基于四方的安全电子商务支付协议研究

甘早斌 肖仕成 李 开 肖国强
(华中科技大学计算机学院 武汉 430074)

摘 要 随着电子商务的迅速发展和普及,电子商务安全支付显得越来越重要,成为影响电子商务发展的关键技术。以国际电子商务支付协议标准SET协议为研究对象,针对其无法确保商品原子性和确认发送原子性的缺陷,进行了一些改进;建立了一个基于四方的、能够自动存取关键电子证据、确保商品原子性和确认发送原子性、仲裁处理交易纠纷的安全电子商务支付协议;给出了协议的形式化描述;最后对基于四方的电子商务支付协议的安全性进行了分析。

关键词 电子商务支付,商品原子性,确认发送原子性,SET协议
中图法分类号 TP309 **文献标识码** A

Secure E-commerce Payment Protocol Based on Four Parties

GAN Zao-bin XIAO Shi-cheng LI Kai XIAO Guo-qiang
(School of Computer Science and Technology, Huazhong University of Science and Technology, Wuhan 430074, China)

Abstract With the rapid development and popularization of electronic commerce, the secure payment in the area has become more and more important and is a key technology that impacts on the development of e-commerce. Aiming at the standard Secure Electronic Transaction protocol (SET), some improvements were done for the SET protocol in order to assure the goods atomicity and certified delivery. Then, this paper proposed a secure e-commerce payment system based on the four parties that can not only support the goods atomicity and certified delivery, but also access the key electronic evidence automatically and deal with the transaction disputes. In the meantime, the formal description of the protocol is presented. Finally, the security of the proposed protocol was compared and analyzed.

Keywords E-commerce payment, Goods atomicity, Confirmation delivery, Secure electronic transaction

1 引言

随着互联网的迅速发展,电子商务的诞生给商家带来了无数的商机,给客户也带来了便利。但鉴于电子商务交易环境的开放性,能否构建一个安全的电子商务支付体系,将是影响电子商务发展的瓶颈技术。当前国际上运用于电子商务支付的协议主要有安全套接层协议SSL[1,2]和安全电子交易协议SET[3,4]等。尤其是SET协议,其具有很高的安全性,已成为电子商务支付协议的国际标准。

SET协议自诞生以来,被国内外专家学者一致认为是电子商务领域最具发展前途的电子商务支付协议,也是目前研究和使用最广泛的电子商务支付协议[5,6]。SET协议虽然具有很高的安全性,但协议本身仍存在一定的缺陷,如协议效率比较低、身份认证模式复杂等[7,8]。为此,国内外学者在协议的算法效率和安全领域提出了很多的改进方案,如改进支付协议的加密算法应用、身份认证模式等[9,10],提出用加密速度更快、安全性更高的AES对称加密算法代替DES对称加密算法,用椭圆曲线密码体制ECC代替RSA公钥算法,用单向身份认证模式取代交叉身份认证模式等[11,12]。但是,在协议的商品原子性和确认发送原子性领域,却很少有文献报道。

SET协议无法确保商品原子性和确认发送原子性,就是说协议不能保证客户付款后能收到货或收到的货与订单相符。而且提取交易关键电子证据难度较大,缺乏一个安全的交易纠纷处理体系。而在电子商务领域,由于客户在退换货活动中的被动地位和退换货活动中诸多的不确定性因素,商品原子性和确认发送原子性在电子商务支付协议中就显得尤为重要。因此,建立一个确保商品原子性和确认发送原子性的电子商务支付协议是非常必要的。

电子支付的原子性问题是一个热点[13]。1996年,Carnegie Mellon大学的J. D. Tygar第一次正式提出了电子支付的原子性概念[14],并提出满足商品原子性和确认发送原子性的电子商务支付协议——Netbill协议[15]。但是,该协议只限于数字商品简单交易模式的电子支付,并不适用于传统商品的电子商务支付。对于传统实物商品的协议原子性研究却甚少,基本上都是提出扩展交易参与方的功能来间接实现,没有提出很好的解决方案。

本文以安全电子商务支付协议国际标准SET协议为研究范型,改进SET协议,设计一个基于四方的安全电子商务支付协议。方案优化了SET协议身份认证模式和交易处理流程,改进了SET协议提取关键电子证据极为不便的一些缺

到稿日期:2010-11-24 返修日期:2011-03-02 本文受国家自然科学基金(70672041),湖北省自然科学基金(2007ABA307)以及中央高校基本科研业务费(2010MS112)资助。

甘早斌(1968—),男,博士后,副教授,主要研究领域为信任计算、电子商务技术、软件Agent技术及其支撑系统理论以及信任计算、软件代码安全,E-mail:ganzb@sina.com;肖仕成(1983—),男,硕士,主要研究领域为电子商务、网络安全。

