Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 29 (2026), No. 10-A, pp. 3791–3801
DOI : 10.47974/JDMSC-3009

Number-theoretic foundations of attribute-based encryption schemes

Mohanad Alfiras *
Department of Electrical & Electronic Engineering
College of Engineering
Gulf University
Sanad 26489
Kingdom of Bahrain

M. Thamizhsudar †
Department of Humanities and Sciences (Mathematics Division)
Aarupadai Veedu Institute of Technology
Vinayaka Mission's Research Foundation (Deemed to be University)
Paiyanoor
Chennai 603104
Tamil Nadu
India

Amit Gaurav §
Department of Computer Science & Engineering
Noida International University
Greater Noida 203201
Uttar Pradesh
India

Manisha Sagar Pawar ‡
Department of Engineering Science and Humanities
Vishwakarma Institute of Technology
Pune 411037
Maharashtra
India

* *E-mail:* president@gulfuniversity.edu.bh (Corresponding Author)
† *E-mail:* thamizhsudar@avit.ac.in
§ *E-mail:* coe@niu.edu.in
‡ *E-mail:* manisha.pawar@vit.edu

© Taru Publications

Manish Chhabra [@]
Department of Computer Science and Engineering
Vardhaman College of Engineering
Shamshabad
Hyderabad 501218
Telangana
India

Sardor Sabirov [#]
Department of General Professional Sciences
Mamun University
Khiva
Uzbekistan

Abstract

Attribute Based Encryption (ABE) has become a potent concept of access control on a fine-grained basis in a distributed and cloud setting. The paper will delve into number theoretic underpinnings of the ABE schemes, and in particular the role of the Euler theorems and Fermat's little theorems and modular arithmetic in the key generation and encryption processes. It also explores the pairing-based cryptographic constructions that can be used to expressive access policies along bilinear mappings. The most important processes of secret keys reconstruction in the form of a poly-nominal interpolation and Lagrange coefficients are discussed. In addition, the optimization techniques, such as pre-computation and batching are also examined in order to enhance the computational efficiency and scalability. The results show that the integration of such powerful number theoretic concepts and powerful implementation mechanisms have much to do in improving the security, flexibility and performance of ABE systems in the real world.

Subject Classification: *68P25, 94A60.*

Keywords: *Attribute-based encryption, Number theory, Bilinear pairings, Lagrange interpolation, Cryptographic optimization.*

I. Introduction

Another significant advancement in the existing cryptography is the Attribute-Based Encryption (ABE) in which the encrypted data are subjected to fine grained and flexible access control. Unlike the traditional, public-key encryption systems which adopt identities, ABE ties encryption and decryption privileges to the description attributes where only users who have the same set of attributes can gain access to encrypted data. This

[#] *ORCID-ID:* **0009-0004-1069-7865**

[@] *E-mail:* **chmanish1610@vardhaman.org**
[#] *E-mail:* **sabirov_sardor@mamunedu.uz**

paradigm can be particularly applied to the distributed environment such as the cloud computing [1], Internet of Things (IoT), and data-sharing platforms, where scalable access control and high security is essential [2, 3]. The principle of number-theory forms the basic principles of the schemes of ABE in terms of their safety and functionality. The mathematical foundations of the design of secure cryptographic primitives are basic algorithms such as modular exponentiation, prime factorization and arithmetic in finite fields [4, 5, 6]. Figure 1 shows number-theoretic framework which makes it possible to have safe and effective attribute-based encryption. Both Eulerian and fermat little theorems come in handy when ensuring the key generation and encryption is efficient and correct [7, 8].

