第 42 卷　第 2 期　　计　算　机　工　程　　2016 年 2 月
Vol. 42　No. 2　　Computer Engineering　　February 2016

·安全技术·　　文章编号：1000-3428(2016)02-0137-05　　文献标识码：A　　中图分类号：TP309.2

基于承签原语与多重签名的改进虚拟交易系统方案

张　泓[1]，曹珍富[1,2]，董晓蕾[1,2]

（1. 上海交通大学计算机科学与工程系，上海 200240；
2. 华东师范大学计算机科学与软件工程学院，上海 200062）

摘　要：四方参与者虚拟交易系统(4P_VES)在引入第三方支付检测和预防合谋欺骗行为后会增加系统交互流程，影响系统性能。为此，通过融合承诺与签名原语定义承签方案，提出改进的 4P_VES 方案。采用承签方案同时实现承诺验证与签名认证功能，简化交互流程，并利用多重签名技术减少签名验证次数。分析结果表明，改进的 4P_VES方案具有不可伪造性、一致性、不可区分性等属性，且能降低虚拟币发行时间，提高系统整体性能。

关键词：虚拟交易系统；虚拟币；融合原语；承签方案；多重签名

中文引用格式：张　泓，曹珍富，董晓蕾. 基于承签原语与多重签名的改进虚拟交易系统方案[J]. 计算机工程，2016，42(2)：137-141，145.

英文引用格式：Zhang Hong，Cao Zhenfu，Dong Xiaolei. Improved Virtual Transaction System Scheme Based on Commitment-signature Primitive and Multisignature[J]. Computer Engineering，2016，42(2)：137-141，145.

Improved Virtual Transaction System Scheme Based on Commitment-signature Primitive and Multisignature

ZHANG Hong[1]，CAO Zhenfu[1,2]，DONG Xiaolei[1,2]

(1. Department of Computer Science and Engineering，Shanghai Jiaotong University，Shanghai 200240，China；
2. School of Computer Science and Software Engineering，East China Normal University，Shanghai 200062，China)

【Abstract】As the third party payment is introduced into a Four-participants Virtual Economy System(4P_VES) to detect and prevent collusion cheat，so many interactions are added，and the system performance is affected. Aiming at the problem，this paper proposes an improved 4P_VES by commitment-signature scheme based on fusion primitive. Commitment-signature scheme realizes commitment verification and signature authentication，and simplifies the interactions. Multisignature reduces the times of signature verification. Analysis result shows that the improved 4P_VES scheme maintain the properties of unforgeability，consistency，unreusability，and it can reduce time cost，improve system overall performance.

【Key words】virtual transaction system；virtual coin；fusion primitive；commitment-signature scheme；multisignature

DOI：10.3969/j.issn.1000-3428.2016.02.025

1　概述

随着互联网的普及，网络经济迅猛发展，极大地改变了人们的生活生产方式，以网络游戏、App 应用、云服务等为代表的虚拟商品和服务日渐成为人们生活中的重要组成部分。虚拟经济呈现良好的发展态势，并在整个经济体中占据相当大的比例。Facebook 2013 年财报显示，第四季度支付收入达2.41亿美元(基本上来自游戏应用收入)，仅次于广告收入[1]。在国内，据腾讯 2013 年财报，腾讯在线游戏第四季度收入达 119.7 亿元，占总收入的 70%[2]。

通常，虚拟交易都是在线上交易系统平台完成。由于虚拟交易频次高、额度小的特点，真实货币不适用于该交易过程，因此虚拟币被线上交易系统平台广泛采用，如腾讯 Q 币、新浪 U 币等。当前虚拟交易的大致流程如下：玩家用户向平台购买虚拟币，然后玩家用虚拟币向在平台上注册并提供虚拟商品或服务的提供商购买虚拟商品或服务，之后提供商可以向平台兑换虚拟币。由于缺乏强有力的监管，相

基金项目：国家自然科学基金资助项目(61161140320，61033014)；国家“973”计划基金资助项目(2012CB723401)。
作者简介：张　泓(1990－)，男，硕士研究生，主研方向为应用密码学、虚拟交易系统安全；曹珍富、董晓蕾，教授、博士、博士生导师。
收稿日期：2015-01-09　　**修回日期：**2015-03-16　**E-mail：**zefan@sjtu.edu.cn

