通用可组合的公平电子支付协议

邓淼磊[①] 王玉磊[②] 周利华[①]
[①](西安电子科技大学计算机学院 西安 710071)
[②](南阳理工学院网络信息中心 南阳 473009)

摘 要：公平性是电子支付协议的一个基本属性。该文基于通用可组合模型，定义了公平电子支付理想函数。在可转化签名理想函数、注册理想函数和安全会话理想函数辅助的混合模型下，构造了一个实现公平电子支付理想函数的公平电子支付协议。新的协议结构简单，通信量较低，并且在任意的和未知的多方环境中运行时仍然是安全的。

关键词：电子支付协议；公平性；通用可组合
中图分类号：TN918 **文献标识码**：A **文章编号**：1009-5896(2009)05-1063-04

Universally Composable Fair Electronic Payment Protocol

Deng Miao-lei[①] Wang Yu-lei[②] Zhou Li-hua[①]
[①](*College of Computer Science*, *Xidian University*, *Xi'an* 710071, *China*)
[②](*Network Information Center*, *Nanyang Institute of Technology*, *Nanyang* 473009, *China*)

Abstract: Fairness is an essential property in e-payment protocol. An ideal functionality of fair e-payment is defined in the universal composability model. In the hybrid model which aided by ideal convertible signature functionality, ideal registration functionality and ideal secure session functionality, a fair electronic payment protocol is constructed to realize this ideal functionality. The new protocol has simpler structure, lower communication overhead and holds secure even when running in an arbitrary and unknown multi-party environment.

Key words: Electronic payment protocol; Fairness; Universal composition

1 引言

电子支付是电子商务的一个重要应用，而公平性是它的一个关键属性。公平电子支付协议从广义上来说属于公平交换协议。公平交换协议可以使参与交换的双方以公平的方式交换信息，这样，要么任何一方都可以得到对方的信息，要么双方都得不到对方的信息。现有的公平交换协议大致可以分为 3 类：(1)逐步秘密交换[1,2]：无需可信第三方的参与，但是要求交换双方具有相同的计算能力，并且通信和计算开销很大。(2)使用在线可信第三方(TTP)的公平交换协议[3,4]：由于使用了一个在线的 TTP 作为公平交换的基础，所以无论从计算上还是在通信上讲，TTP 都会成为一个瓶颈，并且易于遭受拒绝服务攻击。(3)使用离线 TTP 的公平交换协议[5−7]，与在线 TTP 协议不同的是，在没有异常问题的情况下，该类协议不需要 TTP 参与交易的任何一个环节，这类协议是目前公平交换协议研究的重点和热点。

现有的公平交换协议多数是研究者根据经验采用非形式化方法进行设计和分析。也有研究者利用安全协议形式化工具，如扩展 BAN 逻辑[8]，ATL 逻辑[9]，串空间模型[10]等分析公平交换协议安全性。但是，这种建立于 Dolev-Yao 模型之上的安全协议分析方法，被普遍认为没有真正建立起密码学的可靠性。基于通用可组合模型[11]，Yusuke 等人设计了一个交换数据的数字签名的公平交换协议[12]。在他们的协议中，客户需要进行大量签名运算。本文利用可转化签名技术[13,14]，设计一个通用可组合安全的使用离线 TTP 的公平电子支付协议。

2008-04-01 收到，2008-07-24 改回
国家自然科学基金(60573036)资助课题

2 通用可组合模型

通用可组合(UC)模型是用于定义协议安全性的框架，它是根据真实协议和理想协议模拟不可区分方法来定义协议安全的。模型中定义了一个可以提供某种服务的不可攻陷的理想函数 $\mathcal{F}$，虚拟参与者 P' 以及理想攻击者 $\mathcal{S}$。理想函数描述了协议的安全属性。与此相对应，在该模型中还定义了能够实现上述特殊服务的真实协议 π，实际参与者 P 以及真实环境下攻击者 $\mathcal{A}$。攻击者 $\mathcal{A}$ 可以控制实际参与者之间的所有通信。模型中利用一个环境机 $\mathcal{Z}$ 来模拟协议运行的整个外部环境(包括其他并行的协议、攻击者等)。在 UC 模型中，如果真实协议 π 可以在任何环境对于任何攻击者 $\mathcal{A}$ 都有与理想函数 $\mathcal{F}$ 同样的行为，就认为这是协议的一个安全实现。有关 UC 模型的概念和详细讨论见文献[11]。

