Frontiers in Emerging Computer Science and Information Technology (Open Access)

Volume 02, Issue 09, September 2025,
Publish Date: 01-09-2025
PageNo.01-11

A Framework for SM9-Enhanced Key-Policy Attribute-Based Encryption: Design, Security, and Application

Dr. Wei Zhang
Department of Cybersecurity, Tsinghua University, Beijing, China

Prof. Alessandra Romano
Faculty of Computer Science, Sapienza University of Rome, Italy

Dr. Samuel J. Carter
Centre for Cryptography and Network Security, University of Edinburgh, United Kingdom

Dr. Liyana M. Hashim
School of Information Assurance, Universiti Teknologi Malaysia, Johor, Malaysia

ABSTRACT

Background: Attribute-Based Encryption (ABE) provides a powerful mechanism for enforcing fine-grained access control on encrypted data. Key-Policy ABE (KP-ABE) allows data to be encrypted with a set of attributes, where only users whose keys are associated with a policy that satisfies these attributes can decrypt. With the growing adoption of national cryptographic standards like SM9, there is a pressing need for efficient and secure KP-ABE schemes that are compatible with these frameworks.
Objective: This paper introduces a novel SM9-enhanced KP-ABE scheme designed to offer robust security and high performance while aligning with the SM9 standard. The primary goal is to address the limitations of existing schemes, such as computational inefficiency and large ciphertext overhead, providing a practical solution for secure data sharing environments.
Methods: We first establish the necessary cryptographic preliminaries, including bilinear pairings and the core mechanics of the SM9 encryption algorithm. We then formally define the system architecture and the security model for our scheme. The core of our methodology is the detailed construction of the four fundamental algorithms of our KP-ABE scheme: Setup, KeyGen, Encrypt, and Decrypt.
Results: A comprehensive analysis indicates the correctness of our proposed scheme. We provide a rigorous security proof, showing that our scheme is indistinguishable under chosen-plaintext attacks in the standard model. Furthermore, a comparative performance analysis suggests that our scheme is associated with significant advantages in terms of computational costs and ciphertext size when benchmarked against prominent existing KP-ABE schemes.
Conclusion: The proposed SM9-enhanced KP-ABE scheme represents a significant advancement in secure data access control. By successfully integrating with the SM9 standard and demonstrating superior performance, it offers a viable and efficient solution for a wide range of applications, including secure cloud storage, healthcare information systems, and the Internet of Things.

KEYWORDS: Attribute-Based Encryption (ABE), Key-Policy ABE (KP-ABE), SM9 Standard, Fine-Grained Access Control, Cloud Security, Provable Security, Bilinear Pairings.

INTRODUCTION

The proliferation of digital data and the rise of distributed computing paradigms, such as cloud computing and the Internet of Things (IoT), have fundamentally transformed the landscape of information management. While these technologies offer unprecedented convenience and scalability, they also introduce significant security and privacy challenges. A primary concern is the protection of sensitive data stored and shared on untrusted servers.

Traditional all-or-nothing access control models, which rely on pre-defined user roles, are often too rigid for the dynamic and complex sharing scenarios common in modern applications. This has spurred the development of advanced cryptographic primitives capable of enforcing fine-grained access control policies directly on encrypted data.

One of the most promising of these primitives is **Attribute-Based Encryption (ABE)**, a visionary concept introduced by Sahai and Waters [2]. ABE extends the idea of Identity-Based Encryption (IBE) [9, 10] by replacing the notion of a single identity with a more expressive set of descriptive attributes. In an ABE system, a user's keys and the ciphertexts are associated with attributes or policies defined over these attributes. A user can only decrypt a ciphertext if the attributes associated with their key satisfy the policy embedded within the ciphertext, or vice-versa. This paradigm allows data owners to specify complex access rules for their data without needing to know the specific identities of all potential users.

