# P2P环境下的具有隐私保护的信誉协议

孙 波[1] 丁雪峰[2] 司成祥[1] 张 伟[1]
(国家计算机网络应急技术处理协调中心 北京 100029)[1] (四川大学信息管理中心 成都 610065)[2]

**摘 要** 信誉协议通过计算系统用户的信誉评价结果的总合得到最后的信誉结果,然后根据该信誉结果做出相应的决策。在现实情况中信誉系统中的用户往往会反馈一个不诚实的信誉值,因为他们担心他们真实的评价结果会遭到对手的报复。提出一个具有隐私保护的信誉协议,该协议能保证某实体得到其他实体诚实公平的信誉评价。在该协议中使用Shamir门限密钥共享为参与者提供共享子密钥,并利用具有同态性质的可验证密钥共享使得交易员和密钥持有者之间能够验证共享子密钥的正确性。协议中持有共享子密钥的参与者是随机选择的。运用语义安全的ElGamal密码系统和Cramer Shoup密码系统,共享密钥的持有者可以以隐私保护的方法提交他们的信誉值,并由一个可信的代理计算信誉结果提交给信誉引擎。用户可通过访问信誉引擎获得信誉结果。该协议保证了信誉结果计算过程中的隐私保护性和信誉结果的可靠性。

**关键词** ElGamal密码系统,Cramer-Shoup密码系统,Shamir门限密钥共享,同态加密,信誉系统
**中图法分类号** TP918.1 **文献标识码** A

## Privacy Preserving Reputation Protocol for P2P Environment

SUN Bo[1] DING Xue-feng[2] SI Cheng-xiang[1] ZHANG Wei[1]
(National Computer Network Emergency Response Technical Team Coordination Center of China, Beijing 100029, China)[1]
(Information Management Center, Sichuan University, Chengdu 610065, China)[2]

**Abstract** Reputation protocol is used to compute feedback by summing up the individual reputations of other system users. The feedback is then used to make a decision. It is always the case that the entities in a reputation system will provide dishonest feedback due to fear of exposing their privacy which would lead to retaliatory acts from opponents. In this paper, a privacy preserving reputation protocol enable an entity to acquire fair reputation from other entities. In this protocol Shamir Secret Sharing and Verifiable Secret Sharing with homomorphic property are employed to enable the dealer and secret holders to verify the correctness of the shared secret. Moreover a random selection of the participating secret holders is achieved. And using the shared secret key, the secret reputation feedback is attained by decryption. Further more, the nice privacy preserving properties of the semantically secure ElGamal and Cramer Shoup Cryptosystem are used to enable the secret holders to submit their secret reputation feedback in a privacy preserving way and securely access a database of current reputation feedback maintained by a reputation engine.

**Keywords** ElGamal cryptosystem, Cramer-Shoup cryptosystem, Shamir threhold secret sharing, Homomorphic encryption, Reputation system

## 1 引言

信誉系统为服务供应者、服务、商品或其它实体计算并发布信誉值。信誉系统的这种服务已经受到大家越来越多的欢迎。其中最为著名的信誉系统是eBay信誉系统(ebay.com),它用来抑制电子商务中的欺骗行为。其他著名的信誉系统包括EigenTrust信誉系统[1]和PeerTrust信誉系统[2]。

分布式的信誉系统不以集中方式收集和发布信誉值[3]。在分布式信誉系统中,参与者互相提供信誉值并以此评估潜在的交易伙伴的可信度。每个参与者在本地生成他们对某实体的信誉评价并在需要时反馈给系统。

只有在安全反馈时,信誉值才是精确的。然而,我们发现信誉系统的用户因为害怕遭到被评价者的报复或者觉得互相给予好的评价能得到对方的回报等因素,往往不会提供诚实的信誉值[4]。这类情况在分布式系统中一样会出现。在信誉系统中,参与方希望自己提供的信誉值不会被恶意的参与方获得并在将来对他们造成负面的影响。如果参与者的信誉评价值被某些不诚实的参与者获得,他们可能报复或者报答评价者。

