隐私增强直接匿名证明方案研究

陈小峰,冯登国
(中国科学院软件研究所信息安全国家重点实验室中国科学院研究生院,北京 100080)

摘 要: 直接匿名证明方案中采用的匿名性机制是一种"验证者相关的完全或无"保护方案,该保护方案的匿名选择方式比较单一,不能很好的满足实际的需求,如何提高匿名性机制的灵活性是直接匿名证明方案应用的重要问题.本文分析了目前直接匿名证明中匿名性机制的问题,提出了子群隐私增强保护方案并给出了两种实现方式,子群隐私增强保护方案扩展了原始的直接匿名证明方案,为小群体内的隐私性保护提供了可行途径,本文比较分析了两种实现方式的性能和安全性.

关键词: 直接匿名证明; 可信计算平台; 可信平台模块; 匿名认证
中图分类号: TP309 **文献标识码:** A **文章编号:** 0372-2112 (2011) 09-2166-07

Researches on Privacy Enhanced Direct Anonymous Attestation Scheme

CHEN Xiao-feng, FENG Deng-guo
(*State Key Laboratory of Information Security, Institute of Software, Chinese Academy of Sciences, Beijing* 100080, *China*)

Abstract: The direct anonymous attestation proposed by Brickell adopts an anonymous scheme which is "all or none" for verifiers, and the direct anonymous scheme is applicable for only a few scenarios, which can not satisfy the needs in several cases. To design a flexible anonymous scheme becomes a critical issue for deploying the trusted computing platform. We analyze the problems of the anonymous scheme and propose the direct anonymous scheme with sub-group privacy enhancement properties. This proposed scheme provides the privacy solution for the small group, of which we propose two schemes and analyze the performance and security.

Key words: direct anonymous attestation; trusted platform; trusted platform module; anonymous authentication

1 引言

在可信计算组织(TCG)[1]给出的可信计算平台实现方案中,可信平台模块(TPM)是可信计算平台的核心和基础,TPM是嵌入在主机中的一个防篡改的安全芯片,该安全芯片唯一标识了可信计算平台的身份.TPM出厂时都会绑定一个根密钥,不同的TPM拥有不同的根密钥,如果所有的远程认证都基于该根密钥,可信计算平台的隐私性无法得到保障.因此在可信计算平台与远程通信方交互时,需要提供一种远程匿名认证机制来保护可信计算平台的隐私性,在不暴露可信计算平台身份的同时进行远程认证.其中,在TPM规范中提出了两种方案来解决可信计算平台的隐私性保护问题.TPM v1.1规范提出的方案基于一个称为隐私CA(Privacy-CA)的可信第三方.其实现方案如下:TPM首先产生一对称为AIK的RSA公私钥对.然后,TPM将AIK公钥发送给Privacy-CA,请求产生AIK的公钥证书,同时,TPM向Privacy-CA证明其拥有一个真实的EK身份密钥.Privacy-CA给AIK签发证书.在验证阶段,TPM将AIK证书发送给验证者.通过这种方式,可信计算平台可以在通信过程中隐藏自己的真实身份.该方案的最大缺点就是每次通信过程都需要经过Privacy-CA,因此Privacy-CA成为系统的瓶颈.同时,攻击方如果攻陷了Privacy-CA,可信计算平台的隐私性就无从谈起.

为了克服以上的不足,TPM v1.2规范采纳了Brickell等人提出的直接匿名证明方案(Direct Anonymous Attestation, DAA)[2].在这个方案中,TPM无需Privacy-CA的帮助就可以直接向远程验证者证明可信计算平台的真实性.在下文的讨论中将Brickell等人提出的DAA方案称为BCC方案.BCC方案本身存在一些问题阻碍其在可信计算平台中的应用.第一个问题是方案本身非常复杂,主要适用于具有比较强的计算能力的设备如个人计算机,服务器等,针对这个问题,He Ge等人提出一种更适合于嵌入式设备的直接匿名证明方案(HS方案)[3].第二个问题是BCC方案中的可变匿名性机制和TPM的撤销机制不够灵活,阻碍了其在某些特定场合的应用,

收稿日期:2008-01-23;修回日期:2011-01-08

这是因为在 BCC 方案中,只有当 TPM 的秘密已经被泄露,并且公开发布的情况下才能撤销非法的 TPM,为了提高 BCC 方案撤销机制的灵活性,在文献[4]中,作者给出了一种新的撤销方法,即使 TPM 的秘密没有被泄露,也可以撤销 TPM,同时在文献[5,6]中,作者对 BCC 方案进行了扩展,增强了 BCC 方案的隐私性保护.

在 BCC 方案中,其匿名性机制是建立在基名(base name)的基础上,BCC 方案为基名的选择提供了两种选项:如果基名是随机选择的,那么任意两次生成的签名都是不可关联的(unlinkable);如果基名是由验证方选定的,生成的签名是可以关联的,在某一个给定的时间内,如果基名没有变化,那么对于验证者来说在该时间段内签名是可关联的,可信计算平台就没有隐私性可言.在本文中将这种匿名性机制称为"验证者相关的完全或无"匿名性.无论是 BCC 方案还是 HS 方案,都采用了这种"验证者相关的完全或无匿名性".

针对这种"完全或无匿名性",本文提出了更加灵活的匿名性机制,称为子群隐私增强保护方案,这种匿名性机制的一个特点是,子群内的成员签名不仅能证明平台是可信计算平台,还能证明该可信计算平台是属于某个特定的群体,该方案为可信计算平台在小群体如局域网内的认证应用提供了解决方案.

2　预备知识

2.1　知识签名

在构造直接匿名证明方案时用到了知识签名这一工具,它允许一方在不泄露任何有用信息的情况下证明他知道一个秘密值,这种工具本质上是知识的零知识证明或最小泄露证明.

