文章编号:1001-2486(2005)04-0071-04

一种动态门限群签名方案的安全性分析*

郭兴阳[1,2],张 权[1],唐朝京[1]

(1. 国防科技大学 电子科学与工程学院,湖南 长沙 410073; 2. 空军工程大学 电讯工程学院,陕西 西安 710077)

摘 要:门限群签名是群签名的推广,其中只有授权子集才能代表整个群体进行签名。一旦发生纠纷,签名成员的身份可以被追查出来。指出一种动态门限群签名方案有冗余,提出了针对该签名三种攻击。分析结果证明该门限群签名方案不具有防冒充性,不能抵抗合谋攻击,门限的动态更新、群成员注销和系统密钥更新也不安全。

关键词:数字签名;门限群签名;可追查性;防冒充性

中图分类号:TP309 **文献标识码**:A

Cryptanalysis of a Dynamic Threshold Group Signature Scheme

GUO Xing-yang[1,2], ZHANG Quan[1], TANG Chao-jing[1]

(1. College of Electronic Science and Engineering, National Univ. of Defense Technology, Changsha 410073, China;
2. College of Telecommunication Engineering, Air Force Engineering University, Xi'an 710077, China)

Abstract: The threshold group signature is a generalization of group signature, in which only authorized subset can represent the group to generate signature and the identities of signers of a signature can be opened in case of later dispute. We point out the redundancy of a dynamic threshold group signature scheme and demonstrate three attacks on it. The security analysis indicates that the scheme is not secure against framing attack and cannot resist conspiratorial attack and the threshold value cannot be renewed safely.

Key words: digital signature; threshold group signature; traceability; security against framing attack

数字签名是实现网络身份认证、数据完整性保护和非否认服务的基础,也是开展电子商务和签订电子合同的重要工具[5]。使用普通的数字签名时,每个用户都有各自的密钥对,且无论生成签名还是验证签名,都只有一个用户参与。而让多个用户都可以代表整个群体进行签名,在很多情况下是重要且必要的,由此导致了群签名的产生。群签名首次由 Chaum 和 van Heyst 提出[1]。在这种特殊的数字签名中,群体中的任何成员,也只有该群体中的各个成员,可以代表整个群体对一个消息进行签名;而签名的验证者只需要知道该群体的唯一公开密钥,就可验证签名是否有效;产生纠纷时,一个特殊的成员(或部分普通成员合作)可以追查出签名者的身份。在群签名方案中引入秘密分存就形成门限群签名方案[2]。在这种方案中,把各成员利用自己的分存秘密所签署的签名叫做部分签名,而一定数量的部分签名按某种方式结合后就形成门限群签名。目前已经提出了一些门限群签名方案[2-4]。

文献[6]提出了一个良好的门限群签名方案所应具备的8条性质:(1)群签名特性。只有群体中的成员才可以生成有效的部分签名。(2)门限特性。只有当签名人数不小于门限时,才可以生成有效的门限群签名。(3)防冒充性。任何小组不能假冒其他小组生成群签名。(4)验证简单性。签名的验证者可以简单而方便地验证签名是否有效。(5)匿名性。签名的验证者不知道该签名是群体中哪些成员签署的。(6)可追查性。发生纠纷时可以追查出签名者的真实身份。(7)强壮性。恶意成员大于等于门限时仍然无法获取系统秘密参数。(8)系统稳定性。剔除违规成员或加入新成员时,勿须过多改变系统参数和成员参数。

最近,有学者提出了一种带有可信中心的动态门限群签名方案[7](WCF方案)。该方案试图达到以

* 收稿日期:2005-04-23
基金项目:国家自然科学基金资助项目(60472032、60372039)
作者简介:郭兴阳(1977—),男,博士生。

下三个目的:(1)方便地更改门限值;(2)抵抗合谋攻击;(3)方便地加入或注销群成员。本文的研究表明,该方案有冗余,门限更新、群成员注销和系统密钥更新过程不安全,不能抵抗合谋攻击,不能防止冒充。因此 WCF 方案的设计并不太成功。

