New Identity-based Broadcast Encryption with Constant Ciphertexts in the Standard Model

Qing Wu, Wenqing Wang
School of Automation, Xi'an Institute of Posts and Telecommunications,
Xi'an, Shaanxi, 710121 P. R. China
Email: xidianwq@yahoo.com.cn

***Abstract*—How to build an efficient identity-based broadcast system with short ciphertexts is a main challenge at present. The existing constructions with constant size ciphertexts in the standard model are based on the non-standard cryptography assumption. In addition, these constructions cannot solve the trade-off between the private keys and ciphertexts. Hence these methods lead to schemes that are somewhat inefficient in the real world. To overcome these shortcomings, two schemes are introduced at first. The initial construction has constant size ciphertexts and O(|*S*|)-size private keys(where *S* denotes the set of receivers). Then the second scheme achieves constant size ciphertexts and constant size private keys which solve the trade-off between the private keys and ciphertexts. Furthermore, their security rests on the hardness of the decision Diffie-Hellman Exponent problem instead of other strong assumptions. However, both schemes only achieve a weak security-selective-identity security. Finally, two helpful constructions are proposed. They are constructed in the standard model and achieve full security which is stronger than selective-identity security.**

***Index Terms*—Broadcast encryption, standard model, short ciphertexts, identity-based encryption, provable security**

I. INTRODUCTION

The concept of Broadcast Encryption (BE) was introduced by Fiat and Naor in [1]. In a broadcast encryption scheme a broadcaster encrypts a message for some subset of users who are listening on a broadcast channel. Any user in it can use his private key to decrypt the broadcast. Any user outside the privileged set should not be able to recover the message. Recently it has been widely used in digital rights management applications such as pay-TV, multicast communication, and DVD content protection. Since the first scheme appeared in 1994, many BE schemes have been proposed [2-5].

Identity-based encryption (IBE) was introduced by Shamir[6]. It allows for a party to encrypt a message using the recipient's identity as a public key. The ability to use identities as public keys avoids the need to distribute public key certificates. So it can simplify many applications of public key encryption (PKE) and is currently an active research area. The first efficient IBE was proposed by Boneh and Franklin[7] in 2001. They proposed a solution using efficiently computable bilinear maps that was shown to be secure in the random oracle model. Since then, there have been many schemes shown to be secure without random oracles[8-12].

Identity-based broadcast encryption(IBBE)[14] is a generalization of IBE. One public key can be used to encrypt a message to any possible identity in IBE schemes. But in an IBBE scheme, one public key can be used to encrypt a message to any possible group of S identities. Recently, many IBBE schemes had been proposed[13-17]. But the well known construction of IBBE was the scheme of Delerablée [14]. This construction achieved constant size private keys and constant size ciphertexts. However her main scheme was only provable selective-identity security under the random oracles. In [16,17], two schemes with full security were proposed. But they were impractical in real-life practice since their security relied on the complex assumptions which were dependent on the depth of users set and the number of queries made by an attacker. In addition, recent work in [17] had the sublinear-size ciphertexts. Moreover, the authors in [17] used a sub-algorithm at the Encrypt phase to achieve full security.

With this motivation, we propose some new efficient identity-based broadcast encryption schemes in this paper. The initial construction has constant size ciphertexts and O(|*S*|)-size private keys(where *S* denotes the set of receivers). Then the second scheme achieves constant size ciphertexts and private keys, which solve the trade-off between the private keys and ciphertexts. However, both schemes only achieve selective-identity security. Finally, two helpful constructions are proposed, which are constructed in the standard model and achieve full security.

II. Preliminaries

A. Bilinear Diffie-Hellman Exponent(BDHE) Assumption

The BDHE problem is defined as follows: Given a tuple $Y=(g,h,g^{a},\cdots,g^{a^{m}},g^{a^{m+2}},\cdots,g^{a^{2m}})$ compute $e(g,h)^{a^{m+1}}$, where e() is a bilinear pair, (*g*, *h*) are selected from G and $\alpha \in Z_p^*$. The decision BDHE problem is as follows: Given a tuple (Y,T), decide whether $T=e(g,h)^{a^{m+1}}$ or T is a random element in G_1.

doi:10.4304/jsw.6.10.1929-1936

An algorithm B that outputs $b \in \{0, 1\}$ has advantage ε in solving decision BDHE in G if

$$|\Pr[B(Y, e(g,h)^{a^{m+1}})=0]- \Pr[B(Y, T)=0]| \geq \varepsilon .$$

The (t, ε)-BDHE assumption holds if no adversary has at least ε advantage in solving the above problem with polynomial time t.

B. Identity-based Broadcast Encryption

An identity-based broadcast encryption scheme (IBBE) consists of four algorithms and is specified as follows.

Setup Take as input the security parameter, Setup outputs a master secret key and a public key. The *PKG* is given the master secret key, and the public key is made publicized.

Extract Take as input the master secret key and a user identity *ID*. Extract generates a user private key d_{ID}.

Encrypt Take as input the public key and a set of included identities $S=\{ID_1,\ldots, ID_s\}$ with $s \leq m$, and outputs a pair (*Hdr, K*), where Hdr is called the header and *K* is a key for the symmetric encryption scheme. When a message *M* is to be broadcast to users in S, the broadcaster generates (*Hdr*,*K*), computes the encryption *CM* of *M* under the symmetric key *K* and broadcasts (*Hdr*, *S*, *CM*).

Decrypt Take as input a subset $S=\{ID_1, \ldots, ID_s\}$ with $s \leq m$, an identity ID_i and the corresponding private key, a header *Hdr* and the public key, If $ID \in S$, the algorithm outputs the message encryption key K which is then used to decrypt the broadcast body *CM* and recover *M*.