基于离散对数的零知识证明协议已有很多相关研究成果,为了描述这些协议,本文将采用 Camenisch 和 Stadler 给出的标记法[7]来描述基于离散对数的零知识证明协议,例如

$$\mathrm{PK}\{\alpha,\beta,\delta: y = g^{\alpha}h^{\beta} \wedge \tilde{y} = \tilde{g}^{\alpha}\tilde{h}^{\delta} \wedge (u \leqslant \alpha \leqslant v)\}$$

表示"关于整数 α,β,δ 的零知识证明,并且 $y = g^{\alpha}h^{\beta}$,$\tilde{y} = \tilde{g}^{\alpha}\tilde{h}^{\delta}$ 成立,同时 $u \leqslant \alpha \leqslant v$"其中的 $y,g,h,\tilde{y},\tilde{g},\tilde{h}$ 是群 $G = \langle g\rangle = \langle h\rangle$ 和群 $\tilde{G} = \langle\tilde{g}\rangle = \langle\tilde{h}\rangle$ 中的元素.同时可以利用 Fiat-Shamir 启发式[8]将零知识证明转化为对消息 m 的知识签名,如可以记作:$\mathrm{SPK}\{(\alpha): y = g^{\alpha}\}(m)$.

2.2　CL 签名方案

BCC 方案基于 Camenisch-Lysyanskaya(CL)签名方案[9]而构建,该签名方案的最大特点就是设计了一个高效的关于签名的零知识证明协议.

密钥生成　输入 1^k,选择一个特殊 RSA 模 $n = pq$,$p = 2p' + 1$,$q = 2q' + 1$.随机选择 $R_0,\cdots,R_{L-1},S,Z \in QR_n$,输出公钥$(n,R_0,\cdots,R_{L-1},S,Z)$和秘密私钥 p,q,l_n 是 n 的长度.

签名算法　设 l_m 是一个参数,那么输入$(m_0,\cdots,m_{L-1})$,其中 $m_i \in \pm\{0,1\}^{l_m}$,选择一个随机数 e,长度为 $l_e > l_m + 2$,以及一个随机数 v,长度为 $l_v = l_n + l_m + l_r$,其中 l_r 是安全参数.计算 A 使得 $Z \equiv R_0^{m_0}\cdots R_{L-1}^{m_{L-1}}S^vA^e \pmod n$,消息$(m_0,\cdots,m_{L-1})$的签名是$(e,A,v)$.

验证算法　为了验证(e,A,v)是$(m_0,\cdots,m_{L-1})$的合法签名,检查 $Z \equiv R_0^{m_0}\cdots R_{L-1}^{m_{L-1}}S^vA^e \pmod n$,并且检查 $2^{l_e} > e > 2^{l_e-1}$.

2.3　BCC 方案

BCC 方案主要包括了以下几个参与方:(1)颁发者(Issuer),该参与方是发布签名的机构,运行 CL 签名方案的密钥生成算法生成公钥(n,S,Z,R_0,R_1)和私钥 p,q;(2)可信计算平台(Host/TPM),该参与方是带有 TPM 的可信计算平台;(3)验证者(Verifier),验证签名的参与方.

BCC 方案是基于 CL 签名方案构建的.BCC 方案的基本过程是:TPM 选择一个秘密的"消息"f,与颁发者执行一个交互式协议,从颁发者得到对该"消息"f 的 CL 签名,然后 TPM 可以通过关于 CL 签名的零知识证明匿名地向远程验证方证明 TPM 拥有对秘密"消息"f 的 CL 签名.为了检测出假冒 TPM,TPM 必须同时向远程验证方发送假名 $N_V = \zeta^f$,证明 N_V 是通过秘密"消息"f 计算出来的,其中的 ζ 称为基名(base name).在 BCC 方案中,匿名性的控制主要是通过基名完成的.如果在每次做 DAA 签名时基名都是随机选择的,那么 N_V 也是随机的,生成的 DAA 签名具有完全的匿名性.如果基名是由远程验证方预先选定的,那么每次可信计算平台进行签名时生成的 N_V 都是相同的,任意两个签名都可以通过 N_V 关联.下面简单地回顾一下 BCC 方案的各个过程,具体的协议流程可以参考文献[2].

DAA-Join 协议　该协议的参与方是颁发者和可信计算平台,首先可信计算平台生成一个秘密消息 f,然后将其拆分成 f_1 和 f_2.TPM 发送 $U = R_0^{f_0}R_1^{f_1}S^{v'}$ 和 $N_I = \zeta^{f_0+f_1 2^{l_f}}$,其中的 v' 是 TPM 随机选择的.并且通过零知识证明协议证明 U 和 N_I 被正确地构造.DAA 颁发者计算 $A = (Z/(US^{v''}))^{1/e} \bmod n$,将$(A,e,v'')$发送给 TPM,那么 TPM 得到$(f_0,f_1)$的 CL 签名就是$(A,e,v = v' + v'')$.

DAA-Sign 操作　在这个操作中,可信计算平台用秘密消息(f_0,f_1)和(A,e,v)对 TPM 产生的 AIK 公钥进行知识签名.其本质是零知识地证明可信计算平台掌握秘密(f_0,f_1)和 CL 签名(A,e,v),满足 $A^eR_0^{f_0}R_1^{f_1}S^v \equiv Z \bmod n$,TPM 同时计算 $N_V = \zeta^{f_0+f_1 2^{l_f}} \bmod \Gamma$,证明 N_V 是通

过秘密(f_0,f_1)计算的.

DAA-Verify 操作 在这个操作中,验证者验证通过 DAA-Sign 得到的签名的合法性.

定理 1[2] 在$\langle\gamma\rangle$群的 DDH 假设和强 RSA 假设下,BCC 方案实现了一个安全的直接匿名证明系统,满足不可伪造性,匿名性和不可关联性.

