基于零知识证明身份认证与部分盲签名的电子货币支付模型①

Electonic Cash Payment System Based on Zero – knowledge Proof Identity System and Part Blind Signature

韩 建 叶 琳 洪志全 （成都理工大学 信息工程学院 610059）

摘要：电子商务是通过 Internet 网所进行的商务活动，对于电子商务一个非常关键的要求就是要有一个安全高效的电子货币系统。本文简要分析了电子货币在网络安全方面的需求。同时，就安全电子交易提出了一个具有并行零知识证明身份认证系统以及部分盲签名技术的电子货币安全支付模型。并对此支付模型进行了详细分析和技术探讨。

关键词：电子支付 零知识证明 口令系统 部分盲签名

1 引言

正当 Internet 走进千家万户，网络的普及也带动了电子商务的迅速发展。电子商务是通过 Internet 网所进行的商务活动，对于电子商务而言一个非常关键的要求就是要有一个安全高效的电子现金支付系统。自 1982 年 D. Chaum 发表第一篇关于电子现金系统的论文以来，在电子现金支付系统的研究已取得了很多成果。其主要满足下列四个基本要求：

（1）保密性。在实际的交易环境中必须保护用户订购信息及支付信息的安全，使得只有特定的接收方可访问这些信息。

（2）完整性。在实际交易过程中，接收到的消息确实是实际发送的信息，不可能在传输过程中被非法篡改，也不可能是一条伪造消息。

（3）对于网上交易的参与者，系统必须确定其身份，检验其合法性。若交易者非真实，系统将不准进入，以防止假冒事件发生。

另外，这里"确定"的含义并不完全意味着确实知道客户的身份，因为有时由于交易匿名性的需要，不能确认客户的准确身份，但应能做到保证是在与一个可靠的对象通信。

（4）不可否认性。一旦交易结束，交易各方都不能否认自己参与过这次事务。

为了保证上述电子商务活动的安全性，必须有一套有效的安全机制作为保证，这就要建立电子商务信息安全体系。该体系所包含的内容主要有以下几个层次：基本加密算法、安全认证手段和安全应用协议。其中所用的安全技术通常有：加密技术算法（秘密密钥、公开密钥）、公开密钥系统基础设施（PI）、各种认证技术（一次性口令、数字信封、erberos、数字时间戳、CA）、网络系统各层安协全协议（SSL、SET、IPSEC、PPTP、VPN、TLS）、防火墙及保密网关技术等。尽管上述保证系统安全的技术手段已经存在，但安全问题是系统性的问题。鉴于此，本文提出了一种全新的带有零知识身份认证系统以及部分盲签名技术的电子支付安全模型，并对其安全性能进行了系统的分析与探讨。

① 项目基金：珠海市质量检测局资助项目

2 电子支付

电子支付是指单位、个人通过电子终端，直接或间接向银行业金融机构发出支付指令，实现货币支付与资金转移。电子支付的业务类型按电子支付指令发起方式分为网上支付、电话支付、移动支付、销售点终端交易、自动柜员机交易和其他电子支付。而在电子商务支付系统当中电子现金是我们最常选取的支付方式。

电子现金（E－cash）又称为电子货币（E－money）或数字货币（digital cash），是一种非常重要的电子支付系统，它可以被看作是现实货币的电子或数字模拟，电子现金以数字信息形式存在，通过互联网流通。但比现实货币更加方便、经济。它最简单的形式包括三个主体：商家，用户，银行和四个安全协议过程：初始化协议，提款协议，支付协议，存款协议。

电子现金在其生命周期中要经过提取、支付和存款3个过程，涉及用户、商家和银行等3方。用户与银行执行提取协议从银行提取电子现金；用户与商家执行支付协议支付电子现金；商家与银行执行存款协议，将交易所得的电子现金存入银行。支付模型如下所示。

