Information Sciences 276 (2014) 290–294

Contents lists available at ScienceDirect

Information Sciences

journal homepage: www.elsevier.com/locate/ins

Notes on a group-oriented setting's multisigncryption scheme with threshold designcryption

Xiangxue Li [a,b], Haifeng Qian [a,*], Yuan Zhou [a,c]

[a] Department of Computer Science and Technology, East China Normal University, Shanghai 200241, China
[b] State Key Laboratory of Integrated Services Networks, Xidian University, Xi'an 710071, China
[c] National Network Emergency Response Technical Team/Coordination Center, Beijing 100029, China

ARTICLE INFO

Article history:
Received 13 April 2012
Received in revised form 15 November 2013
Accepted 9 February 2014
Available online 20 February 2014

Keywords:
Multisigncryption
Threshold designcryption
Indistinguishability
Unforgeability
Public ciphertext authenticity

ABSTRACT

Zhang et al. proposed recently a group-oriented multisigncryption scheme with threshold designcryption and affirmed that their scheme is secure under standard complexity assumptions. However, the note elaborates concrete attacks on its indistinguishability and unforgeability under their security models. We also provide the impossibility result of public ciphertext authenticity for the scheme.

1. Introduction

Group-oriented multisigncryption is significant in group-based negotiation systems, group key management systems, etc. [2–4,6–8]. Recently, Zhang et al. proposed a group-oriented setting's multisigncryption scheme with threshold decryption (GMTD) where all the senders cooperatively produce the ciphertext, and t out of n receivers can recover the plaintext [9]. The scheme is claimed to achieve indistinguishability, unforgeability, and public ciphertext authenticity and verifiability [9].

By giving concrete attacks, however, the note confirms that Zhang et al.'s GMTD scheme is not secure. More precisely, it does not satisfy indistinguishability, unforgeability, and public ciphertext authenticity.

When examining their security proofs, one may feel confused about some gaps. Consider their security proof of indistinguishability [9]. To answer a signcryption query, the simulator should ascertain the equality $D_{A_i} = cQ_{A_i}$. However, the fact is that $D_{A_i} = cQ_{A_i} = cb_iP$ holds only with negligible probability since $Q_{A_i} = H(ID_i) = b_iP$ (where H is viewed as a random oracle) and D_{A_i} is random (because of the randomness of S and r_i that determine D_{A_i}). On the other hand, it is not the forking lemma in [5] but the general one in [1] should be applied as multi-users are involved in the simulation of their security proof of unforgeability [9].

2. Review of Zhang et al.'s multisigncryption scheme

In Zhang et al.'s GMTD scheme [9], there are a Private Key Generator (PKG), a sender group $\{A_1, \ldots, A_m\}$, a receiver group $B = \{B_1, \ldots, B_n\}$, and a legitimate user $\mathcal{U}$ that wants to designcrypt the ciphertext. The scheme consists of nine algorithms.

* Corresponding author. Tel./fax: +86 21 64023369.
E-mail address: hfqian@cs.ecnu.edu.cn (H. Qian).

http://dx.doi.org/10.1016/j.ins.2014.02.055
0020-0255/

1. Setup: Given the security parameter k, the PKG chooses two groups G_1, G_2 of prime order q, a bilinear map: $e: G_1 \times G_1 \to G_2$ and a generator P of group G_1. The system master key is $MSK = s$ where $s \in_R Z_q^*$, and the public parameters are $param = \{G_1, G_2, P, P_T, Q, e, H_1, H_2, H_3, H_4, H_5, E, E^{-1}\}$ where (E, E^{-1}) are symmetric cipher algorithms, $H_1: \{0,1\}^* \to G_1$, $H_2: \{0,1\}^* \to Z_q^*$, $H_3: \{0,1\}^* \times G_1 \times \{0,1\}^* \to Z_q^*$, $H_4: \{0,1\}^* \times G_1 \to Z_q^*$, and $H_5: G_2^3 \to Z_q^*$ are cryptographic hash functions, and $P_T = sP, Q = e(P, P_T)$.
2. KeyExt: Given an identity $ID \in \{0,1\}^*$, the algorithm returns $D_{ID} = sQ_{ID}$ as the private key, where $Q_{ID} = H_1(ID) \in G_1$ is the corresponding public key.
3. KeyDis: The algorithm uses (t, n)-secret sharing scheme to share the private key D_{ID_B} among the receiver group B.
   (a) Pick $Q_1, \ldots, Q_t \in G_1$ randomly and construct a function $F(x) = D_{ID_B} + \sum_{j=1}^{t-1} x^j Q_j$.
   (b) Compute the sub-private designcryption key $D_{B_i} = F(B_i)$ and sub-verification key $u_{B_i} = e(P, D_{B_i})$.
   (c) Send B_i the secret shadow $D_{B_i}, i = 1, \ldots, n$, and publish $(u_{B_1}, \ldots, u_{B_n})$ as public verification key.
4. Signcrypt: Given the message M and an identity ID_B, the sender A_i performs the following steps, $i = 1, \ldots, m$:
   (a) Pick $r_i \in_R Z_q^*$ and compute $R_i = Q^{r_i}, w_i = e(P_T, Q_B)^{r_i}$.
   (b) Send $(R_i, w_i) \in G_1 \times G_2$ to the other senders via a secret channel.
   (c) Compute $R = \prod_{i=1}^m R_i$ and $W = \prod_{i=1}^m w_i$ after receiving $\{(R_j, w_j) | j \neq i\}$.
   (d) Compute $C = E_{H_2(W)}(M)$, $V = H_3(C, R, ID_B)$, $U_i = r_i H_4(M, R) P_T - H_2(W) D_{A_i}$, $S_i = r_i P_T - V D_{A_i}$.
   The ciphertext by the sender group $\{A_1, \ldots, A_m\}$ is $\sigma = (C, V, U, S)$ where $U = \sum_{i=1}^m U_i$ and $S = \sum_{i=1}^m S_i$.
5. SignPubVer: Given the ciphertext $\sigma = (C, V, U, S)$, any one can check its validity: computes $R = e(P, S) e(P_T, \sum_{i=1}^m Q_{A_i})$ and accepts σ if $V = H_3(C, R, ID_B)$ holds.
6. ShareGen: A legitimate user $\mathcal{U}$ sends the ciphertext σ to each member B_i in the group B and requests for designcryption, $i = 1, \ldots, n$. B_i does the following:
   (a) Check the validity of σ by running SignPubVer algorithm.
   (b) Pick $T_i \in_R G_1$ and compute

