一种加强的基于中国剩余定理的群签名

周素芳[1],杨晓博[1],刘 新[1,2]
(1. 陕西师范大学 计算机科学学院,陕西 西安 710119;
2. 内蒙古科技大学 信息工程学院,内蒙古 包头 014010)

摘 要:陈泽文等在 2004 年提出了基于中国剩余定理的群签名方案。该方案在加入或撤销群成员时其他群成员密钥和群公钥的长度保持不变,从而解决了撤销群成员的困难,提供了一种效率高和计算复杂度小的群签名方案。从该方案的研究中发现其基于 RSA 算法的方案不具有防陷害性和不可伪造性的特征。因此,参照 ElGamal 的算法,提出了一种加强的基于中国剩余定理群签名的新方案。在新方案中,保证了原有算法在加入和撤销成员具有高效性的同时,进一步改进了陈方案的不足,不再要求可信的群中心,并且群成员也分担了群中心的工作量,使系统更具有实效性。

关键词:群签名;中国剩余定理;ElGamal 算法;成员撤销
中图分类号:TP301 **文献标识码**:A **文章编号**:1673-629X(2014)11-0175-03
doi:10.3969/j.issn.1673-629X.2014.11.044

An Enhanced Group Signature Scheme Based on Chinese Remainder Theorem

ZHOU Su-fang[1], YANG Xiao-bo[1], LIU Xin[1,2]
(1. School of Computer Science, Shaanxi Normal University, Xi'an 710119, China;
2. School of Information and Engineering, Inner Mongolia University of Science and Technology, Baotou 014010, China)

Abstract: The group signature scheme based on Chinese remainder theorem was proposed by Chen Zewen etc in 2004. Chen's scheme can keep the secret key of other members and the length of group public key unchanged when joining or canceling a group member, thus, the scheme has solved the problem of withdrawal for the group members and provided a kind of group signature scheme with high efficiency and small computational complexity. In research on the plan, found that the scheme based on RSA algorithm does not have the ability to prevent the frame and fake. Therefore, with the reference to the ElGamal algorithm, a new scheme is put forward which is a kind of strengthening signature based on Chinese remainder theorem. In the new scheme, it can ensure the high efficiency when joining or canceling a group member as the original algorithm. At the same time, the group center does not have to be a trusted and the group members also share the workload of group center, making the system more effective.

Key words: group signature; Chinese remainder theorem; ElGamal algorithm; member canceling

0 引 言

群签名的概念最早由 Chaum 和 Heyst[1] 在 1991 年提出,它应用于一个群体中的任意一个成员可以代表整个群体对消息进行签名的环境。相对于以往的数字签名,群签名使个体可以以匿名的方式代表整个团体进行签名,必要的时候群管理员可以对签名打开并确认签名者的身份,从而保证群成员和群团体的安全性。由于群签名可控的匿名性,使其可以应用于电子商务和电子政务中[2]。

基于中国剩余定理的群签名最早是由陈泽文[3]等在 2004 年提出。其方案保证了在成员加入和撤销的过程中,可以不改变其他有效成员的签名密钥和群公钥的长度,使其只需要乘法运算而不需要指数运算,从而实现了简单快速的群成员加入和撤销。在对 Chen 方案的研究中发现,其基于中国剩余定理利用 RSA 算法没有实现防止成员之间的陷害、不可伪造群成员签

收稿日期:2013-12-11 **修回日期**:2014-03-18 **网络出版时间**:2014-09-11
基金项目:包头市科技计划项目(2012S2005-7)
作者简介:周素芳(1990-),女,河南安阳人,硕士,研究方向为信息安全;刘 新,在读博士,讲师,研究方向为多方保密计算、信息安全。
网络出版地址:http://www.cnki.net/kcms/detail/61.1450.TP.20140911.0956.011.html

