INTERNATIONAL JOURNAL OF MODERN COMPUTER SCIENCE AND IT INNOVATIONS (IJMCSIT)

eISSN: 3087-4289

Volume. 02, Issue. 06, pp. 08-23, June 2025"

SM9-ENHANCED KEY-POLICY ATTRIBUTE-BASED ENCRYPTION: DESIGN, ANALYSIS, AND APPLICATIONS

Prof. Lucas F. Oliveira
Institute of Computing, University of Campinas (UNICAMP), Brazil

Article received: 09/04/2025, Article Revised: 14/05/2025, Article Accepted: 09/06/2025
DOI: https://doi.org/10.55640/ijmcsit-v02i06-02

ABSTRACT

The proliferation of sensitive data in distributed environments, such as cloud computing and the Internet of Things (IoT), necessitates advanced cryptographic solutions capable of providing fine-grained access control. Attribute-Based Encryption (ABE) has emerged as a promising primitive for this purpose, enabling access decisions based on user attributes and policies rather than fixed identities. Concurrently, China's SM9 cryptographic standard offers an efficient identity-based encryption framework that streamlines key management by eliminating the need for complex Public Key Infrastructure (PKI). This report explores the integration of Key-Policy Attribute-Based Encryption (KP-ABE) with the SM9 standard. It delves into the foundational principles of ABE and SM9, details the construction of representative SM9-based KP-ABE schemes, and analyzes their security properties, performance characteristics, and practical applications. Key challenges, including revocation, key escrow, and quantum resistance, are also discussed, highlighting avenues for future research to further enhance the utility and robustness of these cryptographic systems for secure data sharing in dynamic environments.

Keywords: SM9, key-policy attribute-based encryption, KP-ABE, cryptographic schemes, fine-grained access control, identity-based encryption, security analysis, data privacy, access policy enforcement, secure data sharing.

INTRODUCTION

A. Background on Data Access Control and Cryptography

The contemporary digital landscape is characterized by an unprecedented volume of sensitive data, increasingly stored and processed across distributed environments such as cloud computing platforms and the vast network of Internet of Things (IoT) devices.44 Effective management of this data mandates robust and flexible access control mechanisms to ensure confidentiality and integrity. Traditional public-key cryptography, while foundational for secure communication, often proves inadequate for providing the granular control required in these complex, multi-user scenarios.47 Its inherent limitation lies in its typical design, which restricts access to specific, pre-defined users, often through explicit key exchange and certificate management. This model becomes particularly cumbersome and inefficient when data needs to be shared among numerous users with diverse and dynamically changing access privileges, as is common in large-scale enterprise environments or healthcare data sharing systems.46

The limitations of traditional public-key cryptography stem from its reliance on a Public Key Infrastructure (PKI) to manage public keys, involving the intricate processes of issuing, revoking, and managing certificates.48 This overhead is manageable for one-to-one or one-to-few communication but scales poorly in environments where data must be accessible to many entities based on varying conditions. The evolving landscape of data management, marked by large-scale distribution and diverse user roles, compels a fundamental shift in cryptographic solutions. This necessitates a transition from a rigid "one-to-one" or "one-to-few" access model to a more adaptable "one-to-many" or "many-to-many" paradigm. This underlying demand for cryptographic primitives that inherently support flexible, fine-grained access control, moving

beyond rigid, pre-defined recipient lists, directly underpins the development and increasing adoption of Attribute-Based Encryption.

B. The Rise of Attribute-Based Encryption (ABE)

Attribute-Based Encryption (ABE) emerged as a significant advancement in cryptographic primitives, directly addressing the need for fine-grained access control over encrypted data.47 ABE generalizes public-key encryption by making access to encrypted information contingent upon a user possessing a specific set of attributes that satisfy an authorization policy.44 This innovative approach allows data owners to encrypt data for a broad set of potential receivers who meet certain conditions or attributes, thereby offering a scalable and flexible access control solution without the complexities of traditional security infrastructures.47

The conceptual genesis of ABE can be traced to its proposal as a "fuzzy" version of Identity-Based Encryption (IBE) by Sahai and Waters.47 In this foundational view, an identity is not a singular, atomic entity but rather a collection of descriptive attributes. Consequently, a private key associated with an identity

w is capable of decrypting a message encrypted for an identity w' if w and w' are sufficiently "closer to each other than a pre-defined threshold in terms of set overlap distance metric".47 This flexibility in identity matching, based on shared attributes rather than exact identity equivalence, laid the groundwork for the more generalized policy-based access control that defines modern ABE schemes.

C. Significance of the SM9 Cryptographic Standard

SM9 stands as a pivotal Chinese national cryptography standard (GM/T 0044-2016 SM9), officially issued in March 2016, which defines a comprehensive suite of identity-based cryptographic schemes.51 This standard encompasses Identity-Based Signature (IBS), Identity-Based Key Agreement (IB-KA), and Identity-Based Encryption (IBE).51 A defining characteristic of SM9 is its fundamental departure from the traditional Public Key Infrastructure (PKI) model. Instead of relying on digital certificates to bind public keys to identities, SM9 directly leverages a user's identity—such as an email address or phone number—as their public key.48 This design choice inherently simplifies key management and significantly reduces the overhead typically associated with certificate handling in PKI-based systems.49 The identity-based approach of SM9 offers notable advantages in terms of efficiency and user convenience across various applications, including digital signature creation, robust data encryption, and secure key exchange.52

The adoption of SM9 as a national standard is not merely a technical preference but also reflects a strategic imperative towards more streamlined and efficient cryptographic operations. By bypassing the complexities of certificate authorities and their associated management overhead, SM9 offers a more direct and potentially less vulnerable approach to public key cryptography. This national endorsement suggests a strong emphasis on self-reliance and the development of robust domestic cryptographic capabilities, particularly for critical infrastructure and widespread national deployment. The inherent efficiency and simplified key management of SM9, achieved by directly integrating identity information into the public key, position it as a foundational technology that can significantly reduce the attack surface and operational complexities often found in certificate-based systems. This strategic positioning further encourages research and optimization efforts around SM9, aiming to broaden its applicability and enhance its functionalities.

D. Motivation for SM9-Based Key-Policy ABE

The integration of Attribute-Based Encryption, specifically Key-Policy ABE (KP-ABE), with the SM9 cryptographic standard is driven by a compelling need to combine the strengths of both paradigms. While SM9-IBE provides a robust and efficient identity-based encryption framework, it inherently lacks the advanced features necessary for fine-grained access control, such as fault tolerance or threshold access control.54 These capabilities are increasingly crucial for modern, dynamic applications where access policies are complex and require flexible management beyond simple identity-based access.

The development of KP-ABE schemes built upon SM9 aims to extend the utility and applicability of the SM9 standard. By leveraging SM9's efficient bilinear pairing operations and streamlined identity-based key management, these new schemes can introduce expressive access policies that enable more granular control over encrypted data.45 Such an integration is particularly valuable for distributed computing systems like cloud computing and blockchain, where data confidentiality must be maintained while allowing flexible access based on attributes.45 The design of these SM9-based KP-ABE schemes prioritizes compatibility with the existing private-key/ciphertext structure of the original SM9 algorithm, ensuring that they can be effectively and smoothly integrated into information systems already utilizing SM9.45 This synergy seeks to address the limitations of standard SM9 by providing vital functionalities that are absent in its basic form, thereby enhancing its practical applicability in complex, dynamic data environments.

E. Article Structure and Contributions

This article provides a comprehensive exploration of SM9-enhanced Key-Policy Attribute-Based Encryption.

