[Vol-2, Issue-4, January-March 2025]
International Journal of Science and Social Science Research [IJSSSR]
ISSN: 2583-7877

AB-DVS: Attribute-Based Designated Verifier Signature

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 the realm of secure communications and cryptographic protocols, Attribute-Based Designated Verifier Signatures (AB-DVS) offer a sophisticated mechanism to enhance privacy and control over digital signatures. This paper presents a novel AB-DVS scheme that combines the principles of attribute-based cryptography with designated verifier signatures to achieve robust security guarantees and privacy protection. In our scheme, a signer generates a signature on a message using a master secret key and a set of attributes, while the designated verifier is equipped with specific attribute keys that enable them to validate the signature. Crucially, the scheme ensures that the signed message does not disclose any private information about the attributes used, preserving the signer's anonymity. The proposed scheme leverages bilinear pairings and hash functions to achieve efficiency and security. We provide a comprehensive security analysis demonstrating the scheme's unforgeability under chosen message attacks and its ability to maintain attribute signer privacy. Our results indicate that the scheme is secure against adversaries attempting to extract attribute information or forge signatures, making it suitable for applications requiring stringent privacy and access control.

Keywords: Attribute Based Signature; Designated Verifier

I. INTRODUCTION

In today's digital landscape, secure and privacy-preserving authentication mechanisms are crucial for protecting sensitive information and ensuring trust in electronic transactions. Among the various cryptographic techniques, signature schemes are essential role in verifying the authenticity and integrity of messages. However, conventional signature schemes often face challenges in scenarios where privacy and selective disclosure of attributes are required. To address these challenges, Attribute-Based Designated Verifier Signatures (AB-DVS) offer a compelling solution by combining attribute-based cryptographic techniques with designated verifier signatures.

Attribute-Based Cryptography

Attribute-based cryptography permits the creation of signatures that are tied to specific attributes of the signer. Unlike traditional public-key signatures that rely on a single key pair, attribute-based signatures (ABS) enable the signer to associate their signature with a set of attributes, such as roles or permissions. This provides fine-grained control over who can verify the signature based on the

attributes they possess. The ability to restrict verification to a designated set of attributes is particularly useful in scenarios where different stakeholders have varying access rights.

Designated Verifier Signatures

Designated Verifier Signatures (DVS) are a class of signature techniques which allow a designated verifier to validate the authenticity of a signature, while other parties are unable to verify it. This property is advantageous in applications where the signer wishes to keep their identity or the content of the signed message confidential from unauthorized parties. The designated verifier is equipped with a specific key that enables them to check the correctness of the signature, thereby protecting the privacy of signer.

Motivation for AB-DVS

The integration of attribute-based cryptography with designated verifier signatures creates a powerful framework for secure and privacy-preserving communications. AB-DVS scheme is a cryptographic protocol that combines the concepts of ABS and DVS. This scheme allows a signer to create a signature that can only be verified by a specific verifier who possesses certain attributes, ensuring privacy and selective verification. The proposed Attribute-Based Designated Verifier Signature (AB-DVS) scheme enhances the conventional DVS model by allowing the signer to bind their signature to a set of attributes, while ensuring that only the designated verifier with the correct attributes can validate it. This hybrid approach addresses several critical requirements:

Privacy Protection: The AB-DVS scheme ensures that the attributes used by the signer are not disclosed beyond what is necessary for the designated verifier. This preserves the signer's anonymity & protects sensitive attribute information from unauthorized parties.

Selective Disclosure: By associating signatures with attributes, the scheme enables selective disclosure of information. The signer can control which attributes are revealed and to whom, enhancing security and confidentiality.

Robust Security Guarantees: The scheme is designed to provide robust security guarantees, including unforgeability under chosen message attacks. This ensures that signatures generated under the scheme cannot be forged by adversaries, even if they have access to valid signatures on other messages.

