Software Engineering and Applications 软件工程与应用, 2013, 2, 55-61
http://dx.doi.org/10.12677/sea.2013.23010 Published Online June 2013 (http://www.hanspub.org/journal/sea.html)

Cryptanalysis of an Identity-Based Group-Oriented Signcryption Scheme in the Standard Model

Lequn Mo[1,2], Guoxiang Yao[3], Feng Li[1]

[1]Department of Computer Science, Guangdong Communication Polytechnic, Guangzhou
[2]Management School, Jinan University, Guangzhou
[3]College of Information Science, Jinan University, Guangzhou
Email: jason.mok.gz@gmail.com

Received: Apr. 1st, 2013 revised: Apr. 15th, 2013; accepted: Apr. 24th, 2013

Abstract: Group-oriented signcryption is a very useful primitive in the network communication field, which simultaneously provides the functionalities of encryption and signature. Recently, Zhang, Xu, et al. [1] proposed an identity-based group-oriented signcryption scheme and claimed that their scheme is provably secure in a strengthened security model. Unfortunately, by giving concrete attacks, we indicate that this signcryption scheme is not secure under either choose ciphertext attack or choose message attack, in this strengthened security model.

Keywords: Identity-Based; Group-Oriented; Signcryption; Choose Message Attack; CCA

标准模型下一种基于身份的面向群组签密方案的安全性分析

莫乐群[1,2]，姚国祥[3]，李　锋[1]

[1]广东交通职业技术学院计算机工程学院，广州
[2]暨南大学管理学院，广州
[3]暨南大学信息科学技术学院，广州
Email: jason.mok.gz@gmail.com

收稿日期：2013 年 4 月 1 日；修回日期：2013 年 4 月 15 日；录用日期：2013 年 4 月 24 日

摘　要：面向群组的签密方法在现今的网络通信中是一种很有效的数据安全保护手段，它可以在对信息进行个人数字签名的同时对数据进行加密。本文针对 Zhang 和 Xu 等人提出的一种基于身份的面向群组签密方案[1]进行了安全分析，指出该方案存在严重的安全漏洞，并在标准模型下证明该方案无法抵抗择密文攻击以及选择消息攻击的攻击。

关键词：基于身份；面向群组；签密；抗择密文攻击；选择消息攻击

1. 引言

在现今的网络通信中，经常会出现将同一份信息向多个实体发送的情况，如何保证群体中一对多的数据传输安全是一个很重要的研究课题，一种简单的方式就是发送者分别使用各个接受者的公钥进行加密，然后进行点对点传送，显然，这种方法在接收群组规模较大时效率是非常低的，而且发送端的计算压力相当大。

1997 年，Zheng[2]等人首次提出了签密的概念，它指的是在同一个逻辑步骤内同时实现签名和加密

两项功能，是一种同时实现数据保密及信息认证的理想方法。在 2001 年 Boneh 和 Franklin 等人利用双线性对的特点提出了基于身份加密方案[3]之后，基于身份的密码体制得到了迅速的发展和应用，将基于身份密码学与签密进行结合的构造[4]是其中的一个发展方向。2007 年，Duan 等人提出了首个多接收者的基于身份签密方案[5]，他结合 Zheng 等人提出的多接收者签密方案[6]与 Bellare 等人提出的多接收者公钥加密方案[7]相结合，实现仅通过一个对运算就可向多个接收者发送消息，随后出现了大量的基于身份的广播签密方案[8-11]。Zhang 等人为了改善上述方案中出现的一些问题，例如：签密前必须建立专门的接受群体组；必须知道群体各成员的私钥；必须知道接受成员的身份等等，利用双线性映射特点提出了一种基于身份的面向群组签密方案[1]，在该方案中签密者只需对群身份进行信息签密即可让所有接受成员通过各自的私钥进行独立的解签密，另外其参数选择及加密长度可以有效提高计算效率，是一种高效、便捷的安全通信方案。然而，尽管 Zhang 等人对所提出方案在基于 Gentry 等人[12]提出的标准模型下可证安全性进行了论证，但我们发现该方案依然存在严重的安全漏洞，它在基于身份选择密文攻击以及选择消息攻击下是不安全的，并在标准模型下给出了具体的攻击方案。