UC 模型最重要的属性是它能够确保协议在任意的和未知的多方环境中运行时仍然是安全的。这个性质对于在电子商务环境中作为子协议运行的电子支付协议是必须的，因此，本文在 UC 模型中对其进行设计和分析。

3 公平电子支付理想函数

公平电子支付理想函数 $\mathcal{F}_{\text{FEP}}$ 中的协议主体是客户(U)和商家(M)。U 和 M 公平交换签名过的电子支票 C 和电子商品 G。函数 $f_C:\{0,1\}^*\to\{0,1\}$ 和函数 $f_G:\{0,1\}^*\to\{0,1\}$ 分别表示对 C 和 G 的验证，函数 $v(\cdot)$ 是签名验证函数，C 的签名表示为 σ_C。$\mathcal{F}_{\text{FEP}}$ 同时执行了 TTP 的功能。$\mathcal{F}_{\text{FEP}}$ 具有会话标识 sid 并且只接受具有相同会话标识的消息。$\mathcal{F}_{\text{FEP}}$ 的定义如下：

Initiate 一接收到 U 发来的消息(Initiate,sid,C)，如果 U 被攻陷，那么忽略这条消息。否则验证 sid=(U,M,sid′)和 $f_C(C)=1$，如果验证不成立，就忽略这条消息；否则，向攻击者发送(Initiate,sid,C)，当接收到攻击者发来的 ok 消息，记录(U,M,C)并向 M 发送(Initiated,sid)。

Send 一接收到 M 发来的消息(Send,sid,G)，验证 $f_G(G)=1$ 并且存在记录(U,M,C)，如果验证不成立，就忽略这条消息。否则，向攻击者发送(Sent,sid,|G|)，当接收到攻击者发来的消息(Signature,sid,C,σ_C)，验证 $v(C,\sigma_C)=1$。如果验证不成立，那么忽略 M 的消息；否则，记录(U,M,C,σ_C)和(M,U,G)，并向 U 发送(Sent,sid,G)。

Get 一接收到 M 发来的消息(Get,sid)，如果存在记录(U,M,C,σ_C)和(M,U,G)，那么向攻击者发送(Get,sid)，当接收到攻击者发来的 ok 消息，向 M 发送(Sent,sid,C,σ_C)；否则，忽略这条消息。

4 公平电子支付协议

本节设计公平电子支付真实协议 π_{FEP}，参与协议的主体除了客户和商家外，还包含一个 TTP(用 T 表示)。当客户需要从商家处购买电子商品，并且已经协商好了要购买的电子商品和价格之后，就可以通过 π_{FEP} 协议来完成客户签名过的电子支票和商家的电子商品之间的交换。在 π_{FEP} 中，当客户对电子支票进行中间签名并发送给商家以后，TTP 和客户都能将该电子支票的中间签名转化成客户对该电子支票的最终签名，这可以通过可转化签名技术来实现。而且只有拥有相应部分密钥的客户可以进行中间签名，共享另一部分密钥的客户和 TTP 可以将其转化成最终签名。商家有了客户最终签名的电子支票后才能得到相应数目的货款。下面构造可转化签名理想函数 $\mathcal{F}_{\text{CSI}}$。

