www.ietdl.org

Published in IET Information Security
Received on 18th September 2010
Revised on 28th August 2011
doi: 10.1049/iet-ifs.2010.0252

ISSN 1751-8709

Cryptanalysis and improvements of an anonymous multi-receiver identity-based encryption scheme

H. Wang[1,4] *Y. Zhang*[2] *H. Xiong*[3] *B. Qin*[4,*]

[1]*School of Information Engineering, Dalian Ocean University, People's Republic of China*
[2]*National Computer Network Intrusion Protection Center, GUCAS, People's Republic of China*
[3]*School of Computer Science and Engineering, University of Electronic Science and Technology of China, People's Republic of China*
[4]*Department of Computer Engineering and Maths, UNESCO Chair in Data Privacy, Universitat Rovira i Virgili, Tarragona, Catalonia*
[*]*Department of Maths, School of Science, Xi'an University of Technology, People's Republic of China*
E-mail: wanghuaqun8@gmail.com

Abstract: In 2010, Fan *et al.* presented an anonymous multi-receiver identity-based encryption scheme where they adopt Lagrange interpolating polynomial mechanism. They showed that their scheme makes it impossible for an attacker or any other message receiver to derive the identity of a message receiver such that the privacy of every receiver can be guaranteed. They also formally showed that every receiver in the proposed scheme is anonymous to any other receiver. In this work, the authors study the security of Fan *et al.*'s anonymous multi-receiver identity-based encryption scheme. It is regretful that they found their scheme is insecure. Every receiver in Fan *et al.*'s scheme is not anonymous to any other receiver. The authors showed that simple protocol changes can fix these weaknesses and render Fan *et al.*'s scheme. The improved scheme is proved to satisfy the confidentiality and receiver anonymity in the random oracle.

1 Introduction

Multi-receiver communication is of great importance in wireless communications. It deals with the problem of key management effectively such that the entire communication protocol is efficient. Many researchers focused on this topic and proposed many interesting protocols.

In an identity-based encryption (IBE) scheme, every user can select her/his identity (ID) freely, where some meaningful or easily memorised strings are usually selected as ID. Moreover, the problem of the authentication for public keys can also be solved if we take ID to form the public keys. ID-based cryptography has attracted a lot of researchers and has gained some results [1–4]. In 2005, Du *et al.* [5] presented an ID-based broadcast encryption scheme for key distribution. They take use of the matrix operations for encryption and decryption. Unforturely, their scheme is insecure [6]. In 2005, Wang and Wu [7] proposed an ID-based multicast encryption scheme that has a key generation centre and a group centre. All users do not need any computation during the rekeying process. However, the sender must be the group centre. Besides, the problems of key updating were discussed frequently, but no efficient solution has been proposed. In 2010, Fan *et al.* [8] presented an anonymous multi-receiver IBE scheme where they adopt Lagrange interpolating polynomial mechanism to cope with the above problem.

In a multi-receiver encryption environment, a sender can randomly choose receivers. Every multi-receiver encryption scheme can be transformed into a broadcast encryption scheme or a multicast encryption scheme. Beak *et al.* [9] proposed a multi-receiver IBE along with a formal definition and security model for the kind of schemes. They proved the security in the selective-ID model using the random oracle technique. In 2006, Lu and Hu [10] presented a multi-recipient public key encryption with pairing. Their scheme can be applied to broadcast sensitive information in an unsafe distributed environment. All of the multi-receiver IBE schemes proposed in the literature cannot protect the privacy of receivers or do not contain any discussion on this issue. In [8], Fan *et al.* proposed a provably secure and efficient multi-receiver IBE scheme that can achieve the anonymity for every receiver against any other receiver. Everyone can receive a ciphertext broadcasted by a sender, but only the receivers selected by the sender can decipher the ciphertext successfully. Besides, one can examine whether herself/himself is a selected receiver or not. Nobody, except the sender, knows who the other receivers are. They present how to design an efficient anonymous multi-receiver IBE scheme based on Lagrange interpolating polynomial theorem. Fan *et al.*'s scheme can be used in pay-TV or streaming audio/video services. In some situations, such as ordering sensitive TV programmes, a receiver or customer usually expects that any other receiver or customer does not know her/his ID when ordering the TV programmes. Anonymous multi-receiver IBE has a lot of applications. It is valuable to study this type of public key cryptography scheme.

It is regretful that we found Fan *et al.*'s scheme is insecure. Every receiver is not anonymous to any other receiver. We showed that simple protocol changes can fix these weaknesses and render Fan *et al.*'s scheme. The improved scheme is proved to satisfy the confidentiality and receiver anonymity in the random oracle. Our cryptanalysis and improvements will help experts and engineers design and develop anonymous multi-receiver IBE scheme.

The rest of the paper is organised as follows: in Section 2, we review Fan *et al.*'s anonymous multi-receiver IBE scheme. In Section 3, we give anonymity attack on Fan *et al.*'s scheme. In Section 4, we proposed the improvements on Fan *et al.*'s scheme. The security analysis was given in Section 5. We conclude this paper in Section 6.

2 Review of Fan *et al.*'s scheme

In this section, we review the polynomial interpolation method, the characteristics of bilinear groups, some hard problems and Fan *et al.*'s scheme [8]. In this paper, the symbol $a \in_R S$ denotes the element a is uniformly sampled at random from the set S.

2.1 Polynomial interpolation, bilinear groups and hard problems

2.1.1 Lagrange interpolating polynomial theorem: Let $\sum_{i=1}^{t} F_i(x) = \sum_{i=0}^{t-1} a_i x^i$ be a polynomial of degree $t-1 \geq 0$ that passes through the t points $(x_1, y_1), (x_2, y_2), \ldots, (x_t, y_t)$ where for each i

$$F_i(x) = y_i \prod_{1 \leq j \neq i \leq t} \frac{x - x_j}{x_i - x_j} = \begin{cases} y_i, & x = x_i \\ 0, & x \in \{x_1, \ldots, x_t\} - \{x_i\} \end{cases}$$

2.1.2 Bilinear groups: Let $\mathbb{G}_1$ and $\mathbb{G}_2$ be two cyclic groups of prime order q and let P be a generator of $\mathbb{G}_1$. A bilinear mapping e: $\mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$ has the following properties:

1. *Bilinearity:* $e(aP, bQ) = e(P, Q)^{ab}$, $\forall P, Q \in \mathbb{G}_1$ and $a, b \in \mathbb{Z}_q^*$.
2. *Non-degeneracy:* There exist $P, Q \in \mathbb{G}_1$ such that $e(P, Q) \neq 1$.
3. *Computability:* There exists an efficient algorithm to compute $e(P, Q)$ for any $P, Q \in \mathbb{G}_1$.