ABE schemes are generally categorized into two main types: Ciphertext-Policy ABE (CP-ABE) [14] and Key-Policy ABE (KP-ABE) [3]. In CP-ABE, an access policy is embedded into the ciphertext, and a user's private key is associated with a set of attributes. Decryption is possible only if the user's attributes satisfy the ciphertext's policy. This model is analogous to a "gatekeeper" on the data, making it intuitive for systems where the data owner dictates access. Conversely, in a KP-ABE scheme, the roles are reversed: the ciphertext is associated with a set of attributes, and the user's private key is linked to an access policy (or access structure). A user can decrypt a ciphertext if and only if the attributes of the ciphertext satisfy the policy encoded in their private key. This model is highly suitable for systems like sophisticated content filtering or targeted data dissemination, where the *user's authority* dictates what kind of data they can access. Several KP-ABE schemes have been proposed, supporting various access policies ranging from simple monotonic structures [3] to more expressive non-monotonic policies [15] and general circuits [16, 17, 18, 19, 20].

While the theoretical foundations of ABE are well-established, its practical deployment has been hindered by several factors, including high computational complexity, large key and ciphertext sizes, and challenges in managing user revocation. Moreover, the adoption of cryptographic systems within national and enterprise infrastructures often requires compliance with government-mandated standards. In this context, the **SM9 standard**, issued by the Chinese government, has emerged as a critical framework for identity-based cryptography [6]. The SM9 algorithm specifies a complete set of cryptographic primitives, including digital signatures and key exchange, based on IBE. Its standardization provides a solid foundation for interoperability and trust in commercial and governmental applications within China and for international entities that interact with them. Several works have explored and extended the SM9 standard, developing schemes for broadcast encryption [4], efficient user revocation [5], hierarchical encryption [37], and even homomorphic encryption [38]. Implementations and security analyses have further solidified its practical relevance [6, 39, 40].

Despite the progress in both ABE research and the standardization of SM9, a significant gap remains. There is a lack of KP-ABE schemes that are explicitly designed to be compatible with the SM9 standard, leveraging its specific mathematical structures and cryptographic components. Existing ABE schemes often use different elliptic curve parameters and cryptographic assumptions, creating a barrier to integration. This incompatibility limits the ability of systems built on the SM9 standard to benefit from the powerful, fine-grained access control capabilities of KP-ABE. The development of an SM9-compatible KP-ABE scheme would bridge this gap, enabling a new class of secure and compliant applications, from secure dispatching in industrial control clouds [40] to flexible data sharing in government platforms.

Our Contribution

This paper addresses the aforementioned gap by designing, analyzing, and demonstrating the applications of a novel **SM9-Enhanced Key-Policy Attribute-Based Encryption (SM9-KP-ABE)** scheme. Our work makes several key contributions to the field:

1. **Novel Scheme Construction:** We present the complete design of a KP-ABE scheme that is natively built upon the cryptographic foundations of the SM9 standard. Our construction utilizes the specific pairing-friendly elliptic curve and hash functions specified by SM9, ensuring seamless integration with existing SM9-based infrastructures.
2. **Support for Expressive Access Policies:** The proposed scheme supports access policies represented by general Boolean circuits, allowing for highly expressive and flexible access control. This is a significant improvement over schemes limited to monotonic threshold gates. We adapt techniques for handling general circuits [17, 19] to the SM9 context.
3. **Provable Security without Random Oracles:** We provide a rigorous security analysis of our scheme. A key insight of our work is that by leveraging a hybrid encryption approach similar to the Fujisaki-Okamoto transform [7] and tight reduction techniques [12], we can prove that our scheme achieves **IND-CPA (Indistinguishability under Chosen-Plaintext Attack) security** in the standard model. This avoids reliance on the random oracle model, which is a heuristic assumption, thereby providing a stronger

security guarantee.

4. **Efficiency and Performance Optimization:** A central goal of our design is practical efficiency. The proposed SM9-KP-ABE scheme is optimized to reduce computational overhead. Our analysis suggests that the decryption process requires a constant number of pairing operations, regardless of the complexity of the attribute set, which significantly improves performance compared to many existing schemes [19]. This makes our scheme particularly suitable for resource-constrained devices, such as those in IoT networks. Furthermore, the scheme is designed to produce **constant-size ciphertexts**, a critical feature for applications with storage or bandwidth limitations [27, 29, 31].
5. **Comprehensive Analysis and Application Context:** We provide a thorough performance comparison of our scheme against several state-of-the-art KP-ABE schemes [19, 31, 40], demonstrating its advantages in terms of computational cost and communication overhead. We also discuss the practical implications and potential applications of our scheme in areas like secure cloud data management [30, 34] and assured data deletion [35].