本文组织如下：第 2 节介绍作为基础知识的双线性对和方案涉及的模型定义；第 3 节是对基于身份的面向群组签密方案的回顾；第 4 节在安全模型下分别给出基于身份选择密文攻击的安全性分析以及基于选择消息攻击安全性分析；第 5 节是结束语；第 6 节是致谢。

2. 预备知识

2.1. 双线性映射(Bilinear Mapping)

设 G_1 和 G_2 为 2 个大素数阶 p 的循环群，存在一个双线性映射 $e:G_1\times G_1\to G_2$，满足以下特性：

- 双线性：$\forall g_1,g_2\in G_1,\forall a,b\in Z_p^*$，有 $e\left(g_1^a,g_2^b\right)=e\left(g_1,g_2\right)^{ab}$；
- 非退化性：存在 $g_1,g_2\in G_1$ 使得 $e\left(g_1,g_2\right)\neq 1_{G_2}$，其中 1_{G_2} 为群组 G_2 的标识；
- 可计算性：存在一个有效算法计算 $e\left(g_1,g_2\right)$ 其中 $\forall g_1,g_2\in G_1$。

2.2. 困难问题及其假设

定义 1：q-ABDHE (augmented bilinear Diffie-Hellmanexponent assumption)困难问题[12]：设 G_1 和 G_2 为 2 个大素数阶 p 的循环群，存在一个双线性映射 $e:G_1\times G_1\to G_2$，给定生成元 $g_1,g_2\in G_1$ 及 $2q+2$ 个元素 $\left(g_1,g_1^{\alpha^{q+2}},g_2,g_2^{\alpha},g_2^{\left(\alpha^2\right)},\cdots,g_2^{\left(\alpha^q\right)},g_2^{\left(\alpha^{q+2}\right)},\cdots,g_2^{\left(\alpha^{2q}\right)}\right)\in G_1^{2q+2}$，则计算 $e\left(g_1,g_2\right)^{\left(\alpha^{q+1}\right)}$ 困难。

定义 2：q-SDH (q-Strong Diffie-Hellmanassumption)困难问题[13]：设 G_1 和 G_2 为 2 个大素数阶 p 的循环群，存在一个双线性映射 $e:G_1\times G_1\to G_2$，给定生成元 $g_1,g_2\in G_1$ 及 $q+2$ 个元素 $\left(g_1,g_2,g_2^{\alpha},g_2^{\left(\alpha^2\right)},\cdots,g_2^{\left(\alpha^q\right)}\right)\in G_1^{q+2}$，其中 $g_1=\psi\left(g_2\right)$，则计算元组 $\left(r,g_1^{1/\alpha+r}\right)$ 困难，其中 $r\in Z_p^*$。

2.3. 基于身份的面向群组签密方案[1]的标准模型

在本章节，我们对基于身份的面向群组签密方案[1](以下简称 IBGSC 方案)的签密模型及安全模型的定义进行说明。

2.3.1. 签密模型的定义

IBGSC 方案由以下四个模块组成：

Setup (k)：系统建立，输入一个安全参数 k，生成系统的运行参数 *params* 及系统密钥 master-key。算法由 PKG 运行，所生成的系统参数 params 包含消息空间 $M\in\{0,1\}^*$ 被公开，而系统密钥 master-key 则被系统保存。

KeyGen (*params*, *master-key*, G_{ID}, *ID*)：私钥提取，输入系统参数 params、系统密钥 master-key、群组身份 $G_{ID}\in\{0,1\}^*$ 以及该群组的成员身份 $ID\in\{0,1\}^*$，其中 G_{ID} 以及 *ID* 均为任意的字符串，算法由 PKG 运行并计算返回群组成员对应的私钥 d_{ID}。

Signcrypt (*params*, m, d_i ,G_j)：签密，输入系统参数 *params*、消息原文 $m\in M$ 、消息接受者所在的群组身份 G_j 及发送者私钥 d_i，算法计算密文 $\sigma=\text{Signacrypt}\left(m,d_i,G_j\right)$ 并广播给接收群组中的所有成员。

Unsigncrypt (*params*, *m*, G_i, d_i)：解签密，输入系统参数 *params*，密文 σ 及密文接受者所在的群组身份 G_i 及私钥 d_i，计算得到原文 $m = \text{Unsigncrypt}(\sigma, d_{ID}, G_{ID})$，若满足正确性约束条件返回 $m \in M$，否则输出 $\perp$。

