第34卷 第18期 计 算 机 工 程 2008年9月
Vol.34 No.18 Computer Engineering September 2008
·安全技术· 文章编号：1000—3428(2008)18—0171—03 文献标识码：A 中图分类号：TP309

P2P组合交易的公平支付协议

刘义春
(广东商学院广东省电子商务重点实验室，广州 510320)

摘 要：针对P2P交易环境中的多方组合交易模式，提出一个新的乐观公平的离线支付方案。在该方案中，参与协议的任何一方均不具有优势，信任方不需要在线介入支付过程。分析支付中可能出现的争议，并给出解决方案。分析结果验证了该协议的公平性。
关键词：P2P系统；组合交易；公平性

Fair Payment Protocol for P2P Aggregate Transaction

LIU Yi-chun
(Guangdong Key Lab of Electronic Commerce, Guangdong University of Business Studies, Guangzhou 510320)

【Abstract】 This paper proposes a new optimistic fair off-line payment scheme for multi-party aggregate P2P transaction, in which no one has advantage over others. The trusted party need not be involved into exchange unless disputes have occurred. The disputes which might occur are analyzed and handling solution is proposed. Analysis results show fairness of the protocol.
【Key words】 P2P system; aggregate transaction; fairness

1 概述

在P2P系统中，所有节点都是对等的，各节点具有相同的责任与能力并可以协同完成任务。在P2P交易模式中，每一成员可以是客户，从其他成员处购买商品；也可以是商家，向其他成员提供内容服务。

迄今的电子支付研究大多集中于两方简单交易情形，较少考虑多方组合交易等复杂交易模式中的支付问题，而在实际电子商务活动中，多方交易情形经常出现。在组合交易模式中，客户从多个销售商处购买多种商品，因缺少某些商品而导致商品不完整交易，这对客户而言是没有价值的。客户要么购买所有商品，要么一件也不购买。

一个安全的电子商务协议必须满足公平性原则，即在协议执行的任何阶段，参与协议的任何一方都不占优势。为保障交易公平性，常用的方法是协议发起方和响应方将交易商品及相关信息发送给第三方，第三方再转发给相应的主体。其缺点是可信第三方容易成为系统的瓶颈。P2P环境要求最多只能有轻量服务器，高负荷中间方不符合P2P的要求。

Asokan N等人利用乐观并发控制机制提出了一系列乐观公平的交易协议[1-3]。在该方案中，双方正常交易不需可信第三方的参与，只有争议出现时才由可信第三方进行仲裁或协助完成协议。

针对组合交易等复杂交易模式，文献[4]对其公平性等性质进行了分析，提出了支付方案设计原则，但未提出具体的实现协议。

本文针对多方组合交易模式的特点，引入可信第三方，提出了离线支付协议，并就可能出现的争议给出了解决方案。

2 相关密码技术

2.1 密码算法

签名协议采用如下的Schnorr签名算法[5]：

(1)选随机数$k\in Z_q^*$，计算$r=g^k \pmod p$,$e=H(r,m)$,$s=xe+k \pmod q$。

(2)签名算法，$Sig(m,x)=(e,s)$。

(3)签名验证，$H(r',m)=e$，这里$r'=g^s y^e \pmod p$。

其中，p,q是大素数且$q|(p-1)$, $g\in Z_p^*$, $g^q=1 \pmod p$；H为Hash函数；g,p,q,H可由一组用户共用并公开；签名者私钥$x\in Z_q$；公钥$y=g^{-x} \pmod p$。

2.2 时间戳

在电子商务交易协议中，一种对协议可能的攻击是重放攻击(replay attack)。攻击者窃听正常的通信包，然后重新发送这些数据包，以欺骗某一方来完成与上次相同的协议通信流程。防范重放攻击的一种重要手段是时间戳机制。

