Advance Access publication on 15 September 2011
doi:10.1093/comjnl/bxr086

Improved Anonymous Multi-receiver Identity-Based Encryption

HUNG-YU CHIEN*

Department of Information Management, National Chi-Nan University, Nantou, Taiwan
**Corresponding author: redfish6@ms45.hinet.net*

In 2010, Fan *et al.* proposed an efficient anonymous multi-receiver identity-based encryption scheme. This scheme allows a sender to send an encrypted message to a set of designated receivers while preserving receiver anonymity. The scheme is highly efficient for each receiver as it requires only two pairing operations. However, we found that the scheme failed to protect receiver anonymity and the security notation for receiver anonymity captures only semantics in the case of a single receiver, but does not for multiple recipients. In this paper, we present the weaknesses and propose an improved scheme. The improved scheme enhances both security and computational performance.

Keywords: cryptography; multicast; anonymity; pairing; encryption

Received 21 December 2010; revised 20 April 2011
Handling editor: Jong Hyuk Park

1. INTRODUCTION

In a distributed environment, there are many applications that require a sender to efficiently and securely transmit messages to a set of authorized receivers, and only those authorized receivers are allowed to access the content. At times, the set of authorized receivers will change dynamically. Examples of such applications include a conference on VoIP and pay-TV systems. These scenarios require an efficient multi-cast scheme such as those in [1–5] or a multi-receiver encryption scheme such as those in [6–9]. Interestingly, in several application scenarios of multi-cast encryption or multi-receiver encryption, an authorized receiver does not want other entities, except for the operating center, to have identity information (or personal credential information. One example is for pay-TV systems where one want to protect his personal viewing selection, especially in regard to sensitive programs. This makes it necessary to have identity protection or anonymity protection [9] for personal privacy interest. Another interesting application of anonymous multi-receiver encryption scheme is like the recent Tunisia's Jasmine Revolution [10] and its following revolutions (or called Twitter Revolution), where one sender wants to send an encrypted protest proposal to a set of designated persons such that only the designated receiver is able to decrypt and verify the message. For such applications, revealing the identity of each possible receiver would endanger receiver's safety. An interesting property of such applications is that the membership of such group of designated receivers is usually dynamic or even *ad hoc*.

One can implement the earlier-mentioned schemes with either a symmetric-key setting or an asymmetric-key setting. However, key management in a symmetric-key setting is not scalable since the number of shared keys that one entity needs to maintain increases linearly with the number of potential receivers. In contrast, a scheme with an asymmetric-key setting has better scalability. Currently, asymmetric-key settings based on a certificate are very popular, but such settings require an entity to first verify the to-be-used public key and then verify a signature or encrypted messages using the verified public key. This public key verification and certificate maintenance incurs extra overhead. In 1984, Shamir [11] proposed the first identity-based cryptosystem or ID-based cryptosystem, where an entity's public well-known identity (such as social security number, e-mail address or IP address) is used as a public key, such that there is no need to verify the public key before using it. This approach saves on the overhead in public-key maintenance. Therefore, this paper focuses on multi-receiver identity-based encryption schemes that take into consideration receiver privacy.

In 2001, Boneh and Franklin [12] proposed an identity-based encryption scheme using Weil pairing. Subsequent to that, many researchers tried to improve upon the scheme [1, 2, 4–6, 8, 13]. In 2005, Du *et al.* [1] proposed an efficient ID-based multi-cast scheme, but Chien [2] reported a security weakness in the scheme. Later, Lee *et al.* [3] and Yang *et al.* [4], respectively, proposed their own ID-based broadcasting schemes, but did not consider the issue of members joining and leaving.

In 2005, Wang and Wu [5] proposed an identity-based multicast encryption scheme, but only the group center is allowed to multi-cast the message and an efficient algorithm was not proposed to handle membership change. In a multi-receiver encryption scheme, a sender randomly chooses each time a set of authorized receivers. Baek *et al.* [6] proposed a multi-receiver ID-based key encryption scheme and proved the security in the selective-ID model using the random oracle technology. Lu and Hu [7] also proposed a multi-receiver public-key encryption scheme using pairing. Chatterjee and Sarkar [8] proposed the first multi-receiver ID-based encryption scheme with sub-linear cipher-text sizes. None of these schemes, however, consider the issue of receiver anonymity.

To protect signer anonymity, Lal and Kushwah [14] proposed an anonymous ID-based signcryption scheme for multi-receivers in the random oracle model, and Zhang and Xu [15] proposed an ID-based signcryption scheme for multiple receivers in the standard model. To protect receiver's anonymity, Wang *et al.* [16] and Xu [17], respectively, proposed ID-based encryption schemes for multi-receivers. However, in both [16] and [17], each group member needs to maintain two sets of public-key and private-key pairs, and one of the key-pair sets changes as group membership changes. These approaches, however, are inefficient.

Fan *et al.* [9] recently proposed an anonymous multi-receiver encryption scheme that is more efficient than its counterparts and claimed to protect receiver's anonymity. We found, however, that Fan *et al.*'s scheme failed to protect receiver anonymity. The security weaknesses include: (i) an authorized receiver can easily verify whether a specific user is also one of the authorized receivers using only two pairing computations; (ii) a non-authorized entity can tell which entity is an authorized receiver using only $O(n^2)$ computations, *where n is the number of designated receivers*; and (iii) the definition of anonymity in Fan *et al.*'s work only captures and protects the anonymity for a case where there is only one receiver and fails to consider most cases that have more than one receiver.

