无可信中心的新型门限部分盲签名方案

农 强[1],郝艳华[1],吴顺祥[2]
NONG Qiang[1],HAO Yan-hua[1],WU Shun-xiang[2]

1.漳州师范学院 计算机科学与工程系,福建 漳州 363000
2.厦门大学 自动化系,福建 厦门 361005
1.Dept. of Computer Science and Engineering,Zhangzhou Normal University,Zhangzhou,Fujian 363000,China
2.Dept. of Automation,Xiamen University,Xiamen,Fujian 361005,China
E-mail:nong_qiang@163.com

NONG Qiang,HAO Yan-hua,WU Shun-xiang.New threshold partially blind signature scheme without trusted center. Computer Engineering and Applications,2009,45(6):105-108.

Abstract: An efficient ID-based partially blind signature scheme is proposed based on gap diffie-hellman group.In this scheme, the dishonest Private Key Generator (PKG) can not impersonate any user at any time.Then a new ID-based threshold partially blind signature scheme is proposed based on the ID-based partially blind signature scheme.The main idea of the scheme is based on Feldman's verifiable secret sharing scheme which is simple to implement with high secure character.Up to now,it is the first pairing-based cryptography on ID-based threshold partially blind signature.Analysis shows that the proposed scheme is secure and effective.It has provable security properties of blindness,unforgeability and robustness.
Key words: ID-based;Private Key Generator (PKG);partially blind signature;threshold signature

摘 要:基于间隙 Diffie-Hellman (GDH) 群的特点,首先提出了一个有效的基于身份的部分盲签名方案,能够防止私钥产生中心(PKG)伪造签名。而后用所提的部分盲签名方案构造了基于身份的新型门限部分盲签名方案。文中的构造思想主要基于 Feldman 的可证实秘密共享方案,具有实现简单但安全性高的特点。到目前为止,该方案是第一类用双线性对来构造的基于身份的门限部分盲签名方案。分析表明,所提方案具有部分盲性、不可伪造性和强壮性等特性,是安全、有效的。
关键词:基于身份;私钥产生中心;部分盲签名;门限签名
DOI:10.3778/j.issn.1002-8331.2009.06.030 **文章编号**:1002-8331(2009)06-0105-04 **文献标识码**:A **中图分类号**:TP309

1 引言

盲签名[1]是由电子支付匿名性的要求而提出的,它与通常的数字签名不同之处在于,签名者并不知道他所签发文件的具体内容。正是这个特点,使得盲签名这种技术可广泛用于许多领域,类似的应用场合还有电子投票选举和网上招标、投标等。

一方面,电子支付的"隐私权"(或者说匿名性、不可追踪性)问题始终为人们所关注。如果某人进行每一笔电子交易的金额、时间、收款人等信息均为第三方所掌握,那么关于他的行踪、社交和生活方式等大量信息就泄露出来了。其次,为了确保电子支付的安全性和可控性,例如支付证明、偷税漏税、黑市交易洗钱等问题的出现,使得政府部门和税务部门要求电子支付是可审核的,这与前述匿名性是相互矛盾的。因此,有必要求助于一种特殊的措施,而这种特殊的措施即为部分盲签名。1996年,Abe 等[2]首次提出了部分盲签名的概念和实现方案。部分盲签名最突出的一点在于允许签名人在签名中嵌入一个和用户一起协商的公共信息,而这个公共信息不可以被移除或者修改。正是由于这种特性,部分盲签名技术能确保被签消息对签名者的隐秘性,又能阻止消息提供者提供非法消息而滥用签名。

另一方面,在基于盲签名方案的选举系统或者电子支付系统中,通常设置单个管理者进行管理,而这个管理者总是被赋予了选举或者消息签名的权利。这样,如果这个管理者不诚实,那么它可以滥用权力,为了自身的利益进行欺骗性行为。为了防止这种单个管理者的权力滥用,需要使用门限方案让多个管理者一起进行消息签名。

在 Juang 等[3]最初提出 (t,n) 门限盲签名方案之后,Kim 等[4]也提出了一个有效的可证安全的门限盲签名方案,并且声称所提的方案与先前的文献[3]方案相比更为安全有效。然而,在这些已有的门限盲签名方案里,它们大多基于离散对数问题。曹