在时间戳机制中，发送方利用密码操作把当前时间加入到合成消息中，从而避免利用过时的消息对协议进行的重放攻击。可以使用如下非对称密码技术实现时间戳的机制[6]：

(1)$A\rightarrow B$: $M,T_A,Sig_A(M, T_A)$。

(2)B:验证签名，如果验证通过且时戳T_A为有效，接收消息；否则拒绝。

3 组合交易模式的支付协议

不妨将P2P成员的集合视为一个P2P群。一个典型的P2P组合交易系统含有P2P群G中的多个成员：一个买方C；多个数字商品提供者$M_1,M_2,\cdots,M_n$；可信第三方A被引入仲裁支付协议中的争议，保证协议公平性。

考虑这样的情形，买方C决定在P2P群中购买k件不同商品$goods_i$, $i=1,2,\cdots,k$, $k<n$。不妨假定商品分别从k个不同卖方购买，即每一卖方提供一件商品。通过P2P搜寻系统，C在P2P群中查找可提供商品的成员，并在考虑售价、通信成本等因

基金项目：浙江省自然科学基金资助项目(Y106802)；广东省科技计划基金资助项目(2007B010200035)；浙江省教育厅科研基金资助项目(20060239)
作者简介：刘义春(1965－)，男，副教授、博士，主研方向：信息安全
收稿日期：2007-11-28 **E-mail：**liuychun@126.com

素后选择一组合适的卖方M_i, i=1,2,⋯,k。

3.1 支付代币

用于支付的代币由数字便条和银行印戳 2 个部分组成，形式如下：

$DigitalNote=\{SerialNo,BrokerID,GroupID,value,IssueDate,Expiration\}$

$BrokerStamp=Sig_{Broker}(DigitalNote)$

$Token=\{DigitalNote,BrokerStamp\}$

数字便条 *DigitalNote* 由序列号 *SerialNo*、银行标识符 *BrokerID*、P2P 群标识符 *GroupID*、代币面值 *value*、代币发行日期 *IssueDate* 和流通截止日期 *Expiration* 等项组成；银行印戳 *BrokerStamp* 为银行对数字便条的签名；项 *SerialNo* 随机选取且在 P2P 群中唯一。数字便条 *DigitalNote* 为全局唯一的。如果需要在代币兑付前实现银行对代币不可追踪，保证代币的匿名性，可采用盲签名协议让银行对数字便条进行盲签名。

3.2 支付子协议

面向组合交易的支付协议包括交易子协议和争议解决子协议。交易双方在安全可靠的信道上诚实地执行协议时，只需执行交易子协议即可；如果交易中信道发生故障或某一方故意中止协议，可执行争议解决子协议以完成交易过程。

交易子协议分为：

(1)求购及定价阶段

1)$C\rightarrow G$: $C,BrokerID,A,goods\ request$

2)$P_i\rightarrow C$: $P_i,PID_i,desc_i,quoted\ price_i$

where $P_i\in G$

对每一个 i(i=1,2,⋯,k)：

3)$C\rightarrow M_i$: C, TID, PID_i, bid_i

4)$M_i\rightarrow C$: $price_i$, $Sig_{M_i}(TID, PID_i, desc_i)$

(2)交易支付阶段

对每一个 i(i=1,2,⋯,k)：

5)$C\rightarrow M_i$:TID, C, sum, $Sig_C(TID, price_i, sum)$

6)$M_i\rightarrow C$:$E_{s_i}(goods_i)$, $Sig_{M_i}(TID, C, PID_i, TS)$

7)$C\rightarrow M_i$:$DigitalNotes_i$, TS, $Sig_C(TID, M_i, TS)$

8)$M_i\rightarrow C$:TID, M_1, s_i, $Sig_{M_i}(TID, C, sum, TS)$

9)$C\rightarrow M_i$:TID, C, $PK_{M_i}(BrokerStamp_i)$

其中，$E_s(message)$表示使用会话密钥s对$message$的加密；$PK_X(message)$表示用交易方X的公钥对$message$的加密。

在步骤 1)中，买方 C 将支付银行信息、可信方信息、商品需求信息等在可能提供商品的部分 P2P 成员中组播。

在步骤 2)中，多播组$\{P_i\}$每一成员回复买方以商品标识符PID_i、商品描述$desc_i$和商品报价$quoted\ price_i$。项$desc_i$常常是对数字商品Hash值的变换，用以验证商品的有效性。

