基于交互确认机制的公平电子现金交易协议研究*

王 茜，黄林军
（中山大学管理学院，广东 广州 510275）

摘 要：公平性是电子现金交易协议应满足的重要属性，信道不可靠和交易实体不诚实是破坏交易公平性的主要原因。针对于此，借鉴不可否认转换签名的思想，构建交互确认机制，并基于改进的CEMBS可验证算法，提出一种新的公平电子现金交易协议，并对协议属性进行分析。分析表明，该协议有效解决上述原因引起的交易不公平问题，在满足公平性和匿名性的同时，可有效避免交易的模糊状态。

关键词：电子现金；公平性；匿名性；交易协议
中图分类号：TP309 **文献标志码**：A **文章编号**：0529-6579（2010）01-0009-07

Fair e-Cash Transaction Protocol Based on Interactive Confirmer Scheme

WANG Qian, *HUANG Linjun*
(School of Business, Sun Yat-sen University, Guangzhou 510275, China)

Abstract: Fairness is an important attribute that electronic cash transaction protocol should satisfy, as dishonesty of the transaction entity and unreliable communication are the major reasons that harm transaction fairness. Focusing on the transaction unfairness issue caused by dishonest behavior of the transaction entity, and using the methodology of undeniable conversion signature for reference, interactive confirmer mechanism to effectively solve the problem of conflict between fairness and anonymity of electronic cash transaction protocol is established. Based on improved CEMBS verifiable algorithm, a new fair electronic cash transaction protocol is proposed and its attributes are analyzed. The analysis demonstrates that the proposed protocol can effectively avoid the ambiguity of transaction while satisfying the need for fairness and anonymity.

Key words: electronic cash; fair; anonymity; transaction protocol

电子现金由于其保留了传统现金的基本特征，较好地保护消费者的隐私权，成为小额支付中不可替代的电子支付方式。公平性是电子现金交易协议的重要属性，即在执行交易的任何阶段，参与交易的任何一方都不处于劣势[1]。信道不可靠和交易实体不诚实是破坏交易公平性的主要原因。对于该问题的解决，大多数电子现金交易协议均采用以牺牲电子现金的匿名性实现交易的公平性[2-10]。如，Chaum在文［2］中所提出通过解密在每个现金中消费者的身份实现电子现金交易协议的公平性是较为典型解决方案。Rivest and Shamir[3]提出通过消费者向商家表明自己的身份来证明其电子现金拥有者，然后通过数据恢复保持交易公平性。但该方法也要求消费者必须要提供自己的身份信息。在Camp和Tygar提出的可信第三方在线（交易日志L）的交易协议中[4-5]，采用级联式的消息传递方法巧妙的解决这一问题，具有一定的代表性。但由于该方案采用可信第三方在线方式，对每笔交易都要进行在线记录，需要保存大量的数据，成为交易过程中的通信和计算瓶颈。可见，电子现金交易协

* **收稿日期**：2009-01-15
基金项目：国家自然科学基金资助项目（70501033，70971141）；广东省自然科学基金资助项目（5300984，91510275010000491）
作者简介：王茜（1971年生），女，博士，副教授；E-mail：mnswq@mail.sysu.edu.cn

议实现公平性具有一定的特殊性，那么如何在通信信道不可靠或交易双方不诚实的情况下，实现交易协议的公平性和匿名性已成为电子商务支付领域研究的热点。

基于上述分析，充分考虑通信信道可靠性和交易双方的诚实情况，借鉴不可否认转换签名的思想[9-10]，构建交互确认机制，使可信第三方具有消息恢复能力，完成交易确认的签名转换；并基于改进的 CEMBS 可验证算法[11]，提出一种新的公平电子现金交易协议。所提出协议由消费者 C（Custom），商家 M（Merchant），可信第三方 TTP（Trusted Third Party）三个方组成，包括 Transaction 子协议、CTresolve 子协议、MTresolve 协议以及 Abort 协议四个部分。其中，可信第三方 TTP 作为协议的公正方，被消费者和商家所信赖。同时，可信第三方采用离线方式，即在通信信道中断或交易双方不诚实的情况下，可信第三方才参与协议运行，分别向商家和消费者发送各自需求的消息；如果在交易过程中发生通信信道中断，消费者或商家在等待一段合理时间后，可单方中止支付协议的执行。各参与方之间执行的子协议如图 1 所示。

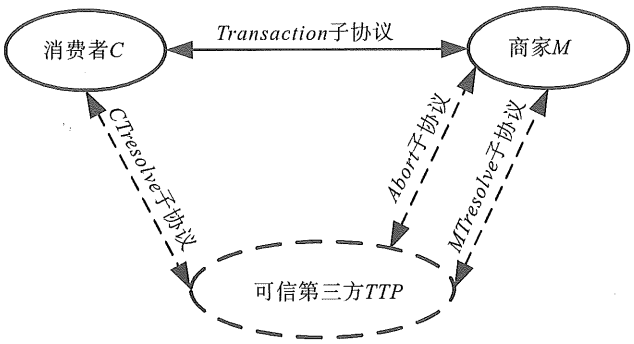

图 1 交互确认机制的公平电子现金交易协议

Fig. 1 Fair e-cash transaction protocol based on interactive confirmear scheme

1 交互确认机制构建

1.1 注册（Registration）

在执行交互确认方案前，消费者 C 需到 TTP 处注册一次，方可与商家 M 执行该方案。通过注册，便于可信第三方 TTP 对消费者 C 的身份进行确认。同时，协议的三个主体均掌握一定的初始化信息，如各自的私有密钥、公开密钥，由 CA 中心颁发的数字证书 $Cert_Z$。