陷，建立了一个基于四方的能够自动存取关键电子证据、确保商品原子性和确认发送原子性、自动仲裁处理交易纠纷的安全电子商务支付协议。

2 基于四方的安全电子商务支付协议设计

基于四方的安全电子商务支付协议交易的参与方包括客户、商家、支付机构、第四方。支付机构指金融机构，能通过金融内部网进行资金划拨服务，如支付网关、第三方支付平台等。第四方是物流方，如邮政、中通等物流公司，其职责为：负责商品货物的运送，监督、协助支付机构解决交易纠纷等。基于四方的安全电子商务支付协议跟 SET 协议一样，主要应用于 B2C 的电子商务运营模式。交易初始化，即交易参与方都需到 CA 认证中心注册证书，下载协议的客户端软件。商家服务器应下载保存支付机构和第四方的数字证书。

基于四方的安全电子商务支付协议中，考虑到交易中可能存在的交易纠纷情况，在电子商务支付协议主协议基础上，设计提供 3 种纠纷处理协议：客户对商品不满意要求退货的退货协议；商品存在非人为质量问题的换货协议；客户申诉商品与客户订购商品不符的交易欺诈纠纷处理协议。

2.1 支付协议主协议形式化描述

基于四方的安全电子商务支付协议交易参与方为客户 C、商家 M、支付机构 P 和第四方 W，支付协议主协议流程如图 1 所示。为了便于对“基于四方的安全电子商务支付协议”的形式化描述，对协议中所用的符号进行说明，如表 1 所列。

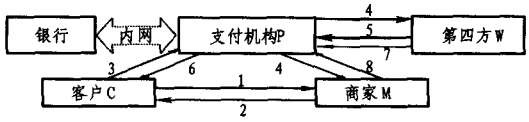

图 1 基于四方的安全电子商务支付协议主协议流程图

(1) $C\rightarrow M$: $\{(OI'||CerC)\}$ $[OI'=D_{skc}(OI)]$

客户 C 浏览商家 M 电子商务网站商品报价，同意报价，对订单 OI 数字签名：$OI'=D_{skc}(OI)$。将 OI' 与客户数字证书报文合并：$OI'||CerC$，发送给商家 M。

(2) $M\rightarrow C$: $\{Y\}$ $[E_{pkc}(OI')=OI, OI''=D_{skm}(OI'), OI'''=D_{pkw}(OI''), Y=D_{skm}(Num||CerP||CerM||CerW||Pay||OI''')]$

商家 M 对收到的 OI' 解密：$E_{pkc}(OI')=OI$，确认订单为客户 C 所发，并根据订单 OI 形成付款要求 Pay。

商家 M 对客户 C 的订单签名信息 OI' 进行数字签名：$OI''=D_{skm}(OI')$，形成订单信息的双重签名信息 OI''，利用第四方 W 公钥对 OI'' 加密（事先保存在商家服务器中）：$OI'''=D_{pkw}(OI'')$。

商家 M 利用商家号、客户号、当前时间戳以及随机数合并生成该交易唯一标识号 Num。商家 M 将交易唯一标识号 Num、支付机构的数字证书 $CerP$、自己的数字证书 $CerM$、第四方 W 的数字证书 $CerW$ 和付款要求 Pay 以及双重签名的加密订单消息 OI''' 报文合并后进行数字签名：$Y=D_{skm}(Num||CerP||CerM||CerW||Pay||OI''')$，并发送给客户 C。

(3) $C\rightarrow P$: $\{Y_1\}$ $[E_{pkm}(Y)=(Num||CerP||CerM||CerW||Pay||OI'''), CK(CerP), PI'=D_{skc}(PI||PAN), PI''=D_{pkp}(PI'), Y_1=D_{skc}(Num||CerC||CerM||CerW||OI'''||PI'')]$

客户 C 收到信息 Y，解密：$E_{pkm}(Y)=(Num||CerP||CerM||CerW||Pay||OI''')$，确认信息 Y 为商家 M 所发。

客户 C 验证支付机构 P 的数字证书：$CK(CerP)$，确认支付机构 P 的身份。

客户 C 按付款要求 Pay 形成支付指令 PI，客户 C 利用支付指令 PI 将自己的账号信息 PAN 报文合并后进行数字签名：$PI'=D_{skc}(PI||PAN)$，再用支付机构 P 的公钥加密：$PI''=D_{pkp}(PI')$。

客户 C 将交易唯一标识号 Num、自己的数字证书 $CerC$、商家 M 的数字证书 $CerM$、第四方 W 的数字证书 $CerW$ 和加密的双重签名订单信息 OI''' 以及 PI'' 报文合并后再签名：$Y_1=D_{skc}(Num||CerC||CerM||CerW||OI'''||PI'')$，并发送给支付机构 P。

