Comment on Anonymous Multi-receiver Identity-based Encryption Scheme

Jianhong Zhang
College of Sciences
North China University of Technology
Beijing, 100144, China
Email: jhzhang@ncut.edu.cn

Yuwei Xu
College of Sciences
North China University of Technology
Beijing, 100144, China
Email: cuiyb@163.com

***Abstract*—Anonymous receiver encryption is an important cryptographic primitive. It can protect the privacy of the receiver. In 2010, Fan *et al* proposed an anonymous multi-receiver ID-based encryption by using Lagrange interpolating polynomial. However, Wang *et al* showed that Fan *et al*'s scheme didn't satisfy the anonymity of the receivers. Then they provided an improved scheme to fix it and showed that the improved scheme was secure. Unfortunately, in this paper, we pointed out that Wang *et al*'s improved scheme did not satisfy the receiver's anonymity by analyzing the security of the scheme yet. After analyzing the reason to produce such flaws, we gave an improved method to repair it and showed that our improved scheme could satisfy the receiver's anonymity. And the improved scheme has the advantage over Wang *et al*'s scheme in terms of computational cost.**

Keywords: Anonymity, multi-receiver ID-based encryption, attack, the improved method

I. Introduction

With the development of information techniques, Group-oriented communication is more and more important in real life, such as network conference and broadcast communication. In cloud computing environment, in order to prevent important data corruption, a client may transmit these data to a set of authorized clouds for backup. And the client may only hope that those authorized clouds are allowed to access the data. To realize such functions, we can adopt broadcast encryption scheme such as those in [3], [4] or a multi-receiver encryption scheme such as those in [6], [**?**], [7] to achieve it. However, for privacy-preserving, a receiver does not want to its identity to be known by the other authorized receivers in many scenarios in that it may concern the sensitive information of the receiver. For example, in the ordering sensitive Pay-TV programmes, a receiver or customer doesn't usually hope that the other customers know her/his identity information and TV-program types. Thus,it is very necessary to have identity information of the receiver anonymous to protect personal privacy interest.

In 2010, Fan *et al* proposed a secure and efficient anonymous multi-receiver IBE scheme [2] by combining Lagrange interpolating polynomial theorem and ID-based encryption. And they claimed that their scheme could protect the receiver's anonymity. Recently, Wang *et al* showed that Fan *et al*'s scheme was insecure and can not achieve the receiver's anonymity in [1]. Then they proposed an improved scheme to fix this weakness. Unfortunately, by analyzing Wang *et al*'s scheme, we found that Wang *et al*'s improved scheme was also insecure and not able to achieve the receiver's anonymity yet. Namely, an authorized receiver can easily verify whether a specific receiver belongs to the authorized receiver. After analyzing the reason to produce such attack, an improved method is proposed to repair it.

II. Preliminaries

In this section, we will fist review some fundamental backgrounds related to the paper.

Let G_1 be a cyclic additive group generated by P with the order prime q, and G_2 be a cyclic multiplicative group with the same order q. Let $e: G_1 \times G_1 \longrightarrow G_2$ be a pairing which satisfies the following conditions [10]:

- Bilinearity: For any $P, Q, R \in G_1$, we have $e(P+Q, R) = e(P, R)e(Q, R)$ and $e(P, R+Q) = e(P, R)e(P, Q)$. In particular, for any $a, b \in Z_q$,
$$e(aP, bP) = e(P, P)^{ab} = e(P, abP) = e(abP, P)$$
- Non-degeneracy: There exists $P, Q \in G_1$, such that $e(P, Q) \neq 1$
- Computability: There is an efficient algorithm to compute $e(P, Q)$ for $P, Q \in G_1$.

The typical way of obtaining such pairing is by deriving them from the Weil pairing or the Tate pairing on an elliptic curve over a finite field.

Computational Diffie-Hellman Problem: Given $P, aP, bP \in G_1$ for randomly chosen $a, b \in_R Z_q$ to abP.