2.1.3 Hard problems

1. *Computational Diffie–Hellman problem:* Given (P, aP, bP) for some $a, b \in \mathbb{Z}_q^*$, compute abP.
2. *Bilinear Diffie–Hellman (BDH) problem:* Given (P, aP, bP, cP) for some $a, b, c \in \mathbb{Z}_q^*$, compute $e(P, P)^{abc} \in \mathbb{G}_2$.
3. *Co-bilinear Diffie–Hellman (Co-BDH) problem [11]:* Given (P, aP, bP, Q) for $a, b \in \mathbb{Z}_q^*$ and $Q \in_R \mathbb{G}_1$, compute $e(P, Q)^{ab}$.
4. *Co-decision bilinear Diffie–Hellman (Co-DBDH) problem [12]:* Given (P, aP, bP, Q, Z) for some $a, b \in \mathbb{Z}_q^*$, $Q \in_R \mathbb{G}_1$ and $Z \in_R \mathbb{G}_2$, decide whether $Z = e(P, Q)^{ab}$.
5. *Modified decision bilinear Diffie–Hellman (DBDH-M) problem [13]:* Given (P, aP, bP, U) for some $a, b \in \mathbb{Z}_q^*$ and $U \in_R \mathbb{G}_1$, decide whether $U = ab^2P$.
6. *xyz-decisional Diffie–Hellman problem (xyz-DDH) [14]:* Given $(P, xP, yP, zP, Q) \in \mathbb{G}_1^5$, decide whether $Q = xyzP$.
7. *Modified xyz-decisional Diffie–Hellman problem (xyz-DDH-M):* Given $(P, xP, yP, zP, Q) \in \mathbb{G}_1^5$, decide whether $Q = xyz^{-1}P$.
8. *General modified xyz-decisional Diffie–Hellman problem (G-xyz-DDH-M):* Given $(P_1, P_2, P_3, xP_1, yP_2, H) \in \mathbb{G}_1^6$, decide whether $H = xy^{-1}P_3$.

Proof: Suppose G-*xyz*-DDH-M is easy, then we obtain *xyz*-DDH-M is also easy as follows:

Given (P, aP, bP, cP, H), we pick $k_1, k_2 \in \mathbb{Z}_q^*$ and compute $P_1 = k_1P$, $P_2 = k_2P$. Then the tuple $(k_1P, k_2P, bP, k_1(aP), k_2(cP), H) = (k_1P, k_2P, bP, a(k_1P), c(k_2P), H)$ can be decided whether $H = ac^{-1}bP = abc^{-1}P$. Thus, *xyz*-DDH-M can be solved.

Based on the difficulty of *xyz*-DDH-M, we know that G-*xyz*-DDH-M is also difficult. □

2.2 Security definition

According to Fan *et al.*'s paper, we present a general model and security notions for anonymous multi-receiver IBE schemes. The security notions are 'Indistinguishability of encryptions under selective multi-ID, chosen ciphertext attacks' (IND-sMID-CCA) [8], 'Anonymous indistinguishability of encryptions under selective-ID, chosen ciphertext attacks' (ANON-sID-CCA) [8], and 'Anonymous indistinguishability of encryptions under selective multi-ID, chosen ciphertext attacks' (ANON-sMID-CCA).

Definition 1 (IND-sMID-CCA) [8]: Let $\mathcal{A}$ be a polynomial-time attacker. Let $\prod$ be a general multi-receiver IBE scheme. $\mathcal{A}$ interacts with a Challenger in the following game:

- *Setup:* The Challenger runs the Setup algorithm. It gives the attacker $\mathcal{A}$ the resulting public parameters param. It keeps the master key secret.
- *Phase 1:* $\mathcal{A}$ outputs target multiple identities $(\mathrm{ID}_1, \ldots, \mathrm{ID}_t)$ where t is a positive integer.
- *Phase 2:* $\mathcal{A}$ issues private key extraction queries. Upon receiving a private key extraction query, denoted by ID_j, the Challenger runs the private key extraction algorithm to obtain $d_j = \mathrm{Extract}(\mathrm{params}, s, \mathrm{ID}_j)$. The only constraint is that $\mathrm{ID}_j \neq \mathrm{ID}_i$ for $i = 1, \ldots, t$.
- *Phase 3:* $\mathcal{A}$ issues decryption queries for target IDs. Upon receiving a decryption query, denoted by (C^*, ID_i) for some $i \in \{1, 2, \ldots, t\}$, the Challenger generates a private key associated with ID_i, which is denoted by d_i. The Challenger returns $D = \mathrm{Decrypt}(\mathrm{params}, C^*, \mathrm{ID}_i, d_i)$ to $\mathcal{A}$.
- *Challenge:* $\mathcal{A}$ outputs a target plaintext pair (M_0, M_1). Upon receiving (M_0, M_1), the Challenger randomly chooses $\beta \in \{0, 1\}$ and creates a target ciphertext $C = \mathrm{Encrypt}(\mathrm{params}, \mathrm{ID}_1, \ldots, \mathrm{ID}_t, M_\beta)$. Then the Challenger returns C to $\mathcal{A}$.
- *Phase 4:* $\mathcal{A}$ issues private key extraction queries as those in Phase 2 and decryption queries for target IDs as those in Phase 3 where a restriction here is that $C^* \neq C$.
- *Guess:* Finally, $\mathcal{A}$ outputs its guess $\beta' \in \{0, 1\}$ and wins the game if $\beta' = \beta$.

We define $\mathcal{A}$'s guessing advantage

$$\mathrm{Adv}_{\prod}^{\mathrm{IND\text{-}sMID\text{-}CCA}}(\mathcal{A}) = \left| \Pr[\beta = \beta'] - \frac{1}{2} \right|$$

The scheme $\prod$ is said to be (τ, ε)-IND-sMID-CCA secure if for any IND-sMID-CCA attacker $\mathcal{A}$, within polynomial running time τ, the guessing advantage $\mathrm{Adv}_{\prod}^{\text{IND-sMID-CCA}}(\mathcal{A})$ is less than ε.

Definition 2 (ANON-sID-CCA) [8]: Let $\mathcal{A}$ be a polynomial-time attacker. Let $\prod$ be a general multi-receiver IBE scheme. $\mathcal{A}$ interacts with a Challenger in the following game:

- *Setup:* The Challenger runs the Setup algorithm. It gives the attacker $\mathcal{A}$ the resulting public parameters params. It keeps the master key secret.
- *Phase 1:* $\mathcal{A}$ outputs a target identity pair $(\mathrm{ID}_1, \mathrm{ID}_2)$. Upon receiving $(\mathrm{ID}_1, \mathrm{ID}_2)$, the Challenger randomly chooses $\beta \in \{0, 1\}$.
- *Phase 2:* $\mathcal{A}$ issues private key extraction queries. Upon receiving a private key extraction query, denoted by ID_j, the Challenger runs the private key extraction algorithm to obtain $d_j = \mathrm{Extract}(\mathrm{params}, s, \mathrm{ID}_j)$. The only constraint is that $\mathrm{ID}_j \neq \mathrm{ID}_i$ for $i = 1, 2$.
- *Phase 3:* $\mathcal{A}$ issues decryption queries for target IDs. Upon receiving a decryption query, denoted by (C, ID_i) for some $i \in \{1, 2\}$, the Challenger generates a private key associated with ID_i, which is denoted by d_i. The Challenger returns $D = \mathrm{Decrypt}(\mathrm{params}, C^*, \mathrm{ID}_i, d_i)$ to $\mathcal{A}$.
- *Challenge:* $\mathcal{A}$ outputs a target plaintext M. The Challenger creates a target ciphertext $C = \mathrm{Encrypt}(\mathrm{params}, \mathrm{ID}_\beta, M)$ and then returns C to $\mathcal{A}$.
- *Phase 4:* $\mathcal{A}$ issues private key extraction queries as those in Phase 2 and decryption queries for target IDs as those in Phase 3 where a restriction here is that $C^* \neq C$.
- *Guess:* Finally, $\mathcal{A}$ outputs its guesses $\beta' \in \{1, 2\}$ and wins the game if $\beta' = \beta$.

We define $\mathcal{A}$'s guessing advantage

$$\mathrm{Adv}_{\prod}^{\text{ANON-sID-CCA}}(\mathcal{A}) = \left|\Pr[\beta = \beta'] - \frac{1}{2}\right|$$

The scheme $\prod$ is said to be (τ, ε)-ANON-sID-CCA secure if for any ANON-sID-CCA attacker $\mathcal{A}$, within polynomial running time τ, the guessing advantage

$$\mathrm{Adv}_{\prod}^{\text{ANON-sID-CCA}}(\mathcal{A})$$

is less than ε.