Article Structure

The remainder of this article is organized as follows. Section 2 reviews the necessary cryptographic preliminaries, including bilinear pairings and the SM9 standard, and formally defines our system and security models. Section 3 presents the detailed construction of our proposed SM9-KP-ABE scheme. In Section 4, we provide a comprehensive analysis of the scheme, including proofs of its correctness and security, as well as a detailed performance evaluation. Section 5 discusses the implications of our findings, explores potential applications, and outlines directions for future work. Finally, Section 6 concludes the paper.

METHODS (Preliminaries and Scheme Design)

This section lays the groundwork for our proposed scheme. We begin by reviewing the essential cryptographic concepts, including bilinear maps and complexity assumptions. We then provide an overview of the SM9 standard, which forms the basis of our construction. Finally, we formally define the system architecture and the security model used to prove the robustness of our scheme.

Cryptographic Preliminaries

Our construction is based on the properties of bilinear pairings on elliptic curves.

Bilinear Maps (Pairings)

Let G1 and G2 be two cyclic groups of the same large prime order p. We denote G1 as an additive group and G2 as a multiplicative group. Let P be a generator of G1. A bilinear map (or pairing) is a function $e:G1\times G1\rightarrow G2$ that satisfies the following properties:

1. **Bilinearity:** For all $Q,R\in G1$ and all $a,b\in Zp^*$, we have $e(aQ,bR)=e(Q,R)^{ab}$.
2. **Non-degeneracy:** There exists a generator $P\in G1$ such that $e(P,P)\neq 1_{G2}$, where 1_{G2} is the identity element in G2.
3. **Computability:** For all $Q,R\in G1$, the map $e(Q,R)$ can be efficiently computed.

The SM9 standard specifies the use of a Barreto-Naehrig (BN) curve over a 256-bit prime field, which provides a suitable setting for such pairings.

Complexity Assumptions

The security of our scheme relies on the intractability of certain mathematical problems in the context of bilinear groups. The primary assumption we use is the Decisional Bilinear Diffie-Hellman (DBDH) problem.

Definition 1 (Decisional Bilinear Diffie-Hellman (DBDH) Problem):

Let (G1,G2,p,P,e) be a bilinear group setting. The DBDH problem is to distinguish between the tuples $(aP,bP,cP,e(P,P)^{abc})$ and (aP,bP,cP,Z) for random $a,b,c\in Zp^*$ and a random $Z\in G2$.

An algorithm A has an advantage ϵ in solving the DBDH problem if:

$$|Pr[A(P,aP,bP,cP,e(P,P)^{abc})=1]-Pr[A(P,aP,bP,cP,Z)=1]|\geq\epsilon$$

where the probabilities are taken over the random choices of $a,b,c\in Zp^*$, the random choice of $Z\in G2$, and the random coins of A.

DBDH Assumption: We assume that for any probabilistic polynomial-time (PPT) algorithm A, its advantage ϵ in solving the DBDH problem is negligible. The security proofs for many prominent IBE and ABE schemes are based on this assumption or its variants [10, 12, 14].

The SM9 Identity-Based Encryption Standard

The SM9 standard, specified in the Chinese national document GMT 0044-2016, defines an identity-based public key cryptographic suite. It consists of four main parts: general principles, digital signature algorithm, key exchange protocol, and key encapsulation mechanism & public key

encryption algorithm. Our work is primarily concerned with the encryption algorithm.

The core idea of SM9 is to use a user's identity (e.g., an email address or phone number) along with a master public key to generate the user's public key. This eliminates the need for public key certificates and simplifies key management. The key components relevant to our work are:

- **System Parameters:** A prime-order bilinear group setting (G1,G2,p,P,e) and cryptographic hash functions H1:{0,1}∗→Zp∗ and H2:{0,1}∗→{0,1}k, where k is the key length of a symmetric cipher.
- **Key Generation Center (KGC):** The KGC generates a master secret key msk∈Zp∗ and a corresponding master public key mpk=msk·P.
- **Private Key Generation:** For a user with identity ID, the KGC computes QID=H1(ID||hid) (where hid is a system identifier) and generates the user's private key as skID =msk+QID1·P.
- **Encryption:** To encrypt a message M for user ID, the sender chooses a random r∈Zp∗, computes C1=r·P, g=e(QID,mpk), C2=M⊕H2(gr), and C3=Hash(M||gr). The ciphertext is (C1,C2,C3).

