Cryptanalysis and Improvement of an ID-Based Threshold Signcryption Scheme[1]

Wei Yuan
Department of Computer Science and Technology, Jilin University, Changchun, China
Email: yuanwei1@126.com

Liang Hu
Department of Computer Science and Technology, Jilin University, Changchun, China
Email: hul@mails.jlu.edu.cn

Hongtu Li
Department of Computer Science and Technology, Jilin University, Changchun, China
Email: li_hongtu@hotmail.com

Jianfeng Chu
Department of Computer Science and Technology, Jilin University, Changchun, China
Email: chujf@jlu.edu.cn

Hui Wang
Department of Computer Science and Technology, Jilin University, Changchun, China
Corresponding author, Email: wh10@mails.jlu.edu.cn

***Abstract*— Signcryption can realize the function of encryption and signature in a reasonable logic step, which can lower computational costs and communication overheads. In 2008, Fagen Li et al. proposed an efficient secure id-based threshold signcryption scheme. The authors declared that their scheme had the attributes of confidentiality and unforgeability in the random oracle model. In this paper, we show that scheme is insecure against malicious attackers and give our attacker method to forge the ciphertext. Following our method, any malicious attacker can forge a valid message in their scheme. Further, we propose a probably-secure improved scheme to correct the vulnerable and give the unforgeability and confidentiality of our improved scheme under the existing security assumption.**

***Index Terms*—Identity-based, Signcryption, Bilinear pairing, Cryptanalysis**

I. INTRODUCTION

Encryption and signature are the two basic cryptographic tools offered by public key cryptography for achieving confidentiality and authentication. Signcryption can realize the function of encryption and signature in a reasonable logic step which is proposed by ZHENG [1] in 1997. Comparing to the traditional way of signature then encryption or encryption then signature, signcryption can lower the computational costs and communication overheads. As a result, a number of signcryption schemes [2][3][4][5][6][7][8]were proposed following ZHENG's work. The security notion for signcryption was first formally defined in 2002 by Baek et al. [9] against adaptive chosen ciphertext attack and adaptive chosen message attack. The same as signature and encryption, signcryption meets the attributes of confidentiality and unforgeability as well.

In 1984, A.Shamir [10] introduced identity-based public key cryptosystem, in which a user's public key can be calculated from his identity and defined hash function, while the user's private key can be calculated by a trusted party called Private Key Generator (PKG). The identity can be any binary string, such as an email address and needn't to be authenticated by the certification authentication. As a result, the identity-based public key cryptosystem simplifies the program of key management to the conventional public key infrastructure. In 2001, Boneh and Franklin [11] found bilinear pairings positive in cryptography and proposed the first practical identity-based encryption protocol using bilinear pairings. Soon, many identity-based [12][14][15][16] and other relational [13][17][18] schemes were proposed and the bilinear pairings became important tools in constructing identity-based protocols.

Group-oriented cryptography [19] was introduced by Desmedt in 1987. Elaborating on this concept, Desmedt and Frankel [20] proposed a (t, n) threshold signature scheme based RSA system [21]. In such a (t,n) threshold signature scheme, any to out of n signers in the group can collaboratively sign messages on behalf of the group for sharing the signing capability.

[1] *corresponding author: Jianfeng Chu

doi:10.4304/jcp.7.6.1345-1352

Identity-based signcryption schemes combine the advantages of identity-based public key cryptosystem and Signcryption. The first identity-based threshold signature scheme was proposed by Baek and Zheng [22] in 2004. Then Duan et al. proposed an identity-based threshold signcryption scheme [23] in the same year by combining the concepts of identity based threshold signature and encryption together. However, in Duan et al.'s scheme, the master-key of the PKG is distributed to a number of other PKGs, which creates a bottleneck on the PKGs. In 2005, Peng and Li proposed an identity-based threshold signcryption scheme [24] based on Libert and Quisquater's identity-based signcryption scheme [25]. However, Peng and Li's scheme dose not provide the forward security. In 2008, another scheme [26] was proposed by Fagen Li et al., which is more efficient comparing to previous scheme.

In this paper, we show that the threshold signcryption scheme of Fagen Li et al. is vulnerable if the attacker can replaces the group public key or even the attacker can intercept the intermediate messages. Further, we propose a probably-secure improved scheme to correct the vulnerable and give the unforgeability and confidentiality of our improved scheme under the existing security assumption.

II. PRELIMINARIES

A. Bilinear pairing

Let G_1 be a cyclic additive group generated by P, whose order is a prime q, and G_2 be a cyclic multiplicative group with the same order q. A bilinear pairing is a map $e: G_1 \times G_1 \to G_2$ with the following properties:

1. Bilinearity: $e(aP, bQ) = e(P, Q)^{ab}$ for all $P, Q \in G_1, a, b \in Z_q$.

2. Non-degenerative: There exists $P, Q \in G_1$ such that $e(P, Q) \neq 1$.

3. Computable: There is an efficient algorithm to compute $e(P, Q)$ for all $P, Q \in G_1$.

B. Computational assumption

Let G_1 and G_2 be two groups of prime order q, let $e: G_1 \times G_1 \to G_2$ be a bilinear pairing and let P be a generator of G_1.