基金项目:国家自然科学基金(the National Natural Science Foundation of China under Grant No.60704042);国家"十一五"科技支撑计划项目资助(the National Project of Scientific and Technical Supporting Programs Funded by Ministry of Science & Technology of China During the 11th Five-year Plan.No.2007BAK34B04);福建省青年科技人才创新项目(No.2008F3110);福建省教育厅科技项目(No.JA08156)。
作者简介:农强(1978-),男,讲师,主要研究方向为密码学与网络安全;郝艳华(1976-),女,讲师,博士,主要研究方向为椭圆曲线密码体制与电子商务安全;吴顺祥,男,教授,博士,主要研究方向为信息安全、人工智能与机器学习。
收稿日期:2008-01-14 修回日期:2008-04-14

珍富等[5]基于改进的 RSA 密码系统提出了一个可证安全的强壮门限部分盲签名方案,其安全性基于分解问题。自 MOV 和 Frey-Ruch 将双线性对引入数字签名后,人们发现利用双线性映射可以高效实现密码学上的加密、签名等应用。2003 年,Vo 等[6]基于双线性对提出了一个新的门限盲签名方案,并给出了安全性证明。随后,更多的基于双线性对的门限盲签名方案被提出,然而,它们主要基于传统的 PKI 架构,具有由 CA 颁发公钥证书所带来的维护成本高、证书链处理过于繁琐等弊端。

考虑在基于身份的公钥密码系统中,用户的公钥可以由其身份标识计算得到,而身份标识可以是姓名、e-mail 地址等公开信息,因而使用方便。所以,基于身份的公钥密码体制成为近年来的研究热点。但目前的许多基于身份的公钥系统都涉及到的密钥托管问题,系统中需要公共可信的私钥产生中心(Private Key Generator,PKG)生成用户的私钥。由于 PKG 掌握各用户的私钥,不诚实的 PKG 可以任意伪造签名,这个问题成为基于身份的公钥密码系统在实际中广泛应用的极大障碍。

基于对以上问题的研究,提出了一个基于身份的新型门限部分盲签名方案,采用系统主密钥和用户提供的随机数共同作用产生用户私钥,消除了 PKG 可以随意伪造用户签名的安全隐患,并满足门限部分盲签名所需的各种性质,是首次将双线性对引入到基于身份的门限部分盲签名方案中。

2 预备知识

2.1 双线性映射

设 G_1 为循环加法群,G_2 为循环乘法群,G_1,G_2 的阶均为素数 q。假定在 G_1,G_2 中计算离散对数问题是困难的。设 $e:G_1\times G_1\to G_2$ 为一个双线性映射,它满足以下 3 个性质:

(1) 双线性。$e(aP,bQ)=e(P,Q)^{ab}$,对 $P,Q\in G_1$ 和 $\forall a,b\in Z_q$ 成立。

(2) 非退化性。$\exists P,Q\in G_1$,使 $e(P,Q)\neq 1$。

(3) 可计算性。如果 $P,Q\in G_1$,则 $e(P,Q)$ 可以在多项式时间内有效计算出来。

定义 1 计算离散对数问题 CDHP(Computational Diffie-Hellman Problem):对于 $a,b\in_R Z_q^*$,P 是 G_1 的生成元,给定 G_1 中的元素 P,aP,bP,计算 abP。

定义 2 计算离散对数假设(Computational Diffie-Hellman(CDH) Assumption):设令 IG 是一个 CDH 参数生成器,输入安全参数 1^k,说 IG 满足 CDH 假设,如果对于充分大的 k,算法 A 解决关于 G_1 的 CDH 问题具有的优势 $Adv_{IG,A}(k)$ 定义为:

$$Adv_{IG,A}(k)=\Pr\left(\begin{array}{l}A(q,G_1,aP,bP)=abP,\\ |(q,G)\leftarrow G(1^k),P\leftarrow G_1,a,b\leftarrow Z_q^*\end{array}\right)\geqslant\varepsilon(k)$$

参数生成器 IG 满足 CDH 假设,如果对任何 k 的概率多项式时间算法 A,优势 $Adv_{IG,A}(k)$ 是可忽略量。在素数阶循环群 G 上,DDHP 在多项式时间内能被解决,但没有任何可能的算法可以解决 CDHP,称 G 为 GDH(Gap Diffie-Hellman)群。GDH 群能在有限域上的超奇异椭圆曲线或超椭圆曲线上找到,双线性映射能通过 Weil 对或 Tate 对构造,本方案基于 GDH 群。