3 子群隐私增强保护方案

在 BCC 方案中,可信计算平台通过 DAA-Join 过程加入到由颁发者确定的一个 DAA 群中,并且该过程一般在可信计算平台出厂前完成.如第 1 节所述,可信计算平台的签名匿名性是"完全或无"的,如果验证方不仅要求可信计算平台证明其拥有颁发者颁发的 DAA 证书,更进一步地,要求其来自于某个特定的子群群体(如具有某个特定的属性),BCC 方案的签名不能够满足这一需求.本节提出了粒度更细,灵活性更高的隐私性保护方案——子群隐私增强保护方案,子群隐私增强保护方案不仅能证明可信计算平台拥有可信的颁发者颁发的 DAA 证书,而且还能证明可信计算平台属于某个特定群体.子群隐私增强保护方案可以应用在 VPN 以及局域网内,如在局域网中可以应用子群隐私增强保护方案,某种资源只有局域网内特定的可信计算平台才能访问,这就要求对访问的可信计算平台进行匿名认证,同时验证方不能对可信计算平台的身份进行追踪.

子群隐私增强保护方案的应用基本框架如图 1 所示.

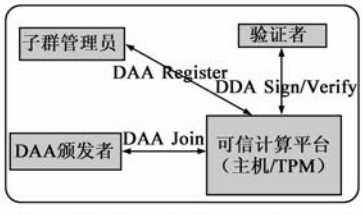

图1 带子群隐私增强保护的直接匿名证明方案

定义 1 带子群隐私增强保护的直接匿名证明方案是由如下几个参与方构成的签名方案:颁发者(Issuer),子群管理员,可信计算平台,验证者.它由下面几个过程构成:

■ 初始化过程(DAA-Setup):给定安全参数 1^k,颁发者产生系统公钥和私钥;

■ 加入过程(DAA-Join):可信计算平台和颁发者之间的一个交互式协议.通过这个协议,可信计算平台得到成员证书和成员私钥;

■ 注册过程(DAA-Register):可信计算平台与子群管理员之间的交互协议,通过这个协议,可信计算平台申请成为子群的一个成员,并发送相关注册信息给子群管理员,子群管理员验证相关信息,将该成员加入相应的子群,并更新子群成员.子群管理员维护两个列表,分别为子群成员有效列表和子群成员撤销列表;

■ 签名过程(DAA-Sign):可信计算平台使用成员证书和成员私钥对给定的消息做匿名签名;

■ 成员更新过程(DAA-Update):子群管理员执行的操作,更新子群成员有效列表和子群成员撤销列表.

直接匿名证明方案必须满足如下的安全特性:

■ 不可伪造性(Unforgeability):有效的成员证书只有 TPM 和颁发者通过加入过程得到,只有拥有成员证书的可信计算平台才能对消息 m 做匿名签名;

■ 匿名性(Anonymity):除非 TPM 出现在撤销列表中,否则不能通过签名确认签名者(即可信计算平台)的身份.可信计算平台的签名不仅对于颁发者是匿名的,对子群管理员也是匿名的;

■ 不可关联性(Unlinkability):验证者确定两个不同的签名是否来自于同一个 TPM 在计算上是困难的.

讨论 1:带子群隐私增强保护的直接匿名证明方案构建在 2.3 节给出的 BCC 方案的基础上,与 BCC 方案不同的是,增加一个子群管理员,并且增加了注册过程和成员更新过程,签名过程也与 BCC 方案有所不同,在下面给定的方案描述中,与 BCC 方案相同的过程将不再描述.

3.1 方案Ⅰ

主要思想:子群管理员维护一个成员有效列表 E_{add} 和成员撤销列表 E_{del},首先子群成员通过 DAA-Register 过程加入子群,在签名时,子群成员 A 做知识签名证明 $\{A:A\in E_{\text{add}}\wedge A\notin E_{\text{del}}\}$.

注册阶段(DAA-Register) 可信计算平台发送基名-假名对$\langle\zeta,N\rangle$给子群管理员,其中 N 是通过可信平台模块的秘密 f 计算出来的($N=\zeta^f \bmod \Gamma$),子群管理员对可信计算平台进行认证,确认该基名-假名对是由符合条件的可信计算平台产生.子群管理员维护两个列表(1)基名-假名对有效列表 E_{add},初始时 $E_{\text{add}}=\{\}$;(2)基名-假名对撤销列表 E_{del},初始时 $E_{\text{del}}=\{\}$.具体步骤为:

(1)可信计算平台利用 TPM 持有的秘密消息 f_i 计算 $N_i=\zeta_i^{f_i} \bmod \Gamma$.将元组$\langle\zeta_i,N_i\rangle$发送给子群管理员;

(2)可信计算平台与子群管理员执行零知识证明交互协议 $\text{PK}\{f_i:N_i=\zeta_i^{f_i}(\bmod\Gamma)\}$,证明$\langle\zeta_i,N_i\rangle$是由可信计算平台产生的;

(3)子群管理员将元组$\langle\zeta_i,N_i\rangle$放入 E_{add}列表,形成新的基名-假名对有效列表 $E'_{\text{add}}=E_{\text{add}}\cup\{\langle\zeta_i,N_i,P_i\rangle\}=\{\langle\zeta_1,N_1,P_1\rangle\cdots\langle\zeta_i,N_i,P_i\rangle\cdots\langle\zeta_n,N_n,P_n\rangle\}$,其中 P_i 是成员在子群中的标识信息.

