一个群签名成员删除方案的密码学分析*

黄振杰[1,2+], 林宣治[1]

[1](漳州师范学院 数学与信息科学系,福建 漳州 363000)

[2](西安电子科技大学 综合业务网国家重点实验室,陕西 西安 710071)

Cryptanalysis of a Member Deletion Scheme for Group Signature

HUANG Zhen-Jie[1,2+], LIN Xuan-Zhi[1]

[1](Department of Mathematics and Information Science, Zhangzhou Teachers College, Zhangzhou 363000, China)

[2](State Key Laboratory of Integrated Service Networks, Xidian University, Xi'an 710071, China)

+ Corresponding author: Phn: +86-596-2591235, E-mail: zhj_huang@hotmail.com

Received 2003-11-26; Accepted 2004-03-02

Huang ZJ, Lin XZ. Cryptanalysis of a member deletion scheme for group signature. *Journal of Software*, 2005,16(3):472−476. DOI: 10.1360/jos160472

Abstract: This paper analyses Wang *et al*.'s member deletion scheme of group signature and shows that in their scheme, after the group manager changes the group's key, the excluded group members can still modify their secret property key, prove their membership and issue valid signatures. So this scheme cannot delete any group member and is insecure.

Key words: digital signature; group signature; member deletion; cryptanalysis; anonymity

摘 要: 分析了王尚平等人提出的群签名成员删除方案,给出在群管理员更换群密钥后,已被删除成员更新其特性密钥、证明其成员资格和产生有效签名的方法,说明该方案是不安全的,不能真正删除群成员.

关键词: 数字签名;群签名;成员删除;密码学分析;匿名性

中图法分类号: TP309 **文献标识码**: A

群签名(group signature)是 Chaum 和 van Heyst[1]在 EUROCRYPT'91 上首先提出的.在群签名中,群成员可以代表群体进行匿名签名,验证者只能验证签名是由群体中的成员所签,而不能确知是哪个成员.群签名的匿名性是可撤消的,必要时可由群管理员打开签名来揭露签名人的身份,使得签名人不能否认是自己签的名.群签名同时提供了匿名性和可追踪性,这种性质称为可撤消匿名性,其匿名性可为合法用户提供匿名保护,其可追踪性又使得可信机构可以追踪违法行为.群签名还具有无关联性,即不能确定两个群签名是否为同一个成员所签.可撤消匿名性和无关联性使得群签名在管理、军事、政治及经济等许多方面有着广泛的应用前景,因此引起许多研究者的注意.

* Supported by the National Natural Science Foundation of China under Grant No.19931010 (国家自然科学基金); the National Grand Fundamental Research 973 Program of China under Grant No.G1999035804 (国家重点基础研究发展规划(973))

作者简介: **黄振杰**(1964−),男,福建漳州人,博士生,副教授,主要研究领域为密码学及其应用;**林宣治**(1966−),男,讲师,主要研究领域为网络安全.

© 中国科学院软件研究所 http://www.jos.org.cn

在实际应用中,签名的群体经常是动态的,也就是说,群成员是不断增、减的,因此如何安全、有效地删除成员是群签名应用的一个重要问题[2].目前这方面的研究还不够成熟,已有的主要成果不多[3−5],这些方案要么存在计算量与被删除成员数线性相关的缺点,要么是不安全的.王尚平等人提出一种计算量与被删除成员数无关的成员删除方案[3],但是,该方案不安全,其所提供的成员删除方案不能真正删除群成员.本文对该方案进行分析,给出在群管理员更换群密钥后,已被删除成员更新秘密特性密钥、证明成员资格和产生有效签名的方法,从而说明该方案是不安全的.

1 王尚平等人的方案

在引述具体方案之前,先简单介绍下文将用到的几个符号,更详细的描述和群签名、知识签名的有关知识请参考文献[3,6].

下文中,$a\in_R A$ 表示 a 是从 A 中随机选取的;$\varphi(n)$为 Euler 函数,表示小于 n 且与 n 互素的数的个数;$SKREP[\alpha,\beta:y=g^{\alpha}h^{\beta}](m)$ 为 y 关于底 g 和 h 的表示的知识签名,用于证明知道α,β满足 $y=g^{\alpha}h^{\beta}$;$SKROOTLOG[\alpha:y=g^{\alpha^e}](m)$ 为 y 关于底 g 的离散对数的 e 次根的知识签名,用于证明知道α满足 $y=g^{\alpha^e}$;$SKPOOTREP[\alpha,\beta:y=g^{\alpha}h^{\beta^e}](m)$ 为 y 关于底 g 和 h 的表示的部分 e 次根的知识签名,用于证明知道α,β满足 $y=g^{\alpha}h^{\beta^e}$.