Definition 3 (ANON-sMID-CCA): Let $\mathcal{A}$ be a polynomial-time attacker. Let $\prod$ be a general multi-receiver IBE scheme. $\mathcal{A}$ interacts with a Challenger in the following game:

- *Setup:* It is the same as the Setup phase in Definition 2.
- *Phase 1:* $\mathcal{A}$ outputs a target identity set $(\mathrm{ID}_1, \mathrm{ID}_2, \ldots, \mathrm{ID}_n)$. Upon receiving $(\mathrm{ID}_1, \mathrm{ID}_2, \ldots, \mathrm{ID}_n)$, the Challenger randomly chooses a identity proper subset $S = (\mathrm{ID}_{\beta_1}, \mathrm{ID}_{\beta_2}, \ldots, \mathrm{ID}_{\beta_t})$, that is, $S \subset (\mathrm{ID}_1, \mathrm{ID}_2, \ldots, \mathrm{ID}_n)$.
- *Phase 2:* $\mathcal{A}$ issues private key extraction queries. Upon receiving a private key extraction query, denoted by ID_j, the Challenger runs the private key extraction algorithm to obtain $d_j = \mathrm{Extract}(\mathrm{params}, s, \mathrm{ID}_j)$. The only constraint is that $\mathrm{ID}_j \neq \mathrm{ID}_i$ for $i = 1, 2, \ldots, n$.
- *Phase 3:* $\mathcal{A}$ issues decryption queries for target IDs. Upon receiving a decryption query, denoted by (C, ID_i) for some $i \in \{1, 2, \ldots, n\}$, the Challenger generates a private key associated with ID_i, which is denoted by d_i. The Challenger returns $D = \mathrm{Decrypt}(\mathrm{params}, C^*, \mathrm{ID}_i, d_i)$ to $\mathcal{A}$.
- *Challenge:* $\mathcal{A}$ outputs a target plaintext M. The Challenger creates a target ciphertext $C = \mathrm{Encrypt}(\mathrm{params}, S, M)$ and then returns C to $\mathcal{A}$.
- *Phase 4:* $\mathcal{A}$ issues private key extraction queries as those in Phase 2 and decryption queries for target IDs as those in Phase 3 where a restriction here is that $C^* \neq C$.
- *Guess:* Finally, $\mathcal{A}$ outputs its guesses $\beta' \in \{1, 2, \ldots, n\}$ and wins the game if $\beta' \in S$.

We define $\mathcal{A}$'s guessing advantage

$$\mathrm{Adv}_{\prod}^{\text{ANON-sID-CCA}}(\mathcal{A}) = \left|\Pr[\beta \in \beta'] - \frac{1}{2}\right|$$

The scheme $\prod$ is said to be (τ, ε)-ANON-sMID-CCA secure if for any ANON-sMID-CCA attacker $\mathcal{A}$, within polynomial running time τ, the guessing advantage

$$\mathrm{Adv}_{\prod}^{\text{ANON-sID-CCA}}(\mathcal{A})$$

is less than ε.

Notes: From the Definitions 2 and 3, we know that ANON-sID-CCA is a special case of ANON-sMID-CCA when $t = 1$ and $n = 2$.

2.3 Fan et al.'s scheme

Let $\mathbb{G}_1$ be an additive group and $\mathbb{G}_2$ be a multiplicative group where both of them are cyclic and each of them is with prime order q. Let P be a randomly chosen generator of $\mathbb{G}_1$ and e be a bilinear mapping such that $e: \mathbb{G}_1 \times \mathbb{G}_1 \to \mathbb{G}_2$.

In Fan *et al.*'s scheme, a sender chooses t receivers and prepares t points $(x_1, y_1), (x_2, y_2), \ldots, (x_t, y_t)$ for them. For every receiver ID_i, the sender sets x_i as the root of $F_i(x) = y_i$ where the receiver's identity, ID_i, is mapped into x_i in $\mathbb{Z}_q^*$. Then it computes $y_i = yQ_i$ as the personal private key of the receiver where y is randomly chosen in $\mathbb{Z}_q^*$ and ID_i is also mapped into Q_i in $\mathbb{G}_1^*$. $\mathbb{G}_1^*$ denotes the set $\mathbb{G}_1/\{O\}$, and O is the ID element in the additive group $\mathbb{G}_1$.

The polynomial

$$\begin{aligned} f_i(x) &= F_i(x)/y_i \\ &= \prod_{1 \le j \neq i \le t} \frac{x - x_j}{x_i - x_j} \\ &= \begin{cases} 1, & x = x_i \\ 0, & x \in \{x_1, \ldots, x_t\} - \{x_i\} \end{cases} \end{aligned}$$

is used for achieving receiver anonymity. In the Encrypt phase of Fan *et al.*'s scheme, the sender computes a parameter R_i for each receiver i by using the above polynomial. The sender takes all R_i's and the other parameters to form a ciphertext encrypted by a secret key σ and then broadcasts it. To decrypt the ciphertext, receiver i takes all R_i's and her/his x_i to reconstruct $\lambda = F_i(x_i)$, which is y_i. Then, the receiver computes the secret key σ via her/his private key and λ. Finally, the receiver can decrypt the ciphertext by using σ.

Fan *et al.*'s anonymous multi-receiver IBE scheme comprises: Setup, Extract, Encrypt, Decrypt.

doi: 10.1049/iet-ifs.2010.0252

- *Setup:* The algorithm works as follows:

1. Pick an integer $s \in \mathbb{Z}_q^*$ and an element $P_1 \in \mathbb{G}_1$ at random.
2. Set $P_{\text{pub}} = sP$.
3. Choose five cryptographic one-way hash functions

$$H: \{0, 1\}^* \rightarrow \mathbb{Z}_q^*,\ H_1: \{0, 1\}^* \rightarrow \mathbb{G}_1^*$$

$$H_2: \mathbb{G}_2 \rightarrow \{0, 1\}^w,\ H_3: \{0, 1\}^w \times \{0, 1\}^* \rightarrow \mathbb{Z}_q^*$$

$$H_4: \{0, 1\}^w \rightarrow \{0, 1\}^w$$

for some positive integer w. The symmetric encryption and decryption functions with a key k are represented by E_k and D_k, respectively.

4. Publish the system parameters $\text{params} = \{q, \mathbb{G}_1, \mathbb{G}_2, e, n, P, P_1, P_{\text{pub}}, H, H_1, H_2, H_3, H_4\}$ and keep the master key s secret.

- *Extract:* Input params, s, and an identity $\text{ID}_i \in \{0, 1\}^*$ for $i \in [1, n]$. The algorithm performs the following tasks:

1. Compute $Q_i = H_1(ID_i) \in \mathbb{G}_1^*$.
2. Set the private key $d_i = s(P_1 + Q_i)$.

- *Encrypt:* Input params, a plaintext message M, and select identities $(\text{ID}_1, \ldots, \text{ID}_t)$ of the receivers where $1 \leq t \leq n$. The algorithm performs the following tasks:

1. Pick a string $\sigma \in \{0, 1\}^w$ at random and set $r = H_3(\sigma, M)$.
2. Pick an integer $\alpha \in \mathbb{Z}_q^*$ at random and set $y = \alpha^{-1} r (\text{mod } q)$.
3. For $i = 1, \ldots, t$, compute $x_i = H(\text{ID}_i)$ and $Q_i = H_1(\text{ID}_i)$.
4. For $i = 1, \ldots, t$, compute

$$f_i(x) = \prod_{1 \leq j \neq i \leq t} \frac{x - x_j}{x_i - x_j} = a_{i,1} + a_{i,2}x + \cdots + a_{i,t}x^{t-1}$$

where $a_{i,1}, \ldots, a_{i,t} \in \mathbb{Z}_q$.

