Proceedings of the Jangjeon Mathematical Society
28 (2025), No. 4, pp. 777 – 789

www.jangjeon.or.kr
http://dx.doi.org/10.17777/pjms2025.28.4.029

A Lightweight Verify Revocable Attribute-Based Ring Signature Scheme

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

[1]Department of Mathematics, Chaudhary Charan Singh University, Meerut - 250004, Uttar Pradesh, India
[2]Department of Mathematics, C.L. Jain College, Firozabad - 283203, Uttar Pradesh, India

goelshivani998@gmail.com; mkgupta2k2@gmail.com; saryusiirohi@gmail.com

Abstract

Ring signatures allow a user to sign messages on behalf of a group, ensuring strong anonymity, while attribute-based signatures enable users to sign data based on predefined attributes without disclosing their identities. In this paper, we propose a Lightweight Verify Revocable Attribute-Based Ring Signature Scheme. Our scheme allows users to anonymously sign messages based on predefined attributes, with an attribute authority retaining the capability to revoke anonymity when required. The verification process offloads most computational tasks to the cloud server, significantly reducing the burden on verifiers. This server-aided verification approach enhances computational efficiency, making the scheme suitable for resource-constrained cloud end-users. Our proposed scheme not only ensures strong security guarantees but also achieves efficient and practical implementation, enhancing its overall performance and applicability.

2000 Mathematics Subject Classification: 68M10, 68P30
Keywords: Attribute-based signature; Revocability; Ring Signature; Server Aided verification
Submitted on 05 July 2024

1 Introduction

A ring signature is a form of digital signature enabling any member of a group to sign a message on behalf of the entire group without disclosing the actual signer's identity. This concept was introduced by Rivest, Shamir, and Tauman in 2001 [20]. Unlike traditional digital signatures, where the identity of the signer is known, ring signatures offer a form of anonymity and privacy, making it impossible to distinguish which member of the group created the signature. To ensure the security of

a cryptosystem with many users, an efficient revocation mechanism is essential to notify when a user's authorization has expired or when a secret key of the user has been compromised. The original secret key cannot be used to access confidential data or generate digital signatures once it has been revoked. The issue of revocation was initially explored within the framework of public key infrastructure (PKI), leading to the development and implementation of various revocation methods. To remove the dependency on PKI, Shamir[22] presented the concept of identity-based encryption (IBE), which was first realized by Boneh and Franklin[2] using bilinear pairing over elliptic curves. Additionally, Sahai and Waters[21] expanded the idea of IBE to attribute-based encryption (ABE) to facilitate fine-grained access control.A revocation mechanism is required in both IBE and ABE scenarios. An Attribute-Based Signature (ABS) is also a cryptographic method that enables individuals or entities to sign digital messages or documents based on a set of predefined attributes or conditions. Introduced to enhance privacy and fine-grained access control, ABS schemes allow a signer to prove that they possess certain attributes without disclosing their actual identity. This signature method is mainly useful in scenarios where both the authenticity of the message and the privacy of the signer are crucial. Maji et al. [17] was the first to introduce this concept. Identity-based signatures [22], in which a signer's identity is represented by a single string rather than a group of characteristics, are extended by ABS. Within ABS, an attribute-certification authority, sometimes referred to as the attribute authority, grants user a certificate for a collection of attributes. An attribute-based signature gives verifier the assurance that the message has been approved by a signer whose collection of attributes satisfies a (potentially) complicated predicate. ABS has a wide range of significant uses. For example, it facilitates the provision of fine-grained access control in anonymous authentication. But in most of the ABS schemes, the computations required by the verifier are intensive, leading to high calculation costs. Some ABS schemes necessitate a large number of pairings during the verification process and each pairing requires high cost. To address this issue, we present a server-aided verification criteria in our paper. In this approach, digital signatures are generated based on predefined attributes or conditions without revealing the signer's identity. During verification, a dedicated server assists the verifier by performing computational tasks, attribute validation, or access policy management. This collaboration significantly reduces the verifier's computational burden, ensuring efficient and secure validation of attribute-based signatures.