1 方案简单描述

在 WCF 方案中,系统有一个可信中心(TC),TC 负责选择系统参数和群的秘密参数。$G_s=\{u_1,u_2,\cdots,u_m\}$为有 m 个成员的群。在 G_s 中,有一个叫指定合成者的特别成员(Clerk),Clerk 负责验证群成员的部分签名的有效性,然后把这些有效的部分签名合成为群签名。如果签名验证人验证了群签名以后,还想知道谁参加了签名,可以在 TC 的帮助下识别签名人的真实身份。TC 可以增加群成员,注销群成员,以及更新系统密钥和门限。WCF 方案的设计者认为该方案能够抵抗伪造攻击和合谋攻击,并具有防冒充性。我们不对 WCF 方案作详细介绍,可参考文献[7]。

2 WCF 动态门限群签名方案的简化

我们发现可以用简化的方法产生合法的门限群签名。在下面的描述中,简化方案与原始方案中相同符号的意义是相同的。

2.1 简化的门限群签名产生过程

(1) u_i 选择随机数 $0<\zeta_i<q$,计算

$$r_{i2}=g^{\zeta_i}\bmod n,\sigma_i=g^{f(x_i)}\bmod n$$

送(r_{i2},σ_i)给 Clerk。

(2)收到所有的 $r_{i2},\sigma_i,i=1,2,\cdots,t$ 后,Clerk 验证

$$V_i=g^{\sigma_i}\bmod n(i=1,2,\cdots,t)$$

随机选取 $0<\delta<q^t\bmod n,0<s_1,v<q$,计算

$$R_1=y^v\delta^e g^{s_1}\bmod n,\quad R_2=\prod_{i=1}^{t}r_{i2}\bmod n$$

并用 t 个签名人的公共值(V_i,x_i)构成多项式函数

$$F(X)=\sum_{i=1}^{t}x_i\prod_{i=1,j\neq i}^{t}\frac{X-V_j}{V_i-V_j}\bmod q$$

送$[R_1,R_2,F(X),(V_i,x_i,i=1,2,\cdots,t)]$给 U_i 中的每个签名人。

(3)每个签名人验证 $F(V_i)=x_i(i=1,2,\cdots,t)$,计算

$$G(x_i)=Y_i\oplus f(x_i),\gamma=F(D),c=h(R_1\parallel R_2\parallel\gamma\parallel M),s_{i3}=\zeta_i-G(x_i)B_i c\bmod q$$

送(s_{i3},M)给 Clerk。

(4)收到所有的$(s_{i3},i=1,2,\cdots,t)$后,Clerk 计算

$$d=e^{-1}\bmod q,s_2=y^{(v-c)d}\delta\bmod n,s_3=\sum_{i=1}^{t}s_{i3}\bmod q,c=h(R_1\parallel R_2\parallel\gamma\parallel M)$$

则信息 M 的门限群签名是$(s_1,s_2,s_3,c,F(X))$。

2.2 简化签名方案的正确性

定理 1 简化方案所产生的门限群签名可以通过验证。

证明 对于信息 M 的门限群签名$(s_1,s_2,s_3,c,F(X))$可以得到

$$R'_1=y^c g^{s_1}s_2^e=y^c g^{s_1}(y^{(v-c)d}\delta)^e=y^c g^{s_1}y^{(v-c)d\bmod q}\delta^e$$
$$=y^c g^{s_1}y^{v-c}\delta^e=y^v\delta^e g^{s_1}=R_1\bmod n$$

注:由于 $y=g^{f(0)}\bmod n$,所以 y 的阶为 q,因此有$(y^{(v-c)d})^e=y^{(v-c)d\bmod q}\bmod n$。

由于 $R'_2=g^{s_3}D^e=R_2\bmod n$ 与原方案相同,因此 $c=h(R'_1\parallel R'_2\parallel\gamma\parallel M)$成立。

2.3 小 结

在简化的方案中,s_1, s_2 完全由 Clerk 产生,这样也可以得到合法的门限群签名。原方案中,如果签名小组信任 Clerk,可以委托 Clerk 用这种简化的方法产生 s_1, s_2。如果不信任 Clerk,也无法阻止 Clerk 用这种方法产生 s_1, s_2。因此对于产生 s_1, s_2,所有签名人的合作是没有必要的。与原方案相比,简化方案所需的计算量和通信量显著减少。在 Clerk 的帮助下,每一个签名人 u_i 只需要子密钥 $G(x_i)$就可以参加签名。WCF 方案中系统注销群成员或更新系统密钥时,为了达到高效率,仅为每个合法成员改变了子密钥 $f(x_*)$。注销的成员仍可在不诚实的 Clerk 帮助下,用子密钥 $G(x_*)$参加签名,因此 WCF 方案没有实现有效的群成员注销。系统密钥更新对安全性也没有提高。