5. For $i = 1, \ldots, t$, compute

$$R_i = \sum_{j=1}^{t} a_{j,i}\, yQ_j = \sum_{j=1}^{t} b_{j,i} Q_j$$

where $b_{j,i} = a_{j,i} y \in \mathbb{Z}_q$.

6. Set the ciphertext $C = \{R_1, \ldots, R_t, rP, \alpha P_{\text{pub}}, \sigma \oplus H_2(e(P_{\text{pub}}, P_1)^r), E_{H_4(\sigma)}(M)\}$.

- *Decrypt:* Input the ciphertext $C = R_1, \ldots, R_t, U_1, U_2, V, W$, params, an identity ID_i and the private key d_i of the receiver with identity ID_i. To decrypt C, the algorithm performs the tasks as follows:

1. Compute $x_i = H(\text{ID}_i)$.
2. Set $\lambda = R_1 + x_i R_2 + \cdots + (x_i^{t-1} (\text{mod } q)) R_t$.
3. Compute $\sigma' = V \oplus H_2((e(U_1, d_i))/(e(U_2, \lambda)))$.
4. Compute $M' = D_{H_4(\sigma')}(W)$.
5. Set $r' = H_3(\sigma', M')$. Test whether $U_1 = r'P$ or not. If true, accept the plaintext message M', that is, $M' = M$; otherwise, reject the ciphertext.

A private key generator (PKG) is established to run Setup. When a user gives her/his ID to the PKG, the PKG inputs its public system parameters, the master key and the user's ID to Extract and returns a private key to the user. Users who have obtained their private keys from the PKG are called members. A user who sends out a message is said to be a sender. A sender can input the PKG's system parameters, the IDs of selected members and a plaintext message to Encrypt to get a ciphertext and then broadcasts it. The members the sender designated are called the receivers. When receiving a ciphertext, every member can input the PKG's system parameters, the ciphertext, her/his ID and her/his own private key to Decrypt. If the member is a receiver, then Decrypt returns the plaintext message; else it returns reject.

3 Anonymity analysis of Fan *et al.*'s scheme

Fan *et al.* formally showed that every receiver in their scheme is anonymous to any other receiver. Everyone can receive transmitted messages because they are broadcasted. Only the designated receivers can decrypt them successfully. Every receiver knows whether herself/himself is one of the designated receivers, but she/he cannot determine the others. We now show that Fan *et al.*'s anonymous multi-receiver IBE scheme cannot satisfy the anonymity.

Input the ciphertext $C = (R_1, \ldots, R_t, U_1, U_2, V, W)$, params, an identity ID_i and the private key d_i of the receiver with identity ID_i. We suppose that the set of the multi-receivers is S_{m}, and $\text{ID}_i \in S_{\text{m}}$. Then, ID_i can compute $x_i = H(\text{ID}_i)$ and yQ_i as follows

$$\begin{aligned} f(x_i) &= R_1 + x_i R_2 + \cdots + x_i^{i-1} R_i + \cdots + x_i^{t-1} R_t \\ &= (a_{1,1} yQ_1 + \cdots + a_{t,1} yQ_t) + (x_i a_{1,2} yQ_1 + \cdots \\ &\quad + x_i a_{t,2} yQ_t) + \cdots + (x_i^{t-1} a_{1,t} yQ_1 + \cdots \\ &\quad + x_i^{t-1} a_{t,t} yQ_t) \\ &= (a_{1,1} + a_{1,2}x_i + \cdots + a_{1,t}x_i^{t-1}) yQ_1 + \cdots \\ &\quad + (a_{t,1} + a_{t,2}x_i + \cdots + a_{t,t}x_i^{t-1}) yQ_t \\ &= yQ_i \end{aligned}$$

(by Lagrange interplating polynomial theorem). At the same time, anyone ID_a that does not belong to S_{m} cannot obtain yQ_a through the above computation.

$$\begin{aligned} f(x_a) &= R_1 + x_a R_2 + \cdots + x_a^{i-1} R_i + \cdots + x_a^{t-1} R_t \\ &= (a_{1,1} yQ_1 + \cdots + a_{t,1} yQ_t) + (x_a a_{1,2} yQ_1 \\ &\quad + \cdots + x_a a_{t,2} yQ_t) + \cdots \\ &\quad + (x_a^{t-1} a_{1,t} yQ_1 + \cdots + x_a^{t-1} a_{t,t} yQ_t) \\ &= (a_{1,1} + a_{1,2}x_a + \cdots + a_{1,t}x_a^{t-1}) yQ_1 \\ &\quad + \cdots + (a_{t,1} + a_{t,2}x_a + \cdots + a_{t,t}x_a^{t-1}) yQ_t \end{aligned}$$

According to the above computation, $f(x_a)$ has nothing to do with Q_a. On the other hand, $yH_1(\text{ID}_a)$ is random. So, the probability that $f(x_a) = yH_1(\text{ID}_a)$ holds is negligible.

Based on the above analysis, we know that

$$\forall \text{ID}_i \in S_{\text{m}}, f(\text{ID}_i) = yQ_i$$

If $\text{ID}_k \in S_{\text{m}}$, then the receiver ID_k can identify whether anyone is one of the designated receivers as follows:

Input ID_l, compute $f(x_l)$. If $e(Q_k, f(x_l)) = e(Q_l, f(x_k))$ holds, then ID_l belongs to S_{m}, that is, ID_l is one of the multi-receiver. The reason is that: if ID_l belongs to S_{m}, that is, ID_l is one of the multi-receiver, then, $f(x_l) = yQ_l$,

$f(x_k) = yQ_k$. So, $e(Q_k, f(x_l)) = e(Q_k, Q_l)^y = e(Q_l, f(x_k))$. If $e(Q_k, f(x_l)) = e(Q_l, f(x_k))$ does not hold, ID_l does not belong to S_m, that is, ID_l is not one of the multi-receiver. The reason is that: $f(x_l) \neq yQ_l$. So, $e(Q_k, f(x_l)) \neq e(Q_l, f(x_k))$.

Thus, every receiver can determine whether the other is one of the designated multi-receivers. Fan *et al.*'s anonymous multi-receiver IBE scheme cannot satisfy the anonymity.

4 Improvements on Fan *et al.*'s scheme

Our improved anonymous multi-receiver IBE scheme is based on Fan *et al.*'s scheme. The notations are the same with Fan *et al.*'s scheme. It also comprises: Setup, Extract, Encrypt and Decrypt. Our improvements have the same Setup and Extract with Fan *et al.*'s. The different parts are Encrypt and Decrypt. So, we only describe the processes of Encrypt and Decrypt in detail.