2 Related Work

Ring signatures [20] are a cryptographic technique that enables a user to sign a message on behalf of a group (or ring) of possible signers. The concept allows for the creation of a signature that is verifiable against a set of public keys without revealing which specific key (or member of the ring) was used to produce the signature. This provides strong anonymity for the actual signer, ensuring their identity remains concealed among the group. Zhang et al. [30] proposed the first identity-based ring signature (IBRS) scheme, allowing a user to generate a ring signature using only

the public identities (like email addresses) of other users in the ring. Baek et al. [1] developed another Identity based ring signature scheme with improved efficiency and security properties. Sahai et al. [21] extended identity based encryption to attribute based encryption by allowing encryption and decryption based on a set of attributes and policies rather than a single identity. Goyal et al. [8] introduced the first KP-ABE scheme where access policies are encoded into the user's private key, and the data is encrypted with a set of descriptive attributes. Then Maji et al. [17] introduced a basic attribute based signature scheme with attribute-based policies, enabling signers to prove possession of attributes without revealing their identity. Further, Li et al. [12] proposed one of the early attribute based ring signature scheme, combining the principles of ABS and ring signatures to achieve attribute-based ring anonymity. In an Attribute based ring signature scheme, a signer can create a ring signature using a set of attributes, and the signature proves that someone with the required attributes within a group has signed the message, but not who specifically. Further, many signature schemes [26, 27, 24, 6] developed Attribute based ring signature schemes with improved efficiency and security properties, addressing practical implementation challenges. Revocable Attribute-Based Ring Signatures (RABRS) extends the concept of Attribute-Based Ring Signatures (ABRS) by incorporating mechanisms for revoking attributes. It addresses the practical need for dynamic and flexible attribute management. Yang et al. [29] presentted a revocable attribute based ring signature technique. Where the attribute authority has the capacity to withdraw a signature's anonymity when needed, yet the data owner can sign messages with strong anonymity. Therefore, even if he is accountable for his signature, the true signer is still free to build a ring however he pleases. Further many related signature schemes[23, 16, 7, 14, 28, 33, 32, 4, 34, 25, 19, 13, 15, 28] came into existance related to revocability, ring signature and attribute based properties. But the primary challenge in the majority of existing ABS schemes is the significant computational overhead associated with the verification algorithm. This computational burden makes the existing schemes unsuitable for deployment on resource-constrained devices.

Motivation and Contribution

Ensuring privacy and accountability in resource-constrained environments, such as IoT and cloud systems, is a significant challenge. While ring signatures provide anonymity, they lack controlled revocation, and attribute-based signatures impose high computational costs. To address these limitations, we propose a Lightweight Verify Revocable Attribute-Based Ring Signature Scheme. Our scheme enables anonymous attribute-based signing with controlled anonymity revocation by an attribute authority. By leveraging server-aided verification, it reduces computational overhead, requiring only a single pairing operation for verification. The proposed scheme ensures strong security guarantees, practical implementation, and applicability in privacy-preserving systems like cloud computing and e-health.

Organization

Our paper is organised into the following sections, in the following order: In Section 3, we provide a concise introduction to relevant concepts and present related definitions, along with a table containing the notations used in the paper with their meanings. Section 4 includes the framework and the system architecture of our signature protocol. Section 5 details the step-by-step construction of our signature technique. In Section 6, we justify the correctness and security of our technique. Finally, in Section 7, we offer concluding remarks, summarizing the key findings and contributions presented in this article and lasts with the refrences.

3 Preliminaries

3.1 Bilinear Pairing

Assume K_1, K_2 are two groups under addition and K_T be the group under multiplication. Each group is of prime order $'q'$.
Consider a pairing $'e'$
$e : K_1 \times K_2 \rightarrow K_T$
that satisfies the following conditions:

1. Bilinearity:

Forall $L_1 \in K_1, L_2 \in K_2$ and $r, s \in Z_q$
We have

$$e(rL_1, sL_2) = e(L_1, L_2)^{rs} \tag{1}$$

Also

$$e(L_1, L_2L_3) = e(L_1, L_2)e(L_1, L_3) \tag{2}$$

2. Non-degeneracy:

For $L_1 \neq 0_{K_1}$ and $L_2 \neq 0_{K_2}, e(L_1, L_2) \neq 1_{K_T}$
The aforementioned bilinear property can be demonstrated through the following equalities:

$$e(rZ_1, sZ_2) = e(sZ_1, rZ_2) = e(rsZ_1, Z_2) = e(rZ_1, Z_2)^s = e(sZ_1, Z_2)^r = ... \tag{3}$$

is referred as bilinear pairing [31].
Here, We define a bilinear system as a tuple $(q, K_1, K_2, K_T, L_1, L_2, e)$.