2.2 门限体制

Shamir 首先提出了门限方案[7]。在 (t,n) 门限方案中,秘密 D 被分为 n 份子秘密 $D_1,D_2,\cdots,D_n$,分配给 n 个人,该方案满足下列条件:

(1) 知道任意 t 个或者更多子秘密 D_i,则容易计算出秘密 D;

(2) 只知道 $t-1$ 个或者更少子秘密 D_i,则无法计算出秘密 D。

在 Shamir 提出第一个门限方案之后,更多的门限签名方案及其改进方案被陆续提出。Feldman 提出了的一个可证实秘密共享方案[8]。在该方案中,任何一方都可以选择一个密钥,并能安全地被分发和验证,由此形成了一个可信任的团体,他们能够证实被分享的秘密。下面将使用这一技术。

3 所提的部分盲签名方案

3.1 系统初始化

输入安全参数 1^k,输出两个阶为 q 的循环群 $(G_1,+)$ 和 $(G_2,\times)$,q 为大素数,P 为 G_1 的生成元。定义 G_1 上的一个双线性映射 $e:G_1\times G_1\to G_2$,同时定义 3 个强无碰撞安全单向 Hash 函数 $H_1:\{0,1\}^*\times G_1\to G_1,H_2:\{0,1\}^*\times G_1\to Z_q^*,H_3:\{0,1\}^*\to Z_q^*$。最后 PKG 选择 $s\in_R Z_q^*$,计算 $P_{pub}=sP$,将 s 秘密保存,公开其系统参数:$Params=\{G_1,G_2,e,q,P,P_{pub},H_1,H_2,H_3\}$。

3.2 密钥提取

签名人选取 $r_A\in_R Z_q^*$,计算 r_AP 并把 r_AP 和 r_A 的使用期限 T_A 以及他的身份信息 ID_A 提交给 PKG。PKG 计算 $Q_A=H_1(ID_A\|T_A,r_AP)$,把 Q_A 作为签名人的公钥。最后 PKG 把 $S_A=sQA$ 作为签名人的部分私钥,通过一个安全信道送给签名人,签名人的私钥为 (r_A,S_A)。

3.3 部分盲签名

假设用户想要得到公钥为 Q_A 的签名人对消息 M 的部分盲签名,且双方已经事先商定 c 作为消息 M 的附加信息。签名过程如下:

(1) 签名人选择 $k\in_R Z_q^*$,计算 $U=kH_3(c)Q_A$,然后将 U 发送给用户;

(2) 用户选择 $t_1,t_2\in_R Z_q^*$,计算 $U'=t_1U+t_1t_2Q_A$,$h=t_1^{-1}H_2(M\|c,U')+t_2$,然后将 h 发送给签名人;

(3) 签名人收到 h 后,计算 $V=(kH_3(c)+h)(r_AQ_A+S_A)$,然后将 V 发送给用户;

(4) 用户收到 V 后,计算 $V'=t_1V$。

(V',U',r_AP,T_A,M,c) 为签名人对消息 M 的部分盲签名,其中 c 为非盲的公共信息。

3.4 验证

验证者首先计算 $Q_A=H_1(ID_A\|T_A,r_AP)$ 和 $h'=H_2(M\|c,U')$,再看等式 $e(V',P)=e(U'+h'Q_A,r_AP+P_{pub})$ 是否成立。如果成立则接受签名,否则认为该签名无效。

4 所提的门限部分盲签名方案

这里的系统参数以及对应于身份 ID 的密钥产生如上,签名人的私钥为 (r_A,S_A),公钥为 Q_A,密钥分发采用了文献[8]的可证实秘密共享方案(Feldman-VSS)。

4.1 密钥分发

(1) 任意选取 $b_l\in Z_q$ 和 $R_l\in G_1$,其中 $1\leqslant l\leqslant t-1$,$b_{t-1}\neq 0$,$R_{t-1}$ 不为 G_1 中的零元;

(2) 令 $g(x)=r_A+b_1x+b_2x^2+\cdots+b_{t-1}x^{t-1}$,$S(x)=S_A+xR_1+x^2R_2+\cdots+x^{t-1}R_{t-1}$,计算部分私钥 $g(i)=r_i$,$S(i)=S_i$ 以及公开信息 $L_i=r_iP$ 和 $Y_i=e(P,S_i)$,并全部发送给成员 Γ_i,$1\leqslant i\leqslant n$。这里 $r_A=g(0)=\sum_{j\in\Phi}\eta_j^{\Phi}r_j$,

