A New Technique for Compacting Secret Key in Attribute-Based Broadcast Encryption

Sébastien Canard[1], Duong Hieu Phan[2], and Viet Cuong Trinh[3,4(✉)]

[1] Orange Labs - Applied Crypto Group, Lannion, France
[2] XLIM - CNRS - University of Limoges, Limoges, France
[3] KINDI Lab, Qatar University, Doha, Qatar
[4] Hong Duc University, Thanh Hóa, Vietnam
cuongtrinhviet@gmail.com

Abstract. Public-key encryption has been generalized to adapt to more and more practical applications. Broadcast encryption, introduced by Fiat and Naor in 1993, aims for applications in pay-TV or satellite transmission and allows a sender to securely send private messages to any subset of users, the target set. Sahai and Waters introduced Attribute-based Encryption (ABE) to define the target set in a more structural way via access policies on attributes. Attribute-based Broadcast Encryption (ABBE) combines the functionalities of both in an efficient way. In the relevant applications such as pay-TV, the users are given a relatively small device with very limited secure memory in a smartcard. Therefore, it is of high interest to construct schemes with compact secret key of users. Even though extensively studied in the recent years, it is still an open question of constructing an efficient ABBE with constant-size private keys for general forms of access policy such as CNF or DNF forms. This question was partially solved at ESORICS '15 where Phuong *et al.* introduced a constant secret-key size ABBE. But they manage restrictive access policies only supporting AND-gates and wildcards. In this paper, we solve this open question and propose an efficient constant-size private key ciphertext-policy attribute-based broadcast encryption scheme for DNF form. In particular, we also present the optimization in implementing our proposed scheme.

Keywords: Attribute-based broadcast encryption · Ciphertext-policy · DNF

1 Introduction

We are actually in a very active period of development of cryptography. Modern technologies, namely cloud computing and big data, require the design of advanced cryptographic schemes supporting new functionalities. In many applications that involve a large set of users, one needs to have stronger and more flexible capabilities to encrypt data than the traditional public key encryption: the encryption should take into account specific policies in such a way that only receivers with suitable rights can decrypt the encrypted messages.

S. Foresti and G. Persiano (Eds.): CANS 2016, LNCS 10052, pp. 594–603, 2016.
DOI: 10.1007/978-3-319-48965-0_38

Attribute-Based Encryption. Sahai and Waters [14] introduced the concept of *attribute-based encryption* (ABE) in which the encryption and decryption can be based on the user's attributes. Since then, there are a lot of development in this area with many interesting results [7,11,13,14,16], to name a few. Actually, there are two categories of ABE: *ciphertext-policy* attribute-based encryption (CP-ABE) and *key-policy* attribute-based encryption (KP-ABE). In a CP-ABE scheme, the secret key is associated with a set of attributes and the ciphertext is associated with an access policy (structure) over the universe of attributes: a user can then decrypt a given ciphertext if the set of attributes related to his/her secret key satisfies the access policy underlying the ciphertext. In contrast, in a KP-ABE scheme, each secret key corresponds to an access policy and a set of attributes is associated with the ciphertext. Concerning the access structure, fine-grained access control is the most desired and also well formalized as boolean formula in disjunctive normal form (DNF) or in conjunctive normal form (CNF).

Attribute-Based Broadcast Encryption. In some practical cases, one may want to remove the right to decrypt to some specific users. The notion of attribute-based broadcast encryption (ABBE) has then been introduced in [10] to address the problem of user revocation. More precisely, in such a system, the broadcaster is capable of revoking any receiver and the collusion of revoked users cannot decrypt any ciphertext even if they possess sufficient attributes to satisfy the access policy. In traditional attribute-based encryption schemes, the revocation can be performed based on attributes (resp., negative attributes as some non-monotonic schemes [11,16]), by adding the AND of a clause containing the attributes corresponding to non-revoked users (resp., negative attributes corresponding to revoked users). However, this will give an inefficient solution as the ciphertext grows linearly to the number of non–revoked users (resp., revoked users), which is large. An attribute-based broadcast encryption (ABBE) scheme should allow individual receivers to be directly revoked in an efficient way.