3.2 Complexity Assumptions

3.2.1 Discrete Logarithm Problem (DLP):

Within the realm of cryptography, one of the fundamental problems is the Discrete Logarithm Problem (DLP). It is defined as follows: Consider a cyclic group K with a generator element k. For any element h in K, there exists an integer j such

that $k^j = h$. This integer j is referred to as the discrete logarithm (or simply the logarithm) of h with base k [18]. This can be written mathematically as $j = log_k h$. it is straightforward to compute h given k and j, determining j from k and h is considered computationally infeasible for sufficiently large groups, which is what provides the cryptographic strength.

3.2.2 Computational Diffie- Hellman (CDH):

To find the discrete logarithm in cyclic groups relates to the Computational Diffie-Hellman (CDH) hypothesis [10]. In a cyclic group K having order t, given (k, k^a, k^b) where k is a generator & $a, b \in \{0, 1, 2, \ldots, t-1\}$, the CDH assumption states that finding k^{ab} is computationally challenging.

3.2.3 Decisional Diffie- Hellman (DDH):

Given a certain group K and its elements (h, h^a, h^b, h^c) to determine whether $h^c = h^{ab}$ is called as DDH problem.

3.3 Notations

Table 1 has been created to clarify the notations used in our signature scheme's construction.

Table 1: Notations used in our construction

Notations	Meaning
γ	The security parameter.
W	The universe of attributes
K	A multiplicative cyclic group of order m
K_1, K_2	Two groups of prime orders p and q respectively
k	Generator of the group K
k_1	Generator of the group K_1
e	The bilinear pairing
$\mathcal{H}$	The hash function.
N	A message.

4 Framework and System Model

4.1 Framework

The following algorithms are included in our signature scheme:
Setup: In this algorithm, a security parameter γ is an input. Outputs are a public parameter PK & a master secret key MSK.
KeyGen: In this algorithm, MSK and attributes of the user are input and output is the signing key of that user.
Sign: In this algorithm, PK, signing key, the attributes of the user and a message are input & output is the signature.

Transform: In this algorithm, input is the signature and output is the transformed signature.
Server-aided verify: In this algorithm, input is the transformed signature and output is a token.
lightverify: In this algorithm, input are the token, PK and the predicate. Ouput is either 0 or 1 that is the validation of the original signature.
Revoke: In this algorithm, input is the attributes of all the users and output is the identity of the real signer.

4.2 System Architecture

Our signature protocol involves five key entities: the attribute authority, the data service provider, the data owner, the data user (or Verifier), & the cloud server, depicted as in Fig. 1.