This paper discusses the weaknesses of Fan *et al.*'s schemes and then proposes a new scheme. The proposed scheme improves security and computational performance. The rest of this paper is organized as follows. Section 2 reviews Fan *et al.*'s scheme and then reports on weaknesses in the scheme. Section 3 proposes our new scheme. Section 4 analyzes its security and evaluates performance. Finally, Section 5 states our conclusions.

2. SECURITY WEAKNESSES IN FAN *ET AL.*'S SCHEME

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

The scheme is based on pairing in elliptic curve systems. Let G_1 be an additive group and G_2 be a multiplicative group where both groups are cyclic with a prime order q. Let P be a randomly chosen generator for G_1 and e be a bilinear mapping such that $e : G_1 \times G_1 \rightarrow G_2$. Fan *et al.*'s scheme consists of four algorithms: Setup, Extract, Encrypt and Decrypt.

Setup: The system initializes global parameters as follows.

(i) Pick up an integer $s \in_R Z_q^*$ and an element $P_1 \in_R G_1$.
(ii) Set $P_{\text{pub}} = sP$.
(iii) Choose five cryptographic hash functions $H : \{0,1\}^* \rightarrow Z_q^*$, $H_1 : \{0,1\}^* \rightarrow G_1^*$, $H_2 : G_2 \rightarrow (0,1)^w$, $H_3 : \{0,1\}^w \times \{0,1\}^* \rightarrow Z_q^*$ and $H_4 : \{0,1\}^w \rightarrow (0,1)^w$ for some integer w. The symmetric encryption and decryption using a key k are denoted as $E_k()$ and $D_k()$, respectively.
(iv) Publish the system parameters $\text{params} \equiv \{q, G_1, G_2, e, n, P, P_1, P_{\text{pub}}, H, H_1, H_2, H_3, H_4\}$ and keep the master key s secret.

Extract: Input the system parameters and an entity identity $\text{ID}_i \in \{0,1\}^*$ for $i \in [1,n]$, the system returns the entity's private key $d_i = s(P_1 + Q_i)$, where $Q_i = H_1(ID_i)$.

Encrypt: When a sender wants to securely send a message M to a set of selected receivers $(\text{ID}'_1, \ldots, \text{ID}'_i, \ldots, \text{ID}'_t)$ with $1 \leq t \leq n$ and each identity is chosen from $(\text{ID}_1, \ldots, \text{ID}_i, \ldots, \text{ID}_n)$, he performs the following tasks.

(i) Pick a string $\sigma \in_R \{0,1\}^w$ and set $r = H_3(\sigma, M)$.
(ii) Pick an integer $\alpha \in_R Z_q^*$ and set $y = \alpha^{-1} r \bmod q$.
(iii) For $i = 1, \ldots t$, compute $x_i = H(\text{ID}'_i)$, $Q_i = H_1(\text{ID}'_i)$, $f_i(x) = \prod_{1 \leq j \neq i \leq t}(x - x_j/x_i - x_j) = a_{i,1} + a_{i,2}x + \cdots + a_{i,t}x^{t-1}$, $R_i = \sum_{j=1}^{t} a_{j,i} y Q_j = \sum_{j=1}^{t} b_{j,i} Q_j$, where $b_{j,i} = a_{j,i} y$.
(iv) Prepare $C \equiv (R_1, \ldots, R_t, U_1 = rP, U_2 = \alpha P_{\text{pub}}, V = \sigma \oplus H_2(e(P_{\text{pub}}, P_1)^r), W = E_{H_4(\sigma)}(M))$, and broadcast C.

Decrypt: Input the cipher-text C, *params* and one private key d_i, an authorized receiver with identity ID'_i decrypts the cipher-text as follows.

(i) Compute $x_i = H(\text{ID}'_i)$, $\lambda = R_1 + x_i R_2 + \cdots + x_i^{t-1} R_t$.
(ii) Compute $\sigma' = V \oplus H_2(e(U_1, d_i)/e(U_2, \lambda))$.
(iii) Compute $M' = D_{H_4(\omega')}(W)$.
(iv) Compute $r' = H_3(\sigma', M')$ and test whether $U_1 \stackrel{?}{=} r'P$ or not. If so, the receiver accepts the plaintext M; otherwise, he rejects the cipher-text.

2.2. Weaknesses in protecting receiver anonymity

Although one of the main goals of Fan *et al.*'s scheme is to protect a receiver's anonymity, we find that the scheme fails to protect the anonymity. (i) Any authorized receiver can easily verify whether another entity is also an authorized receiver using only two pairing operations; (ii) Anyone can find all receivers using $2 \cdot \binom{n}{2}$ pairing operations, provided that there

are $t \geq 2$ authorized receivers in that instance; (iii) Fan *et al.*'s security definition of anonymity only captures the case of a single receiver; therefore, their proof cannot ensure the security of more than one receiver. In the following we assume that there are $t \geq 2$ authorized receivers in that instance.

(1) Any receiver can easily verify whether another entity is also an authorized receiver using only two pairing operations.
Given a cipher-text $C \equiv (R_1, \ldots, R_t, U_1, U_2, V, W)$ with $t \geq 2$. We assume ID'_i is one of the $t \geq 2$ receivers. Then ID'_i can perform the following steps to verify whether another entity ID'_j is also an authorized receiver.