Several ABBE schemes have been proposed in [3,7–10]. As in a broadcast encryption, it is of great importance to construct a scheme with compact secret key. Such a scheme can have practical applications such as in pay-TV or satellite transmission where the user's device are relatively small and the secure memory is often implemented in a smartcard. While broadcast encryption with constant-size secret key has been solved by Boneh, Gentry and Waters in [2], the extension of BGW technique to ABBE setting make the secret key longer, due to the obligation of combining different attributes in the decryption, as shown in [7]. The problem of designing constant-size private key ABBE schemes supporting fine-grained access control was partially solved in ESORICS '15 [12]. But the problem is still open since the proposed non-monotonic scheme only manages restrictive access policies supporting AND-gates and wildcards: they do not treat the case of CNF or DNF forms. More precisely, if the access policy is $A_1 \wedge * \wedge A_2$, where $*$ is a wildcard, then any user whose attribute set contains exactly three attributes (no more no less) and two of them are A_1, A_2 can decrypt the ciphertext. This obliviously can reduce the ciphertext size, however in exchange, the secret key size now is $3 + 2(N_1 + 1)$ elements, where N_1 is the maximal number of wildcards can appear in an access policy, N_1 is fixed at the setup phase.

Our Contributions. Even though extensively studied in the recent years, it is still an open question of constructing an efficient ABBE with constant-size private keys for general forms of access policy such as CNF or DNF. We here solve this open question for the DNF form by providing several new techniques in this field.

Our initial new idea is to extend the Delerablée's technique (for constructing an IBBE scheme [5]) to our context of CP-ABBE. More precisely, each attribute in our ABBE corresponds to an identity in Delerablée's IBBE scheme. To obtain the "broadcast" property, we also add an additional identity for each user. The resulting scheme then contains two kinds of "IBBE identities": one user's identity and the additional identities that represent the attributes the user possesses. We then succeed in combining all these information into a compact secret key. More intuition behind our construction as well as the security proof of our scheme will be given further in the paper.

We give in Table 1 a detailed comparison among our scheme and several other CP-ABE and CP-ABBE schemes supporting fine-grained access control. It shows that, regarding the efficiency, our CP-ABBE scheme enjoys the following properties:

- it is the first efficient CP-ABBE scheme which simultaneously achieves constant-size private key and supports fine-grained access control;
- regarding the decryption, a user in our scheme only needs to compute two parings, in contrast to almost existing CP-ABE and CP-ABBE schemes supporting fine-grained access control where each user needs to perform at least $|I|$ pairings computations in the decryption, where $|I|$ is the number of attributes needed to satisfy a ciphertext policy. Moreover, as we will see, one of the two pairing can be delegated to a third party.

We show at the full version of the paper that our scheme can be truly implemented in a prototype for a smartphone based cloud storage use case. In particular, we show how to alleviate some parts of our scheme so as to obtain a very practical system, and we give some concrete benchmarks.

Organization of the Paper. The paper is now organized as follows. The next section presents the security definitions and the assumptions we need to prove the security. In Sect. 3, we present our new construction. Section 4 is devoted to the security proof of the scheme. Finally, in Sect. 5, we talk about our real implementation.

2 Preliminaries

We give here our main scenario, several preliminaries regarding definition and security model for a CP-ABBE scheme and the security assumptions we will need.

Table 1. n is the maximal number of users, N is the maximal number of attributes, m is the number of clauses in a CNF/DNF access policy, (in some systems from linear secret sharing matrix framework, ℓ denotes the number of rows of the LSSS matrix (the number of attributes in an access formula, counting the reused attributes), ℓ^* denotes the maximal of ℓ which is equal to the size of the attribute universe, $|S_u|$ denotes the number of attributes of a private key, $|I|$ is the number of attributes of a private key to satisfy a ciphertext policy, $|p|$ denotes element in $\mathbb{Z}_p$, P denotes pairing computation, ex denotes the exponentiation, $\mathsf{mex}[v]$ the multi-exponentiation with v terms, mul denotes the multiplication, k_{max} denotes the maximal number of times where one attribute can be reused in an access formula. Note that [8,9] support fully collusion-resistant blackbox traceability