关法律法规也尚未健全,虚拟交易在透明性、公平性方面都有待提高与改善,因此建立一套安全、可靠、透明、高效的虚拟交易系统有十分重要的现实意义。

文献[3]提出 Verito 虚拟交易系统解决方案,模型中有平台、玩家、提供商 3 个参与者相互交互,能够保证透明性、公平性、不可重用性与可扩展性。其主要思想是通过密码学中的承诺原理将虚拟币与其真实售价绑定,从而保证虚拟币的价格在整个生命周期中保持一致。但是该方案的安全性是基于任何 2 个参与者之间都不存在合谋欺骗行为的假设。文献[4]讨论了 Verito 方案中平台与玩家之间合谋的可能性与可行性,并在 Verito 的基础上提出了四方参与者虚拟交易系统(Four-participants Virtual Economy System,4P_VES)方案。4P_VES 方案通过引入第三方支付检测和预防合谋欺骗行为,进一步提高虚拟交易系统的透明性与可靠性。但由于引入第三方支付,增加了交互活动,使整个系统变得更为复杂,在性能上有待改进。

本文在[3-4]的基础上,采用密码学原语融合技术和多重签名方案,改进文献[4]算法,在不影响系统各属性要求的前提下,提高系统性能。本文改进思路为:(1)在平台发行虚拟币时,要对虚拟币真实价格进行承诺绑定,之后对承诺值进行签名。通过将承诺与签名方案融合在一个逻辑过程中,完成承诺与签名的功能,从而提高算法性能。(2)平台将签名后的虚拟币发送给支付方,支付方验证签名,打开承诺值检查通过后再次签名,在后续交易环节中,需要分别验证平台与支付方的签名才能认证虚拟币是否有效。

2 虚拟交易模型

本文是对文献[4]中 4P_VES 方案的改进,其系统模型基本一致,由 4 个参与者构成:平台,提供商,玩家和第三方支付。各参与者之间主要的交互活动有:平台发行虚拟币,玩家购买虚拟商品或服务,提供商兑换虚拟币。在本文模型中,第三方支付扮演了十分重要的角色,除了负责转账等支付功能外,第三方支付还负责监管平台与玩家之间的交易行为,监督是否有合谋欺骗行为存在。图 1 为 4P_VES 基本模型。

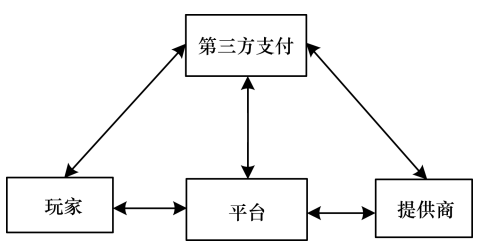

图 1 4P_VES 基本模型

(1)发行虚拟币(平台、玩家、第三方支付):

1)平台公布其当前发行的虚拟币种类、真实价格(包括币种、价钱);

2)玩家选择要购买的虚拟币种类和数量,向平台发送购买请求;

3)平台构造相应数量和币种的虚拟币,然后将虚拟币发送给第三方支付;

4)第三方支付验证虚拟币绑定值是否与标价一致,若一致,则经签名认证后转发给玩家;

5)平台将该批虚拟币计入玩家虚拟账户;

6)第三方支付完成转账。

(2)购买虚拟商品或服务(平台、玩家、提供商):

1)玩家选择要购买的虚拟商品或服务,向提供商发送所需虚拟币,提出购买请求;

2)提供商验证第三方支付的签名,返回交易订单编号;

3)玩家将虚拟币连同订单编号发送给平台;

4)平台检查虚拟币是否属于该玩家,然后将虚拟币从玩家转账给提供商,给玩家返回收据;

5)玩家凭收据向提供商换取虚拟商品或服务。

(3)兑换虚拟币(平台、提供商、第三方支付):

1)提供商向平台发送一批虚拟币,发起兑换请求;

2)平台验证虚拟币真实性,并计算出该批虚拟币总价,并提供证据证明总价;

