



More efficient and flexible approach over traditional Cipher text Policy Attribute Based Encryption (CP-ABE) in form of Constant Cipher text Policy Attribute Based Encryption (CCP-ABE) and Attribute Based Broadcast Encryption (ABBE)

Vishal M. Shah^a, Viral V. Kapadia^b

^a Computer Engineering Department, Sardar Vallabhbhai Patel Institute of Technology, Vasad, India

^b Computer Science & Engineering Department, The M S University of Baroda, India

Abstract— *there are many encryption techniques available to encrypt and decrypt the message for secure communication. Ciphertext Policy Attribute-based Encryption (CP-ABE) allows a new type of encryption methodology which suffering from having large cipher text size and this size increases with increasing number of attributes in the system. In this paper, we have shown evolutionary path from CP-ABE to CCP-ABE to Attribute Based Broadcast Encryption (ABBE) and we have also shown the performance Analysis of different encryption techniques and also comparison with other schemes.*

Keywords— *Cipher-text Attribute based Encryption (CP-ABE), Constant Cipher-text Attribute Based Encryption (CCP-ABE), Attribute-based Broadcast Encryption (ABBE), Broadcast Encryption (BE), Identity Based encryption (IBE), Key policy Attribute based Encryption (KP-ABE).*

I. INTRODUCTION

Research in Cipher text Policy Attribute-Based Encryption (CP-ABE) is a very active and live domain in recent years as far as security is concerned. In constructing CP-ABE, an attribute is a descriptive string associated with an entity and each entity may be tagged with multiple attributes [3]. Many entities may share common attributes, which allow message encryptors to specify a secure data access policy by composing multiple attributes through logical operators such as "\AND", "\OR", etc. For decrypting the message, the decryptor's attributes need to satisfy the access policy [3]. These unique features of CP-ABE solutions make them appealing in many systems that require the expressive data access control for a large numbers of users [3]. But with this unique feature, there is a major problem of the existing CP-ABE schemes, linearly increasing cipher text. In the CP-ABE, the size of a ciphertext increases linearly with respect to the number of included attributes. For example, the message size CP-ABE may start at about 650 bytes, and each additional attribute adds about 300 bytes.

In this paper, we propose an evolutionary path from CP-ABE to Constant Ciphertext Policy Attribute Based Encryption (CCP-ABE), which acquires constant-size of cipher text, regardless of the number of attributes in a logical AND data access policy. Besides the encrypted message and encoded access policy, each cipher text only requires 2 bilinear group elements, which are bounded by 300 bytes in total. Moreover, due to the new construction of CCP-ABE, we can prove that the CCP-ABE is CPA secure. To the best of our knowledge, this is the first few such constructions that achieve these properties [3].

Based on presented CCP-ABE, we further provide a new description named as Attribute Based broadcast Encryption (ABBE) that supports efficient Broadcast Encryption (BE). In existing Broadcast Encryption scheme, a broadcaster encrypts a message for a specified set of receivers who are listening on a broadcast channel [3]. Each receiver in the specified set can decrypt the message while all other receivers that are not in the specified set can't decrypt even though they collude together. However, in a system with large number of users, identifying every decryptor may be impractical. For example, to broadcast a message to all IT students, the encryptor needs to query a central directory to get the contact information from every IT student, in which the operation can be very expensive and time consuming. Using ABBE, an encryptor is able to encrypt the broadcasted messages using CCP-ABE, either with or without the information of each intended receiver. For example, Bob can specify the access policy: "IT" AND "Student" to restrict the broadcast message to all IT students without specifying the receivers explicitly. Furthermore, ABBE significantly reduces the storage overhead compared to other BE schemes [3].

CCP-ABE [3]: There is an efficient Constant Cipher text Policy Attribute Based Encryption (CCP-ABE) scheme that can encrypt a message with an AND-gate access policy. Moreover, CCP-ABE supports non-monotonic data access control policy. To the best of our knowledge, this is the First construction that achieves these properties.