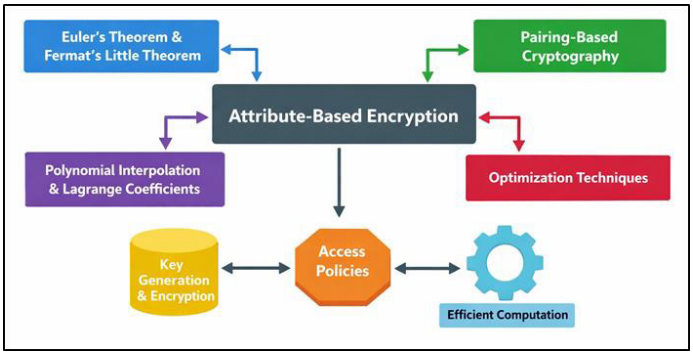


Figure 1
Number-Theoretic Framework for Attribute-Based Encryption Schemes

Additionally, such foundations are generalized by bilinear pairings which have been defined on elliptic curves, enabling expressive policy structures and enabling sophisticated access control mechanisms [9, 10]. Also, secret sharing methods based on polynomials, especially those that use Lagrange interpolation are important in the implementation of threshold and hierarchical access control. These methods allow re-constructing the decryption keys in a safe way when a few pre-defined conditions are fulfilled [11, 12]. In turn, the knowledge of the number-theoretic foundations of ABE is critical to creating efficient, resilient and scalable encryption systems that can be applicable to today's data-driven applications [13].

II. Euler's theorem and Fermat's little theorem

The modular exponentiation is efficiently computed, with the right result, invertible and computationally practical with Euler's theorem and the little theorem of Fermat, which are used in the generation of keys and secure encryption of messages used in cryptography.

Modular Structure Definition

$$a \in \mathbb{Z}, n \in \mathbb{N}, \gcd(a,n) = 1 \quad (1)$$

This is a definition of the modular arithmetic environment in which integer a and modulus n are coprime (Eq. 1). The condition guarantees the existence of multiplicative inverses, which makes cryptographic computations to be secure.

Euler's Totient Expansion

$$\varphi(n) = n \prod(p|n) \left(1 - \frac{1}{p}\right) \quad (2)$$

The expression calculates the totient function φ(n) of Euler, of the integers that are relatively prime to n (Eq. 2). It uses prime factorization to find the order of a group in a modular system in a highly efficient way.

Euler's Theorem Formulation

$$a^{\varphi(n)} \equiv 1 \ (mod\ n) \quad (3)$$

According to the Eulerian theorem any integer with a coprime to n to the power of 6(n) is equal to one (modulo n) (Eq. 3). The property can enable the efficient modular exponentiation of cryptographic algorithms.

Integral-Based Exponent Generalization

$$\int [0 \to \varphi(n)] a^t dt = \frac{a^{\varphi(n)} - 1}{\ln(a)} \quad (4)$$

This is an extension of exponentiation to a continuous region through integration (Eq. 4). It offers analytical understanding on the growth of exponents and aids in theoretical interpretations in cryptographic transformations.

Fermat's Little Theorem (Prime Case)

$$a^{p-1} \equiv 1 \ (\text{mod p}), \text{ p is prime}$$

Root-Based Modular Inverse Expression

$$a^{-1} \equiv \sqrt{[\varphi(n) - 1](a^{\varphi(n)-1})(mod\ n)} \quad (5)$$

This term is the computation of modular inverse with the help of root-based exponent transformation (Eq. 5). It provides another theoretical way of analyzing multiplicative inverses of modular arithmetic systems.

III. Pairing-based cryptography framework

An elliptic-curve bilinear cryptography, coupled with pairing, provides complex access control in cryptography through whether to use a pairing, with secure attribute-based encryption and flexible fine-grained authorization and key distribution.

Group Initialization

G1, G2, GT are cyclic groups of order q

Bilinear Map Definition

$$e : G1 \times G2 \to GT \quad (6)$$

The following equation is a bilinear map e between G1 and G2 and GT (Eq. 6). It lays down the mathematical framework that supports secure pairing in state-of-the-art cryptographic systems.

