International journal of Computer Science & Network Solutions
http://www.ijcsns.com

Nov.2018 -Volume 6.No.3
ISSN 2345-3397

ABE and PBE Encryption Methods: Strengths and Weaknesses

Komeil Safikhani Mahmoodzadeh[1], Seyyed Mohammad Safi[2,*]

[1] *Department of Computer Engineering, Ahvaz Branch, Islamic Azad University, Ahvaz, Iran*

komeil.safikhani@yahoo.com

[2,*] *Department of Computer Engineering, Ahvaz Branch, Islamic Azad University, Ahvaz, Iran*

m.safi85@gmail.com

Abstract

Nowadays, encryption is used in order to determine the access policy and data security. In PBE[1] encryption, the publisher sends a message to a subset of users with access to the broadcasted data, so that only the desired users can decrypt the data and other users cannot access the data even with colliding their key and information. In ABE[2] encryption, a set of attributes is used as the main index to generate the private key. This encryption system can well provide the appropriate access control in environments such as Cloud Control. In this paper, we attempt to explain the strengths and weaknesses of the two ABE and PBE methods, and examine the pioneer methods for their implementation.

Keywords: broadcast encryption, Attribute base encryption, public broadcast encryption

I. Introduction

Encryption methods have always been altered and improved over time. In total, in terms of application, the encryption methods can be divided into four general categories: one-one, many-to-one, one-to-many and many-to-many.

Symmetric encryption is one of the encryption methods used in one-to-one connections. In this encryption method, the encryption key and decryption key are the same, which makes it inappropriate for multiple connections. Nevertheless, in asymmetric encryption methods like public key encryption (PKE[3]) methods, due to differences in decryption and encryption keys, they can be used in many-to-one connections. Due to the creation of too much overhead in key management or the need for multiple encrypted copies of the same data with different keys, one-to-one connections cannot provide fine-grained access control.

In 1979, Shamir (1979) came Up with an approach to share a secret known as the threshold scheme (k, n), in which the secret D was divided into k segments. The reconstruct of secret was possible if all k segments or more were known. In 1984, Shamir (1984) introduced the new

[1] Public Broadcast Encryption
[2] Attribute Base Encryption
[3] Public Key Encryption

Nov.2018 -Volume 6.No.3
ISSN 2345-3397

encryption scheme called Identity base encryption IBE[4] allowing both users to safely communicate to each other without exchanging the public key and through using the unique identity of the recipient such as the IP address. Without exchanging keys, the key leakage risk is minimized.

In 1993, Fiat et al. (1993) proposed a scheme for encryption of the broadcasted data whose purpose was to broadcast information for a subset of a group of people listening to the broadcast channel; so that people outside the set could not decrypt the data even with collusion. Then, D.Boneh et al. (2005) proposed a BDHE-based method with sufficient security and cipher text of constant size. In this method, unlike IBE, ordinary indexes were used to make the group description easier and less expensive.

In the same years, Sahai et al. (2005) suggested the first ABE scheme that uses the IBE and secret sharing idea to generate threshold access control. ABE well combines access control and encryption.

ABE also makes it easier to manage keys through benefiting from attributes combined into encryption parts. The ABE fine-grained access control scheme was proposed by Goyal et al. (2006) and Bethencourt et al. (2007) they added the access control fine-grain features to the attributes based encryption.

In this paper, we investigate the features and objectives of the two PBE and ABE encryption methods proposed in the papers and mathematically compare them.

II. Background

In this section, the mathematical principles improving the PBE and ABE broadcast encryption methods will be discussed, and then the various methods based on these principles will be introduced.