在转换不可否认签名方案中，Z_n^* 是整数模 n 的乘法群，p,p',q,q' 都是素数，$n = pq$；$\varphi(n)$ 是 Euler 函数，$\gcd(n,\varphi(n)) \equiv 1$；，其中 $p = 2p' + 1$，$q = 2q' + 1$。根据签名方案，C 的公私钥 $c,d,e(c < n, e < n)$ 满足：

$$cde \equiv 1(\bmod \varphi(n)n)\text{，且 } de \neq 1(\bmod \varphi(n))\text{；}$$

$$\gcd(c,n) = \gcd(c,\varphi(n)) = \gcd(e,n) = \gcd(e,\varphi(n)) = 1\text{；}$$

对于被加密消息 m，并且公私钥 c,d,e 也必须满足下列条件：

$$\forall m < n^2 : m^{cde} \equiv m(\bmod n^2)$$

$$\forall m < n : m^{cde} \equiv m(\bmod n)$$

具体的注册过程共分为 R_1，R_2 两个步骤：

$$R_1 : C \rightarrow TTP : Cert_C, \zeta, S_a(\zeta),$$

$$Enc_T((d/a,r),((e,n),c))$$

C 随机选取消息 ζ，$\zeta < n^2$ 且 $\gcd(\zeta,n) = 1$，$\gcd(\zeta \pm 1) = 1$。在 Z_n^* 中随机选取随机数 a，$0 < a < n^2$ 且满足 $\gcd(a,n^2) = 1$，即 a 与 n^2 互素；再随机选取安全参数 $r(r \neq 0)$。采用转换不可否认签名方案，计算 $S_a(\zeta) = \zeta^{a/r} n^r (\bmod n^2)$，其中 $0 < S_a(\zeta) < n^2$。用 TTP 的公钥加密 d/a，r 以及 C 的公钥 (e,n)，得到 $Enc_T((d/a,r),((e,n),c))$，发送消息流 $Cert_C,\zeta,S_a(\zeta),Enc_T((d/a,r),((e,n),c))$ 给可信第三方 TTP。

$$R_2 : TTP \rightarrow C : Sign_T(Cert_C, \zeta, S_a(\zeta))$$

可信第三方验证 ζ 是否符合要求，即 $\zeta < n^2$，$\gcd(\zeta,n) = 1$ 且 $\gcd(\zeta \pm 1,n) = 1$；并利用自己的解密私钥 SK_T 对消息 $Enc_T((d/a),((e,n),c))$ 进行解密；同时，利用安全参数 d/a 和 r，将 $S_a(\zeta)$ 转换为 $Sign_C(\zeta) = \zeta^d (\bmod n^2)$。用 C 的公钥 (e,n) 和 TTP 拥有的 RSA 转换签名方案中的验证密钥 c，检验签名是否有效，即 $\zeta \stackrel{?}{=} sign_C(\zeta)^{ce} (\bmod n^2)$。如果签名有效，对消息流 $(Cert_C, S_a(\zeta), \zeta)$ 进行数字签名，传送给 C。可信第三方可利用 $d/a, r$ 解决将来可以产生的纠纷。其中 $(\zeta, S_a(\zeta))$ 称为不可否认签名对。

1.2 ICSP 交互确认协议

交互确认方案用于商家 M 验证 C 所声称的不可否认签名的有效性，即 C 要使 M 确信可信第三方 TTP 可以把 $S_a(m)$ 转化成为一般的数字签名 $Sign_C(m)$。在该方案中，C 向 M 发送消息：

$$C \rightarrow M : m, S_a(m), Sign_T(CertC, \zeta, S_a(\zeta))\text{。}$$

在注册阶段 C 选择的安全参数 r 和 a，将消息 m 采用类似计算 $S_a(\zeta)$ 的方式计算出 $S_a(m)$。$S_a(m) = m^{d/a} n^r (\bmod n^2)$，$\gcd(S_a(m),n) = \gcd(m,n) = 1$。$(m, S_a(m))$ 是由消费者声明有效

的不可否认签名对，并组成消息流，$m,S_a(m)$，$Sign_T(Cert_C,\zeta,S_a(\zeta))$ 发送给 M；M 采用 TTP 公有密钥验证 $Sign_T(Cert_C,\zeta,S_a(\zeta))$ 的有效性。利用交互确认方案使商家 M 相信可信第三方 TTP 将 $S_a(m)$ 转换为采用公钥可验证的一般数字签名方案。具体方案如下：

$$P_1:M\rightarrow C:Q$$

商家选取两个随机数 α,β，其中 $\alpha<n^2$，$\beta<n^2$，其中 α 为素数，$\gcd(\beta,n)=1$，计算 $Q=m^{\alpha}/\zeta^{\beta}(\bmod n^2)$，把 Q 发送给消费者 C；

$$P_2:C\rightarrow M:P$$

C 随机选取 $u<\varphi(n)n/2$，计算 $P=Q^u(\bmod n^2)$ 发送给 M；

$$P_3:M\rightarrow C:v$$

M 随机选取 $v,v<n^2$，且 $\gcd(v,n)=1$，发送 v 给 C；

$$P_4:C\rightarrow M:x$$

C 收到 v 后，计算 $x=u+a/r\cdot v(\bmod(\varphi(n)n/2))$，将 x 传给 M。M 验证公式（1）是否成立。

$$Q^x\stackrel{?}{=}P(S_a(m)^{\alpha}/S_a(\zeta)^{\beta})^v n^{\beta-\alpha}(\bmod(n^2)) \quad (1)$$

