

文章编号:1001-9081(2010)02-0513-04

无证书门限多代理多签名方案

杨长海

(南昌陆军学院 科文教研室,南昌 330103)

(yangchanghai@tom.com)

摘要:结合无证书公钥密码体制、多重代理多重签名和秘密共享技术,首次提出了无证书门限多代理多签名方案。在该方案中,只有达到门限值数量的原始签名者合作才能完成代理授权过程,同时只有达到门限值数量的代理签名者合作才能产生门限多代理多签名。经分析得知,方案同时具有多重代理多重签名和门限签名所需的安全性,如能抵抗伪造攻击和内部成员实施的合谋攻击。

关键词:数字签名;无证书;代理签名;门限多代理多签名

中图分类号: TP309 **文献标志码:** A

Certificateless threshold multi-proxy multi-signature scheme

YANG Chang-hai

(Department of Science and Arts, Nanchang Military Academy, Nanchang Jiangxi 330103, China)

Abstract: This paper proposed a certificateless threshold multi-proxy multi-signature scheme by adopting certificateless cryptography, multi-proxy multi-signature and secret sharing scheme. In this scheme, original signers could cooperatively finish proxy-delegation process only when the number of original signers went up to threshold value, and proxy signers could cooperatively generate threshold multi-proxy multi-signature only when the number of proxy signers went up to threshold value. By analyzing the scheme, it is concluded that the scheme has the security properties which multi-proxy multi-signature and threshold signature need, such as resisting frame attack and conspiracy attack which is caused by inside members.

Key words: digital signature; certificateless; proxy signature; threshold multi-proxy multi-signature

0 引言

自1996年 Mambo 等人^[1]提出代理签名概念以来,代理签名凭借其强大的实用性而得到迅速发展。发展的方向主要体现在两个方面:一方面是将代理签名概念进行延伸提出满足实际需要的数字签名,如多重代理签名^[2]、代理多重签名^[3]、多重代理多重签名^[4]等;另一方面是将代理签名与其他签名体制相结合提出具有多种特殊功能的数字签名,如代理盲签名^[5]、门限代理签名^[6]等。门限代理签名是 Zhang 等人提出的一种集多种特殊功能于一体的数字签名,兼具了门限签名和多重代理签名的特性,即在门限代理签名中,只需要 n 个代理签名者中的任意 t 个或多于 t 个一起合作就能代表原始签名者进行签名。与多重代理签名相比,门限代理签名具有更大的灵活性。

然而,门限代理签名仅仅实现了一个原始签名者将签名权委托给多个代理签名者的情形,对于多个原始签名者将签名权委托给多个代理签名者的情形则无法实现。为此,2003年, Li 等人^[7]将门限代理签名进行了推广,提出了 $(t_1, n_1; t_2, n_2)$ 门限多代理多签名方案。在该方案中,只有 n_1 个原始签名者中的至少 t_1 个合作才能授权给代理签名者;同时,只有 n_2 个代理签名者中的至少 t_2 个合作才能产生有效的代理签名。门限多代理多签名作为一种特殊的数字签名,在某些特殊的场合有着特殊的作用。例如,部分原始签名者或部分代理签名者由于某种原因不能参与授权或签名时,要确保签名的顺利进行,就需要使用门限多代理多签名。随着门限多代理多

签名研究的深入,各种门限多代理多签名方案相继提出。2004年, Tzeng 等人^[8]提出了具有共享验证性质的门限多代理多签名方案。最近,文献^[9]提出了具有多种特性的门限多代理多签名方案,实现了不同类成员具有不等权限、具有消息恢复和只有指定验证者才能验证签名的特性。但以上方案都是在基于传统的公钥证书的密码体制下而提出的,考虑到基于身份的密码体制的优点,文献^[10]利用双线性映射首次提出了基于身份的门限多代理多签名方案。而基于身份的密码体制存在密钥托管问题,为了克服这个缺陷, Al-Riyami 和 Paterson^[11]于2003年提出了无证书公钥密码体制,并成为近年来密码学研究领域的热点课题之一。