原方案 Clerk 在(20)式中验证 s_{i3}的有效性,这个验证没有作用。如果 u_i 企图欺骗 Clerk,可以取随机值 $\epsilon(0<\epsilon<q)$,在第(3)步中计算 $\lambda_i = g^{\epsilon} \bmod n$ 和 $s_{i3} = \zeta_i - \epsilon B_i c \bmod q$,仍能在(20)式中通过验证。在简化方案中删去这个验证并不影响原方案的安全性。

3 对 WCF 方案的三种攻击

3.1 攻击 1

在原方案中,作者显然假定每个签名人并不知道其它签名人 u_* 的化名身份 x_*。因为如果知道,每个签名人自己就可以构造正确的身份识别函数,无需经过 Clerk。原方案还可以进一步简化。在这个攻击中,t 个群成员签名时,一个签名人可以与 Clerk 合作,冒充其它群成员的化名身份参加签名,从而使 TC 无法追查到自己。假设 t 个群成员构成 $U_t = \{u_1, u_2, \cdots, u_t\}$,同意代表整个群对消息 M 签名。$X_r = \{x_1, x_2, \cdots, x_t\}$为该 t 个群成员的化名身份集合。假定 u_t 企图与 Clerk 合作,冒充 $x_v(x_v \notin X_r)$进行签名。这里用 X_v 表示化名身份集合$\{x_1, x_2, \cdots, x_{t-1}, x_v\}$。攻击过程如下:

(1) 在 WCF 方案第(2)步中,Clerk 收到 $r_{i1}, r_{i2}, \sigma_i, i = 1,2,\cdots,t-1$ 后,与 u_t 合作,确定两个化名身份集合 X_v 和 X_r。Clerk 随机选取 $0<\delta<q^t \bmod n, 0<s_1, v<q$,计算

$$B_{ri} = \prod_{x_j \in X_r, x_j \neq x_i} \frac{-x_j}{x_i - x_j} \bmod q \quad i = 1,2,\cdots,t-1$$

$$B_{vi} = \prod_{x_j \in X_v, x_j \neq x_i} \frac{-x_j}{x_i - x_j} \bmod q \quad i = 1,2,\cdots,t-1$$

$$R_1 = y^v \delta^e g^{s_1} \bmod n, R_2 = r_{t2} \prod_{i=1}^{t-1} r_{i2}^{B_{vi}^{-1} B_{ri}} \bmod n$$

用 X_v 和$\{V_1, V_2, \cdots, V_{t-1}, V_v\}$构成多项式 $F_v(X)$。送$[R_1, R_2, F_v(X), V_v, x_v(V_i, x_i, i = 1,2,\cdots,t-1]$给 U_t 中的每个签名人。

(2)由于每个签名人并不知道其它签名人的化名身份,因此不能在第(3)步中发现 $F_v(X)$所代表的化名身份集合里有一个冒充的身份。每个签名人从 $F_v(X)$中得到了化名身份集合 X_v。除 u_t 外每个签名人计算 $G(x_i), \gamma, \lambda_i, c, s_{i1}, s_{i2}, s_{i3}$。这里 $\gamma = F_v(D)$, $s_{i3} = \zeta_i - G(x_i) B_{vi} c \bmod q$。$u_t$ 同样计算 $G(x_t)$, γ, c,并计算

$$B_{rt} = \prod_{x_j \in X_r, x_j \neq x_t} \frac{-x_j}{x_t - x_j} \bmod q, s_{t3} = \zeta_t - G(x_t) B_{rt} c \bmod q$$

$u_i(i = 1,2,\cdots,t-1)$送$(s_{i1}, s_{i2}, s_{i3}, \lambda_i, M)$给 Clerk。$u_t$ 送 s_{t3}给 Clerk。

(3)Clerk 计算

$$d = e^{-1} \bmod q, s_2 = y^{(v-c)d} \delta \bmod n, s_3 = s_{t3} + \sum_{i=1}^{t-1} s_{i3} B_{vi}^{-1} B_{ri} \bmod q$$

