面向有差异群体的联合决策方案

雷 浩[1,2], 冯登国[1], 周永彬[1], 张振锋[1]
(1. 中国科学院软件研究所信息安全国家重点实验室, 北京 100080; 2. 中国科学院研究生院 北京 100049)

摘 要: 公平性、透明性是联合决策的基本安全需求. 结合多机构商务合作背景, 利用具有同态性质的 Paillier 公钥密码系统和门限密码技术, 提出了面向有差异群体的联合决策策略与方案, 并对其安全性进行了分析和证明.

关键词: 联合决策; 元权限; Paillier 公钥密码系统; 门限密码系统
中图分类号: TP309.2 文献标识码: A 文章编号: 0372-2112 (2005) 08-1523-06

A Joint Decision-Making Scheme for Groups with Members Having Different Superiorities

LEI Hao[1,2], FENG Deng-guo[1], ZHOU Yong-bin[1], ZHANG Zhen-feng[1]
(1. *State Key Laboratory of Information Security, Institute of Software, Chinese Academy of Sciences, Beijing* 100080, *China*;
2. *Graduate school of the chinese Academy of science, Beijing* 100049, *China*)

Abstract: The basic requirements of joint decision-making are fairness and transparency. In this paper, combined with commercial background, a joint decision-making policy and scheme for groups with members having different superiorities is proposed by using Paillier public key cryptosystem with homeostasis quality based on threshold technique. The newly presented threshold scheme is also proved and examined.

Key words: joint decision-making; meta permission; paillier public-key cryptosystem; threshold cryptosystem

1 引言

面向群体(Group Oriented)的研究领域包括面向群体的联合决策问题研究[1,2]、面向群体的加密解密体系研究[3~6]以及面向群体的匿名性研究[3]等. 对面向群体问题的研究始于 Y. Desmedt 对群体问题的分析, 提出了群体内成员之间职责的差异性以及群体进行加密解密时的需求[3]; 在随后近 20 年的过程中, 人们提出了各种各样的面向群体加密解密的密码体系[4~6].

面向有差异群体的联合决策问题是在一组互不信任的主体之间以一种公开透明的方式就某个提议进行表决, 其中不同主体之间存在诸如地位、权限大小等方面的差别.

以共同分担风险与利益为目的的商务合作, 其基本运作模式就是在合作机构之间以一种公平合理的方式形成联合决策. 本文结合多机构商务合作背景, 针对面向有差异群体的联合决策问题, 提出一般性的联合决策策略及方案. 文章的其余部分组织如下: 第 1 节简要介绍已有的面向群体的联合决策策略, 并指出其不足. 第 2 节针对多机构商务合作中不同机构股权多少差别的事实, 通过引入"元权限"的概念, 提出表达有差异主体的联合决策策略. 第 3 节在具有同态性质的 Paillier 公钥密码系统和门限解密技术基础上, 给出了不需要可信第三方的公开可验证的联合决策多方计算方案的具体细节. 第 4 节对新构造出的联合决策方案进行分析与证明. 第 5 节总结全文.

2 已有的工作和问题

2002 年, 美国马里兰大学的 Khurana 博士在其博士毕业论文中研究了以下多机构商务合作场景, 提出了对联合资源的访问控制问题: "某个基因公司发现了某个基因片段和某种疾病有关, 试图与制药公司和医院联合使用其发现的基因片段开发治疗这种疾病的药物和疗法. 其中, 基因公司负责基因片段的破解和分析, 制药公司在此基础上负责药品的开发和研制, 医院则负责药品的临床实验. 在合作的中间阶段所产生的研究数据归三个机构共同拥有, 而不是某个机构单独所有, 因而使用时需要联合决策.[1,2]" 不难看出, 对联合资源的访问控制问题本质上是商务合作下面向群体的联合决策问题.

Khurana 博士针对多机构商务合作背景下的联合决策问题, 采用的是不考虑主体差别的、基于成员数量的门限联合决策方案: 对于合作群体的某项具体提议, 需要大家共同表决, 如果群体中同意的人数达到了事先门限所要求的人数, 则本次提议通过; 否则, 则拒绝本次提议[1,2].

该方案存在以下两方面不足:

收稿日期: 2004-01-24; 修回日期: 2005-04-25
基金项目: 国家 973 课题项目(No. G1999035802); 国家自然科学基金项目(No. 60373039); 国家自然科学基金重大研究计划项目(No. 90304007); 国家 863 课题项目(No. 2004AA147070)

(1)一般而言,群体内部成员之间普遍存在职责大小的差异性[3],这一点在商务合作群体中体现的尤为明显:商务合作中,机构所持有股权多少直接决定了其在合作中的地位,因而就表决时的权限大小而言,每个机构实际上是有差异的.因此,不考虑股权多少的差异而带来的权限大小差别,默认为不同主体的权限大小是一样的,联合决策的结果仅依赖赞成成员数量的多少来决定是不符合商务合作原则的.