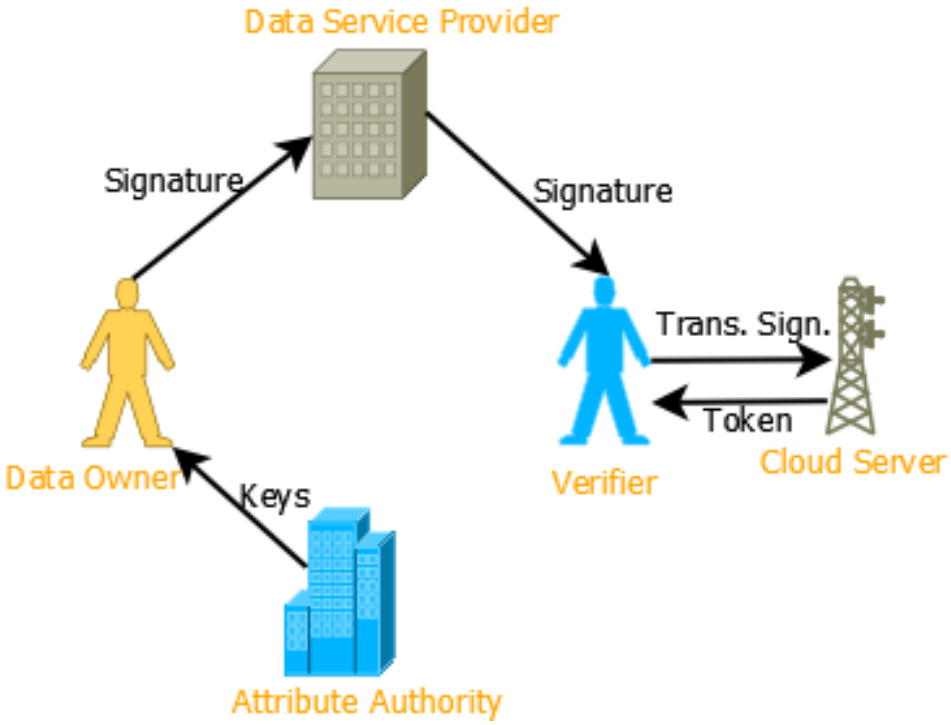

Figure 1: System architecture

The attribute authority generates security parameters & generates keys for the system. It assigns attributes to each user and handles user revocation. It has the capacity to determine the attributes of the original signer of any given signature. The data owner generates & shares data with all users in the ring, creating a digital signature for the data. This signed data is then sent to data service provider. The provider, equipped with sufficient storage and computational resources, offers

services such as data storage, sharing, and processing. The data user takes the data along with the signature from the provider. Using the cloud server, the user can verify if the signature was generated by the data owner whose attributes meet the signing policy. Verifier(data user) sends the transformed signature to the cloud server. Then cloud server sends back a token to the verifier. Using that token verifier easily verifies the original signature in lesser time.

5 Our Construction

Let γ be a security parameter & K be a multiplicative cyclic group having order $m = pq$, where p & q be two prime numbers. K_1 & K_2 are two subgroups of K having orders p & q respectively. $e : K \times K \to K$ be an eficient bilinear map.

5.1 Setup

Suppose $W = \{b_1, b_2, ..., b_j\}$ be the universal set of attributes. The attribute authority AA works in the following way:
$\mathcal{H} : \{0,1\}^* \to K$ is a hash function. k, k_1 be two random generators of K, K_1 respectively. Randomly choose $t \in Z_m$ and calculate $T = e(k,k)^t$.
Hence the master secret key MSK is t & public parameter PK is $\{k, k_1, T, \mathcal{H}, W\}$

5.2 KeyGen

Creating private key and signing key for the user having attribute set $\{b_{i_1}, b_{i_2}, ..., b_{i_n}\}$, $(1 \leq i_y \leq j)$, Suppose $A = b_{i_1} \parallel b_{i_2} \parallel ... \parallel b_{i_n}$, where $\parallel$ represents concatenation. AA randomly chooses $s \in Z_m$. Computing the private key $AK = \{k^t \mathcal{H}(A)^s, k_1^s$ for the user, $k^{b_{i_1} s}, k^{b_{i_2} s}, ..., k^{b_{i_n} s}\}$. Results k^s as public parameter. To create a message signature under an attribute subset $\{b_{l_1}, b_{l_2}, ..., b_{l_{n'}}\}$, $(1 \leq l_y \leq i_n)$ of the user's attribute set $\{b_{i_1}, b_{i_2}, ..., b_{i_n}\}$. Now, the user creates his signing key $SK = \{t_1, t_2\}$ as $t_1 = k^t \mathcal{H}(A)^s \prod_{y=1}^{n'} k^{b_{l_y} s}$ & $t_2 = k_1^s$.

5.3 Sign:

The user randomly chooses $r \in Z_m$ and computes his signature $\beta = \{\beta_1, \beta_2, \beta_3\}$ for the message $N \in \{0,1\}^*$ as

$$\beta_1 = k_1^r \mathcal{H}(A), \beta_2 = k^r, \beta_3 = t_1 \cdot t_2^r \cdot \mathcal{H}(N)^r \tag{4}$$

