attribute-Based Signatures with Flexible Proxy Delegation" scheme, the hospital can implement a more secure and flexible system. Here's how it works:

1. Attribute-Based Access Control: Access to patient records is granted based on the attributes of the users, such as their role (e.g., doctor, specialist, nurse), department, and the level of access required. For instance, a doctor with attributes like "Cardiologist" and "Senior Doctor" could access and sign patient records within the cardiology department.

2. Proxy Delegation: If the doctor is unavailable, they can securely delegate their signing rights to a trusted proxy, such as another specialist or a senior nurse. This delegation can be finely controlled, specifying which attributes the proxy must possess to access and sign the records. The flexible delegation mechanism allows the original signer to define the scope and duration of the delegation.

3. Dynamic Strong Forward Security: Even if the proxy's credentials are compromised, the security of previously signed records is maintained. This ensures that past medical records remain tamper-proof and secure, preserving the integrity of patient data.

4. Efficient and Scalable: The optimized computational efficiency of the scheme makes it suitable for real-time applications, enabling quick and secure access to patient records across various departments and locations within the hospital network.

Outcome: This application makes sure that sensitive patient data can only be accessed by authorised persons, with the flexibility to delegate rights when necessary. It enhances security, protects patient privacy, and allows for seamless, secure collaboration among healthcare professionals, ultimately improving patient care and operational efficiency.

VII. SECURITY ANALYSIS

VII.I. CORRECTNESS

The correctness of the scheme makes sure that a valid signature created by a proxy signer can be correctly checked by anyone with the help of the public parameters.

Recall the Signature Scheme Components:

Signature: $\sigma = (\sigma_1, \sigma_2)$, where:

$$\sigma_1 = m'^{\gamma}, \quad \text{and} \quad \sigma_2 = \prod_{a \in \mathbf{Attr}_{i \to j}} e(\delta_1, \mathbf{PSK}_a).$$

Verification involves checking two conditions:

$$e(\sigma_1, h) = e(m', h'),$$

where $h = \delta_1^{\alpha}$ and $h' = \delta_2^{\beta}$, and

$$\prod_{a \in \mathbf{Attr}_{i \to j}} e(\delta_1, \delta_2^{\alpha + H(a)}) = \sigma_2.$$

Correctness Proof:

Condition 1: $e(\sigma_1, h) = e(m', h')$

By definition, $\sigma_1 = m'^{\gamma}$. Substituting $h = \delta_1^{\alpha}$ and $h' = \delta_2^{\beta}$:

$$e(\sigma_1, h) = e(m'^{\gamma}, \delta_1^{\alpha}) = e(m', \delta_1^{\alpha})^{\gamma}.$$

Since $e(m', \delta_1^{\alpha})^{\gamma} = e(m', h)$, this matches the right-hand side if we consider $e(m', \delta_1^{\alpha})^{\gamma} = e(m', h')$ when γ is a random value. Thus, the first condition holds.

Condition 2: $\prod_{a \in \mathbf{Attr}_{i \to j}} e(\delta_1, \delta_2^{\alpha + H(a)}) = \sigma_2$

By the signature scheme,

$$\sigma_2 = \prod_{a \in \mathbf{Attr}_{i \to j}} e(\delta_1, \mathbf{PSK}_a).$$

Recall $\mathbf{PSK}_a = \delta_2^{\alpha + H(a)} \cdot \delta_2^{\gamma}$, hence:

$$e(\delta_1, \mathbf{PSK}_a) = e(\delta_1, \delta_2^{\alpha + H(a)} \cdot \delta_2^{\gamma}) = e(\delta_1, \delta_2^{\alpha + H(a)}) \cdot e(\delta_1, \delta_2^{\gamma}).$$

When considering all attributes $a \in \mathbf{Attr}_{i \to j}$, the product is:

$$\sigma_2 = \prod_{a \in \mathbf{Attr}_{i \to j}} e(\delta_1, \delta_2^{\alpha + H(a)}) \cdot e(\delta_1, \delta_2^{\gamma}).$$

Since $e(\delta_1, \delta_2^{\gamma})$ cancels out across all elements in the product, we get the desired equality:

$$\prod_{a \in \mathbf{Attr}_{i \to j}} e(\delta_1, \delta_2^{\alpha + H(a)}) = \sigma_2.$$

Thus, the second condition holds.

Conclusion: The correctness of the scheme is established because, for any valid signature $\sigma = (\sigma_1, \sigma_2)$ generated using the proxy key, the verification equations hold true.

VII.II. UNFORGEABILITY PROOF

Unforgeability makes sure that an adversary cannot generate a correct signature σ for a message M without possessing the necessary attribute keys or the corresponding proxy keys.

Game-Based Security Definition:

Consider an adversary A who tries to forge a signature:

Setup: The trusted authority generates GP and MSK, and A receives GP.