得到的门限群签名是$(s_1, s_2, s_3, c, F_v(X))$。

定理 2 攻击 1 所产生的门限群签名可以通过验证。

证明

$$
\begin{aligned}
R'_2 &= g^{s_3} D^c = g^{s_3}\Big(\prod_{i=1}^{t-1} g^{s_{i3} B_{ui}^{-1} B_{ri}}\Big) D^c \\
&= g^{\zeta_t - G(x_t)B_{rt}c}\Big(\prod_{i=1}^{t-1} g^{(\zeta_i - G(x_i)B_{ui}c)B_{ui}^{-1}B_{ri}}\Big) D^c \\
&= g^{\zeta_t - G(x_t)B_{rt}c}\Big(\prod_{i=1}^{t-1} g^{B_{ri}\zeta_i B_{ui}^{-1}} \prod_{i=1}^{t-1} g^{-G(x_i)B_{ri}c}\Big) D^c \\
&= g^{\zeta_t}\Big(\prod_{i=1}^{t-1} g^{\zeta_i B_{ui}^{-1} B_{ri}}\Big) g^{-G(x_t)B_{rt}c}\Big(\prod_{i=1}^{t-1} g^{-G(x_i)B_{ri}c}\Big) D^c \\
&= r_{t2}\Big(\prod_{i=1}^{t-1} r_{i2}^{B_{ui}^{-1}B_{ri}}\Big)\Big(\prod_{i=1}^{t} g^{-G(x_i)B_{ri}c}\Big) D^c \\
&= R_2 g^{-c\sum_{i=1}^{t} G(x_i)B_{ri}} D^c \\
&= R_2 D^{-c} D^c = R_2 \bmod n
\end{aligned}
$$

又因为 $R'_1 = y^c g^{s_1} s_2^e = R_1 \bmod n$，所以 $c = h(R'_1 \| R'_2 \| F_v(D) \| M)$。

u_t 和 Clerk 合作，成功地冒充了化名身份 x_v，并且其他成员觉察不到。由于 $F_v(X)$所代表的化名身份集合 X_v 中没有 x_t，TC 从该签名中只能追查到 u_v 而不是 u_t。这个攻击可以简单地推广到多个不诚实签名人与 Clerk 合作的情况。

3.2 攻击 2

在 WCF 方案中，t 名不诚实的成员组成一个小组，则不需要与 Clerk 合作，而从他们中间选一个成员充当 Clerk，然后利用前面介绍的简化签名产生过程产生签名。显然，他们可以构造一个代表任意签名小组的身份识别函数，而用他们真正的化名身份集合计算所有的 $B_i(i = 1,2,\cdots,t)$，然后在其 Clerk 的帮助下生成一个门限群签名。这样，TC 不能追查到真正的签名小组，该签名小组可以伪造任意成员小组的签名。因此该方案也不能抵抗其作者所指的合谋攻击。

3.3 攻击 3

门限值更改后，如果新的门限 t' 大于旧的门限 t，则新系统中不允许 t 个恶意成员产生门限群签名。

t 个恶意成员私下保留以前的公共参数 $Y_i(i = 1,2,\cdots,m)$。门限值更改后，t 个恶意成员利用其 t 个子密钥 $G(x_*)$构造旧的 $t-1$ 次多项式 $G(x)$，计算 $G(x_i), i = 1,2,\cdots,m$。利用保留的公共参数 Y_* 计算 $f(x_i) = Y_i \oplus G(x_i), i = 1,2,\cdots,m$。然后计算新的子密钥 $G'(x_i) = f(x_i) \oplus Y'_i, i = 1,2,\cdots,m$，其中 Y'_* 为新的公共参数，得到了门限值更新后系统中所有成员的子密钥。然后如攻击 2 所述，t 个恶意成员取 t' 个新的子密钥 $G'(x_i)$可以产生一个门限群签名。

3.4 攻击的危害和防止

攻击 1 和 2 的冒充攻击导致 TC 不能追查签名人的身份，这在群签名中是不允许的。签名人可以利用群体的名义从签名接收方获取利益，一旦发生纠纷，TC 追查签名人时却不能找出真正的签名者。这种情况会导致群成员滥用签名能力。我们没有找到克服这两种攻击的方法。

攻击 3 导致系统不能安全地更换门限。简单的克服方法是 TC 不在公共文件夹中公布 Y_*，而把 $G(x_*)$秘密送给 u_*。显然，如果门限更改后新的门限值 t' 大于旧的门限值 t，而且没有公共参数 Y_* 可以利用，t 个攻击者可以计算旧的 $t-1$ 次多项式 $G(x)$，却无法计算其它成员的子密钥 $f(x_*)$和新的子密钥 $G'(x_*)$。攻击者的 t 个子密钥 $G'(x_*)$又不能达到新的门限值，因此无法产生一个门限群签名。

（下转第 115 页）

参考文献:

[1] Meinders T, Carleer B D, Vegter H, et al. Recent Development in Finite Element Simulations of the Deep Drawing Process[A]. Proceedings Shemet'97, 1997.