为此,本文在文献^[12]的基础上,首次在基于无证书公钥密码体制下提出了一个无证书门限多代理多签名方案。经分析,该方案是一个安全实用的方案。

1 准备知识

1.1 双线性映射

假设 G_1 是一个生成元为 P 的循环加法群,它的阶为素数 q , G_2 是一个阶为 q 的循环乘法群。称映射 e 为双线性映射,若映射 $e: G_1 \times G_1 \rightarrow G_2$ 满足下列性质:

- 1) 双线性性。 $e(aP, bQ) = e(P, Q)^{ab}, \forall P, Q \in G_1, a, b \in \mathbb{Z}_q^*$ 。
- 2) 非退化性。存在一个 $P \in G_1$,使得 $e(P, P) \neq 1$ 。
- 3) 可计算性。对 $P, Q \in G_1$,存在一个有效的算法能够计算 $e(P, Q)$ 。

收稿日期:2009-08-21;修回日期:2009-10-28。

作者简介:杨长海(1978-),男,江西瑞金人,讲师,硕士,主要研究方向:密码学、数字签名。

对于双线性对 $e(P, Q)$ 是可以计算的,但对于双线性对求逆是困难的,即已知 $P \in G_1, e(P, Q) \in G_2$, 计算 $Q \in G_1$ 是个困难问题。

1.2 无证书代理签名

1.2.1 定义

一个无证书代理签名方案包括以下几个过程。

1) 系统初始化过程。给定安全参数,产生系统主密钥 s 和系统参数 $params$ 。

2) 部分私钥提取过程。给定 $params$ 、系统主密钥 s 和用户身份 ID ,产生部分私钥 D_{ID} 。

3) 秘密值生成过程。给定 $params$ 和用户身份 ID ,产生用户的秘密值 x 。

4) 公钥生成过程。给定 $params$ 和用户的秘密值 x ,产生用户公钥 P_{ID} 。

5) 私钥生成过程。给定用户身份信息、秘密值、公钥及部分私钥,产生用户私钥 S_{ID} 。

6) 代理授权过程。给定 $params$ 、原始签名者的私钥和授权证书 m_ω ,产生代理授权密钥,其中 m_ω 描述了成员身份信息、证书的有效时间、代理权限等。

7) 代理私钥产生过程。给定代理授权密钥和代理签名者的私钥,产生代理私钥。

8) 代理签名过程。给定消息 m 、 m_ω 和代理私钥,产生代理签名。

9) 签名验证过程。给定代理签名、原始签名者和代理签名者的身份及公钥,判断验证式是否成立。

1.2.2 敌手模型

在无证书代理签名方案中,有2种类型的敌手。

类型 I 的敌手:不能获得系统主密钥,但可以替换用户的公钥,如不诚实的用户。

类型 II 的敌手:能够获得系统主密钥,从而得到用户的部分私钥,但不能替换用户的公钥,如一个恶意的 KGC 或与 KGC 合作的攻击者。

2 提出的方案

设 $\{A_1, A_2, \dots, A_{n_1}\}$ 是由 n_1 个原始签名者组成的原始组, A_0 是可信的组管理员; $\{P_1, P_2, \dots, P_{n_2}\}$ 是由 n_2 个代理签名者组成的代理组, B_0 是可信的组管理员, KGC 是密钥生成中心。提出的 $(t_1, n_1; t_2, n_2)$ 门限多代理多签名方案包括以下几个过程。

2.1 系统初始化过程

1) KGC 生成两个阶为素数 q 的群 $(G_1, +)$ 和 (G_2, \cdot) , 选择 G_1 的任意一个生成元 $P, e: G_1 \times G_1 \rightarrow G_2$ 是一个双线性映射,选择安全哈希函数 $H_0, H_1, H_3, H_4: \{0, 1\}^* \rightarrow G_1^*$ 。

