第 32 卷 第 17 期 计 算 机 工 程 2006 年 9 月
Vol.32 № 17 Computer Engineering September 2006
·博士论文· 文章编号：1000—3428(2006)17—0030—02 文献标识码：A 中图分类号：TP393.04

一种原子性和公平匿名性的电子支付协议

鲁荣波[1,2]，何大可[1]，缪祥华[1]
(1. 西南交通大学信息安全与国家计算网格实验室，成都 610031；2. 吉首大学数学与计算机科学系，吉首 416000)

摘 要：在分析电子交易的原子性和公平匿名性的基础上，提出了一种可同时实现原子性的公平匿名的电子支付协议，而且在整个支付过程中，可信第三方可以离线，只有发生争议时才参与仲裁解决。给出了协议的 6 个子协议，详细描述了各子协议的执行过程，并且非形式化地分析了协议的原子性和公平匿名性，保证了公平的电子交易和私密性。

关键词：原子性；公平匿名性；电子支付

Electronic Payment Protocol Realizing Atomicity and Fair Anonymity

LU Rongbo[1,2], HE Dake[1], MIAO Xianghua[1]
(1. Laboratory of Information Security and National Computing Grid, Southwest Jiaotong University, Chengdu 610031;
2. Dept. of Mathematics and Computer Science, Jishou University, Jishou 416000)

【Abstract】 Based on analysis of atomicity and fair anonymity of electronic payment, an protocol of electronic payment is proposed to enable not only anonymity but also own-trace and money-trace, which are realized fair anonymity and involvement of the TTP only for conflict resolution. Six sub-protocols are presented, the processes of which are elaborated. Atomicity and fair anonymity of the protocol are validated with non-formalization. The protocol can guarantee the fair electronic transaction and the privacy of the customer.

【Key words】 Atomicity; Fair anonymity; Electronic payment

1 概述

随着以安全电子支付系统为核心的基于互联网的电子商务活动越来越活跃，对电子支付系统安全的特殊需求也不断提升，除了传统的保密性、完整性、非否认性等安全要求之外，公平性和隐私权的保护已经成为这类电子商务协议新的基本要求。

现有的支付系统可分为两类：(1)不保护用户隐私权的系统，造成了用户隐私被滥用的可能；(2)用户匿名的不可跟踪系统，这类系统可以保护用户的隐私，但却为欺诈、洗钱、匿名勒索等犯罪活动提供了可能，使得电子犯罪同样难以追踪，因此上述两类系统都存在缺陷。为了既保护个人的隐私，又避免犯罪，文献[1]中提出了公平匿名性，指出可以借助可信中心，在法律机构的授权下对匿名交易进行匿名撤销。

Tygar提出公平的电子交易应保持原子性[2]，即当买卖双方进行交易时，要么交易完全没有发生，要么交易已经完成，而不会有所谓模棱两可的状态发生。他将电子商务的原子性分为 3 个级别，即货币原子性、商品原子性和可证明原子性。

(1)货币原子性。在一个事物中，若货币的传送是原子的，即这种传送或者发生，或者根本不发生，则称这个事物具备货币原子性。货币原子性是最基本的原子性。

(2)商品原子性。首先，凡满足商品原子性的协议必是货币原子性的，商品原子性的协议要保证付了款而收到货物，收到货物必付了款，绝不会发生付了款而收不到货物，或收到了货物而未付款的情况。

(3)可证明原子性。满足可证明原子性的协议必是满足货币原子性和商品原子性的协议，此外还要保证客户和商家都能验证到底发送了什么货物。

在现有的大部分电子支付协议中要么不具有原子性[3]，要么不满足公平匿名性[4]，刘文远等提出了一种同时实现原子性和公平匿名性的支付协议[5]。但在该方案中，用户选择的致盲消息包含了交易中的支付令牌，因此电子货币(即银行的限制性盲签名)与特定的交易就有关。如果某次交易被启动，但没有成功(这样的情形经常遇到)，此时用户就必须从商家取回支付令牌，并向银行发出取消令牌的命令，这样银行颁发的电子货币未被支付就被撤销，这对于银行的效益和用户的权益都是极为不利的。(限于篇幅，该方案详见参考文献[5])。