• *Encrypt:* Input params, a plaintext message M. Without loss of generality, we assume the ID set of the receivers is $(\mathrm{ID}_1, \ldots, \mathrm{ID}_t)$ where t $(1 \leq t \leq n)$ is selected by the encrypter and n denotes the number of all the users. The algorithm performs the following tasks:

1. Pick a string $\sigma \in_R \{0, 1\}^w$ and set $r = H_3(\sigma, M)$.
2. For $i = 1, \ldots, t$, pick different integers $\alpha_i \in_R \mathbb{Z}_q^*$ and set $y_i = \alpha_i^{-1} r (\mathrm{mod}\, q)$.
3. For $i = 1, \ldots, t$, compute $x_i = H(\mathrm{ID}_i)$ and $Q_i = H_1(\mathrm{ID}_i)$.
4. For $i = 1, \ldots, t$, compute

$$f_i(x) = \prod_{1 \leq j \neq i \leq t} \frac{x - x_j}{x_i - x_j} = a_{i,1} + a_{i,2}x + \cdots + a_{i,t}x^{t-1}$$

where $a_{i,1}, \ldots, a_{i,t} \in \mathbb{Z}_q$.

5. For $i = 1, \ldots, t$, compute $R_i = \sum_{j=1}^{t} a_{j,i} y_j Q_j = \sum_{j=1}^{t} b_{j,i} Q_j$ and $K_{i'} = \sum_{j=1}^{t} a_{j,i} K_j$ where $b_{j,i} = a_{j,i} y_j \in \mathbb{Z}_q$, $K_i = \alpha_i P_{\mathrm{pub}}$, $1 \leq i \leq t$.
6. Compute $V = \sigma \oplus H_2(e(P_{\mathrm{pub}}, P_1)^r)$, $W = E_{H_4(\sigma)}(M)$, and set the ciphertext $C = (R_1, \ldots, R_t, rP, K_{1'}, \ldots, K_{t'}, V, W)$.

• *Decrypt:* Input the ciphertext $C = (R_1, \ldots, R_t, U, K_{1'}, \ldots, K_{t'}, V, W)$, params, an identity ID_i and the private key d_i of the receiver with identity ID_i. To decrypt C, the algorithm performs the tasks as follows:

1. Compute $x_i = H(\mathrm{ID}_i)$.
2. Set $\lambda_i = R_1 + x_i R_2 + \cdots + (x_i^{t-1} (\mathrm{mod}\, q)) R_t$

$$v_i = K_{1'} + x_i K_{2'} + \cdots + (x_i^{t-1} (\mathrm{mod}\, q)) K_{t'}$$

3. Compute $\sigma_i' = V \oplus H_2((e(U_1, d_i))/(e(v_i, \lambda_i)))$.
4. Compute $M' = D_{H_4(\sigma_i')}(W)$.
5. Set $r_i' = H_3(\sigma_i', M')$ and test whether $U = r_i' P$ or not. If it holds, accept the plaintext message M', that is, $M' = M$; otherwise, reject the ciphertext.

5 Analysis of our improved scheme

5.1 Correctness

The decryption of our scheme is correct as follows:

For each $1 \leq i \leq t$, we have that

$$\begin{aligned}
\lambda_i &= R_1 + x_i R_2 + \cdots + x_i^{j-1} R_i + \cdots + x_i^{t-1} R_t \\
&= (a_{1,1} + a_{1,2}x_i + \cdots + a_{1,t}x_i^{t-1}) y_1 Q_1 \\
&\quad + \cdots + (a_{i,1} + a_{i,2} + \cdots + a_{i,t}x_i^{t-1}) y_i Q_i \\
&\quad + \cdots + (a_{t,1} + a_{t,2}x_i + \cdots + a_{t,t}x_i^{t-1}) y_t Q_t \\
&= y_i Q_i \\
v_i &= K_1' + x_i K_2' + \cdots + x_i^{i-1} K_i' + \cdots + x_i^{t-1} K_t' \\
&= (a_{1,1} + a_{1,2}x_i + \cdots + a_{1,t}x_i^{t-1}) K_1 \\
&\quad + \cdots + (a_{i,1} + a_{i,2} + \cdots + a_{i,t}x_i^{t-1}) K_i \\
&\quad + \cdots + (a_{t,1} + a_{t,2}x_i + \cdots + a_{t,t}x_i^{t-1}) K_t \\
&= K_i
\end{aligned}$$

We can obtain

$$\begin{aligned}
\frac{e(U, d_i)}{e(v_i, \lambda_i)} &= \frac{e(U, d_i)}{e(K_i, \lambda_i)} \\
&= \frac{e(rP, s(Q_i + P_1))}{e(\alpha_i P_{\mathrm{pub}}, y_i Q_i)} \\
&= \frac{e(rP, sQ_i) e(rP, sP_1)}{e(P_{\mathrm{pub}}, Q_i)^{\alpha_i y_i}} \\
&= \frac{e(P_{\mathrm{pub}}, Q_i)^r e(P_{\mathrm{pub}}, P_1)^r}{e(P_{\mathrm{pub}}, Q_i)^r} \\
&= e(P_{\mathrm{pub}}, P_1)^r
\end{aligned}$$

Thus

$$\begin{aligned}
\sigma' &= V \oplus H_2\left(\frac{e(U, d_i)}{e(K_i, \lambda_i)}\right) \\
&= V \oplus H_2(e(P_{\mathrm{pub}}, P_1)^r) \\
&= \sigma
\end{aligned}$$

and

$$M' = D_{H_4(\sigma')}(W) = D_{H_4(\sigma)}(E_{H_4(\sigma)}(M)) = M$$

□

5.2 Confidentiality and receiver anonymity

The security requirement of confidentiality is semantic security and receiver anonymity. It means that no useful information about a plaintext message can be gotten from the corresponding ciphertext. Our improved scheme's confidentiality is defined in the security notion 'Indistinguishability of encryptions under selective multi-ID, chosen ciphertext attacks (IND-sMID-CCA) [8, 9]'. Receiver anonymity means that every user only knows whether she/he is one of the exact receivers of a ciphertext, while she/he cannot determine whether any other user is an exact receiver or not. Our improved scheme's ANON-sMID-CCA is defined based on the security notion 'Anonymous

IET Inf. Secur., 2012, Vol. 6, Iss. 1, pp. 20–27
doi: 10.1049/iet-ifs.2010.0252

indistinguishability of encryptions under selective-ID, chosen ciphertext attacks (ANON-sID-CCA) [8, 15]'.

Theorem 1: The improved multi-receiver IBE scheme is $(\tau, q_H, q_{H1}, q_{H2}, q_{H2}, q_{H3}, q_{H4}, q_1, q_2, \varepsilon)$-IND-sMID-CCA secure under the (τ', ε')-Co-DBDH assumption, where $\varepsilon' \geq \varepsilon$ and $\tau' \simeq \tau + (q_{H_1} + q_{H_3} + q_1)\mathcal{O}(\tau_1) + q_2\mathcal{O}(\tau_1 + \tau_2) + (q_H + q_{H_2} + q_{H_4})\mathcal{O}(1)$. ($q_1$, q_2, q_H, q_{H1}, q_{H2}, q_{H3}, q_{H4} denote the number of private key extraction queries, decryption queries and queries to the hash functions H, H_1, H_2, H_3, H_4, respectively. τ_1 and τ_2 denote the computing time for a scalar multiplication in $\mathbb{G}_1$ and a pairing e, respectively.)

Proof: Assume that $\mathcal{A}$ is a $(\tau, q_H, q_{H_1}, q_{H_2}, q_{H_2}, q_{H_3}, q_{H_4}, q_1, q_2, \varepsilon)$, attacker against our improved scheme. By utilising $\mathcal{A}$, the challenger $\mathcal{B}$ can solve the Co-DBDH problem with advantage ε' within running time τ'. Based on the Co-DBDH assumption, our improved scheme's confidentiality is satisfied.