(2)决策计算的结果以及结果的判定需要可信第三方(协同服务器,Coalition Server)来完成[1,2].这一方面导致决策结果计算的正确与否完全寄托于可信第三方,缺乏公开透明性;另一方面决策结果的集中式判定与面向群体的分布式应用环境极不适应.

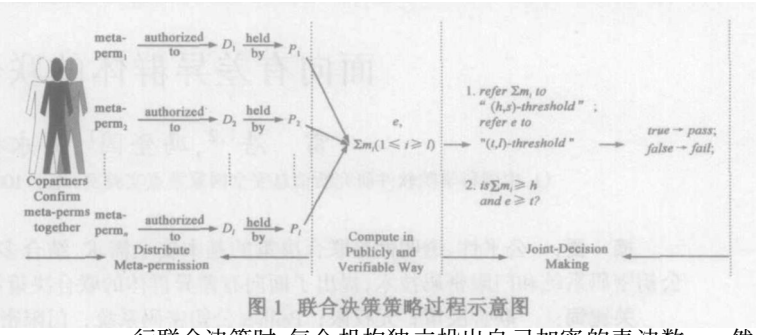

图1 联合决策策略过程示意图

3 联合意图的表达与计算

多机构商务合作体系中存在以下实体:

® 商业机构 $D_i(1\leqslant i\leqslant l)$

如文章开始场景中的私有基因公司,制药公司和医院.一方面它是独立自治的商业机构,另一方面又是进行商务合作的基本单位.假定参与商务合作的机构共有 l 个,记为 $D_i(1\leqslant i\leqslant l)$;

® 机构代言人 $P_i(1\leqslant i\leqslant l)$

多机构商务合作决策中代表机构表决的机构成员,机构 D_i 的代言人记为 $P_i(1\leqslant i\leqslant l)$;

3.1 反映有差异群体的权限机制

若 *JOS* 表示需要联合决策的事件,N 表示自然数集合,则:

® 元权限[7]

将二元组 $(jos, m)\in MetaPerms = JOS\times N$ 称之为元权限,m 称为元权限的值.它是量化权限下针对 jos 授权时的基本单位.制定及分配商务合作中不同机构的元权限值需要与其所持有的股份多少成比例.

® 同质元权限[7]

同质元权限是 (jos, m) 中 jos 相同的元权限;同质元权限的值彼此不同,其值反映了商务合作中的不同机构所持有的股权差异,并且可以进行相加运算.

将多机构商务合作决策中机构代言人 P_i 每次表决的数字称为表决数,记为 $m_i(1\leqslant i\leqslant l)$.若同意提议,则表决数 m_i 为其所持有的元权限值 m;若反对提议,则表决数为 $-m$.

3.2 多机构商务合作下的联合决策策略

①元权限的管理 元权限的管理包括元权限的创建、授予、更改以及撤销.当商务合作关系确立后,由进行商务合作的机构一起根据各个机构在合作中所持有的股权比例,共同商议确定若干不同大小的同质元权限并将其授予相应的机构代言人 P_i;当商务合作中某个机构的股权发生了变化(例如发生了股权转让)或者某个机构退出合作,其所持有的元权限也需随之更改或者撤销,这同样需要进行商务合作的机构共同商议确定.

②联合决策策略 当商务合作中针对某个具体提议进行联合决策时,每个机构独立投出自己加密的表决数 m_i,然后所有机构共同以一种公开可验证的方式计算表决数之和 $\Sigma m_i(1\leqslant i\leqslant l)$.提议是否通过依靠决策门限进行裁决.

决策门限包括权限门限$_{(h,s)}$以及人数门限$_{(t,l)}$,具体策略是:如果总共参与表决有 l 个机构,所持有的同质元权限之和为 s,那么权限门限$_{(h,s)}$要求表决数之和不小于 h,人数门限$_{(t,l)}$要求必须有 t 个赞成,方才通过.

联合决策依靠决策门限裁决,可以保证合作机构的知情权和监督权.

基本思想如图1所示.

4 构造门限联合决策机制

本文假设在同步网络条件下,合作机构两两之间存在一个认证信道(Authenticated Channel,攻击者可以窃听任意参与者之间的通讯内容但是不能篡改).另外,攻击者是具有多项式时间计算能力的静态攻击者(如果攻击者在计算开始之前就确定买通任意的一组数量是有一定限制的参与者做为不诚实参与者,在协议执行以后就不改变了,则称这种攻击者是静态攻击者).

联合决策结果的计算必须满足以下需求:

(1). 表决数的合法性与保密性 合法性是指表决数一定来自集合 $\{m_{i1}=m, m_{i2}=-m\}$,这里 m 是该机构代言人所持有的元权限值;保密性是指表决数究竟是 m_{i1} 还是 m_{i2},则是保密的.

(2). 鲁棒性 表决数之和 $\Sigma m_i(1\leqslant i\leqslant l)$ 需要至少 t 个机构的协作才可以计算出来.