解决这类问题的方法是在信誉系统中计算信誉值时能提

本文受四川省科技支撑计划项目(2012GZ0001),上海市科学技术委员会基金项目(11511505300)资助。
孙 波(1973-),男,博士,教授,主要研究方向为网络与信息安全,E-mail:xjf@mail.nisac.gov.cn;丁雪峰(1974-),男,博士,讲师,主要研究方向为计算机网络,E-mail:dingxf@scu.edu.cn(通信作者);司成祥(1982-),男,博士,工程师,主要研究方向为网络与信息安全;张 伟(1985-),男,博士,工程师,主要研究方向为网络与信息安全。

供隐私保护机制。在隐私保护协议中，计算信誉值时信誉值提供者的信誉评价不会被暴露，也不会有相应的后果。因此参与者将愿意提供诚实的信誉评价。

本文提出了一个分布式环境下的隐私保护信誉协议。在协议中，在该协议中使用 Shamir 门限密钥共享[5]为参与者提供共享子密钥，并利用具有同态性质的可验证密钥共享使得经营者和密钥持有者之间能够验证共享子密钥的正确性。协议中持有共享子密钥的参与者是随机选择的。运用语义安全的 ElGamal 密码系统和 Cramer Shoup 密码系统，共享密钥的持有者可以以隐私保护的方法提交他们的信誉值，并由一个可信的代理计算信誉结果提交给信誉引擎。用户可通过访问信誉引擎获得信誉结果。该协议保证信誉结果计算过程中的隐私保护性和信誉结果的可靠性，其在半可信参与者和恶意参与者的敌手模型下都是安全的。

本文第 2 节给出一些相关的预备知识；第 3 节介绍了设计该协议的基础条件；第 4 节提出隐私保护信誉协议，详细介绍协议的各个阶段；第 5 节讨论敌手模型下协议的安全性；最后讨论后期的研究工作。

## 2 预备知识

这部分给出协议设计的基础知识。

### 2.1 门限密钥共享方案

在门限密钥共享方案中，秘密 $S$ 被分割成 $n$ 份，即 $S_1$，$S_2$，$S_3$，…，$S_n$，然后将它们分发给 $n$ 个秘密共享者，门限值为 $t$，任意 $t$ 个或更多个秘密共享者可恢复出密钥 $S$，而任意$\leqslant t-1$ 个秘密共享者则无法恢复密钥。这个方案被称为$(t,n)$-门限秘密共享方案。Shamir 提出了一个门限秘密共享方案[5]，在他的方案中假设交易员和秘密共享者都是诚实的。但在实际情况中，不诚实或恶意的交易员和秘密共享者是很常见的。为了阻止这些参与者的恶意行为，我们需要可验证的秘密共享方案，这类方案最初是由 BennyChor[6] 提出的。在可验证秘密共享方案中，由交易员给每个秘密共享者分配子秘密，秘密共享者可验证其获得的子秘密的正确性，但不能获得秘密 $S$ 的任何信息。