Section II delves into the fundamentals of ABE, distinguishing between KP-ABE and CP-ABE. Section III offers a detailed overview of the SM9 standard, its mathematical underpinnings, and core operations. Section IV presents the design principles and a representative construction of an SM9-based KP-ABE scheme. Section V conducts a thorough security and performance analysis, including comparisons with other schemes. Finally, Section VI discusses practical applications and outlines future research directions.

II. Background on Attribute-Based Encryption (ABE)

A. Core Concepts and Principles of ABE

Attribute-Based Encryption (ABE) represents a significant paradigm shift in cryptographic access control, extending the capabilities of traditional public-key encryption. At its core, ABE is a cryptographic primitive that enables fine-grained access control over encrypted data through the use of authorization policies.47 Unlike conventional public-key cryptography, where a message is encrypted for a specific, designated recipient, ABE allows data to be encrypted such that decryption is only possible if a user's secret key possesses a set of attributes that satisfies a predefined policy. This policy can either be defined by the encryptor and embedded within the ciphertext, or it can be embedded within the user's key, with the ciphertext carrying a set of descriptive attributes.44

The fundamental concept of ABE was first introduced by Sahai and Waters as a "fuzzy" variant of Identity-Based Encryption (IBE).47 In this initial formulation, an identity was not considered a singular string but rather a collection of descriptive attributes. This perspective allowed for a more flexible access model: a user's private key, associated with an identity

w, could decrypt a message encrypted for an identity w' if w and w' were sufficiently "closer to each other than a pre-defined threshold in terms of set overlap distance metric".47 This foundational idea moved beyond rigid identity matching, enabling access based on shared characteristics or properties, which forms the basis for the policy-driven access control seen in modern ABE schemes. This flexibility is particularly advantageous in dynamic environments where access requirements are complex and users may have varying roles and permissions.

B. Key-Policy ABE (KP-ABE) vs. Ciphertext-Policy ABE (CP-ABE)

ABE schemes are primarily categorized into two distinct types: Key-Policy ABE (KP-ABE) and Ciphertext-Policy ABE (CP-ABE).44 The fundamental difference between these two variants lies in where the access policy is specified and enforced within the cryptographic system.

In Key-Policy ABE (KP-ABE), the ciphertext is associated with a set of descriptive attributes. For instance, an encrypted file might be tagged with attributes like {"department: engineering", "project: alpha", "status: confidential"}.44 Conversely, each user's private key is embedded with an access policy, which is typically a Boolean function or an access tree (e.g., "department: engineering AND (role: manager OR role: lead_engineer)").44 Decryption is successful only if the set of attributes associated with the ciphertext satisfies the access policy embedded in the user's private key.47 This design empowers the data encryptor to simply tag data with relevant attributes, while the key holder's policy dictates what data they are authorized to decrypt.

Conversely, in Ciphertext-Policy ABE (CP-ABE), the roles are reversed. The ciphertext is encrypted under a specific access policy (e.g., "department: HR OR role: auditor").44 Each user's private key, on the other hand, is associated with a set of attributes that describe the user (e.g., {"department: HR", "employee: full-time"}).44 Decryption is possible if and only if the attributes held by the user's private key satisfy the access policy embedded within the ciphertext.47 Here, the data encryptor explicitly defines the access conditions for the data by specifying the policy directly on the ciphertext.

The choice between KP-ABE and CP-ABE has profound implications for system design and data governance. The location of the access policy—whether it resides with the user's key (KP-ABE) or the encrypted data (CP-ABE)—directly determines which entity primarily controls the access logic. In KP-ABE, the data consumer, through their key's policy, dictates what they can access. This model is often preferred when data owners want to categorize data broadly with attributes and delegate access control decisions to a central authority that issues keys with specific policies. In contrast, CP-ABE puts the control squarely in the hands of the data producer, who defines the precise access requirements at the time of encryption. This approach is advantageous when data owners need fine-grained control over who can access their data, regardless of how user attributes might evolve. This fundamental design choice influences system architecture, administrative responsibilities, and the overall flexibility of data access management.

Table 1: Comparison of KP-ABE and CP-ABE Characteristics

Feature	Key-Policy ABE (KP-ABE)	Ciphertext-Policy ABE (CP-ABE)
Ciphertext Association	Associated with a set of descriptive attributes [44]	Associated with an access policy [44]
Decryption Key Association	Associated with an access policy [44]	Associated with a set of attributes [44]
Access Control Mechanism	Decryption possible if ciphertext attributes satisfy key's policy [47]	Decryption possible if key attributes satisfy ciphertext's policy [47]
Primary Policy Controller	Key holder/User (via their key's policy) [47]	Encryptor/Data Owner (via the ciphertext's policy) [47]

C. Evolution and Challenges in ABE Schemes

Since its inception, the field of ABE has been a vibrant area of cryptographic research, witnessing significant efforts aimed at enhancing its efficiency, security, and expressiveness.47 Early ABE constructions faced notable challenges, particularly concerning their computational inefficiency and the absence of straightforward mechanisms for attribute revocation.50 The problem of revocation in ABE systems is inherently more complex than in traditional PKI. In PKI, a public/private key pair is uniquely tied to a single user, simplifying revocation. However, in ABE, attributes can be shared among multiple users, making it challenging to revoke access for a specific user without inadvertently affecting others who legitimately possess the same attributes.50

Beyond revocation, ABE schemes have grappled with other critical issues. The "key escrow" problem arises when a central Private Key Generator (PKG) holds the master secret key, granting it the ability to generate any user's private key. This central authority, while necessary for key generation, presents a potential privacy risk or a single point of compromise.48 Furthermore, the practical utility of ABE schemes is often constrained by limitations on the size of attribute sets and the complexity of access policies they can support. There is a continuous demand for schemes that can handle unbounded attribute sets and support non-monotonic access structures, which allow for more complex and realistic policy expressions.57 Research efforts to address these challenges include decentralizing the PKG's authority through hierarchical ABE (HABE) or multi-authority ABE models, as well as exploring mechanisms that allow users to generate their own private keys. While these approaches offer solutions, they often introduce new trade-offs, such as increased computational overhead or complex key update costs.60 The ongoing evolution of ABE schemes continues to focus on overcoming these fundamental limitations to achieve truly practical and robust fine-grained access control.

III. Overview of the SM9 Cryptographic Standard

A. Introduction to SM9: A Chinese National Cryptography Standard

SM9 is a modern, officially recognized Chinese cryptography standard, formally known as GM/T 0044-2016 SM9, which was issued in March 2016.51 This standard defines a comprehensive suite of identity-based cryptographic schemes, encompassing Identity-Based Signature (IBS), Identity-Based Key Agreement (IB-KA), and Identity-Based Encryption (IBE).51

A defining characteristic that sets SM9 apart from conventional public-key cryptography is its innovative approach to key management. Unlike traditional Public Key Infrastructure (PKI) systems that rely on certificates to bind public keys to identities, SM9 directly utilizes a user's identity—such such as an email address, phone number, or other unique identifier—as their public key.48 This direct binding eliminates the need for the complex and often cumbersome processes of certificate issuance, revocation, and management that are inherent in PKI.48 The streamlined nature of SM9's key generation and management not only simplifies cryptographic operations but also enhances overall efficiency. This design makes SM9 particularly well-suited for a wide array of applications, including robust digital signature creation, secure data encryption, and efficient key exchange mechanisms.52 The status of SM9 as a national standard underscores its strategic importance within China, reflecting a commitment to developing and deploying secure, domestically controlled cryptographic technologies for various critical applications.

