Anonymous Attribute-Based Encryption Supporting Efficient Decryption Test

Yinghui Zhang
State Key Laboratory of Integrated Service Networks (ISN), Xidian University, Xi'an, P.R. China
yhzhaang@163.com

Xiaofeng Chen
State Key Laboratory of Integrated Service Networks (ISN), Xidian University, Xi'an, P.R. China
xfchen@xidian.edu.cn

Jin Li
School of Computer Science and Educational Software, Guangzhou University, Guangzhou, P.R. China
jinli71@gmail.com

Duncan S. Wong
Department of Computer Science, City University of Hong Kong, Hong Kong
duncan@cityu.edu.hk

Hui Li
State Key Laboratory of Integrated Service Networks (ISN), Xidian University, Xi'an, P.R. China
lihui@mail.xidian.edu.cn

ABSTRACT

Attribute-based encryption (ABE) has been widely studied recently to support fine-grained access control of shared data. Anonymous ABE, which is a relevant notion to ABE, further hides the receivers' attribute information in ciphertexts because many attributes are sensitive and related to the identity of eligible users. However, in existing anonymous ABE work, a user knows whether the attributes and the policy match or not only after repeating decryption attempts. And, the computation overhead of each decryption is high as the computational cost grows with the complexity of the access formula, which usually requires many pairings in most of the existing ABE schemes. As a result, this direct decryption method in anonymous ABE will suffer a severe efficiency drawback.

Aiming at tackling the challenge above, we propose a novel technique called match-then-decrypt, in which a *matching phase* is additionally introduced before the *decryption phase*. This technique works by computing special components in ciphertexts, which are used to perform the test that if the attribute private key matches the hidden attributes policy in ciphertexts without decryption. In our proposed construction, the computation cost of such a test is much less than one decryption operation. The proposed construction is proven to be secure. In addition, the results in simulation experiments indicate that the proposed solution is efficient and practical, which greatly improves the efficiency of decryption in anonymous ABE.

Categories and Subject Descriptors

E.3 [**Data Encryption**]: Public key cryptosystems

ASIA CCS'13, May 8–10, 2013, Hangzhou, China.

General Terms

Security

Keywords

Attribute-based encryption; Privacy; Attribute matching; Access control

1. INTRODUCTION

With the rapid development of cloud computing technology, more and more people have uploaded their various types of data into clouds either for ease of sharing or for cost saving. Naturally, people would like to make their private data only accessible to authorized users. In particular, differentiated data access is frequently required in the sense that users with different attributes or roles should be granted different level of access privileges.

Attribute-based encryption (ABE) is envisioned as a highly promising public key primitive for realizing scalable and fine-grained access control systems [15], where differential yet flexible access rights can be assigned to individual users. Especially, ciphertext-policy attribute-based encryption (CP-ABE) [1] puts access policy decisions in the hands of data owners. Though ABE can be directly applied to design secure access control, there is an increasing need to protect user privacy in access control systems. In order to address this problem, anonymous ABE was introduced in [8, 19] and further improved by [11, 12]. In anonymous CP-ABE, a user obtains his attribute secret key and if the attribute set associated with the secret key does not satisfy the access policy in the ciphertext, the user cannot decrypt and guess what access policy was specified by the data owner.

However, in existing anonymous ABE work, the user has to decrypt and decide whether his attributes satisfy the hidden policy in the ciphertext or not. Such a test should be repeated until a successful decryption or all of the possible tests have been considered. The decryption computation overhead in existing work is high as the computational cost grows with the complexity of the access formula, which usually requires many pairings in most of the existing ABE schemes. As a result, this direct decryption method in anonymous ABE will suffer a severe effi-

ciency drawback. Therefore, it is desirable for users to efficiently decide before full decryption whether the hidden policy in a ciphertext matches his attributes. Currently, techniques for attribute matching detection in state-of-the-art CP-ABE schemes are implemented through repeated decryption and hence suffer efficiency limitations. In fact, most of the available detection techniques in CP-ABE schemes have to reveal the access policy in the ciphertext, which violates user privacy. In practice, each user may receive a large number of ciphertexts and such kind of decryption method involves a large computational overhead.

1.1 Our Contribution.

Our contribution are two-folds:

1. We introduce a new technique called match-then-decrypt into the decryption of anonymous ABE, in which a *matching phase* is added before the *decryption phase*. This technique works by computing special components in ciphertexts, which are used to perform the test that if the attribute private key matches the hidden attributes policy in ciphertexts without decryption. In our proposed construction, the computation cost of such a test is much less than one decryption operation.

2. We prove that the proposed construction is secure under the presented model. To be specific, our construction is proven to be selective ciphertext policy and chosen plaintext secure under the Decisional Bilinear Diffie-Hellman assumption and the Decisional Linear assumption. Experimental results show that the novel technique of match-then-decrypt can greatly improve the efficiency of decryption in anonymous ABE.