签名过程(DAA-Sign)　首先可信计算平台与验证方协商选取 E_{add}列表中几个成员作为其匿名隐藏的对象,记为 S_{add},可信计算平台代表 S_{add}中的成员签名,同时在 E_{del}中选取集合 S_{del},证明可信计算平台不在集合 S_{del}中.该签名过程是对 BCC 方案的 DAA-Sign 进行了扩展,分为两个步骤,第一步是进行 BCC 方案的 DAA-Sign 操作,具体的签名可以参考文献[2];之后进行第二阶段的证明,具体步骤如下:

(1)首先从有效列表 E_{add}中选择 t 个基名-假名对(验证者和签名者协商建立),记为 S_{add},其中 $N_1=\zeta_1^f$, $N_2=\zeta_2^f,\cdots,N_t=\zeta_t^f$;并在撤销列表中选择 $S_{\text{del}}\subseteq E_{\text{del}}$;

(2)可信计算平台证明 TPM 持有的秘密 f 满足

$$\{f: f\in S_{\text{add}}=\{\langle N_1,\zeta_1\rangle,\cdots,\langle N_t,\zeta_t\rangle\}\wedge f\notin S_{\text{del}}=\{\langle N_1',\zeta_1'\rangle,\cdots,\langle N_t',\zeta_t'\rangle\}\},$$

为了叙述方便,签名操作分为两步(两步可以合并一起执行):第一步执行 BCC 方案的 DAA-Sign 操作,得到签名 σ_1,第二步执行下面的知识签名得到 σ_2:

$$\sigma_2=\text{SPK}\{f:(N_1\equiv\zeta_1^f \bmod\Gamma\vee\cdots\vee N_t\equiv\zeta_t^f \bmod\Gamma)\wedge N_1'\neq(\zeta_1')^f \bmod\Gamma\wedge\cdots\wedge N_t'\neq(\zeta_t')^f \bmod\Gamma\}(m)$$

不失一般性,假设 $N_i=\zeta_i^f \bmod\Gamma$,其具体的签名操作步骤如下:

(a)证明者选择 $v_1,v_2,\cdots,v_t,w_1,\cdots,w_{i-1},w_{i+1}\cdots w_t$,计算

$$t_1=N_1^{-w_1}\zeta_1^{v_1}\bmod\Gamma,\cdots,t_{i-1}=N_{i-1}^{-w_{i-1}}\zeta_{i-1}^{v_{i-1}}\bmod\Gamma,t_i=\zeta_i^{v_i}\bmod\Gamma,t_{i+1}=N_{i+1}^{-w_{i+1}}\zeta_{i+1}^{v_{i+1}}\bmod\Gamma,\cdots,t_t=N_t^{-w_t}\zeta_t^{v_t}\bmod\Gamma$$

(b)$r=v_i$,对于 $j=1,\cdots,t$,可信计算平台做如下的操作

(ⅰ)可信计算平台选择 $x_j\xleftarrow{R}\{0,1\}^{l_\rho}$;

(ⅱ)可信计算平台计算承诺值

$$U_j=(\zeta_j')^{x_j}\bmod\Gamma,V_j=(N_j')^{x_j}\bmod\Gamma,W_j=U_j^f\bmod\Gamma;$$

(ⅲ)可信计算平台选择 $r_j\xleftarrow{R}\{0,1\}^{l_\rho}$;

(ⅳ)可信计算平台计算

$$\tilde{U}_j=(\zeta_j')^{r_j}\bmod\Gamma,\tilde{V}_j=(N_j')^{r_j}\bmod\Gamma,\tilde{W}_j=U_j^{r_j}\bmod\Gamma;$$

(c)计算 $c=H(\zeta_1\|N_1\|\cdots\|\zeta_t\|N_t\|\zeta_1'\|N_1'\|\cdots\|\zeta_t'\|N_t'\|t_1,\cdots\|t_t\|\tilde{U}_1\|\tilde{V}_1\|\tilde{W}_1\|\cdots\|\tilde{U}_t\|\tilde{V}_t\|\tilde{W}_t\|m)$

(d)$c_1=w_1,\cdots,c_{i-1}=w_{i-1},c_i=c-(c_1+c_2\cdots+c_{i-1}+c_{i+1}\cdots+c_t),c_{i+1}=w_{i+1},\cdots,c_t=w_t$;

(e)对于 $j=1,\cdots,t$,可信计算平台计算 $s_j=r_j+cx_j,s=r+cf$;

(f)$s_1'=v_1,\cdots,s_{i-1}'=v_{i-1},s_i'=v_i+c_if,s_{i+1}'=v_{i+1},\cdots,s_t'=v_t$;

(g)得到的签名为

$$\sigma_2=(U_1,V_1,W_1,\cdots,U_t,V_t,W_t,c_1,\cdots,c_t,s_1,\cdots,s_t,s,s'_1,\cdots,s'_t);$$

(3)最后得到签名 $\sigma=(\sigma_1,\sigma_2)$.

验证阶段(DAA-Verify)　首先利用过程 BCC 方案的 DAA-Verify 过程验证 σ_1 的合法性,σ_2 的验证过程如下,计算如下的信息:

(1)计算

$$\hat{t}_1=N_1^{-c_1}\zeta_1^{s_1'},\cdots,\hat{t}_i=N_i^{-c_i}\zeta_i^{s_i'},\cdots,\hat{t}_t=N_t^{-c_t}\zeta_t^{s_t'}\quad(1)$$

(2)对于 $j=1,\cdots,t$,验证者验证

(a)$U_j,V_j,W_j\overset{?}{\in}\pm\{0,1\}^{l_\Gamma},s_j\overset{?}{\in}\pm\{0,1\}^{l_\Gamma},V_j\overset{?}{\neq}W_j$

(b)验证者计算

$$\hat{U}_j=U_j^{-c}(\zeta_j')^{s_j}\bmod\Gamma,\quad\hat{V}_j=V_j^{-c}(N_j')^{s_j}\bmod\Gamma,\hat{W}_j=W_j^{-c}U_j^s\bmod\Gamma\quad(2)$$

检查如下的等式:

$$c_1+c_2+\cdots+c_t\overset{?}{=}H(\zeta_1\|N_1\|\cdots\|\zeta_t\|N_t\|\zeta_1'\|N_1'\|\cdots\|\zeta_t'\|N_t'\|\hat{t}_1,\cdots\|\hat{t}_t\|\hat{U}_1\|\hat{V}_1\|\hat{W}_1\|\cdots\|\hat{U}_t\|\hat{V}_t\|\hat{W}_t\|m)$$

成员更新(DAA-Update)　管理员如需要撤销某个成员$\langle\zeta_i,N_i,P_i\rangle$,将其从列表 E_{add}中删除 $E_{\text{add}}=E_{\text{add}}-\{\langle\zeta_i,N_i,P_i\rangle\}$,并将其加入 $E_{\text{del}}=E_{\text{del}}\cup\{\langle\zeta_i,N_i,P_i\rangle\}$.