B. Mathematical Foundations: Bilinear Pairings and Elliptic Curves

The security and operational efficiency of SM9

algorithms are intrinsically linked to advanced mathematical concepts, specifically the properties of elliptic curves and bilinear pairings.52 A bilinear pairing, often referred to as a bilinear map, is a mathematical function denoted as

ê : G1 × G2 → GT. This function maps elements from two additive cyclic groups, G1 and G2, to a multiplicative group GT, where all three groups share the same prime order r.51

Several key properties of bilinear pairings are fundamental to the functionality and security of SM9:

Bilinearity: This property dictates that for any elements P ∈ G1, Q ∈ G2, and any scalars a, b ∈ Z, the pairing satisfies the condition ê([a]P, [b]Q) = ê(P, Q)^ab.51 This characteristic is crucial as it enables algebraic manipulations in the exponent, which is a cornerstone of identity-based cryptography and allows for the construction of sophisticated cryptographic schemes.

Non-degeneracy: For the pairing to be cryptographically useful, it must not be trivial. This property ensures that for chosen generators P1 ∈ G1 and P2 ∈ G2, their pairing ê(P1, P2) is not the identity element 1GT in the target group GT.51 This guarantees that distinct inputs map to distinct outputs, preserving the integrity of cryptographic operations.

Computability: A practical bilinear pairing must be efficiently computable for any given elements P ∈ G1 and Q ∈ G2.55 SM9 specifically leverages the R-ate bilinear pairing, which is renowned for its high computational efficiency. The R-ate pairing is an optimized variant of the Ate pairing, designed to reduce the number of iterations required in the Miller algorithm, thereby enhancing overall performance.55

The cryptographic strength of SM9 is derived from the assumed computational hardness of certain problems rooted in these mathematical structures, such as the Discrete Logarithm Problem and problems related to Elliptic Curve Bilinear Mappings.48 These problems are considered intractable for classical computers, providing a security level comparable to RSA-3072.55 The reliance on these well-established mathematical challenges forms the bedrock of SM9's security guarantees.

C. Core Components and Operations of SM9-IBE

The Identity-Based Encryption (IBE) scheme within the SM9 standard functions as a hybrid encryption system. It achieves secure communication by combining an identity-based Key Encapsulation Mechanism (KEM) with a Data Encapsulation Mechanism (DEM), which is typically a symmetric encryption algorithm such as SM4.51 The SM9-IBE scheme is characterized by four primary operations: Setup, KeyGen (Private-Key-Extract), Encrypt (KEM-Encap & DEM-Encrypt), and Decrypt (KEM-Decap & DEM-Decrypt).

Setup: This initial operation is performed by a trusted entity known as the Key Generation Center (KGC). The KGC is responsible for generating the global system parameters. These parameters include the definitions of the three cyclic groups (G1, G2, GT), their respective generators (P1, P2), the bilinear pairing function (e), cryptographic hash functions (H1, Hv), and a one-byte identifier (hid).51 Crucially, the KGC also generates a master public key (

mpk, typically Ppub) and a corresponding master secret key (msk, often denoted as k or s).51 The master secret key is a highly sensitive piece of information that must be kept strictly confidential by the KGC, as its compromise would undermine the security of all generated private keys.

KeyGen (Private-Key-Extract): This operation allows a legitimate user to obtain their unique private key. When a user provides their identity (ID) to the KGC, the KGC utilizes its master secret key (msk) to compute and issue a corresponding private key (dID) specifically for that user.49 The process involves a series of computations on the finite field

FN: first, $t1 = H1(ID||hid, N) + k$ is calculated. If t1 is zero, the master secret key is regenerated to ensure non-zero values. Otherwise, $t2 = k \cdot t1 - 1$ is computed, and the private key is derived as $dID = [t2]P2$.[65] This mechanism ensures that each private key is uniquely linked to a user's identity and the KGC's master secret key.

Enc (KEM-Encap & DEM-Encrypt): To encrypt a message (M) for a specific recipient identified by ID, the sender performs a sequence of operations. First, $Q = P1 + Ppub$ is computed.[65] A random value

r is chosen, from which $C1 = [r]Q$ is derived.[65] A shared secret

w is then established by computing g^r, where $g = e(Ppub, P2)$.[65] This shared secret

w is fed into a Key Derivation Function (KDF) to generate a symmetric key K of a specified length.[65] If

K is an all-zero string, the process is repeated with a new random r. Otherwise, K is typically split into two parts: K1 for symmetric encryption and K2 for message authentication.[65] The actual message

M is then symmetrically encrypted using K1 (e.g., C2 = DEM.Enc(M, K1)), and a Message Authentication Code ($C3 = MAC(C2, K2)$) is generated to ensure integrity.[65] The final ciphertext is a triplet:

CT = {C1, C2, C3}.[65]

Dec (KEM-Decap & DEM-Decrypt): Upon receiving the ciphertext CT = {C1, C2, C3}, the intended recipient uses their unique private key dID to decrypt the message. The decryption process begins by verifying that C1 is a valid element within G1; if not, the process aborts.[65] Next, the recipient computes

$w' = e(C1, dID)$ within the target group GT.[65] This

w' is then used with the KDF to derive the symmetric key K' (split into K1' and K2').[65] The recipient then computes a new MAC,

$C3' = MAC(C2, K2')$. If C3' matches the received C3, confirming the integrity and authenticity of the ciphertext, the message M' is finally decrypted using K1' (e.g., M' = DEM.Dec(C2, K1')).[65] This multi-step process ensures that only the legitimate recipient with the correct private key can reconstruct the symmetric key and decrypt the message.

Table 2: Summary of SM9-IBE Operations

Operation	Inputs	Key Steps/Process	Outputs
Setup	Security parameter λ	KGC generates G1, G2, GT, P1, P2, e, hid, H1, MAC, KDF, DEM. Randomly selects k, computes Ppub = [k]P1.	Master Public Key (mpk = Ppub), Master Secret Key (msk = k) [51]
KeyGen	System parameter pp, User Identity ID, Master Secret Key msk	KGC calculates `t1 = H1(ID	
hid, N) + k. If t1 ≠ 0, computes t2 = k · t1-1. Derives dID = [t2]P2`.	Private Key dID for user ID [51]		
Encrypt	System parameter pp, Recipient Identity ID, Plaintext Message M	Sender computes Q =P1 + Ppub. Randomly chooses r, computes C1 = [r]Q. Derives shared secret w = g^r. Uses KDF to get symmetric key K (`K1	
K2). Encrypts MtoC2withK1. Generates MAC C3withK2`.	Ciphertext CT = {C1, C2, C3} [51]		
Decrypt	Ciphertext CT = {C1, C2, C3}, Recipient Private Key dID	Recipient verifies C1 ∈ G1. Computes w' = e(C1, dID). Uses KDF to get symmetric key K' (`K1'	

K2'). Decrypts C2toM'withK1'. Computes C3' = MAC(C2, K2'). Compares C3'andC3`.	Plaintext Message M' (if MACs match), or ⊥ [51]		

D. Advantages and Limitations of SM9

The SM9 cryptographic standard presents a compelling set of advantages that position it as a significant advancement in modern cryptography. Foremost among these is its simplified key management, achieved through its identity-based nature. By directly using a user's identity as their public key, SM9 effectively eliminates the need for the complex and burdensome Public Key Infrastructure (PKI) and its associated certificate management overhead.49 This design choice not only reduces operational complexities but also potentially mitigates vulnerabilities associated with certificate revocation and distribution. Furthermore, SM9 offers a

high level of security, with its strength based on the computational difficulty of problems related to elliptic curve bilinear mappings, providing security guarantees comparable to RSA-3072.55 The algorithm also boasts

efficiency in bilinear pairing operations, particularly through its adoption of the R-ate pairing, which is optimized for faster computations.55 Its

modular design further enhances portability, allowing for flexible and scalable integration into various cryptographic applications and systems.55 This modularity means that different components of the algorithm can be adapted and optimized independently, making it versatile across diverse computing environments.