(i) Compute $x_i = H(\mathrm{ID}'_i)$,

$$\begin{aligned}\lambda_i &= R_1 + x_i R_2 + \cdots + x_i^{t-1} R_t \\ &= (a_{1,1} y Q_1 + \cdots + a_{t,1} y Q_t) \\ &\quad + x_i (a_{1,2} y Q_1 + \cdots + a_{t,2} y Q_t) \\ &\quad + \cdots + x_i^{t-1} (a_{1,2} y Q_1 + \cdots + a_{t,2} y Q_t) \\ &= (a_{1,1} + a_{1,2} x_i + \cdots + a_{1,t} x_i^{t-1}) y Q_1 \\ &\quad + \cdots + (a_{i,1} + a_{i,2} x_i + \cdots + a_{i,t} x_i^{t-1}) y Q_i \\ &\quad + \cdots + (a_{t,1} + a_{t,2} x_i + \cdots + a_{t,t} x_i^{t-1}) y Q_t \\ &= 0 + \cdots + y Q_i + \cdots + 0 = y Q_i\end{aligned}$$

(ii) Compute $x_j = H(\mathrm{ID}'_j)$ and $\lambda_j = R_1 + x_j R_2 + \cdots + x_j^{t-1} R_t$. This λ_j equals $y Q_j$ if ID'_j is an authorized receiver. But λ_j will be a random value $\in G_1$ and will equal $y Q_j$ with only negligible probability if ID'_j is not an authorized receiver.

(iii) Check whether the equation $e(\lambda_i, Q_j) \stackrel{?}{=} e(Q_i, \lambda_j)$ holds, where $e(\lambda_i, Q_j) = e(Q_i, Q_j)^y$ and $e(Q_i, \lambda_j)$ will equal $e(Q_i, Q_j)^y$ when ID'_j is an authorized receiver. Therefore, if ID'_j is an authorized receiver, then the equation $e(\lambda_i, Q_j) \stackrel{?}{=} e(Q_i, \lambda_j)$ will hold.

It takes two pairing operations to verify whether ID'_j is an authorized receiver.

(2) Anyone can identify all receivers using $O(n^2)$ pairing operations.
Given a cipher-text $C \equiv (R_1, \ldots, R_t, U_1, U_2, V, W)$ with $t \geq 2$. Anyone can perform the following steps to identify all the authorized receivers.

(i) For $1 \leq j \leq n$, compute $x_j = H(\mathrm{ID}_j)$ and $\lambda_j = R_1 + x_j R_2 + \cdots + x_j^{t-1} R_t$.

(ii) For any two identities ID_j and ID_k with $k, j \in [1, n]$, verify whether $e(\lambda_j, Q_k) \stackrel{?}{=} e(Q_j, \lambda_k)$ holds. Obviously, if both ID_j and ID_k are authorized receivers, then the equation should hold because $\lambda_j = y Q_j$, $\lambda_k = y Q_k$ and $e(\lambda_j, Q_k) = e(Q_j, \lambda_k) = e(Q_j, Q_k)^y$; but if either one of them is not an authorized receiver, then the equation will hold with only negligible probability because either λ_j or λ_k is a random value.

The above check takes $2 \cdot \binom{n}{2}$ pairing operations.

(3) The receiver anonymity definition of [9] cannot capture the security semantic of the cases of more than one receiver

To capture the security of anonymity, Fan *et al.* defined the following security notation for anonymity.

Definition ANON-sID-CPA. Let A be a polynomial-time attacker, and Π be a general multi-receiver ID-based encryption scheme. A interacts with a Challenger in the following game:

SETUP: The Challenger runs the *Setup* algorithm. It gives the attacker A the resulting public parameters *params*, but keeps the master key s secret.

PHASE 1: A outputs a target identity pair $(\mathrm{ID}_1, \mathrm{ID}_2)$. Upon receiving $(\mathrm{ID}_1, \mathrm{ID}_2)$, the Challenger randomly chooses $\beta \in \{1, 2\}$.

PHASE 2: A issues private key extraction queries. Upon receiving the query on ID_j, the Challenger returns $d_j = \mathrm{Extract}(\mathrm{params}, s, \mathrm{ID}_j)$ under the constraint that $\mathrm{ID}_j \neq \mathrm{ID}_1$ and $\mathrm{ID}_j \neq \mathrm{ID}_2$.

CHALLENGE: A outputs a target plaintext M. The Challenger returns a target cipher-text $C = \mathrm{Encrypt}(\mathrm{params}, \mathrm{ID}_\beta, M)$ to A.

PHASE 3: A issues private key extraction queries as in PHASE 2.

GUESS: A finally outputs its guess $\beta' \in \{1, 2\}$ and wins the game if $\beta' = \beta$.

2.3. The weakness of the earlier-mentioned definition

From $C = \mathrm{Encrypt}(\mathrm{params}, \mathrm{ID}_\beta, M)$ in the earlier-mentioned security definition, we can see that the sender only chooses one receiver in the encryption. This definition cannot capture the semantic of a multi-receiver setting. Fan *et al.* also defined anonymity security ANON-sID-CCA by extending the above game to adaptive chosen cipher-text attacks. However, the same definition flaw exists in the ANON-sID-CCA notation.