4.1 可转化签名理想函数

可转化签名理想函数 $\mathcal{F}_{\text{CSI}}$ 的定义如下：

Key Generation 一接收到任一主体 P 发来的(KeyGen,sid)，验证 sid=(P,sid′)，如果不成立，就忽略这条消息；否则，向攻击者发送(KeyGen,sid)，当接收到攻击者发来的(PAgorithms,sid,s_1,v_1)，(Agorithms,sid,s_2,v_2)和(Agorithms,sid,s_3,v_2)，向 P 发送(PVerification Algorithm,sid,v_1)和(Verification Algorithm,sid,v_2)。这里 s_1，s_2 和 s_3 描述一个概率多项式时间 ITM，v_1 和 v_1 描述一个确定多项式时间 ITM。

Phaseal Signature Generation 一接收到 P 发来的(PSign,sid,m)，令 $\sigma_1=s_1(m)$，验证 $v_1(m,\sigma_1)=1$，如果验证不成立，向 P 输出 error 消息并中断；否则，记录(Phaseal,m,σ_1)，并向 P 发送(PSignature,sid,m,σ_1)。

Final Signature Generation 一接收到 P 发来的(Sign,sid,m,σ_1)，如果 $v_1(m,\sigma_1)\neq 1$，那么忽略这条消息。否则令 $\sigma_2=s_2(m,\sigma_1)$，验证 $v_2(m,\sigma_2)=1$，如果验证不成立，向 P 输出 error 消息并中断；否则，记录(Fianl,m,σ_2)，并向 P 发送(Signature,sid,m,σ_2)。

一接收到 P 发来的(Sign,sid,m)，令 $\sigma_2=s_3(m)$，验证 $v_2(m,\sigma_2)=1$，如果验证不成立，向 P 输出 error 消息并中断；否则，记录(Fianl,m,σ_2)，并向 P 发送(Signature, sid,m,σ_2)。

Phaseal Signature Verification 一接收到任一主体 Q 发来的(PVerify, sid,m,σ_1,v_1')，如果 $v_1'=v_1$，$v_1(m,\sigma_1)=1$，P 未被攻陷，并且对于任一 σ' 不存在记录(Phaseal,m,σ')，那么向 P 输出 error 消息并中断；否则，向 Q 发送(PVerified,sid,m,$v_1'(m,\sigma_1)$)。

Final Signature Verification 一接收到任一主体 Q 发来的(Verify,sid,m,σ_2,v_2')，如果 $v_2'=v_2$，$v_2(m,\sigma_2)=1$，P 未被攻陷，并且对于任一 σ' 不存在记录(Final,m,σ')，那么向 P 输出 error 消息并中断；否则，向 Q 发送(Verified,sid,m,$v_2'(m,\sigma_2)$)。

在上面构造的可转化签名理想函数中，消息 m 的中间签名是 σ_1，最终签名是 σ_2，相应的验证算法分别是 v_1 和 v_2。

4.2 协议 π_{FEP} 的构造

协议 π_{FEP} 包含两个子协议：交换子协议和争端解决子协议。U 和 M 协商好要购买的电子商品和价格后，开始运行交换子协议。首先，U 向 M 发送它的电子支票和一个签名的时戳 T_C 以及对电子支票的中间签名。接着，M 验证接收的中间签名和时戳，如果有效，就把它的电子商品和一个时戳 T_G 发送给 U。U 接收到电子商品后，如果验证有效，就向 M 发送它对电子支票的最终签名。最后，M 验证电子支票的最终签名，如果有效则接受。

若 M 在 T_G 的时间内收不到电子支票的最终签名，则 M 可以发起争端解决子协议。此时，M 把已经收到的消息和电子商品出示给 T。T 验证中间签名和电子商品，检查 T_C 是否超时，然后将中间签名转化成最终签名并发送给 M，同时将电子商品发送给 U。

下面在混合模型下构造有可转化签名理想函数 $\mathcal{F}_{\text{CSI}}$、注册理想函数 $\mathcal{F}_{\text{REG}}$、安全会话理想函数 $\mathcal{F}_{\text{SCS}}$ 辅助的公平电子支付协议 π_{FEP}，其中 $\mathcal{F}_{\text{REG}}$ 和 $\mathcal{F}_{\text{SCS}}$ 的定义见文献[11]。