表 1 基于四方的安全电子商务支付协议符号说明

符号	说明	符号	说明	符号	说明
C	客户	M	商家	P	支付机构
W	第四方	{ }	需发送的信息	||	报文合并
→	信息发送	[ ]	发送方需做的运算	PAN	客户 C 的银行账户信息
Pay	商家 M 的付款要求	OI	客户 C 的订单	PI	客户 C 的支付指令
CerC	客户 C 的数字证书	CerM	商家 M 的数字证书	CerP	支付机构 P 的数字证书
CerW	第四方 W 的数字证书	pkc	客户 C 的公钥	pkm	商家 M 的公钥
pkp	支付机构 P 的公钥	pkw	第四方 W 的公钥	skc	客户 C 的私钥
skm	商家 M 的私钥	skp	支付机构 P 的私钥	skw	第四方 W 的私钥
Msg	支付是否可完成信息	Msg_1	商家已发货信息	Msg_2	客户已签收货物信息
Tmsg	申请退货信息	$Tmsg_1$	退货申请成功要求客户退货信息	$Tmsg_2$	已退货信息
Hmsg	换货申请信息	$Hmsg_1$	换货申请成功要求客户退货信息	$Hmsg_2$	换货中客户已退货信息
Qmsg	交易欺诈申诉信息	$Qmsg_1$	欺诈申诉处理结果信息	T_1	商家发货时延
T_2	交易申诉时延	T_3	客户退货时延	T_4	客户换货时的退货时延
CK()	对数字证书的有效性进行检测验证	$D_{skc}()$	客户 C 的数字签名	$D_{skm}()$	商家 M 的数字签名
$D_{skp}()$	支付机构 P 的数字签名	$D_{skw}()$	第四方 W 的数字签名	$E_{pkc}()$	对客户 C 的数字签名进行验证，确认信息为客户所发，且信息没有被篡改
$E_{pkm}()$	对商家 M 数字签名进行验证，确认信息为商家所发，且信息没有被篡改	$E_{pkp}()$	对支付机构 P 数字签名进行验证，确认信息为支付机构所发，且信息没有被篡改	$E_{skw}()$	对第四方 W 数字签名进行验证，确认信息为第四方所发，且信息没有被篡改

(4) $P\rightarrow M$: $\{Y_2\}$

$P\rightarrow W$: $\{Y_2\}$ $[E_{pkc}(Y_1)=(Num||CerC||CerM||CerW||OI'''||PI''), CK(CerC), CK(CerM), CK(CerW), E_{skp}(PI'')=PI', E_{pkc}(PI')=(PI||PAN), Y_2=D_{skp}(Num||T_1||Msg)]$

支付机构 P 收到信息 Y_1，对其进行解密：$E_{pkc}(Y_1)=(Num||CerC||CerM||CerW||OI'''||PI'')$，确认信息为客户 C 所发。

支付机构 P 验证客户 C、商家 M 和第四方 W 的数字证书：$CK(CerC)$，$CK(CerM)$，$CK(CerW)$，确认客户 C、商家 M 和第四方 W 的身份。

支付机构 P 用自己的私钥解密 PI''：$E_{skp}(PI'')=PI'$，对

得到的 PI' 再解密：$E_{pkc}(PI')=(PI||PAN)$，确认支付指令由客户 C 所发，并得到客户 C 的账号信息 PAN 和支付指令 PI。

支付机构 P 验证支付指令，即通过金融专网查询客户 C 账户是否有足够余额。若余额不足，取消交易；若客户 C 有足够余额支付，支付机构 P 暂时冻结客户 C 账户里面的相应金额或把相应金额暂时划拨到一临时账户，并生成支付可成功完成的信息 Msg。

支付机构 P 将该交易唯一标识号 Num、发货时延 T_1 和 Msg 报文合并后签名：$Y_2=D_{skp}(Num||T_1||Msg)$，发送给商家 M 和第四方 W（协议规定商家 M 在收到信息 Y_2 后必须打印包括该交易唯一标识号 Num 的发货单，并在时延 T_1 内到第四方 W 处发货）。

(5) $W\rightarrow P$：$\{Y_3\}[E_{pkp}(Y_2)=(Num||T_1||Msg), Y_3=D_{skw}(Num||Msg_1)]$

第四方 W 收到 Y_2，解密：$E_{pkp}(Y_2)=(Num||T_1||Msg)$，确认信息为支付机构 P 所发。同时录入该交易唯一标识号 Num 到本地数据库中，标识交易状态为等待商家发货状态，并启动发货时延 T_1，等待商家 M 发货。

第四方 W 接受商家 M 的发货，检查时延 T_1（商家是否在规定时延内发货），根据该交易唯一标识号 Num 把发货单（相当于订单信息）录入到本地服务器中，生成已发货信息 Msg_1。

第四方 W 报文合并交易唯一标识号 Num 和已发货信息 Msg_1，数字签名：$Y_3=D_{skw}(Num||Msg_1)$，然后发送给支付机构 P。

(6) $P\rightarrow C$：$\{(Num||Msg_1)\}[E_{pkw}(Y_3)=(Num||Msg_1)]$

支付机构 P 收到 Y_3，解密：$E_{pkw}(Y_3)=(Num||Msg_1)$，确认信息为第四方 W 所发。

支付机构 P 把该交易唯一标识号 Num 和商家 M 已发货信息 Msg_1 发送给客户 C，方便客户 C 随时了解整个交易的进程情况。

(7) $W\rightarrow P$：$\{Y_4\}[Y_4=D_{skw}(Num||T_2||Msg_2)]$

第四方 W 发货后，客户 C 签收货物。第四方 W 报文合并交易唯一标识号 Num、交易申诉时延 T_2 和货物已签收信息 Msg_2，数字签名：$Y_4=D_{skw}(Num||T_2||Msg_2)$，然后发送给支付机构 P。