### 2.2 语义安全的 ElGamal 加密方案[7]

1. 初始化

系统初始化方法如下：

(1)随机选取一个素数 $q$，其长度$|q|=k$；

(2)测试 $p=2q+1$ 的素性，如果 $p$ 不是素数，返回第(1)步；

(3)随机选取一个生成元 $h=Z_p^*$，并设置 $g=h^2 mod p$；

(4)令交换群 $G$ 满足 $G=\langle g\rangle$；

(5)令$(p,g)$是公开参数，$G$ 为明文空间；

(6)选取随机数 $x\in Z_{p-1}$为私钥。

(7)计算 $y=g^x \bmod p$，设置$(p,g,y)$为公钥；

2. 加密

发送者选取 $K\in Z_{p-1}$并计算 $m$ 的密文$(c_1,c_2)$，方法如下：

$c_1=g^K \bmod p$

$c_2=y^K m \bmod p$

3. 解密

接收者按下列方法解密密文$(c_1,c_2)$：

$m=\frac{c_2}{c_1^x}(\bmod p)$

### 2.3 Cramer-Shoup 公钥加密系统

一个著名的可证明 IND-CCA2 安全的和实用高效的公钥加密系统是 Cramer-Shoup 公钥加密系统。其构造方法如下。

1. 初始化

令 $G$ 为 $q$ 阶交换群，明文空间为 $G$。用户可以按下列方法建立密钥参数：

(1)选择两个随机数 $g_1,g_2\in_U G$；

(2)选取 5 个随机整数 $x_1,x_2,y_1,y_2,z\in_U[0,q)$；

(3)计算 $c=g_1^{x_1}g_2^{x_2}$，$d=g_1^{y_1}g_2^{y_2}$，$h=g_1^z$；

(4)选取一个 hash 函数 $H:G^3\to[0,q)$；

(5)设置$(g_1,g_2,c,d,h,H)$为公钥，$(x_1,x_2,y_1,y_2,z)$为私钥。

2. 加密

为了加密消息 $m\in G$，发送者随机选择一个整数 $r\in_U[0,q)$，并计算 $u_1=g_1^r$，$u_2=g_2^r$，$e=h^r m$，$\alpha=H(u_1,u_2,e)$，$v=c^r d^{r\alpha}$。密文为$(u_1,u_2,e,v)$。

3. 解密

为解密密文$(u_1,u_2,e,v)$，接收者做如下计算：

(1)$\alpha=H(u_1,u_2,e)$；

(2)输出$\begin{cases} m=e/u_1^z, & \text{如果 } u_1^{x_1+y_1\alpha}u_2^{x_1+y_1\alpha} \\ \text{拒绝}, & \text{其他} \end{cases}$。

在通过数据完整性验证后，加密的后续步骤同语义安全的 ElGamal 加密方案。其中数据完整性验证能阻止任何试图不按照算法的加密步骤构造密文的行为。

### 2.4 同态加密

同态加密是指一种加密算法能使得对密文做任意的代数运算等价于对相应的明文做对应的代数运算。

1. ElGamal 加密系统的乘同态

在 ElGamal 加密系统中，公钥为$(G,q,g,h)$，其中 $h=g^x$，私钥为 $x$。对消息 $m$ 加密后密文为 $E(m)=(g^r,h^r m)$，其中 $r\in[0,q)$。其同态性质表示如下：

$$\begin{aligned} E(x_1)\cdot E(x_2)&=(g^{r_1},h^{r_1}x_1)\cdot(g^{r_2},h^{r_2}x_2)\\ &=(g^{r_1+r_2},h^{r_1+r_2}(x_1\cdot x_2))\\ &=E(x_1,x_2)\end{aligned}$$

2. Shamir 门限秘密共享方案的同态性

在$(t,n)$-秘密共享方案中，$F_I$ 是由 $t$ 个或更多个子秘密中计算出秘密 $S$ 的函数，其中 $I\subseteq\{1,2,\cdots,n\}$且$|I|\geqslant t$，$t$ 为预先设置的门限值：

$S=F_I(S_1,S_2,\cdots,S_t)$

令$\oplus$和$\otimes$是两个定义在秘密和它的子秘密空间的元素上的二元运算。如果$(t,n)$-秘密共享方案对于所有的 $I$ 满足$(\oplus,\otimes)$-同态性质，则当

$S=F_I(S_1,S_2,\cdots,S_t)$和 $S'=F_I(S_1',S_2',\cdots,S_t')$

可很容易地计算

$S\oplus S'=F_I(S_1\otimes S_1',S_2\otimes S_2',\cdots,S_t\otimes S_t')$

Shamir 基于多项式的$(t,n)$-门限秘密共享方案是$(+,+)$-同态的，即满足

$S+S'=F_I(S_1+S_1',S_2+S_2',\cdots,S_t+S_t')$

## 3 协议的设计基础

在描述信誉协议之前，我们先列出协议设计的一些基础。

### 3.1 初始条件

设计协议时假设以下条件成立：

1. 指定交易员是可以被腐化的，也就是他们是不可信的。

2. 诚实的参与者(秘密共享者)想恢复出秘密，即使敌手已经腐化了指定交易员和一些秘密共享者。

3. 敌手的主要攻击目标是阻止秘密共享者重新构造秘密值，进而阻碍协议的正确执行。

4. 恶意秘密共享者可能试图得到其他秘密共享者的子秘密或者腐化交易员。

### 3.2 敌手模型

1. 半可信的秘密共享者

半可信的秘密共享者是遵守协议执行的参与者，然而他们往往好奇其他参与者的秘密值。他们可能通过分析在协议执行过程中获得的中间信息或者通过其他合法手段获得的信息来分析计算其他参与者的共享子秘密。半可信参与者更有可能共谋以达到目的。