5.4 Transform

After getting the signature $\beta = \{\beta_1, \beta_2, \beta_3\}$, the verifier chooses $\alpha \in Z_p$ and $\theta \in [1, n]$, i.e; $1 \leq \theta \leq n$ and calculates $V = e(k,k)^\alpha$. Now the verifier computes the transformed signature $\breve{\beta} = \{\breve{\beta_1}, \breve{\beta_2}, \breve{\beta_3}\}$ as

$$\breve{\beta_1} = k_1^\alpha \prod_{y=1}^{n'} k^{b_{l_y}} \cdot \beta_1, \breve{\beta_2} = \beta_2, \breve{\beta_3} = \prod_{y=1, y \neq \theta}^{n'} k^{b_{l_y} s} k_1^{s\alpha} \cdot \beta_3 \tag{5}$$

Subsequently, the verifier transmits this modified signature $\beta = \{\breve{\beta}_1, \breve{\beta}_2, \breve{\beta}_3\}$ & the message N to the server.

5.5 Server-aided verify

As the server gets the transformed signature. It calculates a token $\breve{A}$ as

$$\frac{e(k, \breve{\beta}_3)}{e(k^s, \breve{\beta}_1 \prod_{y=1}^{n'} k^{b_{l_y}}) e(\breve{\beta}_2, \mathcal{H}(N))} = \breve{A} \tag{6}$$

The server sends this token $\breve{A}$ to the verifier.

5.6 lightverify

After getting the token from the server, verifier calculates

$$\breve{\breve{A}} = e(k^{\alpha} k^{b_{l_\theta}}, k)$$

Now, the verifiers checks the equation

$$\breve{A}\breve{\breve{A}} = V \cdot T \tag{7}$$

If this equation holds then the signature $\beta = \{\beta_1, \beta_2, \beta_3\}$ is true otherwise not.

5.7 Revoke

If the attribute authority has to disclose the signer's attribute identification, after the verification of signature he verifies the accuracy of $\beta_1^p = \mathcal{H}(A^{'})^p \ \forall$ the possible attribute identities $A^{'} \subset W$. if there exists any $A^{'}$ satisfying this equation then $A^{'} = A$ and in this way AA can get the identity of the real signer.

6 Security Analysis

6.1 Correctness

To check the equation 7

$$\breve{A}\breve{\breve{A}} = V \cdot T$$

Now,

$$
\begin{aligned}
\breve{A}\breve{\breve{A}} &= \frac{e(k,\breve{\beta}_3)}{e(k^s,\breve{\beta}_1\prod_{y=1}^{n'}k^{b_{l_y}})e(\breve{\beta}_2,\mathcal{H}(N))}\cdot e(k^\alpha k^{b_{l_\theta}},k)\\
&= \frac{e(k,\prod_{y=1,y\neq\theta}^{n'}k^{b_{l_y}s}k_1^{s\alpha}\cdot\beta_3)}{e(k^s,k_1^\alpha\prod_{y=1}^{n'}k^{b_{l_y}}\cdot\beta_1\prod_{y=1}^{n'}k^{b_{l_y}})e(\beta_2,\mathcal{H}(N))}\cdot e(k^\alpha k^{b_{l_\theta}},k)\\
&= \frac{e(k,\prod_{y=1,y\neq\theta}^{n'}k^{b_{l_y}s}k_1^{s\alpha}\cdot t_1\cdot t_2^r\cdot\mathcal{H}(N)^r)}{e(k^s,k_1^\alpha\prod_{y=1}^{n'}k^{b_{l_y}}\cdot k_1^r\mathcal{H}(A)\prod_{y=1}^{n'}k^{b_{l_y}})e(k^r,\mathcal{H}(N))}\cdot e(k^\alpha k^{b_{l_\theta}},k)\\
&= \frac{e(k,\prod_{y=1,y\neq\theta}^{n'}k^{b_{l_y}s}k_1^{s\alpha}\cdot k^t\mathcal{H}(A)^s\prod_{y=1}^{n'}k^{b_{l_y}s}\cdot k_1^{sr}\cdot\mathcal{H}(N)^r)}{e(k^s,k_1^\alpha\prod_{y=1}^{n'}k^{b_{l_y}}\cdot k_1^r\mathcal{H}(A)\prod_{y=1}^{n'}k^{b_{l_y}})e(k^r,\mathcal{H}(N))}\cdot e(k^\alpha k^{b_{l_\theta}},k)\\
&= \frac{e(k,\prod_{y=1,y\neq\theta}^{n'}k^{b_{l_y}s}k_1^{s\alpha}\cdot k^t\mathcal{H}(A)^s\prod_{y=1}^{n'}k^{b_{l_y}s}\cdot k_1^{sr})}{e(k^s,k_1^\alpha\prod_{y=1}^{n'}k^{b_{l_y}}\cdot k_1^r\mathcal{H}(A)\prod_{y=1}^{n'}k^{b_{l_y}})}\cdot e(k^\alpha k^{b_{l_\theta}},k)\\
&= \frac{e(k,\prod_{y=1,y\neq\theta}^{n'}k^{b_{l_y}s}k_1^{s\alpha}\cdot k^t\prod_{y=1}^{n'}k^{b_{l_y}s})}{e(k^s,k_1^\alpha\prod_{y=1}^{n'}k^{b_{l_y}}\prod_{y=1}^{n'}k^{b_{l_y}})}\cdot e(k^\alpha k^{b_{l_\theta}},k)\\
&= \frac{e(k,\prod_{y=1,y\neq\theta}^{n'}k^{b_{l_y}s}\cdot k^t)}{e(k^s,\prod_{y=1}^{n'}k^{b_{l_y}})}\cdot e(k^\alpha k^{b_{l_\theta}},k)\\
&= \frac{e(k,\prod_{y=1}^{n'}k^{b_{l_y}s}\cdot k^t)}{e(k^s,\prod_{y=1}^{n'}k^{b_{l_y}})}\cdot e(k^\alpha,k)\\
&= e(k,k)^\alpha\cdot e(k,k)^t\\
&= V\cdot T
\end{aligned}
$$