(8) $P\rightarrow M$：$\{(Num||Msg_2)\}[E_{pkw}(Y_4)=(Num||T_2||Msg_2)]$

支付机构 P 收到 Y_4，解密：$E_{pkw}(Y_4)=(Num||T_2||Msg_2)$，确认信息为第四方 W 所发。

支付机构 P 启动交易申诉时延 T_2，客户若要求退换货或交易出现欺诈，必须在时延 T_2 内向支付机构申诉。

支付机构 P 把交易唯一标识号 Num 和客户 C 已签收货物的信息 Msg_2 转发给商家 M，方便商家 M 随时了解整个交易的进程情况。

2.2 退货协议形式化描述

如果客户 C 对商品不满意或商品出现非人为质量问题，要求退货，客户 C 必须要在交易申诉时延 T_2 内向支付机构 P 申诉，启动退货协议。退货协议是商品出现问题时为方便客户退货而设计的协议，基于四方的安全电子商务支付协议退货协议流程如图 2 所示（在主协议流程图基础上增加退货协议）。退货协议形式化描述如下：

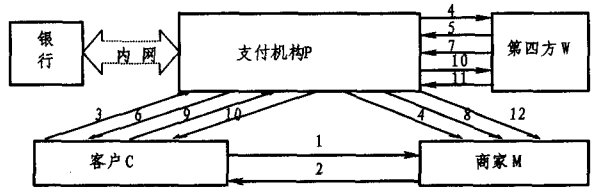

图 2 基于四方的安全电子商务支付协议退货协议流程

(9) $C\rightarrow P$：$\{Y_5\}[Y_5=D_{skc}(Num||Tmsg)]$

客户 C 申请退货，报文合并交易唯一标识号 Num 和申请退货信息 $Tmsg$，数字签名：$Y_5=D_{skc}(Num||Tmsg)$，发送给支付机构 P。

(10) $P\rightarrow C$：$\{Y_6\}$

$P\rightarrow W$：$\{Y_6\}[E_{pkc}(Y_5)=(Num||Tmsg), Y_6=D_{skp}(Num||T_3||Tmsg_1)]$

支付机构 P 收到 Y_5，解密：$Y_5=D_{skc}(Num||Tmsg)$，确认信息为客户 C 所发。

支付机构 P 判断交易是否满足退货条件。若不满足退货条件，驳回退货申请；如满足退货条件，支付机构报文合并交易唯一标识号 Num、退货时延 T_3 和要求客户 C 去第四方 W 处退货的信息 $Tmsg_1$，数字签名：$Y_6=D_{skp}(Num||T_3||Tmsg_1)$，并发送给客户 C 和第四方 W。

(11) $W\rightarrow P$：$\{Y_7\}$

$[E_{pkp}(Y_6)=(Num||T_3||Tmsg_1), Y_7=D_{skw}(Num||Tmsg_2)]$

第四方 W 收到 Y_6，解密：$E_{pkp}(Y_6)=(Num||T_3||Tmsg_1)$，确认信息为支付机构 P 所发，并启动退货时延 T_3（客户 C 收到 Y_6 信息后必须要在退货时延 T_3 内到第四方 W 处退货）。

第四方 W 等待客户 C 退货，客户 C 根据交易唯一标识号 Num 打印退货申请单到第四方 W 处退货。第四方检查时延 T_3 并提取保存在本地服务器上的商家 M 的发货单，比较商品是否相符且是否有人为质量损坏。若一切正常，接受退货并把商品发还给商家 M。

第四方 W 签名交易唯一标识号 Num 和客户 C 已退货的信息 $Tmsg_2$：$Y_7=D_{skw}(Num||Tmsg_2)$，并发送给支付机构 P。

(12) $P\rightarrow M$：$\{(Num||Tmsg_2)\}[E_{pkw}(Y_7)=(Num||Tmsg_2)]$

支付机构 P 收到 Y_7，解密：$E_{pkw}(Y_7)=(Num||Tmsg_2)$，确认信息为第四方 W 所发。支付机构 P 把交易唯一标识号 Num 和客户 C 已退货信息 $Tmsg_2$ 发送给商家 M，以便商家了解整个交易进程情况。

支付机构 P 解冻客户 C 账户里的相应资金或把支付资金从临时账户里面划拨回客户 C 的资金账户，支付取消，整个退货协议结束。

2.3 换货协议形式化描述

如果商品存在非人为质量问题，客户要求换货，客户在规定时间内提出换货申诉，启动换货协议。换货协议是商品出现问题时为方便客户换货而设计的协议，基于四方的安全电子商务支付协议换货协议流程如图 3 所示，换货协议形式化描述如下：

(9) $C\rightarrow P$：$\{Y_8\}[Y_8=D_{skc}(Num||Hmsg)]$

客户 C 对交易唯一标识号 Num 和申请换货信息 $Hmsg$ 数字签名：$Y_8=D_{skc}(Num||Hmsg)$，并发送给支付机构 P。

(10) $P\rightarrow C$：$\{Y_9\}$

$P\rightarrow W$：$\{Y_9\}$ $[E_{pkc}(Y_8)=(Num||Hmsg), Y_9=D_{skp}(Num||T_4||Hmsg_1)]$

