Security Weaknesses of an "Anonymous Attribute Based Encryption" appeared in ASIACCS'13

Payal Chaudhari, Manik Lal Das, Anish Mathuria

DA-IICT, Gandhinagar, India
{payal_chaudhari, maniklal_das, anish_mathuria}@daiict.ac.in

Abstract

Attribute-based Encryption (ABE) has found enormous application in fine-grained access control of shared data, particularly in public cloud. In 2013, Zhang *et al* proposed a scheme called match-then-decrypt [1], where before running the decryption algorithm the user requires to perform a match operation with attribute(s) that provides the required information to identify whether a particular user is the intended recipient for the ciphertext. As in [1], the match-then-decrypt operation saves the computational cost at the receiver and the scheme supports receivers' anonymity. In this paper, we show that Zhang *et al*'s scheme [1] does not support receivers' anonymity. Any legitimate user or an adversary can successfully check whether an attribute is required in the matching phase, in turn, can reveal the receivers' identity from the attribute.

Keywords. Attribute Based Encryption, Anonymity, Anonymous Encryption, Bilinear Pairing.

1 Introduction

With the advancement of cloud computing vast volume of data including sensitive data is outsourced and stored in public clouds. As a result, securing data from unauthorized access is a challenging task, which has recently got attraction from research community. In other words, the cloud system must assure users about the privacy and security of their data, and at the same time, making data available to authorized users.

Attribute-based encryption (ABE) [2], [3] has been considered as a highly capable public key primitive for implementing fine-grained access control system, where differential access rights can be assigned to individual users. There are two kinds of ABE – *key-policy based ABE* (KP-ABE) [2], [3] and *ciphertext-policy based ABE* (CP-ABE) [4]. In KP-ABE each ciphertext is labeled by the encryptor with a set of descriptive attributes and the private key of a user is associated with an access structure that specifies which type of ciphertext the key can decrypt. In CP-ABE a user is identified by a set of attributes which are

included in his private key and the encryptor can decide the access structure while generating the ciphertext that the user can decrypt with his private key. Our discussion in this paper is limited to CP-ABE.

ABE schemes [3], [4] require to send the information about the necessary attributes of receiver along with the ciphertext. From the set of attributes one can identify who is the target receiver, which costs the receiver's privacy. Furthermore, by knowing the receiver's identity, one can guess the nature/meaning of the plaintext (e.g., the plaintext could be examination related if the receiver is a student). Therefore, protecting user's privacy in access control system is an essential requirement in many real applications. In order to meet this requirement, a few anonymous ABE (AABE) schemes have appeared in [5], [6], [7], [8]. In anonymous CP-ABE, access policy is hidden in the ciphertext. A user requires to decrypt a ciphertext using the secret key belongs to his attributes. If his secret key matches with the access policy then the user can successfully decrypt the ciphertext. If the attribute set associated with the secret key does not match with the access policy, then the user cannot decrypt and guess what access policy was specified by the sender. In most of AABE schemes [5], [6], [7], [8] the user is required to run the whole decryption algorithm to verify if he is the intended receiver for the ciphertext, which creates a large overhead on the user because the decryption procedure requires a number of expensive bilinear pairings operations. In 2013, Zhang *et al* [1] proposed an efficient mechanism to address this issue by introducing a matching phase before decryption process. Before decryption the user requires to perform the match procedure using his secret key components to check if he is the intended recipient of the ciphertext.

We found that the scheme proposed in [1] does not provide receiver's anonymity, which is the main claim of the scheme. We show that how one (an attacker or any legitimate user of the system) can find if an attribute is included in the access policy of the ciphertext, in turn, can deduce the identity/attribute of the target receiver of the ciphertext.

The remainder of the paper is organized as follows. Section 2 gives some preliminaries. Section 3 reviews Zhang *et al*'s scheme. Section 4 presents the security flaws of Zhang *et al*'s scheme. We conclude the paper in Section 5.

2 Preliminaries

2.1 Bilinear Mapping

Let G_1 and G_2 be two multiplicative cyclic groups of prime order p. Let g be a generator of G_1. We say G_1 has an admissible bilinear map, $e : G_1 \times G_1 \rightarrow G_2$, into G_2 if e satisfies the following properties:

- Bilinearity: for all $u, v \in G_1$ and $a, b \in Z_p$, $e(u^a, v^b) = e(u, v)^{ab}$.
- Non-degeneracy: $e(g, g) \neq 1$.