本文在文献[4]、[6]的基础上提出了一个可同时实现原子的公平匿名的电子支付协议，与文献[5]相比，用户从银行取出的电子货币与某次具体的交易无关，这样就保证了即使某次交易不成功，但电子货币可以继续使用，而且协议中的可信第三方只有发生争论时才参与在线仲裁，其余时间是可以离线的，可信中心成为通信瓶颈的可能性就大大降低。

2 原子的公平匿名的电子支付协议

协议的主要参与者为用户、银行、可信任第三方 T、商家，其中银行是 2 级可信任实体，是因为对它的信任是建立

基金项目：湖南省自然科学基金资助项目(03JJY6017)；湖南省教育厅基金资助项目(03c327)
作者简介：鲁荣波(1970—)，男，副教授、博士生，主研方向：应用密码学，信息安全理论；何大可，教授、博导；缪祥华，讲师、博士生
收稿日期：2005-09-12 **E-mail：**luorongbo8563@163.com

在对 T 的信任基础上的。

2.1 符号与基本工具

F表示银行；ID_X表示实体X的身份(这里X代表用户A或者商家B)；$Sign_i$ (Y) 表示实体i对消息Y的签名；i→j：Y表示实体i把消息Y发送给j；E_K(M) 表示对消息M用对称密钥K加密；PU_F(K) 表示用银行的公钥K进行加密；用符号‖来代表字符串连接操作。

定义 1 满足$c=H(m \| g \| h \| g^r h^c)$的二元组(c,r)称为$h$关于底$g$的离散对数的知识对消息$M \in \{0,1\}^*$的签名，记为$SPK\{\alpha \mid h= g^{\alpha}\}(M)$。

签名者如果知道一个整数x满足$h= g^x$,可以按如下步骤计算出这一签名：

(1)选择$s \in_R Z_n^*$，计算$h' = g^S$；

(2)$c=H(m \| g \| h \| h')$；

(3)计算 $r=s-cx \bmod n$。

定义 2 满足$c=H(M \| g \| h \| g_1 \| h_1 \| g^r h^c \| g_1^r h_1^c)$的二元组$(c,r)$称为$h$关于底$g$的离散对数和$h_1$关于底$g_1$的离散对数，且它们相等的知识对消息$M \in \{0,1\}^*$的签名，记为$SPK\{\alpha \mid h=g^{\alpha} \wedge h_1= g_1^{\alpha}\}(M)$。

签名者如果知道一个整数x满足$x=log_g h= log_{g_1} h_1$，可以按如下步骤计算出这一签名：

(1)选择$s \in_R Z_n^*$，计算$h' = g^S, h_1=g_1^S$；

(2)$c=H(M \| g \| h \| g_1 \| h_1 \| h')$；

(3)计算 $r=s-cx \bmod n$。

2.2 系统设置

银行F选择两个大素数p、q， $q \mid p-1$，选群G_q以及G_q的一个生成元组(g, g_1, g_2)， H为无碰撞单向散列函数，私钥$x \in Z_q^*$，公开p、q、g、g_1、g_2和H，以及公钥$y= g^x \bmod p$，$h_1=g_1^x \bmod p$，$h_2=g_2^x \bmod p$。

可信中心T：私钥x_T，公钥为$y_T= g_2^{x_T} \bmod p$。

实体X(这里X代表用户A或商家B)到银行注册：X把ID_X以及知识证明$SPK\ (ID_X)$发送给银行F，银行检查其正确性后计算SN_X=H($SPK\ (ID_X)$)，M_X=$Sign_F(SN_X)$。把SN_X，M_X发给用户。将ID_X及身份识别信息记录入数据库，并给用户分配其账号。