1.2 Related Work.

Since the introduction of ABE in implementing fine-grained access control systems [15], a plenty of researches have been done on flexible ABE schemes [1, 5, 6, 7, 8, 10, 11, 12, 13, 14, 17, 18, 19]. ABE comes in two flavors called key-policy ABE (KP-ABE) and ciphertext-policy ABE, which were both mentioned in [6]. The first KP-ABE construction [6] realized the monotonic access policy for key policies. To enable more flexible access policy, Ostrovsky et al. presented the first KP-ABE system that supports the expression of non-monotone formulas in key policies [14]. Bethencourt et al. proposed the first CP-ABE construction [1]. However, the construction [1] is only proved secure under the generic group model. To overcome this weakness, Cheung and Newport presented another construction [5] that is proved to be secure under the standard model. Later, Goyal et al. proposed a bounded CP-ABE scheme with expressive access structures and provable security under the standard model [7]. However, complexity of the construction is extremely high and can just serve as a theoretical feasibility.

All the above CP-ABE schemes suffer from a weakness that the access policy has to be revealed in the ciphertexts since decryptors must know how they should combine their secret key components for decryption. To further achieve recipient-anonymity, Kapadia et al. proposed a CP-ABE scheme [8], which can realize hidden ciphertext policies that are represented by AND of different attributes, but it is not collusion-resistant and needs an online semi-trusted server which may be a performance bottleneck in the system. Shi et al. proposed a predicate encryption scheme [16] that focuses on range queries over huge numbers. The security proof of [16] is based on a security notion weaker than ours, which is called match-revealing security in [16] and the number of attributes must be small because the decryption cost is exponential in the number of attributes. Boneh and Waters proposed a predicate encryption scheme based on the primitive called Hidden Vector Encryption [2]. The scheme in [2] can also realize the anonymous CP-ABE by using the opposite semantics of subset predicates. Furthermore, Katz, Sahai, and Waters proposed a novel predicate encryption scheme supporting inner product predicates [9]. However, their scheme is based on a special type of bilinear groups the order of which is a product of three (or two) large primes, and hence needs to deal with large group elements. Later, a more efficient anonymous CP-ABE scheme was constructed [11]. The security proof was given under the Decisional Bilinear Diffie-Hellman assumption and the Decision Linear assumption. Based on the same assumptions as [11], Jin et al. proposed an anonymous CP-ABE scheme [12] with shorter public parameters. There are also many works proposed to make further improvements on ABE [4, 12, 20, 21]. However, all these ABE schemes implement the attribute matching detection only after decryption and hence lose practicability due to large computation cost.

2. PRELIMINARIES

2.1 Bilinear Pairings

Let $\mathbb{G}$ and $\mathbb{G}_T$ be cyclic multiplicative groups of some large prime order p and we denote the identity of $\mathbb{G}_T$ as 1. We call $\hat{e}$ a bilinear pairing if $\hat{e} : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$ is a map with the following properties:

1. Bilinear: $e(g^a, g^b) = e(g, g)^{ab}$ for all $a, b \in \mathbb{Z}_p$.

2. Non-degenerate: There exists $g_1, g_2 \in \mathbb{G}$ such that $e(g_1, g_2) \neq 1$.

3. Computable: There is an efficient algorithm to compute $e(g_1, g_2)$ for all $g_1, g_2 \in \mathbb{G}$.

2.2 Complexity Assumptions

The Decisional Bilinear Diffie-Hellman (DBDH) Assumption: Let $a, b, c, z \in_R \mathbb{Z}_p$ and $g \in_R \mathbb{G}$ be a generator. We say that the DBDH assumption holds in $\mathbb{G}$ if no probabilistic polynomial-time algorithm can distinguish the tuple $\left[g, g^a, g^b, g^c, \hat{e}(g, g)^{abc}\right]$ from the tuple $\left[g, g^a, g^b, g^c, g^z\right]$ with non-negligible advantage.

The Decision Linear (D-Linear) Assumption: Let $z_1, z_2, z_3, z_4, z \in_R \mathbb{Z}_p$ and $g \in_R \mathbb{G}$ be a generator. We say that the D-Linear assumption holds in $\mathbb{G}$ if no probabilistic polynomial-time algorithm can distinguish the tuple $\left[g, g^{z_1}, g^{z_2}, g^{z_1 z_3}, g^{z_2 z_4}, g^{z_3 + z_4}\right]$ from the tuple $[g, g^{z_1}, g^{z_2}, g^{z_1 z_3}, g^{z_2 z_4}, g^z]$ with non-negligible advantage.

2.3 Access Structure

Intuitively, an access structure, namely a ciphertext policy in CP-ABE, is a rule W that returns either 0 or 1 given a set L of attributes. We say that L satisfies W if and only if W answers 1 on L. Usually, notation $L \models W$ is used to represent the fact that L satisfies W, and the case of L does not satisfy W is denoted by $L \not\models W$.

In our construction, we consider access structures consisting of a single AND-gate supporting multi-value attributes and wildcards. As a generalization of access structures in [5, 21], access structures in our construction are the same as those in [11, 12].