文献[3]提出的方案如下,该方案基于文献[6]的相关方案.

1.1 系统建立

群管理员计算下列值:

- 一个 RSA 模 n 及 3 个公开的指数 $e_1,e_2,e>1$ 且 e_2,e 都与$\varphi(n)$互素;
- 两个整数 $f_1,f_2>1$,在不知道 n 的分解时计算它们的 e_1,e_2 次根是困难的;
- 一个阶为 n 的循环群 $G=\langle g\rangle$,使得在 G 中计算离散对数是困难的;
- 一个元素 $h\in G$,使得计算 h 关于基 g 的离散对数是困难的;
- 任选一个整数 $w\in Z_n$,群管理员的公钥为 $y_R:=h^w$.

群的公钥 $Y=(n,e,e_1,e_2,f_1,f_2,G,g,h,y_R)$,群管理员的私钥为 $\frac{1}{w}$ 及 n 的素因子.

1.2 成员注册与特性密钥更新

成员注册

假设用户 Alice 要注册为群成员,她加入时群的合法成员列表 $C:=\{G_1,G_2,...,G_{m-1}\}$,Alice 加入后,为群的第 m 个成员 G_m,设其私钥为 (x_{G_m},y_{G_m}),其中 $y_{G_m}=x_{G_m}^{e_1}$,公钥为 $z_{G_m}:=g^{y_{G_m}}$,她按如下方法向群管理员注册这些值,以获得成员证书.

计算:

- $\tilde{y}_{G_m}:=r^{e_2}(f_1y_{G_m}+f_2)\bmod n$,其中 $r\in_R Z_n^*$;
- $V_{1G_m}:=SKROOTLOG[\alpha:z_{G_m}=g^{\alpha^{e_1}}]('')$,这里''表示空消息,下同;
- $V_{2G_m}:=SKROOTLOG[\beta:g^{\tilde{y}}=(z_{G_m}^{f_1}g^{f_2})^{\beta^{e_2}}]('')$.

发送 $z_{G_m},\tilde{y}_{G_m},V_{1G_m},V_{2G_m}$ 给群管理员,若 V_{1G_m},V_{2G_m} 都正确,群管理员确信 $\tilde{y}_{G_m}$ 是 z_{G_m} 所含的成员私钥的正确盲化值,群管理员计算

$$\tilde{v}_{G_m}:=(\tilde{y}_{G_m})^{\frac{1}{e_2}}\bmod n.$$

发送 $\tilde{v}_{G_m}$ 给 Alice,Alice 去掉盲化因子 r 得到成员证书:

© 中国科学院软件研究所 http://www.jos.org.cn

$$V_{G_m} := \frac{\tilde{v}_{G_m}}{r} = (f_1 y_{G_m} + f_2)^{\frac{1}{e_2}}.$$

设 Alice 加入群时,群公开特性密钥 $U_G := z_{G_1} z_{G_2} ... z_{G_{m-1}} z'$,其中 z_{G_i} 是群成员 G_i 的公钥 $(1 \le i \le m-1)$,且 $z' \in_R G$,群管理员计算下列值:

- 新的群公开特性密钥 $U_G := z_{G_1} z_{G_2} ... z_{G_m} z''$,其中 $z'' \in_R G$;
- 特性密钥更新算子 $U := \left(\frac{z_{G_m} z''}{z'} \right)^{\frac{1}{e}}$;
- 新成员 G_m 的秘密特性密钥 $U_{G_m} := (z_{G_1} z_{G_2} ... z_{G_{m-1}} z'')^{\frac{1}{e}}$.

群管理员公布新的群公开特性密钥 U_G 及特性密钥更新算子 U,秘密发送秘密特性密钥 U_{G_m} 给 G_m.新成员 G_m 通过验证 $(U_{G_m})^e z_{G_m} = U_G$ 成立,来确定群管理员传送的秘密特性密钥 U_{G_m} 的正确性.

特性密钥更新

群中各个合法成员 $G_i (1 \le i \le m-1)$ 利用特性密钥更新算子 U 及其秘密特性密钥 U_{G_i} 计算其新的秘密特性密钥为 $U_{G_i} := U_{G_i} U$,即

$$U_{G_i} := (z_{G_1} ... z_{G_{i-1}} z_{G_{i+1}} ... z_{G_{m-1}} z')^{\frac{1}{e}} \left(\frac{z_{G_m} z''}{z'} \right)^{\frac{1}{e}}$$

$$= (z_{G_1} ... z_{G_{i-1}} z_{G_{i+1}} ... z_{G_m} z'')^{\frac{1}{e}},$$

并通过验证算式 $(U_{G_i})^e z_{G_i} = U_G$ 来确定 U_{G_i} 的正确性.