如果成立，则认为 $S_a(m)$ 与 $S_a(\zeta)$ 是对应于同一个参数 a，经过相同的计算方式得出的；否则，拒绝中止协议进行。

不可否认数字签名对 $(S_a(m),m)$ 不能采用 $Cert_C$ 中消费者 C 的公有密钥直接进行验证其有效性。只有在可信第三方的帮助下，利用转换签名方案将 $(S_a(m),m)$ 转换成为 $Sign_C(m)$，M 才能利用消费者 C 的公有密钥对消息 m 的签名进行验证。具体过程：

$$M\rightarrow TTP:Cert_C,m,S_a(m)$$

M 将消息流 $Cert_C,m,S_a(m)$ 发送给可信第三方 TTP。可信第三方 TTP 将利用在注册阶段得到的安全参数 d/a，r 和私有转换签名密钥 c，对不可否认签名 $S_a(m)=m^{\frac{a}{r}}n^r(\bmod n^2)$ 进行转换：

$$Sign_C(m)=[(S_a(m)/n^r)^{dr/a}]^c=m^{cd}(\bmod n^2) \quad (2)$$

从式（2）可以得到有效的标准 RSA 的数字签名方案。将 $Sign_d(m)$ 发送给 M，M 获得 $Sign_d(m)$ 之后，采用 $Cert_C$ 提供的公钥 (e,n) 可对数字签名进行验证。

由 $ed\neq 1(\bmod\varphi(n)n)$，则验证签名过程为：

$$Sign_C(m)^e=[(S_a(m)/n^r)^{dr/a}]^{ec}=m^{ecd}(\bmod n^2)=m(\bmod n)$$

1.3　交互确认方案的安全性分析

在方案的安全性分析过程中，假设计算离散对数和破译 RSA 密码算法困难的基础上。

定理 1　已知 C 用安全参数 a 通过注册过程计算方式得到 $S_a(\zeta)$。如果 $S_a(m)$ 也是 C 用参数 a 通过相同的计算方式得到的。通过交互确认方案，M 相信可信第三方可将 $S_a(m)$ 转换为一般可验证的数字签名。

证明　由交互确认方案可知，M 随机选择 α,β，满足：$\alpha<n^2,\beta<n^2$，其中 α 是素数，$\gcd(\beta,n)=1$，使 $Q=m^{\alpha}/\zeta^{\beta}(\bmod n^2)$。$C$ 得到 Q 之后，选取 $u<\varphi(n)n/2$，计算 $P=Q^u=(m^{\alpha}/\zeta^{\beta})^u(\bmod n^2)$。$M$ 得到 P 之后，选取 $v<n^2$，$\gcd(v,n)=1$，将 v 发送给 C。C 得到 v，计算 $x=u+a/(r\cdot v)(\bmod n^2)$，并将 x 传给 M。M 验证 $Q^x=Q^u\cdot Q^{a/r\cdot v}(\bmod n^2)=P\cdot(m^{\alpha}/\omega^{\beta})^{a/r\cdot v}(\bmod n^2)=P\cdot[m^{(a/r)\alpha}/(\omega^{a/r})^{\beta}]^v(\bmod n^2)=P\cdot[S_a(m)^{\alpha}/S_a(\omega)^{\beta}]^v\cdot[n^{\beta-\alpha}]^v\bmod(n^2)$，所以 M 相信可信第三方可将 $S_a(m)$ 转换为一般可验证的数字签名。证毕。

定理 2　已知 C 用参数 a 通过注册过程的计算方式得到 $S_a(\zeta)$。如果 $S_{a'}(m)$ 是消费者用另一参数 a'（选取方式与 a 相同，且 $a\neq a'$）得到的。通过交互确认方案，M 不会接受 $S_{a'}(m)$。

证明　如果 $S_{a'}(m)$ 不是消费者 C 用注册阶段计算方式得到的，要使 M 接受 $S_{a'}(m)$ 的合法性，就必须使 $Q^x=P\cdot[S_a(m)^{\alpha}/S_a(\zeta)^{\beta}]^v\cdot[n^{\beta-\alpha}]^v\bmod(n^2)$ 成立。如果 C 和 M 都严格遵循协议进行交互认证的情况下，从下面的证明过程可知 M 是不会接收 $S_{a'}(m)$ 的合法性的。由交互确认该方案可知：

$$P\cdot[(S_{a'}(m)^{\alpha})/S_a(\zeta)^{\beta}]^v[n^{\beta-\alpha}]^v(\bmod n^2)=P\cdot[(m^{a'/r})^{\alpha}\cdot n^{\alpha r}/((\zeta^{a/r})^{\beta}\cdot n^{\beta r})]^v[n^{\beta-\alpha}]^v\bmod(n^2)=P\cdot[(m^{a\alpha})/(\zeta^{a'\beta})]^{v/r}(\bmod n^2)$$