2) KGC 选择主密钥 $s \in_R \mathbf{Z}_q^*$, 并计算 $P_{pub} = sP$, 将 s 作为主密钥保存起来,公开系统参数 $(G_1, G_2, e, Q, P, P_{pub}, H_0, H_1, H_3, H_4)$ 。

2.2 部分私钥提取过程

对身份 ID_{Ai} 和 ID_{Bj} ($i = 0, 1, \dots, n_1; j = 0, 1, \dots, n_2$), KGC 计算相应的部分私钥 $D_{Ai} = sQ_{Ai}, D_{Bj} = sQ_{Bj}$, 其中 $Q_{Ai} = H_1(ID_{Ai}), Q_{Bj} = H_1(ID_{Bj})$ 。

2.3 秘密值生成过程

用户选取 $x_{Ai} \in_R \mathbf{Z}_q^*, x_{Bj} \in_R \mathbf{Z}_q^*$ 作为自己的秘密值。

2.4 公钥生成过程

用户利用系统参数和秘密值计算并公开公钥 $P_{Ai} = x_{Ai}P, P_{Bj} = x_{Bj}P$ 。

2.5 私钥生成过程

用户利用自己的身份信息、秘密值、公钥及部分私钥,计算相应的私钥 $S_{Ai} = D_{Ai} + x_{Ai}T_{Ai}, S_{Bj} = D_{Bj} + x_{Bj}T_{Bj}$, 其中 $T_{Ai} = H_2(ID_{Ai} \parallel P_{Ai}), T_{Bj} = H_2(ID_{Bj} \parallel P_{Bj})$ 。

2.6 代理授权过程

2.6.1 原始签名者秘密共享

1) 管理员 A_0 选择一个 $t_1 - 1$ 次多项式 $F(x) = S_{A0} + \sum_{k=1}^{t_1-1} a_k x^k, a_k \in G_1$;

2) 管理员 A_0 计算 $F(ID_{Ai})$, 并通过安全信道传给相应的原始签名者 A_i , 公布 $\alpha_k = e(a_k, P)$ ($k = 1, 2, \dots, t_1 - 1$);

3) 原始签名者 A_i 收到 $F(ID_{Ai})$ 后, 首先计算 $\alpha_0 = e(Q_{A0}, P_{pub})e(T_{A0}, P_{A0})$, 然后验证 $e(F(ID_{Ai}), P) = \prod_{k=0}^{t_1-1} \alpha_k^{ID_{Ai}^k}$ 是否成立, 若不成立则要求重发, 否则将 $F(ID_{Ai})$ 作为原始签名者 A_i 从管理员 A_0 处获得的秘密份额。

2.6.2 代理授权的产生

不失一般性, 设 $\{A_1, A_2, \dots, A_{t_1}\}$ 为实际参与授权的原始签名者, m_ω 为授权证书, 描述了成员身份信息、原始组及代理组的门限值 t_1 和 t_2 、证书的有效时间、代理权限等。要完成代理授权, 可通过如下过程产生。

1) 原始签名者 A_i ($i = 1, 2, \dots, t_1$) 选择 $r_{Ai} \in_R \mathbf{Z}_q^*$, 计算 $R_{Ai} = r_{Ai}P$, 将 R_{Ai} 传给指定合成者 C_1 。

2) 指定合成者 C_1 收到 R_{Ai} 后, 计算并公布 $R_A = \sum_{i=1}^{t_1} r_{Ai}P$ 和 $U_A = H_3(m_\omega \parallel ID_A \parallel P_A \parallel R_A)$, 其中 ID_A 为实际参与的原始签名者的身份信息 $ID_{A1} \parallel ID_{A2} \parallel \dots \parallel ID_{At_1}, P_A$ 为实际参与的原始签名者的公钥 $P_{A1} \parallel P_{A2} \parallel \dots \parallel P_{At_1}$ 。