A. Bilinear Map

After the innovation of IBE system by Shamir (1985), key generation for IBE systems remained a challenge. None of the current encryption systems, including the RSA and the Diffie-Hellman protocol, could easily deform to the IBE system. Since then, many achievements have been made having bottleneck due to security requirements. The most efficient achievement occurred when discovering the bilinear mapping. Compared to the previous achievements, bilinear mapping was a precise and safe in making the efficient keys (Antoine 2009). The bilinear map is as follows:

1) Bilinearity:$\left(g_1^a, g_2^b\right) = e(g_1, g_2)^{ab}$. $g_1$and g_2 are the generators of $\mathbb{G}_1$ and $\mathbb{G}_2$ respectively, $a, b \in Z$. (Note that $\mathbb{G}_1$ and $\mathbb{G}_2$ is called the source group, and $\mathbb{G}_\mathrm{T}$ is the target group. When $\mathbb{G}_1 = \mathbb{G}_2$, we call it asymmetric bilinear map.)
2) Computability: The bilinear map e is efficiently computable for any pairs given by $\mathbb{G}_1 \times \mathbb{G}_2$.
3) Non-degeneracy:$e(g_1, g_2)^{ab} \neq 1$. It means the map does not send all pairs in $\mathbb{G}_1 \times \mathbb{G}_2$ to the identity in $\mathbb{G}_\mathrm{T}$ (Boneh et al. 2001).

[4] Identity base Encryption

Nov.2018 -Volume 6.No.3
ISSN 2345-3397

The bilinear maps following these three items are called admissible bilinear maps, actually used in IBE, ABE, and PBE systems. Generally, $\mathbb{G}_1$ and $\mathbb{G}_2$ are elliptic curves defined on finite fields F_q and $\mathbb{G}_T$ is in the finite fields.

Bilinear pairing: Bilinear pairing, maps a pair of points from the source group to the target group. Based on the definition, bilinear map is a specific algorithm of e. In fact, in pairing-based encryption, bilinear map calculates the pair of public and private keys.

B. Security Assumption of Bilinear Map

It is believed that bilinear map is the fundamental solution for IBE, ABE and PBE schemes. Bilinear map security is based on computational Diffie-Hellman (CDH) assumption known as an NP-hard problem. (Boneh et al. 2003) Boneh et al. have proven that for finite groups, if the CDH assumption is true in $\mathbb{G}$, the bilinear mapping will be highly secure. The CDH assumption is as follows: For any cyclic group $\mathbb{G}$ with order q and a randomly chosen generator g, given tuple$\{(g, g^a, g^b) | \, a, b \in Z\}$, computing the value of g^{ab} is called the Diffie-Hellman problem. Anyway, the g^{ab} value is difficult to be computed, since the calculation of the discrete logarithm of a generator g is hard.
Bilinear map security is also based on a CDH extension; this assumption is called the Bilinear-Diffie-Hellman (BDH), which explains that for any given tuple$\{(g, g^a, g^b, g^c) | \, a, b, c \in Z\}$, it is difficult to calculate the pair $e(g, g)^{abc}$ and it is called the Bilinear Diffie-Hellman Problem.

C. BDHE

Security of PBE systems is based on a complexity assumption called the bilinear Diffie-Hellman Exponent assumption (BDHE). This assumption was previously introduced in (Boneh et al. 2005a).
Let $\mathbb{G}$ be a bilinear group of prime order *p*. The ℓ -BDHE problem in $\mathbb{G}$ isstated as follows: (1)
a vector of 2 ℓ + 1 elements.

$$\left(h, g, g^{\alpha}, g^{(\alpha^2)}, \ldots, g^{(\alpha^{\ell})}, g^{(\alpha^{\ell+2})}, \ldots, g^{(\alpha^{2\ell})}\right) \in \mathbb{G}^{2\ell+1}$$

as input, output $e(g, h)^{(\alpha^{\ell+1})} \in \mathbb{G}_1$. Note that the input vector is missing the term $g^{(\alpha^{\ell+1})}$ so that the bilinear map seems to be of little help in computing therequired $e(g, h)^{(\alpha^{\ell+1})}$ (Boneh et al. 2005b).

