# On the Security of a Group Signcryption Scheme from Distributed Signcryption Scheme

Haiyong Bao, Zhenfu Cao, and Haifeng Qian

Department of Computer Science and Engineering,
Shanghai Jiao Tong University,
1954 Huashan Road, Shanghai 200030, PRC
{bhy, zfcao, ares}@sjtu.edu.cn
http://tdt.sjtu.edu.cn

**Abstract.** Signcryption denotes a cryptographic method, which can process encryption and digital signature simultaneously. So, adopting such schemes, computational cost of encryption and signature compared to traditional signature-then-encryption can be reduced to a great extent. Based on the existing distributed signcryption schemes, Kwak and Moon proposed a new distributed signcryption scheme with sender ID confidentiality and extended it to a group signcryption. Their scheme is more efficient in both communication and computation aspects. Unfortunately we will demonstrate that their scheme is insecure by identifying some security flaws. Exploring these flaws, an attacker without any secret can mount universal forging attacks. That is, anyone (not necessary the group member) can forge valid group signatures on arbitrary messages of his/her choice.

## 1 Introduction

In [1], Y. Zheng proposed an asymmetric cryptographic method called signcryption, which can simultaneously provide message confidentiality and unforgeability with a little computational and communicational overhead. After that, several signcryption schemes [2], [3], [4] have been put forward. Then, Mu et al. proposed the distributed signcryption scheme [5]. In such scheme, any party can *"signcrypt"* a message and distribute it to a designed group, and any member in the receiving group can *"unsigncrypt"* the message. However, in most practical circumstances, in order to protect the user's privacy, persons who signcrypt the messages should be anonymous, i.e. requiring sender ID confidentiality. The basic scheme [5] cannot fulfill such properties. In order to make up these flaws, Kwak and Moon generalized the original scheme [5] and presented a new distributed signcryption scheme and extended to group signcryption [6]. They also presented a security analysis of their scheme and claimed that their scheme satisfied all the security requirements of distributed signcryption with sender ID confidentiality and group signcryption. However, this is not the fact.

In this paper, some serious security flaws of Kwak et al.'s scheme are successfully identified. By using our attack methods, anyone (not necessary the group

Y.G. Desmedt et al. (Eds.): CANS 2005, LNCS 3810, pp. 26–34, 2005.

member) can forge valid group signatures on any messages such that the forged messages cannot be opened by the group manager.

The rest of this paper is organized as follows. Section 2 first illustrates some preliminaries of Kwak et al.'s scheme. Section 3 presents the existing distributed signcryption and its extension, which is the basic scheme of Kwak et al.'s scheme. We then review and analyze Kwak et al.'s scheme in section 4 and 5, respectively. Finally, some conclusions and remarks are given in section 6.

## 2 Preliminaries

This section briefly introduces some basic concepts of Kwak et al.'s scheme. We put our emphasis on how to initialize of a group. In Kwak et al.'s scheme, some members of one group can send signcrypted messages to a designated group. Then, any valid member in the designated group can unsigncrypt the message using his/her private key.

**Initialization of a group**
Assume p denotes a large prime number, $Z_p^*$ a multiplicative group of order q for $q|p-1$ and $g \in Z_p^*$ a primitive element. $Hash(\cdot)$ denotes a strong one-way function, $Hash_k(\cdot)$ a keyed one-way hash function with key $k$, and $E_k(D_k)$ a symmetric encryption (decryption).

In order to construct a group including $n$ members, the manager selects a set of integers, $\varepsilon_i \in_R Z_q$, for $i = 1, 2, \cdots, n$, and computes the coefficients $\alpha_0, \cdots, \alpha_n \in Z_q$ of the following polynomial:

$$f(x) = \prod_{i=1}^{n} (x - \varepsilon_i) = \sum_{i=0}^{n} \alpha_i x^i. \tag{1}$$

Define $g \in Z_p^*$ and $g_i = g^{\alpha_i} \bmod p$, for $i = 0, 1, \cdots, n$, which procedures

$$F(\varepsilon_l) = \prod_{i=0}^{n} g_i^{\varepsilon_l^i} = 1 \bmod p, \tag{2}$$

where $\varepsilon_l$ is an element of the set $\{\varepsilon_i\}$.

This is because $F(\varepsilon_l) = g^{f(\varepsilon_l)}$ and $f(\varepsilon_l) = 0$ in $Z_q$.

In [6], the authors specify incorrectly as $F(\varepsilon_l) = \sum_{i=0}^{n} g_i^{\varepsilon_l^i} = 1 \bmod p$. We correct their errors in our description.

For the given $\{\alpha_0, \alpha_1, \cdots, \alpha_n\}$, a new set is defined as $\{\alpha_0', \alpha_1', \cdots, \alpha_n'\}$, where $\alpha_0' = \alpha_0$, $\alpha_n' = \alpha_n$, $\alpha_1' = \cdots = \alpha_{n-1}' = \sum_{i=1}^{n-1} \alpha_i$. Define $\beta_i = g^{\alpha_i'}$ and $A_l = \sum_{i=1, j=1, i \neq j}^{n-1} \alpha_j \varepsilon_l^i$, then equation (2) can be rewritten as

$$F'(\varepsilon_l) = g^{-A_l} \prod_{i=0}^{n} \beta_i^{\varepsilon_l^i} = g^{-A_l} g^{\sum_{i=0}^{n} \alpha_i' \varepsilon_l^i} = 1 \bmod p. \tag{3}$$