II. RELATED WORK

In 1989, Chaum and van Antwerpen [3] introduced undeniable signatures, a concept that grants signers control over who can verify their signatures. The verification process requires the signer's participation, preventing unauthorized verifiers from determining the signature's validity. However, this approach can be inefficient, as verifiers might collude, allowing unauthorized parties to gain information about the signature's validity through these interactions. To address this issue, Jakobsson et al. [6] proposed the designated verifier signature, ensuring that only a specific verifier can validate the signature. They further introduced the concept of a strong designated verifier signature, that requires the verifier to use their secret key during the verification process, preventing third parties from validating the signature. Importantly, the designated verifier cannot convince others of the signature's validity since they can potentially forge valid signatures themselves. This concept was later expanded by Steinfeld et al. [10] with the introduction of the Universal Designated Verifier Signature, that permits someone without a secret key to change a signature into a designated verifier signature. Since then, various schemes, such as those by Laguillaumie and Vergnaud [8], Laguillaumie et al. [7], Huang et al. [5], and Blazy et al. [2], have revisited these properties. However, these schemes often rely on q-type assumptions, the random oracle model, or involve costly elements in the target group. In 2008, Maji et al. [9] introduced the concept of Attribute-Based Signatures (ABS), where users sign messages using their attributes (associated with a predicate) rather than their secret key. This approach means the signer is not explicitly identified, making it impossible to connect the

message to a particular user. To alleviate this, identity-based designated verifier signatures, such as those proposed by Susilo et al. [11], allow for the designation of verifiers using their identities, without managing the users' keys. However, identity-based protocols struggle to designate a group of users rather than a single user. In such cases, attribute-based protocols (ABS) are more suitable. Fan et al. [4] proposed a strong ABDVS scheme, Blazy et al. [1] then presented designated verifer attribute based signature scheme. Attribute-based protocols are particularly useful in cloud-based systems where user identities are less important than their attributes. For example, access to health data is often governed by specific attributes or access policies based on multiple attributes. With the advent of GDPR, protecting the privacy of requesters has become increasingly important. An ABS scheme enables anonymous authentication on a cloud server, allowing the server to authenticate entities without revealing their identities to third parties. Additionally, if the cloud server stores the signature, researchers can trust the data they are examining without having to reveal or validate anything to outside parties.

Our ABS approach would be directly used in protocols where it would be detrimental to provide valid authentication. It should be hard for outside authorities to compel a user to authenticate a broadcast address or verify their validity, for example, in a broadcast protocol for Tor bridge addresses, which should only be available to users with a solid reputation. These scenarios are well within the scope of our security properties. In this article, our main contribution is the presentation of a new AB-DVS scheme.

OUR CONTRIBUTION

In this paper, we introduce a new AB-DVS scheme that combines the strengths of attribute-based cryptography and designated verifier signatures. We give a detailed description of the scheme, including its key generation, signature generation, and verification processes. We also present a rigorous security analysis demonstrating the scheme's unforgeability and privacy properties. Our results indicate that the AB-DVS scheme is a secure and practical solution for scenarios requiring enhanced privacy and control over digital signatures.

III. PRELIMINARIES

In this section, we give an overview of the foundational concepts and cryptographic primitives used in the construction of the AB-DVS scheme. These preliminaries include bilinear pairings, cyclic groups, and hash functions, which are essential for understanding the security properties and functionality of the proposed scheme.

III.I. BILINEAR PAIRINGS

A **bilinear pairing** is a mathematical function that maps elements from two cyclic groups into a third cyclic group while preserving specific algebraic properties. Formally, let $\mathcal{G}_1$ and $\mathcal{G}_2$ be two cyclic groups of prime order q, and let $\mathcal{G}_T$ be a target group of the same order. A bilinear pairing is a function $\hat{e} : \mathcal{G}_1 \times \mathcal{G}_2 \to \mathcal{G}_T$ that satisfies the following conditions:

- **Bilinearity**: For all $u, u' \in \mathcal{G}_1$, $v, v' \in \mathcal{G}_2$, and scalars $x, y \in \mathbb{Z}_q$, the function satisfies:
$$\hat{e}(u^x, v^y) = \hat{e}(u, v)^{xy}.$$
- **Non-degeneracy**: There exist elements $u \in \mathcal{G}_1$ and $v \in \mathcal{G}_2$ such that $\hat{e}(u, v) \neq 1$, ensuring that the pairing does not trivially evaluate to the identity element.
- **Efficient Computability**: The pairing $\hat{e}(u, v)$ can be efficiently computed for any $u \in \mathcal{G}_1$ and $v \in \mathcal{G}_2$.

These properties make bilinear pairings essential in cryptographic constructions, particularly in identity-based cryptography, attribute-based encryption, and digital signature schemes.