(3). 可公开验证性 任何人都确信最后求得的表决数之和 $\Sigma m_i(1\leqslant i\leqslant l)$ 是正确的;

另外,由于 P_i 每次的表决数 m_i 或者为 m_{i1},或者为 m_{i2}.为了防止攻击者通过密文的对比获悉表决数,拟采用概率加密算法.

文献[8]基于 $Z_{n^2}^*$ 上复合高阶剩余类问题的难解性(简称为 *CR*[*n*] 问题),提出了一种具有同态性质(密文之积等于明文之和对应的密文,即 $E_k(m_1+m_2)=E_k(m_1)\cdot E_k(m_2)$ 的概率公钥密码系统:Paillier 公钥密码系统.下面就利用 Paillier 密码系统,并借助于门限加密/解密技术,以一种可公开验证的方式来计算表决数之和 $\Sigma m_i(1\leqslant i\leqslant l)$.

4.1 计算表决数之和的公开可验证方案

门限密码技术[DFST94]是新兴的密码学研究领域.它主要研究:由一个实体发起或执行的密码学操作,如何分散到由多个实体所组成的群体来执行的问题.从实现的过程来看,

包括密钥生成、加密、解密以及结合算法四个部分. 本节结合表决数之和的计算, 以门限版本的 Paillier 公钥密码系统为实现的技术基础, 介绍计算表决数之和的公开可验证方案.

® 密钥生成

设表决人的集合为 $\Gamma = \{P_1, P_2, \cdots, P_l\}$:

(1)随机选择两个强大素数 p, q, 并令 $n = pq$; 其中 $p = 2p' + 1$, $q = 2q' + 1$, $gcd(n, \varphi(n)) = 1$; 根据文献[10]给出的分布式建立 n 的方法, 可以不需要可信第三方.

(2) 令 $\zeta = p'q'$, 随机选择 $\beta \in_R Z_n^*$; 密钥 $sk = \beta\zeta$ 在 $Z_{n\zeta}$ 上按照 Shamir 的秘密分享方案进行分享: $S_i = f(x_i) \bmod n\zeta$, 并将 $s_i (1 \leqslant i \leqslant l)$ 分发给相应的 $P_i (1 \leqslant i \leqslant l)$. 分发完成之后, 则可将密钥 $SK = \beta\zeta$ 销毁.

(3) 随机选择 $(a, b) \in_R Z_n^* \times Z_n^*$, 令 $g = (1 + n)^a b^n \bmod n^2$; 设 b 在 Z_n^* 中的阶为 α, 则 g 在 $Z_{n^2}^*$ 中的阶就是 $n\alpha$(详见附录命题 1 的证明). 公钥包括 g, n 以及 $\theta = \alpha\beta\zeta \bmod n$, 把 (a, b) 销毁.

(4) 设 $VK = v$ 是 $Z_{n^2}^*$ 中平方数(如 1, 4, 9, …)所组成的循环群(详见附录命题 2 的证明)的生成元, 记 $\overline{v} = v^{l!} \bmod n^2$, 验证密钥 $\overline{v}^{s_i} = VK_i = v^{l! s_i} \bmod n^2 (1 \leqslant i \leqslant l)$. 公开 VK, $VK_i (1 \leqslant i \leqslant l)$.

(5)把公钥 (n, g, θ) 以及验证密钥序列 $VK = v$, VK_1, VK_2, …, VK_l 公开. 这里 l 是表决人集合的大小.

® 加密以及计算表决数之和对应的密文

$$c = \prod_1^l c_i$$

每个表决人 $P_i (1 \leqslant i \leqslant l)$ 按照如下方式独立加密各自的表决数 $m_i \in Z_n$: 随机选取 $r_i \in_R Z_n^*$, 按照下列运算计算表决数的加密 $E_k(m_i, r_i) = c_i = g^{m_i} r_i^n \bmod n^2$, 产生表决数对应的加密 c_i;

表决人 P_i 通过和其他机构的表决人之间的两两认证信道, 向 $P_j (1 \leqslant j \leqslant l, j \neq i)$ 广播 c_i;

P_i 收到其他 $l-1$ 个表决数的加密 $c_j (1 \leqslant j \leqslant l, j \neq i)$ 后, 利用 Paillier 公钥密码系统的同态性质, 计算表决数之和对应的密文: $c = \prod_{i=1}^{l} c_i = g^{\sum m_i} (\prod r_i) \bmod n^2 (1 \leqslant i \leqslant l)$; 然后表决人相互比较各自计算的 c 是否相等.

® 部分解密

每个表决人 $P_i (1 \leqslant i \leqslant l)$ 使用所持有的私钥分享 s_i, 按照如下方法计算密文 c 的部分解密 d_i:

$$d_i = c^{2l! s_i} \bmod n^2$$

并做出解密正确性的证明 $Proof_i$: 证明把 $c^{4l!} \bmod n^2$ 和 $v^{l!} \bmod n^2$ 都进行了 s_i 次方而得到 d_i^2 和 v_i. 具体证明办法见下节, 并将 $(d_i, Proof_i)$ 广播给其他表决人.