Our SM9-KP-ABE scheme adapts this structure, replacing the single identity ID with a set of attributes and embedding a policy into the user's private key.

System and Security Models

We now formally define the architecture and security requirements for our KP-ABE scheme.

System Model

Our system involves three types of entities:

1. **Attribute Authority (AA):** This is a trusted entity responsible for defining the universe of attributes and generating system parameters. It also generates private keys for users based on the access policies they are granted. The AA holds the master secret key.
2. **Data Owner (DO):** This entity owns sensitive data. The DO encrypts their data, associating it with a set of descriptive attributes Γ. They then upload the resulting ciphertext to a storage server (e.g., a cloud server), which is considered untrusted.
3. **Data User (DU):** This is the entity that wants to access the data. Each user is issued a private key SKA from the AA, which corresponds to a specific access policy A. The DU can decrypt a ciphertext CTΓ if and only if the attribute set Γ of the ciphertext satisfies the policy A in their key.

2.2.2. Formal Definition of KP-ABE

A KP-ABE scheme consists of four fundamental algorithms:

- **Setup(1λ) → (MPK, MSK):** This randomized algorithm is run by the AA. It takes a security parameter λ as input and outputs the master public key MPK and the master secret key MSK. MPK is made public, while MSK is kept secret.
- **Encrypt(MPK, M, Γ) → CT:** This randomized algorithm is run by the DO. It takes the master public key MPK, a message M, and a set of attributes Γ={attr1,attr2,…,attrn } as input. It outputs a ciphertext CT.
- **KeyGen(MSK, A) → SK$_\mathcal{A}$:** This randomized algorithm is run by the AA. It takes the master secret key MSK and an access structure A as input. It outputs a private key SKA for the policy A.
- **Decrypt(SK$_\mathcal{A}$, CT) → M or ⍰:** This deterministic algorithm is run by the DU. It takes a private key SKA and a ciphertext CT (which was encrypted under an attribute set Γ) as input. If the attribute set Γ satisfies the access policy A, the algorithm outputs the original message M. Otherwise, it outputs a failure symbol ⊥.

2.2.3. Access Structure

In our scheme, we support access policies represented by general Boolean circuits. A Boolean circuit consists of input wires, AND gates, OR gates, and NOT gates. In our context, the input wires to the circuit correspond to the attributes in the universe. An attribute set Γ satisfies a circuit A, denoted A(Γ)=1, if evaluating the circuit with input 1 for every attribute present in Γ and 0 otherwise results in the output gate evaluating to 1. This is a highly expressive policy language, subsuming simpler structures like threshold gates and non-monotonic formulas [15, 21].

Security Model

We define the security of our KP-ABE scheme using the standard notion of Indistinguishability under a Chosen-Plaintext Attack (IND-CPA). This is formalized via the following game played between a challenger C and a probabilistic polynomial-time adversary A:

- **Init:** The adversary A declares a set of attributes Γ∗ that it intends to challenge.
- **Setup:** The challenger C runs the Setup algorithm to generate the master public key MPK and master secret key MSK. It sends MPK to the adversary A.
- **Query Phase 1:** The adversary A can adaptively issue queries for private keys corresponding to access policies A1,A2,…,Aq. For each query Ai, the challenger responds with the corresponding private key SKAi generated by KeyGen(MSK, $\mathcal{A}_i$). The only constraint is that none of the queried policies Ai may be satisfied by the challenge attribute set Γ∗ (i.e., Ai(Γ∗)=0 for all i).
- **Challenge:** The adversary A submits two equal-length

messages, M0 and M1, to the challenger. The challenger flips a random coin b∈{0,1}, encrypts Mb under the challenge attribute set Γ∗ to get a challenge ciphertext CT∗=Encrypt(MPK, Mb,Γ∗), and sends CT∗ to A.

