Comments on FHH Anonymous Multireceiver Encryption

Zhenhua Chen[1], Shundong Li[1], Chunzhi Wang[2], and Mingwu Zhang[2]

(Corresponding author: Zhenhua Chen)

School of Computer Sciences, Shaanxi Normal University[1]

School of Computer Science and Engineering, Hubei University of Technology[2]

(Email: chenzhenhua@stu.snnu.edu.cn)

(Received Nov. 7, 2012; revised and accepted May 18, 2013)

Abstract

Recently, Fan et al. proposed an anonymous multireceiver encryption scheme (FHH) , and they declared that their scheme achieves confidentiality and anonymity. In this letter, We point out that the FHH scheme does not hold the defined security properties. In particular, we state that the FHH scheme does not hold the anonymity but achieves the weaker confidentiality of IND-CPA.

Keywords: Anonymity, confidentiality, lagrange interpolation, multireceiver encryption

1 Introduction

Anonymous multireceiver identity-based encryption, which holds the security of confidentiality and anonymity, has many practical applications such as pay-TV, secure email delivery and copyright distribution and so on. Since Boneh and Franklin [2] construct a practical identity-based encryption with bilinear pairing, several multireceiver identity-based encryptions were proposed [1, 3, 5, 8]. Recently, in order to protect identity privacy, Fan et al. [4] proposed an anonymous multireceiver identity-based encryption, which was derived from BF-IBE [2] and Shamir secret sharing [7]. They indicated that their scheme achieves the confidentiality of IND-CCA and anonymity of ANON-CCA. In this letter, we show that Fan et al.'s scheme [4] does not hold the security of their declared, and indicate that their scheme is only weaker IND-CPA secure but not hold the anonymity.

2 The Model and Security Definitions

The Fan et al.' scheme (FHH) contains four algorithms: $(Setup, Extract, Encrypt, Decrypt)$. Note that *Setup* and *Extract* algorithms are executed by Private Key Generator (PKG), *Encrypt* algorithm is preformed by a sender, and *Decrypt* is carried out by one of receivers.

Defintion 1. ***IND-CCA*** *An anonymous multireceiver identity-based encryption is indistinguishable against adaptive chosen-ciphertext attacks (IND-CCA) if the advantage of an attacker $\mathcal{A}$ is negligible in the following game*

1) *Setup: Runs $(par, s) \leftarrow Setup(1^\lambda)$ and sends par to $\mathcal{A}$.*

2) *Phase-1: $\mathcal{A}$ outputs a target multireceiver set $\mathcal{ID} = (ID_1, \ldots, ID_t)$.*

3) *Phase-2: $\mathcal{A}$ issues private key extraction queries. Upon receiving a private key extraction query of ID_j, the challenger $\mathcal{C}$ runs the private key extraction algorithm to get $d_j \leftarrow Extract(param, s, ID_j)$. The only constraint is that $ID_j \notin \mathcal{ID}$.*

4) *Phase-3: $\mathcal{A}$ issues decryption queries for target identities. Upon receiving a decryption query of (C, ID_i), $\mathcal{C}$ generates a private key d_i associated with ID_i and returns $D \leftarrow Decrypt(par, C, ID_i, d_i)$ to $\mathcal{A}$.*

5) *Challenge: $\mathcal{A}$ outputs a target message pair M_0, M_1. $\mathcal{C}$ randomly chooses $\beta \in \{0, 1\}$ and creates a ciphertext $C^* \leftarrow Encrypt(par, \mathcal{ID}, M_\beta)$ and returns C^* to $\mathcal{A}$.*

6) *Phase-4: $\mathcal{A}$ issues private key extraction queries as those in Phase-2 and decryption queries as those in Phase-3 with a restriction that $C^* \neq C$.*

7) *Output: $\mathcal{A}$ outputs β' and wins the game if $\beta' = \beta$.*

Defintion 2. ***ANON-CCA*** *A multireceiver identity-based encryption is anonymous if the attacker $\mathcal{A}$ has a negligible advantage in the following game*

1) *Setup: Runs $(par, s) \leftarrow Setup(1^\lambda)$ and sends par to $\mathcal{A}$.*

