International Journal of Combined Research & Development (IJCRD)
eISSN:2321-225X; pISSN:2321-2241 Volume: 13; Issue: 7; July- 2024

AN EFFICIENT POST-QUANTUM ATTRIBUTE-BASED ENCRYPTION SCHEME

Dhavala M U
PG Student
Dept. of MCA
The Oxford College of Engineering,
Bommanahalli,
Bengaluru-560068
dhavalamu@gmail.com

Dharamvir
Associate Professor
Dept. of MCA
The Oxford College of Engineering,
Bommanahalli,
Bengaluru-560068
dhiruniit@gmail.com

ABSTRACT

Attribute-based encryption (ABE) is an important technology to ensure data confidentiality and confidentiality in cloud computing. It allows data owners to securely store and share data in the cloud environment. But recent advances in quantum processors have increased the ability to solve complex mathematical problems such as arithmetic and calculating the logarithm of large numbers. This advancement in the quantum computing provides significant security benefits to existing cryptographic systems. Current post-quantum ABE schemes cannot simultaneously provide important features such as authentication, user privacy, and user revocation. In this paper, we introduce the first secure, efficient and post-quantum ABE scheme based on metric level codes. Our scheme enjoys all mentioned features due to utilization of low rank parity check codes. The developed protocol protects against standard format optional plaintext attacks and reactive attacks (a type of optional ciphertext attack). At 256-bit security, its size is approximately 16.5 KB, and its execution time on the desktop is approximately 31.2 milliseconds. Our performance reveals that the planning process is better. than the existing post-quantum and classical schemes.

Key words: Encryption, decryption, data privacy, attribute-based cryptography

INTRODUCTION

In computer networks that use public encryption schemes, the exchange of public keys is important for user authentication. Therefore, the role of trusted authority has become important to create a key pair for public and private users and remove it when necessary**.** [1]. To achieve this goal, a public key system is established as the basis for managing identity information and authenticating users to provide a secure environment. Instead of creating a certificate for each public key, a user's public key can be generated based on the user's identity. This concept was initially suggested by Shamir in 1984 and called

identity-based encryption (IBE) [2]. Because the trust policy publishes each subject's private key based on its identity; the subject is not necessary to secure the public key from the trusted certificate. The initial concept for identity-based encryption (IBE) was proposed by Boneh and Franklin in 2001. [3]. The salient advantage of IBE is could be the secrete key of the trusted authority is removed after registering all users in the system. Afterwards, a key distribution centre will no longer be needed [4]. Inspired by IBE, the first attribute-based encryption (ABE) scheme was developed by Sahai and Waters [5]. They call their idea fuzzy identity-based encryption. In the initial proposal by Sahai and Water, the decryption strategy is built on the proximity of two sets of features. Although simple, this idea might not be easy. [6]. Subsequent research determined how the policy was defined [7]. There are generally two types of policies in ABE: key policy ABE (KP-ABE) [8] and cipher text policy ABE(CP-ABE) [9] In Key Attribute Based Encryption (KP-ABE), the receiver's key is derived from an accessible pattern and the sender encrypts the message using the required attributes. In ciphertext policy attribute-based encryption (CP-ABE) the process is reversed: the sender encrypts the data using an access pattern, and the receiver's private key is generated by his habits. In recent years, people have been considering using cloud servers to increase computing speed, expand data storage space and reduce hardware costs. [10], [11]. Data is often encrypted in cloud storage because users cannot trust cloud servers. Therefore, one of the main issues in this regard is how to ensure the security data of many users in accordance with the law. ABE offers a simple solution to this problem.

In recent years, features like the ability to revoke user access [12] and check the outsourced computation results [13] have been added to ABE. These schemes are based on elliptic curve pairing, which reduces the efficiency. This problem has already been solved in [14] and [15], and the efficiency is significantly increased.

Nowadays, tremendous advances have been made in quantum processors. Using Shor's quantum algorithm [16] and assuming to build strong enough quantum processors, the security of many existing cryptographic methods like RSA and DSA face threats. To address the threats posed by quantum processors, the National Institute of Standards and Technology (NIST) has developed standards for asymmetric encryption, key exchange, and digital signature standards. [17]. Many ABE schemes, which rely on number theoretic problems, have been put forward for enhance data security in cloud computing environments [18], [19]. Unfortunately, none of the existing solutions will protect high-end computers. Lattice-based housing schemes have recently been suggested to prevent threats from quantum processors. [20], [21]. However, these schemes have large key lengths and need to be more efficient.

LITERATURE REVIEW

This research paper investigates effective methods designed for post-quantum ABE with the aim of improving data security and privacy in cloud environments. This survey provides a comprehensive overview of how the performance of algorithms and their

performance can be improved by analyzing the latest developments and new techniques. It highlights important issues, innovations, and the impact of quantum-resistant technologies on protecting cloud-based data from future threats.