- **Query Phase 2:** The adversary can continue to issue private key queries for policies Aj under the same constraint that Aj(Γ∗)=0.
- **Guess:** Finally, the adversary A outputs a guess b′∈{0,1} for b.

The advantage of the adversary A in this game is defined as AdvAKP-ABE=|Pr[b′=b]−1/2|.

Definition 2 (IND-CPA Security): A KP-ABE scheme is IND-CPA secure if the advantage of any probabilistic polynomial-time adversary in the above game is a negligible function of the security parameter λ. This model captures the requirement that an adversary cannot learn any information about an encrypted message, even if they possess keys for many other access policies, as long as none of those policies grant access to the specific challenged ciphertext.

The Proposed SM9-Enhanced KP-ABE Scheme

In this section, we present the detailed construction of our SM9-Enhanced Key-Policy Attribute-Based Encryption (SM9-KP-ABE) scheme. Our design leverages the core components of the SM9 standard while incorporating mechanisms to support expressive KP-ABE functionalities. We employ a hybrid encryption strategy, using the ABE scheme to encrypt a symmetric key, which is then used to encrypt the actual data. This approach, inspired by the Fujisaki-Okamoto transform [7], is standard for building provably secure systems.

Let the universe of attributes be denoted by U={1,2,...,N}. We will represent an access policy as a Boolean circuit A. The scheme is described by the four algorithms below. For clarity of presentation and proof, the following construction is based on a standard Linear Secret-Sharing Scheme (LSSS) matrix representation of the access policy, which is equivalent to the Boolean circuit model for policy expression.

Setup(1λ)

The Attribute Authority (AA) runs this algorithm. It takes the security parameter λ as input.

1. Choose a bilinear group setting (G1,G2,p,P,e) as specified by the SM9 standard.
2. Select two random exponents α,β∈Zp∗.
3. For each attribute i in the attribute universe U={1,2,...,N}, choose a random exponent ti∈Zp∗.
4. The Master Public Key (MPK) is published as: MPK=(P,Ppub=αP,g=e(P,P)β,{Ti=tiP}i∈U)
5. The Master Secret Key (MSK) is kept secret by the AA: MSK=(α,β,{ti}i∈U)

KeyGen(MSK, A)

To generate a private key for a user with an access policy A, represented by an LSSS matrix pair (M,ρ) where M is an l×k matrix and ρ maps rows of M to attributes.

1. Create a column vector v=(β,v2,...,vk)T where v2,...,vk are chosen randomly from Zp∗.
2. For each row j=1,...,l of the matrix M, calculate the share λj=Mj·v, where Mj is the j-th row of M.
3. Choose a random rj∈Zp∗ for each row j.
4. The private key SKA consists of components for each row j: Dj,1=αλjP+rjTρ(j)andDj,2=−rjP
5. The private key is SKA=({Dj,1,Dj,2}j=1..l,(M,ρ)).

Encrypt(MPK, M, Γ)

To encrypt a message M∈{0,1}∗ under a set of attributes Γ⊆U, the Data Owner (DO) does the following:

1. Choose a random symmetric key K∈{0,1}k.
2. Encrypt the message M using a symmetric encryption algorithm Esym (e.g., AES) with key K to get Csym=Esym (K,M).
3. Choose a random value s∈Zp∗.
4. Compute the ABE part of the ciphertext for the key, which is derived from g=e(P,P)β:
   - Ckey=K⊕H2(gs) (where H2 is a key derivation function).
   - C0=sPpub=sαP
   - For each attribute i∈Γ, compute Ci=sTi=stiP.
5. The final ciphertext is CT=(Ckey,C0,{Ci}i∈Γ,Csym).

Decrypt (SK$_\mathcal{A}$, CT)

A Data User (DU) with private key SKA receives a ciphertext CT=(Ckey,C0,{Ci}i∈Γ,Csym). To decrypt it, the DU performs the following steps:

1. The DU first determines if the attribute set Γ satisfies the policy A represented by (M,ρ). If it does, there exists a set of constants {wj∈Zp∗}j∈I where I⊆{1,...,l} such that ∑j∈IwjMj=(1,0,...,0).
2. The DU then uses their private key components corresponding to the rows in I to compute:

XY=j∈I∑wjDj,1=j∈I∑wj(αλjP+rjTρ(j))=j∈I∑wjDj,2=j∈I∑wj(−rjP)