- Computable: e is efficiently computable.

2.2 Complexity assumption

Discrete Logarithm Problem (DLP). Let p and q be two prime numbers such that $q|(p-1)$. Let g be a random element with order $q \in Z_p^*$, and y be a random element generated by g. Then, for any probabilistic polynomial time algorithm $\mathcal{B}$, the probability $\Pr[\mathcal{B}(p,q,g,y) = x$— such that $g^x = y \bmod p]$ is a negligible advantage ϵ.

Decisional Bilinear Diffie-Hellman (BDH) Assumption. Let $a, b, c, r \in_R Z_p$ be chosen at random and g be a generator of G_1. The decisional BDH assumption is that no probabilistic polynomial-time algorithm $\mathcal{B}$ can distinguish the tuple ($A = g^a$, $B = g^b$, C = g^c; $e(g,g)^{abc}$) from the tuple ($A = g^a$, $B = g^b$, C = g^c, $e(g,g)^r$) with more than a negligible advantage ϵ.

The advantage of $\mathcal{B}$ is $\Pr[\mathcal{B}(A, B, C, e(g,g)^{abc}) = 0]$ - $\Pr[\mathcal{B}(A, B, C, e(g,g)^r) = 0] = \epsilon$.

Decisional Linear (D-Linear) Assumption. Let z_1, z_2, z_3,z_4, $r \in Z_p$ be chosen at random and g be a generator of G_1. We say that the D-Linear assumption holds in G if no probabilistic polynomial-time algorithm $\mathcal{B}$ can distinguish the tuple $(g, Z_1{=}g^{z_1}, Z_2{=}g^{z_2}, Z_3{=}g^{z_1 z_3}, Z_4{=}g^{z_2 z_4}, T{=}g^{z_3+z_4})$ from the tuple $(g, Z_1{=}g^{z_1}, Z_2{=}g^{z_2}, Z_3{=}g^{z_1 z_3}, Z_4{=}g^{z_2 z_4}, T{=}g^r)$ with non-negligible advantage ϵ.

The advantage of $\mathcal{B}$ is $\Pr[\mathcal{B}(Z_1,Z_2,Z_3,Z_4, e(g,g)^{z_3+z_4}) = 0]$ - $\Pr[\mathcal{B}(Z_1,Z_2,Z_3,Z_4,e(g,g)^r) = 0] = \epsilon$.

2.3 Access Structure

Let there are n attributes in the universe and each attribute i for all $1 \leq i \leq n$ has value set $V_i = \{v_{i,1}, v_{i,2}, \cdots, v_{i,n_i}\}$. $L = [L_1, L_2, \cdots, L_n]$ is an attribute list, where each L_i represents one value from the value set of attribute i. A ciphertext policy $W = [W_1, W_2, \cdots, W_n]$, where each W_i represents the set of permissible values of an attribute i in order to decrypt the ciphertext or * in case of don't care attribute values. An access structure W is a rule that returns 1 when given a set L of attributes if L matches with W else it returns 0. An attribute list L satisfies W, if $L_i \in W_i$ or $W_i = *$ for all $1 \leq i \leq n$.

3 Zhang et al's Scheme

3.1 The Scheme Structure

The anonymous CP-ABE scheme proposed by Zhang et al consists of four algorithms : **Setup, KeyGen, Encrypt**, and **Decrypt**.

- Setup(1^λ) $\rightarrow$ (PK, MK): The setup algorithm is run by the Attribute Center, a trusted authority. On input a security parameter λ it returns

the system public key PK which is distributed to users, and the master key MK which is kept secret.

- KeyGen(PK, MK, L) $\rightarrow SK_L$: This algorithm is also run by the Attribute Center. On input the public key PK, the master key MK and an attribute List L, it outputs SK_L as the secret key associated with the attribute list L.

- Encrypt(PK, M, W) $\rightarrow CT_W$: This is a probabilistic algorithm that takes input as the public key PK, a message M, and a ciphertext policy W, and it outputs the ciphertext CT_W with respect to W.

- Decrypt(PK, CT_W, SK_L) $\rightarrow M$ or $\perp$: The decryption algorithm is deterministic and it involves two phases, attribute matching detection and decryption algorithm. When a user inputs the system public key PK, a ciphertext CT_W and a secret key SK_L associated with L, the decryption phase proceeds as follows :

  1. Matching Phase: If the attribute list L associated with SK_L matches with the ciphertext policy W of CT_W then it invokes the Decryption algorithm; else, it returns $\perp$.
  2. Decryption algorithm: The decryption algorithm returns the message M.