	$\|ciphertext\|$	$\|sk\|$	$\|pk\|$	Enc time	Dec time	Assump	Revoc
[15]	$2\ell+1$	$\|S_u\|+2$	$N+3$	$(3\ell+2)\mathsf{ex}$	$(2\|I\|+1)P$	q-type	No
[6]	$(\ell+1)$	$k_{max}\|S_u\|+2$	$N+3$	$(2\ell+2)\mathsf{ex}$	$2P$	BDHE	No
[7]	$O(m)$	$O(N)$	$O(N)$	$(\ell+2m)\mathsf{ex}$	$O(\|I\|)P$	GDDHE	Yes
[13]	$3\ell+2$	$2\|S_u\|+2$	$6+N\|p\|$	$(5\ell+2)\mathsf{ex}$	$(3\|I\|+1)P$	q-type	No
[4]	$2\ell^*+2$	$2\ell^*+4$	$2\ell^*+3$	$O(\ell^2)\mathsf{mul}$	$4P$	SXDH	No
[8]	$17\sqrt{n}+2\ell$	$4+\|S_u\|$	$4\sqrt{n}+N$	$(O(\sqrt{n})+3\ell)\mathsf{ex}$	$(10+2\|I\|)P$	q-type	Yes
[9]	$16\sqrt{n}+3\ell$	$2+\sqrt{n}+2\|S_u\|$	$5+5\sqrt{n}$	$(O(\sqrt{n})+3\ell)\mathsf{ex}$	$(9+3\|I\|)P$	q-type	Yes
Ours	$m+1$	1	$O(N.n)$	$2\mathsf{ex}+m\cdot$ $\mathsf{mex}[n+m+N]$	$2P$	GDDHE	Yes

2.1 Practical Scenario

All along the paper, we will consider the following scenario. A company wishes to put in place a CP-ABBE scheme for its staff, so that they can store and share sensitive documents, using a non-trusted cloud platform for storage (such as e.g., Dropbox or GoogleDrive). More precisely, we consider three kinds of attributes in the studied system.

- The role of the user in the company: boss, $\mathsf{manager}$, $\mathsf{developer}$, expert.
- The team in which the user is: $\mathsf{team}_1, \cdots, \mathsf{team}_k$.
- The project on which the user can work: $\mathsf{project}_1, \cdots, \mathsf{project}_\ell$.

Based on that attributes, and a unique specific identity, anyone can encrypt and upload documents, using the CP-ABBE scheme and a chosen DNF access control policy of the form

$$\beta = \mathsf{boss} \vee (\mathsf{manager} \wedge \mathsf{team}_4) \vee (\mathsf{developer} \wedge \mathsf{project}_5) \vee (\mathsf{expert} \wedge \mathsf{project}_2).$$

Finally, anyone with the correct attributes will be able to obtain the document in clear.

2.2 Ciphertext-Policy Attribute-Based Broadcast Encryption

In this paper, we will consider the similar definition and security model for a CP-ABBE scheme as in [7]. Formally, a CP-ABBE scheme consists of three probabilistic algorithms as follows.

Setup$(1^\lambda, n, \{S_u\}_{u\in[n]})$**:** Takes as input the security parameter λ, the maximal number of users n, and the attribute repartition S_u (the user's attribute set) for each user u. It returns the public parameters param of the system, and n private keys sk_u which will be distributed to each respective user. The set $\mathcal{K}$ corresponds to the key space for session keys.

Encrypt$(\mathsf{param}, \mathbb{A}, S)$**:** Takes as input an access policy $\mathbb{A}$, the target set S, and public parameter param. It outputs the session key $K \in \mathcal{K}$, and the header Hdr which includes the access policy $\mathbb{A}$ and the target set S.

Decrypt$(sk_u, \mathsf{Hdr}, \mathsf{param})$**:** Takes as input the header Hdr, the private key sk_u of a user u, together with the parameters param. It outputs the session key K if and only if S_u satisfies $\mathbb{A}$ and $u \in S$. Otherwise, it outputs $\perp$.

Security Model. This security model is called *semantic security with full static collusions*. In fact, a CP-ABBE scheme is said to be secure in this model if given a challenge header and all private keys of revoked users to an adversary. It is impossible for the adversary to infer any information about the session key. Formally, we now recall the security model for a CP-ABBE scheme by the following probabilistic game between an attacker $\mathcal{A}$ and a challenger $\mathcal{C}$.