2) *Phase-1: $\mathcal{A}$ outputs target two identities sets $(\mathcal{ID}_0, \mathcal{ID}_1)$.*

3) *Phase-2: This phase like the Phase-2 in* IND-CCA *game with the constraint that $ID_j \notin \mathcal{ID}_0, \mathcal{ID}_1$.*

4) *Phase-3: This phase like as Phase-3 in* IND-CCA *game.*

5) *Challenge: $\mathcal{A}$ outputs a target message M. Challenger $\mathcal{C}$ randomly selects $\beta \in \{0,1\}$ and creates a ciphertext $C^* \leftarrow Encrypt(par, \mathcal{ID}_\beta, M)$ and returns C^* to $\mathcal{A}$.*

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

7) *Output: $\mathcal{A}$ outputs β' and wins the game if $\beta' = \beta$.*

3 Cryptanalysis of FHH Scheme

3.1 Review of FHH Scheme

The FHH anonymous multireceiver identity-based encryption is derived from BF-IBE scheme [2]. A sender chooses t receivers and prepares t points (x_1, y_1),..., (x_t, y_t) respectively for them. For every receiver 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 $\mathbb{Z}_q$, and then computes $y_i = yQ_i$ as the personal private key of the receiver where y is randomly chosen from $\mathbb{Z}_q$ and ID_i is also mapped into $\mathbb{G}_1$. The anonymity is presented from the following polynomial

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

where

$$\begin{aligned} F_i(x) &= y_i \prod_{1 \le j \ne i \le t} \frac{x - x_j}{x_i - x_j} \\ &= \begin{cases} y_i, & \text{if } x = x_i \\ 0, & \text{if } x \in \{x_1, \ldots, x_t\} \backslash \{x_i\} \end{cases} \end{aligned} \tag{2}$$

The concrete construction of FHH scheme [4] is described as follows.

Setup. Take a security parameter λ as input, this algorithm works as: Pick $s \in \mathbb{Z}_q$ and an element $P_1 \in \mathbb{G}_1$ at random, and set $P_{pub} = sP$; Choose five cryptographic one-way hash functions:

$$H : \mathbb{Z}_q \leftarrow \{0,1\}^*, H_1 : \mathbb{G}_1 \leftarrow \{0,1\}^*, H_2 : \{0,1\}^w \leftarrow \mathbb{G}_2$$
$$H_3 : \mathbb{Z}_q \leftarrow \{0,1\}^w \times \{0,1\}^*, H_4 : \{0,1\}^w \leftarrow \{0,1\}^w$$

Select a symmetric encryption (E_k, D_k) of a key k; Publish the system parameters $par = \langle q, \mathbb{G}_1, \mathbb{G}_2, e, P, P_1, P_{pub}, H, H_1\text{-}H_4 \rangle$ and keep s.

Extract. Take *par* and an identity ID_i as inputs, the algorithm produce the private key of ID_i as: Compute $Q_i = H_1(ID_i) \in \mathbb{G}_1$; Set the private key $d_i = s(P_1 + Q_i)$.

Encrypt. Take *par*, a plaintext M, and multireceiver identities $\mathcal{ID} = (ID_1, \ldots, ID_t)$ as inputs, this algorithm performs:

1) At random pick $\sigma \in \{0,1\}^w$ and set $r = H_3(\sigma, M)$.

2) Select $\alpha \in \mathbb{Z}_q$ randomly. and set $y = \alpha^{-1} r \bmod q$.

3) For $i = 1, \ldots, t$, pick $a_{i,1}, a_{i,2}, \ldots, a_{i,t} \in \mathbb{Z}_q$ and compute $x_i = H(ID_i)$, $Q_i = H_1(ID_i)$, and $f_i(x) = \prod_{1 \le j \ne i \le t} \frac{x - x_j}{x_i - x_j} = a_{i,1} + a_{i,2}x + \ldots + a_{i,t}x^{t-1}$.

4) For $i = 1, \ldots, t$, calculate $R_i = \sum_{j=1}^t a_{j,i} y Q_j = \sum_{j=1}^t b_j Q_j$ where $b_j = a_{j,i} y \in \mathbb{Z}_q$.