6.2 Server-aided verify

If the server is unreliable, it may attempt to manipulate the verification at the server end to convince the verifier that an incorrect signature is valid. However, it cannot follow in our protocol because, in our scheme the verifier first selects a random value α. He keeps it secretly and makes it impossible for the server to extract either α or $V = e(k,k)^\alpha$ from β. Consequently, the server cannot validate an incorrect signature. Even in scenarios where the server collaborates with an attacker, the server receives the transformed signature $\breve{\beta} = \{\breve{\beta}_1, \breve{\beta}_2, \breve{\beta}_3\}$ from the verifier and the original signature $\beta = \{\beta_1, \beta_2, \beta_3\}$ from the attacker. Despite this, the server still cannot find $e(k,k)^\alpha$ due to the absence of certain crucial information $k^\alpha k^{b_{l_\theta}}$. Therefore, our server-aided verification method remains fully secure within our signature scheme.

6.3 Collusion-Resistance

Collusion-resistance in attribute-based signatures ensures that any user cannot create a valid signature unless at least one user alone satisfies the signing policy based on the specified signature attributes. In our signature protocol, the attribute authority AA issues private key to users utilizing unique random numbers for each. Consequently, each user's private key is linked to a distinct number and makes any attempt at collusion among users unsuccessful.

6.4 Comparison Table

We compare our presented scheme in Table 2 with some existing signature schemes [9], [5], [3] and [11] with respect to access policy, server-aided verification property, Rrevocability, Ring signature feature, signature size and the number of pairings used in verification process.

Table 2: Comparision Chart

Papers	**Access**	**SAV**	**SAV-**	**Revocability**	**Ring Sign.**	**Sign. Size**	**Sign. Ver.**
[9]	monotone	×	×	×	×	$(k + t_{max} + 3)\|K\|$	$(k + 5)P$
[5]	LSSS	×	×	×	×	$(k + 3)\|K\|$	$(k + 3)P$
[3]	tree	✓	✓	×	×	(2 no. of att +2)$\|K\|$	$2P + EXP$
[11]	threshold	×	×	×	×	$6\|K\|$	4P
Our scheme	threshold	✓	✓	✓	✓	$3\|K\|$	P

7 Conclusion

We have proposed a Lightweight Verify Revocable Attribute-Based Ring Signature Scheme. Our signature technique allows for anonymous message signing based on predefined attributes while enabling an attribute authority to revoke anonymity when necessary. The incorporation of server-aided verification reduces the computational burden on verifiers as it requires less number of parings. Each pairing consumes high cost. In our scheme only single pairing is used for verification as the maximum computations are done by the cloud server. This feature makes our signature scheme ideal for resource-constrained environments, ensuring efficiency and practicality. our signature scheme enhances performance and applicability in privacy-preserving systems.