3) A_i ($i = 1, 2, \dots, t_1$) 计算 $K_{Ai} = \lambda_{Ai}F(ID_{Ai}) + S_{Ai} + r_{Ai}U_A$, 其中 $\lambda_{Ai} = \prod_{j=1, j \neq i}^{t_1} (-ID_{Aj})(ID_{Ai} - ID_{Aj})^{-1}$, 将 K_{Ai} 作为部分代理授权密钥通过安全信道传给指定合成者 C_1 。

4) 指定合成者 C_1 收到 K_{Ai} 后, 验证下式是否成立。

$$e(K_{Ai}, P) = e(F(ID_{Ai}), P)^{\lambda_{Ai}} e(Q_{Ai}, P_{pub}) e(T_{Ai}, P) e(U_A, R_{Ai})$$

若不成立则要求重发, 否则计算 $K_A = \sum_{i=1}^{t_1} K_{Ai}$, 将 (K_A, R_A) 作为代理授权密钥秘密传给代理签名者 B_j 。

2.7 代理私钥产生过程

B_j ($j = 1, 2, \dots, n_2$) 收到 (K_A, R_A) 后, 验证下式是否成立。

$$e(K_A, P) = e\left(\sum_{i=0}^{t_1} Q_{Ai}, P_{pub}\right) e\left(\sum_{i=0}^{t_1} T_{Ai}, P\right) e(U_A, R_A) \quad (1)$$

若不成立则拒绝代理, 否则接受原始签名者的授权, 并计算代理私钥 $\sigma_{Bj} = t_2^{-1}K_A + S_{Bj}$ 。

2.8 代理签名过程

2.8.1 代理签名者秘密共享

1) 管理员 B_0 选择一个 $t_2 - 1$ 次多项式 $f(x) = S_{B0} + \sum_{k=1}^{t_2-1} b_k x^k, b_k \in G_1$;

2) 管理员 B_0 计算 $f(ID_{Bj})$, 并通过安全信道传给相应的

代理签名者 B_j , 公布 $\beta_k = e(b_k, P)$ ($k = 1, 2, \dots, t_2 - 1$);

3) 代理签名者 B_j 收到 $f(ID_{B_j})$ 后, 首先计算 $\beta_0 = e(Q_{B_0},$

$P_{pub})e(T_{B_0}, P_{B_0})$, 然后验证 $e(f(ID_{B_j}), P) = \prod_{k=0}^{t_2-1} \beta_k^{ID_{B_j}^k}$ 是否成立, 若不成立则要求重发, 否则将 $f(ID_{B_j})$ 作为代理签名者 B_j 从管理员 B_0 处获得的秘密份额。

2.8.2 代理签名的产生

不妨设 $\{B_1, B_2, \dots, B_{t_2}\}$ 为实际参与签名的代理签名者。

为了完成对消息 m 的签名, 可以通过如下过程产生。

1) 代理签名者 B_j ($j = 1, 2, \dots, t_2$) 选择 $r_{B_j} \in_R \mathbf{Z}_q^*$, 计算 $R_{B_j} = r_{B_j}P$, 并将其传给指定的合成者 C_2 ;

2) 签名合成者 C_2 收到 R_{B_j} 后, 计算并公布 $R_B = \sum_{j=1}^{t_2} R_{B_j}$ 和 $U_B = H_4(m \| m_\omega \| ID_B \| P_B \| R_B)$, 其中 ID_B 为实际参与的代理签名者的身份信息 $ID_{B_1} \| ID_{B_2} \| \dots \| ID_{B_{t_2}}$, P_B 为实际参与的代理签名者的公钥 $P_{B_1} \| P_{B_2} \| \dots \| P_{B_{t_2}}$;

3) B_j ($j = 1, 2, \dots, t_2$) 计算 $V_{B_j} = \sigma_{B_j} + \lambda_{B_j}f(ID_{B_j}) + r_{B_j}U_B$, 其中 $\lambda_{B_j} = \prod_{i=1, i \neq j}^{t_2} (-ID_{B_i})(ID_{B_j} - ID_{B_i})^{-1}$, 将 V_{B_j} 作为部分代理签名通过安全信道传给指定签名合成者 C_2 ;