III. Schemes Overview

A. PBE Broadcast Encryption

As its name implies, broadcast encryption is used to securely broadcast data among a group of people. Fiat and Naor (1993) were among the first researchers conducting some studies on broadcast encryption. In their proposed scheme, the data were broadcast for n user in such a way to be resistant to the collusion of t users. The size of cipher text was$O(t \, log^2 \, tlog \, n)$.

Nov.2018 -Volume 6.No.3
ISSN 2345-3397

Naor et al. presented another broadcast scheme which was completely resistant to collusion and was appropriate for all users other than a small group that was revoked. In this scheme, the data were accessible to all recipients and a small part of users with compromised keys could not access the data. The size of the header produced for this scheme for $n-r$ users was $O(r)$ element and the private key size for decryption was $O(log^2 n)$. Then, later on the private key size was reduced to $O(log\ n)$ by Halevy (2002). Dodis and Fazio (2002) developed the public key in Naor's scheme (1993) and achieved a public key dissemination system with a small public key.
Noar and Pinkas (2000) presented a scheme which was appropriate for large groups of users and could revoke $r < t$ users for a fixed$t$. The size of the ciphertext was $O(t)$ and the private keys had fixed sizes. Wallner et al. (1997) and Wong (1998) independently discovered the logicl-key-hierachy scheme for the key management multicast group. In this scheme, the task status should be stable and remain connected to the system for receiving key-update messages. Then, Canetti et al. (1999) improved the parameters in Wallner's scheme.
Finally broadcast encryption completed by Boneh et al. (2005). Using bilinear mappings and BDHE assumption. That broadcast encryption system is composed of three random algorithms.

Setup(n)**.** Takes as input the number of receivers$n$. It outputs n private keys $d_1, \dots, d_n$ and a public key PK.

Encrypt$(\boldsymbol{S}.\boldsymbol{PK})$**.** Takes as input a subset $S \subseteq \{1, \dots, n\}$, and a public key PK. It outputs a pair (Hdr, K) where Hdr is called the header and $K \in \mathcal{K}$ is a message encryption key chosen from a finite key set $\mathcal{K}$. Let M be a message to be broadcast that should be decipherable precisely by the receivers in S. Let C_M be the encryption of Munder the symmetric key K. The broadcast consists of (S, Hdr, C_M). The pair (S, Hdr) is often called the full header and C_M is often called the broadcast body.

Decrypt(S, i, d_i, Hdr, PK). Takes as input a subset $S \subseteq \{1, \dots, n\}$, a user id $i \in \{1, \dots, n\}$ and the private key d_i for user i, a header Hdr, and the public key PK. If $i \in S$, then the algorithm outputs a message encryption key $K \in \mathcal{K}$. Intuitively, user$i$can then use $K$to decrypt the broadcast body C_M and obtain the message body M.
the system be correct, namely that for all subsets $S \subseteq \{1, \dots, n\}$and all $i \in S$, if: $(PK, (d_1, \dots, d_n)) \xleftarrow{R}$*Setup*$(n)$ and $(\text{Hdr}, K) \xleftarrow{R}$*Encrypt* (S, PK)
then *Decrypt* $(S, i, d_i, \text{Hdr}, PK) = K$. (Boneh et al. 2005b)

Subsequently, vast changes were made to the method. One of the changes allowing the user to freely add and remove his friends was proposed by Malek et al. (2012). In this encryption method, the user performs encryption for a group of users with his own key, and only the users considered as client can operate data decryption with their own private key and the parameters available in the public key along with the encryption header. In this cryptography, there is no need to change the key by the CA to restrict the contact person, and the user can simply hide the key from the person being pushed out by removing the person from the header.