协议 π_{FEP} 的描述如下：

当被输入(Initiate,sid,C)触发

(1) U 验证 sid=(U,M,sid′)，如果验证不成立，就忽略这条消息；否则，向 $\mathcal{F}_{\text{CSI}}$ 发送(KeyGen,sid_U)，这里 sid_U=(U,sid)，获得(PVerification Algorithm,sid_U,v_1)和(Verification Algorithm,sid_U,v_2)，U 向 $\mathcal{F}_{\text{REG}}$ 发送(Register,sid_U,v_1)和

(Register, sid_U, v_2)。

(2) U 向 $\mathcal{F}_{\mathrm{CSI}}$ 发送消息(PSign, sid_U, C)和(Sign, sid_U, T_C)，获得(PSignature, sid_U, C,σ_{C1})和(Signature, sid_U, T_C,σ_{TC})，U 通过 $\mathcal{F}_{\mathrm{SCS}}$ 向 M 发送(Send, sid, C,σ_{C1}, T_C, σ_{TC})。

(3) 一接收到(Send, sid, C,σ_{C1},T_C,σ_{TC})，M 验证 $f_C(C)=1$。如果验证不成立，M 中断协议。否则，M 向 $\mathcal{F}_{\mathrm{REG}}$ 发送(Retrieve, sid_U)，获得(Retrieve, sid_U, v_1)和(Retrieve, sid_U, v_2)，然后 M 向 $\mathcal{F}_{\mathrm{CSI}}$ 发送(PVerify, sid_U, C,σ_{C1},v_1)和(Verify, sid_U, T_C,σ_{TC},v_2)，获得(PVerified, sid_U, C,$v_1(C,\sigma_{C1})$)和(Verified, sid_U, T_C,$v_2(T_C,\sigma_{TC})$)。如果 $v_1(C,\sigma_{C1})=1$ 且 $v_2(T_C,\sigma_{TC})=1$，M 输出(Initiated,sid)；否则，M 中断协议。

当被输入(Send,sid,G)触发

(1) M 通过 $\mathcal{F}_{\mathrm{SCS}}$ 向 U 发送(Send,sid, G,T_G)。

(2)一接收到(Send,sid, G,T_G)，U 验证 $f_C(C)=1$。如果不成立，转到(4)；否则，U 向 $\mathcal{F}_{\mathrm{CSI}}$ 发送(Sign, sid_U, C,σ_{C1})，获得(Signature, sid_U, C,σ_{C2})，U 通过 $\mathcal{F}_{\mathrm{SCS}}$ 向 M 发送(Send, sid, C,σ_{C2})。

(3)一接收到(Send,sid, C,σ_{C2})，M 向 $\mathcal{F}_{\mathrm{CSI}}$ 发送(Verify, sid_U, C,σ_{C2},v_2)，获得(Verified, sid_U, C,$v_2(C,\sigma_{C2})$)。如果 $v_2(C,\sigma_{C2})=1$，M 通过 $\mathcal{F}_{\mathrm{SCS}}$ 向 U 发送(Verified,sid)，U 输出(Sent,sid, G)；否则，转到(4)。

(4) M 通过 $\mathcal{F}_{\mathrm{SCS}}$ 向 T 发送(Resolve,sid, C,σ_{C1},G)。

一接收到(Resolve,sid, C,σ_{C1},G)，T 验证 $f_G(C)=1$，如果验证不成立，T 中断协议。否则，T 向 $\mathcal{F}_{\mathrm{REG}}$ 发送(Retrieve, sid_U)，得到(Retrieve, sid_U, v_1)。T 然后向 $\mathcal{F}_{\mathrm{CSI}}$ 发送(PVerify, sid_U, C,σ_{C1},v_1)，获得(PVerified, sid_U, C,$v_1(C,\sigma_{C1})$)。T 验证 $v_1(C,\sigma_{C1})=1$，如果验证不成立，T 中断协议；否则，T 向 $\mathcal{F}_{\mathrm{SCS}}$ 发送(Sign, sid_U, C,σ_{C1})，获得(Signature, sid_U, C,σ_{C2})，然后 T 通过 $\mathcal{F}_{\mathrm{SCS}}$ 向 U 发送 G，U 输出(Sent,sid, G)。