5) Output the ciphertext as $C = \langle R_1, \ldots, R_t, U_1, U_2, V, W \rangle$ where $U_1 = rP$, $U_2 = \alpha P_{pub}$, $V = \sigma \oplus H_2(e(P_1, P_{pub})^r)$, $W = E_{H_4(\sigma)}(M)$.

Decrypt. Take *par*, a ciphertext $C = \langle R_1, \ldots, R_t, U_1, U_2, V, W \rangle$, a receiver identity ID_i and corresponding private key d_i as inputs, the algorithm performs as follows:

1) Compute $x_i = H(ID_i)$;

2) Set $\lambda = R_1 + x_i R_2 + \ldots + (x_i^{t-1} \bmod q) R_t$;

3) Compute $\sigma' = V \oplus H_2(\frac{e(U_1,d_i)}{e(U_2,\lambda)})$ and $M' = D_{H_4(\sigma')}(W)$

4) Set $r' = H_3(\sigma', M')$; Check equation $U_1 \overset{?}{=} r'P$. If true, accept the message M'. i.e., $M = M'$; Otherwise, output $\perp$ to reject the ciphertext.

3.2 Cryptanalysis

3.2.1 Confidentiality Analysis

We attack the confidentiality of IND-CCA by a chosen-ciphertext attack manner. After receiving a challenge ciphertext $C^* = \langle R_1^*, \ldots, R_t^*, U_1^*, U_2^*, V^*, W^*\rangle$, which is a ciphertext of message M_0 or M_1 (Note that M_0, M_1 are chosen by the attacker in challenge phase). The attacker's goal is to guess the message M_β ($\beta \in \{0,1\}$) in ciphertext C^*. The attack is described as follows:

At first, the attacker selects $\gamma \in \mathbb{Z}_q$ and calculates $U_2' = \gamma U_2^*$ and $R_i' = R_i^*/\gamma$ for $i = 1, \ldots, t$. Then the attacker issues a decryption query for ciphertext $C' = \langle R_1', \ldots, R_t', U_1^*, U_2', V^*, W^*\rangle$ like Phase-4 in IND-CCA game. Obviously, $C' \neq C^*$. The challenger returns the message M' for the decryption query C'. If $M' = M_0$, the attacker outputs $\beta' = 0$. Otherwise if $M' = M_1$, the attacker outputs $\beta' = 1$.

Attack feasibility. The modified ciphertext C' holds the consistency of decryption. That is, $\lambda' = R_1' + x_i R_2' + \cdots + x_i^{t-1} R_t' = R_1^*/\gamma + x_i R_2^*/\gamma + \cdots + x_i^{t-1} R_t^*/\gamma = \frac{y}{\gamma} Q_i$, $\sigma' = V^* \oplus H_2\left(\frac{e(U_1^*,d_i)}{e(U_2',\lambda')}\right) = V^* \oplus H_2\left(\frac{e(U_1^*,d_i)}{e(\gamma U_2^*,\frac{y}{\gamma}Q_i)}\right) = V^* \oplus H_2\left(\frac{e(U_1^*,d_i)}{e(U_2^*,\lambda)}\right)$. Then C' and C^* have the same session key σ', which is used to play the key of symmetric encryption $D_{H_4(\sigma')}(W^*)$. Moreover, the verification equation $U_1 \overset{?}{=} H_3(\sigma', M')P$ does not involved the modified components U_2' and R_i' ($i = 1, \ldots, t$).

Remark 1. *The FHH scheme is derived from BF-IBE [2] and Shamir secret sharing [7]. However, BF-IBE is CCA-secure under only one receiver. that is, the combination of BF-IBE and secret sharing scheme will loss the security level under multireceiver.*

Fan et al. declared that FHH scheme achieves forward security and backward security. The related definitions are described as follows.

Forward secrecy [6]. The members who have quit the group should not be able to know the later session keys.

Backward secrecy [6]. New members should not be able to know the session keys generated before they join the group.