名和签名与成员之间的不相关性。

基于上述方案的弱点,文中提出了一种新的方案,基于中国剩余定理利用 ElGamal[4] 算法,是一种非共模的思想,可以在保证高效加入和撤销群成员[5]的同时,使群成员实现真正的匿名性,群成员之间不可伪造其他成员的签名并防止了群成员和管理中心对某个群成员的陷害性。新方案使群成员和群中心在生成群成员密钥时进行交互,不要求群中心是可信的,群成员可以分担群中心的工作量,减少了群中心的计算量。

1 陈方案简介

1.1 系统建立

群中心根据 RSA[6] 算法秘密地选择两个大素数 p,q,计算 $n=pq$,选择 $e \in Z_n$。并求得 d,使 $ed \equiv 1(\mathrm{mod}\Phi(n))$,将 e 作为群中心的公钥,d 作为群中心的私钥。选择一个 Hash 函数 H。随机选择 x_i, $y_i \in Z_n$,使 $x_i \cdot y_i \equiv 1(\mathrm{mod}\Phi(n))$,选择素数 $p_i > y_i$,当 $i \neq j$ 时,使 $\gcd(p_i,p_j)=1$,群中心将 (x_i,p_i,p_i^d) 秘密送给群成员 U_i。U_i 验证等式 $p_i=(p_i^d)^e$ 成立后,将 (x_i,p_i,p_i^d) 作为自己的签名密钥保存起来。群中心秘密将 (ID_i,y_i) 发给群管理人员,其中 ID_i 是 U_i 的身份。现假设系统有 k 个成员,群中心利用中国剩余定理求出同余方程组 $c \equiv y_i(\mathrm{mod}p_i)$, $i=1,2,\cdots,k$ 的解为

$$c \equiv y_1P_1'P_1 + y_2P_2'P_2 + \cdots + y_kP_k'P_k(\mathrm{mod}P)$$

最后群中心将 (n,e,c) 作为群公钥发布。

1.2 群成员加入和撤销

群成员加入:

Alice 向群中心提出申请成为群中的一员。群中心选择 $x_{k+1} \in Z_n$,根据 $x_{k+1}y_{k+1} \equiv 1(\mathrm{mod}\Phi(n))$ 求出 y_{k+1},后选择素数 p_{k+1},使得 $p_{k+1} > y_{k+1}$,并且 $\gcd(p_{k+1},p_i)=1, i=1,2,\cdots,k$,将 y_{k+1}, p_{k+1} 加入并重新计算并发布新的 c。群中心将 $(x_{k+1},p_{k+1},p_{k+1}^d)$ 发送给 Alice 作为其签名密钥,将 $(\mathrm{ID}_{k+1},y_{k+1})$ 发给群管理人员。Alice 成功加入了群中。群中心重新计算 $c \equiv y_1P_1'P_1 + y_2P_2'P_2 + \cdots + y_kP_k'P_k + y_{k+1}P_{k+1}'P_{k+1}(\mathrm{mod}P)$ 并发布。

群成员撤销:

群中心将撤销群中成员 U_i,只需选一个随机数 y_i' 替代 y_i 重新计算 c。

$$c \equiv y_1P_1'P + y_2P_2'P + \cdots + y_i'P_i'P_i + y_kP_k'P_k(\mathrm{mod}P)$$

发布新的 c。群成员 U_i 撤销成功。

1.3 签名与验证

群成员签名:

群成员 U_j 使用 (x_j,p_j^d) 对消息 m 进行签名,只需要计算 $s_j=H(m)^{x_j}(\mathrm{mod}n)$,得到的 (m,s_j,p_j^d) 即为成员 U_j 对消息 m 的签名。

验证:

Bob 对签名 (m,s_j,p_j^d) 进行验证。由群中心的公钥 e,计算 $p_j \equiv (p_j^d)^e(\mathrm{mod}n)$ 与 $y_j \equiv c(\mathrm{mod}p_j)$,然后验证等式 $H(m) \equiv s_j^{y_j}(\mathrm{mod}n)$ 是否成立。若等式成立,则签名正确,否则签名错误。