当被输入(Get,sid)触发

如果 M 获得(Send,sid, C,σ_{C2})，并且 $v_2(C,\sigma_{C2})=1$，则 M 输出(Sent,sid, C,σ_{C2})。否则，M 通过 $\mathcal{F}_{\mathrm{SCS}}$ 向 T 发送(Get, sid)；一接收到(Get,sid)，T 通过 $\mathcal{F}_{\mathrm{SCS}}$ 向 M 发送(Signature, sid, C,σ_{C2})；一接收到(Signature, sid, C,σ_{C2})，M 输出(Sent, sid, C,σ_{C2})。

上面构造的协议中，σ_{TC} 是 T_C 的签名，σ_{C1} 和 σ_{C2} 分别是 C 的中间签名和最终签名。T_C 和 T_G ($T_C > T_G$)的使用实现了协议的及时终止，一旦超时参与方终止协议。

5　安全性证明

定理　根据 UC 安全的定义，在($\mathcal{F}_{\mathrm{CSI}}$, $\mathcal{F}_{\mathrm{SCS}}$, $\mathcal{F}_{\mathrm{REG}}$)辅助的混合模型下，$\pi_{\mathrm{FEP}}$ 可以安全地实现公平支付理想函数 $\mathcal{F}_{\mathrm{FEP}}$。

证明　设 $\mathcal{A}$ 是在($\mathcal{F}_{\mathrm{CSI}}$, $\mathcal{F}_{\mathrm{SCS}}$, $\mathcal{F}_{\mathrm{REG}}$)辅助的混合模型下与真实协议 π_{FEP} 交互的攻击者，可以构造一个理想过程的攻击者 $\mathcal{S}$ (称为仿真器)，使得对于任何环境机 $\mathcal{Z}$ 而言，它与攻击者 $\mathcal{A}$ 和协议 π_{FEP} 以及攻击者 $\mathcal{S}$ 和理想函数 $\mathcal{F}_{\mathrm{FEP}}$ 的交互都是不可区分的。构造的 $\mathcal{S}$ 在其内部对 $\mathcal{Z}$，$\mathcal{A}$ 以及 U 和 M 进行仿真，$\mathcal{S}$ 把 $\mathcal{Z}$ 的输入转发给 $\mathcal{A}$，把 $\mathcal{A}$ 的输出转发给 $\mathcal{Z}$。

(1)首先考虑 U 和 M 都没有被攻陷的情形：

(a)当 S 接收到 $\mathcal{F}_{\mathrm{FEP}}$ 发来的消息(Initiate,sid, C)，它的处理如下：

仿真密钥生成过程。$\mathcal{S}$ 向 $\mathcal{A}$ 发送消息(KeyGen, sid_U)，获得(PAgorithms, sid_U, s_1,v_1)，(Agorithms, sid_U, s_2,v_2)和(Agorithms, sid_U, s_3,v_2)，然后向仿真的 U 发送(PVerification Algorithm, sid_U, v_1)和(Verification Algorithm, sid_U, v_2)。

仿真签名生成和(C,σ_{C1},T_C,σ_{TC})发送过程。$\mathcal{S}$ 向 $\mathcal{A}$ 发送消息(Establish-Session,sid)；一接收到 $\mathcal{A}$ 发来的 ok 消息，向仿真的 M 发送(Establish-Session,sid)。接着 $\mathcal{S}$ 向 $\mathcal{A}$ 发送(Sent,sid,|C,σ_{C1},T_C,σ_{TC}|)；一接收到 $\mathcal{A}$ 的 ok 消息，向仿真的 M 发送(Sent,sid, C,σ_{C1},T_C,σ_{TC})。