1.3 成员删除与特性密钥更新

假设群管理员要从群中删除成员 G_j,他在群公开特性密钥 U_G 中删除公钥 z_{G_j},并改变随机数,然后发布新的群公开特性密钥 U_G 及特性密钥更新算子 U.群中其余成员利用更新算子更新其各自的成员秘密特性密钥,便可在 G_j 被删除后继续生成有效的群签名.

设当前群特性公钥 $U_G := z_{G_1} ... z_{G_m} z'$,其中 $z' \in_R G$,为删除群成员 G_j,群管理员计算:

- 新的群公开特性密钥 $U_G := U_G \frac{z''}{z_{G_j} z'} = z_{G_1} .... z_{G_{j-1}} z_{G_{j+1}} ... z_{G_m} z''$,其中 $z'' \in_R G$.
- 特性密钥更新算子 $U := \left(\frac{z''}{z_{G_j} z'} \right)^{\frac{1}{e}}$.
- 公布新的群特性公钥及更新算子(U_G, U).

群中每个合法成员 G_i 通过更新算子 U 更新其秘密特性密钥 U_{G_i}.

$$U_{G_i} := U_{G_i} U = (z_{G_1} ... z_{G_{i-1}} z_{G_{i+1}} ... z_{G_{j-1}} z_{G_{j+1}} ... z_{G_m} z'')^{\frac{1}{e}}.$$

每个合法的成员 G_i 通过验证 $(U_{G_i})^e z_{G_i} = U_G$ 是否成立判断更新后的 U_{G_i} 的正确性.

1.4 签 名

设群的合法成员有 $G_1,...,G_m$,群的特性公钥 $U_G = z_{G_1} ... z_{G_m} z''$,群成员 G_i 代表群对消息 M 签名.G_i 计算:

- $\tilde{z} := h^r z_{G_i}$,其中 $r \in_R Z_n^*$;
- $d := y_R{}^r$;
- $A = U_{G_i} g^r$;

© 中国科学院软件研究所 http://www.jos.org.cn

- $B=h^r g^{re}$;
- $V_1 \coloneqq SKROOTREP[\alpha,\beta:\tilde{z}=h^{\alpha}g^{\beta^{e_1}}](M)$;
- $V_2 \coloneqq SKROOTREP[\gamma,\delta:\tilde{z}=h^{\gamma}g^{\delta^{e_2}}](M)$;
- $V_3 \coloneqq SKREP[\varepsilon,\varsigma:d=y_R{}^{\varepsilon}\wedge\tilde{z}=h^{\varepsilon}g^{\varsigma}\wedge B=h^{\varepsilon}g^{\varepsilon e}](M)$,

则成员 G_i 对消息 M 的签名为 $(\tilde{z},d,A,B,V_1,V_2,V_3)$.

1.5 验 证

签名的正确性可以通过验证 V_1,V_2,V_3 同时成立来确定,签名人秘密特性密钥 U_{G_i} 的有效性由 $\frac{U_G}{A^e}B=\tilde{z}$ 来保证.

2 密码学分析

本节我们将说明在第 1.3 节被删除的成员 G_j 仍可用和未被删除成员一样的方法更新其秘密特性密钥 U_{G_j},所得到的秘密特性密钥可以通过合法性验证,而且被删除的成员 G_j 用它进行签名所得到的签名能够满足所有验证方程,因此产生的签名是有效群签名.

更新秘密特性密钥

成员 G_j 同样可以用新的更新算子 U 来更新其秘密特性密钥 U_{G_j}.

$$\begin{aligned}U_{G_j} &\coloneqq U_{G_j}U\\ &=(z_{G_1}\ldots z_{G_{j-1}}z_{G_{j+1}}\ldots z_{G_m}z')^{\frac{1}{e}}\left(\frac{z''}{z_{G_j}z'}\right)^{\frac{1}{e}}\\ &=(z_{G_1}\ldots z_{G_{j-1}}z_{G_j}^{-1}z_{G_{j+1}}\ldots z_{G_m}z'')^{\frac{1}{e}}.\end{aligned}$$