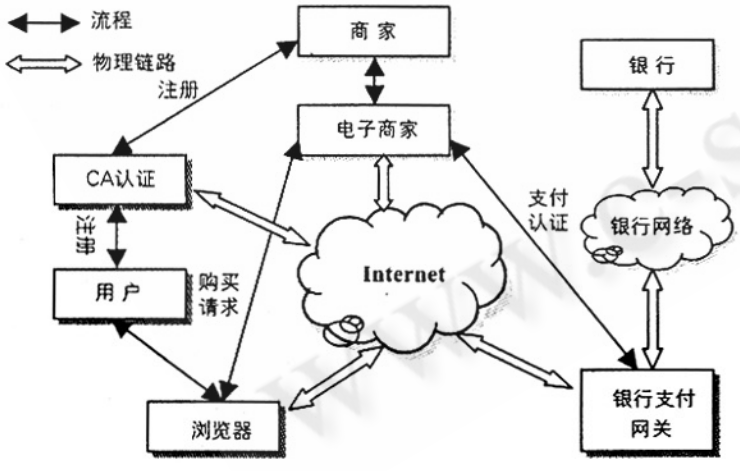

图 1 电子支付模型

3 零知识证明的身份验证系统

根据传统电子支付模型可以发现，在电子现金支付的过程中用户与银行之间的信息传递是最为重要的一环。用户在进行电子交易之前必须与自己的代理银行之间通过注册建立一种安全协议，便于确认在之后的电子交易中用户的真实身份。因此，电子支付需要一个安全的系统来确认用户身份并保障交易是用户本人完成。在本文中提出了一种基于零知识证明的身份验证系统，它将大大提高这一环节的安全性能。

3.1 基本的零知识证明

Jean－Jacques Quisquater 和 Louis Guilou 用一个关于洞穴的故事来解释零知识，见图2，洞穴里面有一个秘密，只有知道咒语的人能打开C和D之间的密门。对其他任何人来说，两条通道都是死胡同。Peggy（P）知道这个洞穴的秘密。她想对 Victor（V）证明这一点，但她不想泄露咒语。下面是她如何使V相信的过程：V站在A点。

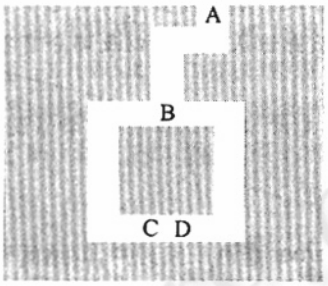

图 2 洞穴示意图

（1）P一直走进洞穴，到达C点或者D点。

（2）在P消失在洞穴中之后，V走到B点。

（3）V向P喊叫，要她：（a）从左通道出来，或者：（b）从右边通道出来

（4）P答应了，如果有必要她就用咒语打开密门。

（5）P和V重复第（1）至第（5）步n次。

基本的零知识协议包括P和V之间的n次交换，可以把它们全部并行完成：

（1）P使用她的信息和n个随机数把这个难题变成n个不同的同构难题，然后用她的信息和随机数解决这n个新难题。

（2）P提交这n个新难题的解法。

（3）P向V透露n个新难题。V无法利用这些新

难题得到关于原问题或其解法的任何信息。

(4) 对这 n 个新难题中的每一个,V 要求 P:a)向他证明新旧难题是同构的,或:b)公开她在第(2)步中提交的解法,并证明它是这个新难题的解。

(5) P 对这 n 个新难题中的每一个都表示同意。

3.2 身份验证系统

基于并行零知识证明的身份验证系统包括身份证明信息(如:口令)、随机数和 N 个不同的同构难题。这种身份验证系统模式不是直接输入口令让系统鉴别,而是用随机数生成 N 个不同的同构难题,知道口令就可以给出这 N 个难题的正确解从而通过系统验证。不知道口令则不可能给出 N 个难题全部正确的解,从而无法通过系统的验证。同时,不知道口令者既使知道 N 个同构难题及其解,也无法得到口令信息。根据并行零知识证明可以设计出满足上述要求的身份验证系统。注册用户验证过程如图 3 所示。