2.3.2. 安全模型

IBGSC 方案的安全模型由以下两个模型组成：

1) 基于身份选择密文匿名不可区分安全模型 (ANON-IND-IBGSC-CCA)

选择密文匿名不可区分是指敌手不能区分同一密文加密者的身份，即敌手不能判断同一个密文是由所选择的特定身份加密还是由某一随机选择的身份加密的，也就是说密文不会泄露接受者的身份。

Game 1：一个 IBGSC 方案在以下挑战者 *C* 和敌手 *A* 的游戏中，若敌手 *A* 不能在多项式时间内以一个不可忽略的概率 ε 赢得游戏，则该方案满足基于身份选择密文匿名不可区分安全。

- Setup：挑战者 *C* 输入一个特定安全参数 *k* 运行算法，并将所产生的系统参数 params 给敌手，同时保密系统密钥 master-key。
- Phase 1：在该阶段敌手发起询问 $q_1, \cdots, q_m$，其中 q_i 为以下询问：

① KeyGen 询问，敌手 *A* 发送群组消息 G_{ID} 及成员消息 *ID* 给挑战者 *C*，*C* 运行 KeyGen 算法，并将产生的对应 G_{ID} 的私钥 d_{ID} 返回给 *A*。这些询问是适应性的，即每个询问 q_i 都可以依赖于 *C* 对在此之前询问 $q_1, \cdots, q_{i-1}$ 的响应。

② Unsigcrypt 询问，敌手 *A* 将用私钥 d_A 签密的密文 σ 及接受群组信息 G_{ID} 发送给挑战者 *C*，*C* 选择身份 ID_B 计算 $d_B = KeyGen(ID_B, G_{ID})$，并将解密结果 $\text{Unsigncrypt}(\sigma, d_B, G_{ID})$ 返回给 *A*，如果 σ 是一个不合法的密文，输出结果为符号 $\perp$。

- Challenge：敌手 *A* 结束询问后，发送所要挑战的 2 个等长的明文 $M_0, M_1 \in M$，身份 G_{ID_0} 及 G_{ID_1}，并且 G_{ID_0} 及 G_{ID_1} 不能在任何 **KeyGen** 询问中出现过。挑战者 *C* 随机选择比特值 $b, c \in \{0,1\}$，并计算密文 $\sigma = \text{Signacrypt}(m_c, d_A, G_b)$，并将 σ 返回给敌手 *A*。
- Guess：继续重复 Phase 1，但不能做关于 G_{ID_0} 及 G_{ID_1} 的私钥提取询问及签密密文 σ 的解签密询问，最后，敌手 A 猜测结果 $b', c' \in \{0,1\}$。如果 $b = b', c = c'$ 则敌手赢得游戏。

2) 自适应选择消息存在性不可伪造安全模型 (EUF-IBGSC-CMA)

自适应选择消息存在性不可伪造是指抵抗适应性选择消息攻击下的存在性伪造安全，即若除了签名之外的任何消息的都是伪造的，则不会有任何有效的输出。

Game 2：一个 IBGSC 方案在以下挑战者 *C* 和敌手 *A* 的游戏中，若敌手 *A* 不能在多项式时间内以一个不可忽略的概率 ε 赢得游戏，则该方案是满足自适应选择消息攻击下存在性不可伪造的。

- Setup：挑战者 *C* 输入一个特定安全参数 *k* 运行算法，并将所产生的系统参数 params 给敌手，同时保密系统密钥 master-key。
- Phase 1：在该阶段敌手发起询问 $q_1, \cdots, q_m$，其中 q_i 为以下询问：

① KeyGen 询问，敌手 *A* 发送群组消息 G_{ID} 及成员消息 *ID* 给挑战者 *C*，*C* 运行 KeyGen 算法，并将产生的对应 G_{ID} 的私钥 d_{ID} 返回给 *A*. 这些询问是适应性的，即每个询问 q_i 都可以依赖于 *C* 对在此之前询问 $q_1, \cdots, q_{i-1}$ 的响应。