1.4 签名的打开

群管理人员若需要对群签名进行打开,给出签名 (m,s_j,p_j^d) 后,计算 $p_j \equiv (p_j^d)^e(\mathrm{mod}n)$ 以及 $y_j \equiv c(\mathrm{mod}p_j)$,根据 y_j 找到相应的 ID_j,就找到了签名中签名者的身份。

2 基于陈方案的攻击

Chen 的基于中国剩余定理的群签名方案在系统建立时,基于 RSA 算法的思想,给每位群成员分发签名密钥时均需要模 n,其方案不能抵御共模攻击[7-8]。下面给出几种可能的攻击方案。

2.1 陷害攻击

任意的群成员 Mallory 可以伪造其他群成员如 Alice 的签名。

Mallory 持有自己的签名密钥 (x_M,p_M,p_M^d),根据群公钥 (n,e,c) 和中国剩余定理可以计算出 $y_M \equiv c(\mathrm{mod}p_M)$。由于 $x_My_M \equiv 1(\mathrm{mod}\Phi(n))$, $x_My_M = k\Phi(n)-1$,同时 $\gcd(e,\Phi(n))=1$,若 $(e,k\Phi(n))=a$,令 $k'=k/a$,则 $\gcd(e,k'\Phi(n))=1$。由于 $d'e \equiv 1\mathrm{mod}(k'\Phi(n))$,则 d' 是与群中心私钥 d 等效的密钥。因为 $(p_A^d)^e \equiv p_A(\mathrm{mod}n)$,则 $y_A \equiv c(\mathrm{mod}p_A)$,又因为 $\gcd(y_A,\Phi(n))=1$,则 $\gcd(y_A,k'\Phi(n))=1$。根据 $x_A'y_A \equiv 1(\mathrm{mod}k'\Phi(n))$ 可以求得 Alice 的私钥 x_A',由 $s_A \equiv H(m)^{x_A}(\mathrm{mod}n)$,Mallory 可以对消息 m 签名 (m,s_A,p_A^d) 来陷害 Alice,任何人也可以验证签名是合法的。

2.2 伪造攻击

任意的合法群成员 Mallory 可以伪造与群中心等效的私钥 d',他可以代替群中心让 Dave 成为群成员。Mallory 选择使 $y_D \equiv c(\mathrm{mod}p_D)$ 成立的 y_D 和素数 p_D,且 $\gcd(y_D,k'\Phi(n))=1$,可计算出 p_D^d;由 $x_Dy_D \equiv 1(\mathrm{mod}k'\Phi(n))$,求出 x_D,将 (ID_D,y_D) 发给群管理人员,(x_D,p_D,p_D^d) 发送给 Dave。Dave 可以使用群公钥 e 去验证并相信是群中心发来的。Dave 对消息 m 生成群签名 (m,s_D,p_D^d)。

通过 1.3 中的方法任何人可以去验证该签名,利用 1.4 中的方法管理员可以打开 Dave 的签名。在有争议的时候可以对群中心保存的所有 (x,p,p^d) 核对来证明 Dave 不是该群成员,这样 Dave 可以有很多伪造群签名的机会。

3　一种增强的基于中国剩余定理的方案

本节构造了一种使用 ElGamal 算法的基于中国剩余定理的群签名方案[9]。

3.1　系统构建

群中心选择一个大素数 p,一个 Hash 函数 h,随机选取 $g, x \in Z_p^*$,计算 $y \equiv g^x \pmod p$,将 (y,p,g) 作为其私钥,将 (x,p,g) 作为与之对应的公钥。群内有 k 个成员,群中心为每一个成员选择一个大素数 p_i ($i = 1,2,\cdots,k$),当 $i \neq j$ 时,$p_i \neq p_j$。群成员随机选取 $x_i \in Z_{p_i}^*$,根据 $y_i \equiv g^{x_i} \pmod{p_i}$ 计算出 y_i,保存 (x_i,p_i,g),将 (y_i,p_i,g^{x_i}) 发给群中心,群中心计算 $y_i \equiv g^{x_i} \pmod{p_i}$ 是否成立,成立则保存并将 (y_i,ID_i) 作为打开的依据发给群管理人员。群中心根据中国剩余定理求出 $c \equiv y_1P_1'P_1 + y_2P_2'P_2 + \cdots + y_kP_k'P_k \pmod P$,将 (x,p,g) 作为私钥保存,将 (y,p,g,c) 作为群公钥公开。