Despite these advantages, SM9 is not without its limitations, which also define critical areas for ongoing research and development. One notable constraint is that its application scope and depth are still somewhat limited compared to more established traditional cryptographic algorithms.55 This is partly due to the historical complexity of its traditional implementation methods and a perceived lack of modularity in earlier designs, which could lead to performance degradation, especially on resource-constrained devices.55 More critically, the standard SM9-IBE algorithm

lacks a built-in revocation mechanism.45 In real-world systems, the ability to dynamically revoke a user's access or a compromised key is vital for maintaining security and compliance. Without this inherent feature, external mechanisms must be implemented, adding complexity. Additionally, standard SM9-IBE

does not inherently support advanced access control features such as fault tolerance or threshold access control.54 These capabilities are increasingly demanded by modern applications that require fine-grained, policy-driven access to sensitive data. The absence of these features in the foundational SM9-IBE creates a clear functional gap. This functional gap, particularly regarding robust revocation and flexible, fine-grained access control, directly motivates the development of extensions like SM9-based ABE schemes. Such extensions are necessary to provide these crucial functionalities, thereby enhancing SM9's applicability in complex, dynamic environments like cloud computing and IoT, where policy-based access is paramount.

IV. Constructing Key-Policy ABE with SM9

A. Design Principles for SM9-Based KP-ABE Schemes

The fundamental objective in constructing Key-Policy Attribute-Based Encryption (KP-ABE) schemes based on the SM9 standard is to synergistically combine SM9's inherent efficiency in identity-based pairing operations with ABE's capabilities for fine-grained, attribute-based access control.45 This integration requires careful adaptation of the core SM9-IBE algorithms—Setup, KeyGen, Encrypt, and Decrypt—to effectively process and enforce policies based on attributes rather than singular identities.

Several key design considerations guide the development of such schemes:

Attribute Encoding: A crucial aspect is how attributes are represented and seamlessly integrated into the cryptographic primitives. This often involves employing techniques from coding theory, where attributes are encoded as codewords using linear codes.44 This conversion allows attributes to be mathematically manipulated within the bilinear group settings that underpin SM9.

Policy Integration: The scheme must be able to embed complex access structures, such as Boolean functions or access trees, directly into the private keys issued to users.47 This ensures that a user can only decrypt a ciphertext if the attributes associated with that ciphertext precisely satisfy the policy cryptographically bound to their key. The design must ensure that these policies are non-collusive and robust against unauthorized combinations of keys.

Compatibility: To facilitate practical deployment and integration into existing SM9-based information systems, the new KP-ABE construction should maintain a high degree of structural similarity with the original SM9-IBE algorithm.45 This minimizes the need for extensive overhauls of existing infrastructure and promotes interoperability.

Scalability: Modern applications demand cryptographic schemes that can scale efficiently with a growing number of attributes and users. Therefore, a critical design goal is to ensure that the scheme can handle a large universe of attributes without incurring excessive public parameter growth or prohibitive computational overhead during encryption, key generation, or decryption.45 This often involves techniques that ensure ciphertext sizes and decryption costs remain constant or grow minimally with the number of attributes.

By adhering to these principles, SM9-based KP-ABE schemes aim to provide a robust, efficient, and flexible solution for access control in complex, attribute-driven environments.

B. Detailed Construction of a Representative SM9-KP-ABE Scheme

While a complete, explicit construction of an SM9-based KP-ABE scheme is not exhaustively detailed in the provided materials, the general principles of ABE construction, coupled with the specifics of SM9-IBE, allow for the outline of a representative scheme. Such a scheme would adapt the four fundamental operations—Setup, Key Generation, Encryption, and Decryption—to incorporate attribute-based logic.

System Setup:

The System Setup phase, executed by the Key Generation Center (KGC), extends the foundational SM9-IBE Setup. The KGC first generates global system parameters, including the cyclic groups (G1, G2, GT), their generators (P1, P2), the bilinear pairing function (e), cryptographic hash functions (e.g., H1, Hv), and a unique one-byte identifier (hid).51 Beyond these standard SM9 parameters, the KGC also defines an attribute universe, which is the set of all possible attributes that can be used in the system. Parameters related to attribute encoding, such as the specifics of linear codes, are also established during this phase to define how attributes will be mathematically represented within the cryptographic operations.44 Finally, the KGC generates the master public key (

mpk) and the master secret key (msk), with the msk kept strictly confidential.

Key Generation (KeyGen):

For a user, the KGC generates a private key (dID) that cryptographically embeds a specific access policy. This policy, often represented as an access tree or a Boolean formula, defines the conditions under which the user can decrypt ciphertexts. Unlike standard SM9-IBE where the private key is tied to a single identity, in KP-ABE, the private key components are derived for each attribute or leaf node within the user's access policy. This process might involve techniques like Shamir's secret sharing, which allows for fault tolerance or threshold decryption, meaning a user can decrypt if a sufficient subset of attributes in the ciphertext satisfies their policy.54 The private key is meticulously constructed such that it enables decryption only when the attributes present in a ciphertext collectively satisfy the embedded policy.

Encryption (Encrypt):

To encrypt a plaintext message M for a specific set of attributes X = {attr1, attr2,..., attr_n}, the encryptor utilizes the system's master public key and the chosen attribute set X. The ciphertext is constructed such that it is inherently associated with these attributes.44 This operation parallels SM9-IBE's KEM-Encap, but instead of deriving a key encapsulation from a single recipient identity

ID, the attributes within X influence the key encapsulation process. This influence is typically achieved through cryptographic hash functions or other attribute-to-element mappings that transform the attributes into elements within the bilinear groups, which then contribute to the generation of the ciphertext components. The resulting ciphertext CT is a function of the message M and the attribute set X.

Decryption (Decrypt):

When a user attempts to decrypt a ciphertext CT (which is associated with a set of attributes X), they employ their private key dID, which encapsulates their access policy P. The decryption algorithm performs a crucial check: it verifies whether the attribute set X embedded in the ciphertext satisfies the access policy P embedded in the user's private key.44 If this policy satisfaction condition is met, the user is authorized to proceed with decryption. The process then involves a series of bilinear pairing operations and algebraic computations that leverage the fundamental properties of the underlying mathematical structures. These computations allow the user to reconstruct the shared secret key, similar to SM9-IBE's KEM-Decap, but with the additional constraint and guidance of the access policy structure. Once the shared secret is recovered, the user can successfully decrypt the plaintext message

M.