1. The challenger $\mathcal{C}$ and the adversary $\mathcal{A}$ are given a system consisting of N attributes.
2. $\mathcal{A}$ outputs a target access policy $\mathbb{A}$, target set S as well as a repartition $\{S_u\}_{u\in[n]}$ which he intends to attack.
3. $\mathcal{C}$ runs the algorithm **Setup**$(1^\lambda, n, \{S_u\}_{u\in[n]})$ and gives to $\mathcal{A}$ the public parameters param and the private keys sk_u corresponding to the users u that $\mathcal{A}$ may control, i.e., S_u doesn't satisfy $\mathbb{A}$ or S_u satisfies $\mathbb{A}$ but $u \notin S$.
4. $\mathcal{C}$ runs the algorithm **Encrypt**$(\mathsf{param}, \mathbb{A}, S)$ and obtains a header Hdr and a session key $K \in \mathcal{K}$. Next, $\mathcal{C}$ draws a bit b uniformly at random, sets $K' = K$ if bit $b = 0$, $K' \xleftarrow{\$} \mathcal{K}$ if bit $b = 1$ and finally gives (K', Hdr) to $\mathcal{A}$.
5. The adversary $\mathcal{A}$ outputs a guess bit b'.

As usual, $\mathcal{A}$ wins the game if $b = b'$, and its advantage is defined as

$$Adv^{ind}(\lambda, n, \{S_u\}_{u\in[n]}, \mathcal{A}) = |2Pr[b = b'] - 1|$$

where the probability is taken over the random bit b and all the bits used in the simulation of the algorithms **Setup**(.), and **Encrypt**(.). The semantic security against full static collusions is defined as follows.

Definition 1. *A* CP-ABBE *scheme is semantically secure against full static collusions if for all randomized polynomial-time adversaries $\mathcal{A}$ and for all access policies involving at most N attributes defined by $\{S_u\}_{\in[n]}$,*

$$Adv^{ind}(1^\lambda, n, \{S_u\}_{u\in[n]}, \mathcal{A})$$

is a negligible function of λ when N, n are at most polynomial in λ.

2.3 Access Structures

Definition 2 (Access Structures). *Let $\{P_1, P_2, \ldots, P_n\}$ be a set of parties. A collection $\mathbb{A} \subseteq 2^{\{P_1,P_2,\ldots,P_n\}}$ is monotone if $\forall B, C$: if $B \in \mathbb{A}$ and $B \subseteq C$ then $C \in \mathbb{A}$. An access structure (respectively, monotone access structure) is a collection (respectively, monotone collection) $\mathbb{A}$ of non-empty subsets of $\{P_1, P_2, \ldots, P_n\}$, i.e, $\mathbb{A} \subseteq 2^{\{P_1,P_2,\ldots,P_n\}} \setminus \{\emptyset\}$. The sets in $\mathbb{A}$ are called the authorized sets, and the sets not in $\mathbb{A}$ are called the unauthorized sets.*

In this paper, we consider the monotone access structures. However, as shown in [15], it is also possible to extend such case to the general access structures, at the cost of a doubled number of attributes in the system.

2.4 Bilinear Maps and $(P, Q, f) - \mathsf{GDDHE}$ Assumptions

Let $\mathbb{G}$, $\widetilde{\mathbb{G}}$ and $\mathbb{G}_T$ denote three finite multiplicative abelian groups of large prime order $p > 2^\lambda$ where λ is the security parameter. Let g be a generator of $\mathbb{G}$ and $\tilde{g}$ be a generator of $\widetilde{\mathbb{G}}$. We assume that there exists an admissible asymmetric bilinear map $e : \mathbb{G} \times \widetilde{\mathbb{G}} \to \mathbb{G}_T$, meaning that for all $a, b \in \mathbb{Z}_p$, (i) $e(g^a, \tilde{g}^b) = e(g, \tilde{g})^{ab}$, (ii) $e(g^a, \tilde{g}^b) = 1$ iff $a = 0$ or $b = 0$, and (iii) $e(g^a, \tilde{g}^b)$ is efficiently computable. In the sequel, the set $(p, \mathbb{G}, \widetilde{\mathbb{G}}, \mathbb{G}_T, e)$ is called a bilinear map group system.