3. AN IMPROVED SCHEME WITH ENHANCED SECURITY AND COMPUTATIONAL PERFORMANCE

In this section, we propose a new scheme to enhance security and computational performance. The security of the proposed scheme is based on the Co-Bilinear Diffie–Hellman (Co-BDH) Problem [18, 19]. The new scheme is depicted in Fig. 1, and the process is described in the following.

DEFINITION 1 (Co-BDH Problem). *Given* $\langle P, aP, bP, Q\rangle$ *for some* $a, b \in_R Z_q^*$ *and* $Q \in_R G_1$, *compute* $e(P, Q)^{ab}$.

Our scheme also consists of four algorithms: Setup, Extract, Encrypt and Decrypt.

Setup: The system initializes the global parameters as follows.

(i) Pick up an integer $s \in_R Z_q^*$ and Set $P_{\text{pub}} = sP$.
(ii) Choose five cryptographic hash functions $H : \{0,1\}^* \to Z_q^*$, $H_1 : \{0,1\}^* \to G_1^*$, $H_2 : G_2 \to (0,1)^w$, $H_3 : \{0,1\}^w \to (0,1)^w$ and $H_4 : \{0,1\}^w \times \{0,1\}^* \to Z_q^*$ for some integer w. The symmetric encryption and decryption using a key k are denoted as $E_k()$ and $D_k()$, respectively.
(iii) Publish the system parameters $\text{params} \equiv \{q, G_1, G_2, e, n, P, P_{\text{pub}}, H, H_1, H_2, H_3\}$ and keep the master key s secret.

Extract: Input the system parameters and an entity identity $\text{ID}_i \in \{0,1\}^*$ for $i \in [1, n]$, the system returns the entity's private key $d_i = sQ_i$, where $Q_i = H_1(\text{ID}_i)$.

Encrypt: When a sender wants to securely send a message M to a set of selected receivers $(\text{ID}'_1, \ldots, \text{ID}'_i, \ldots, \text{ID}'_t)$ with $1 \le t \le n$ and each identity is chosen from $(\text{ID}_1, \ldots, \text{ID}_i, \ldots, \text{ID}_n)$, the sender performs the following tasks.

(i) Pick an integer $r \in_R Z_q^*$ and a random string $\sigma \in_R \{0,1\}^w$, and set $U_1 = rP$.
(ii) For $i = 1, \ldots t$, compute $R_i = \sigma \oplus H_2(e(P_{\text{pub}}, Q_i)^r) = \sigma \oplus H_2(e(P, Q_i)^{rs})$, where $Q_i = H_1(\text{ID}'_i)$.
(iii) Prepare $C \equiv (R_1, \ldots, R_t, U_1 = rP, U_2 = H(\sigma)P, V = E_{H_3(\sigma)}(M), W = H_4(\sigma, M))$, and broadcast C.

Decrypt: Input the cipher-text C, *params* and one private key d_i, an authorized receiver with identity ID'_i decrypts the cipher-text as follows.

Setup: system authority

1. $s \in_R Z_q^*$, $P_{pub} = sP$
2. $H : \{0,1\}^* \to Z_q^*$, $H_1 : \{0,1\}^* \to G_1^*$, $H_2 : G_2 \to \{0,1\}^w$,
   $H_3 : \{0,1\}^w \to \{0,1\}^w$, $H_4 : \{0,1\}^w \times \{0,1\}^* \to Z_q^*$
3. Encryption / decryption function : $E_k()$/ $D_k()$
4. Publish *params* $\equiv \{q, G_1, G_2, e, n, P, P_{pub}, H, H_1, H_2, H_3, H_4\}$

Extract(*params*, ID_i): system authority

1. compute $Q_i = H_1(ID_i)$, return $d_i = sQ_i$

Encrypt(*M*, { ID'_1, ..., ID'_i, ..., ID'_t}): sender

1. $r \in_R Z_q^*$, $\in_R \{0,1\}^w$, $U_1 = rP$
2. For $i = 1 \sim t$, compute $R_i = \sigma \oplus H_2(e(P_{pub}, Q_i)^r) = \sigma \oplus H_2(e(P, Q_i)^{rs})$
3. Set $C \equiv (R_1, ..., R_t, U_1 = rP, U_2 = H(\sigma)P, V = E_{H_3(\sigma)}(M), W = H_4(\sigma, M))$
4. Broadcast C

Decrypt(*C*, *params*, d_i }): receiver ID'_i

1. For $j = 1 \sim t$, compute $\sigma'_j = R_j \oplus H_2(e(U_1, d_j))$
   $= R_j \oplus H_2(e(P, Q_j)^{rs})$
   Verify *whether* $U_2 \stackrel{?}{=} H(\sigma'_j)P$.
   If such an j exists, then go to next step;
   otherwise, ID'_i is not an authorized receiver
2. $M' = D_{H_3(\sigma'_j)}(V)$
3. Verify *whether* $W \stackrel{?}{=} H_4(\sigma'_j, M')$.
   If so, accept M'; otherwise, reject C

FIGURE 1. The proposed anonymous multi-receiver ID-based encryption.