图 3　口令系统验证过程

4 部分盲签名方案的定义

部分盲签名方案是由 Abe 和 Fujisaki 首先提出的。它允许签名者添加一些接收者同意的限制性条款。这样,可以对接收者有所限制,在签名者不知所签署的消息具体内容的情况下,有效地保护签名者的合法权益。

一个部分盲签名方案有三个参与者:签名者、签名接收者、验证者。它有三种算法:密钥生成算法、部分盲签名问题算法、验证算法。

(1) 密钥生成算法是一个概率多项式时间算法,只需要输入一个安全参数,它就输出一个公钥、私钥对。

(2) 部分盲签名问题是一个签名者和接收者之间的交互协议。接收者的公开输入包括签名者与他约定的公开信息。签名者的公开输入包括公开信息和他的公钥。签名者的私人输入包括他的私钥。签名接收者的私人输入包括待签名的消息。当协议中止时,接收者的公开输入显示"完成"或者"未完",接收者的私人信息输出显示"失败"或输出签名者对消息的签名信息。

(3) 验证算法也是一个多项式时间算法,输入签名者的公钥、公开信息和签名信息,输出"接受"或"拒绝"。

5 电子支付安全模型

在现实生活中,人们一般有三种支付方式:现金、支票及信用卡。与之相适应,电子支付协议也可分为这三种模式。随着电子商务的迅速发展,人们越发热衷于一种简单便利的购物方式,这就是网上采购,即用户通过注册代理银行的网站,然后在网上以电子现金的方式与供货商家进行交易。由于这种交易方式是建立在开放的 Internet 之上的,所以在电子支付的过程中系统地安全性能成为人们关注的问题。以下提出一种带有零知识证明身份认证系统以及部分盲签名技术的电子支付模型,并对其安全性进行深入探讨。

5.1 新的电子支付模型概述

该模型是针对 Web 系统网上电子交易设计的,由两部分组成:零知识证明身份认证系统以及部分盲签名的电子现金方案。

5.1.1 初始化协议

首先,在银行 Web 系统中注册用户。注册过程分为两部分完成:

(1) 身份认证。该认证需要用户向银行系统提供一种确认用户身份的证明,如电子版身份证、驾照、护照等等。银行系统将会按照此证明核查用户身份并判断是否可以注册。

(2) 注册。① 银行选择大素数 p,q,满足 $q|p-1$,$g \in Z_p^*$ 且它的阶为 q。② 银行的私钥为 $x \in Z_q^*$,相应的公钥为 $y = g^x \bmod p$。③ H( )是输出在 Z_q 上的公开单向函数。

5.1.2 提款协议

用户想在开通电子支付服务的商家网站中购买商品,商家通过网站建立用户订单并随机选择 $k \in Z_q$,将它通过秘密信道传送给用户,然后用户向银行提出支付请求,并用 $z \in Z_q$ 代表取款金额。银行收到请求后随机生成 n 个同构问题传给用户,用户则按照注册信

息回答问题并将答案反馈给银行，当银行确认 n 个问题全部正确后通过用户的身份验证。以上验证过程采用零知识证明来实现。在银行确认用户的身份之后，用户与银行执行以下协议：

(1) 银行选取随机数 $u,s,d \in Z_q^*$，计算 $a = g^u \bmod p, b = g^s z^d \bmod p$，再将 a,b 发送给用户。