② Sigcrypt 询问，敌手 A 发送签密者身份 ID_A 与明文信息 *m* 给挑战者 *C*，*C* 运行 **Sigcrypt** 计算 $d_A = KeyGen(ID_A, G_{ID_A})$ 及 $\sigma = \text{Signacrypt}(m, d_{ID_A}, G_{ID_A})$，并将签密结果 σ 返回给 *A*。

- Fake：继续重复 Phase 1 至询问结束，最后，敌手发送签密 σ' (签密者密钥 d_B 没有被询问过，密文也没有在签密询问中出现过)给挑战者 *C*，如果解签密结果 $\text{Unsigncrypt}(\sigma', d_B, G_{ID})$ 不为符号 $\perp$，则称敌手赢得游戏。

3. 基于身份的面向群组签密方案介绍

本章节，我们将回顾基于身份的面向群组签密方案的各个算法。

3.1. 各算法回顾

基于身份的面向群组签密方案的具体实现，主要包含以下 4 个算法：

Setup (k)：系统建立，设 G 和 G_T 为 2 个大素数阶 p 的循环群，并存在一个双线性映射 $e:G_1\times G_1\to G_2$，PKG 随机选择生成元 $g,h\in G$，令无碰撞的散列函数 H 满足 $H:\{0,1\}^*\to Z_p$，然后 PKG 随机选择系统密钥 $\text{masker-key}=\alpha\in Z_p$，计算 $g_1=g^\alpha\in G$，并公布系统参数 $\text{params}(g,g_1,h)$。

KeyGen (*params*, *master-key*, G_{ID}, *ID*)：私钥提取，PKG 接收群组身份 G_{ID} 和成员个体身份 *ID*，随机选择 $r_{ID}\in Z_p$，并计算 $R_{ID}=r_{ID}H(ID)$，然后输出个体私钥 $d_{ID}=(r_{ID},h_{ID})$，其中 $h_{ID}=\left(hg^{-R_{ID}}\right)^{1/(\alpha-H(G_{ID}))}$。该算法可以在任何时间执行，以适应发送/接收群组成员的动态变化。不失一般性，设群组 G_{ID} 成员 ID_A 为消息发送者 A，成员 $\{ID_{B_i}\}_{i=(1,\cdots,n)}$ 为接收者 B_i，他们的私钥分别为：

$$d_A=(r_A,h_A)=\left(r_A,\left(hg^{-R_A}\right)^{1/(\alpha-H(G_{ID}))}\right)=\left(r_A,\left(hg^{-r_AH(ID_A)}\right)^{1/(\alpha-H(G_{ID}))}\right)$$

$$d_{B_i}=\left(r_{B_i},h_{B_i}\right)=\left(r_{B_i},\left(hg^{-R_{B_i}}\right)^{1/(\alpha-H(G_{ID}))}\right)=\left(r_{B_i},\left(hg^{-r_{B_i}H\left(ID_{B_i}\right)}\right)^{1/(\alpha-H(G_{ID}))}\right)$$

Signcrypt (*params*, *m*,d_i ,G_i)：签密，签密者 A 为将明文消息 $m\in M$ 发送给接收群组 G_{ID} 中的所有成员，随机选择 $s\in Z_p$，并如下计算签密密文 $\sigma=(u,v,w,\delta,\varphi)$：

$$u=g_1^sg^{-sH(G_{ID})},v=e(g,g)^s,w=m\cdot e(g,h)^{-s},\delta=h_A^{H(m)},\varphi=r_A$$

Unsigncrypt (*params*, *m*, G_i, d_i)：解签密，信息接受群组 G_{ID} 成员 $\{ID_{B_i}\}_{i=(1,\cdots,n)}$ 要解密签密密文 $\sigma=(u,v,w,\delta,\varphi)$，只需计算 $m=w\cdot e\left(u,h_{B_i}\right)v^{r_{B_i}H\left(ID_{B_i}\right)}$ 即可，若约束条件验证等式

$$e(u,\delta)v^{H(m)\varphi H(ID)}w^{H(m)}=m^{H(m)}$$

成立，输出信息 m，否则输出 $\perp$。

3.2 算法正确性[1]