而 M 计算 $Q^x=P\cdot(m^{\alpha}/\zeta^{\beta})^{av/r}(\bmod n^2)$。

根据题设 $a\neq a'$，所以 $Q^x\neq P\cdot[(m^{a\alpha})/(\zeta^{a'\beta})]^{v/r}(\bmod n^2)$。因为 α,β 都是 M 随机选取的，m^{α}/ζ^{β} 具有一定的随机性，而且 v 是 M 选取的随机数，所以 C 是无法直接最后得到正确的结果 Q。因此，M 不相信可信第三方将 $S_{a'}(m)$ 转换为一般的可验证的数字签名。证毕。

定理 3　在交互确认方案中，不会泄漏参数 d/a，r，即只能由可信第三方将 $S_a(m)$ 转化为 $Sign_C(m)$。（即不泄漏 $d/a,r$）。

证明　$d/a,r$ 是消费者 C 用可信第三方 TTP 公钥加密的形式 $Enc_T((d/a,r),((e,n),c))$ 发送

给 *TTP*，所以在传输过程不会泄漏 $S_a(m)$ 与 $Sign_C(m)$。由签名方案和 $S_a(m)$ 的计算过程得知，无法从 $S_a(m)$ 和 $Sign_C(m)$ 得到 d/a 和 r 的信息；而在交互确认方案中并没有涉及私钥 d 和参数 a。所以，除 C 和可信第三方 *TTP* 之外，没有人得知 d/a 和 r，即只能由可信第三方 *TTP* 把 $S_a(m)$ 转化为 $Sign_C(m)$。证毕。

定理4 在方案中，M 无法向除 C，*TTP* 之外的第三者证明 $S_a(m)$ 的有效性。

证明 在交互确认方案中，引入安全参数 r 和参数 u，M 无法知道 a/r 的值，所以在方案中，除 C 和 *TTP* 之外，a/r 不会泄漏给第三者。也就是说，M 只有在 C 的帮助下才能验证 $S_a(m)$ 的有效性，M 无法向除 C，*TTP* 之外的第三者证明 $S_a(m)$ 的有效性。证毕。

定理5 在交互确认方案中，如果 C 用参数 a 对另一消息 $m'(m \neq m')$，采用注册阶段的计算方式得到 $S_a(m')$。通过交互确认方案，M 是不会接受 $S_a(m')$ 的合法性的。

证明 C 选取 $m'(m \neq m')$，用参数 a 采用注册阶段的计算方式得到的 $S_a(m')$。假设 M 接受了 $S_a(m')$。由于 $S_a(m') \neq S_a(m)$，则 $S_a(m')$ 可表示为：$S_a(m') = (\xi m)^{a/r} \cdot n^r (\mathrm{mod}\ n^2)$，其中 $\xi \in \mathbb{Z}_n^*$，且 $\xi \neq 1$。

利用交互确认方案中公式（1），右边 $= P \cdot [S_a(m')^{\alpha}/S_a(\omega)^{\beta}]^{av/r} \cdot [n^{\beta-\alpha}]^{v} (\mathrm{mod}\ n^2)$

由于 α 是一个素数，只要 $\alpha < n^2$，是一定不存在 $\xi \in \mathbb{Z}_n^*$，$\xi = 1(\mathrm{mod}\ n^2)$，可得到 $\xi^a \neq 1(\mathrm{mod}\ n^2)$。如果 C 能够选择正确 x_1, x_2，且 $x_1 \neq x_2$，那么

$$P \cdot [S_a(m')^{\alpha}/S_a(\zeta)^{\beta}]^{a(v_1-v_2)/r} \cdot [n^{\beta-\alpha}]^{v_1-v_2} (\mathrm{mod}\ n^2) = P \cdot [(\xi m)^{\alpha}/\zeta^{\beta}]^{a(v_1-v_2)/r} (\mathrm{mod}\ n^2) = P \cdot (\xi)^{\alpha(v_1-v_2)} \cdot [(m)^{\alpha}/\zeta^{\beta}]^{a(v_1-v_2)/r} (\mathrm{mod}\ n^2)$$

则由公式（1）和公式（2）两式可得：

$$Q^{x_1-x_2}/(P \cdot [(m)^{\alpha}/\zeta^{\beta}]^{a(v_1-v_2)/r}) = \xi^{(v_1-v_2)} (\mathrm{mod}\ n^2) \quad (3)$$

公式（1）左边 $= Q^{x_1-x_2} = P \cdot [(m)^{\alpha}/\zeta^{\beta}]^{a(v_1-v_2)/r} (\mathrm{mod}\ n^2)$ (4)

由公式（3）和公式（4）可得：

$$P \cdot [(m)^{\alpha}/\zeta^{\beta}]^{a(v_1-v_2)/r}/(P \cdot [(m)^{\alpha}/\zeta^{\beta}]^{a(v_1-v_2)/r}) = \xi^{(v_1-v_2)} (\mathrm{mod}\ n^2)$$