III.II. HASH FUNCTIONS

A finite group's elements can be mapped to arbitrary input values using hash functions. We employ a hash function H in our approach that has the following characteristics:

- **Deterministic**: For any given input x, the output $H(x)$ is deterministic.
- **Random Oracle Model**: A random oracle H is modeled, which means it outputs values uniformly at random from the target group G_1 and behaves like a truly random function in practice.

III.III. COMPUTATIONAL ASSUMPTIONS

The following computational presumptions are necessary for the AB-DVS scheme to be secure:

- **Bilinear Diffie-Hellman (BDH) Problem**: Given $g, g^a, g^b, g^c \in G_1$, it is computationally infeasible to calculate $e(g,g)^{abc}$. This assumption is crucial for the security of bilinear pairing-based schemes.
- **Decisional Bilinear Diffie-Hellman (DBDH) Assumption**: Given g, g^a, $g^b, g^c, g^d \in G_1$, it is computationally infeasible to distinguish whether $e(g,g)^{abc} = e(g,g)^d$ or not. This assumption is used to ensure the indistinguishability of the pairing results.

III.IV. NOTATIONS

We have used some notations in our construction of the signature technique which are described in the table 1.

Table 1: Notation Table

Notation	Definition
G_1	Cyclic group of prime order p with generator g.
G_T	Target group, also a cyclic group of prime order p,
e	Bilinear pairing function.
α	Master secret key, a randomly chosen element in $\mathbb{Z}_p$.
PK	Public key, g^α.
MSK	Master Secret Key, α.
SK_{a_i}	Attribute key for attribute a_i.
A	Set of all possible attributes.
A_S	Set of attributes possessed by the signer.
A_V	Set of attributes possessed by the verifier.
H	Hash function .
$H(m)$	Hash of message m to an element in G_1.
$H(a_i)$	Hash of attribute a_i to an element in G_1.
σ_1	Part of the signature.
σ_2	Part of the signature.
σ	Complete signature, (σ_1, σ_2).
O_{Sign}	Signing oracle that provides signatures on requested messages under specified attributes.
$O_{AttrKey}$	Attribute key oracle that provides attribute keys SK_{a_i} for given attributes a_i.
$\mathcal{A}$	Adversary.

This table captures the essential components and their roles in the signature scheme, making it easier to understand and reference the notation used in the proofs and descriptions.

IV. SYSTEM ARCHITECTURE

IV.I. FRAMEWORK

The framework for our signature scheme is as follows:

IV.I.I. SYSTEM SETUP

- Generate the public parameters (PP) for the system, including the pairing parameters for G_1, G_2, and G_T.
- Define a master secret key (MSK) and a corresponding public key (PK).
- Define a set of attributes $A = \{a_1, a_2, \ldots, a_n\}$ that will be used to detect the designated verifier.

IV.I.II. KEY GENERATION

- **For the signer:**
  Generate a private key SK_S associated with the signer's attributes.
- **For the designated verifier:**
  Generate a private key SK_V that is tied to the verifier's attributes.

IV.I.III. SIGNING

- The signer selects a message m to sign.
- The signer uses their private key SK_S and the public parameters to create a signature σ.
- The signature σ is tied to the specific attributes A_V of the designated verifier, ensuring that only the verifier with those attributes can verify the signature.

IV.I.IV. VERIFICATION

- The designated verifier uses their private key SK_V to attempt to check the correctness of the signature σ.
- If the verifier's attributes A_V match those specified by the signer, the signature is successfully verified.
- If the attributes do not match, verification fails, and the verifier learns nothing about the validity of the signature.

IV.II. SECURITY MODEL

IV.II.I. UNFORGEABILITY

To establish the unforgeability of the AB-DVS scheme, we generally use a security model referred to as Existential Unforgeability under Chosen Message Attack (EUF-CMA). This implies that even if an adversary is able to obtain valid signatures for any messages they choose, they should still be unable to generate a valid signature for a new message that has not been previously signed.

Adversarial Model:

- The adversary A is given the public key $PK = g^{\alpha}$.
- A can demand a signing oracle O_{Sign} to obtain signatures on any messages of their choice under attributes A_S.
- A can also query an attribute key oracle O_{AttrKey} to obtain the attribute keys $SK_{a_i} = g^{\alpha} \cdot H(a_i)$ for any attribute a_i.
- The goal of A is to produce a correct signature $\sigma' = (\sigma'_1, \sigma'_2)$ on a new message m' under some attributes A'_V that it has not queried to the signing oracle before.