Assume $\mathcal{B}$ is given $(q, \mathbb{G}_1, \mathbb{G}_2, e, P, aP, bP, Q, Z)$ as an instance of the Co-DBDH problem. $\mathcal{B}$ simulates the environment for $\mathcal{A}$ as follows:

Phase 1: Suppose that $\mathcal{A}$ outputs target multiple identities $(\mathrm{ID}_1, \ldots, \mathrm{ID}_t)$ where t is a positive integer.

Setup: $\mathcal{B}$ sets $P_1 = Q$ and $P_{\mathrm{pub}} = bP$. The public parameters $(q, \mathbb{G}_1, \mathbb{G}_2, e, n, P, P_1, P_{\mathrm{pub}}, H, H_1, H_2, H_3, H_4)$ is given to $\mathcal{A}$, where n denotes the number of all the users.

Let T, T_1, T_2, T_3, T_4 be some tables which will be used for storing the results of querying H, H_1, H_2, H_3, H_4, respectively.

H-query: Input ID_j, $\mathcal{B}$ checks the table T. If there exists (ID_j, x_j) in T, return x_j. Otherwise, pick an integer $x_j \in_R \mathbb{Z}_q^*$ and put (ID_j, x_j) in T, then return x_j.

H_1-query: Input ID_j, $\mathcal{B}$ checks the table T_1. If there exists $(\mathrm{ID}_j, l_j, Q_j)$ in T_1, return Q_j. Otherwise, pick an integer $l_j \in_R \mathbb{Z}_q^*$ and compute $Q_j = l_jP$ for $j \in \{1, 2, \ldots, t\}$ and $Q_j = l_jP - P_1$ for $j \notin \{1, 2, \ldots, t\}$, then put $(\mathrm{ID}_j, l_j, Q_j)$ in T_1 and return Q_j.

H_2-query: Input Z_j, $\mathcal{B}$ checks the table T_2. If there exists (Z_j, δ_j) in T_2, return δ_j. Otherwise, pick a string $\delta_j \in_R \{0, 1\}^w$ and put (Z_j, δ_j) in T_2, then return δ_j.

H_3-query: Input a pair (σ_j, M_j), $\mathcal{B}$ checks the table T_3. If there exists $(\sigma_j, M_j, \rho_j, \Gamma_j)$ in T_3, return ρ_j. Otherwise, pick $\rho_j \in_R \mathbb{Z}_q^*$ and compute $\Gamma_j = \rho_jP$, then put $(\sigma_j, M_j, \rho_j, \Gamma_j)$ in T_3 and return ρ_j.

H_4-query: Input σ_j, $\mathcal{B}$ checks the table T_4. If there exists (σ_j, η_j) in T_4, return η_j. Otherwise, pick $\eta_j \in_R \{0, 1\}^w$ and put (σ_j, η_j) in T_4, then return η_j.

Phase 2: $\mathcal{A}$ issues private key extraction queries for ID_j where $j \notin \{1, 2, \ldots, t\}$. If there exists $(\mathrm{ID}_j, l_j, Q_j)$ in T_1, then compute $d_j = l_jP_{\mathrm{pub}}$; otherwise, choose $l_j \in_R \mathbb{Z}_q^*$ and compute $d_j = l_jP_{\mathrm{pub}}$, $Q_j = l_jP - P_1$, then put $(\mathrm{ID}_j, l_j, Q_j)$ in T_1. Finally, return d_j.

Phase 3: $\mathcal{A}$ issues decryption queries (C^*, ID_i) for ID_i where $i \in \{1, 2, \ldots, t\}$, $C^* = (R_1, \ldots, R_t, U, K_{1'}, \ldots, K_{t'}, V, W)$. $\mathcal{B}$ performs the steps as follows:

1. Search T_3 to obtain (M_j, ρ_j) when $\Gamma_j = U$. If not, return 'reject'.
2. Compute $x_i = H(\mathrm{ID}_i)$.
3. Compute

$$\lambda_i = R_1 + x_iR_2 + \cdots + (x_i^{t-1} (\mathrm{mod}\, q))R_t$$

$$v_i = K_1' + x_iK_2' + \cdots + (x_i^{t-1} (\mathrm{mod}\, q))K_t'$$

4. Compute

$$\sigma' = V \oplus H_2\left(\frac{e(P_{\mathrm{pub}}, \rho_jP_1)e(U, l_iP_{\mathrm{pub}})}{e(v_i, \lambda_i)}\right)$$

where

$$\begin{aligned} e(P_{\mathrm{pub}}, \rho_jP_1)e(U, l_iP_{\mathrm{pub}}) &= e(bP, \rho_jP_1)e(U, l_ibP) \\ &= e(\rho_jP, bP_1)e(U, bl_iP) \\ &= e(U, b(P_1 + Q_i)) \\ &= e(U_1, d_i) \end{aligned}$$

5. Test whether $M_j = D_{H_4(\sigma')}(W)$ or not. If not, return 'reject'; else return M_j.

Challenge: $\mathcal{A}$ outputs a target plaintext pair (M_0, M_1). Upon receiving (M_0, M_1), $\mathcal{B}$ performs the steps as follows:

1. Choose $\beta \in_R \{0, 1\}$.
2. For $i = 1, \ldots, t$, search T_1 to obtain l_i that corresponds to ID_i.
3. Pick $\alpha_i \in_R \mathbb{Z}_q^*$ for $i = 1, 2, \ldots, t$ and $\sigma \in_R \{0, 1\}^w$.
4. Set $U = aP = rP$ and $K = Z$.
5. For $i = 1, 2, \ldots, t$, compute

$$f_i(x) = \prod_{1 \leq j \neq i \leq t} \frac{x - x_j}{x_i - x_j} = a_{i,1} + a_{i,2}x + \cdots + a_{i,t}x^{t-1}$$

where $a_{i,1}, a_{i,1}, \ldots, a_{i,t} \in \mathbb{Z}_q$.

6. For $i = 1, 2, \ldots, t$, compute

$$\begin{aligned} R_i &= \sum_{j=1}^{t} a_{j,i}\alpha_j^{-1}l_jU \left(= \sum_{j=1}^{t} a_{j,i}\alpha_j^{-1}rl_jP\right) \\ &= \sum_{j=1}^{t} a_{j,i}y_jQ_j = \sum_{j=1}^{t} b_jQ_j \Bigg) \end{aligned}$$

7. Create a target ciphertext $C = (R_1, \ldots, R_t, U, \alpha_1P_{\mathrm{pub}}, \ldots, \alpha_tP_{\mathrm{pub}}, \sigma \oplus H_2(K), E_{H_4(\sigma)}(M_\beta))$.
8. Return C to $\mathcal{A}$.

Phase 4: $\mathcal{A}$ issues private key extraction queries and decryption queries as those in *Phase 2* and *Phase 3*. The restriction in the decryption queries is that $C^* \neq C$.

Guess: Finally, $\mathcal{A}$ outputs its guess $\beta' \in \{0, 1\}$. If $\beta' = \beta$, then $\mathcal{B}$ outputs 1. Otherwise, $\mathcal{B}$ outputs 0.

If $K = e(P, Q)^{ab}$, then

$$\begin{aligned} \sigma \oplus H_2(K) &= \sigma \oplus H_2(e(bP, Q)^a) \\ &= \sigma \oplus H_2(e(P_{\mathrm{pub}}, P_1)^r) \end{aligned}$$

Hence, C is a valid ciphertext. Otherwise, C is invalid. On the other hand, $\mathcal{B}$ successfully simulates the random oracles $\{H, H_1, H_2, H_3, H_4\}$, the private key extraction and the decryption oracles in Phases 2, 3 and 4. Hence, we obtain

$$\Pr[\mathcal{B}(P, aP, bP, Q, e(P, Q)^{ab}) = 1] = \Pr[\beta' = \beta]$$

where $|\Pr[\beta' = \beta] - (1/2)| \geq \varepsilon$ according to the assumption in Theorem 1. Therefore we have

$$|\Pr[\mathcal{B}(P, aP, bP, Q, e(P, Q)^{ab}) = 1] - \Pr[\mathcal{B}(P, aP, bP, Q, Z) = 1]| \geq \varepsilon$$

where $Z \in_R \mathbb{G}_2$.