在步骤 3)中，C比较每一个组播成员能够提供的价格、服务及其渠道信息等，并从中选择一组商家$\{M_i\}$(i=1,2,⋯,k)。然后C逐一将交易标识符TID、出价bid_i 发送给商家M_i。3 元组$\{TID, C, M_i\}$唯一地标识C, M_i之间的一次交易。

在步骤 4)中，每一个M_i 回复以商品售价$price_i$，及M_i对TID, PID_i、承诺售价的签名。

步骤 1)~步骤 4)为商品求购及定价阶段，可重复多轮，直至买卖方就交易价格达成一致。一旦协商完毕，支付立即开始。如果未就价格等协商一致，协议立即中止。

在步骤 5)中，C将TID、组合交易总金额sum、买方对价格$price_i$和sum的签名发送给每一个M_i，启动交易。

在步骤 6)中，M_i随机选择一个会话密钥s_i 并用来加密数字商品。然后他将加密后的密文、用作同意启动交易的证据的签名$Sig_{M_i}(TID, C, PID_i, TS)$发送给$C$。

在步骤 7)中，C将应支付每一个M_i的数字便条$DigitalNotes_i$分别发送给M_i，同时将其签名$Sig_C(TID,M_i,TS)$作为已接收数字商品加密件的收据发送给每一卖方。

在步骤 8)中，在对已收到代币的数字便条和商品接受收据进行验证后，M_i将用于解密商品的密钥s_i 以及承诺密钥有效的签名$Sig_{M_i}(TID,C,sum,TS)$发送给买方C。

在收到每一个M_i发送的数字商品密钥之后，买方对商品$goods_i$进行验证，确认是否能用密钥s_i成功地解密所获商品。如果收到的商品解密密钥能有效解密商品，协议继续进行；否则C将调用 3.3 节所述的争议解决子协议。

在步骤 9)中，C分别将与步骤(7)中数字便条对应的银行印戳$BrokerStamp_i$，用M_i的公钥加密后传送给每一个M_i。

如果某M_i最终确认收到的支付为无效，可调用相应的争议解决子协议。

3.3 争议解决子协议

在本方案中，引入一个可信第三方 A 作为仲裁者来处理协议执行中买卖双方的争议。交易中可能有 3 种争议情形出现，下面给出解决这些争议的子协议。

情形 1 卖方宣称其已交付商品的解密密钥但未收到有效的支付代币。

解决这种争议的子协议如下：

1.$M_i\rightarrow A$: TID, M_i, C, TS, $Sig_C(TID, M_i, TS)$, $price_i$, sum, $Sig_C(TID, price_i, sum)$

2.$A\rightarrow C$: TID，M_i

3. $C\rightarrow A$: $DigitalNotes_i$, $BrokerStamp_i$

4a.$A\rightarrow M_i$: $DigitalNotes_i$, $BrokerStamp_i$

or

4b.$A\rightarrow M_i$: $affidavit(M_i, C, price_i)$

M_i 将已从C收到的商品密文接收凭据$Sig_C(TID,M_i,TS)$及交易价格信息发送给仲裁者A。A 验证凭据签名，然后请C传送完整的支付代币。A验证支付的有效性。如果有效，则将支付转发给M_i；否则，A向 M_i开具未从C获得数额为$price_i$的应有支付的仲裁证据$affidavit(C, M_i, price_i)$。

情形 2 买方宣称未收到商家的商品解密钥。

解决这种争议的子协议如下：

1.$C\rightarrow A$: $TID,M_i,PID_i,TS,Sig_{M_i}(TID,C,PID_i,TS),Sig_C(TID,M_i,TS)$