ABBE [3]: Based on CCP-ABE, This is an Attribute Based Broadcast Encryption (ABBE) scheme. Compared with existing BE schemes, ABBE is flexible as it uses both descriptive and non-descriptive attributes, which enables a user to specify the decryptors based on different abstraction levels, with or without exact information of intended receivers. Moreover, ABBE demands less storage overhead compared to existing BE schemes. This paper shows that construction of ABBE requires minimal storage to support all the possible user group formations for BE applications.

II. RELATED WORK

In first fully functional Identity Based encryption (IBE) technique, an identity is a 1-to-1 mapped string to each user. A user can incur a private key corresponding to his/her ID from trusted authority and the ID is used as public key [7]. The cipher text encrypted by a particular ID can only be decrypted by the user with corresponding private key, i.e., the encryption is one-to-one [3].

Attribute Based Encryption (ABE) was first proposed as a fuzzy version of IBE, where an identity is viewed as a set of descriptive attributes. There are two types of ABE proposed, Key Policy Attribute Based Encryption (KP-ABE) and Cipher text Policy Attribute Based Encryption (CP-ABE). In KP-ABE, each cipher text is associated with a set of attributes and each user's private key is embedded with an access policy. Decryption is enabled only if the attributes on the cipher text satisfy the access policy of the user's private key. In CP-ABE, each user has a set of attributes that associate with user's private key and each cipher text is encrypted by an access policy. To decrypt the message, the attributes in the user private key need to satisfy the access policy [2].

Although ABE scheme is capable of constructing strong and flexible data access control model, existing ABE schemes suffers from large cipher text size problem. There is another approach, CP-ABE scheme with constant cipher text size. However, their scheme does not support wildcards (or do-not-care) in its access policy, which makes the number of access policy increase exponentially. Moreover, to decrypt a cipher text, the decryptor's attributes needs to be identical to the access policy. So this model is one-to-one and so an access policy is satisfied by one attribute list or ID [3].

ABE can be used as a perfect cryptographic building block to realize Broadcast Encryption (BE) [8]. In BE, a broadcaster encrypts a message for some set of users who are listening to a broadcasting channel and use their private keys to decrypt the message. Compared with traditional one-to-one encryption schemes, BE is very effective. Instead of sending messages encrypted with each individual recipient's public key, the broadcast encryptor broadcast one encrypted message to be decrypted by multiple eligible recipients with their own private keys.

Many times, it is very difficult to have complete receiver list and it is desirable to be able to encrypt without exact knowledge of possible receivers. Also, existing BE schemes can only support simple receiver list. It is hard to support flexible, expressive access control policies. A broadcast encryption with attribute based mechanism, where expressive attribute based access policy replaces the flat receiver list. Also there are CP-ABE and flat-table mechanism to minimize the number of messages and support expressive access policy [3].

Constant Ciphertext Policy Attribute-Based Encryption [3]

In this section, we present CCP-ABE scheme.

The CCP-ABE scheme consists of four fundamental algorithms:

- Setup (k)

The Setup algorithm takes input k as the number of attributes in the system. It returns public key K_{PU} and master key K_M . The public key is used for encryption while the master key is used for private key generation.

- KeyGen ($K_{PU}; K_M; L$)

The KeyGen algorithm takes the public key K_{PU} , the master key K_M and the user's attribute list L as input. It gives private key of the user as output.

- Encrypt ($K_{PU}; W; M$)

The Encrypt algorithm takes the public key K_{PU} , the specified access policy W and the message M as input. The algorithm outputs cipher text CT such that only a user with attribute list satisfying the access policy can decrypt the message. The cipher text also associates the access policy W .

- Decrypt ($K_{PU}; K_{PR}; CT$)

The Decrypt algorithm decrypts the cipher text when the user's attribute list satisfies the access policy specified in the cipher text. It takes the public key K_{PU} , the private key K_{PR} of the user and the cipher text CT as input. It returns the plaintext M if $L \models W$, where L is the user's attribute list and W is the access.

So using CCP-ABE scheme, the cipher text can be abbreviated to a constant size even with increasing number of attributes.