3)提供商用收到的证据验证总价;

4)平台从提供商虚拟账户中移除该批虚拟币;

5)第三方支付将相应现金从平台转账到提供商账户。

3 相关密码学原理与技术

本文改进方案主要涉及承诺、数字签名、多重签名等密码学原理与技术。

3.1 承诺

承诺是密码学中一个常用的基本原语,是一个两方协议,包含承诺者与接受者 2 个参与者。承诺方案包含 2 个阶段,即承诺阶段和打开阶段;承诺具有隐藏性和绑定性 2 条基本性质[5]。同态承诺还满足同态映射:$m_0, m_1 \in \mathcal{M}$, $Com(m_0 + m_1) = Com(m_0) \odot Com(m_1)$,常用的承诺方案有文献[6-8]方案等。

文献[6]提出基于离散对数假设的 Pedersen 同态承诺方案。

(1)初始化 *ComSetup*( ):生成 2 个大素数 p, q,且满足 $q \mid (p-1)$。构造一个 q 阶子群 $\mathbb{G}_q < \mathbb{Z}_p^*$, $|\mathbb{G}_q| = q$,随机选择生成元 $g \in \mathbb{G}_q$ 与一个群元素 h

$\in \mathbb{G}_q$,其中,$\log_g h$ 为未知。

(2)承诺函数 $Com(m)$:对消息 $m \in \mathbb{Z}_q$ 作承诺,随机选择 $r \in \mathbb{Z}_q$,计算承诺值 $c = g^m h^r$。

(3)承诺打开函数:

$$OpenCom(c,m,r) = \begin{cases} 1 & g^m h^r \equiv c \\ 0 & \text{否则} \end{cases}$$

3.2　数字签名

数字签名方案($\mathcal{M},\mathcal{S},\mathcal{K},\mathcal{SIG},\mathcal{VER}$):$\mathcal{M}$ 是所有消息组成的有限集合,即消息空间;$\mathcal{S}$ 是所有签名组成的有限集合,即签名空间;$\mathcal{K}$ 是密钥空间,包括公钥和私钥;$\mathcal{SIG}$ 是所有签名算法的有限集合;$\mathcal{VER}$ 是所有验证算法的集合[9]。

(1)由密钥生成算法 $Gen(1^n)$,根据安全参数输出一对密钥 $K(pk,sk) \in \mathcal{K}$,密钥长度为 n。

(2)签名算法 $sig_K \in \mathcal{SIG}$,$sig_K: \mathcal{M} \rightarrow S$,采用私钥 sk 签名。

(3)验证算法 $ver_K \in \mathcal{VER}$,$ver_K: \mathcal{M} \times \mathcal{S} \rightarrow \{\text{True}, \text{False}\}$,采用公钥 pk 验证签名:

$$ver_K(m,s) = \begin{cases} \text{True} & s = sig_K(m) \\ \text{False} & s \neq sig_K(m) \end{cases}$$

常用的数字签名有 RSA 签名方案[10]、ElGamal 签名方案[11]等,本文采用 RSA 签名方案。该方案($\mathcal{M},\mathcal{S},\mathcal{K},\mathcal{SIG},\mathcal{VER}$):$\mathcal{M} = \mathcal{S} = \mathbb{Z}_n$;$K = \{(n, p, q, a, b) \mid n = pq, p, q \text{ 是素数}, ab \equiv 1 \bmod \phi(n)\}$,$K = (pk,sk) \in \mathcal{K}$,其中,$pk = (n,b)$;$sk = (p,q,a)$。签名和验证函数如下:

$$sig_K(m) = m^a \bmod n$$

$$ver_K(m,s) = \text{True} \Leftrightarrow m \equiv s^b \bmod n$$

其中,$m, s \in \mathbb{Z}_n$。

3.3　多重签名

Itakura 于 1983 年提出多重签名(multisignature)的概念[12]。在签名阶段,多个签名成员使用各自的签名私钥对消息进行签名,生成一份多重签名;在验证阶段,验证者可以使用签名成员的公共签名公钥来验证签名。多重签名可以分为有序多重签名和广播多重签名[13]。有序多重签名方案中各签名者必须按照预先设定的顺序对消息进行签名。每位签名成员收到消息后,首先验证前一位签名成员的部分签名是否有效,如果有效,则该成员使用自己的签名私钥进行签名,并传递给下一位签名成员;否则,拒绝签名,中止整个多重签名过程,如图 2 所示。广播多重签名方案将消息以广播的形式发送给每位签名成员,各成员使用各自的签名私钥独立完成部分签名,再由签名合成者收集所有部分签名,合成一个多重签名,如图 3 所示。