C. Security model for IBBE

We give the *IND-sID-CCA* security of an IBBE system. The security model is defined by using the following game played between an adversary A and a challenger. Both the adversary and the challenger are given as input *m*, the maximal size of a set of receivers *S*.

Init The adversary A firstly outputs a set $S^*=\{ID_1^*,\cdots,ID_s^*\}$ of identities that he wants to attack (with $s \leq m$).

Setup The challenger runs Setup to obtain a public key PK and sends the public key *PK* to *A*.

***Query phase* 1** The adversary *A* adaptively issues queries $q_1,\cdots,q_{s0}$, where q_i is one of the following:

- Extraction query (ID_i) with the constraint that $ID_i \notin S^*$: The challenger runs Extract on ID_i and sends the resulting private key to the adversary.
- Decryption query for a triple (ID_i, *S*, *Hdr*) with $S \subseteq S^*$ and $ID_i \in S$. The challenger responds with Decrypt(*S*, ID_i, *Hdr*, *PK*).

Challenge When *A* decides that phase 1 is over, the challenger runs Encrypt algrithm to obtain (Hdr^*,*K*) = Encrypt(S^*, *PK*). The challenger then randomly selects $b \in \{0, 1\}$, sets $K_b = K$, and sets K_{1-b} to a random value in $\tilde{K}$. The challenger returns (Hdr^*,K_0, K_1) to *A*.

Query phase 2 The adversary continues to issue queries $q_{s0+1}, \cdots, q_s$, where q_i is one of the following:

- Extraction query (ID_i), as in phase 1.
- Decryption query, as in phase 1, but with the constraint that $Hdr \neq Hdr^*$. The challenger responds as in phase 1.

Guess Finally, the adversary A outputs a guess $b' \in \{0, 1\}$ and wins the game if $b = b'$.

We say that if the above indistinguishability game allow no decryption oracle query, then the IBBE scheme is only chosen plaintext (*IND-ID-CPA*) secure. There have been many methods to convert an *IND-ID-CPA* scheme to an *IND-sID-CCA* scheme. Therefore, we only focus on constructing the *IND-ID-CPA* scheme in this paper.

III. New constructions

Our constructions are based on a HIBE scheme. We first recall it as follows:

Setup To generate system parameters for an HIBE of maximum depth l, select a random generator $g \in G$ and some random elements g_2, g_3, h_i from G (where $i=1,\ldots,l$). Then pick a random $\alpha \in Z_p$ and set $g_1 = g^{\alpha}$. We set $\mathbf{H} = (h_i)$ where $i=1,\ldots,l$. The system parameters are param=($g, g_1, g_2, g_3, \mathbf{H}$) and master key is g_2^{α}.

Extract Given the identity $ID_{k-1}=(v_1,\cdots,v_{k-1})$ and the corresponding private key

$$d_{ID_{k-1}} = (a_0, a_1, a_k, \cdots, a_l) = (g_2^{\alpha}(g_3\prod_{i=1}^{k-1} h_i^{v_i})^{r'}, g^{r'}, h_k^{r'}, \cdots h_l^{r'}),$$

the private key corresponding to $ID_k=(v_1,\cdots,v_k)$ is constructed as follows:

select randomly $r_i \in Z_p$ and compute private keys as follows:

$$\begin{aligned} d_{ID_k} &= (d_0, d', d_{k+1}, \cdots, d_l) \\ &= (a_0 a_k^{v_k}(g_3\prod_{i=1}^{k-1} h_i^{v_i})^{r_i}, a_1 g^{r_i}, a_{k+1}h_{k+1}^{r_i}, \cdots, a_l h_l^{r_i}) \\ &= (g_2^{\alpha}(g_3\prod_{i=1}^{k-1} h_i^{v_i})^{r}, g^{r}, h_{k+1}^{r}, \cdots, h_l^{r}), \end{aligned}$$

where $r = r' + r_i$.

Encrypt To encrypt message *M* under identity $ID_k=(v_1,\cdots,v_k)$, pick randomly $t \in Z_p$ and compute:

$$C = (C_0, C_1, C_2) = (e(g_1, g_2)^t M, g^t, (g_3\prod_{i=1}^{s} h_i^{ID_i})^t).$$

Decrypt Given the ciphertexts $C = (C_0, C_1, C_2)$, the user $ID_k=(v_1,\cdots,v_k)$ uses his private keys $d_{ID_k} = (d_0, d', d_{k+1}, \cdots, d_l)$ to compute

$$M = C_0 \frac{e(C_2, d')}{e(d_0, C_1)}.$$

A. Initial construction

We first give the initial construction.

Setup Select a random generator $g \in G$ and some random elements g_2 , g_3 , h_i from G (where *i=1,...,m*). Then pick a random $\alpha \in Z_p$ and set $g_1 = g^\alpha$. We set $\mathbf{H} = (h_i)$ where *i=1,...,m*. The system parameters are param=($g, g_1, g_2, g_3, \mathbf{H}$) and master key is g_2^α .