- Discrete Logarithm Problem (DLP)
  Given $P, Q \in G_1$, find $n \in Z_q$ such that $P = nQ$ whenever such n exists.
- Computational Diffie-Hellman Problem (CDHP)
  Given $(P, aP, bP) \in G_1$ for $a, b \in Z_q^*$, find the element abP.
- Bilinear Diffie-Hellman Problem (BDHP)
  Given $(P, aP, bP, cP) \in G_1$ for $a, b, c \in Z_q^*$, compute $e(P, P)^{xyz} \in G_2$
- Bilinear Diffie-Hellman Problem (DBDHP)
  Given $(P, aP, bP, cP, \tau) \in G_1^4 \times G_2$ for $a, b, c \in Z_q^*$, decide whether $\tau = e(P, P)^{abc}$

C. Security notions for identity-based Threshold signcryption

The notion of semantic security of public key encryption was extended to identity-based signcryption scheme by Malone-Lee [27]. This was later modified by Sherman et al. [28] which incorporates indistinguishability against adaptive chosen ciphertext and identity attacks (IND-IDTSC-CCA2) and existential unforgeability against adaptive chosen message and identity attacks (EUF-IDTSC). We describe below the security notions for confidentiality and unforgeability given in [29], this is the strongest security notion for this problem.

Confidentiality: A signcryption scheme is semantically secure against chosen ciphertext and identity attacks (IND-IDTSC-CCA2) if no probabilistic polynomial time adversary Eve has a non-negligible advantage in the following game:

1. The challenger C runs the Setup algorithm and sends the system public parameters to the adversary Eve.

2. In the first phase, Eve makes polynomial bounded number of queries to the following oracles.

Extract Oracle: Eve produces an identity ID_i and queries for the secret key of user i. The Extract Oracle returns S_i to Eve.

Signcrypt Oracle: Eve produces a message m, sender identity ID_A and receiver identity ID_B. C computes the secret key S_A from Extract Oracle and returns to Eve, the signcrypted ciphertext from $\text{Signcrypt}\, m, \{S_i\}_{i=1,\ldots,t}, ID_j$.

Unsigncrypt Oracle: Eve produces a sender identity ID_A and receiver identity ID_B and a signcryption σ. The challenger C computes the secret key S_B from Extract Oracle, returning the result of $Unsigncrypt(\sigma, Q_{ID_A}, S_B)$ to Eve. The result returned is $\perp$ if σ is a valid signcryption from U_A to U_B.

3. A produces two messages m_0 and m_1 of equal length from the message space M and an arbitrary sender identity ID_A. The challenger C flips a coin, sampling a bit $b \in \{0,1\}$ and computes $\sigma^* = Signcrypt(m_b, \{S_i\}_{i=1,\ldots,t}, ID_B)$. σ^* is return to Eve as challenge signcrypted ciphertext.

4. Eve is allowed to make polynomial bounded number of new queries as in step 2 with the restrictions that it should not query the Unsigncryption oracle for the unsigncryption of σ^*, the Signcryption Oracle for the signcryption of m_0 or m_1 under the sender identity ID_A and the Extract Oracle for the secret keys of ID_B.

5. At the end of this game, Eve outputs a bit b'. Eve wins the game if $b' = b$.

Unforgeability: A signcryption scheme is existentially unforgeable under chosen message attack (EUF-IDTSC)

if no probabilistic polynomial time adversary Eve has a non-negligible advantage in the following game.

1. The challenger C runs the Setup algorithm to generate the master public and private keys params and msk respectively. C gives system public parameters params to Eve and keeps the master private key msk secret from Eve.
2. The adversary Eve makes polynomial bounded number of queries to the oracles as described in step 2 of the confidentiality game.
3. Eve produces a signcrypted ciphertext σ and wins the game if the private key of sender U_A was not queried in the previous step and $\perp$ is not returned by $Unsigncrypt(\sigma, Q_{ID_A}, S_B)$ and σ is not the output of a previous query to the Signcrypt Oracle with ID_A as sender.

III. Review of Fagen Li's ID-Based Threshold Signcryption Scheme

In this section, we review the identity-based threshold signcryption scheme as proposed by Fagen Li and Yong Yu. The scheme involves four roles: the PKG, a trust dealer, a sender group $U_A = \{M_1, M_2, \ldots, M_n\}$ with identity ID_A and a receiver Bob with identity ID_B.

Setup: Given a security parameter k, the PKG chooses groups G_1 and G_2 of prime order q (with G_1 additive and G_2 multiplicative), a generator P of G_1, a bilinear map $e: G_1 \times G_1 \to G_2$, a secure symmetric cipher (E,D) and hash functions $H_1: \{0,1\}^* \to G_1$, $H_2: G_2 \to \{0,1\}^{n_1}$, $H_3: \{0,1\}^* \to Z_q^*$. The PKG chooses a master-key $s \in_R Z_q^*$ and computes $P_{pub} = sP$. The PKG publishes system parameters $\{G_1, G_2, n_1, e, P, P_{pub}, E, D, H_1, H_2, H_3\}$ and keeps the master-key s secret.

Extract: Given an identity ID, the PKG computes $Q_{ID} = H_1(ID)$ and the private key $S_{ID} = sQ_{ID}$. Then PKG sends the private key to its owner in a secure way.

Keydis: Suppose that a threshold t and n satisfy $1 \le t \le n < q$. To share the private key S_{ID_A} among the group U_A, the trusted dealer performs the steps below.