Let $(p, \mathbb{G}, \widetilde{\mathbb{G}}, \mathbb{G}_T, e)$ be a bilinear map group system and $g \in \mathbb{G}$ (resp. $\tilde{g} \in \widetilde{\mathbb{G}}$) be a generator of $\mathbb{G}$ (resp. $\widetilde{\mathbb{G}}$). We set $g_T = e(g, \tilde{g}) \in \mathbb{G}_T$. Let s, n be positive integers and $P, Q, R \in \mathbb{F}_p[X_1, \ldots, X_n]^s$ be three s-tuples of n-variate polynomials over $\mathbb{F}_p$. Thus, P, Q and R are just three lists containing s multivariate polynomials each. We write $P = (p_1, p_2, \ldots, p_s)$, $Q = (q_1, q_2, \ldots, q_s)$, $R = (r_1, r_2, \ldots, r_s)$ and impose that $p_1 = q_1 = r_1 = 1$. For any function $h : \mathbb{F}_p \to \Omega$ and any vector $(x_1, \ldots, x_n) \in \mathbb{F}_p^n$, $h(P(x_1, \ldots, x_n))$ stands for $\big(h(p_1(x_1, \ldots, x_n)), \ldots, h(p_s(x_1, \ldots, x_n))\big) \in \Omega^s$. We use a similar notation for the s-tuples Q and R. Let $f \in \mathbb{F}_p[X_1, \ldots, X_n]$. It is said that f depends on (P, Q, R), which denotes $f \in \langle P, Q, R\rangle$, when there exists a linear decomposition (with an efficient isomorphism between $\mathbb{G}$ and $\widetilde{\mathbb{G}}$):

$$f = \sum_{1 \le i,j \le s} a_{i,j} \cdot p_i \cdot q_j + \sum_{1 \le i,j \le s} b_{i,j} \cdot p_i \cdot p_j + \sum_{1 \le i \le s} c_i \cdot r_i,$$

where $a_{i,j}, b_{i,j}, c_i \in \mathbb{Z}_p$.

We moreover have $b_{i,j} = 0$ when there is no efficiently computable homomorphism between $\mathbb{G}$ and $\widetilde{\mathbb{G}}$. Let P, Q, R be as above and $f \in \mathbb{F}_p[X_1, \ldots, X_n]$. The $(P, Q, R, f) - \mathsf{GDDHE}$ problem is defined as follows.

Definition 3 ($(P, Q, R, f) - \mathsf{GDDHE}$) [1].
Given the vector $H(x_1, \ldots, x_n) = (g^{P(x_1,\ldots,x_n)}, \tilde{g}^{Q(x_1,\ldots,x_n)}, g_T^{R(x_1,\ldots,x_n)}) \in \mathbb{G}^s \times \widetilde{\mathbb{G}}^s \times \mathbb{G}_T^s$ as above and $T \in \mathbb{G}_T$ decide whether $T = g_T^{f(x_1,\ldots,x_n)}$.

The $(P, Q, R, f) - \mathsf{GDDHE}$ assumption says that it is hard to solve the $(P, Q, R, f) - \mathsf{GDDHE}$ problem if f is linearly independent of (P, Q, R). In this paper, we will prove that our scheme is semantically secure under this assumption.

3 Construction

3.1 Intuition Behind Our Construction

Delerablée's technique. In this paper, we extend the Delerablée's technique of constructing an IBBE scheme [5] into our CP-ABBE context. In [5], the user's private key is of the form $g^{\frac{1}{\alpha+\mathsf{ID}_u}}$, the ciphertext is constructed corresponding to a target set of identities $S = (\mathsf{ID}_{i_1}, \ldots, \mathsf{ID}_{i_k})$ is of the form

$$g^{\prod_{j=i_1}^{j=i_k}(\alpha+\mathsf{ID}_j)}$$

and as long as user's identity is "divided" by S (it means $\mathsf{ID}_u \in S$), she can decrypt. In our scheme, each user u possesses a set of attributes S_u and each clause in the DNF access policy is a set of attributes β_i: as long as there is at least a set β_i which is "divided" by S_u then the user u can decrypt.