The success probability of any probabilistic polynomial-time algorithm $\mathcal{A}$ in solving CDH problem in G_1 is defined to be

$$Succ_{\mathcal{A}}^{CDH} = Pr[\mathcal{A}(P, aP, bP) = abP | a, b \in {Z_q}^*]$$

The CDH assumption states that for every probabilistic polynomial-time algorithm $\mathcal{A}$, $Succ_{\mathcal{A}}^{CDH}$ is negligible.

Bilinear Diffie-Hellman Problem: Given $P, aP, bP, cP \in \mathbb{G}_1$ for randomly chosen $a, b, c \in_R Z_q$ to $e(P, P)^{abc}$.

The success probability of any probabilistic polynomial-time algorithm $\mathcal{A}$ in solving BDH problem in $\mathbb{G}_1$ is defined to be

978-0-7695-4808-1/12 $26.00 © 2012 IEEE
DOI 10.1109/iNCoS.2012.117

$Succ_{\mathcal{A}}^{BDH} =$
$Pr[\mathcal{A}(P, aP, bP, cP) = e(P,P)^{abc} | a, b, c \in Z_q{}^*]$

The BDH assumption states that for every probabilistic polynomial-time algorithm $\mathcal{A}, Succ_{\mathcal{A}}^{BDH}$ is negligible.

Co-decision Bilinear Diffie-Hellman Problem[?]: Given (P, aP, bP, Q, Z) for randomly chosen $a, b \in_R Z_q, Q \in \mathbb{G}_1, Z \in \mathbb{G}_2$, it goal is to determine whether $e(P,Q)^{ab} = Z$.

III. Reviews of Wang *et al*'s Anonymous Multi-receiver ID-based Encryption Scheme

In the following, we review Wang *et al*'s anonymous mutlti-receiver ID-based encryption scheme[1]. The scheme consists of four algorithms. Please the interested readers refer to [1] for detail. In the following, we only review this scheme.

A. Setup

Let $\mathbb{G}_1$ be an additive cyclic group and $\mathbb{G}_2$ be a multiplicative cyclic group, the order of their two groups is the same prime order q. Let P be a randomly chosen generator of $\mathbb{G}_1$ and $e : \mathbb{G}_1 \times \mathbb{G}_1 \to \mathbb{G}_2$ be a bilinear mapping.

PKG randomly chooses an integer $s \in Z_q$ and an random element $P_1 \in \mathbb{G}_1$. Then it sets $P_{pub} = sP$. Choose five cryptographic one-way hash functions $H : \{0,1\}^* \to Z_q^*, H_1\{0,1\}^* \to \mathbb{G}_1^*$, $H_2 : \mathbb{G}_2 \to \{0,1\}^w$, $H_3 : \{0,1\}^w \times \{0,1\}^* \to Z_q$ and $H_4 : \{0,1\}^w \to \{0,1\}^w$ where w is a security factor. The symmetric encryption and decryption functions with a secret key k are represented by E_k and D_k, respectively.

$$Params = \{q, \mathbb{G}_1, \mathbb{G}_2, e, P, P_1, H, H_1, H_2, H_3, H_4, n\}$$

be published and the master private key s is secretly kept.

B. Key Extract

Input system $Params$ and an identity $ID_i \in \{0,1\}^*$, the PKG computes as follows:

1) compute $Q_i = H_1(ID_i)$;
2) then set $d_i = s(P_1 + Q_i)$ as the private key of the user ID_i.

C. Encrypting Algorithm

Take into input system $Param$, a encrypted message M and the selected receiver's identities set $\{ID_1, \cdots, ID_t\}$, the algorithm is executed as follows:

1) Pick a random string $\delta \in \{0,1\}^w$ to compute $r = H_3(\delta, M)$.
2) Then, for $i = 1, 2, \cdots, t$, randomly choose $\alpha_i \in Z_q$ to compute $y_i = \alpha_i^{-1} r \mod q$.
3) And for $i = 1, 2, \cdots, t$, compute $x_i = H(ID_i)$ and $Q_i = H_1(ID_i)$.
4) For $i = 1, 2, \cdots, t$, compute
$$f_i(x) = \prod_{1 \le j \le t, j \ne i} \frac{x - x_j}{x_i - x_j} = a_{i1} + a_{i2}x + \cdots + a_{it}x^{t-1}$$
where coefficient $a_ij \in Z_q$.
5) For $i = 1, 2, \cdots, t$, it computes
$$\begin{aligned} R_i &= \prod_{j=1}^{t} a_{ji} y_j Q_j = \prod_{j=1}^{t} b_{ji} Q_j \\ K_{i'} &= \prod_{j=1}^{t} a_{ji} K_j \\ K_i &= \alpha_i P_{pub} \end{aligned}$$
where $b_{ji} = a_{ji} y_j \in Z_q$.
6) Finally, compute $V = \delta \oplus H_2(e(P_{pub}, P_1)^r), W = E_{H_4(\delta)}(M)$. The resultant ciphertext $C = (R_1, \cdots, R_t, U = rP, K_{1'}, \cdots, K_{t'}, V, W)$.

D. Decrypt phase:

Given a cipertext $C = (R_1, \cdots, R_t, U = rP, K_{1'}, \cdots, K_{t'}, V, W)$, a receiver with identity ID_i can make use of his private key d_i to do the following steps:

1) Compute $x_i = H(ID_i)$.
2) Then compute $\lambda_i = R_1 + x_i R_2 + \cdots + x_i^{t-1} R_t$ and $v_i = K_{1'} + x_i K_{2'} + \cdots + x_i^{t-1} K_{t'}$
3) compute $\delta' = V \oplus H_2(e(U, d_i)/e(v_i, \lambda_i))$
4) compute $M' = D_{H_4(\delta')}(W)$.
5) Finally, compute $r' = H_3(\delta', M)$ and test whether $U = r'P$ or not. If it holds, then the decrypted plaintext is message M.

IV. Anonymity Attack on Wang et al's Scheme

In [1], Wang *et al* gave an improved anonymous multi-receiver encryption scheme by repairing Fan et al's scheme [2]. And they claimed that their anonymous multi-receiver encryption scheme has overcome the drawbacks of which Fan *et al.*'s scheme was not anonymous to any other receiver. Unfortunately, we will show that their improved scheme cannot provide anonymity of the receivers yet. This is to say, a receiver in the designated set can know the identities of the other receivers. In the following, we give the detail attack.

1) Given a ciphertext $C = (R_1, \cdots, R_t, U = rP, K_{1'}, \cdots, K_{t'}, V, W)$;
2) Let i denote an index of the designated receiver set.
3) Upon receiving the ciphertext C, the receiver with the identity ID_i sets two functions $\lambda(x) = \sum_{i=1}^{t} x^{i-1} R_i$ and $v(x) = \sum_{i=1}^{t} x^{i-1} K_i'$ by $(R_1, \cdots, R_t, K_{1'}, \cdots, K_{t'})$ in the ciphertext C. Then it computes λ_i, v_i .

$$\begin{aligned} \lambda_i &= \lambda(x_i) \\ &= \sum_{i=1}^{t} x_i^{i-1} R_i = R_1 + x_i R_2 + \cdots + x_i^{t-1} R_t \\ &= (a_{11} + a_{12}x_i + \cdots + a_{1t}x_i^{t-1}) y_1 Q_1 + \cdots + \\ &\quad (a_{i1} + a_{i2}x_i + \cdots + a_{it}x_i^{t-1}) y_i Q_i + \cdots + \\ &\quad (a_{t1} + a_{t2}x_i + \cdots + a_{tt}x_i^{t-1}) y_t Q_t \\ &= y_i Q_i \end{aligned}$$

$$
\begin{aligned}
v_i &= v(x_i) \\
&= \sum_{i=1}^{t} x_i^{i-1} K_i' = K_1' + x_i K_2' + \cdots + x_i^{t-1} K_t' \\
&= (a_{11} + a_{12}x_i + \cdots + a_{1t}x_i^{t-1})K_1 + \cdots + \\
&\quad (a_{i1} + a_{i2}x_i + \cdots + a_{it}x_i^{t-1})K_i + \cdots + \\
&\quad (a_{t1} + a_{t2}x_i + \cdots + a_{tt}x_i^{t-1})K_t \\
&= K_i = \alpha_i P_{pub}
\end{aligned}
$$

where $x_i = H(ID_i)$ and $Q_i = H_1(ID_i)$

4) According to the above computation, we can obtain

$$
\begin{aligned}
T &= e(\lambda_i, v_i) = e(y_i Q_i, K_i) \\
&= e(\alpha_i^{-1} r Q_i, \alpha_i P_{pub}) \\
&= e(rQ_i, P_{pub}) \\
&= e(Q_i, P_{pub})^r
\end{aligned}
$$