2.$A\rightarrow M_i$: TID, C

3.$M_i\rightarrow A$: s_i,$Sig_{M_i}(TID, C, sum, TS)$

4a.$A\rightarrow C$: s_i ,$Sig_{M_i}(TID, C, sum, TS)$

$A\rightarrow M_i$: $Sig_C(TID, M_i, TS)$

or

4b.$A\rightarrow C$: $affidavit(C, M_i, sum)$

C将用作M_i交付商品密文的证据$Sig_{M_i}(TID, C, PID_i, TS)$，$C$ 的商品密文接收证据Sig_C (TID, M_i, TS)发送给A。A验证签名的有效性，然后请M_i传送密钥。M_i将商品密钥以及承诺密钥有效的签名$Sig_{M_i}(TID, C, sum, TS)$发送给$A$。$A$验证签名有效性，如果有效则将其转发给$C$，否则$A$向 C开具应从M_i获得交易赔偿的仲裁证据$affidavit(C, M_i, sum)$。

情形 3 买方宣称无法用收到的解密钥得到有效商品。

解决这种争议的子协议如下：

1.$C\rightarrow A$: TID, M_i, PID_i , $desc_i$, sum, TS $Sig_{M_i}(TID, C, sum, TS)$, $Sig_{M_i}(TID, PID_i, desc_i)$

2.$A\rightarrow M_i$: TID, C

3. $M_i \rightarrow A$: TID, $goods_i$

4a. $A \rightarrow C$: M_i $goods_i$

or

4b $A \rightarrow C$: $affidavit(C, M_i\ sum)$

C 将已从M_i收到的商品描述信息$desc_i$、商品密钥承诺$Sig_{M_i}(TID, C, sum, TS)$送给$A$。$A$首先验证承诺，有效，则请$M_i$发送数字商品$goods_i$，得到$goods_i$后验证是否与$desc_i$相匹配。若匹配，则将其转发给$C$；否则向$C$开具应从$M_i$获得数额为$sum$的交易赔偿的仲裁证据$affidavit(C, M_i, sum)$。

4 协议分析

4.1 安全性

系统的安全性取决于系统采用的加密和签名算法。由于采用成熟的密码学方法，因此能防范对交易数据的伪造、篡改等外部攻击。

时间戳的使用能有效地防范可能针对协议的重放攻击，即任何交易方不能利用在交易中获得的证据信息事后重新启动协议，图谋非法利益。

4.2 协议公平性

在交易子协议中，买方得到并验证商品的过程先于其向各商家支付代币银行印戳，因此，用户支付时一定已获得有效的商品。如果某商家未发送商品密钥，买方可启动情形 2 的争议解决子协议。如果某卖方提供无效密钥却通过情形 1 的争议解决子协议获得支付，买方还能启动情形 3 的争议解决子协议。不论何种情形，只要买方诚实地执行协议，总能获得有效商品，或获得仲裁方开具的应从商家M_i得到违约赔偿的仲裁证据$affidavit(C, M_i, sum)$。

如果买方抵赖，接收商品密钥后拒绝支付，卖方可向仲裁方递交买方的商品接收收据并提出申诉，通过 3.3 节中情形 1的争议解决子协议获得有效支付，或获得能从买方索取赔偿的仲裁证据$affidavit(C, M_i, price)$。

调用争议解决子协议，使协议中任何一方都不会因为通信故障和其他方无故中止协议而受到损失。协议执行中任何一方均不处于优势地位，协议是公平的。

4.3 执行效率

加解密运算采用对称密钥体制，加解密速度远高于公钥体制。签名采用 Schnorr 签名算法，产生签名所需的大部分计算都可在预处理阶段完成，并且这些预计算与待签名的消息无关，因此，交易中签名计算效率较高。此外 Schnorr 算法只需要较短的签名长度。

由于可信第三方不卷入正常的交易协议，仅仅当争议出现时方才介入交易，因此可信第三方不会成为系统的瓶颈，与在线第三方的交易协议行相比，其具有更高的执行效率。

5 结束语

本文针对多方组合交易情形的 P2P 支付系统，提出了公平的支付协议，分析可能出现的争议情形并给出解决方案。在此支付协议中，除非争议出现，作为可信方的仲裁者不需在线参与交易。协议是公平的、安全的、有效率的、适用于 P2P 多方组合交易的。

参考文献

[1] Asokan N, Schunter M, Waidner M. Optimistic Protocols for Fair Exchange[C]//Proc. of the 4th ACM Conf. on Computer Commun. Security. [S. l.]: ACM Press, 1997: 6-17.