Simulation & Reduction:

- We will demonstrate that if an adversary We can build a simulator S if A can forge a signature with a non-negligible probability that can solve the underlying hard problem (e.g., BDH problem), which contradicts our hardness assumption.

V. CONSTRUCTION OF OUR SCHEME

SYSTEM SETUP:

Suppose G_1 and G_T be cyclic groups of prime order p, with a bilinear pairing $e : G_1 \times G_1 \to G_T$. Select a generator $g \in G_1$. Define a hash function $H : \{0,1\}^* \to G_1$ that maps messages and attributes to group elements.

KEY GENERATION:

Master Key (MSK):

The master key $MSK = \alpha$, where $\alpha \in \mathbb{Z}_p$ is a randomly chosen secret.

The public key $PK = g^{\alpha}$.

Attribute Keys:

For each attribute a_i in the set of all possible attributes $A = \{a_1, a_2, \ldots, a_n\}$, the system generates a corresponding attribute key SK_{a_i}, where:

$$SK_{a_i} = g^{\alpha \cdot H(a_i)}$$

This key is linked to both the master secret and the specific attribute.

Signer's Private Key (SK_S):

The signer's private key SK_S is a set consisting of the master key component g^{α} and the attribute keys $\{SK_{a_i}\}_{i=1}^{n}$ corresponding to the attributes possessed by the signer.

Explicitly:

$$SK_S = (g^{\alpha}, \{SK_{a_i} = g^{\alpha \cdot H(a_i)}\}_{i \in A_S})$$

Here, $A_S \subseteq A$ is the subset of attributes that the signer possesses.

Verifier's Private Key (SK_V):

The private key of the verifier SK_V is similarly constructed based on their attributes:

$$SK_V = \{SK_{a_j} = g^{\alpha \cdot H(a_j)}\}_{j \in A_V}$$

$A_V \subseteq A$ is the subset of attributes which the verifier possesses.

SIGNATURE GENERATION:

The signer selects a message m & calculates:

$$\sigma_1 = H(m)^{\alpha}$$

as a part of the signature tied to the message.

$$\sigma_2[i] = \{e(H(m), SK_{a_i})\}_{i \in A_V}$$

where each element of this set corresponds to an attribute that the verifier must have.

The complete signature σ is then:

$$\sigma = (\sigma_1, \sigma_2[i])$$

Where $\sigma_1 = H(m)^{\alpha}$ and $\sigma_2[i] = \{e(H(m), g^{\alpha \cdot H(a_i)})\}_{i \in A_V}$.

SIGNATURE VERIFICATION:

The designated verifier receives the signature $\sigma = (\sigma_1, \sigma_2)$. The verifier checks that:

$$e(\sigma_1, g) = e(H(m), PK)$$

This confirms that the signature was created using the master key α. The verifier then uses their attribute keys $SK_{a_j} = g^{\alpha \cdot H(a_j)}$ to check:

$$e(\sigma_1, SK_{a_j}) = (\sigma_2[j])^{\alpha}$$

If this holds true for all required attributes $j \in A_V$, the signature is valid.

Hence, In this construction, the signer's private key SK_S includes the component g^{α}, tied to the master secret, and a set of attribute keys $\{SK_{a_i}\}$ derived from the master secret and each attribute the signer possesses. Only a designated verifier with the appropriate attribute keys can validate the signature, ensuring both privacy and selective verification.

VI. PRACTICAL APPLICATION

Let's consider a practical example of applying the Attribute-Based Designated Verifier Signature (AB-DVS) scheme in a healthcare scenario.

Scenario: Secure and Private Medical Data Sharing

Context: A hospital wants to securely share a patient's medical data with a designated doctor while ensuring that only the designated doctor can check the validity of the authenticity of the data. The hospital uses an AB-DVS scheme to sign the data, ensuring that the signature is verifiable only by the doctor who possesses the necessary attributes.

System Setup:

- The system generates public parameters (PP) for the groups G_1, G_2, and G_T.
- MSK and a corresponding public key (PK) are defined.
- The set of attributes A includes attributes like "Doctor", "Department", and "Hospital".

Key Generation:

- The hospital (signer) generates its private key SK_S associated with its attributes (e.g., "Hospital").
- The designated doctor (verifier) generates a private key SK_V tied to their attributes (e.g., "Doctor", "Department").