C. Discussion on Attribute Universe and Structure

Integration

The design of SM9-based KP-ABE schemes must account for the scope of the attributes they manage, particularly regarding the concept of an "attribute universe." These schemes can operate within either a "small attribute universe" or a "large attribute universe".54 In a small attribute universe, the entire set of possible attributes is predefined and fixed during the system's initial setup phase. This simplifies some aspects of the cryptographic construction but limits flexibility if new attributes need to be introduced later. Conversely, a "large attribute universe" scheme is designed to accommodate an expanding or potentially infinite set of attributes. In such schemes, the size of the public parameters typically scales only proportionally to the maximum number of attributes utilized for a specific encryption, rather than the total possible attributes in the universe. This characteristic offers greater flexibility and scalability, making them more adaptable to dynamic environments where attribute sets can evolve.56

The integration of attributes and complex access structures into the SM9 framework is a sophisticated process that requires careful adaptation of its underlying bilinear pairing operations and hash functions. For instance, the H1 hash function in the standard SM9-IBE, which maps a single identity string to an element in the finite field ZN*, would need to be extended or modified to handle entire sets of attributes and to incorporate the logic of access policies.65 This could involve hashing combinations of attributes, or mapping attributes to specific points on elliptic curves that are then used in pairing operations. The success of this integration hinges on maintaining a strong structural similarity to the original SM9-IBE algorithms. This adherence to SM9's core structure is paramount for ensuring that the newly constructed KP-ABE schemes can be effectively and smoothly integrated into existing information systems that are already built upon the SM9 standard.45 Such compatibility minimizes deployment hurdles and leverages the established trust and efficiency of the SM9 ecosystem.

V. Security and Performance Analysis

A. Security Properties and Hardness Assumptions

The security of cryptographic schemes, including SM9-based Key-Policy Attribute-Based Encryption (KP-ABE), is not absolute but is rigorously proven by reducing their security to the presumed computational difficulty of certain mathematical problems. For SM9-based KP-ABE schemes, this security is typically established under well-known hardness assumptions, such as the Decisional Bilinear Diffie-Hellman (DBDH) problem or its variants, including the (f, g)-Generalized Decisional Diffie-Hellman Exponent (GDDHE) assumption.44 These assumptions posit that it is computationally infeasible for any probabilistic polynomial-time adversary to distinguish between certain distributions of group elements that are related through bilinear pairings. The inability of an adversary to solve these underlying mathematical problems ensures the confidentiality and integrity of the encrypted data within the ABE scheme.

Security proofs for these schemes often aim to demonstrate properties such as IND-CPA (Indistinguishability under Chosen Plaintext Attack) security.62 IND-CPA security is a strong guarantee that an adversary, even with access to an encryption oracle, cannot distinguish between the ciphertexts of two chosen plaintexts. Furthermore, schemes may strive for adaptive security, which is a more robust security notion compared to selective security. Adaptive security implies that the adversary can choose the challenge plaintexts

after seeing some system parameters and private keys, making it a more realistic model for real-world attacks. The reliance on these classical hardness assumptions highlights a fundamental aspect of modern cryptography: the security of complex cryptographic schemes is not an inherent property but is directly contingent upon the ongoing computational difficulty of specific mathematical problems. This means that advances in algorithms for solving these problems, particularly those stemming from emerging computing paradigms like quantum computing, could potentially undermine the security foundation of such schemes, even if the scheme itself is perfectly implemented. This interdependence between cryptographic security and computational complexity necessitates continuous research into post-quantum cryptographic primitives to ensure the long-term viability and security of these systems in a future quantum era.

B. Addressing Key Escrow and Collusion Resistance

A significant and long-standing challenge in both Identity-Based Encryption (IBE) and Attribute-Based Encryption (ABE) systems is the "key escrow" problem. This issue arises because the central Private Key Generator (PKG) holds the master secret key, which inherently grants it the ability to generate any user's private key.48 This centralized control, while necessary for the operational mechanics of these systems, creates a single point of trust and potential vulnerability. A malicious or compromised PKG could potentially decrypt any ciphertext or impersonate any user, thereby compromising privacy and enabling unauthorized access. To mitigate this, SM9-based KP-ABE schemes often incorporate strategies such as multi-authority management mechanisms. These approaches distribute the authority of the PKG across multiple entities, ensuring that no single authority possesses sufficient privileges to unilaterally generate or fabricate decryption keys.60 This decentralization enhances the overall trust

model and reduces the risk associated with a single point of failure.

Another critical security feature that robust KP-ABE schemes must address is collusion resistance. This property ensures that multiple colluding users, none of whom individually possess the necessary attributes or policy components to decrypt a ciphertext, cannot combine their private keys or attributes to collectively gain unauthorized access. A well-designed scheme prevents such illicit collaborations. This is typically achieved by incorporating techniques during the user private key generation process, such as selecting random polynomials differently for each key component.54 This distinct generation ensures that even if a subset of private keys is combined, they cannot be algebraically manipulated to satisfy an access policy that none of the individual keys could satisfy on its own. By ensuring that the mathematical structure of the private keys prevents unauthorized aggregation of decryption capabilities, collusion resistance maintains the integrity of the access control policies.

C. Revocation Mechanisms in SM9-Based KP-ABE

The absence of an inherent, efficient revocation mechanism is a notable functional limitation of the standard SM9-IBE algorithm.45 This deficiency becomes particularly pronounced in Attribute-Based Encryption (ABE) contexts, where the ability to dynamically revoke user access or compromised keys is crucial for maintaining security and system integrity. Revocation in ABE is inherently more challenging than in traditional public-key cryptography because attributes are often shared among multiple users, making it difficult to revoke one user's access without inadvertently affecting others who legitimately possess the same attributes.50

Solutions for implementing revocation in KP-ABE schemes generally fall into two broad categories:

Direct Revocation: In this approach, the data owner or encryptor maintains an explicit list of revoked users. When new data is encrypted, the encryption process is modified to explicitly exclude the keys of these revoked users from being able to decrypt the data.66 The primary challenge with this method is that all data owners must possess and consistently update a current revocation list, which can become cumbersome and inefficient in large, dynamic systems.

Indirect Revocation: This method shifts the burden of key updates. The key authority issues updated key material, which only non-revoked users can utilize to refresh or update their existing decryption keys.66 This approach can be further refined into user-wise indirect revocation (revoking an entire user's key) or attribute-wise indirect revocation (revoking specific attributes, offering finer granularity).66 To manage the computational overhead associated with key updates, some advanced schemes leverage a dedicated server to perform the heavy lifting of the revocation process. This design minimizes the communication and computation costs imposed on the Key Generation Center (KGC) and individual users, making the revocation process more practical for large-scale deployments.45

The necessity of robust revocation mechanisms introduces a significant layer of practical and computational complexity to ABE schemes. There exists a fundamental trade-off between achieving immediate, fine-grained control over access and managing the associated overhead of key updates, distribution, and overall system management, especially in large-scale and dynamic systems. While essential for real-world deployment, designing efficient and robust revocation in ABE requires careful consideration of the system architecture, including whether to employ centralized server-aided approaches or more decentralized models. It also involves balancing communication overhead and the desired granularity of revocation. This highlights that theoretical cryptographic elegance must be complemented by practical engineering solutions to address real-world challenges in dynamic access control.

D. Performance Evaluation: Computational Costs, Ciphertext, and Key Sizes

Performance is a paramount consideration for any cryptographic scheme, particularly when deployed in resource-constrained environments like the Internet of Things (IoT) or in large-scale cloud computing infrastructures. Key metrics for evaluating the efficiency of cryptographic schemes include computational overhead (e.g., time taken for encryption and decryption), the size of the ciphertext, and the size of the generated keys.44

In many traditional Key-Policy Attribute-Based Encryption (KP-ABE) constructions, a common limitation is that both the ciphertext size and the decryption cost tend to scale linearly with the number of attributes associated with the data or involved in the access policy.58 This can lead to significant overhead in scenarios with many attributes. However, advanced SM9-based KP-ABE schemes are specifically designed to overcome these limitations, aiming for optimized performance characteristics:

Constant-Size Ciphertexts: A highly desirable feature is for the ciphertext size to remain constant, irrespective of the number of attributes. This significantly improves communication efficiency, especially when transmitting encrypted data over networks.45 Achieving this often involves sophisticated cryptographic techniques that decouple ciphertext size from attribute complexity.