[2] Miller B, Bond R. The Practical Use of Simulation in the Sheet Metal Forming Industry[A]. British Metal forming Technical Conference,2001.

[3] António C C, Castro C F, Sousa L C. Optimization of Metal Forming Processes[J]. Journal Computers & Structures,2004,82(17-19): 1425-1433.

[4] Schenk O, Hillmann M. Optimal Design of Metal Forming Die Surfaces with Evolution Strategies[J]. Journal Computers & Structures,2004,82(21-22):1695-1705.

[5] Acharjee S, Zabaras N. On the Development of a Three-Dimensional Deformation Process Design Simulator[C]. EPD Congress 2004 Edited by M. E. Schlesinger TMS (The Minerals, Metals & Materials Society), 2004.

[6] Veltkamp R C. Survey of Continuities of Curves and Surfaces[R]. CWI Report, CS-R9202, 1992.

[7] Putz B. On Normal Curvature Discontinuity Between Tangent Plane Continuous Patches[J]. Computer Aided Geometric Design, 1996, 13(1): 95-99.

[8] Ganapathysubramanian S. Computational Design of Deformation Process for the Control of the Microstructure-sensitive Properties[D]. Ph. D. Thesis, Cornell University 2004.

[9] 夸克工作室.精通 Pro/Engineering CAD 进阶篇[M].北京:中国青年出版社,(2000):369.

[10] Landau L D, Lifshitz E M. The Energy of a Deformed Rod[A]. In: Theory of Elasticity(third edition). Butterworth-Heinemann, 1997.

[11] Singer L L. Friction and Energy Dissipation at the Atomic Scale: A Review[J]. Journal of Vacuum Science and Technology A.1994, 12(5):2605-2616.

[12] Hotz G, Kerzmann A, Lennerz C, et al. Calculation of Contact Force[A]. ACM Symposium on Virtual Reality Software and Technology (VRST'99), 1999, pp. 180-181.

[13] Salas, Hille, Etgen. Calculus III[M]. Wiley 2003, 9th Edition.

[14] 王兴波,石金龙.一个分析平面曲线拐点的可靠判据[J].湖南理工学院学报(自然科学版),2004,17(2):1-6.

(上接第 74 页)

4 结 论

WCF 动态门限群签名方案是冗余的,本文在不降低安全性的情况下对 WCF 方案进行了简化。由于两种冒充攻击的存在,WCF 方案中可信中心不能有效追查签名人的身份,而且门限更新的安全性脆弱。简化的方案显示 WCF 方案中签名人只有一个子密钥在签名中有作用,因此导致原方案中有一些错误的结论和危险的操作。如该方案不能抵抗合谋攻击,被注销的群成员仍可参加签名,系统密钥更新不起作用。从本文的研究可见文献[7]中作者的设计并不太成功。

参考文献:

[1] Chaum D, van Heyst E. Group signatures[R]. Advances in Cryptology-Eurocrypt'91, LNCS 547. Springer-Verlag, 1992, 257-265.

[2] Desmedt Y, Frankel Y. Shared Generation of Authenticators and Signatures[R]. Advances in Cryptology-Crypto'91, LNCS 576. Springer-Verlag, 1992, 457-469.

[3] Harn L. Group-oriented (t,n) Threshold Digital Signature Scheme and Multisignature[A]. IEE Proceedings, Computers and Digital Techniques, 1994, 141(5): 307-313.

[4] Li C, Hwang T, Lee N. Threshold-multisignature Schemes Where Suspected Forgery Implies Traceability of Adversarial Share Holders[R]. Advances in Cryptology-Eurocrypt'94, LNCS 950. Springer-Verlag, 1995, 194-204.

[5] 刘世栋,杨林,候滨,等.基于 CA 的电子印章系统设计与实现[J].国防科技大学学报,2003,25(1):26-30.

[6] 王贵林,卿斯汉.几个门限群签名方案的弱点[J].软件学报,2000, 11(10): 1326-1332.

[7] 王晓明,陈火炎,符方伟.动态门限群签名方案[J].计算机学报,2004,27(9): 897-902.