® 结合算法

如果每个表决人 $P_i (1 \leqslant i \leqslant l)$ 获得的有效部分解密 d_i 少于 t 个, 则结合算法失败; 否则, 可以按照下面的办法恢复出明文:

$$M = \sum_{i=1}^{l} m_i = L\left(\prod_{j \in \Gamma} d_i^{2u_{0,i}^{\Gamma}}\right) \times \frac{1}{4(l!)^2\theta} \bmod n;$$ 这里符号 $u_{0,i}^{\Gamma} = l! \times \prod_{j \in \Gamma, j \neq i} \frac{j}{j - i} \in Z$, 函数 $L(x) = \frac{x - 1}{n}$, 输入参数为 $S_x = \{x < n^2 \mid x = 1 \bmod n\}$. 结合算法的正确性将在下节证明.

4.2 两个诚实验证者的零知识协议

文献[9]、[12]分别提出了两个重要的诚实验证者的零知识交互协议, 本文利用这两个协议(仅仅是利用, 但并不试图构造这样的协议), 来实现面向有差异群体的联合决策中的有关证明.

一般而言, 在需要执行密码协议的网络中, 交互式证明的代价很高, 一个典型密码协议的内部运算能在几秒钟内完成, 而进行信息交换的时间是它的上百倍, 但这些协议又是不可或缺的, 所以有必要将上述交互式证明转换为非交互式证明. 我们按照 Fiat-Shamir 提出的方法[13]: 将和诚实验证者的交互零知识证明通过哈希函数 $H: \{0,1\}^* \to \{0,1\}^{w_1}$ 转化为数字签名方案. 这里 H 是一个公开的、抗碰撞的哈希函数, 其输出长度(比如 128 比特)为 $w_1 < \min(|p|, |q|)$, 这里 $|p|$, $|q|$ 分别为 p, q 的二进制比特串长度.

这两个协议的非交互式证明是:

® 协议 1 表决数有效性证明协议[9]

协议 1 证明密文 c_i 对应的明文 m_i 一定来自集合 $\{m_{1_i} = m, m_{i2} = -m\}$, 其基本思想是证明者使得验证者相信他知道 $u = c_i / g^{m_i} = x_i^n \bmod n^2$ 的高阶 n 次剩余根 x_i. 由于高阶 n 次剩余的难解性, 从而验证者相信密文 c_i 对应的明文 m_i 一定来自集合 $\{m_{i1} = m, m_{i2} = -m\}$. 假设本次表决数是 $m_i = -m$, 类似可得到 $m_i = m$.

本文使用该协议的非交互式形式: 验证者和证明者共同的输入为 $u_1 = c_i / g^{m_i} = x_{i1}^n \bmod n^2$, $u_2 = c_i / g^{m_i} = x_{i2}^{m} \bmod n^2$. 证明者自己先计算承诺 (a_1, a_2, e_2, z_2), 其中 $r_1, z_2 \in_R Z_n^*$, $a_1 = E_k(0, r_1)$, $a_2 = E_k(0, z_2) u_2^{-e_2}$, e_2 是 $|e_2| = w_1$ 的随机数; 再计算验证者的挑战 $s = H(a_1, a_2, u_1, u_2)$; 最后根据挑战 S 以及 e_2 计算应答 $z_1 = r_1 x_{i1}^{e_1}$, 其中 $e_1 = s - e_2 \bmod 2^{w_1}$; 则 $proof_i = (a_1, a_2, s, e_1, e_2, z_1, z_2)$. 验证者可以首先根据输入 u_1, u_2 以及 $proof_i$ 中的 a_1, a_2, 用哈希函数 H 计算出挑战 $s = H(a_1, a_2, u_1, u_2)$; 然后判断 $s \stackrel{?}{=\!=} e_1 + e_2 \bmod 2^{w_1}$ 以及 $a_1 \stackrel{?}{=\!=} z_1^n u_1^{-e_1} \bmod n^2$ 以及 $a_2 \stackrel{?}{=\!=} z_2^n u_2^{-e_2} \bmod n^2$ 是否成立. 如果上述关系成立, 则接受; 否则, 拒绝.

® 协议 2　解密私钥分享正确性证明协议[9, 11, 12]

协议 2 证明解密密文 d_i 是对密文 c 用正确部分私钥 S_i 解密所产生的, 同时又不暴露部分私钥 S_i, 记 $u = c^{4l!} \bmod n^2$, $d_i^2 = \overline{c}^{s_i} = c^{4l! s_i} \bmod n^2$, 其基本思想是证明 $\log_u d_i^2 = s_i = \log_{\overline{v}} \overline{v}^{s_i}$.