支付机构 P 收到 Y_8 并解密：$E_{pkc}(Y_8)=(Num||Hmsg)$，确认信息为客户 C 所发。

支付机构 P 根据交易唯一标识号 Num 检测是否符合换货条件。若不符合换货条件，驳回换货申请；若符合换货条件，生成同意换货并合并要求客户 C 去第四方 W 处退货的信息 $Hmsg_1$ 和客户 C 的退货时延 T_4。

支付机构 P 报文合并交易唯一标识号 Num、客户 C 的退货时延 T_4 和要求客户退货的信息 $Hmsg_1$：$Y_9=D_{skp}(Num||T_4||Hmsg_1)$，并发送给客户 C 和第四方 W。

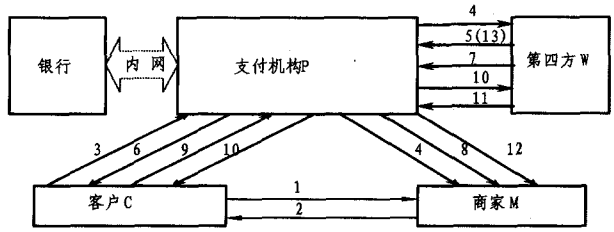

图 3　基于四方的安全电子商务支付协议换货协议流程

(11) $W\rightarrow P$：$\{Y_{10}\}$ $[E_{pkp}(Y_9)=(Num||T_4||Hmsg_1)$，$Y_{10}=D_{skw}(Num||Hmsg_2)]$

第四方 W 收到 Y_9，解密：$E_{pkp}(Y_9)=(Num||T_4||Hmsg_1)$，确认信息为支付机构 P 所发。启动退货时延 T_4，等待客户 C 退货(客户 C 收到 Y_9 信息后必须在退货时延 T_4 内去第四方 W 处退货)。

第四方 W 收到客户 C 退货，检测是否在时延 T_4 内退货，根据该交易唯一标识号 Num 找到保存在本地服务器上的商家 M 的发货单与客户 C 的退货商品进行比较，检查商品是否符合人为质量损坏。

第四方 W 签名交易唯一标识号 Num 和客户换货已退货信息 $Hmsg_2$：$Y_{10}=D_{skw}(Num||Hmsg_2)$，并发送给支付机构 P。

(12) $P\rightarrow M$：$\{(Num||Hmsg_2)\}$ $[E_{pkw}(Y_{10})=(Num||Hmsg_2)]$

支付机构 P 收到 Y_{10}，解密：$E_{pkw}(Y_{10})=(Num||Hmsg_2)$，确认信息为第四方 W 所发。

支付机构 P 报文合并交易唯一标识号 Num 和客户换货已退货信息 $Hmsg_2$，并发送给商家 M。

第四方 W 在商家 M 签收客户 C 退还过来的货物后，启动前述发货时延 T_1，规定商家 M 在规定时延 T_1 内到第四方 W 处发货，协议自动跳转到主协议的第(5)步继续向下执行，直至整个协议完全结束。

2.4　交易欺诈纠纷处理协议形式化描述

如客户购买商品后发现与订单不符，客户必须在纠纷申述时限内向支付机构进行欺诈纠纷申诉，同时启动交易欺诈纠纷处理协议。欺诈纠纷处理协议是为防止商家或客户交易欺诈而设计的协议，基于四方的安全电子商务支付协议欺诈纠纷处理协议流程如图 4 所示，交易欺诈纠纷处理协议形式化描述如下：

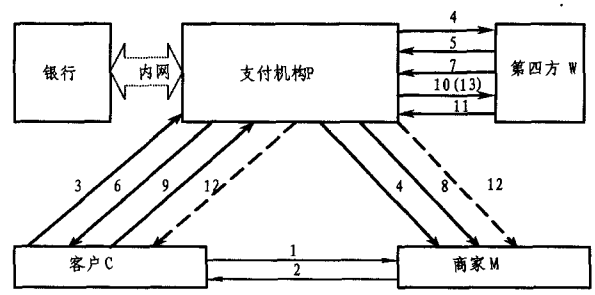

图 4　基于四方的安全电子商务支付协议交易欺诈纠纷处理协议流程

(9) $C\rightarrow P$：$\{Y_{11}\}$ $[Y_{11}=D_{skc}(Num||Qmsg)]$

客户 C 报文合并交易唯一标识号 Num 和交易欺诈申诉信息 $Qmsg$，签名：$Y_{11}=D_{skc}(Num||Qmsg)$，并发送给支付机构 P。

(10) $P\rightarrow W$：$\{Y_{12}\}$ $[E_{pkc}(Y_{11})=(Num||Qmsg), Y_{12}=D_{skp}(Num||CerC||CerM||OI''')]$

支付机构 P 收到信息 Y_{11}，解密：$E_{pkc}(Y_{11})=(Num||Qmsg)$，确认信息为客户 C 所发。

支付机构 P 提取保存在本地服务器上的该交易唯一标识号 Num、客户 C 的数字证书 $CerC$、商家 M 的数字证书 $CerM$ 和加密的双重签名订单信息 OI'''，报文合并后签名：$Y_{12}=D_{skp}(Num||CerC||CerM||OI''')$，并发送给第四方 W。