Extract Given the identity ID_i, *PKG* selects randomly $r_i \in Z_p$ and computes private keys as follows:

$$d_{ID_i} = (d_0, d', d_1, \cdots, d_{i-1}, d_{i+1}, \cdots, d_s)$$

$$= (g_2^\alpha (g_3 h_i^{ID_i})^{r_i}, g^{r_i}, h_1^{r_i}, \cdots, h_{i-1}^{r_i}, h_{i+1}^{r_i}, \cdots h_s^{r_i}).$$

Encrypt Given $S=\{ID_1, \ldots, ID_s\}$ and message *M*, the broadcaster randomly picks $t \in Z_p$ and computes:

$$Hdr = (C_1, C_2) = [g^t, (g_3 \prod_{i=1}^{s} h_i^{ID_i})^t];$$

$$C = (C_0, Hdr) = [e(g_1, g_2)^t M, Hdr].$$

Decrypt Given the ciphertexts $C = (C_0, C_1, C_2)$, any user $ID_i \in S$ uses his private keys d_{ID_i} to compute

$$M = C_0 \frac{e(C_2, d')}{e(d_0 \prod_{j=1, j\neq i}^{s} d_j^{ID_j}, C_1)}.$$

Correctness: In fact,

$$\frac{e(C_2, d')}{e(d_0 \prod_{j=1, j\neq i}^{s} d_j^{ID_j}, C_1)}$$

$$= \frac{e((g_3 \prod_{i=1}^{s} h_i^{ID_i})^t, g^{r_i})}{e(g_2^\alpha (g_3 \prod_{i=1}^{s} h_i^{ID_i})^{r_i}, g^t)}$$

$$= \frac{1}{e(g_1, g_2)^t}.$$

B. Security Analysis

Theorem 3.1 Suppose that the (t, ε) decision BDHE assumption holds, then our new protocol is (t', ε) *-IND-ID-CPA* secure with $t' = t - O(q\tau + q\rho)$, where ρ and τ denote the maximum time for a multiplication and an exponentiation respectively, q denotes the maximum time for queries.

Proof: Suppose there exists a (t, q, ε) attacker *A* against our scheme, then we will construct an algorithm *B* to solve the (t', ε') decision BDHE problem. We define the selective-identity game between *A* and *B* as follows:

Initialization A first outputs a set of identities $S^* = (v_1^*, \cdots, v_s^*)$ with $s \le m$ that it intends to attack. If $s < m$, B pads S^* with $m - s$ zeros on the last to make S^* a vector of length m.

Setup For a random generator g of G and a random $\alpha \in Z_p$, *B* is given as input a tuple (g , h , $g^\alpha, \cdots, g^{\alpha^m}$, $g^{\alpha^{m+2}}, \cdots, g^{\alpha^{2m}}$, *T*). To generate the system parameters, *B* picks a random $\gamma \in Z_p$ and sets $g_1 = g^\alpha$ and $g_2 = g^{\alpha^m} g^\gamma = g^{\gamma + \alpha^m}$. Next, *B* picks randomly $\gamma_1, \cdots, \gamma_m$ in Z_p and sets $h_i = g^{\gamma_i} / Y_{m-i+1}$ and $Y_i = g^{\alpha^i} \in G$, where $1 \le i \le m$. It also picks randomly a μ and sets $g_3 = g^\mu \prod_{i=1}^{m} Y_{m-i+1}^{v_i^*}$. Finally, *B* sends the public keys

$$param = (g, g_1, g_2, g_3, h_1, \cdots, h_m)$$

to *A*. The master key corresponding to these parameters is $g_2^\alpha = g^{(\gamma + \alpha^m)\alpha} = Y_1^\gamma Y_{m+1}$ which is unknown to *B*.

Phase 1: A issues up to m private key queries. Each query is specified as follows: Suppose the adversary A issues a query for an identity v_i .The only restriction is that $v_i \notin S^*$ .This restriction ensures that $v_i - v_j^* \neq 0$. Then B constructs a private key for v_i . It selects randomly a $r' \in Z_p$ and computes the private key corresponding v_i as follows:

$$d_{v_i} = (g_2^\alpha (g_3 h_i^{v_i})^r, g^r, h_1^r, \cdots, h_{i-1}^r, h_{i+1}^r, \cdots, h_s^r),$$

where $r = r' + \frac{\alpha^i}{v_i - v_i^*}$. In deed, we can obtain

$$g_2^\alpha (g_3 h_i^{v_i})^r$$

$$= Y_1^\gamma Y_{m+1} (g^\mu \prod_{j=1}^{m} Y_{m-j+1}^{v_j^*} (\tfrac{g^{\gamma_i}}{Y_{m-i+1}})^{v_i})^r$$

$$= Y_1^\gamma Y_{m+1} (g^\mu \prod_{j=1}^{i-1} Y_{m-j+1}^{v_j^*} \cdot Y_{m-i+1}^{v_i^*} (\tfrac{g^{\gamma_i}}{Y_{m-i+1}})^{v_i} \cdot \prod_{j=i+1}^{m} Y_{m-j+1}^{v_j^*})^r$$

$$= Y_1^\gamma Y_{m+1} (g^{\mu + \gamma_i v_i} \prod_{j=1}^{i-1} Y_{m-j+1}^{v_j^*} Y_{m-i+1}^{v_i^* - v_i} \prod_{j=i+1}^{m} Y_{m-j+1}^{v_j^*})^r \quad (1)$$

where

$$(g^{\mu + \gamma_i v_i} \prod_{j=1}^{i-1} Y_{m-j+1}^{v_j^*} Y_{m-i+1}^{v_i^* - v_i} \prod_{j=i+1}^{m} Y_{m-j+1}^{v_j^*})^r$$

$$= (g^{\mu + \gamma_i v_i} \prod_{j=1}^{i-1} Y_{m-j+1}^{v_j^*} Y_{m-i+1}^{v_i^* - v_i} \prod_{j=i+1}^{m} Y_{m-j+1}^{v_j^*})^{r' + \frac{\alpha^i}{v_i - v_i^*}}$$

$$= (g^{\mu+\gamma_i v_i} \prod_{j=1}^{i-1} Y_{m-j+1}^{v_j^*} Y_{h-i+1}^{v_i^*-v_i} \prod_{j=i+1}^{m} Y_{m-j+1}^{v_j^*})^r (Y_{m-i+1}^{v_i^*-v_i})^{r'+\frac{\alpha^i}{v_i-v_i^*}}$$

$$= (g^{\mu+\gamma_i v_i} \prod_{j=1}^{i-1} Y_{m-j+1}^{v_j^*} Y_{h-i+1}^{v_i^*-v_i} \prod_{j=i+1}^{m} Y_{m-j+1}^{v_j^*})^r (Y_{m-i+1}^{v_i^*-v_i})^{r'} Y_{m+1}^{-1}$$