本文同样使用该协议的非交互式形式: 证明者先计算承诺 (a, b), 其中 $r \in_R \{0, \cdots, 2^{w_2} - 1\}$, $w_2 = |n|$, $a = u^r \bmod n^2$, $b = v^r \bmod n^2$; 然后利用哈希函数计算挑战 $e = H(a, b, u, u', v, v')$, 其中 $u' = d_1^2$, $v' = \overline{v}^{s_i}$; 最后计算应答 $z = r + es_i$, $e \in_R \{0, \cdots, 2^{w_1 + w_2} - 1\}$; 则证明 $Proof_i = (e, z)$. 验证者可以通过验证 $e \stackrel{?}{=\!=} H(u^z u'^{-e}, v^z v'^{-e}, u, u', v, v')$ 是否成立来确定 d_i 是否有效.

5 证明与案例

5.1 证明与分析

本小节针对多机构商务合作的联合决策方案必须满足的三点需求逐一分析和证明.

定理 1 表决数的合法性与保密性可满足.

证明 通过执行 4.2 节的协议 1 两次: $(a_1, a_2, s, e_1, e_2, z_1, z_2)$, $(a_1, a_2, s', e'_1, e'_2, z'_1, z'_2)$, $s \neq s'$, 则每个证明副本中有下述关系成立:

$$E_k(0, z_1) = a_1 u_1^{e_1} \bmod n^2,\ E_k(0, z'_1) = a_1 u_1^{e'_1} \bmod n^2$$

进而有 $E_k(0, z_1/z'_1 \bmod n) = u_1^{e_1 - e'_1} \bmod n^2$. 由于 $e < 2^{w_1} < \min(p, q) < n$, 易知 $gcd(e_1 - e'_1, n^2) = 1$, 从而可以找到 λ_1, λ_2, 使得 $\lambda_1 n^2 + \lambda_2(e_1 - e'_1) = 1$ 成立.

令 $\bar{u}_1 = u_1 \bmod n$, $x = \bar{u}_1^{\lambda_1}(z_1/z'_1)^{\lambda_2} \bmod n$, 由于 $E_k(0, \bar{u}_1) = E_k(0, \bar{u}_1 \bmod n) = u_1^n \bmod n^2$, 于是有: $E_k(0, x) = E_k(0, \bar{u}_1)^{\lambda_1} \cdot E_k(0, z_1/z'_1)^{\lambda_2} = u_1^{\lambda_1 n} u_1^{\lambda_2(e_1 - e'_1)} = u_1^n \bmod n^2$. 同理可对 z_2, z'_2 做出说明. 那么验证者据此就可以计算出使得 $u_1 = E_k(0, x_{i1})$ (如果 $m_i = m$) 或者 $u_2 = E_k(0, x_{i2})$ (如果 $m_i = -m$) 的 x.

因为求高阶剩余根是难解的, 一个诚实验证者据此可确信: 密文 c_i 所对应的明文一定来自集合 $\{m_{i1} = m, m_{i2} = -m\}$. 故表决数的合法性可满足.

尽管表决数的集合大小仅为 2, 但由于表决数是通过概率加密 $c_i = g^{m_i} x_i^n \bmod n^2$ 后发送的, 无法从密文的比对中获取明文信息, 所以不会暴露 m_i.

定理 2 联合决策计算结果 $\sum m_i (1 \leqslant i \leqslant l)$ 的鲁棒性可得到满足.

证明 由于方案中采用了 (t, l) 门限密码技术, 按照 Shamir 秘密分享方案构造了 $t-1$ 次多项式对解密私钥 $SK = \beta\zeta$ 进行分享, 每个机构仅仅掌握各自的部分私钥 S_i, 所以独自无法完成对密文 c 的解密, 必须至少要有 t 个机构的协作;

下面证明从 t 个有效部分密文 d_i, 一定能恢复出密文 c 所对应的明文 $\sum m_i (1 \leqslant i \leqslant l)$.

根据 Lagrange 插值公式, 有:

$$l!\, f(0) = l!\, \beta\zeta = \sum_{i \in \Gamma} u_{0,i}^{\Gamma} f(x_i) \bmod n\zeta$$

于是:

$$c^{4(l!)^2\beta\zeta} = \prod_{i \in \Gamma} c^{4l!\, s u_{0,i}^{\Gamma}} = \prod_{i \in \Gamma} c_i^{2u_{0,i}^{\Gamma}} \bmod n^2$$

从而 $c^{4(l!)^2\beta\zeta} = g^{4(l!)^2\beta\zeta\sum m_i} = (1 + n)^{4(l!)^2\alpha\beta\zeta\sum m_i} b^{2n\beta\zeta 2(l!)^2\sum m_i} \bmod n^2$.