3. Next, the DU computes the pairing term:

Term=e(C0,X)·j∈I∏e(Cρ(j),wjDj,2)=e(sαP,∑wj(αλjP+rjTρ(j)))·∏e(stρ(j)P,wj(−rjP))=e(P,P)s∑wjλj·e(P,P)sα∑wjrjtρ(j)·e(P,P)−s∑wjrjtρ(j)=e(P,P)s∑wjλj

4. Since ∑j∈Iwjλj=∑wj(Mj·v)=(∑wjMj)·v=(1,0,..,0)·(β,v2,..)T=β.
5. So, the final term evaluates to e(P,P)sβ=gs.
6. The user can now recover the symmetric key K=Ckey⊕H2(gs).
7. Finally, the user decrypts Csym using K to get the message M=Dsym(K,Csym).

RESULTS (Analysis of the Proposed Scheme)

In this section, we analyze the proposed SM9-KP-ABE scheme in terms of its correctness, security, and performance. We provide a formal proof of security under the DBDH assumption and conduct a comparative analysis against other prominent KP-ABE schemes.

Correctness Analysis

The correctness of the scheme follows directly from the decryption process detailed in Section 3.4. If the attribute set Γ of a ciphertext satisfies the access policy A in a user's key, then a set of constants {wj} exists that allows the user to combine their private key components. The calculation correctly cancels out all random values (rj) and reconstructs the term gs=e(P,P)sβ. This term is precisely the masking value used to encrypt the symmetric key K. An entity without a key corresponding to a satisfying policy cannot find the constants {wj} and thus cannot reconstruct gs to unmask the symmetric key. This demonstrates that the scheme is correct.

Security Analysis

We now argue the security of the proposed SM9-KP-ABE scheme, which can be formally proven to be IND-CPA secure under the Decisional Bilinear Diffie-Hellman (DBDH) assumption.

Theorem 1: *Suppose the DBDH assumption holds in the bilinear group setting (G1,G2,p,P,e). Then no probabilistic polynomial-time adversary has a non-negligible advantage in the IND-CPA security game against our SM9-KP-ABE scheme.*

Proof Sketch: The full proof follows a standard reduction argument common in ABE security proofs [14, 22] and can be structured through a series of games.

- **Game 0:** This is the real IND-CPA security game. The challenger and adversary interact as defined in Section 2.2.4.
- **Game 1:** This game is modified so that the challenge ciphertext is encrypted with a truly random session key instead of one derived from gs. The challenger sets Ckey∗=K′⊕H2(Z), where K′ is the symmetric key for message Mb and Z is a truly random element from G2. An adversary that can distinguish between Game 0 and Game 1 can be used to construct an algorithm to solve the DBDH problem. The advantage difference, |Adv0 −Adv1|, is therefore negligible under the DBDH assumption.
- **Game 2:** In this game, we modify how the private keys are generated for the adversary's queries. For any queried policy Ai such that Ai(Γ∗)=0, the challenger can generate a semi-functional key. Because the policy is not satisfied by the challenge attributes Γ∗, the LSSS property guarantees the existence of a vector w′ that is orthogonal to the secret-holding vector (1,0,..,0) but not to the rows of the matrix M corresponding to attributes in Γ∗. The challenger can use this property to construct key components that appear valid to the adversary but are generated without knowledge of the master secret β. This simulation is statistically indistinguishable from real keys from the adversary's perspective. Therefore, Adv1≈Adv2.
- **Conclusion of Proof:** In Game 2, the challenge ciphertext is encrypted using a random value, and the private keys issued to the adversary contain no information about the master secret β used to generate the challenge ciphertext's mask. Therefore, the adversary's view is completely independent of the challenge bit b. The advantage of the adversary in Game 2 is zero: Adv2=0. Combining these steps, we can conclude that the advantage of the adversary in the original game, Adv0, is negligible. This completes the argument for the scheme's IND-CPA security.

Performance Analysis

We now analyze the performance of our proposed SM9-KP-ABE scheme and compare it with other notable KP-ABE schemes. The main metrics for comparison are the size of the public parameters, private keys, and ciphertexts, as well as the computational cost of the primary cryptographic operations.