(11) $W\rightarrow P$：$\{Y_{13}\}$ $[E_{pkp}(Y_{12})=(Num||CerC||CerM||OI'''), E_{skw}(OI''')=OI'', E_{pkm}(OI'')=OI', E_{pkc}(OI')=OI, Y_{13}=D_{skw}(Num||Qmsg_1)]$

第四方 W 收到支付机构 P 发送过来的 Y_{12}，解密 $E_{pkp}(Y_{12})=(Num||CerC||CerM||OI''')$，确认为支付机构 P 所发。

第四方 W 解密 OI'''：$E_{skw}(OI''')=OI''$，得到订单的双重签名信息 OI''。

第四方 W 解密双重签名：$E_{pkm}(OI'')=OI'$，$E_{pkc}(OI')=OI$，确认信息为客户 C 和商家 M 共同所发，并得到双方认同的订单信息 OI。

第四方 W 提取保存在本地服务器上的商家 M 的发货单，并与订单信息 OI 比较，生成交易欺诈申诉处理结果信息 $Qmsg_1$：若商品一致，说明是客户 C 恶意申诉；若商品不一致，说明是商家 M 恶意欺诈。

第四方 W 报文合并交易唯一标识号 Num 和交易欺诈申诉处理结果信息 $Qmsg_1$，数字签名：$Y_{13}=D_{skw}(Num||Qmsg_1)$，并发送给支付机构 P。

(12) $P\rightarrow C$：$\{(Num||Qmsg_1)\}$ $[E_{pkw}(Y_{13})=(Num||Qmsg_1)]$

or $P\rightarrow M$：$\{(Num||Qmsg_1)\}$ $[E_{pkw}(Y_{13})=(Num||Qmsg_1)]$

支付机构 P 收到 Y_{13}，解密：$E_{pkw}(Y_{13})=(Num||Qmsg_1)$，确认信息为第四方 W 所发，并得到交易唯一标识号 Num 和交易欺诈申诉处理结果 $Qmsg_1$。支付机构 P 报文合并交易唯一标识号 Num 和交易欺诈申诉处理结果 $Qmsg_1$。

如果是客户恶意申诉，把 $Num||Qmsg_1$ 转发给客户 C，并对客户 C 进行一定的处罚，交易结束。

如果是商家 M 恶意欺诈，把 $Num||Qmsg_1$ 转发给商家 M，并对商家 M 进行一定的处罚，并自动启动退货协议，跳转到上述退货协议的第(10)步，继续完成整个退货协议。

3 协议安全性分析和比较

基于四方的安全电子商务支付协议的主要设计目的是彻底解决电子商务支付协议的商品原子性和确认发送原子性，以确保网络支付的安全，避免电子商务网络交易欺诈现象。

3.1 身份认证模式安全性分析和比较

基于四方的安全电子商务支付协议交易参与方为客户、商家、支付机构和第四方。在信息交互过程中，身份认证模式以支付机构为核心，认证模式如图5所示。

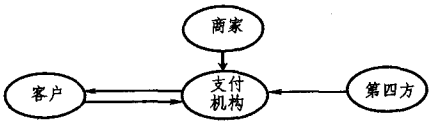

图5 基于四方的安全电子商务支付协议身份认证模式

基于四方的安全电子商务支付协议的身份认证是以支付机构为中心的身份认证模式，协议要求支付机构必须是可信的。支付机构属于银行金融机构，具有很大的公信力，故在实际应用中确实可以担当这个职能。

由图5可知，完成一次交易，客户要验证支付机构的身份有效性，而支付机构要验证客户、商家和第四方的身份有效性，客户、商家和第四方互不验证对方的数字证书。在交易支付过程中，客户向商家提出购买请求，客户首先验证支付机构的数字证书，确认支付机构的身份。支付机构的证书有效，交易才会继续，客户对商家、第四方的证书验证工作交由支付机构来完成。当交易进行到付款阶段，支付机构要验证客户和商家的数字证书和第四方的数字证书，确认客户、商家和第四方的身份。如果交易三方的数字证书有效，交易才会继续进行。一旦其中有一方数字证书无效，交易取消，这样客户、商家、支付机构和第四方的身份都得到了保障。

与原SET协议交叉身份认证模式效率相比(见表2)，基于四方的安全电子商务支付协议完成一次交易需身份认证4次(SET协议完成一次交易需身份认证6次)，有效提高了协议身份认证的效率。

表2 协议交易参与方身份验证次数比较

协议	客户	商家	支付机构	第四方
SET协议	2	2	2	
基于四方的安全电子商务支付协议	1	0	3	0

3.2 资金流安全性分析和比较

分析基于四方的安全电子商务支付协议的资金链，其资金流走向为客户→支付机构→商家。其过程可以用式(1)表示：

$$PI''=D_{pkp}(D_{skc}(PI||PAN)) \tag{1}$$

客户直接与支付机构交互传递支付指令，客户将PI''进行数字签名后直接发送给支付机构，因支付指令已经过客户数字签名，这样就能有效保证支付指令的完整性和防抵赖性。之后用支付机构的公钥对签名的支付指令进行加密，这样支付指令只有支付机构才能解开，有效地保证了支付指令的安全。在该支付协议中，支付机构首先验证客户支付指令的有效性，然后暂时冻结客户账户里面的支付金额或者把资金划拨到一临时账户，等交易成功结束且没有纠纷申诉时才进行资金的划拨。故在交易过程中，金钱不会凭空消失，也不会无故产生，而且客户资金账户的减少数能够等于商家账户的增长数，即协议能满足“金钱原子性”。