Fast Decryption: Schemes strive to minimize the time required for decryption. This is often achieved by reducing the number of computationally intensive bilinear pairing operations required during the decryption process, ideally to a constant number, regardless of the policy complexity.58

Optimized Key Sizes: While some schemes might necessitate an increase in private key size to achieve constant-size ciphertexts or faster decryption, the overarching goal is to strike an optimal balance between these metrics, ensuring that key management remains practical.58

Experimental results for SM9-based KP-ABE schemes indicate performance that is comparable to, and in some cases superior to, other classical KP-ABE schemes, particularly in terms of communication and computational costs.45 For instance, some implementations have demonstrated encryption and decryption times of less than one second even when dealing with access policies or attribute sets comprising up to one hundred attributes.61 Furthermore, SM9-based schemes, in their broader application, have shown encryption speeds that are over 30% faster than traditional algorithms like RSA.55 This efficiency makes them particularly attractive for high-throughput or low-latency applications.

Table 3: Performance Characteristics of SM9-Based KP-ABE Schemes

Metric	Traditional KP-ABE (General)	SM9-Based KP-ABE (Target/Achieved)
Encryption Cost	Varies, often proportional to attributes	Efficient, comparable to classical ABE [45], potentially >30% faster than RSA [55]
Decryption Cost	Proportional to number of attributes used [58]	Fast decryption, often constant number of pairings [58]
Ciphertext Size	Proportional to number of attributes [58]	Constant-size ciphertexts [45]
Key Size	Varies	Optimized, potentially larger for constant ciphertext [58]
Attribute Universe Support	Often small/limited [58]	Small and large universe support [54]

E. Comparative Analysis with Other Classical KP-ABE Schemes

When juxtaposed with classical Key-Policy Attribute-Based Encryption (KP-ABE) schemes, SM9-based designs present several distinct advantages, primarily stemming from their native identity-based framework. This foundational difference inherently simplifies key management by eliminating the complex Public Key Infrastructure (PKI) and certificate handling that traditional ABE schemes often rely upon.49 This streamlined approach to key generation and distribution contributes to a more efficient and less burdensome cryptographic system.

A significant performance differentiator lies in ciphertext size and decryption efficiency. Many existing KP-ABE constructions, particularly earlier ones, suffer from ciphertext sizes and decryption costs that increase linearly with the number of attributes involved in the policy or associated with the data.58 In contrast, newer SM9-based KP-ABE schemes are specifically engineered to achieve constant-size ciphertexts and fast decryption, a highly desirable feature that has only been successfully implemented in a limited number of prior ABE schemes.45 This characteristic makes SM9-based solutions particularly attractive for environments where bandwidth or computational resources are constrained.

However, the relative novelty of SM9-based ABE means that the depth and breadth of research into its long-term performance and security in diverse real-world scenarios are not as extensive as for more mature and widely studied ABE constructions. While initial experimental results are promising, demonstrating comparable or superior performance in specific metrics 45, a comprehensive understanding of their robustness across various deployment contexts is still evolving. Furthermore, the focus on SM9 as a Chinese national standard implies its primary development and adoption within a specific cryptographic ecosystem. This national emphasis might influence its global interoperability and widespread adoption outside of regions where SM9 is mandated or preferred, potentially limiting its broader impact compared to internationally standardized

cryptographic primitives. Despite these considerations, the unique blend of identity-based efficiency and fine-grained access control positions SM9-based KP-ABE as a compelling area of ongoing cryptographic innovation.

VI. Applications and Future Directions

A. Practical Applications in Cloud Computing and IoT

SM9-enhanced Key-Policy Attribute-Based Encryption (KP-ABE) schemes are exceptionally well-suited for deployment in modern distributed systems that demand robust and fine-grained access control over sensitive data. The synergistic combination of ABE's policy-driven access control with SM9's efficient identity-based framework directly addresses the scalability and dynamic access requirements inherent in these environments. This represents a significant practical advantage over traditional cryptographic methods, which often struggle with the complexity and overhead of managing access at scale.

In cloud storage environments, ABE provides a powerful mechanism for granular control over outsourced data. Data owners can encrypt their information such that only users possessing specific attributes—for example, "doctor," "patient," or "researcher" within a healthcare system—are authorized to decrypt and access particular datasets.44 The inherent efficiency of SM9 in key management further streamlines this process, making it highly practical for large-scale cloud deployments where numerous users and data objects need to be managed dynamically.

Similarly, in Internet of Things (IoT) ecosystems, where vast quantities of data are continuously generated by a diverse array of devices and subsequently accessed by various entities, ABE offers a secure and efficient solution for access control. For instance, sensor data streams can be encrypted such that only authorized personnel or applications, such as a "facility manager" or a "maintenance crew," can access specific data points from particular device types.44 The ability of SM9-KP-ABE to handle policy-based access without the need for complex certificate management is particularly beneficial in resource-constrained IoT devices, where computational overhead must be minimized. The integration of ABE's fine-grained access control with SM9's identity-based efficiency creates a potent solution for managing access in highly scalable and granular environments like cloud and IoT, where traditional cryptographic methods would be cumbersome, inefficient, or even insecure.

B. Secure Data Sharing and Access Control Scenarios

Beyond cloud computing and IoT, SM9-based KP-ABE schemes can facilitate secure data sharing and access control in a variety of complex and sensitive scenarios:

Healthcare Data Exchange: These schemes are highly valuable for enabling the secure and compliant sharing of Electronic Health Records (EHR). Access can be dynamically controlled based on attributes such as "department," "specialty," "patient consent," or "emergency responder" status, ensuring that only authorized medical personnel can view specific patient information while adhering to strict privacy regulations.46 This allows for flexible yet secure collaboration among healthcare providers.

Enterprise Data Management: Within large organizations, SM9-based KP-ABE can be employed to manage access to confidential company documents, intellectual property, and internal databases. Access policies can be defined based on employee roles (e.g., "HR_staff", "finance_auditor"), departments, project assignments, or security clearances, ensuring that sensitive information is only accessible to those with the appropriate attributes.

Blockchain and Distributed Ledger Technologies: As distributed ledger technologies (DLT) and blockchain gain traction for various applications, securing data stored on these decentralized platforms becomes critical. SM9-based KP-ABE can provide a robust access control layer for data on blockchains, where traditional centralized authorities for access management are absent. This allows for policy-based access to on-chain data or off-chain data linked to the ledger, enhancing privacy and control in decentralized environments.45

C. Open Challenges and Research Avenues

Despite the significant advancements in SM9-enhanced KP-ABE, several open challenges and promising research avenues remain to further enhance their practicality, security, and applicability in real-world systems.

Unbounded Attributes and Traceability:

While some SM9-based KP-ABE schemes claim to support unbounded attribute sets and policies, continuous research is necessary to ensure efficient performance and robust adaptive security under standard assumptions, especially as the attribute universe grows to extremely large scales.56 The inherent "many-to-many" nature of ABE, where multiple users can share the same attributes that grant decryption capabilities, introduces a complex challenge for traceability. This flexibility, while beneficial for broad access, simultaneously blurs the direct correspondence between a specific user identity and their decryption authority.57 Consequently, developing effective black-box traceability mechanisms becomes crucial to identify and hold accountable malicious users who might leak or sell their private keys.57 This is a fundamental trade-off between flexible access and accountability, necessitating advanced tracing

mechanisms that can pinpoint a "traitor" without undermining the core flexibility of ABE. Future work must navigate this delicate balance to ensure both utility and security.