According to (1), one can obtain

$$g_2^{\alpha}(g_3 \prod_{i=1}^{k} h_i^{v_i})^r$$

$$= Y_1^{\gamma}\ (g^{\mu+\gamma_i v_i} \prod_{j=1}^{i-1} Y_{m-j+1}^{v_j^*} Y_{h-i+1}^{v_i^*-v_i} \prod_{j=i+1}^{m} Y_{m-j+1}^{v_j^*})^r (Y_{m-i+1}^{v_i^*-v_i})^{r'} .$$

Since all the terms in this expression are known to B. Thus, B can compute the first private key component. B computes $Y_i^{\frac{1}{v_i-v_i^*}} g^{r'} = g^r$. Then the second component of private keys is obtained. Similarly, the remaining elements h_i^r can be computed by B since they do not involve a term Y_{m+1}. Thus, B can derive a valid private key for v_i.

Challenge When A decides that Phase 1 is over, it outputs two messages M_0, M_1 on which it wishes to be challenged. Algorithm B picks a random bit b□{0, 1} and responds with the challenge ciphertexts

$$C^* = (C_0^*, C_1^*, C_2^*)$$

$$= (M_b T e(Y_1, h^{\gamma}), h, h^{\mu+\sum_{i=1}^{m} v_i^* \gamma_i}),$$

where $h \in G$. If $T = e(g,h)^{a^{m+1}}$, one can obtain C^* is a valid encryption for Mb. In fact, let $h = g^t$. Then

$$C_0^* = Te(Y_1, h^{\gamma}) M_b$$

$$= e(g,h)^{a^{m+1}}\ e(Y_1, h^{\gamma}) M_b$$

$$= [e(Y_1, g^{\gamma})\ e(Y_1, Y_m)]^t\ M_b$$

$$= e(Y_1, Y_m g^{\gamma})^t\ M_b = e(g_1, g_2)^t\ M_b ;$$

$$C_1^* = g^t ;$$

$$h^{\mu+\sum_{i=1}^{m} v_i^* \gamma_i} = g^{t(\mu+\sum_{i=1}^{m} v_i^* \gamma_i)}$$

$$= (g^{\mu} \prod_{i=1}^{m} Y_{m-i+1}^{v_i^*} \prod_{i=1}^{m} \frac{g^{\gamma_i v_i^*}}{Y_{m-i+1}^{v_i^*}})^t$$

$$= (g_3 \prod_{i=1}^{m} h_i^{v^*})^t = C_2^* .$$

On the other hand, when T is uniform and independent in G_1, C^* is independent of b in the adversary's view.

Phase 2: The adversary continues to issue Extract queries with the constraint that the querying identity $v_i \notin S^*$.

Guess Finally, A outputs a guess $b' \in$ {0, 1}, and wins the game if $b' = b$.

If A wins the game, it means that B knows $T = e(g,h)^{a^{m+1}}$ or random element of G_1. It shows B successfully solves the decision BDH problem. When T is random in G_1 then Pr[B(Y, T) = 0]= 1/2; Otherwise $T = e(g,h)^{a^{m+1}}$, B replies with a valid challenge C* and then |Pr[b = b']−1/2| $\geq \varepsilon$. Therefore, B has that

$$|\Pr[B(Y, e(g,h)^{a^{m+1}}) = 0] - \Pr[B(Y,T) = 0]| \geq \varepsilon .$$

The time complexity of the algorithm B is dominated by the exponentiations and multiplications performed in the extract queries. So the time complexity of B is

$$t = t' + O(q\tau + q\rho) .$$

C. Main construction I

The initial construction achieves constant size ciphertexts. But the private size is O(|S|). In this section, a modified scheme is given where it achieves constant size ciphertexts and constant size private keys.

Let S={ID_1,…, ID_s} with s ≤ m denote the total number of possible users.

Setup Selects a random generator $g \in G$ and some random elements g_2 , g_3 , h_i from G(where i=1,…,m). Then it picks a random $\alpha \in Z_p$ and sets $g_1 = g^{\alpha}$. We set $\mathbf{H} = (h_i)$. The system parameters are

$$param\text{=}(\ g, g_1, g_2, g_3, \mathbf{H})$$

and master key is g_2^{α} .

Extract Given the identity $ID_i \in S$={ID_1,…, ID_s} with s ≤ m, PKG selects randomly $r_i \in Z_p$ and computes private keys as follows:

$$d_{ID_i} = (d_{i0}, d_i', d_{i1})$$

$$= (g_2^{\alpha}(g_3 h_i^{ID_i})^{r_i}, g^{r_i}, (\prod_{j=1, j\neq i}^{s} h_j^{ID_j})^{r_i}) .$$

Encrypt Given S={ID_1,…, ID_s} and message M, the broadcaster randomly picks $t \in Z_p^*$ and computes

$$Hdr = (C_1, C_2) = [g^t, (g_3 \prod_{i=1}^{s} h_i^{ID_i})^t] ;$$

$$C = (C_0, Hdr) = [e(g_1, g_2)^t M, Hdr] .$$

Decrypt Given the ciphertexts $C = (C_0, C_1, C_2)$, any user $ID_i \in S$ uses his private keys d_{ID_i} to compute

$$M = C_0 \frac{e(C_2, d_i')}{e(d_{i0} d_{i1}, C_1)} .$$

Correctness: In fact,

$$\frac{e(C_2, d_i')}{e(d_{i0} d_{i1}, C_1)} = \frac{e((g_3 \prod_{i=1}^{s} h_i^{ID_i})^t, g^{r_i})}{e(g_2^{\alpha}(g_3 \prod_{i=1}^{s} h_i^{ID_i})^{r_i}, g^t)}$$

$$= \frac{1}{e(g_1, g_2)^t} .$$

Security analysis

Theorem 3.2 Suppose that the decision BDHE assumption holds, then our new scheme is *IND-ID-CPA* secure.