Formally, given an attribute list $L = [L_1, L_2, \cdots, L_n]$ and a ciphertext policy $W = [W_1, W_2, \cdots, W_n]$, $L \models W$ if $L_i = W_i$ or $W_i = *$ for all $1 \leq i \leq n$, and otherwise $L \not\models W$. Note that the wildcard $*$ in the ciphertext policy plays the role of "don't care" value.

3. DEFINITION AND SECURITY MODEL

3.1 Definition of Anonymous CP-ABE

An anonymous CP-ABE scheme consists of a suite of four algorithms: Setup, KeyGen, Encrypt, and Decrypt. These algorithms are specified as follows:

- $\mathsf{Setup}(1^\lambda) \rightarrow (PK, MK)$: The setup algorithm is run by the attribute center. 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 private.
- $\mathsf{KeyGen}(PK, MK, L) \rightarrow SK_L$: The key generation algorithm is run by the attribute center. On input the system public key PK, the master key MK and an attribute list L, it outputs SK_L as the attribute secret key associated with the attribute list L.
- $\mathsf{Encrypt}(PK, M, W) \rightarrow CT_W$: The encryption algorithm is run by the encryptor. On input the system public key PK, a message M and a ciphertext policy W, it generates a ciphertext CT_W as the encryption of M with respect to W.
- $\mathsf{Decrypt}(PK, CT_W, SK_L) \rightarrow M$ or $\perp$: The decryption algorithm involves two phases, that is, attribute matching detection and decryption phase. On input the system public key PK, a ciphertext CT_W of a message M under a ciphertext policy W, and a secret key SK_L associated with L, the ciphertext CT_W is tested and decrypted by a user with secret key SK_L as follows:
  1. Matching Phase: It returns $\perp$ to terminate decryption with overwhelming probability if the attribute list L does not satisfy the ciphertext policy W, that is, $L \not\models W$. Otherwise, $L \models W$, the Matching Phase ends by initiating the Decryption Phase.
  2. Decryption Phase: It returns the message M.

3.2 Security Model

We demonstrate security requirements for anonymous CP-ABE systems by modeling the capability of adversaries, and define corresponding security notions. The goals of an adversary in an anonymous CP-ABE system include extracting information of a plaintext from the ciphertext and distinguishing underlying access policies in ciphertexts, which can be integrated the following IND-sCP-CPA game involving an adversary $\mathcal{A}$ and a challenger $\mathcal{S}$.

1. Init: The adversary $\mathcal{A}$ commits to the challenge ciphertext policies W_0^*, W_1^*.
2. Setup: The challenger $\mathcal{S}$ chooses a sufficiently large security parameter λ, and runs the Setup algorithm to get a master key SK and the corresponding public key PK. It retains SK and gives PK to $\mathcal{A}$.
3. Phase 1: In addition to hash queries, the adversary $\mathcal{A}$ issues a polynomially bounded number of queries to the following key generation oracle:
   - KeyGen oracle $\mathcal{O}_{KeyGen}$: The adversary $\mathcal{A}$ submits an attribute list L, if $(L \models W_0^* \wedge L \models W_1^*)$ or $(L \not\models W_0^* \wedge L \not\models W_1^*)$, the challenger $\mathcal{S}$ gives $\mathcal{A}$ the secret key SK_L. Otherwise, it outputs $\perp$.
4. Challenge: Once $\mathcal{A}$ decides that Phase 1 is over, it outputs two equal length messages M_0, M_1 from the message space, on which it wishes to be challenged with respect to W_0^* and W_1^*. It is required that $M_0 = M_1$ if any secret key on L satisfying $L \models W_0^* \wedge L \models W_1^*$ has been queried. The challenger $\mathcal{S}$ randomly chooses a bit $\nu \in \{0, 1\}$, computes $CT_{W_\nu^*} = \mathsf{Encrypt}(PK, M_\nu, W_\nu^*)$ and sends $CT_{W_\nu^*}$ to $\mathcal{A}$.
5. Phase 2: The same as Phase 1.
6. Guess: The adversary $\mathcal{A}$ outputs a guess bit $\nu' \in \{0, 1\}$ and wins the game if $\nu' = \nu$.

The advantage of an adversary $\mathcal{A}$ in the IND-sCP-CPA game is defined as $\mathsf{Adv}_{\text{CP-ABE}}^{\text{IND-sCP-CPA}}(\mathcal{A}) = \left|\Pr[\,\nu' = \nu\,] - \frac{1}{2}\right|$.

Definition 1. *An anonymous CP-ABE scheme is said to be IND-sCP-CPA secure if no probabilistic polynomial-time adversary can break the IND-sCP-CPA game with non-negligible advantage.*

4. THE PROPOSED CONSTRUCTION

In this section, we present a CPA-secure anonymous CP-ABE scheme, which achieves the protection of user privacy and enables efficient attribute matching detection.