安全性分析:

引理 1　方案 I 中的签名所基于的交互式协议是诚实验证者关于知识 f 的统计零知识证明.

证明:关于该协议的零知识证明是比较直观的,下面主要证明该协议是个知识证明协议.也就是要给出一个关于所证明知识的提取器(Knowledge Extractor).假设存在一个知识提取器能回绕调用(rewind)协议中的证明者.证明者发送 $U_j,V_j,W_j,\tilde{U}_j,\tilde{V}_j,\tilde{W}_j,j=1,\cdots,t$ 和 $t_1,\cdots,t_t$ 给验证者,其中 $V_j\neq W_j,j=1,\cdots,t$.为了响应挑战值 c,证明者响应 $s_1,\cdots,s_t,s,s_1',\cdots,s_t'$.为了响应挑战 $c'\neq c$,证明者响应 $\tilde{s}_1,\cdots,\tilde{s}_t,\tilde{s},\tilde{s}_1',\cdots,\tilde{s}_t'$.即给定元组

$$(U_1,V_1,W_1,\tilde{U}_1,\tilde{V}_1,\tilde{W}_1,\cdots,U_t,V_t,W_t,\tilde{U}_t,\tilde{V}_t,\tilde{W}_t,t_1,\cdots,t_t,c_1,\cdots,c_t,s_1,\cdots,s_t,s,s_1',\cdots,s_t')$$

$$(U_1,V_1,W_1,\tilde{U}_1,\tilde{V}_1,\tilde{W}_1,\cdots,U_t,V_t,W_t,\tilde{U}_t,\tilde{V}_t,\tilde{W}_t,t_1,\cdots,t_t,c_1',\cdots,c_t',\tilde{s}_1,\cdots,\tilde{s}_t,\tilde{s},\tilde{s}_1',\cdots,\tilde{s}_t')$$

其中:$c_1+c_2\cdots+c_t=c,c_1'+c_2'\cdots+c_t'=c'$,提取出知识 f.

由于方程(1)和(2)中的等式成立,因此有:

$$N_1^{c_1}\zeta_1^{s_1}=N_1^{c_1'}\zeta_1^{\tilde{s}_1'},\cdots,N_i^{c_i}\zeta_i^{s_i}=N_i^{c_{i-1}'}\zeta_i^{\tilde{s}_{i-1}'},\cdots,N_t^{c_t}\zeta_t^{s_t}=N_t^{c_t'}\zeta_t^{\tilde{s}_t'}\quad(3)$$

$$U_1^{-c}(\zeta_1')^{s_1}=U_1^{-c'}(\zeta_1')^{\tilde{s}_1},V_1^{-c}(N_1')^{s_1}=$$

$$V_1^{-c'}(N_1')^{\tilde{s}_1}, W_1^{-c}U_1^{s} = W_1^{-c'}U_1^{\tilde{s}}, \cdots,$$
$$U_t^{-c}(\zeta_t')^{s_t} = U_t^{-c'}(\zeta_t')^{\tilde{s}_t}, V_t^{-c}(N_t')^{s_t} =$$
$$V_t^{-c'}(N_t')^{\tilde{s}_t}, W_t^{-c}U_t^{s} = W_t^{-c'}U_t^{\tilde{s}} \quad (4)$$

假设

$$\Delta c = c - c', \Delta c_1 = c_1 - \tilde{c_1'}, \cdots, \Delta c_t = c_t - \tilde{c_t'},$$
$$\Delta s_1 = s_1 - \tilde{s}_1, \cdots, \Delta s_j = s_j - \tilde{s}_j, \cdots,$$
$$\Delta s_t = s_t - \tilde{s}_t, \Delta s = s - \tilde{s}, \Delta s_1' = s_1' - \tilde{s}_1', \cdots,$$
$$\Delta s_j' = s_j' - \tilde{s}_j', \cdots, \Delta s_t' = s_t' - \tilde{s}_t'$$

考虑等式(3)和(4),变换得到

$$N_1^{\Delta c_1} = \zeta_1^{\Delta s_1'}, \cdots, N_i^{\Delta c_i} = \zeta_i^{\Delta s_i'}, \cdots, N_t^{\Delta c_t} = \zeta_t^{\Delta s_t'}, U_j^{\Delta c} = (\zeta_j')^{\Delta s_j}, (N_j')^{\Delta s_j} = V_j^{\Delta c}, W_j^{\Delta c} = U_j^{\Delta s}, j = 1, \cdots, t$$

令 $\hat{x}_j = \Delta s_j / \Delta c \bmod \Gamma, j = 1, \cdots, t, \hat{f} = \Delta s / \Delta c = \Delta s_i / \Delta c_i \bmod \Gamma$,

并且 $\hat{f} = \Delta s_i / \Delta c_i \in \{\Delta s_1'/\Delta c_1, \Delta s_2'/\Delta c_2, \cdots, \Delta s_i'/\Delta c_i, \cdots, \Delta s_t'/\Delta c_t\}$,

得到对于 $j = 1, \cdots, t, (\zeta_j')^{\hat{x}_j} = U_j, N_j^{\hat{x}_j} = V_j, U_j^{\hat{f}} = W_j, (\zeta_j')^{\hat{f}} = N_j$ (5)

根据方程式(5),得到

$$(\zeta'_j)^{\hat{x}_j \cdot \hat{f}} = W_j, N_j^{\hat{x}_j} = V_j, j = 1, \cdots, t,$$

因此 $\zeta_j^{\hat{f}} = W_j^{1/\hat{x}_j}, N_j = V_j^{1/\hat{x}_j}, j = 1, \cdots, t$

因为 $V_j \neq W_j, j = 1, \cdots, t$,所以 $V_j^{1/\hat{x}_j} \neq W_j^{1/\hat{x}_j}, j = 1, \cdots, t$,因此 $N_j \neq (\zeta_j')^{\hat{f}}, j = 1, \cdots, t$,也就是说,知识提取器得到 $\hat{f}$ 使得 $(\zeta_j')^{\hat{f}} \neq N_j, j = 1, \cdots, t$,并且 $\hat{f} \in \{\langle \zeta_1, N_1 \rangle, \cdots, \langle \zeta_t, N_t \rangle\}$ 即 $\{\hat{f}: N_1 = (\zeta_1)^{\hat{f}} \vee \cdots \vee N_1 = (\zeta_i)^{\hat{f}} \cdots \vee N_t = (\zeta_t)^{\hat{f}}\}$. 证毕.