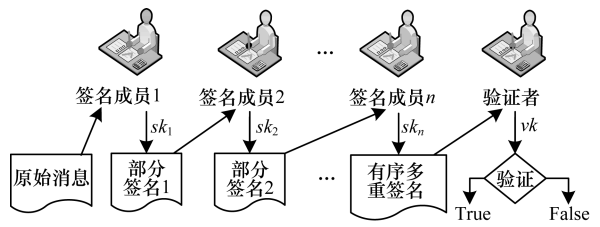

图 2　有序多重签名方案

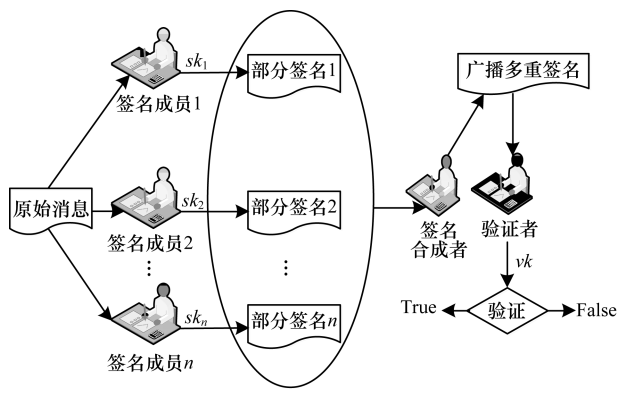

图 3　广播多重签名方案

4　承签方案

承诺与签名是常用的密码学原语,在很多应用场景中(如外包计算、电子货币等)需要两者结合使用。为了简化过程、提高速度,本文定义承签方案,将签名与承诺融合为同一逻辑过程。承签方案需要同时满足签名与承诺的属性要求:不可伪造性,不可否认性,绑定性,隐藏性等。

承签方案($\mathcal{M},\mathcal{W},\mathcal{K},\mathcal{SC},\mathcal{VO}$):$\mathcal{M}$ 是消息空间;$\mathcal{W}$ 是所有可能承诺签名组成的有限集合,即承诺签名空间;$\mathcal{K}$ 是密钥空间,包括签名私钥、验证公钥和承诺打开密钥;$\mathcal{SC}$ 是所有承签算法的有限集合;$\mathcal{VO}$ 是所有验证承诺签名算法的集合。

(1)密钥生成算法 $Gen(1^n)$:生成承签密钥 $K = ((pk,sk),openkey) \in \mathcal{K}$。

(2)承签算法 $sigcom_K \in \mathcal{SC}$,$sigcom_K: \mathcal{M} \rightarrow \mathcal{W}$ 生成承诺签名。

(3)承签验证算法 $veropen_K \in \mathcal{VO}$,$veropen_K: \mathcal{M} \times \mathcal{W} \rightarrow \{\text{True}, \text{Flase}\}$,打开承诺且验证签名,若通过则返回 True,否则返回 Flase。

承签方案需满足如下性质:

(1)不可伪造性。在 sk 未知的情况下,对任意的多项式时间算法 $\mathcal{A}$ 生成消息 m 的承诺签名 w,存在可忽略函数 $\mu(n)$,使得 $\Pr[veropen_K(m,w) = \text{True}] \leqslant \mu(n)$。

(2)不可否认性。给定承诺签名 w,经验证通过,即 $veropen_K(m,w) = \text{True}$,则 w 不是由承签者生成的概率是可忽略的。

(3)绑定性。存在可忽略函数 $\mu(n)$,$\Pr[veropen(sigcom(m,sk,openkey),m',pk,openkey] \leqslant \mu(n)$。