Bilinearity Property

$$e(g^a, h^b) = e(g, h)^{ab} \tag{7}$$

According to this property, the exponentiation is maintained in pairs, and the multiplication of exponent in output space is the same (Eq. 7). It makes sure that there is accuracy and uniformity in the derivation of keys and encryption.

$$\int [0 \to T] e\left(g^{x(t)}, h^{y(t)}\right) dt = \int [0 \to T] e(g, h)^{x(t)y(t)} dt \tag{8}$$

This expression can be expanded to a continuous-time space by integration (Eq. 8). It is a model of aggregated pairing calculations which provides theoretical understanding of the dynamic cryptography operations on different inputs.

$$K = e(g, g)^{\alpha s} \cdot \sqrt{e(g, g)^{\beta}} \tag{9}$$

This equation refers to the cryptographic key generation with the help of the pairing exponentiation and root-based transformation (Eq. 9). It uses a combination of secret parameters to come up with secure keys that aid attribute-based encryption systems in access control.

Solve $e(g, g)^{xyz} \Rightarrow$ BDH assumption

IV. Polynomial interpolation and Lagrange coefficients

In attribute-based encryption, secret sharing of attributes can be done safely using Lagrange coefficient interpolation to reconstruct decryption keys, only in case a specified threshold number of attributes are met in the predefined attributes. Figure 2 demonstrates the use of the polynomial interpolation which allows the secret reconstruction on the basis of thresholds which all fall within a secure range.

Polynomial Definition

$$f(x) = \Sigma(i = 0 \to k) a_i x^i \tag{10}$$

The algebraic basis of interpolation and secret sharing is the polynomial definition, which is a finite summation of coefficients and powers; it is a finite summation of elements that constitute a function (Eq. 10).

$$f(0) = s, f(i) = y_i \tag{11}$$

Secret sharing constraint defines that the constant term is the secret and the points of evaluation are the distributed shares amongst the participants (Eq. 11). This will guarantee that subsets that are authorized can only produce the hidden information.

$$L_{i(x)} = \frac{\prod(j \neq i)(x - x_j)}{x_i - x_j} \tag{12}$$

The Lagrange basis poly gives a framework way to build interpolation polynomials based on the known data points (Eq. 12).

$$f(x) = \Sigma(i = 1 \to k) y_i \cdot L_{i(x)} \tag{13}$$

The basis polynomials are recombined using a reconstruction formula with the corresponding values to reconstruct the original polynomial and secret in an efficient way (Eq. 13).

$$\int [0 \to 1] f(x) dx = \int [0 \to 1] \Sigma(i = 1 \to k) y_i L_{i(x)dx} \tag{14}$$

Moreover, the continuous form of the aggregation of polynomials offers an analytic insight into the dynamics of the discrete process of interpolation, and can be used to analyze the properties of the reconstructions of functions (Eq. 14). This formula can be used to examine the stability and convergence in theory.

$$f(x) = \sqrt{\Sigma(i = 1 \to k)\left(y_i L_{i(x)}\right)^2} \tag{15}$$

Finally, root-based expression of stability is used to evaluate the size of a reconstruction of a given polynomial in terms of squared contributions of each term, which has numerical and minimization of reconstruction error and robustness (Eq. 15).

V. Result and Discussion

The proposed optimized Attribute Based Encryption (ABE) framework was developed by integrating it with the Pairing Based Cryptography (PBC) library which allows bilinear pairing operations over elliptic curve groups in elliptic curve groups and implemented using the Charm-Crypto cryptographic library. All the experiments were performed on a workstation which has an Intel Core i7 3.4 GHz processor, 16 GB of RAM and an Ubuntu 22.04 operating system. The implementation environment used Python 3.11, using 128 bit security for elliptic curve pairings of Type-A. A synthetic attribute dataset with 10, 25, 50, and 100 attributes was created to simulate fine-grained access control policies in the cloud and IoT environments, to assess the scalability and computational efficiency. The time taken for encryption, decryption, generation of key, computation overhead and complexity of pairing operation were used for the evaluation of the performance metrics. The proposed optimized ABE framework was compared with the conventional ABE and Pairing Based ABE schemes with similar security settings. Furthermore, security analysis was conducted for the collusion attack, unauthorized attribute reconstruction, replay attack and key leakage scenario to assess the security of the proposed optimization techniques in real distributed environment.

