一种高效群签名方案的密码学分析

谢 琪
(杭州师范学院信息工程学院 杭州 310036)

摘 要：2005 年，张键红等提出了一种基于 RSA 的高效群签名方案，签名与验证的计算量只需要 9 次模幂乘运算。该文提出了一种伪造攻击方案指出张等的方案是不安全的，任一群成员在撤消中心的帮助下可以不利用自己的秘密参数对任何消息生成有效的群签名。同时，指出了群成员的识别算法是错误的，身份追踪式是与具体签名无关的常量，即身份追踪算法无法追踪到真实的签名者。最后，指出了他们的方案具有关联性。

关键词：群签名；RSA；密码学
中图分类号：TN918.2 **文献标识码**：A **文章编号**：1009-5896(2007)06-1511-03

Cryptanalysis of an Efficient Group Signature Scheme

Xie Qi
(*School of Information and Engineering*, *Hangzhou Teachers College*, *Hangzhou* 310036, *China*)

Abstract: In 2005, Zhang et al. proposed an efficient group signature scheme based on RSA, the total computation cost of signature and verification requires only 9 modular exponentiations. This paper will show that Zhang et al.'s scheme is insecure, any group member colludes with repeal center can generate a valid group signature without using his secret parameters. Additional, it will show that the signer identity verification algorithm is error, identity verification expression is independent of the group signature. That is, the signer identity verification algorithm cannot find who the signer is. Finally, it will show that their scheme is not unlinkable.

Key words: Group signature; RSA; Cryptography

1 引言

1991 年，Chaum 和Van Heyst[1]第一次提出了群签名的概念, 群签名允许群中的任一合法成员代表群对消息进行匿名地签名，如果事后发生争执，群管理员能够打开签名来揭示签名者的真实身份，而验证者能够利用群公钥来验证群签名的正确性。由于群签名在电子现金、电子投票等领域有重要的应用，从而一提出便引起了许多研究者的广泛的注意和深入的研究。

通常的群签名必须满足下列性质：

(1)只有群成员才可以代表整个群体对消息进行签名；

(2)群成员匿名的签发消息；

(3)其他群成员、群管理员、其他群成员的合谋、其他群成员与群管理员合谋都无法伪造一个群成员的合法签名；

(4)一旦发生纠纷，群管理员可以打开群签名识别出真实的签名者。

(5)一旦某个群签名被打开，任何非法攻击者无法找到该成员先前的签名和以后的签名。

(6)群成员可以随意的加入或退出。

然而设计安全高效的群签名方案是个十分困难的问题。现有的群签名方案大多存在以下一个或若干个问题:

(1)伪造攻击和合谋攻击是对群签名十分有效的攻击方法。从文献[2–5]中可知，有些方案存在全局伪造性、有些方案无法抵抗部分成员的合谋攻击、有些方案追查不到伪造者的身份。

(2) 签名者身份的追查效率不高，而且签名者的身份具有链接性。从文献 [2, 6–8]中可知，有些方案在追查签名者身份时需要用群成员的公钥逐个验证身份追查方程，当群成员数比较多时，计算量比较大。有些方案中，一旦某个群签名被打开，任何非法攻击者能找到该成员先前的签名和以后的签名。

(3) 群签名的计算量、通信量和签名长度远远大于一般的数字签名，所以效率低，只有理论上的意义，实用性差。

(4) 群成员的撤销与成员数成线性关系，其系统更新效率低。

目前公认的比较好的方案是Ateniese等[9]提出的基于知识的群签名方案，遗憾的是该方案参数众多，效率不高。2005 年，张键红等[10]提出了一种基于RSA的高效群签名方案，签名与验证的计算量只需要 9 次模幂乘运算。该群签名方案由 3 个实体群管理员、撤消中心和群成员组成，他们假设群管理员和撤消中心不互相合谋的话，该方案是安全的。本文提出了一种伪造攻击方案指出张键红等的方案是不安全的，任一群成员在撤消中心的帮助下可以不利用自己的秘密参数

2005-08-23 收到; 2006-06-20 改回
国家自然科学基金(10271037)和浙江省自然科学基金(Y105067)资助课题

对任何消息生成有效的群签名，从而签名者的身份不会被追踪到。同时，指出了群成员的识别算法是错误的，身份追踪式是与具体签名无关的常量，即身份追踪算法无法追踪到真实的签名者。最后，指出他们的方案不具有不相关性。