定理 2 在$\langle\gamma\rangle$群的 DDH 假设和强 RSA 假设下,方案Ⅰ实现了一个安全的直接匿名证明系统.

证明:根据定理 1 可得,BCC 方案安全地实现了一个直接匿名证明系统,也即满足不可伪造性、匿名性与不可关联性,而方案Ⅰ是在 BCC 方案基础上增加了子群隐私增强保护特性,由引理 1 可得,新增加的签名所基于的协议是一个零知识证明协议,在随机预言机模型下签名中并不会泄露信息,因此扩展后的 BCC 方案即方案Ⅰ仍然满足不可伪造性、匿名性与不可关联性.

3.2 方案Ⅱ

主要思想:该方案基于 CL 累加器[10]. 当有成员加入子群时,子群管理员累加其加入标记 e_i,成员签名时需要提供 e_i 在累加值中的证据 u_i,撤消成员时,子群管理员从累加值中删除对应的 e_i.

子群管理员的初始化过程:

(1)子群管理员随机选择 l_p 比特的素数 p', q',使得 $p = 2p' + 1, q = 2q' + 1$ 为素数,令 $n = pq$, n 的比特位数为 l_n;

(2)子群管理员选择 u, g, h 是群 $QR(n)$的生成元;

(3)子群管理员维护累加值 u,一个子群成员列表 E_{add}和一个子群撤销成员列表 E_{del},列表初始为空.

注册阶段(DAA-Register) 可信计算平台发送通过 DAA-Join 过程得到的成员证书中的 e_i 给子群管理员,子群管理员对可信计算平台的进行认证,确认该 e_i 是由符合条件的可信计算平台产生的. 在通信过程中,假定通信信道是安全的,文献[2]的附录部分给出了如何在可信计算平台与子群管理员之间建立这种安全信道. 某个成员加入时子群管理员执行如下的操作:

(1)更新累加值 $u = f(u, e_i) = u^{e_i}$,并且计算成员证据 u_i,使得 $u = u_i^{e_i}$,将加入标记 e_i 存入 E_{add};

(2)发送 u_i 给可信计算平台,u_i 为 e_i 在累加值 u 中的证据.

签名过程(DAA-Sign) 该签名过程是对 BCC 方案的 DAA-Sign 进行了扩展,分为两个步骤,第一步是进行 BCC 方案的 DAA-Sign 操作,具体的签名可以参考文献[2],得到签名 σ_1;之后进行第二阶段的证明,得到签名 σ_2 的具体步骤如下:

(1)随机选择 $w_1, w_2, w_3 \in_R \{0,1\}^{2^{l_p}}$,计算承诺值 $T_1 = g^{e_i}h^{w_1}, T_2 = u_i h^{w_2}, T_3 = g^{w_2}h^{w_3}$;

(2)计算知识签名:$\text{SPK}\{e_i, w_1, w_2, w_3: T_1 = g^{e_i}h^{w_1} \wedge T_3 = g^{w_2}h^{w_3} \wedge u = T_2^{e_i}h^{-e_i w_2}\}(m)$,计算过程如下:

(a)计算辅助值 $\delta_1 = e_i w_2, \delta_2 = e_i w_3$,选择

$$r_{e_i}, r_{w_1}, r_{w_2}, r_{w_3}, r_{\delta_1}, r_{\delta_2}$$

计算

$$R_1 = g^{r_{e_i}}h^{r_{w_1}}, R_2 = g^{r_{w_2}}h^{r_{w_3}}, R_3 = T_2^{r_{e_i}}h^{-r_{\delta_1}}, R_4 = T_3^{r_{e_i}}g^{-r_{\delta_1}}h^{-r_{\delta_2}}$$

(b)计算 $c = H(g \parallel h \parallel T_1 \parallel T_2 \parallel T_3 \parallel R_1 \parallel R_2 \parallel R_3 \parallel R_4 \parallel m)$;

(c)计算

$$s_{e_i} = r_{e_i} + ce_i, s_{w_1} = r_{w_1} + cw_1, s_{w_2} = r_{w_2} + cw_2,$$
$$s_{w_3} = r_{w_3} + cw_3, s_{\delta_1} = r_{\delta_1} + c\delta_1, s_{\delta_2} = r_{\delta_2} + c\delta_2$$

(3)得到的签名 $\sigma_2 = (c, T_1, T_2, T_3, s_{e_i}, s_{w_1}, s_{w_2}, s_{w_3}, s_{\delta_1}, s_{\delta_2})$;

(4)最后得到签名 $\sigma = (\sigma_1, \sigma_2)$.