所得到的秘密特性密钥 U_{G_j} 能够通过合法性验证:

$$\begin{aligned}(U_{G_j})^e z_{G_j} &=(z_{G_1}\ldots z_{G_{j-1}}z_{G_j}^{-1}z_{G_{j+1}}\ldots z_{G_m}z'')z_{G_j}\\ &=z_{G_1}\ldots z_{G_{j-1}}z_{G_{j+1}}\ldots z_{G_m}z''\\ &=U_G.\end{aligned}$$

上述更新只用到成员 G_j 的旧秘密特性密钥 U_{G_j} 和新的更新算子 U.一方面,旧秘密特性密钥 U_{G_j} 是在成员 G_j 注册为群成员时就从群管理员处得到的,群管理员删除他时不可能删除他早已获得的旧秘密特性密钥 U_{G_j};另一方面,在原方案中新的更新算子 U 是公开的,成员 G_j 当然也能得到,即使将其改为群管理员,只要把新的更新算子 U 秘密发送给未删除成员,也不能保证成员 G_j 不会从其他成员处获得新的更新算子,只要有一个未删除成员与其合谋即可,这样也仍不安全.总之,上述的秘密特性密钥更新是可以做到的.

签名的有效性

成员 G_j 使用上述更新方法所得到的秘密特性密钥 U_{G_j} 可用于签名,所得到的签名能够通过所有的验证.首先,V_1,V_2,V_3 的验证与秘密特性密钥 U_{G_j} 无关,所以对它们的验证与 G_j 被删除前一样都能成立.因此关键的问题是 A,B 需要满足 $\frac{U_G}{A^e}B=\tilde{z}$,以证明 U_{G_j} 仍然有效,下面的式子表明这是成立的.

$$\begin{aligned}\frac{U_G}{A^e}B &=\frac{U_G}{(U_{G_j}g^r)^e}h^r g^{re}\\ &=\frac{z_{G_1}\ldots z_{G_{j-1}}z_{G_{j+1}}\ldots z_{G_m}z''}{z_{G_1}\ldots z_{G_{j-1}}z_{G_j}^{-1}z_{G_{j+1}}\ldots z_{G_m}z''}h^r\\ &=h^r z_{G_j}\\ &=\tilde{z}.\end{aligned}$$

© 中国科学院软件研究所 http://www.jos.org.cn

综上所述,成员 G_j 实际上并未被删除,他还能和其他所有成员一样进行签名,而且得到的签名仍然是有效的,可见文献[3]的成员删除方案是不安全的.

3 结 论

如何安全有效地删除成员是群签名走向实用的一个重要的问题,文献[3]提出一种计算量与被删除成员数无关的群成员删除方案,本文指出该方案是不安全的,它实际上不能删除任何群成员.现有安全的群成员删除方案的计算量都与被删除成员数线性相关,提出计算量与被删除成员数无关的群成员删除方案仍是亟待解决的问题.

References:

[1] Chaum D, Van Heyst E. Group signtures. In: Davies DW, ed. Advances in Cryptology-EUROCRYPT'91. LNCS 547, Berlin: Springer-Verlag, 1991. 257−265.

[2] Ateniese G, Tsudik G. Some open issues and new directions in group signatures. In: Franklin M, ed. Financial Cryptography Conf. LNCS 1648, Berlin: Springer-Verlag, 1999. 196−211.

[3] Wang SP, Wang YM, Wang XF, Qin B, He C, Zou YJ. A new solution scheme for the member deletion problem in group signature by use of renew operator. Journal of Software, 2003,14(11):1911−1917 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/14/1911.htm

[4] Bresson E, Stern J. Efficient revocation in group signature. In: Kim K, ed. Public Key Cryptography—PKC 2001. LNCS 1992, Berlin: Springer-Verlag, 2001. 190−206.

[5] Kim HJ, Lim JI, Lee DH. Efficient and secure member deletion in group signature schemes. In: Won D, ed. Information Security and Cryptology—ICISC 2000. LNCS 2015, Berlin: Springer-Verlag, 2001. 150−161.

[6] Camenisch J, Stadler M. Efficient group signatures schemes for large groups. In: Kaliski BS, ed. Advances in Cryptology—CRYPT'97. LNCS 1294, Berlin: Springer-Verlag, 1997. 410−423.

附中文参考文献:

[3] 王尚平,王育民,王晓峰,秦波,何成,邹又姣.群签名中成员删除问题的更新算子解决方案.软件学报,2003,14(11):1911−1917. http://www.jos.org.cn/1000-9825/14/1911.htm

© 中国科学院软件研究所 http://www.jos.org.cn