2 一种高效的群签名方案简介

一种高效的群签名方案由系统初始化、群成员的加入、群签名的产生、群签名的验证、群成员的识别 5 个阶段组成。

2.1 系统初始化

该群签名方案由 3 个实体：群管理员 GM, 撤消中心 RC 和群成员 B_i 组成(下面的过程以群成员 Bob 为例)。首先，RC 选取 5 个大素数 p_1,p_2,f,p_1',p_2'，且满足 $p_1=2fp_1'+1$ 和 $p_2=2fp_2'+1$，计算 $n_C=p_1p_2$，RC 的 RSA 公钥和私钥对为 $(e_{\mathrm{RC}},d_{\mathrm{RC}})$，$g$ 是 $Z_{n_C}^*$ 中阶为 f 的元素，$h(\cdot)$ 是单向抗碰撞 Hash 函数，RC 公开参数 $(n_C,f,g,e_{\mathrm{RC}},h(\cdot),\mathrm{ID}_{\mathrm{RC}})$，其中 $\mathrm{ID}_{\mathrm{RC}}$ 是 RC 的身份。$\mathrm{SPK}[\gamma:y=g^{\gamma}](m)$ 表示 y 对 g 的知识签名。

其次，GM 选取 2 个大素数 p_3,p_4，且 p_3-1 和 p_4-1 含有大素因子，计算 $n_G=p_3p_4$，GM 的 RSA 公钥和私钥对为 (e_G,d_G)，离散对数公钥和私钥对为 (y_G,x_G)，公开参数 (n_G,y_G,e_G,ID_G)，其中 ID_G 是 GM 的身份。

2.2 群成员的加入

群成员不妨设 Bob 要加入群，他随机选择一个数 $k\in Z_f^*$，秘密保存 k，并计算其身份 $\mathrm{ID}_B=g^k \bmod n_C$ 和 $\delta=\mathrm{SPK}[\gamma:\mathrm{ID}_B=g^{\gamma}](m)$，并把二元组 (ID_B,δ) 发送给 GM，其目的是向群成员证明他知道秘密值 k 和提交身份。GM 首先通过 (ID_B,δ) 验证知识签名的正确性。其次，随机选择一个数 $\alpha\in Z_f^*$，并为 Bob 计算他的成员资格证书：

$$r_G=g^{\alpha} \bmod n_C,\quad s_G=\alpha+r_Gx_Gh(\mathrm{ID}_B) \bmod f,$$
$$w_G=(\mathrm{ID}_G)^{-d_G} \bmod n_G$$

并通过秘密信道把 (s_G,r_G,w_G) 发送给 Bob，把 $(\mathrm{ID}_B,g^{s_G},r_G)$ 发送给 RC。Bob 通过 $g^{s_G}=r_Gy_G^{r_Gh(\mathrm{ID}_B)} \bmod n_C$ 和 $\mathrm{ID}_G=(w_G)^{-e_G} \bmod n_G$ 来验证成员资格证书 (s_G,r_G,w_G) 的正确性；RC 通过 $g^{s_G}=r_Gy_G^{r_Gh(\mathrm{ID}_B)} \bmod n_C$ 来验证 Bob 是合法的群成员，同时计算 $w_C=(\mathrm{ID}_{\mathrm{RC}}r_Gy_G^{r_Gh(\mathrm{ID}_B)}\mathrm{ID}_B)^{-d_{\mathrm{RC}}} \bmod n_C$ 并发送给 Bob，在群成员数据库中存储 $(w_C,\mathrm{ID}_B,g^{s_G},r_G)$。Bob 通过验证 $w_C{}^{-e_{\mathrm{RC}}}=(\mathrm{ID}_{\mathrm{RC}}r_Gy_G^{r_Gh(\mathrm{ID}_B)}\mathrm{ID}_B) \bmod n_C$ 来确定 w_C 的正确性，如果成立，则 Bob 的成员资格证书为 (s_G,r_G,w_G,w_C)。