Thus, $\varepsilon' \geq \varepsilon$ and $\tau' \simeq \tau + (q_{H_1} + q_{H_3} + q_1)\mathcal{O}(\tau_1) + q_2\mathcal{O}(\tau_1 + \tau_2) + (q_H + q_{H_2} + q_{H_4})\mathcal{O}(1)$, where τ_1 and τ_2 denote the computing time for a scalar multiplication in $\mathbb{G}_1$ and a pairing e, respectively. □

Notes: The proving process is very similar with Fan *et al.*'s proving process. The differences exist in Phase 3, Challenge and Phase 4. In order to make our paper self-contained, we describe the whole proving process in detail.

Theorem 2: In the received ciphertext, it is computational difficult to build the relation of the receivers.

Proof: Suppose the received ciphertext is $C = (R_1, \ldots, R_t, U, K'_1, \ldots, K'_t, V, W)$. From the Encrypt procedure, we know that

$$\begin{aligned}\lambda(x) &= R_1 + xR_2 + x^2R_3 + x^3R_4 + \cdots + x^{t-1}R_t \\ &= f_1(x)y_1Q_1 + f_2(x)y_2Q_2 + \cdots + f_t(x)y_tQ_t \\ &= f_1(x)\alpha_1^{-1}rQ_1 + f_2(x)\alpha_2^{-1}rQ_2 \\ &\quad + \cdots + f_t(x)\alpha_t^{-1}rQ_t\end{aligned}$$

and

$$\begin{aligned}v(x) &= K'_1 + xK'_2 + x^2K'_3 + x^3K'_4 + \cdots + x^{t-1}K'_t \\ &= f_1(x)\alpha_1P_{\text{pub}} + f_2(x)\alpha_2P_{\text{pub}} + \cdots + f_t(x)\alpha_tP_{\text{pub}}\end{aligned}$$

For polynomials $f_i(x)$, $1 \leq i \leq t$, it satisfies

$$f_i(x) = \begin{cases} 1, & x = x_i \\ 0, & x \in \{x_1, \ldots, x_t\} - \{x_i\} \end{cases}$$

Thus, when the variable x denotes the values $\{x_1, x_2, \ldots, x_t\}$, the function $\lambda(x)$ obtains the values $\{\alpha_1^{-1}rQ_1, \alpha_2^{-1}rQ_2, \ldots, \alpha_t^{-1}rQ_t\}$ and $v(x)$ obtains $\{\alpha_1P_{\text{pub}}, \alpha_2P_{\text{pub}}, \ldots, \alpha_tP_{\text{pub}}\}$. As α_i, $1 \leq i \leq t$ is picked at random from $\mathbb{Z}_q^*$, then the values $\{\alpha_1^{-1}rQ_1, \alpha_2^{-1}rQ_2, \ldots, \alpha_t^{-1}rQ_t\}$ are pairwise independent, and the values $\{\alpha_1P_{\text{pub}}, \alpha_2P_{\text{pub}}, \ldots, \alpha_tP_{\text{pub}}\}$ are also pairwise independent.

When the variable x does not belong to $\{x_1, x_2, \ldots, x_t\}$, the attacker can obtain $(P, P_{\text{pub}}, \{\text{ID}_1, \ldots, \text{ID}_n\}, U, v(x), \lambda(x))$. According to G-*xyz*-DDH-M problem, the attacker cannot decide which t users satisfy the relation of $\lambda(x) = f_1(x)\alpha_1^{-1}rQ_1 + f_2(x)\alpha_2^{-1}rQ_2 + \cdots + f_t(x)\alpha_t^{-1}rQ_t$.

On the other hand, r is also picked from $\mathbb{Z}_q^*$ and V, W are random in the random oracle. So, U, V, W cannot help to build the relation of the receivers.

Thus, in the received ciphertext, it is computational difficult to build the relation of the receivers. □

Notes: Our receiver anonymity attack succeeds through building the relation of the receivers. For any two receivers $(\text{ID}_i, \text{ID}_j)$, the relation of $e(Q_i, \lambda(x_j)) = e(Q_j, \lambda(x_i))$ holds. Thus, Fan *et al.*'s scheme does not satisfy Theorem 2.

Theorem 3: The improved multi-receiver IBE scheme is $(\tau, q_H, q_{H1}, q_{H2}, q_{H3}, q_{H4}, q_1, q_2, \varepsilon)$-ANON-sID-CCA secure under the (τ', ε')-DBDH-M assumption, where $\varepsilon' \geq \varepsilon$ and

$$\tau' \simeq \tau + (q_{H_1} + q_{H_3} + q_1)\mathcal{O}(\tau_1) + q_2\mathcal{O}(\tau_1 + \tau_2) + (q_H + q_{H_2} + q_{H_4})\mathcal{O}(1)$$

($q_1, q_2, q_H, q_{H_1}, q_{H_2}, q_{H_3}, q_{H_4}$ denote the number of private key extraction queries, decryption queries and queries to the hash functions H, H_1, H_2, H_3, H_4, respectively. τ_1 and τ_2 denote the computing time for a scalar multiplication in $\mathbb{G}_1$ and a pairing e, respectively.)

Notes: The proof process of the above theorem is the same as Theorem 3 in Fan *et al.*'s paper [8]. Thus, we omit this proof process. In fact, when the number of receivers is one, our scheme is the same as Fan *et al.*'s scheme. Fan *et al.* scheme's Theorem 3 is proved when $t = 1$. Our scheme's Theorem 3 considers also the case $t = 1$. So, the proof processes of the two theorems are the same.

Theorem 4: The improved multi-receiver IBE scheme is ANON-sMID-CCA secure under the G-xyz-DDH-M assumption and DBDH-M assumption.

Proof: The attacker trys to decide the receiver through two methods: (1) the attacker decides the receivers through building the relation of the receivers in the received ciphertext; (2) the attacker decides the receivers through decryption queries and private key extraction queries. We will show the two methods cannot succeed.

We prove this theorem by contrary evidence. Suppose $\mathcal{A}$ can succeed to attack the ANON-sMID-CCA of our improved multi-receiver IBE scheme. From Theorem 2, we know that the attack method (1) cannot succeed. Then, $\mathcal{A}$ can only decide the receivers through the attack method (2). We consider the special case, that is, $t = 1$. Thus, if the attacker $\mathcal{A}$ can decide the receiver, then it is paradoxical with Theorem 3. So, the improved multi-receiver IBE scheme is ANON-sMID-CCA secure according to Theorems 2 and 3. As Theorem 2 succeeds based on G-*xyz*-DDH-M assumption and Theorem 3 succeeds based on DBDH-M assumption, our improved multi-receiver IBE scheme is ANON-sMID-CCA secure under the G-*xyz*-DDH-M assumption and DBDH-M assumption. □

Notes: Why Fan *et al.*'s scheme cannot satisfy the receiver anonymity? The flaw exists that they only consider a receiver in their proving process. Our improved multi-receiver IBE's anonymity is proved in the multi-receiver case. Thus, our improved anonymous multi-receiver IBE scheme is ANON-sMID-CCA secure.