(2) 用户选取随机数 $t_1,t_2,t_3,t_4 \in Z_q^*$，计算

$\eta = g^k \bmod p$

$\alpha = a g^{t_1} y^{t_2} \bmod p$

$\beta = b g^{t_3} z^{t_4} \bmod p$

$\varepsilon = H(\alpha \| \beta \| z \| \eta)$

$e = \varepsilon - t_2 - t_4 \bmod q$

最后将 e 发送给银行。

(3) 银行计算

$c = e - d \bmod q \quad r = r - cx \bmod q$ 再将签名(r,c,s,d)发送给用户。

(4) 用户收到签名(r,c,s,d)后，计算

$\rho = r + t_1 \bmod q \quad \omega = c + t_2 \bmod q$

$\sigma = s + t_3 \bmod q \quad \delta = d + t_4 \bmod q$

验证 $\omega + \delta = H(g^{\rho} y^{\omega} \| g^{\sigma} z^{\delta} \| z \| \eta)$ 是否成立。成立则将 $\{z,\rho,\omega,\sigma,\delta,\eta\}$ 作为电子现金。

5.1.3 支付协议

(1) 用户提供给商家电子现金 $\{z,\rho,\omega,\sigma,\delta,\eta\}$，并用零知识向商家证明他知道 k。

(2) 商家验证 $\omega + \delta = H(g^{\rho} y^{\omega} \| g^{\sigma} z^{\delta} \| z \| \eta)$ 是否成立，来确定该电子现金的有效性。同时由商家自己选取的随机数 k 可以保证商家知道此电子现金是否花费过。

5.1.4 存款协议

商家把 $\{z,\rho,\omega,\sigma,\delta,\eta\}$ 传输给银行，银行检测电子现金的合法性，如果该现金合法则在商家的帐户上添加电子现金中的面额，完成整个电子现金支付过程。

5.2 安全性能分析

以上提出的电子支付模型在身份验证与电子现金交易的过程中具有较高的安全性能。首先，基于零知识的身份验证系统可以保障用户能够重复在别人面前登录银行系统，而不必担心口令泄露。因为同构的难题及其解并未给出关于用户口令的准确信息故增加了口令破解的难度。虽然，这样会增加用户进入系统的复杂性，但是考虑到用户将无须为保障帐户安全经常更换口令而造成的记忆难度，这种代价是值得的。

其次，电子交易的过程运用了部分盲签名的技术，是基于 Abe – Okamoto 部分盲签名方案设计的一种离线电子现金方案。它在支付时不要求银行同时在线，这是在线电子现金不具备的优点。下面对此方案的性质和功能进行简要分析：

(1) 它满足盲签名的四条性质。不可伪造性、不可抵赖性、盲性和不可跟踪性。可以有效地保持签署消息的盲性。

(2) 该部分盲签名方案是基于 Okamoto – Schnorr 忙签名提出的，签名的长度较短，实现速度相对较快。

(3) 因为签名中加入了限制性条款即共识信息，它可以对签名者和接受者的权利和义务以及签署消息的性质加以说明。而且共识信息不容修改，一旦改动签名将不会成立。

虽然该电子现金是不可分的，但是因为采用部分盲签名，所取的电子现金面额可以在现金数据中标明，比用普通盲签名构造的方案具有更大的灵活性。

6 结论

本文介绍了一种基于零知识证明身份验证系统和部分盲签名的电子现金支付模型。这一模型可以利用已有的零知识证明系统和盲签名方案来构筑电子现金，对拓宽研究电子现金的视野具有一定的价值。通过实践证明了在本文的电子现金方案中，攻破电子现金的难度相当于提出的密码学前提假设的难度。在未来的工作中将致力于提高电子现金方案的效率，并试图将方案的安全性建立在更一般性的密码学假设的基础上。

参考文献

1 [美]Bruce Scheier 著，吴世忠、祝世雄、张文政等译，应用密码学，机械工业出版社，2000 年 1 月。

2 D. Chaum, Blind signature for untreaceable payments, In Advance in Cryptology, Proc Crypto' 82, Lecture Notes in Computer Science, Springer – Verlag, 1983, 199 – 203.

3 M. Abe, T. Okamoto, Provably Secure Partially Blind Signatures, Crypto' 2000, LNCS, Vol. 1880, 271 – 286.

4 陈良、高成敏，网络安全技术与应用，2005.4 52 – 54。