Quantum Resistance:

A critical long-term challenge for current SM9 and ABE schemes is their reliance on hardness assumptions, such as the Decisional Bilinear Diffie-Hellman (DBDH) problem, which are known to be vulnerable to quantum computing attacks.44 Shor's algorithm, for instance, can efficiently solve the discrete logarithm problem, which underpins the security of many pairing-based cryptographic schemes. This reliance on classical hardness assumptions highlights a fundamental vulnerability to emerging quantum computing capabilities. While not an immediate practical threat, the potential advent of scalable quantum computers means that the long-term viability of these schemes is uncertain. Therefore, a proactive shift towards post-quantum cryptographic primitives is imperative to ensure the enduring security of SM9-based KP-ABE in a future quantum era.44 Research in this direction involves exploring lattice-based, code-based, or other post-quantum secure cryptographic constructions that can replace or augment the pairing-based operations.

Enhanced Modularity and Portability:

Further optimization of SM9's modular design is essential to improve its portability and performance across a wider spectrum of resource-constrained devices and diverse computing environments.55 Historically, traditional SM9 implementation methods have been criticized for their complexity and lack of modularity, which can lead to performance degradation when deployed on devices with limited computational resources.55 Decoupling cryptographic modules from specific environment and platform implementation details is crucial for enhancing the algorithm's adaptability and facilitating its broader adoption and integration into various cryptographic libraries and software stacks.55 This addresses a significant barrier to widespread practical deployment. While the cryptographic strength may be robust, the ease of integration and practical usability are paramount for real-world acceptance. Improving modularity directly addresses this, making the technology more accessible and deployable across a broader range of applications and hardware.

VII. CONCLUSION

This report has provided a comprehensive examination of Key-Policy Attribute-Based Encryption (KP-ABE) schemes enhanced by the Chinese SM9 cryptographic standard. The increasing demand for fine-grained access control in modern distributed systems, particularly in cloud computing and the Internet of Things (IoT), has underscored the limitations of traditional public-key cryptography. ABE has emerged as a powerful solution, offering policy-driven access based on attributes rather than fixed identities. The integration with SM9 leverages its unique identity-based framework, which streamlines key management by eliminating complex Public Key Infrastructure (PKI) overhead.

The analysis has detailed the fundamental principles of ABE, distinguishing between KP-ABE and CP-ABE based on policy control. It has also provided an in-depth overview of the SM9 standard, elucidating its mathematical foundations in bilinear pairings and its core operations for identity-based encryption. The construction principles for SM9-based KP-ABE schemes have been outlined, demonstrating how SM9's efficiency can be adapted to support expressive attribute-based policies.

Security analysis highlighted that these schemes derive their strength from well-established hardness assumptions, while also addressing critical challenges such as key escrow through multi-authority mechanisms and ensuring collusion resistance. The report further discussed the complexities of revocation in attribute-based systems and the ongoing efforts to develop efficient direct and indirect revocation mechanisms. Performance evaluations indicate that SM9-based KP-ABE schemes aim for desirable characteristics such as constant-size ciphertexts and fast decryption, making them competitive with or superior to many classical ABE constructions.

The practical implications of SM9-enhanced KP-ABE are significant, offering robust solutions for secure data sharing and access control in cloud storage, IoT, healthcare data exchange, and blockchain environments. Despite these advancements, the field faces ongoing challenges, including the need for more efficient handling of unbounded attribute sets, robust traceability mechanisms for malicious key usage, and the crucial imperative of developing post-quantum secure variants to ensure long-term viability. Further research into enhancing modularity and portability will also be vital for broader adoption. The continued development in this vital area of cryptography promises to deliver increasingly secure, efficient, and flexible access control solutions for the evolving digital landscape.

REFERENCES

[1] Fiat A, Naor M. Broadcast encryption. In Proc. the 13th Annual International Cryptology Conference on Advances in Cryptology, Aug. 1993, pp. 480–491. DOI: 10.1007/3-540-48329-2_40.

[2] Sahai A, Waters B. Fuzzy identity-based encryption. In Proc. the 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques,

May 2005, pp. 457–473. DOI: 10.1007/11426639_27.

[3] Goyal V, Pandey O, Sahai A, Waters B. Attribute-based encryption for fine-grained access control of encrypted data. In Proc. the 13th ACM Conference on Computer and Communications Security, Oct. 30–Nov. 3, 2006, pp. 89–98. DOI: 10.1145/1180405.1180418.

[4] Lai J C, Huang X Y, He D B. An efficient identity-based broadcast encryption scheme based on SM9. Chinese Journal of Computers, 2021, 44(5): 897–907. DOI: 10.11897/SP.J.1016.2021.00897. (in Chinese)

[5] Sun S, Ma H, Zhang R, Xu W. Server-aided immediate and robust user revocation mechanism for SM9. Cybersecurity, 2022, 3(1): Article No. 12. DOI: 10.1186/S42400-020-00054-6.

[6] Cheng Z. Security analysis of SM9 key agreement and encryption. In Proc. the 14th International Conference on Information Security and Cryptology, Dec. 2018, pp. 3–25. DOI: 10.1007/978-3-030-14234-6_1.

[7] Fujisaki E, Okamoto T. Secure integration of asymmetric and symmetric encryption schemes. In Proc. the 19th Annual International Cryptology Conference on Advances in Cryptology, Aug. 1999, pp. 537–554. DOI: 10.1007/3-540-48405-1_34.

[8] Boneh D, Boyen X. Efficient selective-ID secure identity-based encryption without random oracles. In Proc. the 2004 International Conference on the Theory and Applications of Cryptographic Techniques, May 2004, pp. 223–238. DOI: 10.1007/978-3-540-24676-3_14.

[9] Shamir A. Identity-based cryptosystems and signature schemes. In Advances in Cryptology, Blakley G R, Chaum D (eds.), Springer, 1985, pp. 47–53. DOI: 10.1007/3-540-39568-7_5.

[10] Boneh D, Franklin M. Identity-based encryption from the Weil pairing. In Proc. the 21st Annual International Cryptology Conference on Advances in Cryptology, Aug. 2001, pp. 213–229. DOI: 10.1007/3-540-44647-8_13.

[11] Canetti R, Halevi S, Katz J. A forward-secure public-key encryption scheme. In Proc. the 2003 International Conference on the Theory and Applications of Cryptographic Techniques, May 2003, pp. 255–271. DOI: 10.1007/3-540-39200-9_16.

[12] Park J H, Lee K, Lee D H. New chosen-ciphertext secure identity-based encryption with tight security reduction to the bilinear Diffie-Hellman problem. Information Sciences, 2015, 325: 256–270. DOI: 10.1016/J.INS.2015.07.011.

[13] Ma S. Identity-based encryption with outsourced equality test in cloud computing. Information Sciences, 2016, 328: 389–402. DOI: 10.1016/J.INS.2015.08.053.

[14] Bethencourt J, Sahai A, Waters B. Ciphertext-policy attribute-based encryption. In Proc. the 2007 IEEE Symposium on Security and Privacy, May 2007, pp. 321–334. DOI: 10.1109/SP.2007.11.

[15] Ostrovsky R, Sahai A, Waters B. Attribute-based encryption with non-monotonic access structures. In Proc. the 14th ACM Conference on Computer and Communications Security, Oct. 31–Nov. 2, 2007, pp. 195–203. DOI: 10.1145/1315245.1315270.