$S_A=S(0)=\sum_{j\in\Phi}\eta_j^{\Phi}S_j$,其中 $\eta_j^{\Phi}=\prod_{l\in\Phi,l\neq j}\frac{l}{l-j}$,集合 $\Phi\subset\{1,2,\cdots,n\}$且$|\Phi|\geqslant t$,$\Phi$ 为参加签名的成员集合;

(3) 成员 Γ_i 通过公开信息 $L_i=r_iP$ 和 $Y_i=e(P,S)$ 验证 r_i 和 S_i 的有效性,若通过验证则将 (r_i,S) 作为私钥,并广播 L_i 和 Y_i。

4.2　签名

假设用户想要获得签名群体对消息 M 的部分盲签名,且已经与其中至少 t 个成员事先商定 c 作为消息 M 的附加信息,则签名过程如下:

(1) $\Gamma_i,i\in\Phi$ 任意生成一个 $t-1$ 次多项式 $f_i(x)=a_{i0}+a_{i1}x+a_{i2}x^2+\cdots+a_{it-1}x^{t-1}$,并广播 $A_{il}=a_{il}Q_A,0\leqslant l\leqslant t-1$。$\Gamma_i$ 发送 $f_i(j)$ 给 Γ_j,Γ_j 通过验证 $f_i(j)Q_A=\sum_{l=0}^{t-1}j^lA_{il}$ 是否成立来判断 $f_i(j)$ 是否有效。若 Φ 中所有成员都通过验证,最后每个成员 Γ_i 计算得到他拥有的部分随机数 $k_i=\sum_{j\in\Phi}f_i(j)$ 并计算 $U_i=k_iH_3(c)Q_A$,将 U_i 发送给用户;

(2) 用户计算 $U=\sum_{i\in\Phi}\eta_i^{\Phi}U_i$,$r_AP=\sum_{i\in\Phi}\eta_i^{\Phi}L_i$,并选取 $t_1,t_2\in_R Z_q^*$,计算 $U'=t_1U+t_1t_2Q_A$,$h=t_1^{-1}H_2(M\|c,U')+t_2$,然后将 h 发送给成员 Γ_i;

(3) Φ 中的每个成员 Γ_i 计算 $V_i=(k_iH_3(c)+h)(r_iQ_A+S)$,并将 V_i 发送给用户;

(4) 用户通过验证 $(e(L_i,Q_A)\cdot Y)^{(k_iH_3(c)+h)}=e(P,V_i)$ 是否成立,来验证 Φ 中的每个成员 Γ_i 的部分签名是否有效。若 Φ 中的每个成员 Γ_i 的部分签名都是有效的,则计算 $V=\sum_{i\in\Phi}\eta_i^{\Phi}V_i$,并进行脱盲变换 $V'=t_1V$,最后得到消息 M 的签名为 (V',U',r_AP,T_A,M,c)。

4.3　验证

验证者首先计算 $Q_A=H_1(ID_A\|T_A,r_AP)$ 和 $h'=H_2(M\|c,U')$,然后验证等式 $e(V',P)=e(U'+h'Q_A,r_AP+P_{pub})$ 是否成立,来验证签名的合法性:

$$\begin{aligned}e(V',P)&=e(t_1V,P)=e\Big(t_1\sum_{i\in\Phi}\eta_i^{\Phi}V_i,P\Big)=\\&e\Big(t_1\sum_{i\in\Phi}\eta_i^{\Phi}((k_iH_3(c)+h)(r_iQ_A+S_i)),P\Big)=\\&e\Big(t_1\sum_{i\in\Phi}\eta_i^{\Phi}(k_iH_3(c)+h)\sum_{i\in\Phi}\eta_i^{\Phi}(r_iQ_A+S_i),P\Big)=\\&e(t_1(kH_3(c)+h)(r_AQ_A+S_A),P)=\\&e((t_1kH_3(c)+H_2(M\|c,U')+t_1t_2)(r_A+s)Q_A,P)=\\&e(t_1U+t_1t_2Q_A+H_2(M\|c,U')Q_A,r_AP+P_{pub})=\\&e(U'+h'Q_A,r_AP+P_{pub})\end{aligned}$$