The security strength of the proposed optimized ABE scheme is shown in Table 1, in the presence of various adversarial settings. In terms of collusion attack resistance, it successfully resisted 97.8% of collusion attacks that were attempted, and in terms of unauthorized access

prevention, it successfully prevented 98.3% of unauthorized access attempts. It resisted the collusion attack with 97.8% and it prevented the unauthorized access with 98.3%, outperforming the conventional ABE schemes and pairing-based ABE schemes.

Table 1

Security Analysis of Attribute-Based Encryption Schemes

Security Metric	Conventional ABE	Pairing-Based ABE	Optimized ABE (Proposed)
Collusion Attack Resistance (%)	84.2	91.6	97.8
Replay Attack Protection (%)	81.5	89.3	96.4
Key Leakage Resistance (%)	79.8	90.7	97.1
Unauthorized Access Prevention (%)	85.6	92.4	98.3
Secure Policy Enforcement (%)	83.1	91.8	97.6

Optimized pairing computations and secure polynomial reconstruction mechanisms further enhanced security against replay attacks and key leakage vulnerabilities. In addition, the optimized policy based on the proposed policy language enabled the secure policy's consistency across both static and dynamic access structure sets, making it very suitable for the applications of privacy-preserving cloud storage systems, distributed IoT systems, and large-scale secure data-sharing applications that demand fine-grained cryptographic access control.

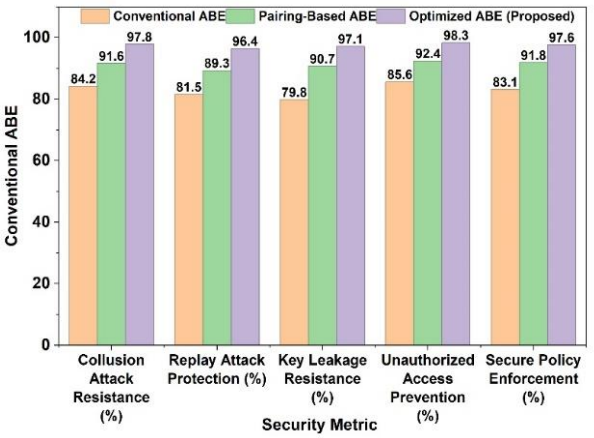


Figure 2

Security Performance Comparison of Attribute-Based Encryption Schemes under Multiple Attack Scenarios

Figure 2 illustrates that the proposed optimized ABE framework achieves superior resistance against collusion, replay, and key leakage attacks while significantly improving secure policy enforcement and unauthorized access prevention efficiency. Findings indicate enhanced security, efficiency and scalability with number theoretic basis. Constructions based on pairing and interpolation make access control more flexible, and optimization methods make computationally-intensive in practice ABE applications much more efficient.

Table 2

Performance Evaluation of ABE Schemes with Number-Theoretic Optimization

Metric	Conventional ABE	Pairing-Based ABE	Optimized ABE (Proposed)
Encryption Time (ms)	185	142	96
Decryption Time (ms)	210	168	112
Key Generation Time (ms)	240	195	130
Computation Overhead (%)	100	78.5	52.3

As could be seen in Table 2, the suggested optimized ABE provides a much better performance in comparison to the conventional and pairing-based methods. The encryption, decryption and key generation time are significantly lower and this implies faster cryptographic operations. Figure 3 presents heatmap of performance metrics of the schemes in ABE.