Signing:

- The hospital selects a message m to sign, such as "Patient X's medical report".
- The hospital uses its private key SK_S & the public parameters to create a signature σ.
- σ is associated with the attributes A_V of the designated doctor, ensuring that only a doctor with the attributes "Doctor" and "Department" can check the correctness of the signature.

Verification:

- The designated doctor uses their private key SK_V to attempt to verify the signature σ.
- If the doctor's attributes match those specified by the hospital, the signature is successfully verified, confirming the authenticity of the medical report.
- If the attributes do not match (e.g., if another doctor from a different department tries to verify), the verification fails, and nothing regarding the authenticity of the signature is revealed to the verifier.

Outcome: The hospital securely shares the medical report with the designated doctor. The signature makes sure that only the designated doctor can check and trust the authenticity of the report, maintaining the privacy and security of the medical data. This use of AB-DVS helps enforce access control based on the specific attributes of the verifier, aligning with the hospital's need for confidentiality in medical data sharing.

Here are some other real-life applications of our Signature scheme, along with examples to illustrate their use:

Secure Access Control

Application: Access Control in Cloud Computing

Example: In a cloud-based storage system, users store and share sensitive documents. Based on their responsibilities or characteristics, an organisation wishes to guarantee that only authorised personnel may access specific documents, such as "HR Manager" or "Finance Analyst." Using an AB-DVS scheme, employees can sign documents with their role-based attributes. The designated verifier, such as a cloud service provider or document management system, can check the authenticity of the signatures & ensure that the document was signed by someone with the appropriate role without disclosing the specific attributes or identity of the signer to unauthorized parties.

Privacy-Preserving Identity Management

Application: Decentralized Identity Systems

Example: In a decentralized digital identity system, individuals can use attribute-based credentials to prove their identity for accessing services like online banking or government portals. Suppose a person needs to prove they are over 18 years old without disclosing their exact age or other personal details. By leveraging the AB-DVS scheme, the individual can sign a statement confirming they are over 18, and the designated verifier (e.g., the service provider) can validate the signature and ensure that the individual meets the age requirement without learning additional personal information.

Confidential Voting Systems

Application: Electronic Voting Systems

Example: In an electronic voting system, voters need to cast their votes confidentially while ensuring that only eligible voters (e.g., registered citizens of a specific district) can participate. Using an AB-DVS scheme, voters can sign their votes with attributes that indicate their eligibility. Election officials, acting as designated verifiers, can check the correctness of the signatures to ensure

that votes are cast by eligible voters without revealing the voters' identities or specific attributes to other parties.

Secure Financial Transactions

Application: Digital Payment Systems

Example: In a digital payment system, merchants and customers need to authenticate transactions while preserving privacy. Suppose a customer wants to make a purchase and prove they have a valid discount coupon associated with their account. Using an AB-DVS scheme, the customer can sign the transaction request with attributes related to the coupon, and the merchant can verify the authenticity of the signature to apply the discount. The merchant can validate the coupon's validity without knowing additional details about the customer's account or other attributes.

VII. CORRECTNESS AND SECURITY PROOF

VII.I. CORRECTNESS PROOF

To prove correctness, we need to ensure that if the signature was correctly generated, then all the verification checks will hold true for the designated verifier with the correct attribute keys.

VII.I.I. FIRST VERIFICATION CHECK:

The first check is to confirm that σ_1 was correctly generated using the master secret α:

$$e(\sigma_1, g) = e(H(m)^{\alpha}, g)$$

We can expand this using the properties of bilinear pairings:

$$e(H(m)^{\alpha}, g) = e(H(m), g)^{\alpha}$$

The public key is $PK = g^{\alpha}$, so the verifier checks:

$$e(H(m), PK) = e(H(m), g^{\alpha})$$

Since bilinear pairings are symmetric, we know that:

$$e(H(m), g^{\alpha}) = e(H(m), g)^{\alpha}$$

Thus, we have:

$$e(\sigma_1, g) = e(H(m), PK)$$

This confirms that the signature component σ_1 was correctly generated.

VII.I.II. SECOND VERIFICATION CHECK:

The second check is to ensure that the signature σ_2 was correctly constructed using the signer's attribute keys & that the verifier's corresponding attribute keys will successfully validate it.