(4)隐藏性。在承诺签名打开前(即 *openkey* 未知)$m_0, m_1 \in \mathcal{M}, m_0 \neq m_1, w_0 := sigcom_K(m_0), w_1 := sigcom(m_1)$,随机选择 $w_t \leftarrow_R \{w_0, w_1\}$,对任意多项式时间算法 $\mathcal{A}$,猜测 $t' \leftarrow \{0,1\}$,存在可忽略函数 $\mu(n)$,使得 $\Pr[t = t'] = \frac{1}{2} + \mu(n)$。

5 4P_VES 改进方案

5.1 基于融合原语的改进方案

在 4P_VES 方案中,平台发行虚拟币时,首先将发行价格与虚拟币通过承诺技术进行绑定,然后再对承诺值签名认证,以保证虚拟币的不可伪造性。第三方支付在收到平台发送的虚拟币后,先验证平台签名,再打开承诺验证绑定值是否与标价一致。上述发行过程需要经历 4 个步骤,如图 4 所示。本文将承诺与签名 2 个密码学原语融合成一个逻辑过程,直接完成对虚拟币承诺绑定和签名认证,在后续过程中,可以一步完成验证签名和打开承诺,如图 5 所示,从而提高算法性能。

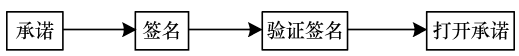

图 4 原语融合前的虚拟币发行过程

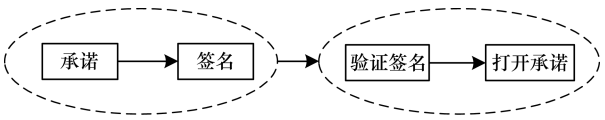

图 5 原语融合后的虚拟币发行过程

在 4P_VES 中,采用 Pedersen 同态承诺方案,将虚拟币与真实价格绑定:$C = Com(m) = g^m h^r$,然后再对承诺值 C 签名认证:$S = sig_{vk}(C) = C^a \bmod n$,$n = pq, p, q$ 是素数,$ab \equiv 1 \bmod \varphi(n)$,其中,签名公钥 $pk = (n, b)$;签名私钥 $sk = (p, q, a)$。支付方首先验证平台签名,验证 $C \equiv S^b \bmod n$ 是否成立。签名验证通过后,再使用打开承诺的钥匙(m, r)打开承诺 C,判断 $C \equiv g^m h^r$ 是否成立。

现将上述承诺与签名原语融合,在同一步骤中完成承诺并签名:$SC = SigCom(m) = sig_{vk}(Com(m)) = g^{am} h^{ar} \bmod n$;验证签名与打开承诺也可一步完成:

$$Verify(SC, m', r, b) = \begin{cases} 1 & (SC)^b \equiv g^{m'} h^r \\ 0 & \text{否则} \end{cases}$$

5.2 基于多重签名的改进方案

在 4P_VES 方案中,发行虚拟币需要同时有平台与第三方支付的签名,平台在绑定虚拟币真实价格后签名认证,发送给第三方支付,第三方支付打开承诺验证真实价格后对虚拟币再次签名认证,从而防范合谋欺骗。以上 2 次签名分别保证了虚拟币的不可伪造性与系统的抗合谋性。在后续交易过程中,需要分别验证平台与第三方支付的签名,带来较大的时间开销。为此,本文引入多重签名方案,平台先进行签名认证,之后将部分签名发送给第三方支付,第三方支付验证部分签名,打开承诺检查承诺值,然后生成多重签名 *MS*。在后续验证过程中,只需使用多重签名验证公钥打开 *MS* 即可验证虚拟币的真实性与一致性,节省了时间开销,提高了整体性能。基于多重签名的改进方案如图 6所示。