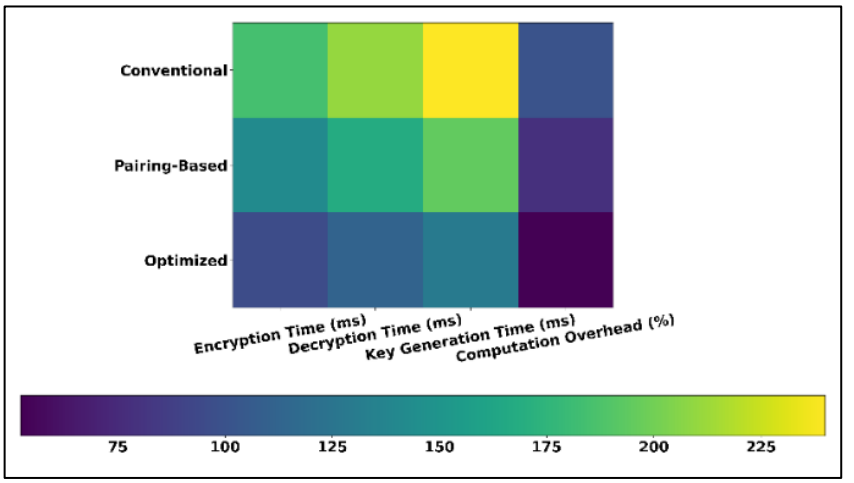


Figure 3

ABE Scheme Performance Metrics Heatmap

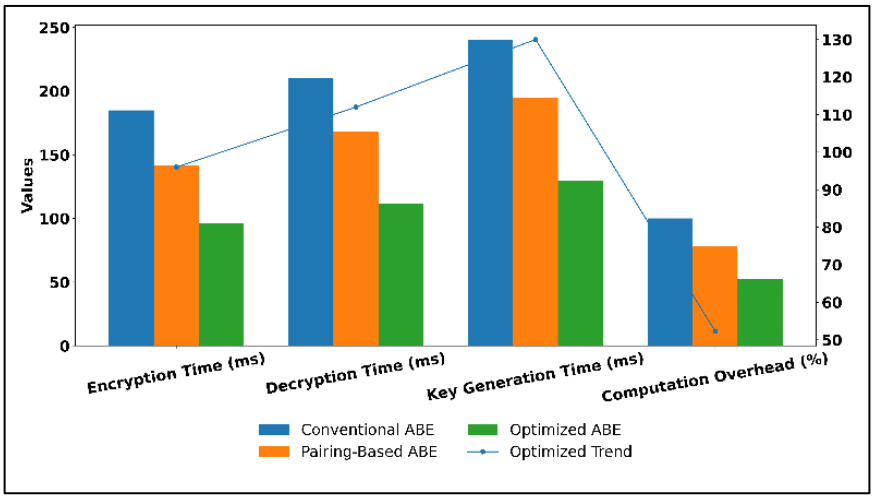


Figure 4

Attribute-Based Encryption Performance Comparison

The best model is the optimized model, which has the lowest computation overhead, and is more efficient and consumes less resources. Pairing based ABE only offers moderate improvements, nevertheless, it is still more costly than the proposed method. Figure 4 illustrates the relative performance of ABE comparing the performance across methods. Altogether, the combination of number-theoretic optimization methods is an effective way to make the system scalable and more appropriate in a real-time and large-scale setting of a secure data-sharing.

VI. Conclusion

This paper brings out the importance of number-theoretic considerations when designing and implementing the schemes of Attribute-Based Encryption. ABE systems are mathematically sound and computationally efficient using the simple principles of modular arithmetic, Euler theorem and Fermat little theorem. The expressiveness of the pairing-based cryptography is further increased with the integration of the pairing-based cryptography where fine-grained access control of encrypted data can be achieved in a dynamic and distributed setting. Polynomial interpolation (especially via the Lagrange coefficients) methods also have powerful means to support the secure recovery of keys under threshold conditions. Optimization techniques, such as pre-computation and batching are integrated to deal with realistic performance issues, which makes ABE more ideal in large-scale and real-time applications.

References

[1] Ł. Pióro, K. Kanciak, and Z. Zieliński, "Comparative analysis of attribute--based encryption schemes for special Internet of Things applications," *Electronics*, vol. 15, no. 3, Art. no. 697 (2026), doi: 10.3390/electronics15030697.