Proof: It is similar with the proof of Theorem 3.1. It is given as follows: Suppose there exists a attacker A against our scheme, then we will construct an algorithm B

to solve the decision BDHE problem. We define the selective-identity game between *A* and *B* as follows:

Initialization *A* first outputs a set of identities $S^* = (v_1^*, \cdots, v_s^*)$ with $s \le m$ that it intends to attack.

Setup For a random generator g of G and a random $\alpha \in Z_p$, *B* is given as input a tuple (g , h , $g^{\alpha}, \cdots, g^{\alpha^m}$, $g^{\alpha^{m+2}}, \cdots, g^{\alpha^{2m}}$, *T*). To generate the system parameters, *B* picks a random $\gamma \in Z_p$ and sets $g_1 = g^{\alpha}$ and $g_2 = g^{\alpha^m} g^{\gamma} = g^{\gamma+\alpha^m}$. Next, *B* picks randomly $\gamma_1, \cdots, \gamma_m$ in Z_p and sets $h_i = g^{\gamma_i} / Y_{m-i+1}$ and $Y_i = g^{\alpha^i} \in G$, where $1 \le i \le m$. It also picks randomly a μ and sets $g_3 = g^{\mu} \prod_{i=1}^{m} Y_{m-i+1}^{v_i^*}$. Finally, *B* sends the public keys

$$param = (g, g_1, g_2, g_3, h_1, \cdots, h_m)$$

to *A*. The master key corresponding to these parameters is $g_2^{\alpha} = g^{(\gamma+\alpha^m)\alpha} = Y_1^{\gamma} Y_{m+1}$ which is unknown to *B*.

Phase 1: *A* issues up to m private key queries. Each query is specified as follows: Suppose the adversary *A* issues a query for an identity v_i .The only restriction is that $v_i \notin S^*$ .This restriction ensures that $v_i - v_j^* \ne 0$. Then B constructs a private key for v_i . Suppose that $v_i \in S' = (v_1', \cdots, v_s')$, then it selects randomly a $r' \in Z_p$ and computes the private key corresponding v_i as follows:

$$d_{v_i} = (g_2^{\alpha}(g_3 h_i^{v_i})^r, g^r, (\prod_{j=1, j\ne i}^{s} h_j^{v_j'})^r)),$$

where $r = r' + \frac{\alpha^i}{v_i - v_i^*}$. In deed, we can obtain

$$g_2^{\alpha}(g_3 h_i^{v_i})^r$$

$$= Y_1^{\gamma} Y_{m+1} (g^{\mu} \prod_{j=1}^{m} Y_{m-j+1}^{v_j^*} (\tfrac{g^{\gamma_i}}{Y_{m-i+1}})^{v_i})^r$$

$$= Y_1^{\gamma} Y_{m+1} (g^{\mu} \prod_{j=1}^{i-1} Y_{m-j+1}^{v_j^*} \cdot Y_{m-i+1}^{v_i^*} (\tfrac{g^{\gamma_i}}{Y_{m-i+1}})^{v_i} \cdot \prod_{j=i+1}^{m} Y_{m-j+1}^{v_j^*})^r$$

$$= Y_1^{\gamma} Y_{m+1} (g^{\mu+\gamma_i v_i} \prod_{j=1}^{i-1} Y_{m-j+1}^{v_j^*} Y_{m-i+1}^{v_i^*-v_i} \prod_{j=i+1}^{m} Y_{m-j+1}^{v_j^*})^r \qquad (2)$$

where

$$(g^{\mu+\gamma_i v_i} \prod_{j=1}^{i-1} Y_{m-j+1}^{v_j^*} Y_{m-i+1}^{v_i^*-v_i} \prod_{j=i+1}^{m} Y_{m-j+1}^{v_j^*})^r$$

$$= (g^{\mu+\gamma_i v_i} \prod_{j=1}^{i-1} Y_{m-j+1}^{v_j^*} Y_{m-i+1}^{v_i^*-v_i} \prod_{j=i+1}^{m} Y_{m-j+1}^{v_j^*})^{r' + \frac{\alpha^i}{v_i - v_i^*}}$$

$$= (g^{\mu+\gamma_i v_i} \prod_{j=1}^{i-1} Y_{m-j+1}^{v_j^*} Y_{h-i+1}^{v_i^*-v_i} \prod_{j=i+1}^{m} Y_{m-j+1}^{v_j^*})^{r'} (Y_{m-i+1}^{v_i^*-v_i})^{r' + \frac{\alpha^i}{v_i - v_i^*}}$$

$$= (g^{\mu+\gamma_i v_i} \prod_{j=1}^{i-1} Y_{m-j+1}^{v_j^*} Y_{h-i+1}^{v_i^*-v_i} \prod_{j=i+1}^{m} Y_{m-j+1}^{v_j^*})^{r'} (Y_{m-i+1}^{v_i^*-v_i})^{r'} Y_{m+1}^{-1}$$

According to (2), one can obtain

$$g_2^{\alpha}(g_3 \prod_{i=1}^{k} h_i^{v_i})^r$$

$$= Y_1^{\gamma} \ (g^{\mu+\gamma_i v_i} \prod_{j=1}^{i-1} Y_{m-j+1}^{v_j^*} Y_{h-i+1}^{v_i^*-v_i} \prod_{j=i+1}^{m} Y_{m-j+1}^{v_j^*})^{r'} (Y_{m-i+1}^{v_i^*-v_i})^{r'} .$$

Since all the terms in this expression are known to *B*. Thus, *B* can compute the first private key component. *B* computes $Y_i^{\frac{1}{v_i - v_i^*}} g^{r'} = g^r$. Then the second component of private keys is obtained. Similarly, the remaining elements h_i^r can be computed by *B* since they do not involve a term Y_{m+1} . Thus, *B* can derive a valid private key for v_i .