Title: Efficient Post-Quantum Attribute-Based Encryption from Rank Metric Codes
Authors: Junqing Gong, Junzuo Lai, Haibo Tian
Abstract: This paper introduce an efficient attribute-based encryption based on rank metric programs suitable for post-quantum cryptography. The scheme leverages the error-correcting capabilities of rank metric programs to ensure security against quantum attacks, while maintaining efficiency suitable for practical deployment in cloud computing environments.
Title: Key Management for Rank Metric Code-Based Cryptosystems
Authors: Pascal Véron, Bertrand Granado, Caroline Fontaine
Abstract: This paper addresses key management issues in rank metric code-based cryptosystems, particularly in the context of attribute-based encryption for cloud computing. It examines efficient key generation, distribution, and revocation mechanisms suitable for practical deployment in large-scale distributed environments.

EXISTING SYSTEM

We present the first efficient, semantically safe, postquantum PEKS algorithm based-on computational degree. This solution all ows cloud servers to use search engines to securely search for the content users' data-needs**.** An existing scheme is protected from keyword guessing attacks, reaction attacks, and key exposure. Check the search results using bloom filter and bloom filter. We implemented this strategy in C++ on a desktop computer. With 256-bit security level encryption, it can perform all necessary steps for keyword searching and valid search terms in just 22.5 milliseconds. Additionally, the public key length for this security level is approximately 5 KB. We found that these techniques are more effective than existing post-quantum techniques.

Disadvantages

- There exists no proposed attribute-based encryption based on rank metric codes method which is not in an existing system.
- There isn’t any scheme which is semantically secure, or simply CPA-secure.

PROPOSED SYSTEM

This system announced the post-quantum attribute encryption (ABE) method based on metric codes that ensure the security and performance of the key length and the encryption and decryption time complexity depending on the number of attributes. Recently, metric codes have received more attention than performance, making Hamming metric codes useful in cryptographic applications. [22], [23], [24]. The superior length and performance of metric codes encourage their use in creating encryption systems (ABE). Our proposal follows the principle of ciphertext character-based encryption (CP-ABE) as it allows the sender to define the access pattern that is effective for shared data. In our proposal, the input model is created

using the Bloom filter. [25]. A Bloom filter is a hash-based data structure used to evaluate the membership of elements in a set. The system starts the process of creating filters and identifying members. Our method uses low-level probabilistic (LRPC) coding, which has the advantage of decision speed and requires little memory to store the parity check.

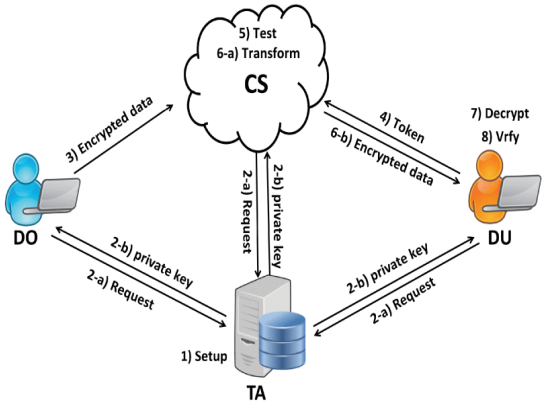

Fig 1. System model architecture

Advantages

• **Post-quantum security in standard model:** We demonstrate the security of our program by considering that solving the optimality problem and ensuring LRPC indistinguishability in the decision problem of LRPC codes is a difficult task. So far, no classical or quantum algorithms have been introduced to address these problems.

• **User revocation:** In the proposed scheme, whenever the user access is revoked, all cloud data matching the user's attributes is re-encrypted so the revoked user cannot access it.

• **Completeness**: Once the data is retrieved from the cloud server, the end-user can efficiently verify if the entire dataset stored in the cloud has been searched. This capability assures that the verification process is both thorough and swift.

• **User privacy**: When a user submits a data search request to the cloud server, it is encrypted using the user's key and then delivered to the cloud server. Therefore, the cloud server conducts the search for the requested data without having access to the user's attributes.

IMPLEMENTATION

Implementation is typically leveraging lattice-based cryptography to ensure post-quantum security. The scheme involves the generation of public parameters, a master secret key, and attribute keys for users. The encryption process encrypts data using a set of attributes, and only users with matching attributes and corresponding keys can decrypt the data. Key components include efficient algorithms for key generation, encryption, and decryption, alongside mechanisms for handling attribute revocation and dynamic policy updates. The implementation focuses on optimizing performance to handle large attribute sets and ensuring scalability and practicality for real-world applications, maintaining robust security against quantum adversaries.