在原有SET协议中，其资金流走向为：客户→商家→支付机构→商家。其过程可以用式(2)、式(3)、式(4)表示：

$$PI'=D_{skc}(PI) \tag{2}$$

$$PI''=E_k(PI') \tag{3}$$

$$P=E_{pkp}(PAN||K) \tag{4}$$

客户先数字签名支付指令，再用对称密钥K加密经过签名的支付指令，用支付机构的公钥加密付款要求PAN和对称密钥K后形成数字信封发给商家，再由商家转发给支付机构。此举不但给了恶意商家故意延迟把支付指令发送给支付机构的机会，同时增加了客户账户等私密信息暴露在网络上的时间，而且增加了加密重数，增加了支付机构的加解密工作。

在本改进方案中，支付指令直接由客户与支付机构交互，直接杜绝了恶意商家延迟发送支付指令给支付机构的欺诈行为，而且大大减少了客户的支付指令和资金账户等私密信息暴露在网络上的时间，从源头上减少了客户私密信息泄露的机会。

3.3 信息流安全性分析和比较

基于四方的安全电子商务支付协议以SET协议为范型，基本没有破坏原有SET协议的安全。交易过程中，每一步的信息传输都采用数字摘要、数字签名等技术来保证信息的完整性和不可抵赖性，采用加密算法保证支付信息的安全性，而且在交易过程中产生了一个唯一的交易唯一标识号来标示本次交易。交易标识号的产生由时间戳的一部分组成，能有效防止网络的重放攻击。

在原SET协议中，客户的订单信息只直接发送给商家，如果某些商家恶意修改客户的订单信息，发生纠纷，而协议又无法为客户提供有效的电子证据，这就会给客户带来某些不必要的麻烦和损失。基于四方的安全电子商务支付协议中，客户要把用第四方公钥加密的经过客户、商家双重签名的订单信息发送给支付机构，这样可信的第三方机构——支付机构就保存有了本次交易的电子证据。一旦发生交易纠纷，支付机构可以联合第四方仲裁处理。而且支付机构不能解开客户的订单信息，故客户购物信息对支付机构保密，存在一定的匿名性，保护了客户的隐私。

3.4 商品的原子性和确认发送原子性分析和比较

SET协议无法确保商品原子性和确认发送原子性，而基于四方的安全电子商务支付协议彻底解决了电子商务的商品原子性和确认发送原子性。基于四方的安全电子商务支付协议由主协议、退货协议、换货协议以及存在交易欺诈的纠纷处理协议组成。主协议中，商家是否发货由第四方监督确认，这样完全保证客户订购商品后能够收到货，也就是说确保了商品的原子性。

基于四方的安全电子商务支付协议中，客户发送支付指令给支付机构时，也把经双重签名的订单信息用第四方的公钥加密后发送给支付机构，用作纠纷仲裁的电子证据文件。具体过程可以用式(5)来表示：

$$OI'''=D_{pkw}(D_{skm}(D_{skc}(OI))) \tag{5}$$

当交易出现欺诈纠纷时，支付机构可以利用该电子证据OI'''和第四方协同解决。支付机构发送电子证据OI'''给第四方，第四方解密该电子证据文件OI'''，得到双重签名的订单信息OI''，验证客户和商家的数字签名，确认订单信息为客户和

商家双方承认，再与保存在本地服务器上的订单进行比较、仲裁处理，这样就保证了交易的确认发送原子性。具体过程可用式(6)来表示：

$$E_{pkc}(E_{pkm}(E_{skw}(OI^{m})))=OI \quad (6)$$

基于四方的安全电子商务支付协议的主协议、退货协议、换货协议以及存在交易欺诈的纠纷处理协议中各协议的组合，经验证能够确保交易的商品原子性和确认发送原子性，有效地保证了客户的权益。而且，在电子商务活动中，也存在一些商家库存没货的欺诈，即商家没有商品，却在网上商城展示商品出售。当有客户向该商家订购该商品后，商家再低价寻找同类商品卖给客户，以赚取利润，即为零库存欺骗。基于四方的安全电子商务支付协议明确规定了客户在发送订单以后商家必须在规定时间内发货，这样就可以有效避免商家的零库存欺诈。

基于四方的安全电子商务支付协议的退货协议和换货协议能够保护客户的消费者权益。若客户对网络购物的商品不满意，只要提出申诉，协议可以根据客户的选择自动执行退换货协议，而不需要客户做很多额外的取证工作。而且当交易出现欺诈时，客户进行申诉，自动执行交易欺诈纠纷处理协议，协议能自动提取电子证据文件进行交易仲裁，而不用客户和商家进行很多繁杂的电子证据收集工作，为客户和商家都提供了便利。