[2] Asokan N, Shoup V, Waidner M. Optimistic Fair Exchange of Digital Signatures[C]//Proc. of EUROCRYPT'98. [S. l.]: Springer-Verlag, 1998: 591-606.

[3] Asokan N, Shoup V. Asynchronous Protocols for Optimistic Fair Exchange[C]//Proc. of IEEE Symposium on Research in Security and Privacy. [S. l.]: IEEE Press, 1998: 86-99.

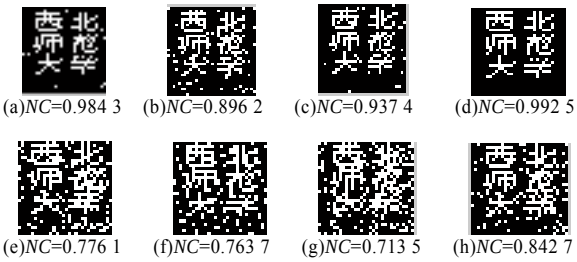
[4] Wang G, Das A. Models and Protocol Structures for Software Agent Based Complex E-commerce Transactions[C]//Proc. of the 2nd Int. Conf. on Electronic Commerce and Web Technologies. [S. l.]: Springer-Verlag, 2001: 121-131.

[5] Schnorr C P. Efficient Signature Generation for Smart Card[J]. Journal of Cryptology, 1991, 4(3): 161-174.

[6] Mao Wenbo. 现代密码学理论与实践[M]. 王继林, 译. 北京: 电子工业出版社, 2004-07.

(上接第 170 页)

缩攻击；图 4(b)为 QF=80%的 JPEG 压缩攻击；图 4(c)为直径为 1.0、阈值为 10.0 的模糊攻击；图 4(d)为对比度增强 5%的攻击；图 4(e)为高斯噪声(0.01)的攻击；图 4(f)为中心 1/4 剪切的攻击；图 4(g)为 3×3 的窗口进行中值滤波的攻击；图 4(h)为锐化攻击。



(a)NC=0.984 3 (b)NC=0.896 2 (c)NC=0.937 4 (d)NC=0.992 5

(e)NC=0.776 1 (f)NC=0.763 7 (g)NC=0.713 5 (h)NC=0.842 7

图 4 攻击后提取的不可见水印及 NC 值

6 结束语

利用可见水印技术提出一种多功能数字水印算法，本文对此进行尝试并取得不错的效果。但由于可见水印系统和不可见水印系统是相互独立、自成体系的，因此如何减少这两种水印之间的相互影响是算法的关键。下一步工作就是解决此问题，并实现用于图像内容完整性验证的(半)脆弱水印与可见水印、不可见水印两者或三者相结合的多功能数字水印算法，实现图像的多重保护。

参考文献

[1] Huang C H, Wu J J. Attacking Visible Watermarking Schemes[J]. IEEE Transactions on Multimedia, 2004, 6(1): 16-30.

[2] 罗 永, 成礼智, 徐志宏, 等. 基于带参数整数小波变换可见数字水印[J]. 软件学报, 2004, 15(2): 238-249.

[3] Slewis A, Knowles G. Image Compression Using the 2-D Wavelet Transform[J]. IEEE Transactions on Image Processing, 1992, 1(2): 244-250.

[4] Kankanhalli M, Ramakrishnan K R. Adaptive Visible Watermarking of Images[C]//Proc. of ICMCS'99. Florence, Italy: [s. n.], 1999.

[5] Beegan A P, Iyer L R, Bell A E. Design and Evaluation of Perceptual Masks for Wavelet Image Compression[C]//Proceedings of the 10th IEEE Digital Signal Processing Workshop. Pine Mountain, GA, USA: [s. n.], 2002-10.

[6] 王向阳, 杨红颖. 基于人眼视觉特性的快速图像编码算法[J]. 软件学报, 2003, 14(11): 1964-1970.