仿真密钥检索和签名验证过程。$\mathcal{S}$ 向 $\mathcal{A}$ 发送消息(Retrieve, sid_U, v_1)和(Retrieve, sid_U, v_2)；一接收到 $\mathcal{A}$ 发来的 ok 消息，向仿真的 M 发送(Retrieve, sid_U, v_1)和(Retrieve, sid_U, v_2)。接着 $\mathcal{S}$ 向 $\mathcal{F}_{\mathrm{FEP}}$ 发送 ok 消息。

(b)当 S 接收到 $\mathcal{F}_{\mathrm{FEP}}$ 发来的消息(Send,sid,|G|)，它的处理如下：

仿真(G,T_G)的发送过程。$\mathcal{S}$ 向 $\mathcal{A}$ 发送(Send,sid, |G,T_G|)，获得 $\mathcal{A}$ 发来的 ok 消息。

仿真签名生成和(C,σ_{C2})的发送过程。$\mathcal{S}$ 向 $\mathcal{A}$ 发送(Sent, sid,|C,σ_{C2}|)；一接收到 $\mathcal{A}$ 发来的 ok 消息，向仿真的 M 发送(Sent,sid, C,σ_{C2})。

仿真(Verified,sid)的发送过程。$\mathcal{S}$ 向 $\mathcal{A}$ 发送|Verified, sid|；一接收到 $\mathcal{A}$ 发来的 ok 消息，向 $\mathcal{F}_{\mathrm{FEP}}$ 发送(Signature, sid, C,σ_{C2})。

(c)当 $\mathcal{S}$ 接收到 $\mathcal{F}_{\mathrm{FEP}}$ 发来的消息(Get,sid)，$\mathcal{S}$ 向 $\mathcal{F}_{\mathrm{FEP}}$ 发送(Send,sid, C,σ_{C2})。

(2) U 被攻陷的情形：

(a)当 $\mathcal{A}$ 指示被攻陷的 U 向 $\mathcal{F}_{\mathrm{FEP}}$ 发送(Send,sid, C', σ'_{C1}, T'_C,σ'_{TC})，$\mathcal{S}$ 的处理如下：

$\mathcal{S}$ 向 $\mathcal{A}$ 发送(Send, sid,|C',σ'_{C1},T'_C,σ'_{TC}|)；一接收到 $\mathcal{A}$ 发来的 ok 消息，$\mathcal{S}$ 向仿真的 M 发送(Send,sid, C',σ'_{C1},T'_C, σ'_{TC})。接着 $\mathcal{S}$ 仿真签名的验证过程，$\mathcal{S}$ 向仿真的 M 发送(PVerified, sid_U, C',$v_1(C',\sigma'_{C1})$)和(Verified, sid_U, T'_C, $v_2(T'_C,\sigma'_{TC})$)；如果 $v_1(C',\sigma'_{C1})=1$ 且 $v_2(T'_C,\sigma'_{TC})=1$，$\mathcal{S}$ 向 $\mathcal{F}_{\mathrm{FEP}}$ 发送 ok 消息。

(b)当 $\mathcal{A}$ 指示被攻陷的 U 向 $\mathcal{F}_{\mathrm{SCS}}$ 发送(Send,sid, C', σ'_{C2})，$\mathcal{S}$ 的处理如下：

$\mathcal{S}$ 向 $\mathcal{A}$ 发送(Sent,sid,|C',σ'_{C2}|)；一接收到 $\mathcal{A}$ 发来的 ok 消息，$\mathcal{S}$ 向仿真的 M 发送(Sent, sid, C',σ'_{C2})。

接着 $\mathcal{S}$ 仿真签名的验证过程。$\mathcal{S}$ 向仿真的 M 发送(Verified, sid_U, C',$v_2(C',\sigma'_{C2})$)。如果 $v_2(C',\sigma'_{C2})=1$，$\mathcal{S}$ 的仿