4) 签名合成者 C_2 收到 V_{B_j} 后, 验证下式是否成立:

$$e(V_{B_j}, P) = e(t_2^{-1}K_A, P)e(f(ID_{B_j}), P)^{\lambda_{B_j}} e(Q_{B_j}, P_{pub})e(T_{B_j}, P)e(U_B, R_{B_j}) \quad (2)$$

若不成立则要求重发, 否则计算 $V = \sum_{j=1}^{t_2} V_{B_j}$, 将 (R_A, R_B, V) 作为对消息 m 的门限多代理多签名。

2.9 签名验证过程

为验证 (R_A, R_B, V) 的有效性, 验证者首先计算 $Q_{A_i} = H_1(ID_{A_i})$, $Q_{B_j} = H_1(ID_{B_j})$, $T_{A_i} = H_2(ID_{A_i} \| P_{A_i})$, $T_{B_j} = H_2(ID_{B_j} \| P_{B_j})$, $U_A = H_3(m_\omega \| ID_A \| P_A \| R_A)$, $U_B = H_4(m \| m_\omega \| ID_B \| P_B \| R_B)$, 然后验证下式是否成立。

$$e(V, P) = e\left(\sum_{i=0}^{t_1} Q_{A_i}, P_{pub}\right)e\left(\sum_{j=0}^{t_2} Q_{B_j}, P_{pub}\right) \times \prod_{i=0}^{t_1} e(T_{A_i}, P_{A_i}) \prod_{j=0}^{t_2} e(T_{B_j}, P_{B_j})e(U_A, R_A)e(U_B, R_B) \quad (3)$$

若成立, 则接受签名, 否则拒绝。

3 方案分析

3.1 正确性分析

1) 代理签名者可通过式(1)验证代理授权的有效性。

证明

$$\begin{aligned} e(K_A, P) &= e\left(\sum_{i=1}^{t_1} K_{A_i}, P\right) = \\ &= e\left(\sum_{i=1}^{t_1} (\lambda_{A_i}F(ID_{A_i}) + S_{A_i} + r_{A_i}U_A), P\right) = \\ &= e\left(\sum_{i=1}^{t_1} \lambda_{A_i}F(ID_{A_i}), P\right)e\left(\sum_{i=1}^{t_1} S_{A_i}, P\right)e\left(\sum_{i=1}^{t_1} r_{A_i}U_A, P\right) = \\ &= e(S_{A_0}, P)e\left(\sum_{i=1}^{t_1} S_{A_i}, P\right)e(U_A, R_A) = \\ &= e\left(\sum_{i=0}^{t_1} (D_{A_i} + x_{A_i}T_{A_i}), P\right)e(U_A, R_A) = \\ &= e\left(\sum_{i=0}^{t_1} D_{A_i}, P\right)e\left(\sum_{i=0}^{t_1} x_{A_i}T_{A_i}, P\right)e(U_A, R_A) = \end{aligned}$$

$$e\left(\sum_{i=0}^{t_1} Q_{A_i}, P_{pub}\right) \prod_{i=0}^{t_1} e(T_{A_i}, P_{A_i})e(U_A, R_A)$$

2) 签名合成者可通过式(2)验证部分签名的有效性。

证明

$$\begin{aligned} e(V_{B_j}, P) &= e(\sigma_{B_j} + \lambda_{B_j}f(ID_{B_j}) + r_{B_j}U_B, P) = \\ &= e(t_2^{-1}K_A + S_{B_j}, P)e(f(ID_{B_j}), P)^{\lambda_{B_j}}e(U_B, R_{B_j}) = \\ &= e(t_2^{-1}K_A, P)e(D_{B_j} + x_{B_j}T_{B_j}, P)e(f(ID_{B_j}), P)^{\lambda_{B_j}} \\ &= e(U_B, R_{B_j}) = \\ &= e(t_2^{-1}K_A, P)e(Q_{B_j}, P_{pub})e(T_{B_j}, P_{B_j})e(f(ID_{B_j}), P)^{\lambda_{B_j}} \\ &= e(U_B, R_{B_j}) \end{aligned}$$