1) Choose $F_1, \ldots, F_{t-1}$ uniformly at random from G_1^*, construct a polynomial $F(x) = S_{ID_A} + xF_1 + \cdots + x^{t-1}F_{t-1}$ and compute $S_i = F(i)$ for $i = 0, \ldots, n$. Note that $S_0 = S_{ID_A}$.

2) Send S_i to member M_i for $i = 1, \ldots, n$ secretly. Broadcast $y_0 = e(S_{ID_A}, P)$ and $y_j = e(F_j, P)$ for $j = 1, \ldots, t-1$

3) Each M_i then checks whether his share S_i is valid by computing $e(S_i, P) = \prod_{j=0}^{t-1} y_j^{i^j}$. If S_i is not valid, M_i broadcasts an error and requests a valid one.

Signcrypt: Without loss of generality, we assume that $M_1, \ldots, M_t$ are the t members who want to cooperate to signcrypt a message m on behalf of the group U_A.

1) Each M_i chooses $x_i \in_R Z_q^*$, computes $R_{1i} = x_i P$ and $R_{2i} = x_i P_{pub}$, and sends (R_{1i}, R_{2i}) to the clerk C.

2) The clerk C computes $R_1 = \prod_{i=1}^{t} R_{1i}$, $R_2 = \prod_{i=1}^{t} R_{2i}$, $\tau = e(R_2, Q_{ID_B})$, $k = H_2(\tau)$, $c = E_k(m)$, and $h = H_3(m, R_1, k)$. Then the clerk C sends h to M_i for $i = 0, \ldots, t$.

3) Each M_i computes the partial signature $W_i = x_i P_{pub} + h\eta_i S_i$ and sends it to the clerk C, where $\eta = \prod_{j=1, j\neq i}^{t} -j(i-j)^{-1} \bmod q$.

4) When receiving M_i's partial signature W_i, the clerk C verifies its correctness by checking if the following equation holds:

$$e(P, W_i) = e(R_{1i}, P_{pub})(\prod_{j=0}^{t-1} y_j^{i^j})^{h\eta_i}$$

If all partial signatures are verified to be legal, the clerk C computes $W = \sum_{i=1}^{t} W_i$; otherwise rejects it and requests a valid one. The final threshold signcryption is $\sigma = (c, R_1, W)$.

Unsigncrypt: When receiving σ, Bob follows the steps below.

1) Compute $\tau = e(R_1, S_{ID_B})$ and $k = H_2(\tau)$.

2) Recover $m = D_k(c)$

3) Compute $h = H_3(m, R_1, k)$ and accept σ if and only if the following equation holds:

$$e(P, W) = e(P_{pub}, R_1 + hQ_{ID_A})$$

IV. Cryptanalysis of Fagen Li's ID-Based Threshold Signcryption Scheme

A. Forgery attack

Suppose that an attacker can control the communication channel, which means that she can gain each user's corresponding ciphertext in the channel and modify or forge it to replace the original one. Then she will try to disrupt the scheme as follows:

All the attack process will be finished in the Signcrypt stage. We describe it as follows:

1. The attacker records (R_{1i}, R_{2i}) sent from M_i for $i = 0, \ldots, t$.

2 The attacker intercepts h sent from clerk C. Then she computes $R_1 = \prod_{i=1}^{t} R_{1i}$ and $R_2 = \prod_{i=1}^{t} R_{2i}$ using (R_{1i}, R_{2i}), computes $\tau = e(R_2, Q_{ID_B})$, and $k = H_2(\tau)$. Further, she

selects a message m' which she wants to forge, computes $c' = E_k(m')$, and $h' = H_3(m', R_1, k)$. Finally, she sends h' to M_i for $i = 0,\ldots,t$.

3. The attacker intercepts W_i sent from M_i , for $i = 0,\ldots,t$ .Note that the message $W_i = x_i P_{pub} + h\eta_i S_i$ here. Then she computes

$$W_i' = R_{2i} + (W_i - R_{2i}) \cdot h/h'$$
$$= x_i P_{pub} + (x_i P_{pub} + h'\eta_i S_i - x_i P_{pub}) \cdot h/h'$$
$$= x_i P_{pub} + h\eta_i S_i$$

and send W_i' to clerk C.

4. Because $W_i' = x_i P_{pub} + h\eta_i S_i$ .The verification function $e(P, W_i') = e(R_{1i}, P_{pub})(\prod_{j=0}^{t-1} y_j^{i^j})^{h\eta_i}$ will hold. Then the clerk C will send $\sigma = (c, R_1, W')$, where $W' = \sum_{i=1}^{t} W_i'$, to the receiver.

The attacker intercepts $\sigma = (c, R_1, W')$, computes $W = \sum_{i=1}^{t} W_i$, and sends $\sigma' = (c', R_1, W)$ to the receiver.

In the Unsigncrypt stage:

After receiving σ' , the receiver Bob executes the following steps

1. He will compute $\tau = e(R_1, S_{ID_B})$ and $k = H_2(\tau)$.

2. He will recover $m' = D_k(c')$.

3. He will compute $h' = H_3(m', R_1, k)$ here. Then the equation $e(P, W) = e(P_{pub}, R_1 + h'Q_{ID_A})$ will hold. Because

$$e(P, W) = e(P, \sum_{i=1}^{t} W_i)$$
$$= e(P, \sum_{i=1}^{t} (x_i P_{pub} + h'\eta_i S_i))$$
$$= e(P, R_2 + h'S_{ID_A})$$
$$= e(P_{pub}, R_1 + h'Q_{ID_A})$$

So the receiver accepts the forged message m' .