Our adaptation. When applying the above technique in ABE's context, the result is in the reversed form in which a user can decrypt if S_u is "divided" by β_i. To deal with this problem, we employ a reversed technique to generate the user's private key by using the user's "reversed" attribute set $\mathcal{U} \setminus S_u$, where $\mathcal{U}$ is the attribute universe. Now, if β_i is "divided" by S_u then $\mathcal{U} \setminus S_u$ is "divided" by $\mathcal{U} \setminus \beta_i$. We then produce the ciphertext in the same way as in [5] (by using $\mathcal{U} \setminus \beta_i$ instead of β_i).

Re-use randomness vs. collusion. In our ABBE scheme, the access policy contains many clauses, each clause β_i corresponds to a target set in the Delerablée's IBBE scheme, and it is related to a ciphertext component C_i. In order to make the decryption work, all the components C_i are required to use the same randomness and the collusion can take some advantage in exploiting this point. In order to neutralize the advantage of the adversary, we will make use of the "dummy technique" by choosing a random dummy attribute set in creating each C_i. Consequently, each C_i is randomized since the random dummy attribute set now plays the role of a fresh randomness.

3.2 Our Scheme

We now describe our scheme which uses the type 3 paring.

Setup$(1^\lambda, n, \{S_u\}_{\in[n]})$**:** Assume that the maximum number of attributes is N, the maximum number of clauses in an access policy is N'.
Assume that the attribute universe is $\mathcal{U} = \{A_1, \ldots, A_N\} \in \mathbb{Z}_p^N$, the dummy attribute universe is $\mathcal{U}' = \{B_{i,j}\}_{\substack{i\in[N']\\ j\in[N']}} \in \mathbb{Z}_p^{N'\times N'}$, suppose that the set of identities of users in the system is $\mathcal{ID} = \{\mathsf{ID}_1, \ldots, \mathsf{ID}_n\} \in \mathbb{Z}_p^n$. The algorithm generates a bilinear map group system $D = (p, \mathbb{G}, \widetilde{\mathbb{G}}, \mathbb{G}_T, e)$, then chooses $h \xleftarrow{\$} \widetilde{\mathbb{G}}, g \xleftarrow{\$} \mathbb{G}$ and $\alpha, \gamma \xleftarrow{\$} \mathbb{Z}_p$. Finally, it outputs:

$$\mathsf{param} = (\mathcal{U}, \mathcal{U}', \mathcal{ID}, D, \{h^{\alpha^r\cdot\gamma^t}\}_{\substack{r=0,\ldots,N\\ t=0,\ldots,n+N'}}, h^{\frac{\gamma}{\alpha}}, \ldots, h^{\frac{\gamma^{n+N'}}{\alpha}}, g^\alpha, e(g,h))$$

and

$$sk_u = g^{\frac{1}{(\gamma+\mathsf{ID}_u)\cdot\prod_{i\in\mathcal{U}\setminus S_u}(\alpha+A_i)}}.$$

Encrypt$(\mathsf{param}, \beta = (\beta_1 \vee \beta_2 \vee \cdots \vee \beta_m), S)$**:** the algorithm first checks that $\beta_i \neq \beta_j$ for all $i, j \in [m], i \neq j$, then picks a random $k \in \mathbb{Z}_p$ then computes:

$$C_0 = g^{-k.\alpha}, K = e(g,h)^k$$
$$C_1 = h^{k.\prod_{j\in[m]}(\gamma+B_{1,j})\cdot\prod_{i\in\mathcal{U}\setminus\beta_1}(\alpha+A_i)\cdot\prod_{i\in S}(\gamma+\mathsf{ID}_i)}, \ \ldots,$$
$$C_m = h^{k.\prod_{j\in[m]}(\gamma+B_{m,j})\cdot\prod_{i\in\mathcal{U}\setminus\beta_m}(\alpha+A_i)\cdot\prod_{i\in S}(\gamma+\mathsf{ID}_i)}$$

Finally, it outputs K and $\mathsf{Hdr} = (C_0, C_1, \ldots, C_m)$ which includes β and S.