Remark 2. *Fan et al. declared that FHH scheme achieves forward security and backward security. Actually, the FHH scheme is neither forward secure nor backward secure. Since anyone can obtain the session key σ' through transforming the target ciphertext c^* into the other ciphertext C' though the session key σ' is randomly chosen in every session.*

3.2.2 Anonymity Analysis

We attack the anonymity by an explicit way. In challenge phase, the attacker provides two receiver set $\mathcal{ID}_0 = \{ID_{0,1}, \ldots, ID_{0,t}\}$ and $\mathcal{ID}_1 = \{ID_{1,1}, \ldots, ID_{1,t}\}$ to the challenger and receives a challenged ciphertext $C^* = \langle R_1^*, \ldots, R_t^*, U_1^*, U_2^*, V^*, W^*\rangle$. The attacker's goal is to determine who is the receiver identity set $\mathcal{ID}_\beta$ where $\beta \in \{0,1\}$. We attack the anonymity as follows:

For $k = 0, 1,\ i = 1, \ldots, t$, computes $x_{k,i} = H(ID_{k,i})$ and $\lambda_{k,i} = R_1^* + x_{k,i} R_2^* + \ldots + (x_{k,i}^{t-1} \bmod q) R_t^*$. Checks whether the equations (3) hold for $k = 0, 1$

$$\frac{\lambda_{k,1}}{x_{k,1}} = \frac{\lambda_{k,2}}{x_{k,2}} = \ldots = \frac{\lambda_{k,t}}{x_{k,t}} \tag{3}$$

If $k = 0$ for above equation holds, then outputs $\beta' = 0$. Otherwise, if $k = 1$ for the equation holds, outputs $\beta' = 1$.

Attack correctness. Suppose that $\mathcal{ID}_0$ is selected challenge identity set, i.e., $\beta = 0$. Then for $i = 1, \cdots, t$, $x_i = H(ID_{0,i})$, $Q_i = H_1(ID_{0,i})$ and $R_i^* = \sum_{j=1}^t a_{j,i} y Q_{0,j} = \sum_{j=1}^t b_j Q_{0,j}^*$, it has

$$\begin{aligned}
\lambda_{0,i} &= R_1^* + x_i R_2^* + \cdots + x_i^{t-1} R_t^* \\
&= (a_{1,1} y Q_{0,1} + \cdots + a_{t,1} y Q_{0,t}) \\
&\quad + x_i (a_{1,2} y Q_{0,1} + \cdots + a_{t,2} y Q_{0,t}) \\
&\quad + \cdots + x_i^{t-1} (a_{1,t} y Q_{0,1} + \cdots + a_{t,t} y Q_{0,t}) \\
&= (a_{1,1} + a_{1,2} x_i + \cdots + a_{1,t} x_i^{t-1}) y Q_{0,1} \\
&\quad + \cdots + (a_{i,1} + a_{i,2} x_i + \cdots + a_{i,t} x_i^{t-1}) y Q_{0,i} \\
&\quad + \cdots + (a_{t,1} + a_{t,2} x_i + \cdots + a_{t,t} x_i^{t-1}) y Q_{0,t} \\
&= 0 + \cdots + y Q_{0,i} + \cdots + 0 = y Q_{0,i}
\end{aligned} \tag{4}$$

However, if $\beta = 1$ and $R_i^* = \sum_{j=1}^t a_{j,i} y Q_{1,j}$ ($Q_{1,j} \neq Q_{0,j}$), the recovered λ by Lagrange interpolating polynomial will be an random element in $\mathbb{G}_1$, since it does not hold the consistency of secret share/reconstruction. Obviously, under this case, $\beta = 1$, we can obtain

$$\frac{\lambda_{1,1}}{H_1(ID_{1,1})} \neq \frac{\lambda_{1,2}}{H_1(ID_{1,2})} \neq \cdots \neq \frac{\lambda_{1,t}}{H_1(ID_{1,t})}$$

We now reconsider $\beta = 0$. As $\lambda_{0,i} = yQ_{0,i}$ in Equation (4), we have

$$\lambda_{0,1} = yQ_{0,1}, \lambda_{0,2} = yQ_{0,2}, \ldots, \lambda_{0,t} = yQ_{0,t}$$

Thus, $\frac{\lambda_{0,1}}{Q_{0,1}} = \frac{\lambda_{0,2}}{Q_{0,2}} = \cdots = \frac{\lambda_{0,t}}{Q_{0,t}} = y$ if $\mathcal{ID}_0 = (ID_{0,1}, ID_{0,2}, \cdots, ID_{0,t})$ is the chosen identity set in the ciphertext. Thus, we can check whether the equation (3) holds to decide which multireceiver set is chosen.