5　安全性分析

这一章主要对门限部分盲签名方案进行一些安全性讨论,确切的说,主要关注方案的部分盲性、不可伪造性和强壮性等属性。

定理 1　文中所提的门限部分盲签名方案具有部分盲性。

证明　关于部分盲性的定义可参考文献[9]。由签名算法,如果给定一个有效的部分盲签名 (V',U',r_AP,T_A,M,c) 以及在签名发行过程中交换的数据 (U,h,V),下列等式成立:

$$V'=t_1V \tag{1}$$

$$h=t_1^{-1}H_2(M\|c,U')+t_2 \tag{2}$$

$$U'=t_1U+t_1t_2Q_A \tag{3}$$

显然,必存在一个唯一的盲因子 $t'_1\in Z_q^*$ 满足等式(1);同理,也必存在另一个唯一的盲因子 $t'_2\in Z_q^*$ 满足等式(2),其中 $t'_2=h-t_1^{-1}H_2(M\|c,U')$。对于等式(3),根据双线性映射的非退化性,有:

$$e(U',r_AP+P_{pub})=e(t_1U+t_1t_2Q_A,r_AP+P_{pub})\Leftrightarrow U'=t_1U+t_1t_2Q_A \tag{4}$$

因为 (V',U',r_AP,T_A,M,c) 是有效的部分盲签名,因此 $e(V',P)=e(U'+H_2(M\|c,U')Q_A,r_AP+P_{pub})$ 成立。以下考虑两个盲因子 (t'_1,t'_2) 满足等式(4),证明如下:

$$\begin{aligned}&e(t'_1U+t'_1t'_2Q_A,r_AP+P_{pub})=\\&e(t'_1U+t'_1(h-t_1^{-1}H_2(M\|c,U'))Q_A,r_AP+P_{pub})=\\&e(t'_1U+t'_1hQ_A,r_AP+P_{pub})e(H_2(M\|c,U')Q_A,r_AP+P_{pub})^{-1}=\\&e(t'_1kH_3(c)Q_A+t'_1hQ_A,r_AP+P_{pub})e(V',P)^{-1}e(U',r_AP+P_{pub})=\\&e(t'_1(kH_3(c)+h)(r_AQ_A+sQ_A),P)e(V',P)^{-1}e(U',r_AP+P_{pub})=\\&e(V',P)e(V',P)^{-1}e(U',r_AP+P_{pub})=e(U',r_AP+P_{pub})\end{aligned}$$

从以上的推导过程可知盲因子 (t'_1,t'_2) 总是存在且能满足等式(4)的定义,所以在任何视野中看到的部分盲签名的生成协议是无链接的,这一点与文献[9]所证明签名的部分盲性原理相同。

其次,本文的部分盲签名方案将公共信息 c 与签名人的私钥 (r_A+s) 绑定在一起,而除了签名者本人外,任何其他人都不知道私钥 (r_A+s),所以公共信息 c 在嵌入部分盲签名后,任何人想篡改公共信息 c 必须先解决 CDH 问题,这与 CDH 问题的困难性假设相矛盾,所以提出的方案防止了对公共信息 c 的篡改。

定理 2　在随机预言模型下,若文中提出的部分盲签名方案在适应性选择消息攻击以及身份攻击下是存在可伪造的,则 CDH 困难问题在 Gap Diffie-Hellman(GDH)群 G_1 中可解。

证明　假设 PKG 想伪造签名,由于 $V=(kH_3(c)+h)(r_AQ_A+S_A)$,其中 $S=(kH_3(c)+h)S_A$ 显然可以被 PKG 用其私钥 s 来产生,这样 PKG 就可以计算 $(kH_3(c)+h)r_AQ_A=V-S$,进而可以计算 $r_AQ_A=(kH_3(c)+h)^{-1}(V-S)$(求逆在 Z_q^* 进行)。这样 PKG 对于随机的 Q_A,r_AP 在不知道 r_A 的情况下可计算 r_AQ_A,这与 CDH 问题难解相矛盾。