3) 验证者可通过式(3)验证门限多代理多签名的有效性。

证明

$$\begin{aligned} e(V, P) &= e\left(\sum_{j=1}^{t_2} V_{B_j}, P\right) = \\ &= e\left(\sum_{j=1}^{t_2} (\sigma_{B_j} + \lambda_{B_j}f(ID_{B_j}) + r_{B_j}U_B), P\right) = \\ &= e\left(\sum_{j=1}^{t_2} (t_2^{-1}K_A + S_{B_j}), P\right)e(S_{B_0}, P)e(U_B, R_B) = \\ &= e(K_A, P)e\left(\sum_{j=0}^{t_2} S_{B_j}, P\right)e(U_B, R_B) = \\ &= e\left(\sum_{i=0}^{t_1} Q_{A_i}, P_{pub}\right)e\left(\sum_{j=0}^{t_2} Q_{B_j}, P_{pub}\right) \times \\ &= \prod_{i=0}^{t_1} e(T_{A_i}, P_{A_i}) \prod_{j=0}^{t_2} e(T_{B_j}, P_{B_j})e(U_A, R_A)e(U_B, R_B) \end{aligned}$$

3.2 安全性分析

1) 方案具有可区分性。由于 m_ω 中包含了原始签名者和代理签名者的信息, 所以任何人都可以从签名中区分该签名是代理签名还是普通签名。

2) 方案具有可识别性和不可否认性。由于在验证过程中需要用到实际参与授权的原始签名者和实际参与签名的代理签名者的公钥, 因此验证者可以从签名中识别出实际参与授权和签名的成员, 同时, 实际参与的原始签名者不能否认自己参与了授权, 实际参与的代理签名者也不能否认自己参与了签名。

3) 方案具有不可伪造性。一方面, 攻击者不能伪造原始签名者的授权。首先考虑攻击者直接伪造原始签名者的私钥的情形。对类型 I 的敌手可以选取秘密值 $x_{A_i}' \in_R \mathbf{Z}_q^*$, 将原始签名者的公钥替换成 $P_{A_i}' = x_{A_i}'P$, 但由于类型 I 的敌手不知道主密钥 s , 从而不知道原始签名者的部分私钥 $D_{A_i} = sQ_{A_i}$, 因而很难构造出一个有效的私钥 $S_{A_i}' = D_{A_i} + x_{A_i}'T_{A_i}'$, 其中 $T_{A_i}' = H_2(ID_{A_i} \| P_{A_i}')$; 而对类型 II 的敌手可以拥有主密钥 s , 但不能获得秘密值 x_{A_i} , 同理不能由 $S_{A_i} = D_{A_i} + x_{A_i}T_{A_i}$ 获得有效的私钥。其次, 考虑在不知道原始签名者的私钥的情况下, 攻击者伪造原始签名者授权的情形。不妨设攻击者试图伪造身份为 ID_{A_i} ($i = 1, 2, \dots, t_1$) 的原始签名者的代理授权密钥 (K_A, R_A) , 并能通过验证式(1)。对类型 I 的敌手可以将原始签名者的公钥替换成 $P_{A_i}' = x_{A_i}'P$, 计算 $T_{A_i} = H_2(ID_{A_i} \| P_{A_i}')$, $Q_{A_i} = H_1(ID_{A_i})$, 攻击者也可随机选取 $R_A \in G_1$, 计算 $U_A = H_3(m_\omega \| ID_A \| P_A \| R_A)$, 其中 ID_A 为 $ID_{A_1} \| ID_{A_2} \| \dots \| ID_{A_{t_1}}$, P_A 为 $P_{A_1}' \| P_{A_2}' \| \dots \| P_{A_{t_1}}'$, 从而计算出 $e\left(\sum_{i=0}^{t_1} Q_{A_i}, P_{pub}\right)e\left(\sum_{i=0}^{t_1} T_{A_i}, P\right)e(U_A, R_A)$ 。但根据双线性对求逆问题的困