B. Key replacement attack

Fagen Li et al.'s scheme is insecure from the view of a malicious attacker who can control the communication channel.

The attacker intercepts the ciphertext $\sigma = (c, R_1, W)$ from sender.

1) Randomly choose $\alpha, x \in Z_q^*$ and prepare a forged message m'

2) Compute $R_1' = xP$, $R_2' = xP_{pub}$, $\tau' = e(R_2', Q_{ID_B})$, $k' = H_2(\tau)$, $c' = E_{k'}(m')$, $h' = H_3(m', R_1', k')$.

3) Compute $W' = \alpha P_{pub}$, set $Q_A' = (\alpha - x)P / h'$ as a public key of U_A

4) The final ciphertext is $\sigma' = (c', R_1', W')$.

5) Attacker sends the forged ciphertext and the replaced public key to the receiver.

After receiving the ciphertext $\sigma' = (c', R_1', W')$, the receiver

1) Compute $\tau = e(R_1', S_{ID_B}) = e(R_2', Q_{ID_B}) = \tau'$, $k = H_2(\tau) = H_2(\tau') = k'$

2) Recover $m = D_k(c') = D_{k'}(c') = m'$, $h = H_3(m', R_1', k') = h'$.

3) Verify $e(P, W') \stackrel{?}{=} e(P_{pub}, R_1' + hQ_{ID_A}')$

$\because e(P_{pub}, R_1' + hQ_{ID_A}') = e(P_{pub}, xP + h \cdot (\alpha - x)P / h') = e(P_{pub}, \alpha P) = e(P, W')$

$\therefore$ The equation $e(P, W') = e(P_{pub}, R_1' + hQ_{ID_A}')$ set.

In the view of the attacker, [26] can be simulated as following basic Signcryption scheme:

A sender "Alice" with key pairs $\{Q_{Alice} = H_1(Alice), S_{Alice} = sH_1(Alice)\}$

A receiver "Bob" with key pairs $\{Q_{Bob} = H_1(Bob), S_{Bob} = sH_1(Bob)\}$

Alice chooses $x \in Z_q^*$, $R_1 = xP$, $R_2 = xP_{pub}$, $\tau = e(R_2, Q_{Bob})$, $k = H_2(\tau)$, $c = E_k(m)$, $h = H_3(m, R_1, k)$, $W = xP_{pub} + hS_{Alice}$ and sends $\sigma = (c, R_1, W)$ to Bob as the ciphertext of his message.

There is a small mistake of the definition $H_3 : \{0,1\}^* \to Z_q^*$. We think the authors' real intention is $H_3 : \{0,1\}^* \times G_1 \times \{0,1\}^* \to Z_q^*$ to meet $h = H_3(m, R_1, k)$. In this hash function, any message about the sender is not contained. If an attacker Eve say "I am Alice" to Bob, Bob can not distinguish only with the hash value h. Our attack just utilizes this attribute of Li's scheme.

Suppose that H_3 is defined as $H_3 : \{0,1\}^* \times G_1 \times \{0,1\}^* \times G_1 \to Z_q^*$, and $h = H_3(m, R_1, k, Q_{Alice})$. The attacker Eve intercepts the ciphertext $\sigma = (c, R_1, W)$ from sender Alice and she runs the algorithm of forging ciphertext like:

1) Randomly choose $\alpha, x \in Z_q^*$ and prepare a forged message m'

2) Compute $R_1' = xP$, $R_2' = xP_{pub}$, $\tau' = e(R_2', Q_{Bob})$, $k' = H_2(\tau)$, $c' = E_{k'}(m')$, $h' = H_3(m', R_1', k', Q_{Alice}')$.

3) Compute $W' = \alpha P_{pub}$, set $Q_{Alice}' = (\alpha - x)P / h'$ as a public key of U_A

4) The final ciphertext is $\sigma' = (c', R_1', W')$.

5) Send the forged ciphertext and the replaced public key to the receiver.

She will meet a hard problem that if she wants to compute h' , Q_{Alice}' is necessary or if she wants to computes Q_{Alice}' , h' must be known. As a result, if she can

succeed in forging the ciphertext, she must own the ability to solve the DL problem.

V. THE IMPROVEMENT OF FAGEN LI ET AL.' SCHEME

The scheme involves four roles: the PKG, a trust dealer, a sender group $U_A = \{M_1, M_2, \ldots, M_n\}$ with identity ID_A and a receiver Bob with identity ID_B.

Setup: Given a security parameter k, the PKG chooses groups G_1 and G_2 of prime order q (with G_1 additive and G_2 multiplicative), a generator P of G_1, a bilinear map $e: G_1 \times G_1 \to G_2$, a secure symmetric cipher (E,D) and hash functions $H_1: \{0,1\}^* \to G_1$, $H_2: G_2 \to \{0,1\}^{n_1}$, $H_3: \{0,1\}^* \times G_1 \times \{0,1\}^* \times G_1 \to Z_q^*$. The PKG chooses a master-key $s \in_R Z_q^*$ and computes $P_{pub} = sP$. The PKG publishes system parameters $\{G_1, G_2, n_1, e, P, P_{pub}, E, D, H_1, H_2, H_3\}$ and keeps the master-key s secret.