验证结果 $\xi^{(v_1-v_2)} (\mathrm{mod}\ n^2) = 1$。但是根据定理5的题设，$\xi^{(v_1-v_2)} (\mathrm{mod}\ n^2) \neq 1$，出现结果与题设相矛盾的情况。所以，商家 M 是不会接受 $S_a(m')$ 的合法性的。证毕。

2 基于交互确认机制的公平电子现金交易协议

公平电子现金交易协议采用 Brands 电子现金方案[12]，是目前高效电子现金方案之一。执行提取现金之后，消费者得到电子现金 $Coin = (A, B, Sign_B(A,B,M_p))$，其中 $Sign_B(A,B,M_p) = (z,a,b,r)$ 是银行对该电子现金的数字签名，并满足 $g^r = h^{H_0(A,B,z,a,b,M_p)} \cdot a$ 和 $A^r = z^{H_0(A,B,z,a,b,M_p)} \cdot b$。为讨论方便，各子协议所使用的主要标记符号列于表1。

表1 协议中的符号标记

Table 1 Notation Summary

符号	含义	符号	含义
$SK\_Z, Z \in (C,M,T)$	Z私有密钥	msg	订购的数字商品
$PK\_Z, Z \in (C,M,T)$	Z的公有密钥	TID	交易的唯一标识
$Sign_Z Z \in (C,M,T)$	Z的数字签名	$PRICE$	订购商品的价格
$ORDER$	订购商品的定单	$DESC$	订购商品的描述
$Random()$	随机函数	$h()$	强单向 Hash 函数
$ID_Z Z \in (M,T)$	商家和 TTP 的标识	M_p	支付的总额

2.1 Transaction 协议

交易协议完成在正常情况下，消费者支付电子现金并得到订购的数字商品；商家 M 发送数字商品之后，获得支付的电子现金和消费者确认收到商品的应答消息，以确认完成交易协议性。在交易协议中，数字商品的发送有机的融合到支付过程中，并将订购商品的描述通过 *Hash* 函数嵌入支付的现金，使可信第三方 *TTP* 将支付现金与交易相对应。

步骤1：消费者订购商品

1）消费者提取交易时间戳，并与商家标识 ID_M 一起生成此次交易的唯一标识：$TID = Random(ID_M, DATE/TIME)$；

2）订单 *ORDER* 包括预先协商好价格 *PRICE*，订购商品的描述 *DESC*；生成收到订购商品应答消息 $msg_2 = (TID, ORDER)$；利用交互确认方案中注册阶段的转换不可否认签名计算 $S_a(msg_2) = (msg_2)^{d/a} \cdot n^r (\mathrm{mod}\ n^2)$，形成消息流 $m_{C1} := msg_2, S_a(msg_2), Sign_{TTP}(\zeta, S_a(\zeta))$ 发送给商家。

3）消费者本地保存订单，以及订购商品的 *Hash* 值 $m_T = Sign_T(h(msg))$，作为验证订购商品内容和品质的证据。

步骤2：商家发送加密的订购商品。

1）商家收到 m_{C1} 后，执行提出交互确认该方案，验证 $Q^x \stackrel{?}{=} P \cdot [S_a(msg_2)^{\alpha}/S_a(\zeta)^{\beta}] \cdot n^{(\beta-\alpha)} (\mathrm{mod}$

n^2），确认可信第三方能够将消费者的不可否认 $S_a(msg_2)$ 转换为一般的可验证签名，作为消费者收到订购商品的不可否认证据；

2）商家计算 $NRT_M = h(TID, DESC, PRICE, DATE/TIME, ID_M)$；随机选择 $\omega \in_R Z_q^*$，令 $W = g^{\omega} \bmod n$，$V_T = msg(PK\_T)^{\omega} \bmod n$，$V = (msg)^{v} \bmod n$，$V_S = (V_T)^{v} \bmod n$；随机选择 $u \in_R \{1,2,\cdots,q-1\}$，令 $k = g^{u} \bmod n$，$K = ((PK\_T)^{v})^{u} \bmod n$，$r = u - l\omega$，则 $c = H(g \| W \| (PK\_T)^{v} \| V_S/V \| k | K)$；

3）商家签名 $(ID_M, NRT_M, TID, ORDER, DATE/TIME) \| (W, V_T) \| (r, l, V)$，得 $Sign_M((ID_M, NRT_M, TID, ORDER, DATE/TIME) \| (W, V_T) \| (r, l, V))$，并发送给消费者；

4）商家本地保存 NRT_M，$ORDER$，(W, V_T)，(r, l, V)，V, V_T, V_S，$DATE/TIME$。

步骤 3：消费者接收加密商品并支付

1）消费者接收到商家发送的数据包 m_{M1}，利用商家公开密钥验证商家的数字签名，解析数据包；

2）$NRT_C = h(TID, ORDER -> DESC, ORDER -> PRICE, DATE/TIME, ID_M)$，验证 $NRT_C \stackrel{?}{=} m_{M1} -> NRT_M$ 是否相等，以确保商家认可此次交易，以及比较 ID_M 为所期望商家标识；若不相等，取消此交易，执行 Abort 协议；否则继续执行如下步骤；