通过下面的推导可以得出签密方案是正确的：

$$e(u,\delta)=e\left(g_1^sg^{-sH(G_{ID})},h_A^{H(m)}\right)=e\left(g^{s(\alpha-H(G_{ID}))},\left(hg^{-R_A}\right)^{\frac{H(m)}{\alpha-H(ID_A)}}\right)$$

$$=e\left(g^s,h^{H(m)}g^{-R_AH(m)}\right)=e\left(g^s,h^{H(m)}\right)\cdot e\left(g^s,g^{-R_AH(m)}\right)$$

$$=e(g,h)^{sH(m)}e(g,g)^{-sR_AH(m)}=e(g,h)^{sH(m)}e(g,g)^{-sH(m)r_AH(ID_A)}$$

$$e(u,\delta)v^{H(m)\varphi H(ID)}w^{H(m)}=e(u,\delta)\cdot e(g,g)^{sH(m)r_AH(ID_A)}m^{H(m)}\cdot e(g,h)^{-sH(m)}=m^{H(m)}$$

4. 对 Zhang 和 Xu 等人方案的安全性分析

Zhang 和 Xu 等人认为他们所提出的方案对于身份选择密文攻击以及选择消息攻击下是可证安全的，但在本章节中，我们将会在标准模型下证明这两种攻击依然可行。

4.1. 基于身份选择密文攻击的安全性分析

Zhang 和 Xu 等人认为他们所提出的方案在基于身份选择密文匿名不可区分安全模型(ANONIND-IBGSC-CCA)下是语义安全的，但实际上却存在敌手 A 可以通过以下方式一直赢得 Game 1：

- Setup：挑战者 C 输入一个特定安全参数 k 运行算法，将所产生的系统参数 params 给敌手 A，同时保密系统密钥 master-key。
- Phase 1：敌手 A 不做任何询问。
- Challenge：敌手 A 结束询问后，发送所要挑战的 2 个等长的明文 $M_0,M_1\in M$，身份 G_{ID_0} 及 G_{ID_1}，并且 G_{ID_0} 及 G_{ID_1} 不能在任何 KeyGen 询问中出现过。挑战者 C 随机选择比特值 $b,c\in\{0,1\}$，并计算密文

$\sigma = \text{Signacrypt}(m_c, d_A, G_b)$，并将 $\sigma = (u, v, w, \delta, \varphi)$ 返回给敌手 A，其中

$$u = g_1^s g^{-sH(G_{ID})}, v = e(g,g)^s, w = m \cdot e(g,h)^{-s}, \delta = h_A^{H(m)}, \varphi = r_A$$

- Guess：敌手 A 随机选择 $s' \in Z_p$ 构造密文 $\sigma' = (u', v', w', \delta', \varphi')$ 及 $\sigma^* = (u', v', w^*, \delta', \varphi')$，其中：

$$\begin{aligned} &u' = u^{s'} = g_1^{s \cdot s'} g^{-s \cdot s' H(G_{ID})} = g^{s \cdot s'(\alpha - H(G_{ID}))}, \\ &v' = v^{s'} = e(g,g)^{s \cdot s'}, w' = w^{s'} / M_0^{s'-1} = m^{s'} \cdot e(g,h)^{-s \cdot s'} / M_0^{s'-1}, \\ &w^* = w^{s'} / M_0^{s'-1} = m^{s'} \cdot e(g,h)^{-s \cdot s'} / M_1^{s'-1} \delta' = \delta = h_A^{H(m)}, \varphi' = \varphi = r_A. \end{aligned}$$

构造完成后，敌手 A 发出关于 σ' 及 σ^* 的 **Unsigcrypt** 询问，由于 $\sigma' \neq \sigma$ 且 $\sigma^* \neq \sigma$ 所以，挑战者 C 首先根据公式 $m = w \cdot e(u, h_A) v^{r_A H(ID_A)}$ 进行解签密，可得 σ' 的解签密明文为：

$$\begin{aligned} &m' = w' \cdot e(u', h_A) v'^{r_A H(ID_A)} \\ &= m^{s'} / M_0^{s'-1} \cdot e(g,h)^{-s \cdot s'} e\left(g^{s \cdot s'(\alpha - H(G_{ID}))}, \left(h g^{-R_A} \right)^{\frac{1}{\alpha - H(ID)}} \right) e(g,g)^{s \cdot s' \cdot r_A H(ID)} \\ &= m^{s'} / M_0^{s'-1} \cdot e(g,h)^{-s \cdot s'} e(g,h)^{-s \cdot s'} e(g,g)^{-s \cdot s' r_A H(ID_A)} e(g,g)^{s \cdot s' \cdot r_A H(ID)} = m^{s'} / M_0^{s'-1} \end{aligned}$$