Note: for a ciphertext C, Q_i, P_{pub}, r are fixed.

5) For the receiver with identity ID_i, it can obtain $r = H_3(\delta, M)$ from decryption process.
6) To reveal the identities of the other receivers, the receiver with identity ID_i compute as follows by the formation the above T and r:

For $l = 1$ to n and $l \neq i$

{

$x_l = H(ID_l), Q_l = H_1(ID_l)$;

$\lambda_l = \lambda(x_l), v_l = v(x_l)$;

If $e(\lambda_l, v_l) = e(Q_l, P_{pub})^r$

then

output the identity ID_l

}

The corresponding ID_l is the identity of the designated receiver set.

According to the above step 6, we know that any receiver can determine whether the other is one of the designated multi-receivers. It means that Wang *et al.*'s improved anonymous multi-receiver encryption scheme cannot satisfy the anonymity yet.

The reason to such attack is that given a ciphertext C, $r = H_3(M, \delta)$ can be recovered by plaintext M and the symmetrical key δ which encrypts the plaintext. To overcome such attack, we only makes that any designated receiver cannot recover r.

V. An Improved Scheme

The main idea in the improved scheme is to make that r cannot be recovered in the decryption phase. The notations in the improved scheme are the same to these of Wang *et al.*'s scheme. We focus on the improvement of encryption algorithm and decryption algorithm. The other algorithms are the same to these of Wang *et al*'s scheme except a hash function $H_5 : \{0,1\}^* \to \{0,1\}^z, z < w$ in Setup phase.

A. Encrypting Algorithm

Input system $Param$, a encrypted message M and the designated receiver's identities set $\{ID_1, \cdots, ID_t\}$, the algorithm is executed as follows:

1) Pick a random number $r \in Z_q^*$ to compute $U = rP$.
2) Then, for $i = 1, 2, \cdots, t$, randomly choose $\alpha_i \in Z_q$ to compute $y_i = \alpha_i^{-1} r \mod q$.
3) And for $i = 1, 2, \cdots, t$, compute $x_i = H(ID_i)$ and $Q_i = H_1(ID_i)$.
4) For $i = 1, 2, \cdots, t$, compute

$$f_i(x) = \prod_{1 \le j \le t, j \neq i} \frac{x - x_j}{x_i - x_j} = a_{i1} + a_{i2}x + \cdots + a_{it}x^{t-1}$$

where coefficient $a_{ij} \in Z_q$.

5) For $i = 1, 2, \cdots, t$, it computes

$$
\begin{aligned}
R_i &= \prod_{j=1}^{t} a_{ji} y_j Q_j = \prod_{j=1}^{t} b_{ji} Q_j \\
K_i &= \alpha_i P_{pub}
\end{aligned}
$$

where $b_{ji} = a_{ji} y_j \in Z_q$.

6) Finally, randomly choose $\delta \in \{0,1\}^{w-z}$ to compute

$$
\begin{aligned}
V &= \delta || H_5(M||K_1|| \cdots ||K_t) \oplus H_2(e(P_{pub}, P_1)^{rh}) \\
W &= E_{H_4(\delta)}(M)
\end{aligned}
$$

Where $h = H_5(R_1|| \cdots ||R_t)$

The resultant ciphertext is $C = (R_1, \cdots, R_t, U = rP, K_1, \cdots, K_t, V, W)$.