4.1 Construction

- $\mathsf{Setup}(1^\lambda)$: Let $\mathbb{G}, \mathbb{G}_T$ be cyclic multiplicative groups of prime order p, and $\hat{e} : \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_T$ be a bilinear map. Define a hash function $H : \{0,1\}^* \rightarrow \mathbb{G}$. Assume there are n attributes in universe and the universal attribute set is $\mathcal{U} = \{\omega_1, \omega_2, \cdots, \omega_n\}$. And, each attribute has multiple values, where $S_i = \{v_{i,1}, v_{i,2}, \cdots, v_{i,n_i}\}$ is the multi-value set for ω_i and $|S_i| = n_i$. The attribute center chooses $y \in_R \mathbb{Z}_p$, $g_1, g_2 \in_R \mathbb{G}$. Next the attribute center computes $Y = \hat{e}(g_1, g_2)^y$. The system public key is published as $PK = \langle g, g_1, g_2, Y\rangle$. The master key is $MK = \langle y\rangle$.
- $\mathsf{KeyGen}(PK, MK, L)$: Let $L = [L_1, L_2, \cdots, L_n]$ be the attribute list for the user who obtains the corresponding attribute secret key. The attribute center chooses $r_1, r_2, \cdots, r_{n-1} \in_R \mathbb{Z}_p$ and computes $r_n = y - \sum_{i=1}^{n-1} r_i \mod p$. Also, the attribute center chooses $r \in_R \mathbb{Z}_p$ and $\{\hat{r}_i, \lambda_i, \widehat{\lambda}_i \in_R \mathbb{Z}_p\}_{1 \leq i \leq n}$, sets $\hat{r} = \sum_{i=1}^{n} \hat{r}_i$, and computes $\left[\widehat{D}_0, D_{\Delta,0}\right] = [g_2^{y-\hat{r}}, g_1^r]$. For $1 \leq i \leq n$, the attribute center computes

$$\left[D_{\Delta,i}, D_{i,0}, D_{i,1}, \widehat{D}_{i,0}, \widehat{D}_{i,1}\right] =$$

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

  where $L_i = v_{i,k_i}$. The secret key is

$$SK_L = \langle \widehat{D}_0, D_{\Delta,0}, \{D_{\Delta,i}, D_{i,0}, D_{i,1}, \widehat{D}_{i,0}, \widehat{D}_{i,1}\}_{1 \leq i \leq n}\rangle.$$

- $\mathsf{Encrypt}(PK, M, W)$: To encrypt a message $M \in \mathbb{G}_T$ under a ciphertext policy $W = [W_1, W_2, \cdots, W_n]$, an encryptor chooses $s, s', s'' \in_R \mathbb{Z}_p$, and computes $\widetilde{C} = MY^s$, $C_\Delta = \hat{e}(g, g)^s Y^{s'}$, $C_0 = g^s$, $\widehat{C}_0 = g_1^{s'}$, $C_1 = g_2^{s''}$, $\widehat{C}_1 = g_1^{s-s''}$. Then for $1 \leq i \leq n$ and $1 \leq t \leq n_i$, the encryptor computes $\left[C_{i,t,\Delta}, C_{i,t,0}, \widehat{C}_{i,t,0}\right]$ as follows:

1. If $v_{i,t} \in W_i$, then $\left[C_{i,t,\Delta}, C_{i,t,0}, \widehat{C}_{i,t,0}\right] =$

$$\left[H(i||v_{i,t})^{s'}, H(0||i||v_{i,t})^{s''}, H(1||i||v_{i,t})^{s-s''}\right].$$

2. If $v_{i,t} \notin W_i$, then $\left[C_{i,t,\Delta}, C_{i,t,0}, \widehat{C}_{i,t,0}\right]$ are random elements in $\mathbb{G}$.

Then the ciphertext of M with respect to W is

$$CT_W = \langle C_\Delta, C_0, \widehat{C}_0, \widetilde{C}, C_1, \widehat{C}_1, \{\{C_{i,t,\Delta}, C_{i,t,0}, \widehat{C}_{i,t,0}\}_{1\le t\le n_i}\}_{1\le i\le n}\rangle.$$

- Decrypt(PK, CT_W, SK_L): The ciphertext CT_W is tested and decrypted by a user with secret key SK_L as follows:

1. Matching Phase: The user checks whether $L \models W$ in terms of the following Equality (1). To be specific, $L \models W$ if and only if Equality (1) holds:

$$\frac{C_\Delta}{\hat{e}(g, C_0)} = \frac{\hat{e}\left(\widehat{C}_0, \widehat{D}_0 \prod_{i=1}^n D_{\Delta,i}\right)}{\hat{e}\left(\prod_{i=1}^n C_{i,t,\Delta}, D_{\Delta,0}\right)}, \quad (1)$$

where $L_i = v_{i,t}$. If $L \not\models W$, it returns $\perp$. Otherwise, it initiates the Decryption Phase if $L \models W$.