2.3 取款协议

用户随机选择$t \in Z_q$，计算$h=g_1^{t^{-1}} g_2$，$W=h_1^{t^{-1}} h_2$，$I=y_T^t$，$V= SPK\{\alpha \mid g_1=(h/ g_2)^{\alpha} \wedge I= y_T^{\alpha}\}(m)$。这里$m$是用户身份的识别信息。用户发送$V$和$W$银行，银行验证$V$和$W=h^x \bmod p$是否成立，如果成立则和用户之间执行一个公平盲签名协议，协议的详细过程见参考文献[6]。盲协议完成后，用户得到银行颁发的电子货币$EC=(\rho, \theta, \sigma, \delta, \xi, \zeta, t^p)$，银行从用户的账号上减去相应的金额。

当 A 想购买 B 的商品时，A 和 B 执行如下的交换协议：第 1 步：B 把加密了的产品或者收据发送给 A；第 2 步：A 把电子货币发送给 B；第 3 步：B 把加密密钥发给 A。

2.4 支付协议

(1) A→B：支付请求 Purchase_order；

(2)B→A：SN_B；用对称密钥K加密的产品或者收据C=E_k(product/receipt)；用可信中心T公钥加密对称密钥K得到的K_T=PU_T(k)；H_M =PR_M{H[H(C)，K_T，SN_B]}。

(3)A验证以上消息为正确后， A→F：PU_F (K_2)；E_{K_2}(EC，SN_A，M_A, SN_B)，其中EC为从银行得到的电子货币。

F→A： M_B

A→B： EC

(4)B把K发送给A，A解密C= E_k(product/receipt)，得到要购买的产品或者收据。

2.5 存储协议

B把(PU_F(k)，E_k(EC)发送给银行，银行验证电子货币的正确性后，存入B的账户。

2.6 完成协议

如果交换协议在第 1 步或第 2 步被中断，那么执行完成协议可以使得另一方从可信中心 T 那里得到所需要的，完成协议用到两个布尔变量：finished 和 Proved，finished 表示 A 是否支付出电子货币和收到密钥 K，Proved 表示 B 是否互相提供了秘密知识证明。两个变量为真都用 true 表示，失败的值都用 false 表示。参与交易的实体都可以执行以下步骤完成子协议：

(1)B→T：Requst, E_k(product/receipt), K_t，H_M

T：IF(finished=true)

T→B：EC

ELSE

T→B：要求B发送知识证明SPK (ID_B)

B→T：知识证明SPK (ID_B)

T：Proved=true

(2)A→T：Requst，$Sign_B$ (SN_B)，EC，E_k(product/receipt), K_t，H_M

T→A：K

T：finished=true

IF(Proved=true)

T→F：M_B，SPK (ID_B)，请求执行存储协议。

B 如果在第 2 步中没有收到电子货币，那么它执行以上操作完成子协议；同样如果 A 在第 3 步没有收到加密密钥，那么 A 执行以上操作完成子协议。如果 A 在第 3 步没有收到加密密钥，而 B 在第 2 步中收到了所有相关消息，则 A 执行完成子协议来获得加密密钥。

2.7 身份追踪协议

用户A在银行取出的电子货币是可撤销匿名性的，银行只需将存的钱传给可信方，可信方可计算出用户的身份：$I=(\xi / g_1)^{x_T} = y_T^t$，并验证$V= SPK\{\alpha \mid I=(\xi / g_1)^{\alpha} \wedge y_T= g_2^{\alpha}\}(m)$以确保正确，以此可对付洗钱之类的犯罪。

2.8 货币追踪协议

当银行将用户取款时银行观察到的所有数据传给可信方后，可信方可以计算出 ξ，即 $\xi = g_1 g_2^t = g_1 I^{x_t^{-1}}$，并验证$SPK\{\alpha \mid (\xi / g_1)=I^{\alpha} \wedge g_2= y_T^{\alpha}\}(m)$，以此可以对付勒索一类的犯罪。

3 原子性分析

(1)A 没有执行第 2 步

如果 A 发出了购买请求而不打算完成支付，它可以不把电子货币发给 B，它也不必执行完成协议，如果 B 执行了完成协议，可信中心 T 将检查 A 是否在以前执行了完成协议(finished=true)，如果 A 没有执行，T 将不会把电子货币发送给 B，因为可信方没有可发送的电子货币。

（下转第 34 页）