Extract: Given an identity ID, the PKG computes $Q_{ID} = H_1(ID)$ and the private key $S_{ID} = sQ_{ID}$. Then PKG sends the private key to its owner in a secure way.

Keydis: Suppose that a threshold t and n satisfy $1 \le t \le n < q$. To share the private key S_{ID_A} among the group U_A, the trusted dealer performs the steps below.

1) Choose $F_1, \ldots, F_{t-1}$ uniformly at random from G_1^*, construct a polynomial $F(x) = S_{ID_A} + xF_1 + \cdots + x^{t-1}F_{t-1}$

2) Compute $S_i = F(i)$ for $i = 0, \ldots, n$. ($S_0 = S_{ID_A}$). Send S_i to member M_i for $i = 1, \ldots, n$ secretly.

3). Broadcast $y_0 = e(S_{ID_A}, P)$ and $y_j = e(F_j, P)$ for $j = 1, \ldots, t-1$.

4) Each M_i then checks whether his share S_i is valid by computing $e(S_i, P) = \prod_{j=0}^{t-1} y_j^{i^j}$. If S_i is not valid, M_i broadcasts an error and requests a valid one.

Signcrypt: Let $M_1, \ldots, M_t$ are the t members who want to cooperate to signcrypt a message m on behalf of the group U_A.

1) Each M_i chooses $x_i \in_R Z_q^*$, computes $R_{1i} = x_i P$, $R_{2i} = x_i P_{pub}$, $\tau_i = e(R_{2i}, Q_{ID_B})$ and sends (R_{1i}, τ) to the clerk C.

2) The clerk C (one among the t cooperating players) computes $R_1 = \prod_{i=1}^{t} R_{1i}$, $\tau = \prod_{i=1}^{t} \tau_i$, $k = H_2(\tau)$, $c = E_k(m)$, and $h = H_3(m, R_1, k, Q_{ID_A})$.

3) Then the clerk C sends h to M_i for $i = 0, \ldots, t$.

4) Each M_i computes the partial signature $W_i = x_i P_{pub} + h\eta_i S_i$ and sends it to the clerk C, where $\eta = \prod_{j=1, j\neq i}^{t} -j(i-j)^{-1} \bmod q$.

5) Clerk C verifies the correctness of partial signatures by checking if the following equation holds:

$e(P, W_i) = e(R_{1i}, P_{pub})(\prod_{j=0}^{t-1} y_j^{i^j})^{h\eta_i}$

If all partial signatures are verified to be legal, the clerk C computes $W = \sum_{i=1}^{t} W_i$; otherwise rejects it and requests a valid one.

6) The final threshold signcryption is $\sigma = (c, R_1, W)$.

Unsigncrypt: When receiving σ , Bob follows the steps below.

1) Compute $\tau = e(R_1, S_{ID_B})$ and $k = H_2(\tau)$.

2) Recover $m = D_k(c)$

3) Compute $h = H_3(m, R_1, k, Q_{ID_A})$ and accept σ if and only if the following equation holds:

$e(P, W) = e(P_{pub}, R_1 + hQ_{ID_A})$

VI. SECURITY ANALYSIS OF OUR IMPROVED SCHEME

In this section, we will give a formal proof on Unforgeability and Confidentiality of our scheme under CDH problem and DBDH problem.

Theorem 1 (Unforgeability): Our improved scheme is secure against chosen message attack under the random oracle model if CDH problem is hard.

Proof: Suppose the challenger C wants to solve the CDH problem. That is, given (aP, bP) , C should computes abP .

C chooses system parameters $\{G_1, G_2, n_1, e, P, P_{pub}, E, D, H_1, H_2, H_3\}$, sets $P_{pub} = aP$, and sends parameters to the adversary E (the hash functions H_1, H_2, H_3 are random oracles).

H_1 query: C maintains a list L_1 to record H_1 queries. L_1 has the form of $(ID, \alpha, Q_{ID}, S_{ID})$. Suppose the adversary Eve can make H_1 queries less than q_{H_1} times. C selects a random number $j \in [1, q_{H_1}]$. If C receives the j-th query, he will return $Q_{ID_j} = bP$ to Eve and sets $(ID_j, \perp, Q_{ID_j} = bP, \perp)$ on L_1 . Else C selects $\alpha_i \in Z_q^*$, computes $Q_{ID_i} = \alpha_i P$, $S_{ID_i} = \alpha_i P_{pub}$, returns Q_{ID_i} to E and sets $(ID_i, \alpha_i, Q_i, S_i)$ on L_1 .

H_2 query: C maintains a list L_2 to record H_2 queries. L_2 has the form of (τ, k) . If C receives a query about τ_i , selects $k_i \in Z_q^*$, returns k_i to E, and sets (τ_i, k_i) on L_2 .

H_3 query: C maintains a list L_3 to record H_3 queries. L_3 has the form of (m, R, k, Q, h) . If C receives a query about $(m_i, R_{1i}, k_i, Q_{ID_i})$, selects $h_i \in Z_q^*$, returns h_i to Eve, and sets $(m_i, R_{1i}, k_i, Q_{ID_i}, h_i)$ on L_3 .