3.2 Detailed Scheme

- **Setup**(1^λ): Let G_1, G_2 be cyclic multiplicative groups of prime order p, and $e : G_1 \times G_1 \rightarrow G_2$ be a bilinear map. $H : \{0,1\}^* \rightarrow G_1$ is a function that takes a string as input and outputs a member in G_1. The attribute center chooses $y \in_R Z_p$, g, g_1, $g_2 \in_R G_1$, and computes $Y = e(g_1, g_2)^y$. The system public key is $PK = \langle g, g_1, g_2, Y \rangle$ The master key MK is a pair $\langle y \rangle$.

- **KeyGen**(PK, MK, L): Let L=$[L_1, L_2, \cdots, L_n]$ be the attribute list for the user who requires a secret key. The attribute center chooses $r_1, r_2, \cdots, r_{n-1} \in_R Z_p$ and computes $r_n = y - \sum_{i=1}^{n-1} r_i \ mod\ p$. Then, the attribute center chooses $r \in_R Z_p$ and $\{\hat{r_i}, \lambda_i, \hat{\lambda_i} \in_R Z_p\}_{1 \le i \le n}$, sets $\hat{r} = \sum_{i=1}^{n} \hat{r_i}$ and computes $[\hat{D_0}, D_{\Delta,0}] = [g_2^{y-\hat{r}}, g_1^r]$. For $1 \le i \le n$, the attribute center computes

  $[D_{\Delta,i}, D_{i,0}, D_{i,1}, \hat{D}_{i,0}, \hat{D}_{i,1}] =$

  $[g_2^{\hat{r_i}} H(i \| v_{i,k_i})^r, g_2^{\lambda_i}, g_1^{r_i} H(0 \| i \| v_{i,k_i})^{\lambda_i}, g_1^{\hat{\lambda}_i}, g_2^{r_i} H(1 \| i \| v_{i,k_i})^{\hat{\lambda}_i}]$, where $L_i = v_{i,k_i}$

  The secret key is

  $SK_L = \langle \hat{D_0}, D_{\Delta,0}, \{D_{\Delta,i}, D_{i,0}, D_{i,1}, \hat{D}_{i,0}, \hat{D}_{i,1}\}_{1 \le i \le n} \rangle$

- **Encrypt**(PK, M, W): For encryption of a message M with respect to access control policy W, data owner selects s, $s\prime$, $s\prime\prime \in_R Z_p$ and computes $\tilde{C} = MY^s$, $C_\Delta = e(g,g)^s Y^{s\prime}, C_0 = g^s, \hat{C}_0 = g_1^{s\prime}, C_1 = g_2^{s\prime\prime}, \hat{C}_1 = g_1^{s-s\prime\prime}$. Then, for $1 \leq i \leq n$ and $1 \leq j \leq n_i$ the encryptor computes $[C_{i,j,\Delta}, C_{i,j,0}, \hat{C}_{i,j,0}]$ as follows:
If $v_{i,j} \in W_i$ then $[C_{i,j,\Delta}, C_{i,j,0}, \hat{C}_{i,j,0}] =$
$[H(i\|v_{i,j})^{s\prime}, H(0\|i\|v_{i,j})^{s\prime\prime}, H(1\|i\|v_{i,j})^{s-s\prime\prime}]$
else, if $v_{i,j} \notin W_i$ then $[C_{i,j,\Delta}, C_{i,j,0}, \hat{C}_{i,j,0}]$ will be random elements.
The encryptor prepares $CT_W =$
$\langle C_\Delta, C_0, \hat{C}_0, \tilde{C}, C_1, \hat{C}_1, \{\{C_{i,j,\Delta}, C_{i,j,0}, \hat{C}_{i,j,0}\}_{1\leq j\leq n_i}\}_{1\leq i\leq n}\rangle$

- **Decrypt**(PK, CT_W, SK_L): A user checks first the matching phase and if it matches then he decrypts the ciphertext CT_W using his secret key SK_L as follows:

  1. Matching Phase: The user checks if his attributes L satisfies W or not by checking the following equality.
  $$\frac{C_\Delta}{e(g,C_0)} = \frac{e(\hat{C}_0, \hat{D}_0 \prod_{i=1}^n D_{\Delta,i})}{e(\prod_{i=1}^n C_{i,j,\Delta}, D_{\Delta,0})}$$
  If the equality does not hold then the decryption procedure is aborted; else, the Decryption algorithm is initiated.
  2. Decryption algorithm: The user recovers message M using the following computation
  $$M = \frac{\tilde{C} \prod_{i=1}^n e(C_{i,j,0}, D_{i,0}) e(\hat{C}_{i,j,0}, \hat{D}_{i,0})}{\prod_{i=1}^n e(C_1, D_{i,1}) e(\hat{C}_1, \hat{D}_{i,1})}$$

Correctness:

For matching phase :

$$\begin{aligned}
&\frac{e(\hat{C}_0, \hat{D}_0 \prod_{i=1}^n D_{\Delta,i})}{e(\prod_{i=1}^n C_{i,j,\Delta}, D_{\Delta,0})} \\
=&\frac{e(g_1^{s\prime}, g_2^{y-\hat{r}} \prod_{i=1}^n g_2^{\hat{r}_i} H(i\|v_{i,k_i})^r)}{e(\prod_{i=1}^n H(i\|v_{i,j})^{s\prime}, g_1^r)} \\
=&e(g_1^{s\prime}, g_2^{y-\hat{r}} \prod_{i=1}^n g_2^{\hat{r}_i}) \\
=&e(g_1, g_2)^{ys\prime} \\
=&\frac{C_\Delta}{e(g,C_0)}
\end{aligned}$$

For Decryption phase :

$$\frac{\tilde{C}\prod_{i=1}^{n} e(C_{i,j,0}, D_{i,0})e(\hat{C}_{i,j,0}, \hat{D}_{i,0})}{\prod_{i=1}^{n} e(C_1, D_{i,1})e(\hat{C}_1, \hat{D}_{i,1})}$$

$$= \frac{MY^s \prod_{i=1}^{n} e(H(0\|i\|v_{i,j})^{s''}, g_2^{\lambda_i})e(H(1\|i\|v_{i,j})^{s-s''}, g_1^{\hat{\lambda}_i})}{\prod_{i=1}^{n} e(g_2^{s''}, g_1^{r_i}H(0\|i\|v_{i,k_i})^{\lambda_i})e(g_1^{s-s''}, g_2^{r_i}H(1\|i\|v_{i,k_i})^{\hat{\lambda}_i})}$$

$$= \frac{MY^s}{\prod_{i=1}^{n} e(g_2^{s''}, g_1^{r_i})e(g_1^{s-s''}, g_2^{r_i})}$$

$$= \frac{Me(g_1, g_2)^{ys}}{e(g_1, g_2)^{\sum_{i=1}^{n} r_i s}}$$

$$= \frac{Me(g_1, g_2)^{ys}}{e(g_1, g_2)^{ys}}$$

$$= M$$

4 Security Flaws in Zhang et al's Scheme

The scheme in [1] has claimed that it provides receiver's anonymity, and the ciphertext does not disclose the identity of the receiver. The scheme has also argued that if any receiver succeeds in decryption of a message, s/he will not be able to identify who else can decrypt the same ciphertext. We show that the scheme [1] does not provide receiver's anonymity. In particular, the parameters used in the *matching phase* allow the user to deduce the target receiver's information.

We assume that any user inside or outside the system has knowledge of all attributes used in the system. The adversary or any legitimate user can successfully check if a particular attribute is included in ciphertext. The attributes which allow the attacker to make the attack successful are $\hat{C}_0$ and $\{\{C_{i,j,\Delta}\}_{1\leq j\leq n_i}\}_{1\leq i\leq n}$. To check whether an attribute $v_{i,j}$ is included in ciphertext the adversary calculates $D'_{\Delta,i,j} = H(i\|v_{i,j})$. Next the adversary checks if equation 1 holds for an attribute $v_{i,j}$.

$$e(\hat{C}_0, D'_{\Delta,i,j}) = e(C_{i,j,\Delta}, g_1) \tag{1}$$

If the above equality holds true then the adversary can conclude that the attribute used in the equation is included in ciphertext access policy. With this information the adversary now checks if a specific attribute, which may be an identity of a user (or linked to a user), is integrated in the access policy. If so, the adversary can figure out who is the target receiver of the ciphertext.