In the future, we plan to optimize our scheme by exploring batch verification to further reduce computational costs. We aim to enhance revocation mechanisms using decentralized attribute management and blockchain technology. Extending the scheme to multi-authority environments and conducting security analysis against quantum threats are also key directions. These efforts will ensure scalability, robustness, and applicability across diverse domains.

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.

References

[1] Baek, J., Safavi-Naini, R., and Susilo, W. On the integration of public key data encryption and public key encryption with keyword search. In *Information Security: 9th International Conference, ISC 2006, Samos Island, Greece, August 30-September 2, 2006. Proceedings 9* (2006), Springer, pp. 217–232.

[2] Boneh, D., and Franklin, M. Identity-based encryption from the weil pairing. In *Annual international cryptology conference* (2001), Springer, pp. 213–229.

[3] Chen, Y., Li, J., Liu, C., Han, J., Zhang, Y., and Yi, P. Efficient attribute based server-aided verification signature. *IEEE Transactions on Services Computing 15*, 6 (2021), 3224–3232.

[4] Delerablée, C., Gouriou, L., and Pointcheval, D. Attribute-based signatures with advanced delegation, and tracing. In *Cryptographers' Track at the RSA Conference* (2024), Springer, pp. 224–248.

[5] Ding, S., Zhao, Y., and Liu, Y. Efficient traceable attribute-based signature. In *2014 IEEE 13th international conference on trust, security and privacy in computing and communications* (2014), IEEE, pp. 582–589.

[6] Escala, A., Herranz, J., and Morillo, P. Revocable attribute-based signatures with adaptive security in the standard model. In *Progress in Cryptology–AFRICACRYPT 2011: 4th International Conference on Cryptology in Africa, Dakar, Senegal, July 5-7, 2011. Proceedings 4* (2011), Springer, pp. 224–241.

[7] Gardham, D., and Manulis, M. Revocable hierarchical attribute-based signatures from lattices. In *International Conference on Applied Cryptography and Network Security* (2022), Springer, pp. 459–479.

[8] Goyal, V., Pandey, O., Sahai, A., and Waters, B. Attribute-based encryption for fine-grained access control of encrypted data. In *Proceedings of the 13th ACM conference on Computer and communications security* (2006), pp. 89–98.

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

[10] Hellman, M. New directions in cryptography. *IEEE transactions on Information Theory 22*, 6 (1976), 644–654.

[11] Kang, Z., Li, J., Shen, J., Han, J., Zuo, Y., and Zhang, Y. Tfs-abs: Traceable and forward-secure attribute-based signature scheme with constant-size. *IEEE Transactions on Knowledge and Data Engineering 35*, 9 (2023), 9514–9530.

[12] Li, J., and Kim, K. Attribute-based ring signatures. *Cryptology ePrint Archive* (2008).

[13] Li, X., Yang, G., Xiang, T., Xu, S., Zhao, B., Pang, H., and Deng, R. H. Make revocation cheaper: Hardware-based revocable attribute-based encryption. In *2024 IEEE Symposium on Security and Privacy (SP)* (2024), IEEE Computer Society, pp. 100–100.

[14] Ling, S., Nguyen, K., Phan, D. H., Tang, K. H., Wang, H., and Xu, Y. Fully dynamic attribute-based signatures for circuits from codes. In *IACR International Conference on Public-Key Cryptography* (2024), Springer, pp. 37–73.

[15] Liu, L., Hsu, C., Au, M. H., Harn, L., Cui, J., and Zhao, Z. A revocable and comparable attribute-based signature scheme from lattices for iomt. *Journal of Systems Architecture 154* (2024), 103222.

[16] Lu, A., Li, W., Yao, Y., and Yu, N. Tcabrs: An efficient traceable constant-size attribute-based ring signature scheme for electronic health record system. In *2021 IEEE Sixth International Conference on Data Science in Cyberspace (DSC)* (2021), IEEE, pp. 106–113.