3.2　群成员加入与撤销

群成员加入:Alice 需要加入签名群中。Alice 向群中心申请,群中心选择不同于其他群成员的大素数 p_{k+1} 发送给 Alice,Alice 随机选择 $x_{k+1} \in Z_{p_{k+1}}^*$ 并根据 $y_{k+1} \equiv g^{x_{k+1}} \pmod{p_{k+1}}$ 计算出 y_{k+1},Alice 分别将 (x_{k+1},p_{k+1},g) 与 $(y_{k+1},p_{k+1},g^{x_{k+1}})$ 作为私钥保存和发给群中心,群中心验证后将 $(y_{k+1},\mathrm{ID}_{k+1})$ 发给群管理人员。群中心重新计算 c 并发布。

群成员撤销:群中心撤销成员 U_j,随机选择 $y_j'(y_j' \neq y_j \pmod{p_j})$,将 y_j 改为 y_j',其他成员密钥信息保持不变,重新计算 c 并发布,则群成员 U_j 撤销。

3.3　签名与验证

群成员签名:Alice 对消息 m 签名并加入时间戳 T[10],随机选取 k_A,计算 $a_A \equiv g^{k_A} \pmod{p_A}$,$s_A \equiv h(m,T)x_A - a_Ak_A \pmod{(p_A-1)}$,将 (m,a_A,s_A,p_A,T) 发给群中心,群中心收到后计算 $t = T' - T$ (T' 为收到签名的时间),如果超过规定时间则拒绝,否则计算 $y_A \equiv c \pmod{p_A}$ 后验证等式 $a_A^{a_A}g^{s_A} \equiv y_A^{h(m,T)} \pmod{p_A}$ 是否成立,若成立,确信 (m,a_A,s_A,p_A,T) 是 Alice 对消息 m 的签名。群中心随机选择 k 并使用自己的私钥 (x,p,g) 对消息进行重新签名:$a \equiv g^k \pmod p$,$s \equiv h(m)x - ak \pmod{(p-1)}$,则群对消息 m 的最终签名为 (m,r,s),为了打开签名,需要和 p_A 相关联。

验证签名:Bob 收到签名后,用群公钥 (y,p,g) 验证等式 $a^ag^s \equiv y^{h(m)} \pmod p$ 是否成立,成立则签名正确,否则不正确。

3.4　签名打开

某个签名有争议时,群中心可以对签名打开[11],首先找到与签名相关联的 p_i,计算 $y_i \equiv c \pmod{p_i}$ 后和群管理人员保存的成员公钥信息 (y_i,ID_i) 对照,可确定签名者的身份。

4　效率及安全性分析

文中的效率及安全性分析是基于文献[12-13]的方法。

4.1　效率分析

改进方案在成员加入时,每个群成员的个人私钥由群成员自己计算得到,不需要群中心为他们分别产生,分担了群中心一部分工作量,只需要群中心对每个群成员发送过来的信息进行验证,这样不需要群中心有高效的计算能力。而在其他环节的计算和原始方案类似。

4.2　抗合谋攻击

如果群内有 $k+1$ 个成员,即使 k 个成员合谋也无法求出第 $k+1$ 个成员的密钥对 $(x_{k+1},y_{k+1},p_{k+1})$。已知 k 组密钥对 $(x_i,y_i,p_i)(i = 1,2,\cdots,k)$ 与 $c \equiv y_1P_1'P_1 + y_2P_2'P_2 + \cdots + y_kP_k'P_k + y_{k+1}P_{k+1}'P_{k+1} \pmod P$ 可求得 y_{k+1} 和 p_{k+1},求 x_{k+1} 需要计算 $y_{k+1} \equiv g^{x_{k+1}} \pmod{p_{k+1}}$,由于其基于离散对数困难性的[14],所以求不出 x_{k+1},无法得到第 $k+1$ 个成员的密钥对 $(x_{k+1},y_{k+1},p_{k+1})$。