假定存在一个攻击者 F(非 PKG)能产生一个有效的部分盲签名 (V',U',h',r_AP,T_A,M,c),那么根据神谕重放技术[10]和分叉引理[10],存在另一个有效的算法 Sim 能产生两个有效的部分盲签名 (V',U',h',r_AP,T_A,M,c) 和 $(V',U',h'_1,r_AP,T_A,M,c)$,其中 $h'\neq h'_1$。使用两个有效的部分盲签名,Sim 能以一个不可忽略的概率求得 CDH 问题的解,这与 CDH 问题的困难性假设相矛盾,从而证明本方案是不可伪造的。具体证明过程如下:

给定 CDH 问题的任意一个实例 (P,aP,bP),Sim 设置 $Q_A=aP$,$r_AP+P_{pub}=bP$。在 Sim 与 F 执行了多项式次部分盲签名发布

协议后,Sim 得到两个部分盲签名 (V',U',h',r_AP,T_A,M,c) 和 $(V',U',h'_1,r_AP,T_A,M,c)$,其中 $h'\neq h'_1$。因为这两个部分盲签名是有效的,所以得到

$$e(V',P)=e(U'+h'Q_A,r_AP+P_{pub}) \quad (5)$$

$$e(V'_1,P)=e(U'+h'_1Q_A,r_AP+P_{pub}) \quad (6)$$

从方程(5)和(6)能推导出 $V'-h'abP=V'_1-h'_1abP$,从而得到 $abP=\frac{V'-V'_1}{h-h'_1}$。即 Sim 解决了 CDH 问题,这与 CDH 问题的困难性假设相矛盾,所以本文提出的基于身份的部分盲签名方案是不可伪造的。

定理 3[11] 若基于身份的门限签名是可模拟的,且它所基于的基于身份的签名是不可伪造的,则该基于身份的门限签名也是不可伪造的。

以上已经证明了所提的基于身份的部分盲签名方案是不可伪造的,接下来主要证明所提的基于身份的门限部分盲签名是可模拟的。

定义 3[11] 基于身份的门限签名是可模拟的(simulatable),若其满足以下条件:

(1)密钥分发是可模拟的:存在模拟器(simulator)使得在已知 PKG 的公开参数以及用户的 ID 条件下能够模拟出在执行密钥分发协议时攻击者的观察(view);

(2)签名是可模拟的:存在模拟器,使得在已知基于身份的门限签名的公开参数、消息 m、和对应的签名,以及 $t-1$ 个部分密钥和对应的用于验证的公开信息时,可模拟出在签名执行时攻击者的观察。

引理 1 文中提出的门限部分盲签名方案是可模拟的。

证明 (1)假设攻击者贿赂了 Γ_i 用户,其中 $1\leqslant i\leqslant t-1$,攻击者知道这 $t-1$ 个人的部分私钥,验证部分私钥的公开信息 $Y_i=e(P,S)$,以及公开参数和 Q_A,攻击者计算 $Y_0=e(P_{pub},Q_A)$,通过拉格朗日内插法计算 $Y(x)=e(P,S(x))=e(P,\sum_{0\leqslant i\leqslant t-1}a_iS)=\prod_{i=0}^{t-1}Y_i^{a_i}$,其中 $a_i=\prod_{\substack{0\leqslant j\leqslant t-1\\ j\neq i}}\frac{x-j}{i-j}$,则攻击者可求出 $Y_t=Y(0)$,由上述过程知 Y_t 是正确的,且等同于真实密钥分发过程中用户 Γ_t 发布的公开信息。同理可模拟出 $L_i=r_iP$,因此密钥分发是可模拟的。