6 Performance analysis and comparisons

We analyse our scheme's performance based on two cases: (1) computation and communication cost comparisons; (2) properties comparisons.

doi: 10.1049/iet-ifs.2010.0252

Table 1 Performance analysis and comparisons

	DWGW[5]	LHL [16]	CS [17]	Ours
cost of Encrypt	$(t+1)$GM $+ 2(t-1) + 1e$	$\left(\frac{t}{2}+2\right)$GM $+\left(\frac{t}{2}-1\right)$GA $+ 1e$	$(jt+\tau+2)$ GM $+ (jn)$ GA $+ 1e$	$2(t^2+1)$ GM $+ 2t(t-1)$ GA $+ 1e$
cost of Decrypt	tGM $+ (t-2)$GA $+ 2e$	$\left(\frac{t}{2}-1\right)$GM $+\left(\frac{t}{2}-2\right)$GA $+ 2e$	$(j\hat{S})$ GM $+ (j\hat{S}-j+1)$ GA $+ 2e$	$2(t-1)$GM $+ 2(t-1)$ GA $+ 2e$
size	$(t+1)v + \|M\|$	$(t+1)v + \|M\|$	$(t+1)v + \hat{\omega} + \|M\|$	$(2t+1)$ $v + \hat{\omega} + \|M\|$
Anon	no	no	no	yes
IBE	yes	no	yes	yes

In the encryption and decryption, the bilinear pairing, exponentiation computation in $\mathbb{G}_2$, point multiplication and point addition in $\mathbb{G}_1$ are more time-consuming then the other algorithms, such as *Hash* function, symmetric encryption, symmetric decryption etc. We only consider these expensive computations in our comparison. The communication cost can be expressed according to the ciphertext size. At the same time, we also consider the properties comparison. We consider the properties: receiver anonymity, ID based etc.

From Table 1, we know that the computation cost of our scheme is higher than [5, 16, 17]. At the same time, the communication cost is also higher. Why do we design this scheme? This is because that our scheme is tailored for receiver anonymity. Furthermore, the security of receiver anonymity has been formally proved in Theorem 4.

- $|\mathrm{ID}|$: the bit length of an ID
- j: an integer, $1 \leq j \leq |\mathrm{ID}|$
- n: the number of all users
- t: the number of receivers, $1 \leq t \leq n$
- $\hat{S}$: the number of the subgroups which S is divided into
- GA: addition in $\mathbb{G}_1$ or multiplication in $\mathbb{G}_2$
- GM: multiplication in $\mathbb{G}_1$ or exponentiation computation in $\mathbb{G}_2$
- e: bilinear pairing mapping
- v: the bit length of an element in $\mathbb{G}_1$
- $|M|$: the bit length of a plaintext message
- $\hat{\omega}$: the total bit length of the IDs of all receivers

7 Conclusion

In this paper, we point out that Fan *et al.*'s scheme does not satisfy the anonymity. Taking use of the bilinear pairing, we give the attack method. Our anonymity analysis showed that every receiver in Fan *et al.*'s scheme is not anonymous to any other receiver. Fan *et al.*'s scheme is insecure. We showed that simple protocol changes can fix these weaknesses and render Fan *et al.*'s scheme. The improved scheme is proved to satisfy the confidentiality and receiver anonymity in the random oracle. We will study more efficient anonymous multi-receiver encryption scheme in the future.

8 Acknowledgments

The authors sincerely thank the Editor for allocating qualified and valuable referees. The authors sincerely thank the anonymous referees for their very valuable comments. This research is supported in part by Natural Science Foundation of Liaoning Province (no. 20102042), by China Post-doctor Science Fund (no. 20110490061), by Program for Liaoning Excellent Talents in University (no. LJQ2011078) and by the Spanish government through project CONSOLIDER INGENIO 2010 CSD2007-0004 'ARES', TSI2007-65406-C03-01 'E-AEGIS', TIN2009-11689 'RIPUP', 'eVerification' TSI-020100-2009-720, by the Government of Catalonia under grant 2009 SGR 1135, and by the NSF of China through projects 60970116, 61003214, 60970140 and 61173154. The authors also acknowledge support by the Fundamental Research Funds for the Central Universities of China to Project 3103004, and Shaanxi Provincial Education Department through Scientific Research Program 2010JK727.

9 References

1 Shamir, A.: 'Identity-based cryptosystems and signature schemes'. Proc. CRYPTO 84, 1984, (*LNCS*, **196**), pp. 47–53
2 Boneh, D., Franklin, M.: 'Identity-based encryption from the weil pairing', *SIAM J. Comput.*, 2003, **32**, (3), pp. 586–615
3 Boyen, X., Waters, B.: 'Anonymous hierarchical identity-based encryption (without random oracles)'. Proc. CRYPTO 2006, 2006, (*LNCS*, **4117**), pp. 290–307
4 Abdalla, M., Kiltz, E., Neven, G.: 'Generalised key delegation for hierarchical identity-based encryption', *IET Inf. Secur.*, 2008, **2**, (3), pp. 67–78
5 Du, X., Wang, Y., Ge, J., Wang, Y.: 'An id-based broadcast encryption scheme for key distribution', *IEEE Trans. Broadcast.*, 2005, **51**, (2), pp. 264–266
6 Chien, H.: 'Comments on an efficient id-based broadcast encryption scheme', *IEEE Trans. Broadcast.*, 2007, **53**, (4), pp. 809–810
7 Wang, L., Wu, C.: 'Efficient identity-based multicast scheme from bilinear pairing', *IEE Proc. Commun.*, 2005, **152**, (6), pp. 877–882
8 Fan, D., Huang, L., Ho, P.: 'Anonymous multireceiver identity-based encryption', *IEEE Trans. Comput.*, 2010, **59**, (9), pp. 1239–1249
9 Baek, J., Safavi-Naini, R., Susilo, W.: 'Efficient multi-receiver identity-based encryption and its application to broadcast encryption'. PKC 2005, 2005, (*LNCS*, **3386**), pp. 380–397
10 Lu, L., Hu, L.: 'Pairing-based multi-recipient public key encryption'. Proc. 2006 Int. Conf. on Security & Management, 2006, pp. 159–165
11 Yuen, T., Wei, V.: 'Fast and proven secure blind identity-based signcryption from pairings'. CT-RSA, 2005, (*LNCS*, **3376**), pp. 305–322
12 Wei, V., Yuen, T., Zhang, F.: 'Group signature where group manager members open authority are identity-based'. ACISP 2005, 2005, (*LNCS*, **3574**), pp. 468–480
13 Chabanne, H., Phan, D., Pointcheval, D.: 'Public traceability in traitor tracing schemes'. Proc. EUROCRYPT 2005, 2005, (*LNCS*, **3494**), pp. 542–558
14 Laguillaumie, F., Vergnaud, D.: 'Time-selective convertible undeniable signatures'. CT-RSA 2005, 2005, (*LNCS*, **3376**), pp. 154–171
15 Bethencourt, J., Chan, H., Perrig, A., Shi, E., Song, D.: 'Anonymous multi-attribute encryption with range query and conditional decryption'. Technical Report, Carnegie Mellon University, CMU-CS-06-135, 2006
16 Lee, J.W., Hwang, Y.H., Lee, P.J.: 'Efficient public key broadcast encryption using identifier of receivers'. Information Security Practice and Experience, 2006, pp. 153–164
17 Chatterjee, S., Sarkar, P.: 'Multi-receiver identity-based key encapsulation with shortened ciphertext'. Progress in Cryptology-INDOCRYPT 2006, 2006, pp. 394–408