3）由 (W, V_T) 和 (r, l, V) 可计算出 (W, V_S)，验证 $k \stackrel{?}{=} g^{r} W^{c} \bmod n \stackrel{?}{=} g^{u} \bmod n$，$((PK\_T)^{v})^{r} (V_S/V) \bmod n \stackrel{?}{=} ((PK\_T)^{v})^{u} \bmod n \stackrel{?}{=} K$，$l \stackrel{?}{=} H(g \| W \| (PK\_T)^{v} \| V_S/V \| k \| K)$，以保证 (r, l, V) 是订购商品 msg 的 CEMBS 的可验证加密；若等式不成立执行 *Abort* 协议；

4）消费者计算 $A_1 = g_1^{u_1 s}$，$A_2 = g_2^{s}$ 及支付电子现金 $COIN = (A, B, M_p, Sign_B(A, B, M_p))$；再随机选择 $s_1, s_2 \in_R Z_q$，并计算 $t = H_2(A_1, A_2, M_p, DATE/TIME)$，$n_1 = g_1^{ts_1}$，$n_2 = g_2^{ts_2}$，并随同电子现金一起发送给商家；

5）商家验证支付的电子现金是否为银行所发以及 A_1, A_2 的构造是否正确，并计算 $d = H_1(A, A_1, A_2, B, ID_M, DATE/TIME, DESC)$，发送给消费者生成有效的支付信息，其中包含 ID_M 和 $DESC$ 作为消费者订购商品的非否认证据，使可信第三方确认此笔现金对应该笔交易；

6）消费者计算 $r_1 = d_1 u_1 s + s_1 \bmod q$，$r_2 = d_1 s + s_2 \bmod q$，形成由商家和消费者共同构成的有效支付信息 r_1, r_2，发送给商家；消费者本地保存 $r_1, r_2, t, M_p, DATE/TIME$；

7）商家验证等式 $g_1^{r_1} \stackrel{?}{=} A^{d_1} n_1^{1/t}$，$g_2^{r_2} \stackrel{?}{=} A_2^{d_1} n_2^{1/t}$，确认 r_1, r_2 是否为有效的支付信息，$M_p \stackrel{?}{=} PRICE$ 支付金额是否与价格相等；商家本地保存 $A_1, A_2, B, M_p, DATE/TIME, n_1, n_2, r_1, r_2$。

步骤 4：商家发送订购商品。

1）商家利用消费者的公钥加密订购商品 $Enc_C(msg)$；

2）并利用私有签名密钥签名，得数据包 $Sign_M(TID, Enc_C(msg))$，将其发送给消费者。

步骤 5：消费者发送收到订购商品确认信息

消费者在等待一段合理时间后，没有收到商家发送的订购商品，执行 CTresolve 协议，否则执行下列步骤：

1）用商家的签名公开密钥 PK_M 验证其签名，解析数据包，得到订购商品 msg；计算 $h(msg)$，并解密 $m_T = Sign_T(h(msg))$，并验证 $m_T -> h(msg) \stackrel{?}{=} h(msg)$；

2）如果相同，向商家发送收到订购商品的确认信息 $Sign_C(msg_2)$；否则，消费者向可信第三方发送数据包 $\tilde{m}_C$ 执行 CTresolve 协议。

3）商家在等待一段合理的时间后，仍没有收到消费者订购商品的确认信息，则执行 MTresolve 协议；否则，Transaction 协议结束。

2.2　CTresolve 协议

在交易协议执行过程中，由于交易商家的不诚实，例如商家收到消费者的有效支付，不发送消费者订购的商品，消费者在等待一段合理的时间后，执行 CTresolve 协议。

步骤 1：消费者向 *TTP* 发送不可否认消息 $\tilde{m}_C := m_{C2} | (d_1, A) | m_T | Sign_C(msg_2)$

步骤 2：可信第三方的验证及解密

1）可信第三方收到消费者的数据包，用消费者的公钥 PK_C 验证数据包 $\tilde{m}_C$，并解析数据包；计算 $NRT_T = h(TID, DESC, PRICE, DATE/TIME, ID_M)$，并验证 $NRT_T \stackrel{?}{=} \tilde{m}_C -> NRT_C \stackrel{?}{=} m_{M1} -> NRT_M$ 是否成立；若相等，则表明消费者没有修改交易数据，双方均认可此次交易；否则，取消本次交易的运行；

2）可信第三方首先以 NRT_C 为索引查找交易记录，如果此交易记录存在，则发送对应协议的运行结果；否则，可信第三方解析数据包，得到消费者支付的电子现金 $COIN$，并利用 $\tilde{m}_C$ 数据包中的

相关数据，计算 $d_1 = H_1(A, A_1, A_2, B, ID_M, DATE/TIME, DESC)$，比较 $\widetilde{m}_C -> d_1 \stackrel{?}{=} d_1$ 确认该支付现金对应此笔交易；

3）利用扩展 CEMBS 加密验证算法，用私钥 SK_T 解密订购商品 $\xi = W^{SK\_T} \bmod n$，并使其公钥加密 ξ，得到 $Enc_C(\xi)$，发送给消费者；消费者收到 $Enc_C(\xi)$ 后，通过计算 $msg = V_T/\xi \bmod n$，得订购数字商品。