2. Decryption Phase: The user decrypts and computes M as follows:

$$M = \frac{\widetilde{C} \prod_{i=1}^n \hat{e}\left(C_{i,t,0}, D_{i,0}\right) \hat{e}\left(\widehat{C}_{i,t,0}, \widehat{D}_{i,0}\right)}{\prod_{i=1}^n \hat{e}\left(C_1, D_{i,1}\right) \hat{e}\left(\widehat{C}_1, \widehat{D}_{i,1}\right)},$$

where $L_i = v_{i,t}$.

4.2 Consistency of the Proposed Construction

For $1 \le i \le n$, suppose $L_i = v_{i,t}$. We first show that Equality (1) holds, which means the attribute matching detection is valid in decryption of the proposed construction. Indeed,

$$\begin{aligned}
&\frac{\hat{e}\left(\widehat{C}_0, \widehat{D}_0 \prod_{i=1}^n D_{\Delta,i}\right)}{\hat{e}\left(\prod_{i=1}^n C_{i,t,\Delta}, D_{\Delta,0}\right)} \\
= \ &\frac{\hat{e}\left(g_1^{s'}, g_2^{y-\hat{r}} \prod_{i=1}^n \left(g_2^{\hat{r}_i} H(i||v_{i,t})^r\right)\right)}{\hat{e}\left(\prod_{i=1}^n H(i||v_{i,t})^{s'}, g_1^r\right)} \\
= \ &\hat{e}\left(g_1^{s'}, g_2^{y-\hat{r}} \left(\prod_{i=1}^n g_2^{\hat{r}_i}\right)\right) = \hat{e}\left(g_1^{s'}, g_2^{y-\hat{r}} g_2^{\hat{r}}\right) \\
= \ &\hat{e}\left(g_1^{s'}, g_2^{y}\right) = \hat{e}\left(g_1, g_2\right)^{ys'} \\
= \ &\frac{C_\Delta}{\hat{e}(g, C_0)}.
\end{aligned}$$

On the other hand, the message can be successfully recovered as follows:

$$\begin{aligned}
&\frac{\widetilde{C} \prod_{i=1}^n \hat{e}\left(C_{i,t,0}, D_{i,0}\right) \hat{e}\left(\widehat{C}_{i,t,0}, \widehat{D}_{i,0}\right)}{\prod_{i=1}^n \hat{e}\left(C_1, D_{i,1}\right) \hat{e}\left(\widehat{C}_1, \widehat{D}_{i,1}\right)} \\
= \ &\frac{\widetilde{C} \prod_{i=1}^n \hat{e}\left(H(0||i||v_{i,t})^{s''}, g_2^{\lambda_i}\right) \hat{e}\left(H(1||i||v_{i,t})^{s-s''}, g_1^{\hat{\lambda}_i}\right)}{\prod_{i=1}^n \hat{e}\left(g_2^{s''}, g_1^{r_i} H(0||i||v_{i,t})^{\lambda_i}\right) \hat{e}\left(g_1^{s-s''}, g_2^{r_i} H(1||i||v_{i,t})^{\hat{\lambda}_i}\right)} \\
= \ &\frac{MY^s}{\prod_{i=1}^n \hat{e}\left(g_2^{s''}, g_1^{r_i}\right) \hat{e}\left(g_1^{s-s''}, g_2^{r_i}\right)} \\
= \ &\frac{M\hat{e}(g_1, g_2)^{ys}}{\prod_{i=1}^n \hat{e}\left(g_1, g_2\right)^{sr_i}} = \frac{M\hat{e}(g_1, g_2)^{ys}}{\hat{e}\left(g_1, g_2\right)^{ys}} = M.
\end{aligned}$$

4.3 Security Results

THEOREM 1. *If there exists a polynomial-time adversary $\mathcal{A}$ that can attack the proposed construction in the IND-sCP-CPA model with advantage ϵ, then ϵ is negligible and $\epsilon \le \epsilon_{DBDH} + n\epsilon_{DL}$, where ϵ_{DBDH} and ϵ_{DL} respectively denotes the advantage of a distinguisher of a DBDH challenge and a D-Linear challenge, and n represents the total number of attributes in universe.*

PROOF. (Sketch) Suppose that the adversary $\mathcal{A}$ commits to the challenge ciphertext policies $W_0^* = \left[W_{0,1}^*, W_{0,2}^*, \cdots, W_{0,n}^*\right]$ and $W_1^* = \left[W_{1,1}^*, W_{1,2}^*, \cdots, W_{1,n}^*\right]$ at the beginning of the game. Based on the IND-sCP-CPA security model, we use a sequence of hybrid games to prove that $\mathcal{A}$ cannot win the original security game denoted by $\mathbf{G}$ with non-negligible probability. We begin by slightly modifying the game $\mathbf{G}$ into a game $\mathbf{G}_0$. The definitions of games $\mathbf{G}$ and $\mathbf{G}_0$ are the same except the generation of the challenge ciphertext. In $\mathbf{G}_0$, to be precise, if the adversary did not obtain the secret key SK_L with respect to the attribute list L satisfying the condition of $[L \models W_0^* \wedge L \models W_1^*]$, then the challenge ciphertext component $\widetilde{C}$ is a random element in $\mathbb{G}_T$ regardless of the random coin, while the rest of the challenge ciphertext are generated in a normal way. On the other hand, if the adversary obtained the secret key SK_L whose associated attribute list L is such that $[L \models W_0^* \wedge L \models W_1^*]$, then the challenge ciphertext is generated correctly. In this case, we have $\mathbf{G} = \mathbf{G}_0$. In any case, we have