Attribute-Based Broadcast Encryption [3]

Based on CCP-ABE, ABBE is flexible and efficient having cipher text is still constant in size. Compared to existing BE schemes, In ABBE, Encryptor does not need to store a large number of key materials, i.e., public key and private key. By carefully organizing the attributes in the system, the storage overhead of each user can be reduced from $O(N)$ to O

($\log N + m$), where N is the number of users in the system and $m \ll N$ is the number of descriptive attributes in the system. Also in ABBE, an encryptor enjoys the flexibility of encrypting broadcast data using either a specific list of decryptors or an access policy without giving an exact list of decryptors.

ABBE scheme facilitates flexibility of expressive access policy and efficiency of small Ciphertext and public key. Moreover, any group member can encrypt/decrypt the message simultaneously to satisfy the many-to-many secure group communication requirements [1].

III. PERFORMANCE ANALYSIS

In this section, we have shown ABBE performance and compare with other related schemes such as Flat-Table ABE [6], BGW Broadcasting Encryption [4], Non flat-Table ABE, ACP (Access Control Polynomial) [5], etc. This performance analysis is in terms of computational overhead (number of crypto-graphic operations needed in encryption and decryption), communicational overhead (number and size of the messages) and storage overhead (system data stored on users or system center) [3].

Table 1^[3] Performance Analysis – Communication and Storage overhead

	Communication Overhead		Storage Overhead	
	Single Receiver	Multiple Receiver	Center	User
ABBE	$O(1)$	$O(\log N)$	N/A	$O(\log N+m)$
Flat-Table CP-ABE	$O(\log N)$	$O(\log N)$	$O(\log^2 N)/O(N)$	$O(\log N)$
Non-Flat-Table CP-ABE	$O(\log N)$	$O(l * \log N)$	$O(N)$	$O(\log N)$
ACP	$O(N)$	$O(N)$	$O(N)$	$O(1)$

Table 2^[3] Performance analysis - Computational overhead

	Computational Overhead	
	Encryption	Decryption
ABBE	$O(\log N)$	$O(\log N)$
BGW	$O(M)$	$O(M)$
ACP	$O(M^2)$	$O(1)$

Table 1 and table 2, given below, Shows performance analysis in terms of communication-storage overhead and computational overhead respectively where, N – Number of group members, l - Number of leaving members, M – number of receiver [3]. Below two tables shows the comparison of ABBE and different related schemes in terms of communication, storage and computational overhead.

So ABBE significantly reduces the storage and communication overhead to the order of $O(\log N)$, where N is the system size [3]. Due to page limit we haven't included full details of CCP-ABE and ABBE set-up, encryption details as well as decryption details.

IV. CONCLUSION

In this paper, we have shown the evolutionary path from CP-ABE to CCP-ABE to ABBE. We have shown the effectiveness and flexibility of CCP-ABE and ABBE over traditional CP-ABE. We have also shown the performance of different related encryption techniques with ABBE in terms of communication, storage and computational overhead and based on theoretical assumption, we have shown ABBE with many existing BE solutions and we have shown that ABBE achieve better trade-offs between storage and communication overhead.

REFERENCES

- [1] Zhou, Z., Huang, D. 2010. Constructing Efficient Attribute-Based Broadcast Encryption.
- [2] Bethencourt, J., Sahai A. and Waters, B. 2007. Cipher-text Policy Attribute-Based Encryption.
- [3] Zhou, Z. and Huang, D. 2010. On Efficient Ciphertext-Policy Attribute-based Encryption and Broadcast Encryption.
- [4] Boneh, D., Sahai A. and Waters, B. Pages 573-592 2006. Fully Collusion Resistant Traitor Tracing with short Ciphertext and private keys.
- [5] Zou, X., Dai, Y. and Bertino, E. Pages 538-546 2008. A Practical and Flexible Key Management Mechanism for Trusted Collaborative Computing.
- [6] Cheung, L., Cooley, J., Khazan, R., and Newport, C. 2007. Collusion Resistant group key management using Attribute-based Encryption.
- [7] Boneh, D. and Waters, B. 2003. Identity-Based Encryption from the Weil pairing.
- [8] Fiat, A. and Naor, M. 1994. Broadcast Encryption, advances in Cryptography – Crypto93.