4 协议模型检测仿真实验验证

利用国际上流行的安全协议检测工具——符号模型检测工具 SMV(Symbolic Model Checking)对协议的电子交易支付原子性进行安全检测实验验证。

根据基于四方的安全电子商务支付协议交易参与方：商家、客户、支付机构以及第四方，可将协议模块分为 4 个模块。利用协议的 4 个模块分别建立 4 个有限状态模型，将协议转换成有限状态系统，然后转换成 SMV 工具独有的 SMV 程序语言，同时利用 CTL(Computation Tree Logic)公式来表示协议要验证的性质，最后输入到 SMV 工具。如果协议满足 CTL 描述的性质，系统输出结果为 True，否则将输出 False，并列出导致该结果的反例。

本次实验验证协议的电子商务支付原子性，即金钱原子性、商品原子性和确认发送原子性。金钱原子性 CTL 公式描述为客户 C 支付了货款，商家 M 才能得到货款，且只有客户 C 支付了货款，商家 M 才能得到货款；商品原子性 CTL 公式描述为商家 M 收到货款，客户 C 必能收到商品，且客户 C 成功收到商品，商家 M 必能收到货款；确认发送原子性 CTL 公式描述为交易成功后，仲裁方必能收到客户 C、商家 M 都承认的电子证据文件。

利用基于四方的安全电子商务支付协议 SMV 有限状态模型，将其转换成 SMV 程序，将 SMV 程序及其必须满足的原子性 CTL 公式输入到 SMV 检测工具中运行，得到的结论都为 True。文献[6]利用 SMV 工具对 SET 协议进行了原子性验证，证明了 SET 协议只满足金钱原子性，不满足商品原子性和确认发送原子性。而实验证明改进后的基于四方的安全电子商务支付协议满足电子支付的金钱原子性、商品原子性以及确认发送原子性，进一步保证了电子支付的安全性要求。

结束语 在电子商务活动中，由于客户对货物的认可度和对交易是否存在欺诈不能在第一时间获知，故电子商务支付必须在客户对商品完全满意且没有交易纠纷申诉时才告结束。基于四方的安全电子商务支付协议改进了 SET 协议，建立了以支付机构为中心的身份认证模式，改进了交易支付流程。设计客户支付指令由客户和支付机构直接交互，建立了一个监督机制，解决了商品的原子性和确认发送原子性，设计建立了一个公平、便捷的交易纠纷处理协议，有效保证了电子商务的安全支付，并给出了协议的形式化描述。

下一步的工作主要为改进协议数据结构，扩展协议对借记卡的支持。同时，提高基于四方的安全电子商务支付协议的算法效率，进一步改进和完善协议。

参 考 文 献

[1] Mitchell J C, Shmatikoy V, Stern U. Finite-state analysis of SSL 3.0[C]// Proc. of the 7th USENIX Security Symposium. San Antonio, Texas, January 1998: 201-216

[2] Shin Y S, Gupta M, Myers S. A Study of the Performance of SSL on PDAs[C]// Proc. of the IEEE Conf. on Computer Communications Workshops. Rio de Janeiro, Brazil, April 2009: 1-6

[3] Visa, Master. SET secure electronic transactions specification — book1: business description[S]. May 1997

[4] Visa, Master. SET secure electronic transactions specification — book3: formal protocol definition[S]. May 1997

[5] Zhang X, Huang Q L, Peng P. Implementation of a suggested E-commerce model based on SET protocol[C]// Proc. of the 8th International Conf. Software Engineering Research, Management and Applications. Montreal, Canada, May 2010: 67-73

[6] Lu S M, Zhang J L, Luo L M. The automatic verification and improvement of SET protocol model with SMV[C]// Proceedings of the International Symposium on Information Engineering and Electronic Commerce. Ternopil, May 2009: 433-436

[7] Brlek S, Hamadou S, Mullis J. A flaw in the electronic commerce protocol SET[J]. Information Processing Letters, 2006, 97(3): 104-108

[8] Shen Z H, Wang H. An improved SET protocol payment system [C]// Proc. of International Conf. on Computer and Communication Technologies in Agriculture Engineering. Chengdu, China, June 2010: 400-403

[9] 黄少寅，陈勇，高传善. SETBOC—— 一种新型的基于单向身份认证的安全电子交易协议[J]. 通信学报，2003，24(12)：170-176

[10] 陈庆锋，白硕，王驹. SET 协议中问题的分析及解决方案[J]. 计算机学报，2002，23(2)：202-209

[11] Sanchez A C, Scanchez R R. The rijndael block cipher (AES proposal): a comparison with DES[C]// Proc. of the IEEE 35th Annual International Carnahan Conf. on Security Technology. London, October 2001: 229-234

[12] Koblitz N. Elliptic Curve Cryptosystems [J]. Mathematics of Computation, 1987, 48(177): 203-209

[13] 刘义春，张焕国，王丽娜. 电子支付协议的原子性研究综述[J]. 计算机科学，2005，32(2)：93-96，113

[14] TYGAR J D. Atomicity in electronic commerce[C]// Proc. of the 15th Annual ACM Symposium on Principles of Distributed Computing. May 1996: 8-26

[15] Cox B, Tygar J D. NetBill Security and Transaction Protocol[C]// Proc. of the 1st USENIX Workshop on E-Commerce. July 1995: 77-88