2. 恶意秘密共享者

恶意秘密共享者不一定会遵守协议的执行，他们可能在参与其他的协议，设计复杂的攻击策略，共谋攻击以得到其他参与者的共享子秘密。他们的目标包括得到对其他参与者的非法控制权，造成其他秘密共享者无法正常使用信誉系统。

### 3.3 设计特征

1. 我们设计的协议运行在 P2P 网络环境中。在实际实施中包含两层网络，描述如下：

(1)在上一层网络架构上包含了用于监视、计算和提供私有保护的超级节点。

(2)在下一层网络构架包括所有的普通节点，包括半可信节点和恶意节点。

2. 具有同态性质的 Shamir 门限秘密共享方案将被用于实现以下目标：

(1)在特定的会话中随机选取秘密共享者来得到反馈的信誉值 。

(2)信誉反馈请求以密文形式发送给秘密共享者，只有合法的秘密共享者才可以解密并得到请求内容。

(3)利用 Shamir 门限秘密共享方案的同态性质，指定交易员和秘密共享者都能验证其子秘密是否正确。

3. 语义安全的 ElGamal 密码系统被用于秘密共享者(普通节点)和指定交易员(超级节点)之间的通信中，实现安全通信和隐私保护。

4. 运用 CCA2-安全的 Cramer-Shoup 密码系统，指定交易员可以安全成功地计算总的信誉值。

## 4 具有隐私保护的信誉协议

### 4.1 系统建立阶段

一群秘密共享者选举他们最信任的第三方为指定交易员(DD)，并选择一个后备的指定交易员(BDD)以备 DD 不可用时代替 DD 工作。

为了使用语义安全的 ElGamal 密码系统 $\varepsilon$，DD 将选择 $p$ 和 $g$ 作为公钥。DD 选取私钥 $x$，并计算公钥 $X$。然后公布公钥$(p,g,X)$，私钥 $x$ 保密。

DD 和秘密共享者共同建立 Cramer-Shoup 密码系统$\mathbb{E}$。公钥为$(g_1,g_2,c,d,h,H)$，DD 保管好私钥$(x_1,x_2,y_1,y_2,z)$。

### 4.2 生成共享子秘密及分配信誉阶段

在这个阶段，输入秘密 $S\in GF(p)$和一个公开 hash 函数，输出 $S$ 的共享子秘密 $S_i$，其中 $i=1,2,3,\cdots,n$。步骤如下：

1. DD 选择一个大素数 $p>\max(S,n)$。

2. DD 选取 $t-1$ 个随机独立系数 $a_1,a_2,\cdots,a_{t-1}$，其中 $0\leqslant a_i\leqslant p-1$。

3. 产生随机多项式 $f(u)=a_0+a_1u+a_2u^2+\cdots+a_{t-1}u^{t-1}$，并设置 $a_0=S$。

4. 计算每一个参与者的共享子秘密并分配给每个参与者共享子秘密$(i,S_i)$，其中 $S_i=f(i)$，$1\leqslant i\leqslant n$。

5. DD 计算所有共享子秘密的 hash 值 $H(S_i)$，其中 $1\leqslant i\leqslant n$。

6. DD 利用同态加密方案加密多项式的 $t$ 个系数 $a_0,a_1,\cdots,a_t$，然后广播所有系数的密文 $E(a_0),E(a_1),\cdots,E(a_{t-1})$和秘密的 hash 值 $H(S)$。

7. DD 利用密钥 $S$ 加密信誉反馈请求，并发送给共享者，因此只有能恢复秘密的共享者才能解密得到信誉反馈请求。

8. DD 管理一个保存所有共享子秘密 hash 值以及秘密 $S$ 的 hash 值的公开文件。

9. 在收到请求后，秘密共享者首先验证其子秘密是否正确：

秘密共享者利用相同的 hash 函数计算出 $H(S_i)$，然后与公开文件中对应的 hash 值比较，若相同，则利用加法和乘法同态性计算并比较下列等式：

$$E(f(i))=E(a_0)\oplus(E(a_1)\otimes E(i^1))\oplus\cdots\oplus(E(a_{t-1})\otimes E(i^{t-1}))$$