同理，σ^* 的解签密明文为：

$$m^* = w^* \cdot e(u', h_A) v'^{r_A H(ID)} = m^{s'} / M_1^{s'-1}$$

然后，挑战者 C 会根据约束条件

$$e(u, \delta) v^{H(m) \varphi H(ID)} w^{H(m)} = m^{H(m)}$$

进行检验，检验结果如下：

1) 若 $m = M_0$，则 $m' = m, \delta' = h_A^{H(m')}$ 并且 m' 可以通过下面约束条件的检验：

$$\begin{aligned} &e(u', \delta') v'^{H(m') \varphi H(ID)} w'^{H(m')} \\ &= e(u', \delta') \cdot e(g,g)^{s \cdot s' H(m') r_A H(ID_A)} m'^{H(m')} \cdot e(g,h)^{-s \cdot s' H(m')} = m'^{H(m')} = m^{H(m)} \end{aligned}$$

2) 若 $m = M_1$，则 $m^* = m, \delta' = h_A^{H(m^*)}$ 并且 m^* 可以通过下面约束条件的检验：

$$\begin{aligned} &e(u', \delta') v'^{H(m^*) \varphi H(ID)} w'^{H(m^*)} \\ &= e(u', \delta') \cdot e(g,g)^{s \cdot s' H(m^*) r_A H(ID)} m^{*H(m^*)} e(g,h)^{-s \cdot s' H(m^*)} = m^{*H(m^*)} = m^{H(m)} \end{aligned}$$

所以对于敌手 A 的两个解签密请求 (σ', σ^*)，挑战者 C 将会返回结果 $(m, \perp)$ 或者 $(\perp, m)$，则敌手 A 可以根据解签密结果猜测出 $c' \in \{0,1\}$，使得 $m_{c'} = m_c$。

然后敌手 A 再次构造签密密文 $\sigma'' = (u'', v'', w'', \delta'', \varphi'')$ 及 $\sigma^{**} = (u^{**}, v'', w'', \delta'', \varphi'')$，其中：

构造完成后，敌手 A 再次发出关于 σ'' 及 σ^{**} 的解

$$\begin{aligned} &u'' = u \cdot g^{s'} g^{-s' H(G_{ID_0})} = g_1^{s+s'} g^{-sH(G_{ID})} g^{-s'(\alpha - H(G_{ID_0}))} \\ &v'' = v \cdot e(g,g)^{s'} = e(g, g^s) \cdot e(g, g^{s'}) = e(g, g^s g^{s'}) = e(g,g)^{s+s'} \\ &w'' = w \cdot e(g,h)^{-s'} = m \cdot e(g, h^{-s}) e(g, h^{-s'}) = m \cdot e(g,h)^{-(s+s')} \\ &\delta'' = \delta = h_A^{H(m)}, \varphi'' = \varphi = r_A \\ &u^{**} = u \cdot g^{s'} g^{-s' H(G_{ID_1})} = g_1^{s+s'} g^{-sH(G_{ID})} g^{-s'(\alpha - H(G_{ID_1}))} \end{aligned}$$

签密询问，由于 $\sigma'' \neq \sigma$ 且 $\sigma^{**} \neq \sigma$ 所以，挑战者 C 首先根据公式 $m = w \cdot e(u, h_A) v^{r_A H(ID_A)}$ 进行解签密：

1) 若 $G_{ID} = G_{ID_0}$，则

$u'' = g_1^{s+s'} g^{-(s+s')H(G_{ID})} = g^{(s+s')(\alpha - H(G_{ID}))}$ 并且可得 σ'' 的解签密明文：

$$\begin{aligned} m'' &= w'' \cdot e(u'', h_A) v''^{r_A H(ID_A)} \\ &= m \cdot e(g,h)^{-(s+s')} e\left(g^{(s+s')(\alpha - H(G_{ID}))}, \left(hg^{-R_A}\right)^{\frac{1}{\alpha - H(ID)}} \right) e(g,g)^{(s+s') \cdot r_A H(ID)} = m \end{aligned}$$