4.3　不可伪造性

Mallory 如果在 Alice 和群中心通信的时候截获了 Alice 的 p_A,仍然不可以伪造其签名。Alice 的私钥 x_A 在整个系统中都没有和任何人进行交换,是由 Alice 自己产生并保管的,如果要求,必须经过计算等式 $y_A \equiv g^{x_A} \pmod{p_A}$ 来求得,又由于等式是基于离散对数困难性的,所以任何人无法伪造 Alice 的签名,即使是和群中心合谋。

5　结束语

文中对陈等提出的基于中国剩余定理的群签名方案的安全性进行了分析,由于其在系统建立时是基于共模的,所以其存在成员被陷害和伪造成员签名的攻击,在此基础上给出了一种用 ElGamal 算法构造的基于中国剩余定理的群签名方案。该方案在成员创建和撤销时和原方案同样快捷,同时该方案是非共模的,可以抵抗共模攻击,成员私钥由成员自己产生,保证了群成员私钥安全性的同时减轻了群中心的计算负担。

参考文献:

[1] Chaum D, van Heyst E. Group signatures[C]//Proc of EUROCRYPT'91. [s. l.]: [s. n.], 1991: 257-265.

[2] Boneh D, Boyen X, Shacham H. Short group signatures[C]// Proc of CRYPTO 2004. [s. l.]: Springer-Verlag, 2004.

[3] 陈泽文,张龙军,王育民,等. 一种基于中国剩余定理的群

(下转第 181 页)

户不知晓的情况下无限制发送信息,造成的经济损失也不可估量。

2.3.4　隐私窃取

绝大多数恶意软件都含有隐私窃取行为,可能窃取的用户隐私多种多样,包括 SMS 消息、手机号码、用户账户、密码等。由于 SMS 信息中可能含有用户证书,所以凡是收集 SMS 信息的行为都应高度关注。

3　结束语

通过分析总结已知 Android 平台下恶意代码行为特征,可以看出,Android 恶意软件行为多种多样。八成以上恶意软件重包装其他合法 app。然而,检测每天出现的大量 app 是否经过重包装是一个巨大挑战,同时大量第三方 Android 市场上众多 app 的出现也增加了检测难度。超过三分之一的 Android 恶意软件发掘平台漏洞来提升它们的权限。此外,由于缺乏对相关 API 的良好控制,半数左右的恶意软件在后台通过 SMS 信息订购收费服务。

当前 Android 市场存在众多问题,然而现存的手机安全防护软件依然落后于恶意代码技术的发展,不能提供有力保障。传统的基于签名方法并不适用于手机恶意软件检测,同时由于手机资源和电池容量约束,在手机上部署复杂的监测技术也不现实。因此,提出有效的手机恶意软件检测技术与模型至关重要。

参考文献:

[1] 王　伟. Android 病毒行为自动分析工具的设计与实现[D]. 天津:南开大学,2012.

[2] 吕海军,陈前斌,吴小平. 智能手机病毒的发展及其对策研究[J]. 信息安全与通信保密,2008(1):80-82.

[3] 杨卫军,余彦峰,张佩军. Android 手机恶意软件取证技术研究[J]. 警察技术,2012(5):8-11.

[4] 翁雪城,场零江. 恶意代码的分析与检测技术的研究[J]. 科技资讯,2012(5):19-20.

[5] Christodorescu M,Jha S. Static analysis of executables to detect malicious patterns[C]//Proceedings of the 12th conference on USENIX security. Berkeley,CA,USA:[s. n.],2003.

[6] 孙润康,展　娴,邵玉如,等. Android 手机安全检测与取证分析系统[J]. 信息网络安全,2013(3):71-74.