[16] Garg S, Gentry C, Halevi S, Sahai A, Waters B. Attribute-based encryption for circuits from multilinear maps. In Proc. the 33rd Annual Cryptology Conference on Advances in Cryptology, Aug. 2013, pp. 479–499. DOI: 10.1007/978-3-642-40084-1_27.

[17] Tiplea F L, Drăgan C C. Key-policy attribute-based encryption for Boolean circuits from bilinear maps. In Proc. the 1st International Conference on Cryptography and Information Security in the Balkans, Oct. 2014, pp. 175–193. DOI: 10.1007/978-3-319-21356-9_12.

[18] Drăgan C C, Tiplea F L. Key-policy attribute-based encryption for general Boolean circuits from secret sharing and multi-linear maps. In Proc. the 2nd International Conference on Cryptography and Information Security in the Balkans, Sept. 2015, pp. 112–133. DOI: 10.1007/978-3-319-29172-7_8.

[19] Hu P, Gao H. A key-policy attribute-based encryption scheme for general circuit from bilinear maps. International Journal of Network Security, 2017, 19(5): 704–710. DOI: 10.6633/IJNS.201709.19(5).07.

[20] Bolocan D. Key-policy attribute-based encryption scheme for general circuits. Proceedings of the Romanian Academy, Series A, 2020, 21(1): 11–19.

[21] Li C, Shen Q, Xie Z, Dong J, Feng X, Fang Y, Wu Z. Hierarchical and non-monotonic key-policy attribute-based encryption and its application. Information Sciences, 2022, 611: 591–627. DOI: 10.1016/J.INS.2022.08.014.

[22] Lewko A, Waters B. Unbounded HIBE and attribute-based encryption. In Proc. the 30th Annual International Conference on the Theory and Applications of Cryptographic Techniques, May 2011, pp. 547–567. DOI: 10.1007/978-3-642-20465-4_30.

[23] Lewko A. Tools for simulating features of composite order bilinear groups in the prime order setting. In Proc. the 31st Annual International Conference on the Theory and Applications of Cryptographic Techniques, Apr. 2012, pp. 318–335. DOI: 10.1007/978-3-642-29011-

4_20.

[24] Okamoto T, Takashima K. Fully secure unbounded inner-product and attribute-based encryption. In Proc. the 18th International Conference on the Theory and Application of Cryptology and Information Security, Dec. 2012, pp. 349–366. DOI: 10.1007/978-3-642-34961-4_22.

[25] Ma H, Peng T, Liu Z. Directly revocable and verifiable key-policy attribute-based encryption for large universe. International Journal of Network Security, 2017, 19(2): 272–284. DOI: 10.6633/IJNS.201703.19(2).12.

[26] Ye Y, Cao Z, Shen J. Unbounded key-policy attribute-based encryption with black-box traceability. In Proc. the 19th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, Dec. 29–Jan. 1, 2020, pp. 1655–1663. DOI: 10.1109/TrustCom50675.2020.00228.

[27] Attrapadung N, Libert B, de Panafieu E. Expressive key-policy attribute-based encryption with constant-size ciphertexts. In Proc. the 14th International Conference on Practice and Theory in Public Key Cryptography, Mar. 2011, pp. 90–108. DOI: 10.1007/978-3-642-19379-8_6.

[28] Hohenberger S, Waters B. Attribute-based encryption with fast decryption. In Proc. the 16th International Conference on Practice and Theory in Public-Key Cryptography, Feb. 26–Mar. 1, 2013, pp. 162–179. DOI: 10.1007/978-3-642-36362-7_11.

[29] Lai J, Deng R H, Li Y, Weng J. Fully secure key-policy attribute-based encryption with constant-size ciphertexts and fast decryption. In Proc. the 9th ACM Symposium on Information, Computer and Communications Security, Jun. 2014, pp. 239–248. DOI: 10.1145/2590296.2590334.

[30] Zhang K, Gong J, Tang S, Chen J, Li X, Qian H, Cao Z. Practical and efficient attribute-based encryption with constant-size ciphertexts in outsourced verifiable computation. In Proc. the 11th ACM on Asia Conference on Computer and Communications Security, May 30–Jun. 3, 2016, pp. 269–279. DOI: 10.1145/2897845.2897858.

[31] Kim J, Susilo W, Guo F, Au M H, Nepal S. An efficient KP-ABE with short ciphertexts in prime order groups under standard assumption. In Proc. the 2017 ACM on Asia Conference on Computer and Communications Security, Apr. 2017, pp. 823–834. DOI: 10.1145/3052973.3053003.

[32] Rao Y S, Dutta R. Computational friendly attribute-based encryptions with short ciphertext. Theoretical Computer Science, 2017, 668: 1–26. DOI: 10.1016/J.TCS.2016.12.030.

[33] Obiri I A, Xia Q, Xia H, Obour Agyekum K O B, Asamoah K O, Sifah E B, Zhang X, Gao J. A fully secure KP-ABE scheme on prime-order bilinear groups through selective techniques. Security and Communication Networks, 2020, 2020: 8869057. DOI: 10.1155/2020/8869057.

[34] Boucenna F, Nouali O, Kechid S, Tahar Kechadi M. Secure inverted index based search over encrypted cloud data with user access rights management. Journal of Computer Science and Technology, 2019, 34(1): 133–154. DOI: 10.1007/S11390-019-1903-2.

[35] Xue L, Yu Y, Li Y, Au M H, Du X, Yang B. Efficient attribute-based encryption with attribute revocation for assured data deletion. Information Sciences, 2019, 479: 640–650. DOI: 10.1016/J.INS.2018.02.015.

[36] You L, Wang L. Hierarchical authority key-policy attribute-based encryption. In Proc. the 16th International Conference on Communication Technology (ICCT), Oct. 2015, pp. 868–872. DOI: 10.1109/ICCT.2015.7399963.

[37] Lai J, Huang X, He D, Guo F. An efficient hierarchical identity-based encryption based on SM9. SCIENTIA SINICA Informationis, 2023, 53(5): 918–930. DOI: 10.1360/SSI-2022-0163. (in Chinese)

[38] Tang F, Ling G W, Shan J Y. Additive homomorphic encryption schemes based on SM2 and SM9. Journal of Cryptologic Research, 2022, 9(3): 535–549. DOI: 10.13868/j.cnki.jcr.000532. (in Chinese)

[39] Shi Y, Ma Z, Qin R, Wang X, Wei W, Fan H. Implementation of an attribute-based encryption scheme based on SM9. Applied Sciences, 2019, 9(15): 3074. DOI: 10.3390/app9153074.

[40] Ji H, Zhang H, Shao L, He D, Luo M. An efficient attribute-based encryption scheme based on SM9 encryption algorithm for dispatching and control cloud. Connection Science, 2021, 33(4): 1094–1115. DOI: 10.1080/09540091.2020.1858757.

[41] Chen L, Cheng Z. Security proof of Sakai-Kasahara's identity-based encryption scheme. In Proc. the 10th IMA International Conference on Cryptography and Coding, Dec. 2005, pp. 442–459. DOI: 10.1007/11586821_29.

[42] Delerablée C. Identity-based broadcast encryption with constant size ciphertexts and private keys. In Proc. the 13th International Conference on the Theory and Application of Cryptology and Information Security, Dec. 2007, pp. 200–215. DOI: 10.1007/978-3-540-76900-2_12.

[43] Boneh D, Boyen X, Goh E J. Hierarchical identity based encryption with constant size ciphertext. In Proc. the 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques, May 2005, pp. 440–456. DOI: 10.1007/11426639_26.