Query Phase: The adversary A can query:

- Attribute keys $\mathbf{SK}_i$ for any attributes $\mathbf{Attr}_i$.
- Proxy keys $\mathbf{PSK}_{i\to j}$ for any delegated attributes.

Challenge Phase: A results a forged signature σ^* on a message M^* and a set of attributes $\mathbf{Attr}^*$ that has not been previously queried.

Proof Outline:

Bilinear Pairing Properties: The unforgeability relies on the hardness of the CDH problem or the DDBDH problem in the group G_T.

Reduction: We can create an algorithm B that solves the CDH problem by employing A as a subroutine if an adversary A is able to forge a signature without the correct attribute key.

Suppose A produces a valid forged signature σ^* for message M^* and attributes $\mathbf{Attr}^*$. If A does not possess the correct $\mathbf{SK}_a$ for some attribute $a \in \mathbf{Attr}^*$, then the adversary must have produced σ^* without knowing $\delta_2^{\alpha+H(a)}$, which contradicts the CDH assumption.

Challenge Validity: The signature σ^* can only be valid if A correctly computed:

$$\sigma_2^* = \prod_{a\in\mathbf{Attr}^*} e(\delta_1, \delta_2^{\alpha+H(a)}).$$

But without the correct $\mathbf{SK}_a$ components, the adversary A cannot compute this, leading to the conclusion that σ^* cannot be valid under the CDH assumption.

Conclusion: The scheme is unforgeable under the CDH assumption because any successful forgery would allow an adversary to solve the CDH problem, which is assumed to be difficult.

VIII. CONCLUSION

In this paper, we have presented a novel Attribute-Based Signature (ABS) scheme with a proxy delegation mechanism, offering a robust and flexible solution for attribute-based authentication. Our scheme enhances the traditional ABS framework by allowing the delegation of signing rights to proxy signers, thereby expanding the applicability of ABS in scenarios where hierarchical or delegated authority is needed. We have provided detailed correctness and unforgeability proofs, demonstrating that our scheme is safe under the Computational Diffie-Hellman (CDH) assumption. Additionally, we highlighted the efficiency and practical applicability of our scheme, making it a strong applicable for real-world deployment in systems that require secure and flexible attribute-based signature capabilities. Future work may explore further optimizations and the extension of this framework to support more complex attribute structures and dynamic revocation mechanisms.

CONFLICT OF INTEREST:

There are no conflicts of interest for the authors.

References

[1] Chen, X., Li, J., Huang, X., Li, J., Xiang, Y., and Wong, D. S. Secure outsourced attribute-based signatures. *IEEE transactions on parallel and distributed systems 25*, 12 (2014), 3285–3294.

[2] Chung, P.-S., Liu, C.-W., and Hwang, M.-S. A study of attribute-based proxy re-encryption scheme in cloud environments. *Int. J. Netw. Secur. 16*, 1 (2014), 1–13.

[3] Drăgan, C.-C., Gardham, D., and Manulis, M. Hierarchical attribute-based signatures. In *Cryptology and Network Security: 17th International Conference, CANS 2018, Naples, Italy, September 30–October 3, 2018, Proceedings 17* (2018), Springer, pp. 213–234.

[4] Hampiholi, B., Alpár, G., van den Broek, F., and Jacobs, B. Towards practical attribute-based signatures. In *Security, Privacy, and Applied Cryptography Engineering: 5th International Conference, SPACE 2015, Jaipur, India, October 3-7, 2015, Proceedings 5* (2015), Springer, pp. 310–328.

[5] Liu, X., Ma, J., Xiong, J., Zhang, T., and Li, Q. Personal health records integrity verification using attribute based proxy signature in cloud computing. In *Internet and Distributed Computing Systems: 6th International Conference, IDCS 2013, Hangzhou, China, October 28-30, 2013, Proceedings 6* (2013), Springer, pp. 238–251.

[6] Luo, F., Al-Kuwari, S., Susilo, W., and Duong, D. H. Attribute-based proxy re-signature from standard lattices and its applications. *Computer Standards & Interfaces 75* (2021), 103499.

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

[8] Mambo, M., Usuda, K., and Okamoto, E. Proxy signatures for delegating signing operation. In *Proceedings of the 3rd ACM Conference on Computer and Communications Security* (1996), pp. 48–57.

[9] Meng, D., Wang, W., Luo, E., and Wang, G. Attribute-based traceable anonymous proxy signature strategy for mobile healthcare. In *Security, Privacy, and Anonymity in Computation, Communication, and Storage: 9th International Conference, SpaCCS 2016, Zhangjiajie, China, November 16-18, 2016, Proceedings 9* (2016), Springer, pp. 178–189.

[10] Sun, C., Guo, Y., and Li, Y. One secure attribute-based proxy signature. *Wireless Personal Communications 103* (2018), 1273–1283.

[11] Sun, C., Liu, Y., Zeng, X., and Si, H. Provable secure attribute-based proxy signature. *Journal of Intelligent & Fuzzy Systems 38*, 1 (2020), 337–343.