The rest of game is same with the Theorem 3.1. So we omit them.

D. Efficiency analysis

Our constructions achieve *O*(1)-size ciphertexts. The private key of initial construction private key is linear in the maximal size of *S*. The second scheme achieves O(1)-size private keys which solves the trade-off of the private keys and ciphertexts. In addition, $e(g_1, g_2)$ can be precomputed, so there is no pair computations at the phase of Encryption. Furthermore, the security of the proposed schemes are reduced to the decision BDHE assumption. This assumption is more natural than those in the existing schemes. Table 1 gives the comparisons of efficiency with other schemes.

Note: λ is a security parameter. m and |*S*| denote the maximal size of the set of receivers and the size of receivers for one encryption . PK and pk are public key and private key separately.

TABLE I.
COMPARISONS OF EFFICIENCY

[16]	O(λ)	O(|S|)	O(1)
[17]: 1st scheme	O(m)	O(|S|)	O(1)
[17]: 2nd scheme	O(m)	O(1)	O(1)
[17]: 3rd scheme	O(m)	O(1)	Sublinear of |S|
Ours initial	O(m)	O(|S|)	O(1)
Ours 2nd scheme	O(m)	O(1)	O(1)

IV. EXTENSIONS

The proposed schemes only achieve the selective-identity security. A natural extension is to construct the efficient scheme with the strong security. In this section, we will give two methods to achieve it.

A The first motivation

An well-known construction of IBE was given by Waters[9]. It achieves full security(adaptive security) . It works as follows:

Setup Selects a random generator $g \in G$ and some random elements g_2 , g_3 , h_i from G(where i=1,…,m). Then it picks a random $\alpha \in Z_p$ and sets $g_1 = g^{\alpha}$. We set $\mathbf{H} = (h_i)$. The system parameters are

$$param=(g, g_1, g_2, g_3, \mathbf{H})$$

and master key is g_2^{α} .

Extract Given the identity $ID=\{v_1,\ldots, v_s\}$ with $v_i \in \{0,1\}$, PKG selects randomly $r \in Z_p$ and computes private keys as follows:

$$d_{ID} = (d_0, d_1) = (g_2^{\alpha}(g_3 \prod_{j=1}^{s} h_j^{v_j})^r, g^r) .$$

Encrypt To encrypt message M under an identity ID, pick $t \in Z_p^*$ at random and compute

$$C = (C_0, C_1, C_2) = (e(g_1, g_2)^t M, g^t, (g_3 \prod_{i=1}^{s} h_i^{v_i})^t) .$$

Decrypt Given the ciphertexts $C = (C_0, C_1, C_2)$, the user with ID uses his private keys d_{ID_i} to compute

$$M = C_0 \frac{e(C_2, d_1)}{e(d_0, C_1)} .$$

Our first construction is based on this scheme. It is described as follows:

Setup Selects a random generator $g \in G$ and some random elements g_2 , g_3 , h_{ij} from G(where i=1, ⋯ , s, j=1, ⋯ , n). Then it picks a random $\alpha \in Z_p$ and sets $g_1 = g^{\alpha}$. We set $\mathbf{H}_i = (h_{ij})$ for i=1, ⋯ , s, j=1, ⋯ , n. The system parameters are

$$param=(g, g_1, g_2, g_3, \mathbf{H}_1, \cdots, \mathbf{H}_s)$$

and master key is α .

Extract Given the identity $ID_i=\{v_{i1},\ldots, v_{in}\}$ with $v_{ij} \in \{0,1\}$, PKG selects randomly $r \in Z_p$ and computes private keys as follows:

$$d_{ID} = (g_2^{\alpha}(g_3 \prod_{j=1}^{s} h_{ij}^{v_{ij}})^r, g^r, \mathbf{H}_1^r, \cdots, \mathbf{H}_{i-1}^r, \mathbf{H}_{i+1}^r, \cdots, \mathbf{H}_s^r),$$

where $\mathbf{H}_j^r = (h_{j1}^r, \cdots, h_{jn}^r)$.

Encrypt To encrypt message M under an identity ID, pick $t \in Z_p^*$ at random and compute

$$C = (C_0, C_1, C_2) = (e(g_1, g_2)^t M, g^t, (g_3 \prod_{i=1}^{s} F_i)^t) ,$$

where $F_i = \prod_{j=1}^{n} h_{ij}^{v_{ij}}$.

Decrypt Given the ciphertexts $C = (C_0, C_1, C_2)$, the user with ID uses his private keys d_{ID} to compute

$$M = C_0 \frac{e(C_2, d_1)}{e(d_0 \prod_{j=1, j\neq i}^{s} F_j^r, C_1)} ,$$

where $d_0 = g_2^{\alpha}(g_3 \prod_{j=1}^{s} h_{ij}^{v_{ij}})^r, d_1 = g^r$. In addition, the user has obtained his private key d_{ID} . Then he computes F_i^r by using $\mathbf{H}_i^r = (h_{i1}^r, \cdots, h_{in}^r)$.