[7] 童振飞,杨　庚. Android 平台恶意软件的静态行为检测[J]. 江苏通信,2011,5(1):39-42.

[8] Rieck K,Holz T,Willems C,et al. Learning and classification of malware behavior[C]//Proc of detection of intrusions and malware,and vulnerability assessment. [s. l.]:[s. n.],2008:108-125.

[9] Christodorescu M,Jha S,Kruegel C. Mining specifications of malicious behavior[C]//Proceedings of the 1st India software engineering conference. [s. l.]:[s. n.],2008:5-14.

[10] Egele M,Scholte T,Kirda E,et al. A survey on automated dynamic malware analysis techniques and tools[J]. ACM Computing Surveys,2012,44(2):6-47.

[11] Burguera I,Zurutuza U,Nadjm-Tehrani S. Crowdroid:behavior-based malware detection system for Android[C]//Proceedings of the 1st ACM workshop on security and privacy in smartphones and mobile devices. Chicago:ACM,2011:15-26.

[12] Schmidt A D,Bye R,Schmidt H G,et al. Static analysis of executables for collaborative malware detection on Android[C]//Proc of IEEE international conference on communications. Dresden:IEEE,2009:1-5.

[13] 吴俊昌,骆培杰,程绍银,等. 基于权限分类的 Android 应用程序的静态分析[C]//第四届信息安全漏洞分析与风险评估大会. 北京:出版者不详,2011:41-48.

[14] Zhou Yajin,Jiang Xuxian. Dissecting Android malware:characterization and evolution[C]//Proc of IEEE symposium on security and privacy. San Francisco,CA:IEEE,2012:95-109.

(上接第 177 页)

签名方案[J]. 电子学报,2004,32(7):1062-1065.

[4] ElGamal T. A public key cryptosystem and a signature scheme based on discrete logarithms[J]. IEEE Transactions on Information Theory,1985,31(4):469-472.

[5] Ateniese G,Song D,Tsudik G. Quasi-efficient revocation of group signatures[J]. LNCS,2003,2357:183-197.

[6] Rivest R L,Shamir A,Adleman L. A method for obtaining digital signatures and public key cryptosystems[J]. Communications of ACM,1978,21(2):120-126.

[7] 史来婧. 基于中国剩余定理的群签名方案的研究[D]. 西安:西安电子科技大学,2012.

[8] 李新社. 群签名安全性分析与改进研究[C]. 西安:西安电子科技大学,2009.

[9] 邓宇乔. 基于动态属性的数字签名方案[J]. 计算机工程与应用,2013,49(15):19-22.

[10] 陈辉焱,李　巍,苏艳芳. 一种基于证书的代理环签名方案[J]. 计算机工程,2012,38(16):149-152.

[11] 程小刚,王　箭,杜吉祥. 群签名综述[J]. 计算机应用研究,2013,30(10):2881-2886.

[12] 陈道伟,施荣华,樊翔宇. 存在可实施强制签名特权集的门限群签名方案[J]. 计算机应用研究,2012,29(1):319-321.

[13] 黄　斌,史　亮,邓小鸿. 一个群签名方案的安全性分析[J]. 计算机工程,2013,39(4):151-153.

[14] Diffie W,Hellman M E. New directions in cryptograph[J]. IEEE Transactions on Information Theory,1976,22(6):644-654.

一种加强的基于中国剩余定理的群签名

作者： 周素芳， 杨晓博， 刘新， ZHOU Su-fang， YANG Xiao-bo， LIU Xin

作者单位： 周素芳,杨晓博,ZHOU Su-fang,YANG Xiao-bo(陕西师范大学 计算机科学学院,陕西 西安,710119)， 刘新,LIU Xin(陕西师范大学 计算机科学学院，陕西 西安 710119; 内蒙古科技大学 信息工程学院，内蒙古 包头 014010)

刊名： 计算机技术与发展 ISTIC

英文刊名： Computer Technology and Development

年，卷(期)： 2014(11)