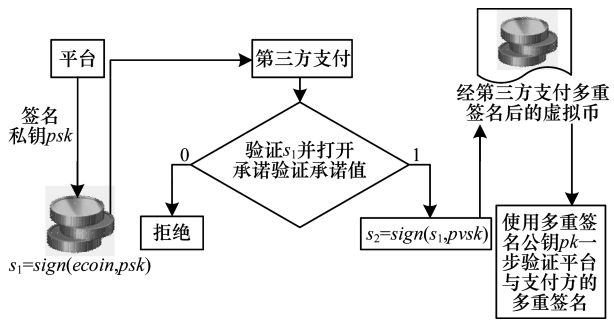

图 6 基于多重签名的改进方案中虚拟币发行过程

6 系统属性分析

本文在承诺和签名 2 个部分对 4P_VES 方案做了改进,可能影响原有系统的属性,因此,需要重新讨论改进方案的不可伪造性、一致性、不可区分性等属性。在基于多重签名的改进方案中,不可伪造性、一致性由多重签名的安全性来保证,而不可区分性与承诺有关,在此改进方案中未对承诺方案有所改动,所以,仍然满足不可区分性。

6.1 不可伪造性

任何敌手在平台签名密钥未知的情况下,多项式时间内生成能够通过签名验证的虚拟币的概率可忽略,即:给定验证虚拟币函数 *Verify*( ),平台签名密钥 *sk* 未知,对任意概率多项式时间算法 $\mathcal{A}$ 生成虚拟币,存在可忽略函数 $\mu(k)$ 使得:$\Pr[Verify(\mathcal{A}()) = \text{True}] \leqslant \mu(k)$。在基于融合原语的改进方案中,承诺与签名融合到同一逻辑步骤 *SigCom*(m)中。其攻击模型如下:敌手生成 SC'并声称是 m 的承诺签名,发送给挑战者,挑战者调用 $Verify(SC', m, r, b)$函数验证签名并打开承诺。如果挑战者验证通过,则敌手获胜,即 $SC'^b \equiv g^m h^r$。假设 $SC' = g^x h^y$,则 $g^{xb} h^{yb} \equiv g^m h^r$,即 $g^{bx-m} = h^{r-hy}$,根据强 RSA 假设,在平台签名私钥 a 未知的情况下,多项式时间内构造出 SC'并通过验证的概率是可忽略的。所以,以上方案满足不可伪造性。

6.2　一致性

虚拟币的绑定价格在整个生命周期中是保持一致的,即平台在生成虚拟币后不能改变虚拟币的绑定值。形式化表示为:平台做出承诺 $C = Com(m_1)$ 后不能将 C 揭示为 m_2。

在融合原语改进方案中,生成 SC 后不能变更 SC 所对应的绑定值 m。其攻击模型如下:敌手做出承诺签名 $SC = g^{am}h^{ar} \bmod n$,并提供密钥 (m', r', b),$m' \neq m$,挑战者使用该密钥打开验证 SC,如果通过,则敌手获胜。即:

$$\begin{aligned}\Pr[Adv\ wins] &= \Pr[Verify(SC, m_2, r_2, b) = 1] \\ &= \Pr[(SC)^b \equiv g^{m_2}h^{r_2}] \\ &= \Pr[g^{m_2}h^{r_2} = (g^{am_1}h^{ar_1})^b \wedge m_2 \neq m_1] \\ &= \Pr[g^{m_2}h^{r_2} = g^{m_1}h^{r_1} \wedge m_2 \neq m_1]\end{aligned}$$

其中,$r_2 = (m_1 - m_2)(\log_g h)^{-1} + r_1$,根据离散对数假设,概率 $\Pr[Adv\ wins]$ 可忽略。所以,该方案满足一致性。

6.3　不可区分性

在融合原语改进方案中,2 枚虚拟币对应的承诺签名 SC_1, SC_2 对平台而言不可区分。$SC_1 = g^{am_1}h^{ar_1} \bmod n$,$SC_2 = g^{am_2}h^{ar_2} \bmod n$,由于 Pedersen 承诺方案满足完全隐藏性[6],$g^{m_1}h^{r_1}$ 与 $g^{m_2}h^{r_2}$ 是不可区分的,因此无法区分 SC_1 与 SC_2,该方案满足不可区分性。

7　系统性能评估

在基于融合原语的改进方案中,在发行虚拟币阶段,由于融合了承诺与签名 2 个原语,节省了近一半的计算开销。随着发行虚拟币批量的增大,承诺与签名逐渐成为影响性能的主要因素,图 7 描述了改进方案与原方案的平均虚拟币发行时间比值随着发行量的变化趋势,由图 7 可见,该比值随发行量增大接近于 0.5。