因为 p, q 是两个强大素数: $p = 2p' + 1$, $q = 2q' + 1$, 这里 p', q' 也均为素数, 所以 $\lambda(n) = lcm(p-1, q-1) = 2p'q' = 2\zeta$. 对于 $\forall b \in Z_{n^2}^*$, $b^{n\lambda(n)} = 1 \bmod n^2$[8], 故:

情况 1: 当 $\beta \in {}_R Z_n^*$ 为偶数时, 根据上式, 有: $b^{n\beta\zeta} = 1 \bmod n^2$, 所以 $(b^{2n\beta\zeta})^{2(l!)^2\sum m_i} = 1 \bmod n^2$;

情况 2: 当 $\beta \in {}_R Z_n^*$ 为奇数时, 有 $(b^{2n\beta\zeta}) = 1 \bmod n^2$, 同样有 $(b^{2n\beta\zeta})^{2(l!)^2\sum m_i} = 1 \bmod n^2$. 所以无论那种情况, $(b^{2n\beta\zeta})^{2(l!)^2\sum m_i} = 1 \bmod n^2$ 都成立, 故 $c^{4(l!)^2\beta\zeta} = (1+n)^{4(l!)^2\alpha\beta\zeta\sum m_i} \bmod n^2 = 1 + 4(l!)^2 n\alpha\beta\zeta\sum m_i \bmod n^2$

进而 $L(\prod_{j \in \Gamma} c_j^{2u_{0,j}^{\Gamma}} \bmod n^2) = 4(l!)^2\alpha\beta\zeta\sum m_i = \sum m_i \times 4(l!)^2\alpha\beta\zeta \bmod n = \sum m_i \times 4(l!)^2\theta \bmod n$. 由于 θ 是公钥的一部分, $l!$ 从而 $(l!)^2$ 是众所周知的, 故表决数之和 $\sum m_i$ 可恢复.

定理 3 联合决策结果 $\sum m_i (1 \leqslant i \leqslant l)$ 是可公开验证的.

证明 首先, 根据定理 1 的证明过程知道, 每个机构的表决数的合法性是可公开验证的;

其次, 根据 Paillier 公钥密码体制的同态性质, 有 $c = \prod c_i = g^{\sum m_i}(b \prod r_i)^n (1 \leqslant i \leqslant l)$. 从而可确保 c 就是联合决策结果 $\sum m_i (1 \leqslant i \leqslant l)$ 所对应的密文;

最后在协作解密的过程中, 根据协议 2, 每个部分解密的有效性同样是可公开验证的; 又由定理 2 可确保合成算法的正确性;

综上可知, 联合决策结果 $\sum m_i (1 \leqslant i \leqslant l)$ 是可公开验证的.

此外, 从文献[8]知道: 从密文恢复出明文等价于求解复合阶剩余类计算 Class[n] 困难问题, 所以对于攻击能力为多项式时间有界的窃听者, 表决数是不会暴露的.

5.2 方案应用

本节以文章开头所提出的三个机构之间的商务合作为例, 说明联合决策过程的安全性和有效性. 假定他们按照所持有股权的比例, 共同商议确定了如下配置:

假定三家机构就所研究的药物的专利转让产生了分歧, 需要进行联合决策. 其中, 基因公司和医院同意转让, 而药厂拒绝转让. 他们按照方案所规定的步骤进行如下表决和决策:

表 1 面向有差异群体的商务合作配置表

机构名称	持股比例	元权限值	表决数集合	部分私钥	决策门限 (k, s)	解密门限 (t, l)
基因公司	29%	7	$\{7, -7\}$	S_1	$(12, 24)$ 注: $s = 24 = 7 + 11 + 6$, 为本次决策每个机构所持有的同质元权限之和.	$(2, 3)$
药厂	45%	11	$\{11, -11\}$	S_2		
医院	25%	6	$\{6, -6\}$	S_3		

(1) 基因公司加密自己的表决数 $c_1 = E_k(7, x_1)$, 并附上表决数的有效性证明 $proof_1 = (a_{11}, a_{12}, b_1, e_{11}, e_{12}, z_{11}, z_{12})$;

药厂加密自己的表决数 $c_2 = E_k(-11, x_2)$, 并附上表决数的有效性证明 $proof_2 = (a_{21}, a_{22}, b_2, e_{21}, e_{22}, z_{21}, z_{22})$;

医院加密自己的表决数 $c_3 = E_k(6, x_2)$, 并附上表决数的有效性证明 $proof_3 = (a_{31}, a_{32}, b_3, e_{31}, e_{32}, z_{31}, e_{32})$;

(2) 互相广播自己表决的加密 c_i 以及表决数的有效性证明 $proof_i = (a_{i1}, a_{i2}, b_i, e_{i1}, e_{i2}, z_{i1}, z_{i2})$, 这里 $1 \leqslant i \leqslant 3$; 各自计算出 $\sum m_i (1 \leqslant i \leqslant 3)$ 对应的密文 $c = \prod c_i (1 \leqslant i \leqslant 3)$;