这里显然 $e(u'', \delta'') v''^{H(m'')\varphi H(ID)} w''^{H(m'')} = m^{H(m)}$

2) 若 $G_{ID} = G_{ID_1}$，则

$u^{**} = g_1^{s+s'} g^{-(s+s')H(G_{ID})} = g^{(s+s')(\alpha - H(G_{ID}))}$ 并且可得 σ^{**} 的解签密明文：

$$\begin{aligned} m^{**} &= w'' \cdot e(u'', h_A) v''^{r_A H(ID)} \\ &= m \cdot e(g,h)^{-(s+s')} e\left(g^{(s+s')(\alpha - H(G_{ID}))}, \left(hg^{-R_A}\right)^{\frac{1}{\alpha - H(ID)}} \right) e(g,g)^{(s+s') \cdot r_A H(ID)} = m \end{aligned}$$

这里显然 $e(u^{**}, \delta'') v''^{H(m^{**})\varphi H(ID)} w''^{H(m^{**})} = m^{H(m)}$

所以对于敌手 A 的两个解签密请求 (σ'', σ^{**})，挑战者 C 将会返回结果 $(m, \perp)$ 或者 $(\perp, m)$，则敌手 A 可以根据解签密结果猜测出 $b' \in \{0,1\}$，使得 $G_{b'} = G_b$。

综上，敌手 A 将赢得 Game 1。

4.2. 选择消息攻击的安全性分析

Zhang 和 Xu 等人认为他们所提出的方案在自适应选择消息存在性不可伪造安全模型(EUF-IBG-SC-CMA)下是语义安全的，但实际上却存在敌手 A 可以通过以下方式一直赢得 Game 2：

- Setup：挑战者 C 输入一个特定安全参数 k 运行算法，并将所产生的系统参数 params 给敌手 A，同时保密系统密钥 master-key。
- Phase 1：敌手 A 做一次 KeyGen 询问及关于明文信息 $m \in M$ 的 Sigcrypt 询问，得到私钥 $d_A = (r_A, h_A) = \left(r_A, \left(hg^{-R_A}\right)^{1/(\alpha - H(G_{ID}))} \right)$ 及签密密文 $\sigma = (u, v, w, \delta, \varphi)$，其中：

$$u = g_1^s g^{-sH(G_{ID})}, v = e(g,g)^s, w = m \cdot e(g,h)^{-s}, \delta = h_A^{H(m)}, \varphi = r_A$$

- Guess：敌手 A 进行 KeyGen 询问,得到 $d_B = (r_B, h_B) = \left(r_B, \left(hg^{-R_B}\right)^{1/(\alpha - H(G_{ID}))} \right)$，

并随机选择 $r' \in Z_p$ 构造密文 $\sigma' = (u', v', w', \delta', \varphi')$，其中：

$$\begin{aligned} u' &= u^{r'} = g_1^{s \cdot r'} g^{-s \cdot r' H(G_{ID})} = g^{s \cdot r'(\alpha - H(G_{ID}))} \\ v' &= v^{r'} = e(g,g)^{s \cdot r'} \\ w' &= w^{r'} = m^{r'} e(g,h)^{-s \cdot r'} \\ \delta' &= \delta = h_B^{H(m)}, \varphi' = \varphi = r_B \end{aligned}$$

构造完成后，敌手 A 发出关于 σ' 的解签密询问，由于 $\sigma' \neq \sigma$ 所以，挑战者 C 首先根据公式 $m = w \cdot e(u, h_B) v^{r_A H(ID_B)}$ 进行解签密，可得 σ' 的解签密明文为：

$$\begin{aligned} m' &= w' \cdot e(u', h_B) v'^{r_A H(ID_B)} \\ &= m^{r'} \cdot e(g,h)^{-s \cdot r'} e\left(g^{s \cdot r'(\alpha - H(G_{ID}))}, \left(hg^{-R_B}\right)^{\frac{1}{\alpha - H(G_{ID})}} \right) e(g,g)^{s \cdot r' \cdot r_B H(ID_B)} = m^{r'} \end{aligned}$$