(i) For $j = 1, \ldots t$, compute $\sigma'_j = R_j \oplus H_2(e(U_1, d_j)) = R_j \oplus H_2(e(P, Q_j)^{rs})$ and verify whether $U_2 \stackrel{?}{=} H(\sigma'_j)P$. If there is a σ'_k satisfying the equation for some k for $1 \leq k \leq t$, then go to the next step; otherwise, ID'_i is not an authorized receiver.

(ii) Derive $M' = D_{H_3(\sigma'_k)}(V)$

(iii) Verify whether $W \stackrel{?}{=} H_4(\sigma'_k, M'))$. If so, the receiver accepts the message M'; otherwise, he rejects the cipher-text.

The rational of the proposed scheme is as follows. The privacy of the encryption key σ for each broadcast is based on the Co-BDH Problem instance $(U_1 = rP, P_{\mathrm{pub}} = sP, Q_i)$; therefore, only the authorized receiver ID'_i is able to derive the secret key σ. The anonymity of each receiver is ensured because $H_2(e(P, Q_i)^{rs})$ is the only value correlating to each authorized receiver and the value $e(P, Q_i)^{rs}$ is random that any entity (except the sender and the receiver himself) cannot tell it from a random value.

4. SECURITY ANALYSIS

In this section, we analyze the correctness and security of the proposed scheme.

(1) Correctness
If ID'_i is an authorized receiver, then this receiver can compute $e(U_1, d_i) = e(rP, sQ_i) = e(P, Q_i)^{rs} = e(P_{\mathrm{pub}}, Q_i)^r$, can derive the right σ from one of $(R_1, \ldots, R_t)$ and then decrypts the cipher-text.

(2) Privacy of the message
To decrypt the cipher-text, one should own the secret key $H_3(\sigma)$, which is a random value $\in_R \{0, 1\}^w$. The only way to derive σ is to compute $H_2(e(P, Q_i)^{rs})$ for some ID_i belonging to the authorized receiver set. Given $U_1 = rP$, $P_{\mathrm{pub}} = sP$ and Q_i, one would face the Co-BDH problem to compute $e(P, Q_i)^{rs}$ if he is not an authorized receiver.

(3) Anonymity of receivers
In the cipher-text, the only receiver-related value is $\{R_i = \sigma \oplus H_2(e(P_{\mathrm{pub}}, Q_i)^r)\}$. From $(R_1, \ldots, R_t)$, a *legitimate* receiver ID_i can derive $H_2(e(P_{\mathrm{pub}}, Q_i)^r) = H_2(e(P, Q_j)^{rs})$ of another *legitimate* receiver ID_j. But the value $H_2(e(P, Q_j)^{rs})$ is a random value on which ID_i has no way to verify whether it is a valid value or not and has no way to ensure whether ID_j is also an authorized receiver.

THEOREM 1. *The security (the confidentiality of the encryption) of the proposed scheme is secure if the Co-BDH Problem is hard.*

Proof. Given a cipher-text $C \equiv (R_1, \ldots, R_t, U_1 = rP, U_2 = H(\sigma)P, V = E_{H_3(\sigma)}(M), W = H_4(\sigma, M))$ where $R_i = \sigma \oplus H_2(e(P_{\mathrm{pub}}, Q_i)^r) = \sigma \oplus H_2(e(P, Q_i)^{rs})$, it is easy to see that one should derive the encryption key σ to decrypt the cipher-text and the only way to derive σ is to derive the value $e(P_{\mathrm{pub}}, Q_i)^r$ (or $e(P, Q_i)^{rs}$) first. However, given $(U_1 = rP, P_{\mathrm{pub}} = sP, Q_i = H_1(ID_i))$, one should face the Co-BDH Problem to compute $e(P_{\mathrm{pub}}, Q_i)^r$ (or $e(P, Q_i)^{rs}$). Since the Co-BDH is hard, the confidentiality of the proposed scheme is secure. □

THEOREM 2. *The receiver anonymity of the proposed scheme is secure if the Co-BDH problem is hard.*

Proof. To prove the receiver anonymity protection, we should differentiate an adversary who is a legitimate receiver and an adversary who is not a legitimate receiver.

For an adversary U who is not a legitimate receiver, the only receiver-identity-related values in a cipher-text $C \equiv (R_1, \ldots, R_t, U_1 = rP, U_2 = H(\sigma)P, V = E_{H_3(\sigma)}(M), W = H_4(\sigma, M))$ are $\{R_i = \sigma \oplus H_2(e(P_{\mathrm{pub}}, Q_i)^r)\}$. U might try the following two approaches to verify whether an entity ID_i is an authorized receiver. (i) Deriving the encryption key σ first and then verifying whether the equation $U_2 \stackrel{?}{=} H(\sigma)P$ holds; or (ii) deriving σ and M first, and then verifying whether the equation $W \stackrel{?}{=} H_4(\sigma, M)$ holds. The two approaches all need to derive σ, and it requires U to compute $e(P, Q_i)^{rs}$ and $H_2(e(P, Q_i)^{rs})$. However, U should face the Co-BDH problem to compute $e(P, Q_i)^{rs}$, given $((U_1 = rP, P_{\mathrm{pub}} = sP, Q_i = H_1(ID_i))$ if he does not have the secret key sQ_i.

For an adversary ID_i who is a legitimate receiver, he is more powerful than a non-legitimate entity since he can compute the secret key σ and $H_2(e(P, Q_j)^{rs})$ from $R_i = \sigma \oplus H_2(e(P, Q_j)^{rs})$ for any legitimate ID_j. However, the value $H_2(e(P, Q_j)^{rs})$ is random that ID_i cannot tell it from a random value.