难性,攻击者要从 $e(K_A, P) = e\left(\sum_{i=0}^{t_1} Q_{Ai}, P_{pub}\right) e\left(\sum_{i=0}^{t_1} T_{Ai}, P\right) e(U_A, R_A)$ 中求出 K_A 是不可能的,即类型 I 的敌手不能伪造代理授权密钥 (K_A, R_A) 。同理,类型 II 的敌手进行类似攻击也不能成功。

另一方面,攻击者不能伪造代理签名者的签名。类似上面的分析,攻击者不能通过直接伪造代理签名者的私钥来伪造签名。另外,攻击者也不可能伪造门限多代理多签名 (R_A, R_B, V) ,使其通过验证式:

$$e(V, P) = e\left(\sum_{i=0}^{t_1} Q_{Ai}, P_{pub}\right) e\left(\sum_{j=0}^{t_2} Q_{Bj}, P_{pub}\right) \times \prod_{i=0}^{t_1} e(T_{Ai}, P_{Ai}) \prod_{j=0}^{t_2} e(T_{Bj}, P_{Bj}) e(U_A, R_A) e(U_B, R_B)$$

因为即使攻击者能获得等式左边,也不可能由此式获得 V ,这将面临求解双线性对求逆问题。

4) 方案能抵抗内部成员的合谋攻击。在原始签名者秘密共享和代理签名者秘密共享过程中,我们采用的都是可验证秘密共享方案,因此,即使有 $t_1 - 1$ 个内部成员合谋也不可能完成代理授权过程,任意 $t_2 - 1$ 个内部成员合谋也不可能产生有效的签名。

4 结语

现有的门限多代理多签名方案均是在传统的基于证书的公钥密码体制或基于身份的密码体制下设计的,考虑到无证书密码体制的优点,本文提出了一个无证书门限多代理多签名方案。经分析,该方案满足门限多代理多签名所需的安全性性质。

参考文献:

[1] MAMBO M, USUDA K, OKAMOTO E. Proxy signatures: Delegation of the power to sign messages[J]. IEICE Transactions on Fundamentals, 1996, E79-A(9): 1338 - 1354.

- [2] HWANG S J, SHI C H. A simple multi-proxy signature scheme [C]// Proceedings of the 10th National Conference on Information Security. Hualien: [s. n.], 2000: 134 - 138.
- [3] YI LI-JIANG, BAI GUO-QIANG, XIAO GUO-ZHEN. Proxy multi-signature scheme: A new type of proxy signature scheme[J]. Electronics Letters, 2000, 36(6): 527 - 528.
- [4] HWANG S J, CHEN C C. A new multi - proxy multi - signature scheme[C]// 2001 National Computer Symposium: Information Security. Taipei: [s. n.], 2001: F016 - F026.
- [5] LIN W D, JAN J K. A security personal learning tools using a proxy blind signature scheme[C]// Proceedings of International Conference on Chinese Language Computing. Illinois, USA: [s. n.], 2000: 273 - 277.
- [6] ZHANG K. Threshold proxy signature schemes[C]// Proceedings of the 1997 Information Security Workshop. Japan: [s. n.], 1997: 191 - 197.
- [7] LI L H, TZENG S F, HWANG M S. Generalization of proxy signature based on discrete logarithms [J]. Computers & Security, 2003, 22(3): 245 - 255.
- [8] TZENG S F, YANG C Y, HWANG M S. A nonrepudiable threshold multi-proxy multi-signature scheme with shared verification [J]. Future Generation Computer Systems, 2004, 20(5): 887 - 893.
- [9] 杨长海,唐西林. 具有多种特性的门限多代理多签名方案[J]. 计算机工程, 2009, 35(13): 160 - 162.
- [10] 杨长海,唐西林. 基于身份的门限多代理多签名方案[J]. 计算机应用研究, 2009, 26(2): 702 - 704.
- [11] AL-RIYAMI S S, PATERSON K G. Certificateless public key cryptography [C]// Proceedings of Asiacrypt 2003, LNCS 2894. Berlin: Springer-Verlag, 2003: 452 - 473.
- [12] 陈虎,张福泰,宋如顺. 可证安全的无证书代理签名方案[J]. 软件学报, 2009, 20(3): 692 - 701.