$$\widetilde{u}_i = e\left(D_{B_i}, \sum_{i=1}^n Q_{A_i}\right), \quad \widetilde{v}_i = e\left(T_i, \sum_{i=1}^n Q_{A_i}\right), \quad \widetilde{w}_i = e(T_i, P), \\ x_i = H_5(\widetilde{u}_i, \widetilde{v}_i, \widetilde{w}_i), \quad X_i = T_i + x_i D_{B_i}. \tag{1}$$

   (c) Send $\widetilde{\sigma_i} = (i, \widetilde{u}_i, \widetilde{v}_i, \widetilde{w}_i, x_i, X_i)$ to $\mathcal{U}$.
7. ShareVer: $\mathcal{U}$ computes $x_i' = H_5(\widetilde{u}_i, \widetilde{v}_i, \widetilde{w}_i)$ and accepts $\widetilde{\sigma_i}$ as a valid share if

$$x_i' = x_i, \quad e\left(X_i, \sum_{i=1}^n Q_{A_i}\right) = \widetilde{v}_i \widetilde{u}_i^{x_i'}, \quad e(X_i, P) = \widetilde{w}_i u_i^{x_i'}, \quad i = 1, \ldots, n. \tag{2}$$

8. ShareCom: After collecting at least t valid shares, $\mathcal{U}$ performs the following:
   (a) Compute $N_j = \prod_{i=1}^t \frac{i}{i-j} (\mathrm{mod}\ q)$ and

$$w' = e(Q_B, S) \left(\prod_{j=1}^t \widetilde{u}_j^{N_j}\right)^V.$$

   (b) Recover message M by computing $M = E_{H_2(w')}^{-1}(C)$.
9. SignVer: The user $\mathcal{U}$ computes $R = e(P, S) e\left(P_T, \sum_{i=1}^m Q_{A_i}\right)$ and accepts the message M if

$$e(P, S - U) = Q^{1 - H_4(M,R)} e\left(P_T, \sum_{i=1}^m Q_{A_i}\right)^{H_2(w') - V}.$$

For Zhang et al.'s GMTD scheme, the properties of indistinguishability, unforgeability and public ciphertext authenticity are defined in [9].

Definition 2.1 (*Indistinguishability*). An identity-based multisigncryption scheme with threshold designcryption achieves the indistinguishability against adaptive chosen ciphertext attack if no polynomially bounded adversary $\mathcal{A}$ has a non-negligible advantage in the following IND-GMTD experiment.

Experiment IND-GMTD:

1. $I \leftarrow \mathsf{Setup}(1^\lambda)$; $(1^l, st) \leftarrow \mathcal{A}(selecting, n, I)$, $1 \leqslant l \leqslant n$.
2. For $i = 1, \ldots, m$ Do $D_{S_i} \leftarrow \mathsf{KeyExt}(I, ID_{S_i})$.
3. For $j = m+1, \ldots, l$ Do $D_{R_j} \leftarrow \mathsf{KeyExt}(I, ID_{R_j})$.
4. For $k = 1, \ldots, n$ Do $\{D_{R_{j_k}}, u_{R_{j_k}}\} \leftarrow \mathsf{KeyDis}(I, ID_{R_j})$.
5. $(M_0, M_1, M, coins) \leftarrow \mathcal{A}_{\mathsf{Signcrypt}(\cdot), \mathsf{ShareGen}(\cdot)}(k, finding, st)$, where $|M_0| = |M_1| = l$, $|M| = n - l$, $|coins| = n - 1$.
6. For $i = l+1, \ldots, n$ Do $D_{R_i} \leftarrow \mathsf{KeyExt}(I, ID_{R_i}, coins_i)$.
7. For $j = 1, \ldots, n$ Do $\{D_{R_{i_j}}, u_{R_{i_j}}\} \leftarrow \mathsf{KeyDis}(I, ID_{R_i}, coins_i)$.