2.3 群签名的产生

群成员 Bob 想对消息 m 产生群签名，他利用资格证书 (s_G,r_G,w_G,w_C) 执行下列步骤，任取 $q_1,q_2,q_3\in Z_f^*$，计算 $z_1=q_3^{e_{\mathrm{RC}}}g^{q_1} \bmod n_C$，$z_2=q_2^{e_G} \bmod n_G$，$u=h(z_1,z_2,m)$，$r_1=q_1+(s_G+k)u \bmod f$，$r_2=q_3w_C^u \bmod n_C$，$r_3=q_2w_G^u \bmod n_G$，最后所得的群签名为 (u,r_1,r_2,r_3,m)。

2.4 群签名的验证

验证者收到群签名 (u,r_1,r_2,r_3,m) 后，计算 $z_1'=\mathrm{ID}_{\mathrm{RC}}^ug^{r_1}r_2^{e_{\mathrm{RC}}} \bmod n_C$，$z_2'=\mathrm{ID}_G^ur_3^{e_G} \bmod n_G$，$u'=h(z_1',z_2',m)$，并判断 $u=u'$ 是否成立来确定群签名的合法性。

2.5 群成员的识别

由于 RC 保存着群成员的信息 $(w_C,\mathrm{ID}_B,g^{s_G},r_G)$，一旦群成员对某个群签名 (u,r_1,r_2,r_3,m) 有争执，RC 可以通过下面的步骤追查出真实的签名者，他计算 $\eta=(1/u) \bmod \varphi(n_C)$，$\delta=\mathrm{ID}_{\mathrm{RC}}^ug^{r_1} \bmod n_C$，$\mathrm{ID}_B=\dfrac{[g^{r_1}/(\delta g^{us_G})]^{\eta}}{w_C^{e_{\mathrm{RC}}}} \bmod n_C$，满足上式的 (ID_B,g^{s_G}) 所对应的成员即为真实签名者。

3 密码学分析

本节提出了一种伪造攻击方案指出张键红等方案是不安全的，任一群成员在撤消中心 RC 的帮助下可以不利用自己特有的资格证书、对任何消息生成有效的群签名，从而无法追踪到签名者的真实身份。同时，指出了群成员的识别算法是错误的，群签名的身份追踪式是一个与具体群签名无关的常量。最后，指出他们的方案不具有不相关性。

3.1 伪造攻击

Bob 在撤消中心 RC 的帮助下，可以不利用自己特有的资格证书 (s_G,r_G,k,w_C) 产生消息 m 的有效群签名 (u,r_1,r_2,r_3,m)，而且不会被追踪到。

步骤 1 Bob 任取 $r_1,q\in Z_f^*$，计算 $z_1=g^{r_1} \bmod n_C$，$z_2=q^{e_G} \bmod n_G$，$u=h(z_1,z_2,m)$，$r_3=qw_G^u \bmod n_G$，然后把 u 发送给 RC。

步骤 2 RC 计算 $r_2=\mathrm{ID}_{\mathrm{RC}}^{-ud_{\mathrm{RC}}} \bmod n_C$，并把 r_2 发送给 Bob。Bob 得到关于消息 m 的有效群签名 (u,r_1,r_2,r_3,m)，因为

$$z_1'=\mathrm{ID}_{\mathrm{RC}}^ug^{r_1}r_2^{e_{\mathrm{RC}}}=\mathrm{ID}_{\mathrm{RC}}^ug^{r_1}(\mathrm{ID}_{\mathrm{RC}}^{-ud_{\mathrm{RC}}})^{e_{\mathrm{RC}}}=g^{r_1}=z_1 \bmod n_C,$$
$$z_2'=\mathrm{ID}_G^ur_3^{e_G}=\mathrm{ID}_G^u(qw_G^u)^{e_G}=\mathrm{ID}_G^u(q((\mathrm{ID}_G)^{-d_G})^u)^{e_G}=q^{e_G}$$
$$=z_2 \bmod n_G,$$

所以，$u'=h(z_1',z_2',m)=h(z_1,z_2,m)=u$，伪造攻击成功。

显然，在上述的伪造过程中，Bob 没有利用自己特有的资格证书 (s_G,r_G,k,w_C)，仅用到 w_G，而 $w_G=(\mathrm{ID}_G)^{-d_G} \bmod n_G$ 是一个不包含群成员个人信息的常量，所有群成员拥有的 w_G 是一样的，所以伪造的群签名中不包含签名者的个人信息，所以无法追踪到真实的签名者。