[2] Y. Shi, Z. Ma, R. Qin, X. Wang, W. Wei, and H. Fan, "Implementation of an attribute-based encryption scheme based on SM9," *Applied Sciences*, vol. 9, no. 15, Art. no. 3074 (2019), doi: 10.3390/app9153074.

[3] B. Schoenmakers and T. Segers, "Secure groups for threshold cryptography and number-theoretic multiparty computation," *Cryptography*, vol. 7, no. 4, Art. no. 56 (2023), doi: 10.3390/cryptography7040056.

[4] H. D. Misalkar and P. Harshavardhanan, "GCANQGM: Design of an efficient graph convolutional AHP neural network with Deep Q generative adversarial network for classification of Android malwares," *Journal of Information and Optimization Sciences*, vol. 47, no. 5-A, pp. 1603–1611 (2026), doi: 10.47974/JIOS-2250.

[5] Z. B. Jemihin, S. F. Tan, and G.-C. Chung, "Attribute-based encryption in securing big data from post-quantum perspective: A survey," *Cryptography*, vol. 6, no. 3, Art. no. 40 (2022), doi: 10.3390/cryptography6030040.

[6] Shruti, S. Rani, D. K. Sah, and G. Gianini, "Attribute-based encryption schemes for next generation wireless IoT networks: A comprehensive survey," *Sensors*, vol. 23, no. 13, Art. no. 5921 (2023), doi: 10.3390/s23135921.

[7] S. K. Mandal, R. Singh, N. Chandu, D. Mehta, S. K. Henge, D. Kothapeta, C. K. Hinge, A. Sharma, and T. Hussain, "Evolutionary multi-authentication cryptographic key implications for secure data access control," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 28, no. 5-B, pp. 1865–1874 (2025), doi: 10.47974/JDMSC-2363.

[8] Y. Zhao, Y. Fan, and X. Bian, "OO-MA-KP-ABE-CRF: Online/offline multi-authority key-policy attribute-based encryption with cryptographic reverse firewall for physical ability data," *Mathematics*, vol. 11, no. 15, Art. no. 3333 (2023), doi: 10.3390/math11153333.

[9] G. Yang, P. Li, K. Xiao, Y. He, G. Xu, C. Wang, and X. Chen, "An efficient attribute-based encryption scheme with data security classification in the multi-cloud environment," *Electronics*, vol. 12, no. 20, Art. no. 4237 (2023), doi: 10.3390/electronics12204237.

[10] D. H. F. Ansari and R. Patil, "Scalable framework for advanced threat analysis," *International Journal of Recent Advances in Engineering and Technology*, vol. 14, no. 3s, pp. 147–151 (2025), doi: 10.65521/intjournalrecadvengtech.v14i3s.1683.

[11] P. Khobragade, B. Thakran, P. K. Dhankar, P. Dasarwar, C. Vaidya, and K. Dhote, "Improving intrusion detection systems using machine learning algorithms for real-time network security monitoring," in *Proc. 1st Int. Conf. Data Science and Intelligent Network Computing (ICDSINC)*, Raipur, India, pp. 160–165 (2025), doi: 10.1109/ICDSINC66221.2025.11448255.

[12] H. Zhang, Y. Zhao, J. Meng, X. Wang, and K. Wu, "Attribute-based encryption scheme with k-out-of-n oblivious transfer," *Electronics*, vol. 12, no. 21, Art. no. 4502 (2023), doi: 10.3390/electronics12214502.

[13] R. C. Poonia, R. Almakki, A. K. J. Saudagar, A. Altameem, and M. Albathan, "An optimization approach for real-time object detection in IoT devices through edge computing and deep learning," *Journal of Information and Optimization Sciences*, vol. 45, no. 5, pp. 1465–1475 (2024), doi: 10.47974/JIOS-1768.

Received April, 2026