步骤3：可信第三方同时转发 $Sign_C(msg_2)$ 及 $COIN$ 给商家，作为消费者收到订购商品的确认信息，从而协议达到公平性。

2.3 MTresolve 协议

支付过程中，由于通信信道中断或交易消费者不诚实，例如：消费者收到商家发送的订购商品，并没发送收到订购商品的确认信息，则商家在等待一段合理的时间后，执行 MTresolve 协议，具体执行步骤如下：

步骤1：商家向 TTP 发送不可否认消息 $\widetilde{m}_M = m_{C1} \| m_{C2} \| m_T \| Enc_{TTP}(msg)$；

步骤2：可信第三方的验证及转换不可否认签名

1）可信第三方收到商家的数据包 $\widetilde{m}_M$ 后，解析数据包；

2）计算 $NRT_T = h(TID, DESC, PRICE, DATE/TIME, ID_M)$，并验证 $NRT_T \stackrel{?}{=} m_{C2} -> m_{M1} -> NRT_M \stackrel{?}{=} m_{C2} -> NRT_C$ 等式是否成立；如果成立，则表明商家没有修改交易数据，双方认可此次交易；

3）可信第三方首先以 NRT_M 为索引查找交易记录，如此交易记录存在，则发送对应协议的运行结果；

4）可信第三方 TTP 用私钥 SK_TTP 解析 $Enc_{TTP}(msg)$ 计算 $h(msg)$，比较 $h(msg) \stackrel{?}{=} m_T -> h(msg)$，并与商家发送的商品相比较；如果相同，则用消费者公钥加密消费者订购商品 msg 送给消费者。

步骤3：可信第三方 TTP 提取 $m_{C1} -> S_a(msg)$，将其转换为一般可验证签名 $Sign_C(msg_2)$；同时向商家发送，作为消费者收到订购商品的非否认证据。

2.4 Abort 协议

在交易协议中，消费者在接收消息 m_{M1} 之后，验证 $NRT_C \stackrel{?}{=} m_{M1} -> NRT_M$，如果不相等，表明商家不同意此次交易，或由于通信信道中断等原因，在等待一段合理时间之后，仍没有消息，则执行 Abort 协议，取消本次交易。

步骤1：消费者向可信第三方发送消息 $m_{M1} \| m_{C1}$ 取消协议。

步骤2：可信第三方验证及发送 Abort 消息

1）可信第三方 TTP 比较 $NRT_C \stackrel{?}{=} m_{M1} -> NRT_M$，如果不相等，则取消本次交易；

2）可信第三方 TTP 向消费者发送 $Sign_T(Abort, TID)$，取消本次交易；同时，也向商家发送 $Sign_T(Abort, TID)$ 通知商家取消本次交易，并保存 $m_{M1} \| m_{C1}$ 作为取消本次交易的证据。

3 交易协议的属性分析

3.1 公平性分析

基于交互确认机制的电子现金交易协议满足公平性，即在交易双方不诚实的情况下，可信第三方使用扩展 CEMBS 算法和交互确认方案，完成交易确认的签名转换，使其对加密商品具有恢复能力，并依据订购商品的确认信息分别向消费者和商家发送各自需求的消息，以达到协议公平性。现对该协议公平性详细分析如下：

1）如果消费者与商家行为都是正确的，并且通信信道都是可靠的，消费者在发送有效的支付信息后，能够得到订购数字商品 $Enc_C(msg)$；商家也可以得到消费者有效支付，并收到消费者收到订购商品的确认信息 $Sign_C(msg_2)$。协议满足公平性，同时没有破坏协议的匿名性。

2）在通信信道中断和商家不诚实情况，即当消费者发送消息 m_{C1} 之后，在等待一段合理时间之后或者商家不同意此次交易，则发送 $m_{C1} \| m_{M1}$ 激活 Abort 协议，取消本次交易。TTP 不再接收 MTresolve 协议的请求，根据公平性的定义，显然协议也是满足公平性的。由于商家不诚实，消费者得到可验证的加密商品后，向商家进行了有效支付。在等待一段合理时间之后，消费者并没有从商家得到订购商品，消费者使用 $\widetilde{m}_C$ 调用 CTresolve 协议。TTP 判定 $NRT_T \stackrel{?}{=} m_{C1} -> NRT_C \stackrel{?}{=} m_{M1} -> NRT_M$ 相应条件后，表明商家和消费者均同意此次交易。利用扩展 CEMBS 验证算法可解析数据包，并向消费者发送 $Enc_C(\xi)$。消费者利用 $msg = \frac{V_T}{\xi} (\bmod n)$ 可得到订购商品 msg。同时可信第三方 TTP 将消费者支付现金 $COIN$ 以及消费者收到订购商品的确认信息发送给商家，从而在通信中断或商家不诚实情况下，协议满足公平性。