验证阶段(DAA-Verify) 首先利用过程 BCC 方案的 DAA-Verify 过程验证 σ_1 的合法性,σ_2 的验证过程如下:

计算

$$R_1' = g^{s_{e_i}}h^{s_{w_1}}T_1^{-c}, R_2' = g^{s_{w_2}}h^{s_{w_3}}T_3^{-c}, R_3' = T_2^{s_{e_i}}h^{-s_{\delta_1}}u^{-c}, R_4' = T_3^{s_{e_i}}g^{-s_{\delta_1}}h^{-s_{\delta_2}} \quad (6)$$

验证 $c \stackrel{?}{=} H(g \parallel h \parallel T_1 \parallel T_2 \parallel T_3 \parallel R_1' \parallel R_2' \parallel R_3' \parallel R_4' \parallel m)$

成员更新(DAA-Update)

(1)增加新成员 e_i 后子群中的成员更新证据 $u_i =$

$u_i^{e_i}$,子群管理员更新累加值 $u = u^{e_i} \bmod n$, $E_{\text{add}} = E_{\text{add}} \cup \{e_i\}$;

(2)撤销一个成员时(成员标识为 $\tilde{e}$),根据扩展欧几里德算法,计算 a, b 使得 $ae_i + b\tilde{e} = 1$,更新成员证据:$u_i = u_i^b u^a$,撤销一个成员后的累加值为:$u = u^{\tilde{e}^{-1} \bmod (p-1)(q-1)} \bmod n$, $E_{\text{add}} = E_{\text{add}} - \{\tilde{e}\}$.

安全性分析

引理 2　在强 RSA 假设下,令 n 是 RSA 模数,给定 $u, g \in QR(n)$,并且 g 是群 $QR(n)$ 的生成元,存在 $x, y \in Z_n$, $g^x \equiv u^y (\bmod n)$,那么 $y \mid x$.

证明　令 $GCD(x, y) = r$,那么根据欧拉定理,存在 α, β,使得 $\alpha x + \beta y = r$,那么 $g = g^{(\alpha x + \beta y)/r} = (u^{\alpha y} g^{\beta y})^{1/r} = (u^{\alpha} g^{\beta})^{y/r}$,如果 $y > r$,那么根据该式,就可以求出 g 的 y/r 次方跟,这与强 RSA 假设矛盾,又因为 $GCD(x, y) = r$,所以 $y = r$, $y \mid x$.

引理 3　在强 RSA 假设下,方案Ⅱ中的签名所基于的交互式协议是诚实验证者关于知识 e_i, u_i 的统计零知识证明.

证明　协议的完备性和零知识性容易证明,下面证明其合理性,也就是要给出一个关于所证明知识 e_i, u_i 的提取器(Knowledge Extractor).在交互式协议中,知识提取器回应两个不同的挑战值,得到两组可接受的值 $(T_1, T_2, T_3, c, s_{e_i}, s_{w_1}, s_{w_2}, s_{w_3}, s_{\delta_1}, s_{\delta_2})$ 和 $(T_1, T_2, T_3, \tilde{c}, \tilde{s}_{e_i}, \tilde{s}_{w_1}, \tilde{s}_{w_2}, \tilde{s}_{w_3}, \tilde{s}_{\delta_1}, \tilde{s}_{\delta_2})$,假设

$$\Delta c = \tilde{c} - c, \Delta e_i = \tilde{s}_{e_i} - s_{e_i}, \Delta w_1 = \tilde{s}_{w_1} - s_{w_1}, \Delta w_2 = \tilde{s}_{w_2} - s_{w_2}, \Delta w_3 = \tilde{s}_{w_3} - s_{w_3}, \Delta \delta_1 = \tilde{s}_{\delta_1} - s_{\delta_1}, \Delta \delta_2 = \tilde{s}_{\delta_2} - s_{\delta_2}$$

由式(6)可得

$$R_1' = g^{s_{e_i}} h^{s_{w_1}} T_1^{-c} = g^{\tilde{s}_{e_i}} h^{\tilde{s}_{w_1}} T_1^{-\tilde{c}}, \quad (7)$$

$$R_2' = g^{s_{w_2}} h^{s_{w_3}} T_3^{-c} = g^{\tilde{s}_{w_2}} h^{\tilde{s}_{w_3}} T_3^{-\tilde{c}}$$

$$R_3' = T_2^{s_{e_i}} h^{-s_{\delta_1}} u^{-c} = T_2^{\tilde{s}_{e_i}} h^{-\tilde{s}_{\delta_1}} u^{-\tilde{c}}, \quad (8)$$

$$R_4' = T_3^{s_{e_i}} g^{-s_{\delta_1}} h^{-s_{\delta_2}} = T_3^{\tilde{s}_{e_i}} g^{-\tilde{s}_{\delta_1}} h^{-\tilde{s}_{\delta_2}}$$

由式(7)、(8)可得 $T_1^{\Delta c} = g^{\Delta e_i} h^{\Delta w_1}$, $T_3^{\Delta c} = g^{\Delta w_2} h^{\Delta w_3}$, $T_2^{\Delta e_i} = h^{\Delta_{\delta_1}} u^{\Delta c}$, $T_3^{\Delta e_i} = g^{\Delta \delta_1} h^{\Delta \delta_2}$,

由引理 2 可得:$\Delta c \mid \Delta e_i, \Delta c \mid \Delta w_1$,因此 $e_i = \dfrac{\Delta e_i}{\Delta c}$;

由于 $T_3^{\Delta c} = g^{\Delta w_2} h^{\Delta w_3}$ 和 $T_3^{\Delta e_i} = g^{\Delta \delta_1} h^{\Delta \delta_2}$,得到 $g^{\Delta c \Delta \delta_1} h^{\Delta c \Delta \delta_2} = g^{\Delta e_i \Delta w_2} h^{\Delta e_i \Delta w_3}$, $\Delta \delta_1 = \dfrac{\Delta e_i \Delta w_2}{\Delta c}$;

$u = T_2^{\Delta e_i / \Delta c} / h^{\Delta \delta_1 / \Delta c}$, $u = u_i^{e_i}$,将 $\Delta \delta_1 = \dfrac{\Delta e_i \Delta w_2}{\Delta c}$ 代入,得到 $u_i = \dfrac{T_2}{h^{\frac{\Delta w_2}{\Delta c}}}$;

得到知识 $(e_i, u_i) = (\dfrac{\Delta e_i}{\Delta c}, \dfrac{T_2}{h^{\frac{\Delta w_2}{\Delta c}}})$;

定理 3　在 $\langle \gamma \rangle$ 群的 DDH 假设和强 RSA 假设下,方案 *II* 实现了一个安全的直接匿名证明系统.