(2)攻击者对签名的模拟。攻击者根据 U 和 $U_i(1\leqslant i\leqslant t-1)$,利用拉格朗日内插法计算得到 $U_t=U(0)$,因 $U_t=k_tH_3(c)Q_A=\sum_{0\leqslant i\leqslant t}f_j(0)H_3(c)Q_A=\sum_{0\leqslant i\leqslant t-1}f_j(0)H_3(c)Q_A+f_t(0)H_3(c)Q_A$,攻击者可求出 $f_t(0)H_3(c)Q_A=U_t-\sum_{0\leqslant k\leqslant t-1}f_k(0)H_3(c)Q_A$,攻击者知道 $f_i(x)$ 和 k_1,将 1 代入 $f_i(x)$ 求得 $f_i(1)$,其中 $1\leqslant i\leqslant t-1$,又由 $k_1=\sum_{0\leqslant j\leqslant t}f_j(1)=\sum_{0\leqslant j\leqslant t-1}f_j(1)+f_t(1)$ 可计算出 $f_t(1)$,同理攻击者可算出 $f_t(2)$,…,$f_t(t-1)$,由上述结果所求得的 $f_t(1)Q_A,f_t(2)Q_A,\cdots,f_t(0)Q_A$,采用拉格朗日内插法可求得多项式 $f_t(x)Q_A=(a_{t0}Q_A)+(a_{t1}Q_A)x+(a_{t2}Q_A)x^2+\cdots+(a_{tt-1}Q_A)x^{t-1}$。则攻击者就模拟出了 $A_{tl}=a_{tl}Q_A,0\leqslant l\leqslant t-1$。攻击者根据签名 (V',U',r_AP,T_A,M,c),$t-1$ 个部分私钥 (r_i,S) 以及对应的公开信息 (L_i,Y),由 $V_i=(k_iH_3(c)+h)(r_iQ_A+S)$ 和 V 用拉格朗日内插法可构造出多项式 $V(x)$,满足 $V(0)=V,V(i)=V_i$,则攻击者将 t 带入可计算得到 $V_t=V(t)$,因此签名是可模拟的。

综上所述,由引理 1 和定理 2,得出此基于身份的门限部分盲签名方案是不可伪造的。

定理 4 文中所提的门限部分盲签名方案具有强壮性。

证明 强壮性是指即使恶意攻击者贿赂了某些成员(最多 $t-1$ 个)使其在签名协议中不按照规定执行,最后仍然可以计算出正确的签名。本方案在私钥分发和部分随机数产生的每一步中都有广播用来验证部分私钥以及部分随机数的公开信息,这保证了私钥分发和随机数产生具有强壮性;而签名中,通过验证 $(e(L_i,Q_A)\cdot Y)^{(k_iH_3(c)+h)}=e(P,V_i)$ 就能够确认成员 Γ_j 是否是诚实的。因此,此门限部分盲签名方案的强壮性得到保证。

6 结束语

由于基于身份的公钥密码系统避免了基于证书的公钥密码系统中繁琐的证书管理,因而在实际应用中更加方便快捷。然而因为其自身固有的密钥托管问题,使该类方案不可避免地存在着安全隐患。文中所提的基于身份的新型门限部分盲签名方案,消除了 PKG 可以随意伪造用户签名的安全隐患,并达到了预期的安全要求。在实际应用中,为阻止权力滥用,所提方案将特别适用于基于盲签名的多管理者选举系统和安全电子现金系统。

参考文献:

[1] Chaum D.Blind signature for untraceable payments[C]//Crypto'82. New York:Prenum Publishing Corporation,1982:199-204.

[2] Abe M,Fujisaki E.How to date blind signatures[C]//Asiacrypt96. Berlin:Springer-Verlag,1996:244-251.

[3] Juang W S,Lei C L.Blind threshold signatures based on discrete logarithm[C]//Proceedings of the 2nd Asian Computing Science Conference.[S.l.]:Springer-Verlag,1996,1179:172-181.

[4] Kim J,Kim K,Lee C.An efficient and provably secure threshold blind signature[C]//International Conference on Information Security and Cryptology-ICISC'01,2002,2288:318-327.

[5] 曹珍富,朱浩瑾,陆荣幸.可证安全的强壮门限部分盲签名[J].中国科学 E 辑:信息科学,2005,35(12):1254-1265.

[6] Vo D L,Zhang F,Kim K.A new threshold blind signature scheme from pairings[C]//SCIS2003,Itaya,Japan,2003,1(2):233-238.

[7] Shamir A.How to share a secret[J].Communications of the ACM,1979,22(11):612-613.

[8] Feldman P.A practical scheme for non-interactive verifiable secret sharing[C]//Proc of the 28th IEEE Sympt on the Foundations of Computer Science.Los Angeles:IEEE,1987:427-437.

[9] Chow S S M,Hui L C K,Yiu H S M,et al.Two improved partially blind signature schemes from bilinear pairings[EB/OL]. http://eprint.iacr.org/2004/108.pdf.

[10] Pointcheval D,Stern J.Security arguments for digital signatures and blind signatures[J].Journal of Cryptology,2000,13(3):316-396.

[11] Baek J,Zheng Yu-liang.ID-based threshold signature scheme from the bilinear pairings[C]//IAS'04 Track of ITCC'04.LasVegas:IEEE Computer Society,2004:124-128.