Signcrypt query: If C receives a query about Signcrypt with message m_i , identity ID_i

1. Select $x_i \in Z_q^*, W_i \in G_1$

2. Look-up L_1, L_2, set $Q_{ID_i} = \alpha_i P$ in L_1, $k_i = k_i$ in L_2, and compute $R_i = x_i Q_{ID_i}$

3. Set $h_i = H_3(m_i, R_i, k_i, Q_{ID_i})$.

4. Return (h_i, W_i) to Eve.

Finally, Eve output a forged signcryption (m, h_i, W_i, Q_{ID_i}). If $Q_{ID_i} \neq Q_{ID_j}$, Eve fails. Else, if $Q_{ID_i} = Q_{ID_j}$, Eve succeeds in forging a signcryption.

As a result, C gains two signcryption ciphertexts which meet:

$$e(P, W_i) = e(P_{pub}, R_i + h_i Q_{ID_i})$$

$$e(P, W_j) = e(P_{pub}, R_j + h_j Q_{ID_j})$$

Thus,

$$e(P, (W_i - W_j)) = e(P_{pub}, (R_i + h_i Q_{ID_i}) - (R_j + h_j Q_{ID_j})) \quad (1)$$

Note $Q = Q_{ID_i} = Q_{ID_j}$,

(1) can be expressed as $e(P, (W_i - W_j)) = e(P_{pub}, (R_i - R_j) + (h_i - h_j)Q)$ (2)

$\because P_{pub} = aP, Q_{ID_j} = bP$

(2) can be expressed as $e(P, (W_i - W_j)) = e(aP, ((\alpha_i - \alpha_j) + (h_i - h_j))bP)$

$\therefore W_i - W_j = ((\alpha_i - \alpha_j) + (h_i - h_j))abP$

Hence, the CDH problem $abP = \dfrac{W_i - W_j}{(\alpha_i - \alpha_j) + (h_i - h_j)}$ can be computed by C with aP and bP.

Theorem 2 (Confidentiality): Our improved scheme is secure against adaptive chosen ciphertext and identity attack under the random oracle model if DBDH problem is hard.

Proof: Suppose the challenger C wants to solve the DBDH problem. That is, given (P, aP, bP, cP, τ), C should decide whether $\tau = e(P, P)^{abc}$ or not. If there exists an adaptive chosen ciphertext and identity attacker for our improved scheme, C can solve the DBDHP.

C chooses system parameters $\{G_1, G_2, n_1, e, P, P_{pub}, E, D, H_1, H_2, H_3\}$, sets $P_{pub} = aP$, and sends parameters to the adversary E (the hash functions H_1, H_2, H_3 are random oracles).

H_1 query: C maintains a list L_1 to record H_1 queries. L_1 has the form of $(ID, \alpha, Q_{ID}, S_{ID})$. Suppose the adversary Eve can make H_1 queries less than q_{H_1} times. C selects a random number $j \in [1, q_{H_1}]$. If C receives the j-th query, he will return $Q_{ID_j} = bP$ to Eve and sets $(ID_j, \perp, Q_{ID_j} = bP, \perp)$ on L_1. Else C selects $\alpha_i \in Z_q^*$, computes $Q_{ID_i} = \alpha_i P$, $S_{ID_i} = \alpha_i P_{pub}$, returns Q_{ID_i} to E and sets $(ID_i, \alpha_i, Q_i, S_i)$ on L_1.

H_2 query: C maintains a list L_2 to record H_2 queries. L_2 has the form of (τ, k). If C receives a query about τ_i, selects $k_i \in Z_q^*$, returns k_i to E, and sets (τ_i, k_i) on L_2.

H_3 query: C maintains a list L_3 to record H_3 queries. L_3 has the form of (m, R, k, Q, h). If C receives a query about $(m_i, R_{1i}, k_i, Q_{ID_i})$, selects $h_i \in Z_q^*$, returns h_i to Eve, and sets $(m_i, R_{1i}, k_i, Q_{ID_i}, h_i)$ on L_3.

Signcrypt query: If C receives a query about Signcrypt with message m_i, identity ID_i

1. Select $c_i \in Z_q^*, W_i \in G_1$

2. Look-up L_1, L_2, set $Q_{ID_i} = \alpha_i P$ in L_1, $k_i = k_i$ in L_2. Compute $R_i = c_i P$,if $ID_i \neq ID_j$. Else, if $ID_i = ID_j$, compute $R_i = cP$

3. Set $h_i = H_3(m_i, R_i, k_i, Q_{ID_i})$.

4. Return (h_i, W_i) to Eve.

After the first stage, Eve chooses a pair of identities on which he wishes to be challenged on (ID_i, ID_j). Note that Eve can not query the identity of ID_A. Then Eve outputs two plaintexts m_0 and m_1. C chooses a bit $b \in \{0,1\}$ and signcrypts m_b. To do so, he sets $R_1^* = cP$, obtains $k^* = H_2(\tau)$ from the hash function H_2, and computes $c_b = E_{k_1^*}(m_b)$. Then C chooses $W^* \in G_1$ and sends the ciphertext $\sigma^* = (c_b, R_1^*, W^*)$ to Eve. Eve can performs a second series of queries like at the first one. At the end of the simulation, she produces a bit b' for which he believes the relation σ^*=Signcrypt$(m_{b'}, \{S_i\}_{i=1,\ldots,t}, ID_j)$ holds. If $b = b'$, C outputs $\tau = e(R_1^*, S_{ID_j}) = e(cP, abP) = e(P, P)^{abc}$. Else, C outputs $\tau \neq e(P, P)^{abc}$. So C can solve the BDDH problem.