This proves the anonymity protection of the proposed scheme. □

5. PERFORMANCE EVALUATION

In this section, we compare the performance of our scheme with Fan *et al.*'s scheme in terms of computation and communication. To assess communication performance, we consider cipher-text message length, and define the following notation. Let L_{Q} denote the length of one elliptic curve point, L_{H} denotes that of one hash value and L_{Enc} denotes that of one symmetric encryption of the message. Then the cipher-texts of both Fan *et al.*'s scheme and our scheme consume $(t+2)L_{\mathrm{Q}} + L_{\mathrm{H}} + L_{\mathrm{Enc}}$, where t denotes the number of the designated receivers. The two schemes share the same communication performance.

To evaluate the computation, we define the following notations. Let C_{H} denote the computation cost of one hashing operation, C_{M} for one modular multiplication, C_{E} for one modular exponentiation, C_{P} for one pairing operation, C_{Enc} for one symmetric encryption of one message or one decryption of

an encrypted message, C_{SM} for one scalar point multiplication of elliptic curves and t denotes the number of receivers. The setup phases of the two schemes are the same and they are executed only once—they share the same performance. The extract phase is executed only once for each entity in the two schemes, but our scheme demands one less point addition than Fan et al.'s scheme for each extract operation.

The multi-receiver encryption generation in Fan *et al.*'s scheme demands $(2t + 3)C_H + (2t^2 - t + 1)C_M + (t^2 - t + 1)C_E + C_P + C_{Enc} + (t + 2)C_{SM}$ computations, and the cipher-text decryption in Fan et al.'s scheme demands $3C_H + (t-1)C_M + C_E + 2C_P + C_{Enc} + tC_{SM}$. The multi-receiver encryption preparation in our scheme demands $tC_H + tC_E + t \quad C_P + C_{Enc} + 1C_{SM}$. To test whether one is an authorized receiver in our scheme, each potential receiver should derive $\sigma'_j = R_j \oplus H_2(e(U_1, d_j))$ and test whether $U_2 \stackrel{?}{=} H(\sigma'_j)$ holds, and each receiver, on average, tries $t/2$ such operations to find a match. Therefore, each receiver takes $t/2C_P + (t + 1)C_H + C_{Enc}$ computations on average. Performance comparisons are summarized in Table 1. From Table 1, we can see that our scheme outperforms Fan *et al.*'s scheme in terms of security, the two schemes share the same communication performance, but it is difficult to compare the computational performance of the two schemes without substituting the notation with practical values. To further quantitatively assess the two schemes' computational performance, we first simplify the cost formulas and then evaluate the formulas using timing results from well-known implementations [20, 21] in the following.

In Table 1, the most dominating operations are C_M, C_E, C_P and C_{SM}, and the C_{Enc}s in the two schemes are the same. Therefore, we can simplify the encryption preparation cost of Fan et al.'s scheme as $(2t^2 - t + 1)C_M + (t^2 - t + 1)C_E + C_P + (t + 2)C_{SM}$ and simplify the encryption preparation cost of our scheme as $tC_E + tC_P + 1C_{SM}$. The cipher-text decryption cost of Fan *et al.*'s scheme is simplified as $(t-1)C_M + C_E + 2C_P + tC_{SM}$, and the cost of our decryption is simplified as $t/2C_P$.

Basically, the computational complexity of a pairing computation is linear with the length of the order of the underlying groups in terms of the number of multiplications in the underlying fields, where the complexity of multiplication is linear with the bit length of the underling field and the extension degree. Further, the computational complexity of scalar point multiplication $Q = kP$ in elliptic curves is roughly equal to $|q|^*$ the cost of point doubling $+w(k)^*$ the cost of point addition, where q is the order of the curves, $|q|$ is the bit length of the order and $w(k)$ is the weight of k.

In the following, we compare the two schemes using the timing results from Stobauer's implementation, an implementation of an arithmetic of a supersingular curve with group order 160 bits and an extension field of 1028 bits, on a Pentium M 1400 MHz processor and 512 MB RAM using Windows XP and JDK 1.4.1 [21, page 52]. The multiplication and the exponentiation in the extended field, respectively, take 0.163 and 195.08 ms, the point addition and the point doubling, respectively, take 0.661 and 0.59 ms, the scalar point multiplication takes 454.89 ms and the Tate pairing takes 624 ms. Based on these timing results, we estimate the computational cost of the two schemes in Table 2. In the first row, we list the number of authorized receivers, the second row lists the estimated timing cost of Fan *et al.*'s encryption, the third row lists the timing cost of our scheme, and the fourth row and the fifth row, respectively, list the timing cost of decryption in Fan *et al.*'s scheme and in our scheme.

For example, when the number of receivers is two, then the encryption preparations in Fan *et al.*'s scheme takes 1213 ms while our scheme takes 2093 ms; but it takes 337 354 ms in Fan *et al.*'s scheme while our scheme takes only 34 856 ms when the number of receivers is 42. The timing cost of encryptions of the two schemes is depicted in Fig. 2. From the figure, we can see that the timing cost of Fan *et al.*'s scheme grows much faster than our scheme because the cost of Fan *et al.*'s scheme is linear with $(2t^2 - t + 1)C_M + (t^2 - t + 1)C_E$.