Decrypt$(sk_u, \mathsf{Hdr}, \mathsf{param})$**:** the algorithm first finds the set β_j such that $\beta_j \subset S_u$ and checks that $u \in S$, then computes $K' =$

$$h^{\frac{1}{\alpha}(\prod_{i\in[m]}(\gamma+B_{j,i})\cdot\prod_{i\in S_u\setminus\beta_j}(\alpha+A_i)\cdot\prod_{i\in S,i\neq u}(\gamma+\mathsf{ID}_i)-\prod_{i\in[m]}B_{j,i}\cdot\prod_{i\in S_u\setminus\beta_j}A_i\cdot\prod_{i\in S,i\neq u}\mathsf{ID}_i)}$$

Note that it is able to compute K' from the param. It finally computes

$$K = (e(C_0, K')\cdot e(sk_u, C_j))^{\frac{1}{\prod_{i\in[m]}B_{j,i}\cdot\prod_{i\in S_u\setminus\beta_j}A_i\cdot\prod_{i\in S,i\neq u}\mathsf{ID}_i}}.$$

4 Security

Intuitively, following the security model in the Sect. 2.2 we need to prove that given all elements corresponding to the public global parameters, the private decryption keys of corrupted users, and the challenge header, the adversary $\mathcal{A}$ cannot distinguish between a real session key K and a random element in $\mathbb{G}_T$. Therefore, if we define P, Q, R to be the list of polynomials consisting of all elements corresponding to the public global parameters, the private decryption keys of corrupted users, and the challenge header, we need to prove that the following $(P, Q, R, f) - \mathsf{GDDHE}$ assumption holds (that means f is independent to (P, Q, R)), where f corresponds to the real session key. The definition of P, Q, R and f for our $(P, Q, R, f) - \mathsf{GDDHE}$ instance is given by Fig. 1.

Lemma 1. *In the* $(P, Q, R, f) - \mathsf{GDDHE}$ *assumption above,* (P, Q, R) *and* f *are linearly independent.*

The semantic security of our scheme now is stated as follows.

Theorem 1. *If there exists an adversary* $\mathcal{A}$ *that solves the semantic security of our scheme with advantage* $Adv^{ind}(.)$*, then we can construct a simulator to solve an instance of the* $(P, Q, R, f) - \mathsf{GDDHE}$ *problem above with the same advantage* $Adv^{ind}(.)$*.*

We refer the proofs of the above lemma and theorem to the full version of the paper.

$$P = \left\{ \alpha, -k\alpha, \left(\frac{1}{(\gamma + \mathsf{ID}_u) \prod_{i \in \mathcal{U} \setminus S_u} (\alpha + A_i)} \right)_{u \in [n']} \right\}$$

$$Q = \left\{ \left(\alpha^r \cdot \gamma^t \right)_{\substack{r=0,\ldots,N \\ t=0,\ldots,n+N'}}, \left(\frac{\gamma^i}{\alpha} \right)_{i \in [n+N']}, \right.$$

$$\left. \left(k \cdot \prod_{j \in [m]} (\gamma + B_{i,j}) \prod_{j \in \mathcal{U} \setminus \beta_i} (\alpha + A_j) \cdot \prod_{j \in S} (\gamma + \mathsf{ID}_j) \right)_{i=1,\ldots,m} \right\}$$

$$R = \{1\}, \qquad f = k$$

for all n' corrupted user u, $1 \leq n' < n$.

Fig. 1. $(P, Q, R, f) - \mathsf{GDDHE}$ instance

5 Implementation and Optimization

We have implemented our CP-ABBE in the scenario given in Sect. 2.1. We have tested several values for the number n of users and the maximum number of attributes N, we also give some tricks when implementing to optimize the encryption phase and decryption phase. We refer the optimization and benchmarks of our implementation to the full version of the paper.

Acknowledgments. This work was partially supported by the French ANR Project ANR-12-INSE-0014 SIMPATIC and partially conducted within the context of the Vietnamese Project Pervasive and Secure Information Service Infrastructure for Internet of Things based on Cloud Computing.