(3) 比较各自计算的密文 $c = \prod c_i (1 \leqslant i \leqslant 3)$ 是否相等; 如果相等则利用各自的私钥 S_i 产生 c 所对应的部分解密 $d_i (1 \leqslant i \leqslant 3)$, 并根据协议 2 附上各自部分解密有效性的证明 $Proof_i(e_i, z_i) (1 \leqslant i \leqslant 3)$, 广播出去:

基因公司的部分解密 $d_1 = D_{s_1}(c)$; $proof_1(e_1, z_1)$;

药厂的部分解密 $d_2 = D_{s_2}(c); prof_2(e_2, z_2);$

医院的部分解密 $d_3 = D_{s_3}(c); prof_3(e_3, z_3);$

(4) 每个机构首先验证部分解密的有效性, 在确信持有两个有效部分解密的基础上, 可以通过运行结合算法而获得明文 $\sum m_i (1 \leqslant i \leqslant 3) = 2$. 由于表决数之和 2 小于决策门限 12, 所以本次表决不通过.

6 结论

公平性、透明性是联合决策的基本安全需求. 本文结合多机构商务合作背景, 介绍了面向群体联合决策的基本概念, 研究了面向有差异群体的联合决策策略与方案. 方案包括三部分: 刻画有差异实体的权限表达体制实现了权限大小和股权多少的对等; 可公开验证的多方计算技术保证以透明、公正的方式来计算最终决策结果; 采用门限技术判定最终决策是否有效保证了其他合作方对联合决策的知情权和监督权.

附录　关于文中参数选择的有关证明

命题 1　$n = pq$, p 与 q 是两个强大素数, 其中 $p = 2p' + 1$, $q = 2q' + 1$, $\zeta = p'q'$, $gcd(n, \varphi(n)) = 1$, 随机选择 $(a, b) \in_R Z_n^* \times Z_n^*$, 设 b 在 Z_n^* 中的阶为 α, 令 $g = (1 + n)^a b^n \bmod n^2$, 则 g 在 $Z_{n^2}^*$ 中的阶为 $n\alpha$.

证明: 因为 $a \in Z_n^*$, 故 $gcd(a, n) = 1$, 那么 a 在 Z_n^* 上的阶为 $ord(a) = n$; $b \in Z_n^*$, 根据欧拉定理, 有 $b^{\varphi(n)} = 1 \bmod n$, 因为 b 在 Z_n^* 中的阶为 α, 所以必有 $\alpha \mid \varphi(n)$. 又因为 $gcd(n, \varphi(n)) = 1$, 所以 $gcd(n, \alpha) = 1$, 进而 $lcm(n, \alpha) = n\alpha$. 又易知 $Z_n \times Z_n^* \cong Z_{n^2}^*$, 而 $a \in Z_n^* \subset Z_n$, 所以 $ord[(a, b)] = n\alpha$, 即 g 在 $Z_{n^2}^*$ 中的阶就是 $n\alpha$.

命题 2　条件同命题 1, 则 $Z_{n^2}^*$ 中平方数所组成的集合 g 是阶为 $n\zeta$ 的循环群.

证明: 容易证明 $Z_{n^2}^*$ 中平方数所组成的集合 G 为群;

下面证明 $Z_{n^2}^*$ 中平方数的个数为 $n\zeta$.

根据文献[14](190 页定理 1): Z_p 中有个 $\frac{p-1}{2}$ 平方数. 我们有 $Z_{p^2}^*$ 中有 $\frac{p(p-1)}{2}$ 个平方数, 因为从 1 到 p^2 的自然数中, 除去 $p, 2p, \cdots, (p-1)p$ 这 $p-1$ 个数外, 其余的 $p^2 - (p-1) = p(p-1)$ 个数都与 p^2 互素; 又因为这 $p(p-1)$ 个数中, 有: $I^2 = (-1)^2 \bmod p^2$, $2^2 = (-2)^2 \bmod p^2$, $\cdots$, $\left(\frac{p(p-1)}{2}\right)^2 = \left(-\frac{p(p-1)}{2}\right)^2 \bmod p^2$, 即这 $p(p-1)$ 个数中, 有 $\frac{p(p-1)}{2}$ 个是平方数. 做 $Z_{n^2}^* \alpha Z_{p^2}^* \times Z_{q^2}^*$ 上的映射 $f(x) = (x \bmod p^2, x \bmod q^2)$, 易知 $f(x)$ 是 $Z_{n^2}^* \mapsto Z_{p^2}^* \times Z_{q^2}^*$ 上的满同态, 且 $Ker(f) = \{1\}$, 根据同态基本定理, 有 $Z_{n^2}^* \cong Z_{p^2}^* \times Z_{q^2}^*$.