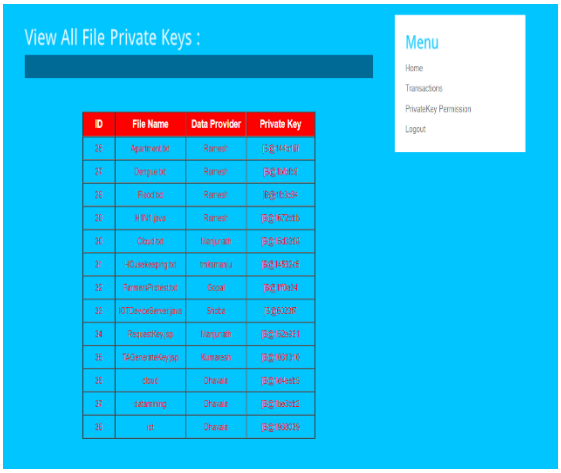

Fig 2. View all file private key

Cloud servers are designed to store information about users, data providers, and related content. They act as a central repository providing access to all document-related information. This includes important details like file ID, file name, and file details, all of which are stored in encrypted form for security purposes. The server also records each document's signature and the date and time it was sent. Additionally, members' information is turned off, providing a complete overview of information management and ownership. By accessing this information, users can clearly understand the characteristics and history of each document. These guidelines promote effective data management and ensure that authorized users have access to all information related to the data.

Fig 3. View all file information in the cloud

RESULTS

Efficient post-quantum attribute-based encryption (ABE) schemes are designed to increase security against threats arising from advances in quantum computing. The main idea of ABE is to provide effective control of access to encrypted data, where decryption depends on user attributes rather than unique keys. In the post-quantum context, these techniques use cryptographic foundations resistant to quantum attacks, such as lattice-based or code-based encryption techniques, to ensure that encryption remains secure despite the great power of quantum computers. The solution includes quantum-resistant algorithms for simplicity and security. It is based on complex mathematical problems, such as those based on crystal lattices, which are considered problematic for quantum computers. The performance of post-quantum ABE schemes is characterized by their ability to manage large-scale devices without major outages, ensuring that the encryption and decryption methods are still valid for real-world use.

Test No	TEST NAME	INPUT GIVEN	EXPECTED RESULT	ACTUAL RESULT	DESCRIPTION
1	Valid Developer Name	a	Accept the input as valid	Passed	Ensure the system accepts a standard name format.
2	Password Requirements	P@ssw0rd!	Password meets complexity requirements.	Passed	Test for a strong password with special characters, numbers, and uppercase letters.
3	Valid Email Address	dhanvika@gmail.com	Accept the input as a valid email address.	Passed	Check for standard email format compliance.
4	Valid Domain name	Android	Accept the input as a valid	Passed	Verify the system accepts a standard name format
5	Valid Location	Bangalore	Accept the input as valid location information.	Passed	Check for acceptance of common location format.

Table: Test case of authentication

Key results from implementing such a scheme include reduced computational overhead, making it feasible for devices with limited processing power, and improved scalability, allowing it to manage numerous attributes and users efficiently. Additionally, the scheme maintains a strong security model, providing assurances that only users with the correct attributes can decrypt the data, thereby protecting sensitive information from unauthorized access even in a post-quantum era. To achieve this, projects often use advanced mathematical techniques such as homomorphic encryption or layered algorithms to improve the balance between security and performance. The result is a strong, future-proof encryption method in quantum technology that protects the confidentiality and integrity of information, leading to major advances in business cryptography.

CONCLUSION

The proposed function uses low-degree polynomial (LRPC) codes, thus achieving high performance and low latency while ensuring security against guesses. Its stability depends on the unknown discrepancy of LRPC and the complexity of the best decision problem in the decision-making process, while classical and quantum algorithms still fail to solve the problem many times. It is also providing resistance to reactive attacks (a type of arbitrary ciphertext attack). The solution also includes the user revocation function: When the user's access rights need to have revoked, the cloud server re-encrypts all data without changing the user's key, speeding up the re-encryption process. In the presented scheme, the user has the ability to verify the correctness and the completeness of data received from the cloud server using Bloom filter. At the 256-bit security level, the key parameter and the execution time of the scheme on the desktop are about 16.5KB and 31.2 ms, respectively. Our implementation results show that the efficiency of the introduced scheme is advanced compared to the existing classical and post quantum ones. We have analysed the security of the presented scheme against a specific type of chosen cipher text attack known as reaction attacks. However, proving security features of the proposed scheme against chosen cipher text attacks remains as a future work.

REFERENCE

[1] S. Choudhury, K. Bhatnagar, and W. Haque, *Public Key Infrastructure Implementation and Design*. Hoboken, NJ, USA: Wiley, 2002.

[2] A. Shamir, ‘‘Identity-based cryptosystems and signature schemes,’’ in *Proc. Workshop Theory Appl. Cryptograph. Techn.* Berlin, Germany: Springer, 1984, pp. 47–53.

[3] D. Boneh and M. Franklin, ‘‘Identity-based encryption from the Weil pairing,’’ in *Annu. Int. Cryptol. Conf.* Berlin, Germany: Springer, 2001, pp. 213–229.

[4] Z. Lu, G. Qu, and Z. Liu, ‘‘A survey on recent advances in vehicular network security, trust, and privacy,’’ *IEEE Trans. Intell. Transp. Syst.*, vol. 20, no. 2, pp. 760–776, Feb. 2019.

[5] A. Sahai and B. Waters, ‘‘Fuzzy identity-based encryption,’’ in *Proc. Annu.*