真和主体没被攻陷时的仿真相同。

否则，$\mathcal{S}$ 仿真争端解决过程。$\mathcal{S}$ 向 $\mathcal{A}$ 发送(Sent, sid, $|C,\sigma_{C1},G|$)；一接收到 $\mathcal{A}$ 发来的 ok 消息，$\mathcal{S}$ 向仿真的 T 发送(Sent,sid, C,σ_{C1},G)。接着 $\mathcal{S}$ 仿真 T 最终签名生成过程，$\mathcal{S}$ 向 $\mathcal{A}$ 发送(Sent,sid,$|G|$)；一接收到 $\mathcal{A}$ 发来的 ok 消息，$\mathcal{S}$ 向攻陷的 U 发送(Sent,sid, G)，向 $\mathcal{F}_{\text{FEP}}$ 发送(Signature, sid, C,σ_{C2})。

(c)一接收到 $\mathcal{F}_{\text{FEP}}$ 发来的(Get,sid)，$\mathcal{S}$ 仿真 M 获得 T 最终签名的过程，$\mathcal{S}$ 向 T 发送(Get,sid)，向 $\mathcal{A}$ 发送|Signature, sid, C,σ_{C2} |；一接收到 $\mathcal{A}$ 发来的 ok 消息，$\mathcal{S}$ 向 $\mathcal{F}_{\text{FEP}}$ 发送 ok 消息。

(3) M 被攻陷的情形：

(a)当 $\mathcal{A}$ 指示被攻陷的 M 向 $\mathcal{F}_{\text{SCS}}$ 发送(Send, sid, G')，$\mathcal{S}$ 向 $\mathcal{A}$ 发送(Send,sid,$|G'|$)；一接收到 $\mathcal{A}$ 发来的 ok 消息，$\mathcal{S}$ 向仿真的 U 发送(Send,sid, G')。如果 $f_G(G')=1$，$\mathcal{S}$ 的仿真和主体没被攻陷时的仿真相同。

否则，当 $\mathcal{A}$ 指示被攻陷的 M 向 $\mathcal{F}_{\text{SCS}}$ 发送(Resolve, sid, C,σ_{C1},G)时，$\mathcal{S}$ 仿真争端解决过程；仿真的 U 最后收到 (Sent, sid, G)，$\mathcal{S}$ 向 $\mathcal{F}_{\text{FEP}}$ 发送(Signature,sid, C,σ_{C2})。

(b)当被攻陷的 M 向 $\mathcal{F}_{\text{SCS}}$ 发送(Get,sid)时，$\mathcal{S}$ 仿真 M 获得 T 最终签名的过程；$\mathcal{S}$ 最后向仿真的 M 发送(Signature, sid, C,σ_{C2})，向 $\mathcal{F}_{\text{FEP}}$ 发送 ok 消息。

从上面的构造可以看出，$\mathcal{S}$ 的仿真是完美的。即对于任何环境机 $\mathcal{Z}$ 而言，它与 $\mathcal{A}$ 和 π_{FEP} 以及 $\mathcal{S}$ 和 $\mathcal{F}_{\text{FEP}}$ 的交互是不可区分的。

6 结束语

在电子商务中，交易双方往往是互不信任的。交易中的任意一方总担心另一方在交易过程中处于比自己更加有利的位置，从而可能使自己蒙受损失。公平的电子支付方案和协议就是为解决这类问题而设计的。本文基于通用可组合模型，设计了一个公平的电子支付协议。本协议涉及到一个可信第三方 TTP，但只有在产生争端的时候，才会涉及 TTP，正常的支付过程并不需要 TTP 的参与。协议是通用可组合安全的，确保了协议在任意的和未知的多方环境中运行时仍然是安全的。

参 考 文 献

[1] Ketchpel S. Transaction protection for information buyers and sellers[C]. Proceedings of the Dartmouth Institute for Advanced Graduate Studies: Electronic Publishing and the Information Superhighway, Boston, USA, May, 1995: 76–83.