若上面的等式成立，则密钥共享者接受其子秘密是正确的。

10. 若所有秘密共享者的子秘密是正确的，则交易阶段结束。DD 安全地销毁 $S,a_1,a_2,\cdots,a_{t-1}$和私钥 $x$。

11. 若对于第 $i$ 个秘密共享者发现其子秘密是错误的，则他公开指控 DD，其他诚实的秘密共享者可以判断是 DD 还是指控者作弊。

### 4.3 信誉反馈阶段

1. 令子秘密 $S_i$，$i\subseteq\{1,2,\cdots,n\}$且$|i|\geqslant t$是由所有秘密共享者恢复的子秘密。每一个秘密共享者都需要恢复并验证其子秘密，最后恢复出秘密 $S$，并利用秘密 $S$ 解密得到信誉反馈请求。然后每个秘密共享者准备其秘密的信誉值(在此，如果信誉值是正的，则 $t_i=1$，如果信誉值是负的，则 $t_i=0$)。

2. New York：Springer-Verlag，2001：第 $i$ 个秘密共享者利用公钥为$(p,g,X)$的 ElGamal 密码体制加密他的信誉反馈 $m_i=2^{t_i}$后得到$\varepsilon(2^{t_i})$。

3. 第 $i$ 个秘密共享者利用 DD 的公钥$(g_1,g_2,c,d,h,H)$加密他的子秘密 $f(i)$和信誉反馈密文 $\varepsilon(2^{t_i})$，得到$\mathbb{E}(f(i)\parallel\varepsilon(2^{t_i}))$，然后将此密文发送给 DD。

### 4.4 秘密与信誉重建阶段

在这个阶段，输入子秘密 $S_i$，$i\subseteq\{1,2,3,\cdots,n\}$且$|i|\geqslant t$，

(下转第 371 页)

准确性也将是今后长期研究的课题。

## 参 考 文 献


[1] 王然风. 基于支持向量回归技术的大型复杂机电设备故障诊断研究与应用[D]. 太原:太原理工大学,2005

[2] Puggina N, Venturini M. Development of a Statistical Methodology for Gas Turbine Prognostics [J]. Journal of Engineering for Gas Turbines and Power,2012,134

[3] Luo Hua-geng,Ghanime G,Wang Li-ping. Arma Model for Turbine and Compressor Clearance Forecasting[C]//Proceedings of ASME Turbo Expo 2010:Power for Land,Sea and Air GT2010. Glasgow,UK,June 2010:14-18

[4] 吴庚申,梁平,龙新峰,等. 基于 ARMA 的汽轮机转子振动故障序列的预测[J]. 华南理工大学学报:自然科学版,2005,33(7):67-73

[5] Vapnik V. The Nature of Statistical Learning Theory [M]. New York:Springer,1995

[6] Song Zhao-qing,Cui He,Hu Yu-nan. Research and Development of Support Vector Machine Theory[J]. Journal of Naval Aeronautical and Astronautical University,2008,23:143-148

[7] 顾亚祥,丁世飞. 支持向量机研究进展[J]. 计算机科学,2011,38(2):14-17

[8] 朱大奇,史慧. 人工神经网络原理及应用[M]. 北京:科学出版社,2006


(上接第 336 页)

以及 hash 函数,重建秘密 $S$ 和信誉值。

1. 首先,DD 利用其私钥$(x_1,x_2,y_1,y_2,z)$解密密文$\mathbb{E}(f(i)\|\epsilon(2^{t_i}))$,恢复出信誉反馈值 $\epsilon(2^{t_i})$和所有的子秘密 $f(i)$(注意到在 Cramer-Shoup 加密方案中,子秘密 $f(i)$的完整性得到保证)。

2. DD 通过计算和比较每个子秘密的 hash 码来验证其正确性。

3. 若有 $t$ 或超过 $t$ 个子秘密可用,则 DD 可利用 Shamir 门限秘密共享方法计算并恢复出多项式 $f(u)$和秘密 $S=a_0$。

4. DD 通过计算和比较秘密 $S$ 的 hash 值来验证其正确性。然后 DD 可确信信誉反馈密文 $\epsilon(2^{t_i})(i\subseteq[1,n])$ 来自于诚实的秘密共享者。

### 4.5 信誉计算阶段

DD 在收到信誉反馈密文 $\epsilon(2^{t_i})(i\in[1,n])$后,运用 ElGamal 密码系统的乘法同态性做如下计算:

首先 DD 将所有的信誉反馈密文相乘得到

$$\epsilon(2^{t_1})\cdot\epsilon(2^{t_2})\cdot\cdots\cdot\epsilon(2^{t_n})$$

利用 ElGamal 密码系统的乘法同态性可计算

$$\epsilon(2^{t_1})\cdot\epsilon(2^{t_2})\cdot\cdots\cdot\epsilon(2^{t_n})=\epsilon(2^{t_1}\cdot 2^{t_2}\cdot\cdots\cdot 2^{t_n})=\epsilon(2^{t_1+t_2+\cdots+t_n})$$

结果中的指数 $2^{t_1+t_2+\cdots+t_n}$ 是总的信誉反馈值。DD 解密得到这个总信誉反馈值,然后发送给信誉引擎。

信誉引擎保存此信誉反馈的记录,并设置一个过期的时间节点,然后公布此信誉反馈值以及发布时间。任何需要信誉系统服务的人都可以从信誉引擎中获得信誉反馈值、发布时间和过期时间。

## 5 安全性分析

隐私保护的信誉协议里具有半可信参与者和恶意参与者。

半可信参与者能正确遵照协议执行,其目标是获得其他参与者的信誉反馈值,他们可能共谋以达到目标。在我们的协议中,所有的信誉反馈都是密文传输的,而且必须有 $t$ 个或更多个参与者才能恢复出秘密 $S$ 和信誉反馈,而这 $t$ 个参与者是从 $n$ 个参与者中随机选取的。这种随机选取法使得半可信参与者很难利用共谋攻击达到目标,并且每个参与者的信誉反馈是加密的,不知道 DD 的私钥,则无法恢复出这些信誉反馈。因此,对于半可信参与者,我们的信誉协议能够保护每个参与者的隐私。

恶意参与者不一定遵守协议的执行,可能根据自己的需要做一些偏离协议的行为,他们可能设计复杂的攻击策略,或者与其他参与者共谋以达到攻击目标。他们的目标包括获得其他参与者的本地信誉反馈,获得对其他参与者的控制权。

在我们的协议中,秘密 $S$ 及其共享子秘密的 hash 值是可验证的。在计算信誉反馈前,DD 通过验证这些 hash 值的正确性来确保参与者遵守协议的执行。一旦发现有恶意的参与者,协议就不会继续向下执行。因此也杜绝了恶意参与者参与协议。

因此我们的隐私保护信誉协议对于半可信参与者和恶意参与者都是安全的。

**结束语** 本文提出了一个能以隐私保护方式产生信誉反馈值的信誉协议。在我们的隐私保护信誉协议中,信誉反馈请求以密文的方式发送。在信誉反馈时,参与者的隐私得到保护,不诚实的参与者也能被发现。因此诚实的参与者能够提供他们的真实信誉反馈,最后得到一个真实的总信誉反馈值 。通过分析得到,我们的隐私保护信誉协议对于半可信参与者和恶意参与者都是安全的。

## 参 考 文 献


[1] Kamvar S D,Schlosser M T,GarciaMolina H. The enginetrust algorithm for reputation manegement in P2P networks[C]// Proc. of 12th Intl. Conf. on World Wide Web(WWW2003). New york:Springer-Verlag,2003:344-51

[2] Xiong L, Liu L. Supporting reputation-based trust in peer-tp-peer communities[J]. IEEE transaction on knowledge and data engineering,2004,12(7):843-857

[3] Pederson T. Non-interactive and information secure verifiable secret sharing[C]// Proc. of Advances in Cryptology-Crypto'91. New york:Springer-Verlag,1991:129-140

[4] Resnick P, Zeckhauser R. Trust among strangers in internet transactions[J]. The economics of the internet and e-commerce, 2002,11:127-157

[5] Shamir A. How to share a secret[C]//Communications of ACM 22,1979. New york:Springer-Verlag,1979:612-613

[6] Chor B, Goldwasser S, Micali S, et al. verifiable secret sharingand achieving simultaneity in the presence of faults[C]//Proc. of the 26th Annual symposium on foundation of computer science, 1985. New york:Springer-Verlag,1985:383-395

[7] Mao Wen-bo. Modern cryptography:Theory and Practice[M]. Prentice Hall PTR,2003:514-590