For example, suppose that a University has three different departments *Computer Science, Electrical Engineering, and Mechanical Engineering.* The attribute categories and their corresponding value sets are as follows.

- For the attribute *Role*, $W_{Role} = \{$*Dean, Teacher, Student, Administrative Staff*$\}$.

- For the attribute *Department*, $W_{Dept} = \{CS, EL, ME\}$.
- For the attribute *Course*, $W_{Course} = \{PhD, MS, BS\}$.

Assume that Dean wants to send a confidential notice to all teachers in an encrypted form using the scheme [1], then the Dean generates an encrypted message. For simplicity we are not showing all ciphertext components, instead, we provide the ciphertext components for the attribute *Role*.

$$C_{\Delta} = e(g,g)^{s} Y^{s\prime}$$
$$C_0 = g^s$$
$$\hat{C}_0 = g_1^{s\prime}$$
$$\tilde{C} = MY^s$$
$$C_1 = g_2^{s\prime\prime}$$
$$\hat{C}_1 = g_1^{s-s\prime\prime}$$

$$\{C_{Role,Teacher,\Delta}, C_{Role,Teacher,0}, \hat{C}_{Role,Teacher,0}\} =$$
$$\{H(Role\|Teacher)^{s\prime}, H(0\|Role\|Teacher)^{s\prime\prime},$$
$$H(1\|Role\|Teacher)^{s-s\prime\prime}\ \}$$

For other attributes such as *Student*, *Dean* and *Administrative staff* random values are provided.

The adversary now checks whether a *Teacher* is the intended recipient of the ciphertext by following equation.
$e(\hat{C}_0, H(Role\|Teacher)) = e(C_{Role,Teacher,\Delta}, g_1)$.
The correctness of the equation is given below.

$$e(\hat{C}_0, H(Role\|Teacher))$$
$$= e(g_1^{s\prime}, H(Role\|Teacher))$$
$$= e(H(Role\|Teacher)^{s\prime}, g_1)$$
$$= e(C_{Role,Teacher,\Delta}, g_1)$$

We note that to recover the whole access policy the adversary requires $n_i \times n$ bilinear pairing operations. Let $m = \max(n_i)_{1 \le i \le n}$. Therefore, to disclose the receiver's identity the adversary requires at most *O(mn)* bilinear pairing operations.

5 Conclusion

We have shown that Zhang *et al*'s scheme lacks receiver's anonymity. With the set of all attributes anyone can successfully check whether an attribute is required to decrypt the ciphertext in the matching phase, in turn, can reveal the receivers' identity from the attribute(s) used in the matching phase.

References

[1] Y. Zhang, X. Chen, J. Li, D. Wong, and H. Li. Anonymous Attribute-based Encryption Supporting Efficient Decryption Test. In Proceedings of the ACM SIGSAC Symposium on Information, Computer and Communications Security, pp. 511–516, 2013.

[2] A. Sahai and B. Waters. Fuzzy Identity Based Encryption. In Proceedings of Advances in Cryptology - Eurocrypt, LNCS 3494, Springer, pp. 457–473, 2005.

[3] V. Goyal, O. Pandey, A. Sahai and B. Waters. Attribute-based Encryption for Fine-grained Access Control of Encrypted Data. In Proceedings of the ACM conference on Computer and Communications Security, pp. 89–98, 2006.

[4] J. Bethencourt, A. Sahai and B. Waters. Ciphertext-Policy Attribute-Based Encryption. In Proceedings of IEEE Symposium on Security and Privacy, pp. 321–334, 2007.

[5] A. Kapadia, P. P. Tsang, and S. W. Smith. Attribute-based Publishing with Hidden Credentials and Hidden Policies. In Proceedings of Network and Distributed System Security Symposium, pp.179–192, 2007.

[6] S. Yu, K. Ren, and W. Lou. Attribute-based Content Distribution with Hidden Policy. In Proceedings of Workshop on Secure Network Protocols, IEEE, pp. 39–44, 2008.

[7] J. Li, K. Ren, B. Zhu, and Z. Wan. Privacy-aware Attribute-based Encryption with User Accountability. In: Information Security, LNCS 5735, Springer, pp. 347–362, 2009.

[8] T. Nishide, K. Yoneyama, and K. Ohta. Attribute-based Encryption with Partially Hidden Encryptor-specified Access Structures. In Proceedings of Applied Cryptography and Network Security, LNCS 5037, Springer, pp. 111–129, 2008.