B. Decrypt phase:

Given a ciphertext $C = (R_1, \cdots, R_t, U = rP, K_1, \cdots, K_t, V, W)$, a receiver with identity ID_i can make use of his private key d_i to do the following steps:

1) Compute $x_i = H(ID_i)$.
2) Then compute

$$\lambda_i = R_1 + x_i R_2 + \cdots + x_i^{t-1} R_t$$

3) compute $\delta || H_5(M||K_1|| \cdots ||K_t) = V \oplus H_2((e(U, d_i)/e(K_i, \lambda_i))^h)$, where $h = H_5(R_1|| \cdots ||R_t)$.
4) then parse $\delta || H_5(M||K_1|| \cdots ||K_t)$ to extract δ and $h_5 = H_5(M||K_1|| \cdots ||K_t)$.
5) compute $M' = D_{H_4(\delta)}(W)$.
6) Finally, test whether $h_5 = H_5(M'||K_1|| \cdots ||K_t)$ or not. If it holds, then the decrypted plaintext is message M.

In the following, we show that the improved scheme is correct. This is to say, if a receiver belongs to the designated receiver set, then it must decrypt the ciphertext to the corresponding message.

Since for any receiver with the identity ID_i, $1 \le i \le t$, it can compute $x_i = H(ID_i)$ and input it into the function $\lambda(x)$.

$$
\begin{aligned}
\lambda_i &= \lambda(x_i) = \sum_{i=1}^{t} x_i^{i-1} R_i = R_1 + x_i R_2 + \cdots + x_i^{t-1} R_t \\
&= (a_{11} + a_{12}x_i + \cdots + a_{1t}x_i^{t-1}) y_1 Q_1 + \cdots + \\
&\quad (a_{i1} + a_{i2}x_i + \cdots + a_{it}x_i^{t-1}) y_i Q_i + \cdots + \\
&\quad (a_{t1} + a_{t2}x_i + \cdots + a_{tt}x_i^{t-1}) y_t Q_t \\
&= y_i Q_i
\end{aligned}
$$

Then, we have

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

Thus, we can obtain

$$\begin{aligned}&\textbf{step}1: \delta||H_5(M||K_1||\cdots||K_t) = \\ &\qquad V \oplus H_2((\frac{e(U,d_i)}{e(K_i,\lambda_i)})^h) \\ &\textbf{step}2: parse\,\delta||H_5(M||K_1||\cdots||K_t)\,to\ obtain\ \delta \\ &\textbf{step}3: M = D_{H_4(\delta)}(W) = M\end{aligned}$$

It means that our improved scheme satisfies correctness.

In our improved scheme, random number r cannot be recovered by the designated receiver. And r appears in the rP formation. Given rP, P_{pub}, Q_i, anyone cannot obtain $e(P_{pub},Q_i)^r$, because the hardness of solving $e(P_{pub},Q_i)^r$ is equivalent to solve the bilinear Diffie-Hellman problem.

For the confidentiality of improved scheme, we don't discuss here. The security proof is similar to one in Wang *et al.*'s scheme. Please the interested reader refer to [1] for the detail.

Theorem 1. The improved scheme satisfies the receiver anonymity if the BDH problem is hard.

Proof. To prove the receiver anonymity, we divide the adversaries into two classes. The one is the non-authorized receiver, the other is the authorized receiver. For the authorized receiver's attack, it is the more powerful than the non-authorized receiver's attack. If the non-authorized receiver's attack is successful, then the authorized receiver's attack is also successful. Thus, we only consider the authorized receiver's attack.

Given a ciphertext $C = (R_1,\cdots,R_t,U = rP,K_1,\cdots,K_t,V,W)$, without loss of generality, we assume that the authorized receiver with identity ID_i is the adversary, the attacked specific receiver's identity is ID_j. Then it can obtain K_j, y_jQ_j, $e(P_{pub},Q_i)^r$ and $e(P_{pub},P_1)^r$ for the adversary. According the above decrypting algorithm, to distinguish the specific receiver with identity ID_j, it must determine whether $T = e(P_{pub},Q_j)^r \stackrel{?}{=} e(K_j, y_jQ_j)$. However, given $(U = rP, P_{pub}, Q_j, T)$, it is equivalent to the hardness of solving the Co-decision Bilinear Diffie-Hellman problem to distinguish $e(P_{pub},Q_j)^r = e(K_j,y_jQ_j)$.