VII. CONCLUSION

In this paper, we show that the threshold signcryption scheme of Fagen Li et al. is vulnerable if the attacker can replaces the group public key. Then we point out that the receiver uses the senders' public key without any verification in the unsigncrypt stage cause this attack. Further, we propose a probably-secure improved scheme to correct the vulnerable and give the unforgeability and confidentiality of our improved scheme under the existing security assumption.

ACKNOWLEDGMENT

The authors would like to thank the editors and anonymous reviewers for their valuable comments. This work is supported by the National Natural Science Foundation of China under Grant No. 60873235 and

60473099, the National Grand Fundamental Research 973 Program of China (Grant No. 2009CB320706), Scientific and Technological Developing Scheme of Jilin Province (20080318), the National High Technology Research and Development Program 863 of China under Grant No. 2011AA010101. and Program of New Century Excellent Talents in University (NCET-06-0300).

REFERENCES

[1] Zheng Y Digital signcryption or How to achieve cost (signature & Encryption)<< cost (signature) + cost (encryption), In Proc. Advances in CRYPTO'97, LNCS 1294, pp.165-179, Springer-Verlag,1997.
[2] Bao F., Deng R H, A signcryption scheme with signature directly verifiable by public key. PKC'98 LNCS, vol.1431, pp55-59, Springer-Verlag, 1997.
[3] Chow S.S.M., Yiu S.M., Hui L.C.K., Chow K.P., Efficient forward and provably secure ID-based signcryption scheme with public verifiability and public ciphertext authenticity. ICISC'03 LNCS, vol.2971, pp.352-269, Spring-Verlag, 2004.
[4] Boyen X, Multipurpose identity based signcryption: a swiss army knife for identity based cryptography. CRYPT'03 LNCS, vol.2729, pp.383-399, Springer-Varlag, 2003.
[5] Mu Y., Varadharajan V., Distributed signcryption, INDOCRYPT'00. LNCS, vol.1977, pp.155-164, Springer-Varlag, 2000.
[6] Yang G., Wong D.S., Deng X., Analysis and improvement of a signcryption scheme with key privacy, ISC'05. LNCS, vol.3650, pp.218-232, Springer-Varlag, 2005.
[7] SteinFeld R., Zheng Y., A signcryption scheme based on integer factorization. ISW'00. LNCS, vol 1975, pp.308-322, Springer-Varlag, 2000.
[8] Libert B., Quisquater J., Efficient signcryption with key prevacy from gap Diffie-Hellman groups. PKC'04 LNCS vol.2947, pp.187-200, Springer-Varlag, 2004.
[9] Baek J., Steinfeld R., Zheng Y., Formal proofs for the security of signcryption, PKC'02 LNCS vol.2274, pp.80-98, Springer-Varlag, 2002.
[10] A. Shamir,"Identity-based cryptosystems and signature schemes", CRYPTO'84 LNCS 196, pp.47-53, Springer-Varlag, 1984.
[11] D. Boneh, M. Franklin, Identity-based encryption from well pairing, CRYPTO'01, LNCS 2139, pp.213-229, Springer-Varlag, 2001.
[12] P.S.L.M. Barreto, B. Libert, N. Mccullagh, J.J. Quisquater, Efficient and provably-secure identity-based signatures and signcryption from bilinear maps ASIACRYPT'05, LNCS 3788, pp.515-532, Springer-Verlag, 2005.
[13] X. Huang, W. Susilo, Y. Mu, E Zhang, Identity-based ring signcryption schemes: cryptographic primitives for preserving privacy and authenticity in t he ubiquitous world, 19th International Conference on Advanced Information Networking and Applications, pp.649-654, Taiwan, 2005.
[14] Fagen Li, Hu Xiong, Xuyun Nie, A new multi-receiver ID-based signcryption scheme for group communications, ICCCAS'2009, pp.296-300, 2009.
[15] Yiliang Han, Xiaolin Gui, Multi-recipient signcryption for secure group communication, ICIEA 2009, pp.161-165.
[16] Zhengping Jin, Qiaoyan Wen, Hongzhen Du, An improved semantically-secure identity-based signcryption scheme in the standard model, Computers and Electrical Engineering 36(2010), pp.545-552,Elsevier, 2010.
[17] Zhenhua Liu, Yupu Hu, Xiangsong Zhang, Hua Ma, Certificateless signcryption scheme in the standard model, Information Sciences 180(2010), pp.452-464, Elsevier, 2010.
[18] Yong Yu, Bo Yang, Ying Sun, Sheng-lin Zhu, Identity based signcryption scheme without random oracles, Computer Standards & Interfaces 31(2009), pp.56-62, Elsevier, 2009.
[19] Y. Desmedt, Society and group oriented cryptography: a now concept, CRYPTO'87, LNCS 293, pp.120-127, Springer-Varlag, 1987.
[20] Y. Des. Frankel, Shared generation of authenticators and signatures, CRYPTO'91, LNCS 576, pp.457-469, Springer-Varlag, 1991.
[21] R. L. Rivest, A. Shamir, L. Adleman, A method for obtaining digital signatures and public-key cryptosystems, Communications of the ACM, Vol.21, No.2, pp.120-126, 1978.
[22] J. Baek, Y. Zheng, Identity-based threshold signature scheme from the bilinear pairings, International Conference on Information Technology 2004, pp.124-128, Las Vegas, Nevada, USA, 2004.
[23] S. Duan, Z. Cao, R. Lu, Robust ID-based threshold signcryption scheme from pairings, International Conference on Information security, pp.33-37, Shanghai, China, 2004.
[24] C. Peng, X. Li, An identity-based threshold signcryption scheme with semantic security, Computational Intelligence and Security 2005, LNAI 3902, pp.173-179, Springer-Varlag, 2005.
[25] B. Libert, J.J. Quisquater, Anew identity based signcryption schemes from pairings, 2003 IEEE information theory workshop, pp.155-158, Paris, France, 2003.
[26] Fagen Li, Yong Yu, An efficient and Provably Secure ID-Based Threshold Signcryption Scheme, ICCCAS 2008, 488-492.
[27] Malone Lee J:Identity based signcryption. In: Cryptology ePrint Archive. Report 2002/098, 2002.
[28] Chow S.S.M., Yiu S.M., Hui L.C.K., Chow K.P.: Efficient forward and provably secure ID-based signcryption scheme with public verifiability and public ciphertext authenticity. In: Lin, J.-I., Lee, D.-H. (eds.) ICISC 2003. LNCS, vol. 2971, pp.352-369. Springer-Varlag, 2004.
[29] Boyen X.: Multipurpose identity based signcryption: a Swiss army knife for identity based cryptography. In: Boneh, D. (ed.) CRYPTO 2003. LNCS, vol. 2729, pp.383-399. Springer-Varlag, 2003.