3.2 身份识别算法分析

下面指出张键红等的方案中群成员的身份识别算法是错误的，群签名的身份追踪式是一个与具体群签名无关的常量，也就是说，对任一有效的群签名，利用该算法追查真实的签名者，所有的群成员都可能是真实的签名者。

因为对某个群签名 (u,r_1,r_2,r_3,m)，考虑到 $\eta=(1/u) \bmod \varphi(n_C)$，$\delta=\mathrm{ID}_{\mathrm{RC}}^ug^{r_1} \bmod n_C$，所以，$\dfrac{[g^{r_1}/(\delta g^{us_G})]^{\eta}}{w_C^{e_{\mathrm{RC}}}}=\dfrac{[g^{r_1}/(\mathrm{ID}_{\mathrm{RC}}^ug^{r_1}g^{us_G})]^{\eta}}{w_C^{e_{\mathrm{RC}}}}=\dfrac{w_C{}^{-e_{\mathrm{RC}}}}{\mathrm{ID}_{\mathrm{RC}}g^{s_G}} \bmod n_C$，也就是说，$\dfrac{[g^{r_1}/(\delta g^{us_G})]^{\eta}}{w_C^{e_{\mathrm{RC}}}}$ 是一个与具体的群签名 (u,r_1,r_2,r_3,m)

无关的常量 $\frac{w_C^{-e_{\mathrm{RC}}}}{\mathrm{ID}_{\mathrm{RC}}g^{s_G}}$，任何群成员的资格证书都满足该追踪式。

例如，另一个群成员 Bom 的身份是 ID_B'，其资格证书为 (s_G', r_G', w_G, w_C')，其中 $r_G' = g^{\alpha'} \bmod n_C$，$s_G' = \alpha' + r_G' x_G h(\mathrm{ID}_B') \bmod f$, $w_G' = (\mathrm{ID}_{\mathrm{RC}} r_G' y_G^{r_G' h(\mathrm{ID}_B')} \cdot \mathrm{ID}_B')^{-d_{\mathrm{RC}}} \bmod n_C$，RC 保存着他的信息 $(w_C', \mathrm{ID}_B', g^{s_G'}, r_G')$。则对 Bob 产生的群签名 (u, r_1, r_2, r_3, m)，RC 会错误地认为 Bom 也是真实的签名者，因为

$$\frac{[g^{r_1}/(\delta g^{us_G'})]^{\eta}}{(w_C')^{e_{\mathrm{RC}}}} = \frac{[g^{r_1}/\mathrm{ID}_{\mathrm{RC}}^{u} g^{r_1} g^{us_G'}]^{\eta}}{(w_C')^{e_{\mathrm{RC}}}} = \frac{\mathrm{ID}_{\mathrm{RC}} r_G' y_G^{r_G' h(\mathrm{ID}_B')} \mathrm{ID}_B'}{\mathrm{ID}_{\mathrm{RC}} g^{s_G'}}$$
$$= \frac{g^{s_G'} \mathrm{ID}_B'}{g^{s_G'}} = \mathrm{ID}_B' \bmod n_C$$

3.3 不相关性分析

不妨设 Bob 产生了两个群签名 (u, r_1, r_2, r_3, m) 和 $(u', r_1', r_2', r_3', m')$，一旦有人知道群签名 (u, r_1, r_2, r_3, m) 是由 Bob 产生的，则他首先如验证过程一样计算 $z_1 = \mathrm{ID}_{\mathrm{RC}}^{u} g^{r_1} r_2^{e_{\mathrm{RC}}} \bmod n_C$ 和 $z_1' = \mathrm{ID}_{\mathrm{RC}}^{u'} g^{r_1'} (r_2')^{e_{\mathrm{RC}}} \bmod n_C$，然后通过检查

$$(g^{r_1'} r_2'^{\,e_{\mathrm{RC}}} (z_1')^{-1})^{u} = (g^{r_1} r_2^{e_{\mathrm{RC}}} z_1^{-1})^{u'} \bmod n_C$$