LEMMA 1. *Under the DBDH assumption, the difference between advantages of $\mathcal{A}$ in game $\mathbf{G}$ and game $\mathbf{G}_0$ is negligible in the security parameter λ. To be specific, we have* $|\Pr[\mathcal{E}] - \Pr[\mathcal{E}_0]| \le \epsilon_{\text{DBDH}}$.

Subsequently, we modify the game $\mathbf{G}_0$ by changing the ciphertext components $\{\{C_{i,t,\Delta}, C_{i,t,0}, \widehat{C}_{i,t,0}\}_{1\le t\le n_i}\}_{1\le i\le n}$ and define a sequence of games as follows. For $v_{i,t}$ such that $(v_{i,t} \in W_{0,i}^* \wedge v_{i,t} \in W_{1,i}^*)$ or $(v_{i,t} \notin W_{0,i}^* \wedge v_{i,t} \notin W_{1,i}^*)$, the components $\{C_{i,t,\Delta}, C_{i,t,0}, \widehat{C}_{i,t,0}\}$ are generated as in the real game through the sequence of all the games. In the case that there exists $v_{i,t}$ such that $(v_{i,t} \in W_{0,i}^* \wedge v_{i,t} \notin W_{1,i}^*)$ or $(v_{i,t} \notin W_{0,i}^* \wedge v_{i,t} \in W_{1,i}^*)$, the components $\{C_{i,t,\Delta}, C_{i,t,0}, \widehat{C}_{i,t,0}\}$ generated normally in game $\mathbf{G}_{l-1}$ are replaced with the random elements from the group $\mathbb{G}$ in the new modified game $\mathbf{G}_l$ regardless of the random coin. The process is repeated until there is no component $v_{i,t}$ satisfying $(v_{i,t} \in W_{0,i}^* \wedge v_{i,t} \notin W_{1,i}^*)$ or $(v_{i,t} \notin W_{0,i}^* \wedge v_{i,t} \in W_{1,i}^*)$. In the last game of the sequence, the advantage of the adversary $\mathcal{A}$ is zero since that $\mathcal{A}$ is given a ciphertext chosen from the same distribution regardless of the random coin. By replacing the well-formed ciphertext components in $\mathbf{G}_{l-1}$ with the random elements from the group $\mathbb{G}$ in $\mathbf{G}_l$ in this way, we can embed a D-Linear challenge into the ciphertext such that a distinguisher of $\mathbf{G}_{l-1}$ and $\mathbf{G}_l$ leads to a distinguisher of the D-Linear challenge. To be specific, we have

LEMMA 2. *Under the D-Linear assumption, the difference between advantages of $\mathcal{A}$ in game $\mathbf{G}_{l-1}$ and game $\mathbf{G}_l$ is negligible in the security parameter λ. Specifically, we have* $|\Pr[\mathcal{E}_{l-1}] - \Pr[\mathcal{E}_l]| \le \epsilon_{\text{DL}}$ *for* $1 \le l \le l_{max}$.

Suppose that the above games sequentially compose $\{\mathbf{G}, \mathbf{G}_0, \mathbf{G}_1, \cdots, \mathbf{G}_{l_{max}}\}$, where $\mathbf{G}$ is the original attack game and $\mathbf{G}_{l_{max}}$ is the last one which gives no advantage to $\mathcal{A}$. Let $\mathcal{E}$ be the event that $\nu' = \nu$ in the original game $\mathbf{G}$ and $\mathcal{E}_l$ be the event that

$\nu' = \nu$ in $\mathbf{G}_l$ for $0 \leq l \leq l_{max}$. Then, we have $\epsilon = \left|\Pr[\mathcal{E}] - \frac{1}{2}\right| = |\Pr[\mathcal{E}] - \Pr[\mathcal{E}_{l_{max}}]|$. From the triangle inequality, it follows that

$$\begin{aligned} \epsilon &\leq |\Pr[\mathcal{E}] - \Pr[\mathcal{E}_0]| + \sum_{l=1}^{l_{max}} |\Pr[\mathcal{E}_{l-1}] - \Pr[\mathcal{E}_l]| \\ &\leq \epsilon_{\text{DBDH}} + n\epsilon_{\text{DL}}. \end{aligned}$$

Then it is obvious that ϵ is negligible, and hence the proposed scheme is IND-sCP-CPA secure under the DBDH assumption and the D-Linear assumption. ■

REMARK 1. *We can apply the Canetti-Halevi-Katz technique [3] to obtain a selective ciphertext policy and chosen ciphertext secure extension based on strongly existentially unforgeable one-time signatures.*

5. PERFORMANCE COMPARISON

In this section, we compare the security and efficiency performance of the proposed scheme with some existing CP-ABE schemes [1, 5, 11, 12].