3）由于消费者的不诚实，交易协议仍然满足

公平性。从支付协议执行过程可以看出，对商家不存在没有得到有效支付而发送订购商品的情况。如果商家得到消费者的有效支付，向消费者发送其订购商品 $Enc_C(msg)$ 之后，商家由于通信信道中断或由于消费者不诚实，没有从消费者收到确认收到商品的信息。这时商家发送消息流 $m_{C1} \| m_{C2} \| m_T \| Enc_T(msg)$ 激活 MTresolve 协议。可信第三 *TTP* 方进行 $m_T -> h(msg) \stackrel{?}{=} h(msg)$ 的比较，如果相等，利用交易确认方案将不可否认签名 $S_a(msg_2)$ 转换为 $Sign_C(msg_2)$，并发送给商家 M，作为消费者收到订购商品的确认信息。同时，*TTP* 将 $Enc_C(msg)$ 发送给消费者，从而达到协议的公平性。

3.2　匿名性分析

匿名性是电子现金交易协议的基本要求，也是电子现金交易协议交易的最大优点。基于交互确认机制的电子现金交易协议在满足公平性的同时，即保护合法消费者匿名性和隐私权，并没有破坏协议的匿名性。即消费者对商家和银行是完全匿名的，商家不会根据支付信息中 A'_1, A'_2, A, B, M_p，$Sign_B(A, B, M_p)$ 计算出消费者身份字密钥 u 和提取该电子现金的密钥 s，合法消费者的匿名性和隐私在协议中得到保护。

但是任何企图进行非法交易的消费者，本协议利用现金跟踪和提款人跟踪，可揭露其身份，去除其匿名性。交易协议在现金跟踪中，本协议根据提款信息，可以识别该电子现金。银行向 *TTP* 传递信息，*TTP* 根据 A'_2 计算 $(A'_2)^{(X_T^{-1})} = (h_T^s)^{X_T^{-1}} = (g_2^{s \cdot X_T})^{X_T^{-1}} = g_2^s = A_2$，并把 A_2 返回给银行。同时向银行证明 $\log_{g_2} h_T = \log_{A'_2} A_2$。银行可识别电子现金，监视敲诈、勒索等不法行为。在消费者的跟踪过程中，本协议用于揭露伪造电子现金或洗黑钱不法消费者的身份。银行向 *TTP* 传送支付信息，*TTP* 计算 $A_2^{X_T} = (g_2^s)^{X_T} = (g_2^{X_T})^s = h_T^s = A'_2$，并把 A'_2 返回给银行。同时，向银行证明 $\log_{g_2} h_T = \log_{A'_2} A_2$，银行将根据 A'_2 找到消费者的身份字 I。最后，可根据 I 在消费者账户找到该消费者，从而揭露其匿名性。

4　结束语

在充分考虑通信信道可靠性和交易双方诚实的情况下，借鉴不可否认转换签名的思想，提出一种离线可信第三方的公平电子现金交易协议。该协议基于 CEMBS 可验证加密算法和交互确认方案，有效解决电子现金交易协议的公平性和匿名性之间的矛盾，通过分析表明协议既满足公平性又满足匿名性，从而保护了交易双方的利益；同时，可信第三方 *TTP* 采用离线方式，减少了协议数据存贮量，提高了协议执行效率；最后，协议运行过程中，可由参与实体单方中止协议的执行，从而能够避免交易双方无限等待，防止交易处于模糊状态。本文的研究为电子现金公平交易协议的设计提供了新的思路和方法。

参考文献：

[1] 周展飞，周典萃，王贵林，等. 电子商务协议的公平性[J]. 电子学报，2000，28(9)：13－15.

[2] CHAUM D, FIAT A, NAOR M. Untraceable electronic cash[C]. Proceeding in cryptology-crypto'88, California: Springer-Verlag, 1990: 319－327.

[3] RIVEST R L, SHAMIR A. Payword and micromint: two simple micropayment scheme[C]// Proceeding of 13th Ann EUROCRYPT Conference Theory and Applications of Cryptologic Techniques, 1996: 69－87.

[4] TYGAR J D. Atomicity versus anonymity: distributed transactions for electronic commerce[C]. Proceedings of the Twenty-fourth International Conference on Very Large-Databases, IEEE Press, 1998: 1－12.

[5] CAMP J. An atomicity-generating protocol for anonymous currencies[J]. IEEE Transactions on Software Engineering, 2001, 27(3): 272－278.

[6] ABOUD S. Anonymous and non-repudiation e-payment protocol[J]. American Journal of Applied Sciences, 2007, 4(8): 538－542.

[7] WANG C H. The design of a novel e-cash system with the fairness property and its implementation in wireless communications[J]. Journal of Computers, 2007, 18(2): 47－59.

[8] 韩志耕，罗军舟. 一个公平的多方不可否认协议[J]. 计算机学报，2008，31(10)：1705－1715.

[9] MAO W, PATERSON K. Convertible undeniable standard RSA signatures [C]//Cryptology-Cryptographers' Track, RSA Conference 2000, Springer-Verlag, 2000: 200－217.

[10] 邓所云，詹榜华，胡正名等. 一个优化的公平的电子支付方案[J]. 计算机学报，2002，25(10)：1094－1098.

[11] WANG Q, YANG D L. Anonymous and atomic e-cash transaction protocol with off-line TTP[J]. Journal of Harbin Institute of Technology, 2004, 11(5): 558－563.

[12] BRANDS S. Untraceable off-line cash in wallets with observers[C]. Proceeding Advanced in Cryptology-Crypto'93, California: Springer-Verlag, 1993: 302－318.