是否成立来确定 $(u', r_1', r_2', r_3', m')$ 是否由 Bob 产生。正确性证明如下：

由群签名的产生过程可知，$z_1 = q_3^{e_{\mathrm{RC}}} g^{q_1} \bmod n_C$，$g^{r_1} = g^{q_1} (g^{s_G} \mathrm{ID}_B)^{u} \bmod n_C$，$r_2^{e_{\mathrm{RC}}} = (q_3 w_C)^{e_{\mathrm{RC}} u} \bmod n_C$，所以，

$$g^{r_1} r_2^{e_{\mathrm{RC}}} z_1^{-1} = g^{q_1} (g^{s_G} \mathrm{ID}_B)^{u} (q_3 w_C)^{e_{\mathrm{RC}} u} (q_3^{e_{\mathrm{RC}}} g^{q_1})^{-1}$$
$$= (g^{s_G} \mathrm{ID}_B w_C^{e_{\mathrm{RC}}})^{u} \bmod n_C$$

由于对同一个群成员而言，每次产生不同的群签名时 $g^{s_G} \mathrm{ID}_B w_C^{e_{\mathrm{RC}}}$ 是个不变的常量，所以对两个不同的群签名 (u, r_1, r_2, r_3, m) 和 $(u', r_1', r_2', r_3', m')$，可以通过检查

$$(g^{r_1'} r_2'^{\,e_{\mathrm{RC}}} (z_1')^{-1})^{u} = (g^{r_1} r_2^{e_{\mathrm{RC}}} z_1^{-1})^{u'} = (g^{s_G} \mathrm{ID}_B w_C^{e_{\mathrm{RC}}})^{uu'} \bmod n_C$$

来确定是否是同一个群成员产生的，即张键红等的方案不具有不相关性。

4　结束语

本文指出了张键红等提出的一种基于 RSA 的高效群签名方案是不安全的，群成员与撤消中心合谋就可以不利用自己特有的资格证书而产生有效的群签名，而签名者的身份不会被追踪到；同时指出了他们方案的身份追踪算法是错误的，身份追踪式是与具体签名无关的常量；最后指出了他们的方案具有相关性，一旦某个成员的某个签名被打开，则他先前的群签名和以后的群签名都能被识别出。

参 考 文 献

[1] Chaum D and Heyst F. Group signature[A]. EUROCRYPT'91, LNCS 547, Berlin: Springer-verlag, 1992: 257–265.

[2] Wang G L. Security analysis of several group signature schemes[A]. In: Indocrypt'2003, LNCS2904, Berlin: Springer-Verlag, 2003: 252–265.

[3] Joye M, Lee N Y, and Hwang T. On the security of the Lee-Chang group signature scheme and its derivatives[A]. In: Information Security (ISW'99), LNCS 1729, Berlin: Springer-Verlag, 1999: 47–51.

[4] Joye M, Kim S, and Lee N Y. Cryptanalysis of two group signature schemes[A]. In: Information Security (ISW'99), LNCS 1729, Berlin: Springer-Verlag, 1999: 271–275.

[5] Wang G L. On the security of a group signature scheme with forward security[A]. In: Information Security and Cryptography (ICISC 2003), LNCS 2971, Berlin: Springer-Verlag, 2004: 27–39.

[6] Lysyanskaya A and Ramzan Z. Group blind signature: A scalable solution to electronic cash[A]. Financial Cryptography (FC '98), LNCS 1465, Berlin:Springer-Verlag, 1998: 184–197.

[7] Tseng Y M and Jan J K. Improved group signature scheme based on the discrete logarithm problem[J]. *Electron. Lett.*, 1999, 35(1): 37–38.

[8] Sun H M. Comment: Improved group signature scheme based on the discrete logarithm problem[J]. *Electron. Lett.*, 1999, 35(16): 1323–1324.

[9] Ateniese G, Camenisch J, Joye M, and Tsudik G. A practical and provably secure coalition-resistant group signature scheme[A]. In: CRYPTO 2000, LNCS1880, Berlin: Springer-Verlag, 2000: 255–270.

[10] 张键红，伍前红，邹建成，王育民. 一种高效的群签名[J]. 电子学报，2005, 33(6): 1113–1115.
Zhang J H, Wu Q H, Zou J C, and Wang Y M. An efficient group signature scheme[J]. *Acta Electronica Sinca*, 2005, 33(6): 1113–1115.

谢　琪：　男，1968 年生，副教授，博士，研究方向为密码学和信息安全.