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

[18] Mir, U. H., Lone, P. N., Singh, D., and Mishra, D. A public and private key image encryption by modified approach of vigener cipher and the chaotic maps. *The Imaging Science Journal 71*, 1 (2023), 82–96.

[19] RAJU, Y. S., et al. Revocable attribute-based data storage in mobile clouds. *International Journal of Engineering Research and Science & Technology 20*, 2 (2024), 672–681.

[20] Rivest, R. L., Shamir, A., and Tauman, Y. How to leak a secret. In *Advances in Cryptology—ASIACRYPT 2001: 7th International Conference on the Theory and Application of Cryptology and Information Security Gold Coast, Australia, December 9–13, 2001 Proceedings 7* (2001), Springer, pp. 552–565.

[21] Sahai, A., and Waters, B. Fuzzy identity-based encryption. In *Advances in Cryptology–EUROCRYPT 2005: 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Aarhus, Denmark, May 22-26, 2005. Proceedings 24* (2005), Springer, pp. 457–473.

[22] Shamir, A. Identity-based cryptosystems and signature schemes. In *Advances in Cryptology: Proceedings of CRYPTO 84 4* (1985), Springer, pp. 47–53.

[23] Su, Q., Zhang, R., Xue, R., and Li, P. Revocable attribute-based signature for blockchain-based healthcare system. *IEEE Access 8* (2020), 127884–127896.

[24] Wang, C., Xu, X., Li, Y., and Shi, D. Integrating ciphertext-policy attribute-based encryption with identity-based ring signature to enhance security and privacy in wireless body area networks. In *Information Security and Cryptology: 10th International Conference, Inscrypt 2014, Beijing, China, December 13-15, 2014, Revised Selected Papers 10* (2015), Springer, pp. 424–442.

[25] Wang, N., Zhou, D., Huang, Y., and Liu, C. A traceable and revocable attribute-based encryption scheme with escrow-free in cloud storage. *Available at SSRN 4953959*.

[26] Wenqiang, W., and Shaozhen, C. An efficient attribute-based ring signature scheme. In *2009 International Forum on Computer Science-Technology and Applications* (2009), vol. 1, IEEE, pp. 147–150.

[27] Wenqiang, W., and Shaozhen, C. Attribute-based ring signature scheme with constant-size signature. *IET Information Security 4*, 2 (2010), 104–110.

[28] Xue, Q., Lu, Z., and Zhang, T. Attribute-based proxy signature scheme with dynamic strong forward security. *International Journal of Sensor Networks 44*, 4 (2024), 214–225.

[29] Yang, T., Yu, B., Wang, H., and Li, J. Revocable attribute-based ring signature scheme with constant size signature. In *2015 IEEE International Conference on Computer and Communications (ICCC)* (2015), IEEE, pp. 100–104.

[30] Zhang, F., and Kim, K. Id-based blind signature and ring signature from pairings. In *Advances in Cryptology—ASIACRYPT 2002: 8th International Conference on the Theory and Application of Cryptology and Information Security Queenstown, New Zealand, December 1–5, 2002 Proceedings 8* (2002), Springer, pp. 533–547.

[31] Zhang, F., Safavi-Naini, R., and Susilo, W. An efficient signature scheme from bilinear pairings and its applications. In *Public Key Cryptography–PKC 2004: 7th International Workshop on Theory and Practice in Public Key Cryptography, Singapore, March 1-4, 2004. Proceedings 7* (2004), Springer, pp. 277–290.

[32] Zhang, Y., Lei, H., Wang, B., Wang, Q., Lu, N., Shi, W., Chen, B., and Yue, Q. Traceable ring signature schemes based on sm2 digital signature algorithm and its applications in the data sharing scheme. *Frontiers of Computer Science 18*, 2 (2024), 182815.

[33] Zhang, Y., Zhao, J., Zhu, Z., Gong, J., and Chen, J. Registered attribute-based signature. In *IACR International Conference on Public-Key Cryptography* (2024), Springer, pp. 133–162.

[34] Zhu, C., Ding, J., Wei, X., Lu, Y., and Sun, Y. Efficient revocable attribute-based keyword search against keyword guessing attack. In *2024 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC)* (2024), IEEE, pp. 155–162.