Correctness: If the ciphertext is valid, then one can verify the following equation holds.

$$\frac{e(C_2, d_1)}{e(d_0 \prod_{j=1, j\neq i}^{s} F_j^r, C_1)}$$
$$= \frac{e((g_3 \prod_{i=1}^{s} F_i)^t, g^r)}{e(g_2^{\alpha}(g_3 \prod_{j=1}^{s} h_{ij}^{v_{ij}})^r \prod_{j=1, j\neq i}^{s} F_j^r, C_1)}$$
$$= \frac{e((g_3 \prod_{i=1}^{s} h_i^{v_i})^t, g^r)}{e(g_2^{\alpha}(g_3 \prod_{j=1}^{s} F_i)^r, C_1)}$$
$$= \frac{1}{e(g_2^{\alpha}, g^t)} = \frac{1}{e(g_2, g_1)^t} .$$

B Main construction II

The first construction has constant size ciphertexts but the size of its private grows linearly in the number of users in set ***S***. Hence we give the following extension.

Setup Selects a random generator $g \in G$ and some random elements g_2 , g_3 , h_{ij} from G(where i=1, ⋯ , s, j=1, ⋯ , n). Then it picks a random $\alpha \in Z_p$ and sets $g_1 = g^{\alpha}$. We set $\mathbf{H}_i = (h_{ij})$ for i=1, ⋯ , s, j=1, ⋯ , n. The system parameters are

$$param=(g, g_1, g_2, g_3, \mathbf{H}_1, \cdots, \mathbf{H}_s)$$

and master key is α .

Extract Given the identity $ID_i=\{v_{i1},\ldots, v_{in}\}$ with $v_{ij} \in \{0,1\}$, PKG selects randomly $r \in Z_p$ and computes private keys as follows:

$$d_{ID} = (d_0, d_1, d_2) = (g_2^{\alpha}(g_3 \prod_{j=1}^{s} h_{ij}^{v_{ij}})^r, g^r, \prod_{j=1, j\neq i}^{s} F_j^r),$$

where $F_i = \prod_{j=1}^{n} h_{ij}^{v_{ij}}$.

Encrypt To encrypt message M under an identity ID, pick $t \in Z_p^*$ at random and compute

$$C = (C_0, C_1, C_2) = (e(g_1, g_2)^t M, g^t, (g_3 \prod_{i=1}^{s} F_i)^t) ,$$

where $F_i = \prod_{j=1}^{n} h_{ij}^{v_{ij}}$.

Decrypt Given the ciphertexts $C=(C_0,C_1,C_2)$, the user with *ID* uses his private keys d_{ID} to compute

$$M=C_0\frac{e(C_2,d_1)}{e(d_0d_2,C_1)}.$$

Correctness: If the ciphertext is valid, then one can verify the following equation holds.

$$\frac{e(C_2,d_1)}{e(d_0d_2,C_1)}=\frac{e((g_3\prod_{i=1}^{s}F_i)^t,g^r)}{e(g_2^{\alpha}(g_3\prod_{j=1}^{s}h_{ij}^{v_{ij}})^r\prod_{j=1,j\neq i}^{s}F_j^r,C_1)}$$

$$=\frac{e((g_3\prod_{i=1}^{s}h_i^{v_i})^t,g^r)}{e(g_2^{\alpha}(g_3\prod_{j=1}^{s}F_i)^r,C_1)}=\frac{1}{e(g_2^{\alpha},g^t)}=\frac{1}{e(g_2,g_1)^t}.$$

C Security Analysis

The security of the proposed scheme is reduced to the hardness of weak Decisional Bilinear Diffie-Hellman Inversion (wDBDHI) Problem. It is defined as follows: Given a tuple $Y=(g,h,g^a,\cdots,g^{a^m})$, compute $e(g,h)^{a^{m+1}}$, where e() is a bilinear pair, (*g*, *h*) are selected from *G* and $\alpha\in Z_p^*$. The decision wDBDHI problem is as follows: Given a tuple (Y,T), decide whether $T=e(g,h)^{a^{m+1}}$ or T is a random element in G_1. An algorithm *B* that outputs $b\in\{0,\ 1\}$ has advantage ε in solving decision BDHE in G if

$$|\Pr[B(Y,\ e(g,h)^{a^{m+1}})=0]-\Pr[B(Y,T)=0]|\geq\varepsilon.$$

The (t,ε)-wDBDHI assumption holds if no adversary has at least ε advantage in solving the above problem with polynomial time *t*.

Theorem 4.1 Suppose that the decision wDBDHI assumption holds, then our new scheme is *IND-ID-CPA* secure.

The proof can be obtained from [9, 11].

Recently, a new technique is applied to IBE. It is called Dual Encryption Technique [18,19]. This technique can be applied to modify our two constructions in section III.

IV. CONCLUSIONS

This paper discusses the constructions of identity-based broadcast encryption with short ciphertexts in the standard model. It is an interesting problem to construct constant-size private keys correspondingly. We propose an initial scheme at first. It has constant size ciphertexts and O(|*S*|)-size private keys. And under the selective-identity security model, we reduce its security to the decision BDHE assumption which is more natural than those in the existing schemes. Based on this initial work, our main scheme is presented. It achieves the constant size ciphertexts and constant size private keys which solves the trade-off of ciphertexts and private keys.

Unfortunately, both schemes only achieve the selective-identity security. So we give two solutions finally. Two solutions bring two new schemes. Both schemes achieve the full security, which is stronger than selective-identity security.

However, in our schemes, the total number of possible users must be fixed in the setup. It is an interesting problem to construct a scheme without the above constraints in the standard model.

ACKNOWLEDGMENT

This work was supported in part by the Nature Science Foundation of China under Grant (No.61075055), Natural Science Foundation of Shaanxi Province (No.2010JQ8004) and Xi'an Institute of Posts & telecommunications Science Foundation for Middle-aged and Young Scientists (No.110-0402).