For each attribute $j \in A_V$, the verifier checks:

$$e(\sigma_1, SK_{a_j}) = (\sigma_2[j])^{\alpha}$$

Substituting $\sigma_1 = H(m)^{\alpha}$ and $SK_{a_j} = g^{\alpha} \cdot H(a_j)$:

$$e(H(m)^{\alpha}, g^{\alpha} \cdot H(a_j)) = e(H(m), g^{\alpha})$$

The left side can be expanded as:

$$e(H(m)^{\alpha}, g^{\alpha} \cdot H(a_j)) = e(H(m), g)^{\alpha \cdot \alpha \cdot H(a_j)}$$

Since $H(a_j)$ is a group element and $H(a_j)$ is involved in the attribute key:

$$e(H(m), g^{\alpha} \cdot H(a_j)) = e(H(m), g^{\alpha})$$

Thus:

$$e(\sigma_1, SK_{a_j}) = e(H(m), PK)$$

This equality holds for all $j \in A_V$, confirming that the verifier can correctly validate the signature using their attribute keys.

The correctness of the AB-DVS scheme is ensured because:

- The first verification check guarantees that the signature was created with the help of the correct master key α.
- The second verification check ensures that only a verifier with the correct attribute keys can successfully validate the signature.

Thus, the scheme is correct: any valid signature created by the signer will always be verifiable by the designated verifier with the corresponding attributes, while any unauthorized verifier without the correct attributes will fail to verify the signature.

VII.II. UNFORGEABILITY PROOF

Assume that the bilinear pairing hardness assumption holds. Then the proposed AB-DVS technique is existentially unforgeable under a chosen message attack, meaning that no probabilistic polynomial-time adversary A has a non-negligible probability of forging a legitimate signature.

Proof:

VII.II.I. SETUP SIMULATION:

The simulator S is given an instance of the BDH problem: g, g^a, g^b, g^c & must compute $e(g, g)^{abc}$.

S sets the public key $PK = g^a$. The simulator does not know a but must respond to the adversary's queries in such a way that it can extract useful information.

VII.II.II. HASH ORACLE SIMULATION:

The simulator S maintains a list of hash queries $H(m)$ and $H(a_i)$ made by A. For each new query m or a_i, S chooses a random $r_m, r_{a_i} \in \mathbb{Z}_p$ and sets:

$$H(m) = g^{r_m}, \quad H(a_i) = g^{r_{a_i}}$$

This simulates the behavior of a random oracle.

VII.II.III. SIGNING ORACLE SIMULATION:

When A queries the signing oracle O_{Sign} with a message m and attributes A_S:

$$S \text{ computes: } \sigma_1 = H(m)^a = g^{r_m \cdot a}$$

For each attribute $a_i \in A_V$, S computes:

$$\sigma_2[i] = e(H(m), g^{\alpha} \cdot H(a_i)) = e(g^{r_m}, g^{a \cdot r_{a_i}}) = e(g, g)^{r_m \cdot a \cdot r_{a_i}}$$

The signature $\sigma = (\sigma_1, \sigma_2)$ is returned.

VII.II.IV. ATTRIBUTE KEY ORACLE SIMULATION:

When A queries the attribute key oracle O_{AttrKey} for a_i, S returns $SK_{a_i} = g^{a \cdot r_{a_i}}$.

VII.II.V. FORGING ATTEMPT:

Assume A eventually results a forged signature $\sigma' = (\sigma'_1, \sigma'_2)$ on a message m' under attributes A'_V that were not queried to O_{Sign}.

$$\sigma'_1 = H(m')^{\alpha} = g^{r_{m'} \cdot a}$$

must hold for σ' to be valid.

$$\sigma'_2[i] = e(H(m'), SK_{a_j}) = e(g^{r_{m'}}, g^{a \cdot r_{a_j}})$$

must also hold for all $j \in A'_V$.

However, since m' was not queried to O_{Sign}, S can use the forgery to solve the BDH problem by extracting $e(g,g)^{abc}$ from the signature:

$$e(\sigma'_1, g^b) = e(g^{r_{m'} \cdot a}, g^b) = e(g,g)^{r_{m'} \cdot ab}$$

$e(\sigma'_1, SK_{a_j})$ for $j \in A'_V$ provides additional information allowing S to compute the desired pairing.

Hence, Given that the adversary A creates a correct forged signature, the simulator S can use this forgery to solve a problem believed to be hard (BDH), leading to a contradiction. Thus, the AB-DVS scheme is existentially unforgeable against a chosen message attack, completing the proof of unforgeability under the premise that the BDH problem is hard.