Table 1 mainly presents the security comparison with respect to the complexity assumption, the security model and anonymity. Note that anonymity can be applied to protect users' privacy. From the security comparison in Table 1, it is clear that only Nishide et al's scheme [11], Li et al's scheme [12] and ours achieve the goal of protecting users' privacy and they have the same access policy. It is important to note that only the proposed construction enjoys the desirable property of match-then-decrypt, and hence can be used to alleviate the computation burden of users in the attribute-based setting.

On the other hand, it is indispensable for receivers to perform attribute matching detection (*i.e.*, decryption test) in attribute-based setting. Considering the protection of user privacy, we only compare the cost of attribute matching detection of schemes [11, 12] with that of ours in Figure 1. Our experiment is simulated on a LINUX machine with Intel Core 2 processors running at 2.40 GHz and 2G memory. The order p of groups $\mathbb{G}$ and $\mathbb{G}_T$ is set as a prime of length 160 bits. It is obvious that the proposed scheme is significantly more efficient than schemes [11, 12]. The reason is that the cost of attribute matching detection is mainly determined by the number of fundamental cryptographic operations, especially the most expensive *pairing* operation. And, the number of *pairing* operations for attribute matching detection is constant in the proposed scheme and linearly grows with n in schemes [11, 12].

6. CONCLUSION

The notion of anonymous ABE can be applied to hide the receivers' attribute information in ciphertexts. However, the decryption computation overhead is high as the computational cost grows with the complexity of the access formula. Aiming at improving the decryption efficiency, in this paper, we introduced a new technique called match-then-decrypt into the decryption of anonymous ABE, in which a *matching phase* is added before the *decryption phase*. This technique performs the test that if the attribute private key matches the hidden attributes policy in ciphertexts without decryption. In the proposed construction, the computation cost of such a test is much less than one decryption operation. Our construction is proven to be secure. In particular, experimental results show that the proposed solution is efficient and practical, and that the novel technique of match-then-decrypt can greatly improve the efficiency of decryption in anonymous ABE.

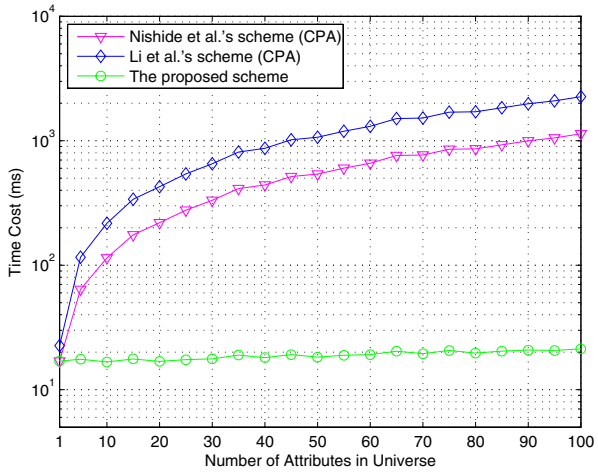

Figure 1: Comparison of cost for attribute matching detection.

7. ACKNOWLEDGMENTS

We are grateful to the anonymous referees for their invaluable suggestions. This work is supported by the National Natural Science Foundation of China (Nos.61272455, 61272457, and 61100224), China 111 Project (No.B08038), the Program for Changjiang Scholars and Innovative Research Team in University (IRT1078), and the Fundamental Research Funds for the Central Universities (Nos.K50511010001 and JY10000901034). Particularly, this work is supported by the Graduate Student Innovation Fund of Xidian University (Research on key security technologies of large-scale data sharing in cloud computing).

8. REFERENCES

[1] J. Bethencourt, A. Sahai, and B. Waters. Ciphertext-policy attribute-based encryption. In *Proc. of SP'07*, Oakland, California, USA, May 20-23, pages 321–334, 2007.

[2] D. Boneh and B. Waters. Conjunctive, subset, and range queries on encrypted data. In *Proc. of TCC'07*, KNAW Trippenhuis Amsterdam, The Netherlands, volume 4392 of *LNCS*, pages 535–554. Springer Berlin-Heidelberg, 2007.

[3] R. Canetti, S. Halevi, and J. Katz. Chosen-ciphertext security from identity-based encryption. In *Proc. of EUROCRYPT'04*, volume 3027 of *LNCS*, pages 207–222. Springer Berlin-Heidelberg, 2004.

[4] M. Chase and S. S. Chow. Improving privacy and security in multi-authority attribute-based encryption. In *Proc. of CCS'09*, New York, NY, USA, pages 121–130. ACM Press. 2009.