[2] 熊焰, 张伟超, 苗付友, 王行甫. 一种基于计算能力的无需可信第三方公平非抵赖信息交换协议[J]. 电子学报, 2006, 34(3): 563–566.
Xiong Yan, Zhang Wei-chao, Miao Fu-you, and Wang Xing-fu. A fair non-repudiation protocol without TTP based on entity's computing power[J]. *Acta Electronica Sinica*, 2006, 34(3): 563–566.

[3] Han S, Chang E, and Dillon T. Secure e-transactions protocol using intelligent mobile agents with fair privacy[J]. *Studies in Computational Intelligence*, 2007, 37(3): 307–326.

[4] 张青, 温巧燕. 一种新的公平交换协议[J]. 北京邮电大学学报, 2006, 29(5): 63–65.
Zhang Qing and Wen Qiao-yan. A new fair exchange protocol[J]. *Journal of Beijing University of Posts and Telecommunications*, 2006, 29(5): 63–65.

[5] Oniz C, Savas E, and Levi A. An optimistic fair e-commerce protocol for large e-goods[C]. Proceedings of the Seventh IEEE International Symposium on Computer Networks, USA, June, 16-18, 2006: 214–219.

[6] Liang Xiao-hui, Cao Zhen-fu, and Lu Rong-xing. Efficient and secure protocol in fair document exchange[J]. *Computer Standards & Interfaces*, 2008, 30(3): 167–176.

[7] 樊利民, 廖建新. 公平的移动小额支付协议[J]. 电子与信息学报, 2007, 29(11): 2599–2602.
Fan Li-min and Liao Jian-xin. Fair mobile micropayment protocol[J]. *Journal of Electronics & Information Technology*, 2007, 29(11): 2599–2602.

[8] Almudena A, Juan M, and Izquierdo A. A formal analysis of fairness and non-repudiation in the RSA-CEGD protocol[C]. International Conference on Computational Science and Its Applications, Singapore , May, 2005: 1309–1318.

[9] 文静华, 李祥, 张焕国等. 基于 ATL 的公平电子商务协议形式化分析[J]. 电子与信息学报, 2007, 29(4): 901–905.
Wen Jing-hua, Li Xiang, and Zhang Huan-guo, *et al.*. Formal analysis of fair e-commerce protocols based on ATL[J]. *Journal of Electronics & Information Technology*, 2007, 29(4): 901–905.

[10] Aybek M, Steve K, and Eike R. Analysis of a multi-party fair exchange protocol and formal proof of correctness in the strand space model[C]. International Conference on Financial Cryptography and Data Security, Roseau, February, 2005: 255–269.

[11] Canetti R. Universally composable security: A new paradigm for cryptographic protocols[C]. In 42th IEEE Annual Symposium on Foundations of Computer Science, Nevada, USA. October, 14-17, 2001: 136–145. (Revised version(2005) available at http://eprint.iacr.org/2000/067).

[12] Yusuke Okada, Yoshifumi Manabe, and Tatsuaki Okamoto. An optimistic fair exchange protocol and its security in the universal composability framework[J]. *Int. J. of Applied Cryptography*, 2008, 1(1): 70–78.

[13] Hao W and Heq G. Achieving fairness in wireless environment[C]. IEEE 6th CAS Symposium on Emerging Technologies: Mobile and Wireless Communication. Shanghai, China, 2004: 117–120.

[14] 王皓, 欧毓毅, 凌捷等. 新的公平电子合同签署协议[J]. 计算机工程与设计, 2007, 28(14): 3480–3487.
Wang Hao, Ou Yu-yi, and Ling Jie, *et al.*. New fair contract signing protocol[J]. *Computer Engineering and Design*, 2007, 28(14): 3480–3487.

邓淼磊： 男，1977 年生，博士生，讲师，研究方向为安全协议设计和分析.

王玉磊： 女，1973 年生，硕士，讲师，研究方向为信息安全.

周利华： 男，1942 年生，博士生导师，教授，主要研究方向为网络安全.