REFERENCES

[1] Fiat and M. Naor. "Broadcast encryption". In: Douglas R. Stinson, eds. Crypto. Lecture Notes in Computer Science, volume 773, Berlin: Springer-Verlag, 1993, pp. 480-491.

[2] Y. Dodis and N. Fazio. "Public key broadcast encryption for stateless receivers". In: Feigenbaum J., eds. ACM Workshop on Digital Rights Management, Lecture Notes in Computer Science, volume 2696, Berlin: Springer-Verlag, 2002, pp. 61-80.

[3] Y. Dodis and N. Fazio. "Public key broadcast encryption secure against adaptive chosen ciphertext attack". In: Desmedt Y., eds. Public Key Cryptography, Lecture Notes in Computer Science, volume 2567, Berlin: Springer-Verlag, 2003, pp. 100-115.

[4] D. Boneh , C. Gentry and B. Waters,. "Collusion resistant broadcast encryption with short ciphertexts and private keys". In: Shoup V., eds. CRYPTO, Lecture Notes in Computer Science, volume 3621,Berlin: Springer-Verlag, 2005, pp. 258-275.

[5] Delerablèe, P.Paillier and D. Pointcheval. "Fully collusion secure dynamic broadcast encryption with constant-size ciphertexts or decryption keys". In: Tsuyoshi Takagi,et al., eds. Pairing-Based Cryptography, Lecture Notes in Computer Science, volume 4575, Berlin: Springer-Verlag, 2007, pp. 39-59.

[6] Shamir. "Identity-based Cryptosystems and Signature Schemes". In: Wagner D., eds., Crypto, Lecture Notes in Computer Science, volume 196, Berlin: Springer-Verlag, 1984, pp. 47-53.

[7] Boneh, M. Franklin. "Identity Based Encryption from the Weil Pairing". In: Joe Kilian,eds. CRYPTO, Lecture Notes in Computer Science, volume 2139, Berlin: Springer-Verlag, 2001, pp. 213-229.

[8] Boneh, X. Boyen. "Efficient Selective-ID Identity Based Encryption without Random Oracles". In: Christian Cachin,et al., eds. Eurocrypt, Lecture Notes in Computer Science, volume 3027, Berlin:Springer-Verlag, 2004, pp. 223-238.

[9] Waters. “Efficient identity-based encryption without random oracles”. In R. Cramer, editor, Proceedings of Eurocrypt 2005, LNCS 3494, Berlin: Springer-Verlag, 2005.
[10] Boneh, X. Boyen, and E. J. Goh. “Hierarchical Identity Based Encryption with Constant Size Ciphertext”. In: Cramer R.,eds. Eurocrypt, Lecture Notes in Computer Science, volume 3494, Berlin: Springer-Verlag, 2005, pp. 440-456.(Full version available on Cryptology ePrint Archive Report 2005/015)
[11] S. Chatterjee and P. Sarkar. “New Constructions of Constant Size Ciphertext HIBE Without Random Oracle”. In M.S. Rhee and B. Lee (Eds.): ICISC, Lecture Notes in Computer Science, volume 4296, pp. 310–327, Berlin: Springer-Verlag, 2006.
[12] C. Gentry. “Practical identity-based encryption without random oracles”. In:Serge Vaudenay,eds. EUROCRYPT, Lecture Notes in Computer Science, volume 4004, 2006, pp. 445-464.
[13] Y. Mu, W. Susilo and Y. Lin et al. “Identity-Based Authenticated Broadcast Encryption and Distributed Authenticated Encryption”. In: Michael J. Maher, eds. ASIAN 2004, Lecture Notes in Computer Science, volume 3321, Berlin: Springer-Verlag, 2004, pp. 169-181.
[14] C. Delerablée. “Identity-Based Broadcast Encryption with Constant Size Ciphertexts and Private Keys”. In: Kaoru Kurosawa, eds. ASIACRYPT, Lecture Notes in Computer Science, volume 4833,Berlin: Springer-Verlag, 2007, pp. 200-215.
[15] X. Du, Y. Wang and J. Ge. et al. “An ID-Based Broadcast Encryption Scheme for Key Distribution”. IEEE TRANSACTIONS ON BROADCASTING. Vol.51, Issue:2, 2005, pp. 264-266 .
[16] Y. L. Ren, D.W. Gu. “Fully CCA2 secure identity based broadcast encryption without random oracles”. Information Processing Letters. Vol. 109, 2009, pp. 527–533.
[17] C. Gentry, B. Waters. “Adaptive Security in Broadcast Encryption Systems”. EUROCRYPT 2009, LNCS 5479, 2009, pp. 171–188.
[18] B. Waters. Dual system encryption: realizing fully secure ibe and hibe under simple assumptions. In Advances in Cryptology - CRYPTO 2009, volume 5677 of LNCS, pages 619-636, Springer, 2009.(The full paper appeared Cryptology ePrint Archive Report 2009/385)
[19] Lewko and B. Waters. New Techniques for Dual System Encryption and Fully Secure HIBE with Short Ciphertexts. TCC 2010, LNCS 5978, pp. 455–479, Springer, 2010.

Qing Wu was born in 1975. She received the M.E. and Ph.D. degrees in Applied Mathematics form Xidian University, Xi’an, China in 2005 and 2009, respectively. Now she is working at School of Automation, Xi’an Institute of Posts and Telecommunications, Xi’an, China. Her research interests include information security, network security, pattern recognition and machine learning.

Wang Wenqing is with the School of Automation, Xi’an University of Posts and Telecommunications, he received the M.S. degrees from Xi’an University of Architecture and Technology, and the Ph.D. degree from Northwestern Polytechnical University in 2003. His current research interests are in complex systems robust control, process control, and information security.