[5] L. Cheung and C. Newport. Provably secure ciphertext policy abe. In *Proc. of CCS'07*, New York, NY, USA, pages 456–465. ACM Press. 2007.

[6] V. Goyal, O. Pandey, A. Sahai, and B. Waters. Attribute-based encryption for fine-grained access control of encrypted data. In *Proc. of CCS'06*, New York, NY, USA, pages 89–98. ACM Press. 2006.

[7] V. Goyal, A. Jain, O. Pandey, and A. Sahai. Bounded ciphertext policy attribute based encryption. In *Proc. of*

Table 1: Security Comparison of CP-ABE Schemes

Schemes	Expressiveness	Complexity assumption	Security model	Anonymity
BSW [1]	Type 1 [a]	Generic group model	CPA	×
CN [5]	Type 2 [b]	DBDH	CPA	×
NYO [11]	Type 3 [c]	DBDH, D-Linear	CPA	✓
LRZW [12]	Type 3	DBDH, D-Linear	CPA	✓
The proposed scheme	Type 3	DBDH, D-Linear	CPA	✓

[a] Tree-based structure.
[b] AND-gates on positive and negative attributes with wildcards.
[c] AND-gates on multi-valued attributes with wildcards.

ICALP'08, volume 5126 of *LNCS*, pages 579–591. Springer Berlin-Heidelberg, 2008.

[8] A. Kapadia, P. P. Tsang, and S. W. Smith. Attribute-based publishing with hidden credentials and hidden policies. In *Proc. of NDSS'07*, San Diego, California, USA, February 28-March 2, pages 179–192. The Internet Society, 2007.

[9] J. Katz, A. Sahai, and B. Waters. Predicate encryption supporting disjunctions, polynomial equations, and inner products. In *Proc. of EUROCRYPT'08*, volume 4965 of *LNCS*, pages 146–162. Springer Berlin-Heidelberg, 2008.

[10] A. Lewko, T. Okamoto, A. Sahai, K. Takashima, and B. Waters. Fully secure functional encryption: Attribute-based encryption and (hierarchical) inner product encryption. In *Proc. of EUROCRYPT'10*, volume 6110 of *LNCS*, pages 62–91. Springer Berlin-Heidelberg, 2010.

[11] T. Nishide, K. Yoneyama, and K. Ohta. Abe with partially hidden encryptor-specified access structure. In *Proc. of ACNS'08*, New York, USA, June 3-6, volume 5037 of *LNCS*, pages 111–129. Springer Berlin-Heidelberg, 2008.

[12] J. Li, K. Ren, B. Zhu, and Z. Wan. Privacy-aware attribute-based encryption with user accountability. In *Proc. of ISC'09*, Pisa, Italy, September 7-9, volume 5735 of *LNCS*, pages 347–362. Springer Berlin-Heidelberg, 2009.

[13] T. Okamoto and K. Takashima. Fully secure functional encryption with general relations from the decisional linear assumption. In *Proc. of CRYPTO'10*, volume 6223 of *LNCS*, pages 191–208. Springer Berlin-Heidelberg, 2010.

[14] R. Ostrovsky, A. Sahai, and B. Waters. Attribute-based encryption with non-monotonic access structures. In *Proc. of CCS'07*, New York, pages 195–203. ACM Press. 2007.

[15] A. Sahai and B. Waters. Fuzzy identity-based encryption. In *Proc. of EUROCRYPT'05*, volume 3494 of *LNCS*, pages 557–557. Springer Berlin-Heidelberg, 2005.

[16] E. Shi, J. Bethencourt, T.-H. Chan, D. Song, and A. Perrig. Multi-dimensional range query over encrypted data. In *Proc. of SP'07*, pages 350–364. 2007.

[17] B. Waters. Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization. In *Proc. of PKC'11*, volume 6571 of *LNCS*, pages 53–70. Springer Berlin-Heidelberg, 2011.

[18] S. Yamada, N. Attrapadung, G. Hanaoka, and N. Kunihiro. Generic constructions for chosen-ciphertext secure attribute based encryption. In *Proc. of PKC'11*, volume 6571 of *LNCS*, pages 71–89. Springer Berlin-Heidelberg, 2011.

[19] S. Yu, K. Ren, and W. Lou. Attribute-based content distribution with hidden policy. In *Proc. of NPSec'08*, Orlando, Florida, USA, pages 39–44. 2008.

[20] S. Yu, K. Ren, W. Lou, and J. Li. Defending against key abuse attacks in kp-abe enabled broadcast systems. In *Proc. of Securecomm'09*, Athens, Greece, September 14-17, volume 19 of *LNCS*, pages 311–329. Springer Berlin-Heidelberg, 2009.

[21] S. Yu, C. Wang, K. Ren, and W. Lou. Attribute based data sharing with attribute revocation. In *Proc. of ASIACCS'10*, New York, NY, USA, pages 261–270. ACM Press. 2010.