TABLE 1. Performance comparisons of two anonymous multi-receiver schemes.

	Fan *et al.*'s scheme	Ours	Comparison
Receiver anonymity protection	No	Yes	Our scheme outperforms Fan *et al.*'s in terms of security
Multi-receiver encryption preparation	$(2t+3)C_H + (2t^2-t+1)C_M + (t^2-t+1)C_E + C_P + C_{Enc} + (t+2)C_{SM}$	$tC_H + tC_E + tC_P + C_{Enc} + 1C_{SM}$	Our scheme outperforms Fan *et al.*'s in terms of encryption computations[a]
Cipher-text decryption	$3C_H + (t-1)C_M + C_E + 2C_P + C_{Enc} + tC_{SM}$	$t/2C_P + (t+1)C_H + C_{Enc}$	Our scheme outperforms Fan *et al.*'s in terms of decryption computations[a]
Length of multi-receiver encryption	$(t+2)L_Q + L_H + L_{Enc}$	$(t+2)L_Q + L_H + L_{Enc}$	Our scheme and Fan *et al.*'s share the same communication performance

[a]We assess the computation performance of these two schemes using a practical parameter setting in Table 2.

TABLE 2. Estimated timing results of the two schemes in terms of the number of receivers.

The number of authorized receives	2	7	12	17	22	27	32	37	42
Encryption preparation in Fan *et al.*'s scheme (ms)	1213	9035	26 626	53 989	91 121	138 024	194 697	261 141	337 354
Encryption preparation in our scheme (ms)	2093	6188	10 283	14 379	18 474	22 570	26 665	30 760	34 856
Cipher-text decryption in Fan *et al.*'s scheme (ms)	2353	4628	6903	9178	11 454	13 729	16 004	18 279	20 555
Cipher-text decryption in our scheme (ms)	624	2184	3744	5304	6864	8424	9984	11 544	13 104

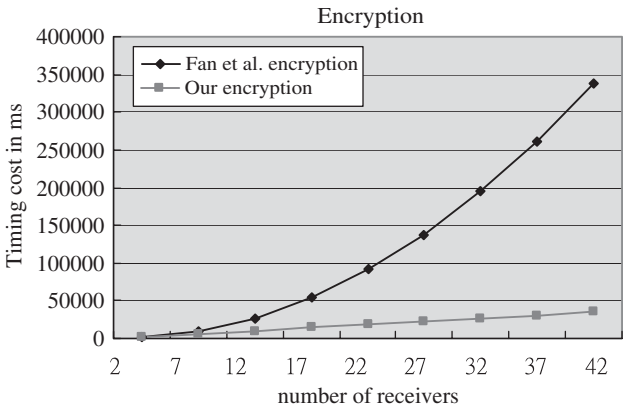

FIGURE 2. Encryption timing costs of the two schemes.

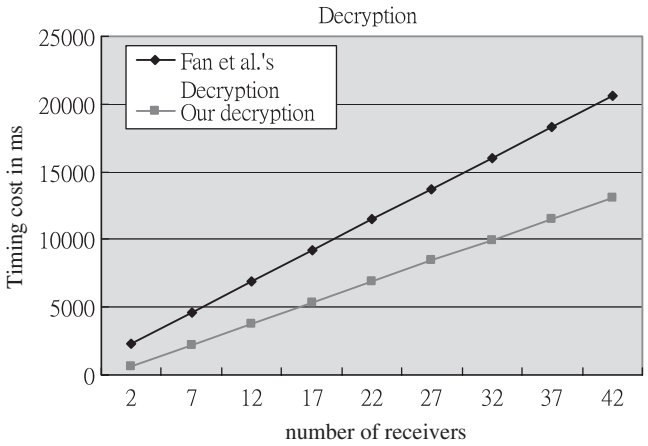

FIGURE 3. Decryption timing costs of the two schemes.

Now we compare the timing cost of decryptions of the two schemes in terms of the number of receivers. When the number of receivers is two, Fan *et al.*'s decryption takes 2353 ms and our scheme takes 624 ms. When the number of receivers is 42, Fan *et al.*'s decryption takes 20 555 ms but our scheme takes only 13 104 ms. Figure 3 depicts the timing cost of the decryptions of the two schemes. From the figure, we can see that the costs of decryptions of the two schemes are linear with the number of receivers, but Fan *et al.*'s scheme grows faster than ours. This occurs because Fan *et al.*'s decryption is linear with $(t-1)C_{\mathrm{M}} + tC_{\mathrm{SM}}$ while ours is linear with $t/2C_{\mathrm{P}}$. We can see that our scheme out-performs Fan et al.'s scheme, especially as the number of receivers increases. Considering the two potential applications, we described- PayTV and twitter revolution, and the number of potential receivers depends on each application scenario. The number of potential receivers for each pay-TV broadcasting ranges from only 3–5 receivers up to maybe several thousand receivers (or even more), depending on the popularity of the broadcast program. The number of receivers in one twitter revolution broadcasting would be smaller, and is usually limited by one person's social relation. For most of the applications, the number of receivers would be larger than five, and our scheme outperforms, in such circumstances, Fan *et al.*'s scheme in terms of computational complexity.