(上接第509页)

4 结语

本文针对保护私有信息的集合交集问题进行了研究。在半诚实模型下,基于点积协议设计了安全高效的协议,对协议的正确性给予理论证明并分析了协议的安全性、复杂度。当然协议还存在一定的不足:首先,协议是基于半诚实模型的,在实际应用中,如何有效保证半诚实模型的实现以及如何应对参与方的恶意欺骗或主动攻击还有待探讨;其次,文中协议都是由某一参与方获取协议结果,然后再发送给其他参与方。在实际应用中,如何有效保证参与方发送结果的真实性以及防止相互勾结即协议对各参与方的公平性、公正性问题还有待探讨。

参考文献:

- [1] YAO A C. Protocols for secure computations[C]// Proceedings of the 23rd Annual IEEE Symposium on Foundations of Computer Science. Washington, DC: IEEE Computer Society, 1982: 160 - 164.
- [2] GOLDBREICH O. Secure multi-party computation (manuscript version 1.3) [EB/OL]. [2009 - 08 - 01]. <http://theory.lcs.mit.edu/~oded>.
- [3] DU W L, ATALLAH M J. Secure multi-party computation problems and their applications: A review and open problems[C]// Proceedings of New Security Paradigms Workshop. New York: ACM, 2001: 11 - 20.
- [4] 仲红,黄刘生,罗永龙. 基于安全多方求和的多候选人电子选举方案[J]. 计算机研究与发展, 2006, 43(8): 1405 - 1410.

- [5] FREEDMAN M J, NISSIM K, PINKAS B. Efficient private matching and set intersection[C]// EUROCRYPT 2004, LNCS 3027. Berlin: Springer-Verlag, 2004: 1 - 19.
- [6] KISSNER L, SONG D. Privacy - preserving set operations [C]// CRYPTO 2005: The 25th Annual International Cryptology Conference, LNCS 3621. Berlin: Springer-Verlag, 2005: 241 - 257.
- [7] KIAYIAS A, MITROFANOVA A. Testing disjointness of private datasets[C]// FC'05: Ninth International Conference on Financial Cryptography and Data Security, LNCS 3570. Berlin: Springer-Verlag, 2005: 109 - 124.
- [8] 李顺东,司天歌,戴一奇. 集合包含与几何包含的多方保密计算[J]. 计算机研究与发展, 2005, 42(10): 1647 - 1653.
- [9] YE QING - SONG, WANG HUA - XIONG, TARTARY C. Privacy - preserving distributed set intersection[C]// The 3rd International Conference on Availability, Reliability and Security. Washington, DC: IEEE Computer Society, 2008: 1332 - 1339.
- [10] ATALLAH M J, DU WEN-LIANG. Secure multi-party computational geometry[C]// Proceedings of the 7th International Workshop on Algorithms and Data Structures, LNCS 2125. London: Springer-Verlag, 2001: 165 - 179.
- [11] TZENG W-G. Efficient oblivious transfer schemes[C]// PKC 02: Proceedings of 2002 International Workshop on Practice and Theory in Public-Key Cryptography, LNCS 2274. Berlin: Springer-Verlag, 2001: 159 - 171.