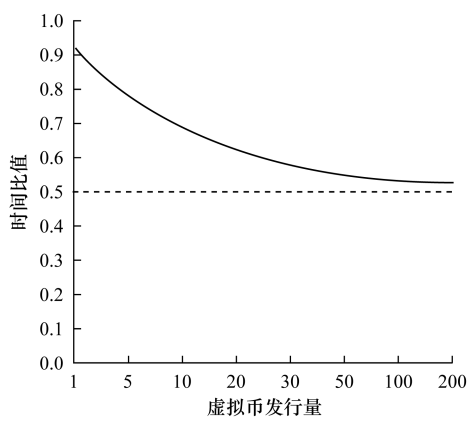

图 7　2 种方案平均虚拟币发行时间比值随发行量的变化趋势

在基于多重签名的改进方案中,每个虚拟币只有在发行阶段需要经历 2 次签名认证(一次是在多重签名过程中由第三方支付验证平台签名,另一次是玩家得到虚拟币时验证签名),在其他阶段只需要直接验证多重签名即可。表 1 比较了改进方案与 4P_VES的验证签名次数。由此可见,改进方案减少了签名验证次数,从而提高系统性能。

表 1　方案验证签名次数比较

交易阶段	基于多重签名的改进方案	4P_VES 方案
发行虚拟币	2	0
购买虚拟商品或服务	1	2
兑换虚拟币	1	2

8　结束语

本文首先融合承诺与签名原语定义承签方案,然后在 4P_VES 的基础上,分别采用承签方案和多重签名技术,提出 4P_VES 的改进方案,在保证可靠虚拟交易系统原有属性的前提下,提高系统性能。本文未讨论如何将承诺与动态累加器相融合、动态累加器与签名相融合等问题,今后可以继续在这些方面展开研究,进一步简化系统交互,提高系统性能。

参考文献

[1] Facebook Annual Report 2013[EB/OL]. (2013-07-15). http://investor.fb.com/annuals.cfm.

[2] Tencent Financial Reports 2013[EB/OL]. (2013-02-15). http://tencent.com/en-us/content/ir/rp/2013/attachments/201302.pdf.

[3] Bhaskar R, Guha S, Laxman S, et al. Verito: A Practical System for Transparency and Accountability in Virtual Economies[C]//Proceedings of Network & Distributed System Security Symposium. New York, USA: ACM Press, 2013.

[4] Zhang Hong, Cao Zhenfu, Dong Xiaolei, et al. 4P_VES: A Collusion-resistant Accountable Virtual Economy System[C]//Proceedings of the 16th International Conference on Information and Communications Security. Berlin, Germany: Springer, 2014: 61-73.

[5] 张宗洋. 承诺和零知识的非延展属性研究[D]. 上海: 上海交通大学, 2012.

[6] Pedersen T P. Non-interactive and Information-theoretic Secure Verifiable Secret Sharing[C]//Proceedings of Cryptology-CRYPTO'91. Berlin, Germany: Springer, 1992: 129-140.

[7] Haitner I, Horvitz O, Katz J, et al. Reducing Complexity Assumptions for Statistically-hiding Commitment[C]//Proceedings of Cryptology-EUROCRYPT'05. Berlin, Germany: Springer, 2005: 58-77.

(下转第 145 页)

证据冲突冲突的情况下,融合结果的分配精度也比较理想。通过表 3 可以看出,当有新证据源加入时,经典 D-S 证据理论和 Yager 方法对命题 A 的融合结果仍然为 0,存在一票否决的情况。文献[11]方法有效解决了一票否决的问题,但是收敛速度慢,分配精度不够,未知领域 Θ 没有明显下降。相比文献[11]方法,本文提出的方法随着支持命题 A 证据的增加,融合结果收敛速度更快,未知领域 Θ 的范围更小,较好地反映了实际情况下的融合结果,可靠性较高。