Wei Yuan was born in Chengde of Hebei province of China in 1984. He began the study of computer science at Jilin University in 2003 and got his bachelor degree in 2007. Then he continued his research on information security and received his master degree in 2010. Now he is a PhD candidate of the college of computer science and technology of Jilin University.

His main research interests include cryptography and information security. he have participated in several projects include two National Natural Science Foundations of China and

one National Grand Fundamental Research 973 Program of China and published more than 10 research papers from 2007.

Liang Hu was born in 1968. He has his BS degree on Computer Systems Harbin Institute of Technology in 1993 and his PhD on Computer Software and Theory in 1999. Currently, he is the professor and PhD supervisor of College of Computer Science and Technology, Jilin University, China.

His main research interests include distributed systems, computer networks, communications technology and information security system, etc. As a person in charge or a principal participant, Dr Liang Hu has finished more than 20 national, provincial and ministerial level research projects of China.

Hongtu Li was born in Siping of Jilin, China on Mar. 17 1984. In 2002, Li Hongtu began the study of computer science at Jilin University in Jilin, Changchun, China. And in 2006, Li Hongtu got bachelor's degree of computer science. In the same year, Li Hongtu began the master's degree study in network security at Jilin University. After 3 years study, Li Hongtu got his master's degree in 2009. From then on, Li Hongtu began the doctor's degree in the same field of study at the same University.

From 2009, he has got a fellowship job. He worked in grid and network security laboratory as an ASSISTANT RESEACHER at Jilin University. From 2006 to now, he has published several papers. The list of published articles or books is as follows:

"Identity -Based Short Signature Without Random Oracles Model", International Conference of ICT Innovation and Application-ICIIA2008, Guangzhou, China, 2008.

"Registration and private key distribution protocol based on IBE", the 5th International Conference on Frontier of Computer Science and Technology-FCST2010, Changchun, China, 2010.

"Certificateless authenticated key agreement protocol against KCI and KRA", The 2011 International Conference on Network Computing and Information Security-NCIS'11 and the 2011 International Conference on Multimedia and Signal Processing-CMSP'11, Guilin, China, 2011.

Expect network security, he also interested in grid computing, wireless networks, intrusion detection and so on. From 2006 to now, he have participated in or led several projects include two National Natural Science Foundations of China and one National Grand Fundamental Research 973 Program of China.

Jianfeng Chu, born in 1978, Ph.D. , Now he is the teacher of the College of Computer Science and Technology, Jilin University, Changchun, China. He received the Ph.D. degree in computer structure from Jilin University in 2009. His current research interests focus on information security and cryptology.

An important objective of the projects is to probe the trend of network security, which can satisfy the need of constructing high-speed, large-scale and multi-services networks. Various complex attacks can not be dealt with by simple defense. And to add mechanisms to network architecture results in decreasing performance. In a word, fundamental re-examination of how to build trustworthy distributed network should be made.

Hui Wang, born in 1970, accepts the system of computer professional undergraduate and postgraduate education, access to software engineering master's degree at Jilin University as a recruitment management, has long been engaged in recruit students' management, systems development, data statistic and analysis work. Proficient in word, Excel, PowerPoint and word processing software, proficiency and skill VB, VFP, PHP, C + + programming development environment, familiar with FrontPage, Dreamweaver webpage editing software.