B. ABE Encryption

Nov.2018 -Volume 6.No.3
ISSN 2345-3397

Many schemes have been so far proposed. As an encryption system, ABE has to provide reliability over data. Since ABE has internal access control, user authentication and deletion must be performed by a trusted authority. In addition, all ABE systems have to be resistant to key collision attacks and prevent user's collaboration to access data that they are not authorized to access it. One of the ABE foundations is threshold policy access control. In the threshold policy access control, a set of descriptive attributes is employed to tag the user and the cipher text. A user with a set of attributes W can decrypt the cipher text with the W' tag only if W and W' have k common attributes. This idea is originated from IBE (Shamir et al. 1984); so that a string of characters is considered as an identity. The threshold (W, k) provides error tolerance to the coarse-grained access control, and it is practically used in encryption by means of biometrics using general information as input. Threshold access control in fuzzy IBE is based on polynomial interpolation. In polynomial system, each user chooses from $k-1$ level $q(x) = a_0 + a_1 + \cdots + a_{k-1}x^{k-1}$ to interact with the private key and combine attributes in the polynomial. If the user's private key matches more than k attributes of the cipher text, it can encrypt the cipher text, which is fully different from the common original secret share scheme (Shamir et al. 1979). Since in the ABE system the user is related to the random polynomial, several users cannot effectively combine their attributes and collide with each other.

Compared to the threshold policy, the key policy can provide fine-grained access control. In the key policy, the cipher text is tagged with a set of attributes, and the private key interacts with a more general access control structure. One of the faults of the key policy is that the access policies are in the user's private key. Moreover, the data owner has to trust the key distributor and storage server to save all expressive access controls in a plain-text. In 2006, Goyal et al. proposed the first key policy scheme (KP-ABE) that was considered very much (Qiao, et al. 2014).

As the key-policy, cipher text-policy is another fine-grained access control. In the cipher text-policy, attributes interact with the key; while in cipher text-policy the access control is in the cipher text. In this way, the data owner can determine who can perform decryption. Furthermore, if in some place, there the policies must be continuously changed, the cipher text-policy can be more flexible, since the data owner only needs to update the access structure in the cipher text. This feature brings Cipher text-policy closer to role based access control (RBAC). In the threshold and key policy access controls, resistance to collision is ensured by a secret sharing scheme (SSS) with a random polynomial for each private key. Anyway, in cipher text-policy, SSS will no longer operate, since the access structure has moved away from the key and only the ciphertext has the attributes. The cipher text policy should employ a two-level random masking method, which uses groups with efficiently computable bilinear map in order to randomize the private key. This extra step make the system more complicated and damages the performance (Qiao, et al. 2014).

Bethencourt et al. (2007) introduced the new ciphertext-policy scheme (CP-ABE) that was improved by Waters (2011). Several ABE schemes have used ciphertext-policy, due to the high efficiency of this feature.

IV. Conclusion

What differentiates the ABE and PBE encryption methods is their goal of encryption. Nevertheless, to achieve these goals, the methods use different mathematics. For instance, as

Nov.2018 -Volume 6.No.3
ISSN 2345-3397

previously mentioned, in ABE, it is necessary to divide a secret into several segments in order to achieve a threshold access control. This is possible by using the Shamir's method as well as polynomials; while in PBE method, the keys must be combined to make the header from which, the authorized users can obtain the session key. The security complexity of mathematics used to this end is based on the bilinear Diffie-Hellman exponent assumption (BDHE). Making the header in PBE method leads to not requiring changing the other user's key in order to retrieve the key, and only the header is created in such a way that only the authorized users can retrieve that session key. The keys are calculated once and they will be independently used many times. Encryption is done without the need for a third party to split the key.

Due to different approaches and attitudes, really, a good measure cannot be found to assess these two schemes. The multiplicity of attributes in ABE enlarges the ciphertext as well as complicating the computation process for encryption. Since there is no attribute assignment in PBE, the ciphertext will have a constant length. Concerning PBE, it is worth to note the need for a public key in the encryption and decryption processes, which will linearly grow with increased number of users. This issue makes the broadcast public key encryption non-optimal, even by considering that the length of the ciphertext length is constant. Finally, it must be stated that the two encryption methods are appropriate for the group encrypted communication due to their one-to-many feature. However, the cost of this achievement is greater computing and larger ciphertext that makes these methods inappropriate for small groups.