5　结束语

针对 D-S 证据理论在处理高度冲突证据时面临的规则失效问题,本文基于矛盾系数,提出了一种新的改进方法,在一定程度上弥补了 D-S 证据理论的不足。新的方法改进了经典 D-S 证据理论丢弃冲突信息的做法,充分利用了各证据体之间的冲突信息,采用冲突信息求得各证据间的矛盾系数,再计算各证据对于命题的权值,应用权值信息对加权基本概率分布函数进行改进,最后对证据进行融合。算例分析结果证明,相比其他方法,本文方法更符合人们的客观预期,融合结果的收敛速度更快。

参考文献

[1] Dempster A P. Upper and Lower Probabilities Induced by a Multiplicated Mapping[J]. Annals of Mathematical Statistics,1967,38(2):325-339.

[2] Shafer G. A Mathematical Theory of Evidence[M]. New Jersey,USA:Princeton University Press,1976.

[3] Wu Zhiwei. Attribute Reduction Based on Evidence Theory in Incomplete Decision Systems[J]. Information Sciences,2008,178(5):1355-1371.

[4] Hua Zhongsheng, Gong Bengang, Xu Xiaoyan. A DS-AHP Approach for Multi-attribute Decision Making Problem with Incomplete Information[J]. Expert System with Application,2008,34(3):2221-2227.

[5] 陈赠明. 群决策环境下证据理论决策方法应用研究[D]. 合肥:合肥工业大学,2006.

[6] Lin Tzu-chao. Partition Belief Median Filter Based on Demspter-Shafer Theory for Image Processing[J]. Pattern Recognition,2008,41(1):139-151.

[7] Otman B, Yuan Xiaohong. Engine Fault Diagnosis Based on Multisensor Information Fusion Using Dempster-Shafer Evidence Theory[J]. Information Fusion, 2007, 8(4):379-386.

[8] Zeng Dehuai, Xu Jianmin, Xu Gang. Data Fusion for Traffic Incident Detection Using D-S Evidence Theory with Probabilistic SVMs[J]. Journal of Computers, 2008,3(10):36-43.

[9] 丁迎迎,李洪瑞. 一种简单有效的处理冲突证据的 D-S 改进方法[J]. 指挥控制与仿真,2011,32(2):22-25.

[10] Yager R R. On the Dempster-Shafer Framework and New Combination Rules[J]. Information Sciences, 1987,41(2):93-137.

[11] 孙　全,叶秀清,顾伟康. 一种新的基于证据理论的合成公式[J]. 电子学报,2000,28(8):117-119.

[12] Murphy C K. Combining Belief Functions When Evidence Conflicts[J]. Decision Support Systems,2000, 29(1):1-9.

[13] 熊彦铭,杨战平,屈新芬. 基于模型修正的冲突证据组合新方法[J]. 控制与决策,2011,26(6):883-887.

[14] 邓　勇,施文康,朱振福. 一种有效处理冲突证据的组合方法[J]. 红外与毫米波学报,2004,23(1):27-32.

[15] 许红波,丁建江,胡伟稿. DS 规则推广及其在飞机目标识别中的应用研究[J]. 雷达与对抗,2006,1(1):34-38.

编辑　顾逸斐

(上接第 141 页)

[8] Nguyen M H, Ong S J, Vadhan S. Statistical Zero-knowledge Arguments for NP from Any One-way Function[C]//Proceedings of the 47th Annual IEEE Symposium on Foundations of Computer Science. Washington D. C. ,USA:IEEE Press,2006:3-14.

[9] Stinson D R. Cryptography: Theory and Practice[M]. Boca Raton,USA:CRC Press,2005.

[10] Rivest R L,Shamir A,Adleman L. A Method for Obtaining Digital Signatures and Public-key Cryptosystems[J]. Communications of the ACM,1978,21(2):120-126.

[11] ElGamal T. A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms[J]. IEEE Transactions on Information Theory,1985,31(4):10-18.

[12] Itakura K, Nakamura K. A Public-key Cryptosystem Suitable for Digital Multisignatures[J]. NEC Research & Development,1983,(71):1-8.

[13] 王晓峰,张　璟,王尚平. 多重数字签名方案及其安全性证明[J]. 计算机学报,2008,31(1):176-183.

编辑　陆燕菲