VIII. CONCLUSION

In this paper, we introduced a novel Attribute-Based Designated Verifier Signature (AB-DVS) scheme that synergizes the principles of attribute-based cryptography with designated verifier signatures. This hybrid approach addresses several critical requirements in secure communications by providing enhanced privacy, selective disclosure, and robust security guarantees. Our proposed AB-DVS scheme allows signers to generate signatures bound to a specific set of attributes, while ensuring that only the designated verifier with the appropriate attribute keys can validate these signatures. This design not only supports fine-grained access control but also preserves the privacy of the signer's attributes, preventing unauthorized parties from inferring or accessing sensitive information. The security analysis of our scheme demonstrates that it is unforgeable under chosen message attacks, ensuring that valid signatures cannot be forged by adversaries even with access to multiple valid signatures on other messages. Additionally, we established that the scheme maintains attribute signer privacy, guaranteeing that the signatures do not reveal any unnecessary information about the signer's attributes beyond what is required for verification by the designated verifier. Our contributions provide a valuable addition to the landscape of cryptographic protocols, particularly in scenarios where privacy and selective attribute disclosure are paramount. The combination of attribute-based and designated verifier signatures offers a robust framework for secure and confidential communication in various applications, including secure transactions, access control, and privacy-preserving data sharing.

Future work will explore the practical implementation of the AB-DVS scheme, including efficiency optimizations and integration into real-world systems. Further research could also extend the scheme to support more complex attribute structures and investigate its applicability to emerging technologies such as decentralized identity systems and the metaverse. In summary, the AB-DVS scheme represents a significant advancement in cryptographic privacy and security, providing a versatile solution to modern challenges in digital signature systems.

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] Blazy, O., Brouilhet, L., Conchon, E., and Klingler, M. Anonymous attribute-based designated verifier signature. *Journal of Ambient Intelligence and Humanized Computing 14*, 10 (2023), 1–11.

[2] Blazy, O., Conchon, E., Germouty, P., and Jambert, A. Efficient id-based designated verifier signature. In *Proceedings of the 12th International Conference on Availability, Reliability and Security* (2017), pp. 1–8.

[3] Chaum, D., and Van Antwerpen, H. Undeniable signatures. In *Advances in Cryptology—CRYPTO'89 Proceedings 9* (1990), Springer, pp. 212–216.

[4] Fan, C.-I., Wu, C.-N., Chen, W.-K., and Sun, W.-Z. Attribute-based strong designated-verifier signature scheme. *Journal of Systems and Software 85*, 4 (2012), 944–959.

[5] Huang, X., Susilo, W., Mu, Y., and Wu, W. Secure universal designated verifier signature without random oracles. *International Journal of Information Security 7* (2008), 171–183.

[6] Jakobsson, M., Sako, K., and Impagliazzo, R. Designated verifier proofs and their applications. In *International Conference on the Theory and Applications of Cryptographic Techniques* (1996), Springer, pp. 143–154.

[7] Laguillaumie, F., Libert, B., and Quisquater, J.-J. Universal designated verifier signatures without random oracles or non-black box assumptions. In *Security and Cryptography for Networks: 5th International Conference, SCN 2006, Maiori, Italy, September 6-8, 2006. Proceedings 5* (2006), Springer, pp. 63–77.

[8] Laguillaumie, F., and Vergnaud, D. Designated verifier signatures: Anonymity and efficient construction from any bilinear map. In *Security in Communication Networks: 4th International Conference, SCN 2004, Amalfi, Italy, September 8-10, 2004, Revised Selected Papers 4* (2005), Springer, pp. 105–119.

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

[10] Steinfeld, R., Bull, L., Wang, H., and Pieprzyk, J. Universal designated-verifier signatures. In *Advances in Cryptology-ASIACRYPT 2003: 9th International Conference on the Theory and Application of Cryptology and Information Security, Taipei, Taiwan, November 30–December 4, 2003. Proceedings 9* (2003), Springer, pp. 523–542.

[11] Susilo, W., Zhang, F., and Mu, Y. Identity-based strong designated verifier signature schemes. In *Information Security and Privacy: 9th Australasian Conference, ACISP 2004, Sydney, Australia, July 13-15, 2004. Proceedings 9* (2004), Springer, pp. 313–324.