References:

I. Antoine, J. (2009). Introduction to identity-based cryptography. *Identity-Based Cryptography, 2*, 1.

II. Bethencourt, J., Sahai, A., & Waters, B. (2007). Ciphertext-policy attribute-based encryption. *Security and Privacy, 2007. SP'07. IEEE Symposium on* (pp. 321-334). IEEE.

III. Boneh, D., & Franklin, M. (2001). Identity-based encryption from the Weil pairing. *Annual international cryptology conference* (pp. 213-229). Springer.

IV. Boneh, D., Gentry, C., & Waters, B. (2005a). Collusion resistant broadcast encryption with short ciphertexts and private keys. *Annual International Cryptology Conference* (pp. 258-275). Springer.

V. Boneh, D., Boyen, X., & Goh, E.-J. (2005b). Hierarchical identity based encryption with constant size ciphertext. *Annual International Conference on the Theory and Applications of Cryptographic Techniques* (pp. 440-456). Springer.

VI. Boneh, D., Mironov, I., & Shoup, V. (2003). A secure signature scheme from bilinear maps. *Cryptographers' Track at the RSA Conference* (pp. 98-110). Springer.

VII. Canetti, R., Malkin, T., & Nissim, K. (1999). Efficient communication-storage tradeoffs for multicast encryption. *International conference on the theory and applications of cryptographic techniques* (pp. 459-474). Springer.

VIII. Dodis, Y., & Fazio, N. (2002). Public key broadcast encryption for stateless receivers. *ACM Workshop on Digital Rights Management* (pp. 61-80). Springer.

IX. Fiat, A., & Naor, M. (1993). Broadcast encryption. *Annual International Cryptology Conference* (pp. 480-491). Springer.

Nov.2018 -Volume 6.No.3
ISSN 2345-3397

X. Goyal, V., Pandey, O., Sahai, A., & Waters, B. (2006). Attribute-based encryption for fine-grained access control of encrypted data. *Proceedings of the 13th ACM conference on Computer and communications security* (pp. 89-98). Acm.

XI. Halevy, D., & Shamir, A. (2002). The LSD broadcast encryption scheme. *Annual International Cryptology Conference* (pp. 47-60). Springer.

XII. Malek, B., & Miri, A. (2012). Adaptively Secure Broadcast Encryption with Short Ciphertexts. *IJ Network Security*, *14*(2), 71-79.

XIII. Naor, D., Naor, M., & Lotspiech, J. (2001). Revocation and tracing schemes for stateless receivers. *Annual International Cryptology Conference* (pp. 41-62). Springer.

XIV. Naor, M., & Pinkas, B. (2000). Efficient trace and revoke schemes. *International Conference on Financial Cryptography* (pp. 1-20). Springer.

XV. Qiao, Z., Liang, S., Davis, S., & Jiang, H. (2014). Survey of attribute based encryption. *2014 15th IEEE/ACIS International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD)* (pp. 1-6). IEEE.

XVI. Sahai, A., & Waters, B. (2005). Fuzzy identity-based encryption. *Annual International Conference on the Theory and Applications of Cryptographic Techniques* (pp. 457-473). Springer.

XVII. Shamir, A. (1979). How to share a secret. *Communications of the ACM*, *22*(11), 612-613.

XVIII. Shamir, A. (1984). Identity-based cryptosystems and signature schemes. *Workshop on the theory and application of cryptographic techniques* (pp. 47-53). Springer.

XIX. Wallner, D., Harder, E., & Agee, R. (1999). *Key management for multicast: Issues and architectures.*

XX. Waters, B. (2011). Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization. *International Workshop on Public Key Cryptography* (pp. 53-70). Springer.

XXI. Wong, C., Gouda, M., & Lam, S. (1998). Secure group communications using key graphs. *ACM SIGCOMM Computer Communication Review.28*, pp. 68-79. ACM.