对于约束条件 $e(u,\delta)v^{H(m)\varphi H(ID)}w^{H(m)}=m^{H(m)}$ 检验，显然有：

$$\begin{aligned}&e(u',\delta')v'^{H(m')\varphi H(ID)}w'^{H(m')}\\&=e(u',\delta')\cdot e(g,g)^{s\cdot r'H(m')r_BH(ID_B)}m'^{H(m')}\cdot e(g,h)^{-s\cdot r'H(m')}\\&=e\left(g^{s\cdot r'(\alpha-H(G_{ID}))},\left(hg^{-R_B}\right)^{\frac{H(m')}{\alpha-H(G_{ID})}}\right)e(g,g)^{s\cdot r'R_B}m'^{H(m')}\cdot e(g,h)^{-s\cdot r'H(m')}=m'^{H(m')}\end{aligned}$$

所以挑战者 C 将返回明文 $m^{r'}$ 给敌手 A，并且 $m^{r'}\neq\perp$。

综上，根据安全模型，敌手 A 将会赢得 Game 2。

综合上述在标准模型下对两个安全模型进行挑战的结果，敌手可以轻易赢得 Game，该面向群组的签密方案是不安全的，并由于安全模型已经被攻破，所以也已没有改进方案的必要了，除非是提出一个完全全新的方案。

5. 结束语

本文中，我们指出了 Zhang 和 Xu 等人所提出的基于身份的面向群组签密方案存在严重的安全隐患，他们对于基于身份选择密文攻击以及选择消息攻击是不安全的。根据该方案的所提出的安全模型，我们还给出了具体的攻击方案。

6. 致谢

这里，我们要感谢各位审稿专家认真的审阅及各种帮助性的建议。本文获得了国家自然科学基金项目(61272415，61272413，61133014)，广东省自然科学基金项目(S2011010002708)，广东省科技计划项目(2010A011200038，2011B090400324)，广东省工程研究中心专项(GCZX-A1103)，广州市科技计划项目(2011J4300047)的资助。

参考文献 (References)

[1] 张波, 徐秋亮. 基于身份的面向群组签密方案[J]. 通信学报, 2009, 30(11): 23-28.

[2] Y. L. Zheng. Digital signcryption or how to achieve cost (signature & encryption) << cost (signature) + cost (encryption). Lecture Notes in Computer Science 1294, Berlin: Springer-Verlag, 1997: 165-179.

[3] D. Boneh, M. Franklin. Identity based encryption from the weilpairing. Lecture Notes in Computer Science 2139, Berlin: Springer-Verlag, 2001: 213-229.

[4] J. Malone. Identity based Signcryption Cryptology ePrint Archive. Report 2002/098, 2002.

[5] S. S. Duan, Z. F. Cao. Efficient and provably secure multi-receiveridentity-based signcryption. ACISP 2006. Lecture Notes in Computer Science 4058, Berlin: Springer-Verlag, 2006: 195-206.

[6] Y. L. Zheng. Signcryption and its applications in efficient public keysolutions. ISW 1997. Lecture Notes in Computer Science 1396, Berlin: Springer-Verlag, 1998: 291-312.

[7] M. Bellare, A. Boldyreva and S. Micali. Public-key encryption ina multi-user setting: Security proofs and improvements. Advancesin Cryptology-EUROCRYPT 2000. Lecture Notes in Computer Science 1807, Berlin: Springer-Verlag, 2000: 259-274.

[8] Y. Yu, B. Yang, X. Y. Huang, et al. Efficient identity-based signcryptionscheme for multiple receivers. ATC 2007. Lecture Notes in Computer Science 4610. Berlin: Springer-Verlag, 2007: 13-21.

[9] M. J. Bohio, A. Miri. An authenticated broadcasting scheme for wirelessad hoc network. 2nd Annual Conference on Communication Networks and Services Research (CNSR). 2004: 69-74.

[10] Y. Mu, W. Susilo and Y. X. Lin. Identity-based authenticated broadcast encryption and distributed authenticated encryption. Advances in Computer Science—ASIAN 2004: Proceedings of the 9th Asian Computing Science Conference. Lecture Notes in Computer Science 3321. Berlin: Springer-Verlag, 2004: 169-181.

[11] F. G. Li, X. G. Xin and Y. P. Hu. Identity based broadcast signcryption. Computer Standards and Interfaces, 2008, 30(1-2): 89-94.