Thus, the improved scheme achieves the anonymity protection of the receivers.

In the following, we briefly analyze the efficiency of our scheme. In terms of communication overhead, to achieve a standard security level of 2^{80}, we let p be a 512-bit long prime number. and Thus, in Wang *et al*'s scheme, the length of each ciphertext is $1024t + w + |E|$ bits. and the length of each ciphertext in our improved scheme is also $1024t + w + |E|$ bits, where $|E|$ denotes the length of symmetrical encryption algorithm E. In terms of the computational cost, the computation to produce a ciphertext in Wang *et al*'s scheme is $(3t+1)M + 1P_e$, however, the computation to produce a ciphertext in the improved scheme is $(2t_1)M + 1P_e$, where M denotes the scale multiplication of point in group $\mathbb{G}_1$, P_e is a pairing operation and t is the member number of the receivers set. According to the above analysis, the improved scheme has the advantage over Wang *et al*'s scheme in terms of computational cost.

VI. Conclusion

Anonymous multi-receiver encryption is a way to protect the privacy of the receivers. Recently, Wang *et al* gave an improved anonymous multi-receiver encryption scheme to achieve privacy-preserving of the receivers. However, we show that Wang *et al.*'s improved anonymous multi-receiver encryption scheme is insecure in this paper. It fails to achieve the receiver's anonymity. An authorized receiver can easily verify whether a specific user belongs to the authorized receivers. Then we give the corresponding attack and analyze the reason to produce such attack. To overcome this weakness, we have proposed an improved scheme which can repair the receiver anonymity protection .

Acknowledgment

This work is supported by Beijing Natural Science Foundation (No:4122024), and the Nova Programma (No:2007B-001) and Beijing Natural Science Foundation Programm and Scientific Research Key Program of Beijing Municipal Commission of Education (NO:KZ2008 10009005).

References

[1] H.Wang,Y.Zhang, H.Xiong, B. Qin,Cryptanalysis and improvements of an anonymous multi-receiver identity-based encryption scheme,IET Information. Security., 2012, Vol. 6, Iss. 1, pp. 20-27

[2] Fan, D., Huang, L., Ho, P.: Anonymous multireceiver identity-based encryption, IEEE Trans. Comput., 2010, vol.59(9), pp.1239-1249

[3] Du, X., Wang, Y., Ge, J. and Wang, Y. An Id-based broadcast encryption scheme for key distribution. IEEE Trans. Broadcast., vol.51, pp.264-266, 2005.

[4] Chien, H.Y. Comments on an efficient ID-based broadcast encryption scheme. IEEE Trans. Broadcast., vol.53, pp.809-810,2007.

[5] Rong Weijian, Certificateless Partially Blind Signature Scheme, Journal of Zhangzhou Normal university, vol.4(2), pp 44-47, 2008.

[6] Baek, J., Safavi-Naini, R. and Susilo, W. Efficient Multi-Receiver Identity-Based Encryption and Its Application to Broadcast Encryption. PKC 2005, LNCS 3386, pp. 380-397, 2005.

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

[8] M.Mambo, K.Usuda and E.Okamot. Proxy signature: delegation of the power to sign messages. IEICE Trans. Fundamentals, Vol. E79-A, NO.9, pp 1338-1353, 1996.

[9] Shamir,A., Identity Based on Cryptosystems and Signature Schemes. Crypto'84, LNCS 196, pp.47-53, 1984.

[10] Boneh, D. and Franklin, M., Identity-based encryption from the weil pairing. SIAM J. Comput., vol.32, pp.586-615, 2003.

[11] Z. Tan, Z. Liu, and C. Tang. Digital proxy blind signature schemes based on DLP and ECDLP. MM Research Preprints, MMRC, AMSS, Academia Sinica, Beijing, December 21, 2002, 212-217

[12] David Chaum, Blind signatures for untraceable payments, Advances in Cryptology - Crypto '82, Springer-Verlag (1983),