6. CONCLUSIONS

In this paper, we have shown that although Fan *et al.*'s scheme aimed to protect receiver anonymity, it failed to fully meet this aim, and the security notation for anonymity captures only the semantic of a single-receiver case. In Fan *et al.*'s scheme, an authorized receiver can easily verify whether a specific user is also one of the authorized receivers using two pairing operations, and a non-authorized entity can identify all the receivers using only $O(n^2)$ pairings. To improve the scheme, we have proposed a new scheme that improves receiver anonymity protection and also out-performs Fan *et al.*'s scheme in terms of computational performance.

FUNDING

This work is partially supported by the Taiwan National Science Council with project number NSC99-2218-E-260-002.

REFERENCES

[1] Du, X., Wang, Y., Ge, J. and Wang, Y. (2005) An Id-based broadcast encryption scheme for key distribution. *IEEE Trans. Broadcast.*, **51**, 264–266.

[2] Chien, H.Y. (2007) Comments on an efficient ID-based broadcast encryption scheme. *IEEE Trans. Broadcast.*, **53**, 809–810.

[3] Lee, J.W., Hwang, Y.H. and Lee, P.J. (2006) Efficient Pubic Key Broadcast Encryption Using Identifier of Receivers. *ISPEC 2006*, Hangzhou, China. Lecture Notes in Computer Science 3903, pp. 153–164. Springer.

[4] Yang, C., Cheng, X., Ma, W. and Wang, X. (2006) A New Id-Based Broadcast Encryption Scheme. *Autonomic and Trusted Computing 2006*, Wuhan, China. Lecture Notes in Computer Science 4158, pp. 487–492. Springer.

[5] Wang, L. and Wu, C.-K. (2005) Efficient identity-based multicast scheme from bilinear pairing. *IEE Proc. Commun.*, **152**, 877–882.

[6] Baek, J., Safavi-Naini, R. and Susilo, W. (2005) Efficient Multi-Receiver Identity-Based Encryption and Its Application to Broadcast Encryption. *PKC 2005*, Switzerland. Lecture Notes in Computer Science 3386, pp. 380–397.

[7] Lu, L. and Hu, L. (2006) Pairing-Based Multi-Recipient Public Key Encryption. *Proc. 2006 Int. Conf. Security & Management*, Las Vegas, Nevada, USA. pp. 159–165.

[8] Chatterjee, S. and Sarkar, P. (2006) Multi-Receiver Identity-Based Key Encapsulation with Shortened Ciphertext. *INDOCRYPT 2006*, Kolkata, India. Lecture Notes in Computer Science 4329, pp. 394–408. Springer.

[9] Fan, D., Huang, L.Y. and Ho, P.H. (2010) Anonymous multi-receiver identity-based encryption. *IEEE Trans. Comput.*, 2010, http://doi.ieeecomputersociety.org/10.1109/TC.2010.23.

[10] Eltahawy, Mona. *Tunisia's Jasmine Revolution*. Washington Post. 2011-01-15 [2011-01-15]. http://www.washingtonpost.com/wp-dyn/content/article/2011/01/14/AR2011011405084.html (accessed April 18, 2011).

[11] Shamir, A. (1984) Identity Based on Cryptosystems and Signature Schemes. *Crypto'84*, Barbara, California, USA. Lecture Notes in Computer Science 196, pp. 47–53. Springer.

[12] Boneh, D. and Franklin, M. (2003) Identity-based encryption from the weil pairing. *SIAM J. Comput.*, **32**, 586–615.

[13] Gentry, C. (2006) Practical Identity-Based Encryption Without Random Oracles. *Advances in Cryptology -EUROCRYPT 2006*, Saint Petersburg, Russia. Lecture Notes in Computer Science 4004, pp. 445–464.

[14] Lal, S. and Kushwah P. (2009) Anonymous ID Based Signcryption Scheme for Multiple Receivers. Cryptology ePrint Archive, Report 209/345.pdf.

[15] Zhang, B. and Xu, Q. (2010) An ID-based anonymous signcryption scheme for multiple receivers. *Int. J. Adv. Sci. Technol.*, **20**, 9–24.

[16] Wang, X., Wang, A.-L. and Wang L.Y. (2009) Efficient ID-based secure encryption scheme for anonymous receivers. *J. Netw.*, **4**, 641–648.

[17] Xu, X.-Y. (2009) Efficient Privacy of Message Encryption Algorithm for Anonymous Receivers in E-commerce. *Proc. 2nd Int. Conf. Biomedical Engineering and Informatics 2009*, Tianjin, China. pp. 1–4.

[18] Yuen, T.H. and Wei, V.K. (2005) Fast and Proven Secure Blind Identity-Based Signcryption from Pairings. *CT-RSA 2005*, San Francisco, CA, USA. Lecture Notes in Computer Science 3376, pp. 305–322.

[19] Chien, H.-Y. (2008) Selectively convertible authenticated encryption in the random oracle model. *Comput. J.*, **51**, 419–434.

[20] Barreto, P.S.L.M., Galbraith, S., O'hEigeartaigh, C. and Scott, M. (2007) Efficient pairing computation on supersingular abelian varieties. *Des. Codes Cryptogr.*, **42**, 239–271; Cryptology ePrint Archive: Report 2004/375.

[21] Stobauer, M. (2004) Efficient algorithms for pairing based cryptosystems. Diploma Thesis, Darmstad University of Technology.