所以如果 x 是 $Z_{n^2}^*$ 的平方数, 则 $(x \bmod p^2) \times (x \bmod q^2)$ 分别对应的就是 $Z_{p^2}^* \times Z_{q^2}^*$ 的平方数, 它们之间一一对应. 又因为 $Z_{p^2}^* \times Z_{q^2}^*$ 中的平方数为 $\frac{p(p-1)}{2} \times \frac{q(q-1)}{2} = pqp'q' = n\zeta$ 个平方数, 所以 $Z_{n^2}^*$ 中的平方数的个数为 $n\zeta$ 个, 即群 G 的阶为 $|G| = n\zeta$.

最后证明群 G 为循环群:

令 G_1 表示 $Z_{p^2}^*$ 中平方数所组成的集合, G_2 表示 $Z_{q^2}^*$ 中平方数所组成的集合. 因为 $Z_{p^2}^*$ 和 $Z_{q^2}^*$ 都是循环群[14], 所以 G_1 和 G_2 也都是循环群, 做 $G \mapsto G_1 \times G_2$ 上的映射:

$\varphi(x) = (x \bmod p^2, x \bmod q^2)$, 易知 $\varphi(x)$ 是 $\mapsto G_1 \times G_2$ 上的同构, 所以是 G 循环群.

参考文献:

[1] Khurana H. Negotiation and management of coalition resources[D]. USA: University of Maryland, 2002.

[2] Khurana H, Gligor V, Linn J. Reasoning about joint administration of access policies for coalition resources[A]. Amin Tjoa Eds. Proceedings of the International Conference for Distributed Computer Systems - ICDCS[C]. New York: IEEE Press, July 2002. 429- 452.

[3] Y Desmedt. Society and group oriented cryptography: a new concept [A]. C Pomerance Eds Advance in Cryptology - Crypto '87[C], Berlin: Springer-Verlag, 1988, Volume 293 of LNCS, 120- 127.

[4] Yvo Desmedt, Yair Frankel. Threshold Cryptosystems[A]. G Brassard Eds. Advance in Cryptology? Crypto' 89[C]. Berlin: Springer-Verlag, 1989, Volume 435 of LNCS, 305- 315.

[5] T Wang. Cryptosystem for group oriented cryptography[A]. I B Damgard Eds. Advances in Cryptology-Eurocrypt' 90[C]. Berlin: Springer-Verlag, 1990. Volume 473 of LNCS, 352- 360.

[6] W P Ma, M H Lee. Group Oriented Cryptosystems Based on Linear Access Structures[A]. J I Lim, D H Lee Eds. Information Security and Cryptology-ICISC 2003[C]. Berlin: Springer-Verlag, 2004. Volume 2971 of LNCS, 370- 376.

[7] 雷浩, 冯登国, 周永彬, 黄建. 基于量化权限的门限访问控制方案[J]. 软件学报, 2004, 15(11): 1680- 1688.

[8] Paillier P. Public-Key cryptosystems based on composite degree residuosity classes[A]. J Stern Eds. Eurocrypt' 99[C]. Berlin: Springer Verlag 1999. Volume 1592 of LNCS, 223- 238.

[9] Damgård I, Jurik M. A generalization, a Simplification and Some Applications of Paillier's Probabilistic Public-Key System[A]. K Kim Eds. PKC2001[C]. Berlin: Springer Verlag, 2001, Volume 1992 of LNCS, 119- 136.

[10] Damgård I, and Koprowski M. Practical threshold RSA signatures without a trusted dealer[A]. B Pfitzmann Eds. Advances in Cryptology-Eurocrypt2001 [C]. Berlin: Springer-Verlag, 2001, Volume 2045 of LNCS, 152- 165.

[11] Fouque PA, Poupard G, Stern J. Sharing decryption in the context of voting or lotteries[A]. Y Frankel Eds. Financial Crypto '00[C]. Berlin: Springer-Verlag, 2000, Volume 1962 of LNCS, 90- 104.

[12] Baudron O, Fouque PA, Pointcheval D. Practical Multi-Candidate Election System[A]. N Shavit Eds. Proc of the ACM Symposium on Principles of Distributed Computing[C]. New York: ACM Press, 2001. 274- 283.

[13] Amos Fiat, Adi Shamir. How to prove yourself: practical solutions of identification and signature problems[A]. A M Odlyzko Eds. Advances in Cryptology-Crypto '86[C]. Berlin: Springer-Verlag, 1987, Volume 263 of LNCS, 186- 194.

[14] 潘承洞, 潘承彪著. 初等数论[M]. 北京: 北京大学出版社, 1994. 190- 191, 241- 242.

作者简介:

雷 浩 男, 1975 年出生于陕西合阳, 博士研究生, 主要研究方向为系统安全体系结构与信息安全技术. E-mail: leiyok@is.iseas.ac.cn.

冯登国 男, 1965 年出生于陕西靖边, 研究员, 博士生导师, 主要研究领域为密码学、信息安全.

张振锋 男, 1972 年出生于河南南阳, 副研究员, 博士, 主要研究方向为密码学、信息安全理论与技术.

周永彬 男, 1973 年出生于山东阳信, 博士, 主要研究领域为应用密码学、网络与信息安全理论与技术.