Our attack is very fast since it does not involve any oracle query and pairing operation.

Remark 3. *Anyone can deduce the authorized receivers because he can publicly compute λ_i for all $ID_i \in \mathcal{ID}$ and these λ_i are linear to Q_i. Then, the FHH scheme does not achieve a weaker security of* IND-CPA. *Actually, the FHH scheme cannot achieve the anonymity of* ANON-CCA *since our attack does not involved any decryption query.*

Proposition 1. *The FHH scheme does not capture the confidentiality of* IND-CCA *and the anonymity of* ANON-CCA. *In particular, the FHH scheme only achieves the confidentiality of* IND-CPA *security.*

4 Concluding Remark

In this work, we pointed out that a multireceiver encryption proposed by Fan et al. provides neither confidentiality of IND-CPA nor anonymity that they had previously declared. We stated that the their scheme only achieves the weaker confidentiality of IND-CPA. We also showed that a trivial secret sharing cannot achieve the anonymity in the multiple identities privacy preservation.

Acknowledgments

The authors would like to express their deep appreciation for the valuable comments provided by anonymous reviewers. This work was supported by the National Natural Science Foundation of China(No. 61070189, 61272435, 61370224, 61170135), the Fundamental Research Funds for the Central Universities(No. GK201304008), and the Natural Science Foundation of Guangdong(No. S2012010010383).

References

[1] J. Baek, R. S. Naini, and W. Susilo. Efficient multireceiver identity-based encryption and its application to broadcast encryption. In *PKC 2005*, LNCS 3386, pages 23–26, 2005.

[2] D. Boneh and M. Franklin. Identity-based encryption from the weil pairing. *SIAM Journal of Computing*, 32(3):586–615, 2003.

[3] C. Delerablee. Identity-based broadcast ecryption with constant size ciphertexts and private keys. In *Asiacrypt 2007*, LNCS 4833, pages 200–215, 2007.

[4] C. I. Fan, L. Y. Huang, and P. H. Ho. Anonymous multireceiver identity-based encryption. *IEEE Transactions on Computers*, 59(9):1239–1249, 2010.

[5] J. Hur, C. Park, and S. O. Hwang. Privacy-preserving identity-based broadcast encryption. *Information Fusion*, 13(4):293–306, 2012.

[6] R. Molva and A. Pannetrat. Network security in the multicast framework. In *Advanced Lectures in Networking*, LNCS 2497, pages 59–82, 2002.

[7] A. Shamir. How to share a secret. *Communications of the ACM*, 22(11):612–613, 1979.

[8] Y. M. Tseng, Y. H. Huang, and H. J. Chang. Privacy-preserving multireceiver id-based encryption with provable security. *International of Communication Systems*, doi:10.1002/dac2395, 2012.

Zhenhua Chen received her B.S. degree from Lanzhou University in 1998, and the M.S. degree from Nanjing University of Science and Technology in 2007. She is currently studying at School of Computer Sciences, Shaanxi Normal University as a Ph.D. candidate. She had been worked at Institute of Huaiyin Technology from 1998 to 2007 and at Beijing University of Technology as a associate professor from 2007 to 2011 respectively. Her research interests include cryptography and information security..

Shundong Li received his Ph. D. degree from Xi'an Jiaotong University in 2003, and had been worked in Tsinghua University as Post-doctor from 2003 to 2005. From 2005 to 2007, he had been an associate professor at Beijing Normal University. He is currently a professor and supervisor of Ph.D. at School of Computer Science, Shaanxi Normal University. His research interests focus on secure multi-party computation and confidential data mining.

Chunzhi Wang, Ph.D, professor. She is currently working at School of Computer Science and Engineering, Hubei University of Technology. Her research interests focus on network security.

Mingwu Zhang, Ph.D, professor. He is currently working at School of Computer Science and Engineering, Hubei University of Technology. His research interests are in the area of applied cryptography and network security, distributed trust and privacy protection, secure and fair multiparty computation, etc.