证明　根据定理 1 可得,BCC 方案安全地实现了一个直接匿名证明系统,也即满足不可伪造性、匿名性与不可关联性,而方案Ⅱ是在 BCC 方案基础上增加了子群隐私增强保护特性,由引理 3 可得,新增加的签名所基于的协议是一个零知识证明协议,在随机预言机模型下签名中并不会泄露信息,因此扩展后的 BCC 方案即方案Ⅱ仍然满足不可伪造性、匿名性与不可关联性.

3.3　方案比较Ⅰ和Ⅱ

从实现上来看,两种方案都是 BCC 方案的一种扩展,并且都能在 TPM v1.2 的基础上实现.本节将比较方案Ⅰ和Ⅱ的不同.

本文所提出的两个方案都增加了 BCC 方案的灵活性.由于在计算过程中 TPM 的计算量是一个非常重要的性能指标,因此我们将比较在签名和注册过程中 TPM 的计算量.主要的计算参数为:$l_n = 2048$, $l_n = 368$, $l_n = 104$

表 1　方案Ⅰ和方案Ⅱ的性能比较

	签名操作/TPM 计算量	验证操作	注册操作/TPM 计算量	签名长度(字节)
方案Ⅰ	$(6t-1)$E + $(2t-1)$M/$2t$E + 2M	$8t$E + $4t$M	1E + 1M/1E + 1M	$4896t - 1632$
方案Ⅱ	14E + 14M/0E + 0M	12E + 8M	0	10926

方案Ⅰ随着子群成员数的增加签名和验证的效率都会降低.而方案Ⅱ的签名长度以及签名效率不会因为子群成员数的增加而增加.签名和验证算法中的主要运算为模幂、模乘,分别用 E,M 表示,本文主要从签名和验证,注册操作方面比较这两个方案(见表 1),表中 t 表示子群成员的个数.方案Ⅰ中签名算法和验证算法的计算量与成员个数线性相关,特别是在较大群体中,随着 t 的增大,签名算法和验证算法的效率将会明显降低.方案Ⅱ验证算法的计算量为常量,在较大群体中效率高于方案Ⅰ.方案Ⅰ中签名长度、签名和验证算法的计算量和成员个数线性相关,在 t 不是很大的情况下较为实用,方案Ⅱ解决了方案Ⅰ的不足,签名长度、签名和验证算法的计算量均独立于子群成员个数.最后,方案Ⅰ的一个额外的特性是不仅能证明可信计算平台属于某个特定群体同时还能证明不属于某个群体,而方案Ⅱ做不到这一点;方案Ⅰ中的操作需要 TPM 的参与,因此其安全性根植于 TPM,而方案Ⅱ中的操作不需要 TPM 的参与,如果攻击方攻破主机,攻击方就可以提取 e_i, u_i,安全性相对较低.

4　结论

本文针对 Brickell 等人提出的直接匿名证明方案的

“验证者相关的完全或无”匿名性机制的缺陷,提出了子群隐私增强保护的直接匿名证明方案,并且给出了两种具体的实现方式.两种实现方式各有不同,在性能和效率上存在着差别,可以适用于不同的应用场景,对提出的方案进行了安全性的分析,分析表明增加的特性并不会影响原始 BCC 方案的安全性.

参考文献

[1] ISO/IEC 11889 Parts 1 – 4. The Trusted Computing Group Trusted Platform Module Specification Version 1.2[S].

[2] E Brickell, J Camenisch, L Chen. Direct anonymous attestation [A]. Vijay Atluri. ACM Conference on Computer and Communications Security 2004[C]. NewYork: ACM PRESS, 2004. 132 – 145.

[3] He Ge, Stephen R Tate. A direct anonymous attestation scheme for embedded devices[A]. Andrew C Yao. Public Key Cryptography 2007[C]. Berlin, Heidelberg: Springer-Verlag, 2007. 16 – 30.

[4] Ernie Brickell, Jiangtao Li. Enhanced privacy ID: A direct anonymous attestation scheme with enhanced revocation capabilities[A]. Vijay Atluri. the 6th Workshop on Privacy in the Electronic Society (WPES)[C]. New York, USA: ACM, 2007. 52 – 57.

[5] Jan Camenisch. Better privacy for trusted computing platforms [A]. Refik Molva. ESORICS 2004[C]. Berlin, Heidelberg: Springer-Verlag, 2004. 73 – 88.

[6] Jan Camenisch. Protecting (anonymous) credentials with the trusted computing group′s TPM V1.2[A]. Simone Fischer-Hübner. SEC 2006[C]. Berlin, Heidelberg: Springer-Verlag, 2006. 135 – 147.

[7] Camenisch J, Stadler M. Efficient group signature schemes for large groups [A]. Burton S Kaliski Jr. CRYPTO’97[C]. Berlin, Heidelberg: Springer-Verlag, 1997. 410 – 424.

[8] A Fiat, A Shamir. How to prove yourself: Practical solutions to identification and signature problems[A]. Andrew M. Odlyzko, CRYPTO ’86[C]. Berlin, Heidelberg: Springer-Verlag, 1986. 186 – 194.

[9] J Camenisch, A Lysyanskaya. A signature scheme with efficient protocols[A]. Stelvio Cimato. SCN 2002[C]. Berlin, Heidelberg: Springer-Verlag, 2003. 268 – 289.

[10] Jan Camenisch, Anna Lysyanskaya. Dynamic accumulators and application to efficient revocation of anonymous credentials[A]. Rebecca Wright. CRYPTO 2002[C]. Berlin, Heidelberg: Springer-Verlag, 2002. 61 – 76.

作者简介

陈小峰 男,1980 年出生于浙江金华,博士,中国科学院软件所,主要研究领域为网络安全,可信计算.

E-mail: loiscxf@hotmail.com

冯登国 男,1965 年出生于陕西,博士,中国科学院软件所,研究员,信息安全国家重点实验室主任,主要研究领域为网络安全.