References

1. Boneh, D., Boyen, X., Goh, E.-J.: Hierarchical identity based encryption with constant size ciphertext. In: Cramer, R. (ed.) EUROCRYPT 2005. LNCS, vol. 3494, pp. 440–456. Springer, Heidelberg (2005). doi:10.1007/11426639_26
2. Boneh, D., Gentry, C., Waters, B.: Collusion resistant broadcast encryption with short ciphertexts and private keys. In: Shoup, V. (ed.) CRYPTO 2005. LNCS, vol. 3621, pp. 258–275. Springer, Heidelberg (2005). doi:10.1007/11535218_16
3. Canard, S., Trinh, V.C.: Private ciphertext-policy attribute-based encryption schemes with constant-size ciphertext supporting CNF access policy (2015). http://eprint.iacr.org/2015/891
4. Chen, J., Gay, R., Wee, H.: Improved dual system ABE in prime-order groups via predicate encodings. In: Oswald, E., Fischlin, M. (eds.) EUROCRYPT 2015. LNCS, vol. 9057, pp. 595–624. Springer, Heidelberg (2015). doi:10.1007/978-3-662-46803-6_20
5. Delerablée, C.: Identity-based broadcast encryption with constant size ciphertexts and private keys. In: Kurosawa, K. (ed.) ASIACRYPT 2007. LNCS, vol. 4833, pp. 200–215. Springer, Heidelberg (2007). doi:10.1007/978-3-540-76900-2_12
6. Hohenberger, S., Waters, B.: Attribute-based encryption with fast decryption. In: Kurosawa, K., Hanaoka, G. (eds.) PKC 2013. LNCS, vol. 7778, pp. 162–179. Springer, Heidelberg (2013). doi:10.1007/978-3-642-36362-7_11

7. Junod, P., Karlov, A.: An efficient public-key attribute-based broadcast encryption scheme allowing arbitrary access policies. In: ACM Workshop on Digital Rights Management, pp. 13–24. ACM Press (2010)
8. Liu, Z., Cao, Z., Wong, D.S.: Blackbox traceable CP-ABE: how to catch people leaking their keys by selling decryption devices on eBay. In: Sadeghi, A.-R., Gligor, V.D., Yung, M. (eds.) ACM CCS 2013, Berlin, Germany, pp. 475–486. ACM Press, 4–8 November 2013
9. Liu, Z., Wong, D.S.: Practical attribute-based encryption: traitor tracing, revocation, and large universe. In: ACNS 15 (2015)
10. Lubicz, D., Sirvent, T.: Attribute-based broadcast encryption scheme made efficient. In: Vaudenay, S. (ed.) AFRICACRYPT 2008. LNCS, vol. 5023, pp. 325–342. Springer, Heidelberg (2008). doi:10.1007/978-3-540-68164-9_22
11. Ostrovsky, R., Sahai, A., Waters, B.: Attribute-based encryption with non-monotonic access structures. In: Ning, P., di Vimercati, S.D.C., Syverson, P.F. (eds.) ACM CCS 2007, Alexandria, Virginia, USA, pp. 195–203. ACM Press, 28–31 October 2007
12. Phuong, T.V.X., Yang, G., Susilo, W., Chen, X.: Attribute based broadcast encryption with short ciphertext and decryption key. In: Pernul, G., Ryan, P.Y.A., Weippl, E. (eds.) ESORICS 2015. LNCS, vol. 9327, pp. 252–269. Springer, Heidelberg (2015). doi:10.1007/978-3-319-24177-7_13
13. Rouselakis, Y., Waters, B.: Practical constructions and new proof methods for large universe attribute-based encryption. In: Sadeghi, A.-R., Gligor, V.D., Yung, M. (eds.) ACM CCS 2013, Berlin, Germany, pp. 463–474. ACM Press, 4–8 November 2013
14. Sahai, A., Waters, B.: Fuzzy identity-based encryption. In: Cramer, R. (ed.) EUROCRYPT 2005. LNCS, vol. 3494, pp. 457–473. Springer, Heidelberg (2005). doi:10.1007/11426639_27
15. Waters, B.: Ciphertext-policy attribute-based encryption: an expressive, efficient, and provably secure realization. In: Catalano, D., Fazio, N., Gennaro, R., Nicolosi, A. (eds.) PKC 2011. LNCS, vol. 6571, pp. 53–70. Springer, Heidelberg (2011). doi:10.1007/978-3-642-19379-8_4
16. Yamada, S., Attrapadung, N., Hanaoka, G., Kunihiro, N.: A framework and compact constructions for non-monotonic attribute-based encryption. In: Krawczyk, H. (ed.) PKC 2014. LNCS, vol. 8383, pp. 275–292. Springer, Heidelberg (2014). doi:10.1007/978-3-642-54631-0_16