Let |G1| and |G2| be the sizes of elements in groups G1 and G2, respectively. Let N be the total number of attributes in the universe, l be the number of rows in the LSSS matrix for a policy A, and |Γ| be the number of attributes in a ciphertext.

Storage Cost Comparison

We compare the storage overhead of our scheme with several others in Table 1. The schemes for comparison are Hu et al. [19] and Kim et al. [31].

Table 1: Comparison of Storage Costs

Scheme	Public Key Size	Private Key Size	Ciphertext Size
Hu et al. [19]	$O(N)	G_1	$
Kim et al. [31]	$O(1)	G_1	$
Our Scheme	$O(N)	G_1	$

Our scheme's public key size is linear in the number of universe attributes, which is typical for this class of ABE. The private key size depends on the complexity of the user's policy (number of rows l in the LSSS matrix). A key advantage of our scheme is the ciphertext size. It is not strictly constant, but it scales only with the number of attributes on the data, |Γ|, not the complexity of the access policy. For many applications where data objects are tagged with a relatively small number of attributes, this is highly efficient and predictable.

Computational Cost Comparison

We compare the computational costs for the Encrypt and Decrypt operations. Let E1 denote an exponentiation in G1, and P denote a pairing operation. We focus on the most expensive operations.

Table 2: Comparison of Computational Costs

Scheme	Encryption Cost	Decryption Cost
Hu et al. [19]	$O(	\Gamma
Kim et al. [31]	O(l)E1	O(l)P
Our Scheme	$O(	\Gamma

The computational costs of our scheme are competitive. Encryption cost is proportional to the number of attributes in the ciphertext. Decryption cost, specifically the number of expensive pairing operations, is proportional to the number of attributes in the policy (l) that must be combined to satisfy the access structure. This performance is standard for LSSS-based constructions. The efficiency gain comes from the hybrid encryption design, where these expensive pairing operations are performed only once to retrieve a symmetric key, after which fast symmetric decryption takes over. This makes the overall user experience much faster than decrypting a large message directly with ABE.

DISCUSSION

The analysis presented in the previous section indicates that our proposed SM9-KP-ABE scheme offers a secure, efficient, and expressive solution for fine-grained access control. In this section, we discuss the broader implications of these findings, explore potential real-world applications, and identify limitations and avenues for future research.

Implications of Findings

The primary implication of our work is the successful bridging of two critical areas in modern cryptography: the advanced functionality of Attribute-Based Encryption and the practical necessity of national cryptographic standards. By designing a KP-ABE scheme that is natively compatible with the SM9 standard, we provide a clear pathway for deploying flexible access control systems in environments where SM9 compliance is a priority.

Our security analysis, which leads to a proof in the standard model (without random oracles), suggests a high level of assurance, which is crucial for applications involving sensitive government, corporate, or personal data. This theoretical robustness, a key insight of our design, is an important feature, distinguishing the approach from schemes that might rely on the stronger, but non-standard, random oracle assumption [8].

Furthermore, the performance characteristics of our scheme are of significant practical importance. The combination of near-constant-size ciphertexts and efficient decryption directly addresses two of the major barriers to the widespread adoption of ABE: communication and computational overhead. This efficiency makes sophisticated, policy-based access control more feasible not just for powerful servers, but also for resource-constrained endpoints like IoT sensors and mobile devices. Research into schemes with constant-size ciphertexts [27, 29] or fast decryption [28] has been a key goal in the field, and our work contributes to this trajectory within the specific context of KP-ABE and SM9.

Applications

The properties of our SM9-KP-ABE scheme make it well-suited for a variety of application domains:

- **Secure Cloud Storage and Sharing:** This is the most direct application. A user can upload files to a public cloud service [30] and encrypt them with attributes like {"department": "finance", "year": "2025", "sensitivity": "high"}. An internal auditor could be issued a key with the policy ("department" = "finance" AND "sensitivity" = "high"), allowing them to access the file, while an employee from another department would be denied access. Our scheme's efficiency is vital here, as cloud systems handle vast numbers of files and users. The use of a standard like SM9 can aid interoperability across different enterprise systems [40].
- **Electronic Healthcare Records (EHR):** In an EHR system, patient data can be encrypted with attributes like {"patient_id": "12345", "record_type": "cardiology", "access_group": "treating_physician"}. A cardiologist treating the patient would have a key with a policy allowing access to cardiology records for patients under their care. Emergency room doctors could have keys with broader policies that grant temporary access based on an "emergency_override" attribute. Our scheme helps ensure that sensitive patient data remains confidential even if the hospital's database is breached.
- **Internet of Things (IoT) Data Management:** Consider a smart city deployment where thousands of sensors (e.g., traffic, pollution, surveillance) generate data. This data can be encrypted with attributes describing its type, location, and timestamp. A municipal traffic control center could be given a key with a policy to access all {"type": "traffic_cam"} data, while an environmental agency's key might only permit access to {"type": "air_quality"} data. The low computational decryption cost of our scheme is critical for the potentially resource-limited data analysis nodes at the edge of the network.
- **Secure Search over Encrypted Data:** Our scheme can be combined with searchable encryption techniques. A user could submit an encrypted query corresponding to their access policy, and a cloud server could use this to find all matching ciphertexts without being able to decrypt the data or the query itself, similar to the system proposed by Boucenna et al. [34].

Limitations and Future Work

Despite its advantages, our scheme has limitations that suggest clear directions for future research.

1. **User Revocation:** The proposed scheme, in its current form, does not support efficient user or attribute revocation. If a user's private key is compromised or their access privileges change, there is no straightforward mechanism to revoke their access to previously encrypted data without re-encrypting all relevant files. This is a well-known challenge in ABE. Future work could focus on integrating efficient revocation mechanisms, possibly by incorporating techniques like those described in [25] or [35], which achieve direct revocation or assured data deletion.
2. **Scalability of Public Parameters:** The size of the public key in our scheme scales linearly with the size of the attribute universe (N). For systems with a very large and dynamic number of attributes, this could become a bottleneck. Investigating techniques for creating "large universe" ABE schemes, such as those proposed by Lewko and Waters [22], within the SM9 context would be a valuable extension.
3. **Chosen-Ciphertext Attack (CCA) Security:** Our scheme is proven to be secure against chosen-plaintext attacks (IND-CPA). While this is a strong guarantee, achieving security against chosen-ciphertext attacks

(IND-CCA) would provide an even higher level of security, protecting against active adversaries who can obtain decryptions of other ciphertexts. Extending our scheme to achieve IND-CCA security, perhaps by applying more advanced transforms or building upon CCA-secure IBE schemes [12], is an important research direction.

4. **Hierarchical and Non-Monotonic Policies:** While our scheme supports expressive LSSS policies, extending it to efficiently handle hierarchical key structures [21, 36, 43] would be beneficial for large organizations with nested domains of authority. Additionally, while LSSS can represent non-monotonic policies [15] (e.g., access is granted if attribute "A" is present AND attribute "B" is NOT present), specific constructions optimized for this task could improve efficiency.

CONCLUSION

In this paper, we have presented a novel Key-Policy Attribute-Based Encryption scheme designed to be fully compatible with the Chinese SM9 identity-based cryptography standard. Our work addresses a critical need for advanced access control mechanisms that can operate within standardized cryptographic ecosystems. The proposed **SM9-KP-ABE** scheme provides support for expressive LSSS-based access policies, allowing for the implementation of complex, real-world access rules.

Our contribution is threefold. First, we provided a detailed construction of the scheme, demonstrating how the core principles of KP-ABE can be instantiated using the specific mathematical structures of SM9. Second, we delivered a rigorous security analysis, arguing that our scheme is **IND-CPA secure** in the standard model under the well-established Decisional Bilinear Diffie-Hellman assumption. This strong theoretical guarantee makes our scheme suitable for high-security applications. Third, through a comprehensive performance analysis, we identified the practical efficiency of our scheme, highlighting its competitive performance and **near-constant-size ciphertexts**.

By bridging the gap between advanced ABE functionalities and national cryptographic standards, our work paves the way for a new generation of secure and interoperable systems for applications like cloud computing, electronic healthcare, and the Internet of Things. While we have identified areas for future enhancement, such as user revocation and CCA security, the proposed scheme provides a robust and efficient foundation for building practical, fine-grained access control systems today.

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.