

一种基于智能卡的匿名公平移动支付系统

程杰仁^{1,2} 蔡志平¹ 殷建平¹ 张 玲¹

(国防科技大学计算机学院 长沙 410073)¹ (湘南学院数学系 郴州 423000)²

摘 要 提出了一种基于智能卡的匿名公平移动支付系统模型,基于该模型提出了一个可追踪匿名的脱线式数字现金协议,它使用智能卡作为分布匿名代理,实现了数字现金的动态匿名和兑零的功能;证明了匿名数字现金满足安全性和可追踪匿名性,该协议的效率高基于盲签名和匿名代理服务器技术的协议。提出了一个关于时间敏感商品的公平移动支付方案,即使用智能卡实现交易中中介功能,减少了使用时间戳和全局统一时钟的代价。业已证明该方案是公平的。

关键词 移动支付,时间敏感商品,智能卡,数字现金,可追踪匿名,公平性

中图法分类号 TP309 **文献标识码** A

Fair and Anonymous Mobile Payment System Utilizing Smart Card

CHENG Jie-ren^{1,2} CAI Zhi-ping¹ YIN Jian-ping¹ ZHANG Ling¹

(School of Computer Science, National University of Defense Technology, Changsha 410073, China)¹

(Department of Mathematics, Xiangnan University, Chenzhou 423000, China)²

Abstract A fair and anonymous mobile payment system model utilizing smart card was proposed. An anonymous off-line digital-cash payment protocol was presented. It uses smart card as a distributed anonymity provider agent based on Schnorr signature scheme. It provides dynamic accountable anonymity and changing for digital-cash. It was proved that secure and accountable anonymity of digital-cash was guaranteed. The protocol was proved efficiency in mobile environments. A protocol for fair exchange time-sensitive goods was proposed. Our approach utilizes smart card on the customer's side partly taking over the duties of the intermediary party. Besides supporting disconnected operations, our approach also allows the proper handling of time-sensitive items, a feature that previous protocols lack.

Keywords Mobile payment, Time-sensitive, Smart card, Digital cash, Accountable anonymity, Fairness

1 引言

移动支付是使用个人移动设备为购买商品或者服务而提供的支付过程。个人移动设备包括移动电话、PDA 和移动电脑等。使用移动设备支付的两大优势是设备的安全性和方便性。个人移动设备属于用户专有,因此与 PC 机相比不容易泄密,用户可以在任何无线网络能覆盖的场所进行支付以及通过移动设备浏览交易日志、帐单等。但是由于个人移动设备使用电池运行时间短,其处理器计算能力和存储有限,因而移动设备很难支持复杂的密码运算,如公钥加解密和签名等。无线网络可靠性差,数据包容易丢失,移动设备经常断连,重传数据包使得支付所需的时间加长,因此不适合购买时间敏感商品。

目前已有的移动支付系统可以概括为基于代理、基于移动 Agent 和无代理的三类移动支付系统。它们基本上属于在线支付系统即在支付过程中商家需要银行协助验证数字现金的有效性,当银行同时收到大量的数字现金验证请求时,系统执行效率较低。在线支付系统一般不考虑匿名。由于顾客不

希望自己的购买记录、地址或其他购买信息被商家或者银行追踪,因此匿名性成为了支付系统是否被用户接受的一个关键因素。因此在顾客计算资源有限、网络带宽有限、无线网络可靠性低的移动通信环境中实现可追踪匿名的脱线支付系统是非常重要的。

Chaum^[1]率先基于盲签名算法设计了脱线式匿名数字现金,它对顾客的计算能力要求高,顾客与银行之间需多次通信,开销大。Chan 等^[2]提出了可证明安全脱线的 e-cash 方案,匿名性基于 RSA 的安全性。Wang^[3]基于 Schnorr 的不可抵赖签名算法实现匿名性,他使用匿名代理服务器构造匿名数字现金,该签名算法的效率比 RSA 的高。Asokan, Zhou, Vogt, Qing 和 Kremer^[8-13]等在公平性(fairness)研究领域有较好的研究成果。他们设计了固定网络环境下的非否认公平协议并且分析了协议的公平性。Vogt^[4]提出了在移动环境中实现公平交易的初步方案。但是以上协议对顾客的计算能力和网络性能要求较高,只适合于使用 PC 机的固定网络环境,而且固定服务器作为一个可信计算环境(Trusted Processing Environment, TPE)需要严格的安全策略,如果大量

到稿日期:2010-03-15 返修日期:2010-06-16 本文受国家自然科学基金资助项目(60603062, 60603015),高等学校全国优秀博士学位论文作者资助项目(2007B4),湖南省教育厅科研项目(07C718),公安部应用创新计划(2007YYCXHNST072)资助。

程杰仁(1974—),男,博士生,讲师,主要研究方向为信息安全, E-mail: cjr22@163.com; 蔡志平 博士,主要研究方向为信息安全; 殷建平 教授,博士生导师,主要研究方向为人工智能、模式识别、信息安全等; 张 玲 博士,主要研究方向为信息安全。

顾客同时向服务器请求盲化数字现金,会使服务器负载过重,产生瓶颈。目前智能卡在电子支付领域应用广泛。其主要用于专用网络的支付和互联网络的支付,如 IC 电话卡,电子钱包。若将智能卡作为一个 TPE,与昂贵的 IBM 4758 PCI 卡相比,智能卡相对便宜,但是其处理和存储能力有限,因而智能卡是一个不能完全可信的 TPE。Karjoth 已经证明只要关键运算(如加解密和签名)基于可信硬件环境,其他处理(如对密文的运算)可以在非可信环境下进行^[14]。因此,本文提出了一种基于智能卡的匿名公平移动支付系统。

2 基于智能卡的匿名公平移动支付系统模型

本节将移动支付系统定义为四元组 $MP = \langle G, GE, PT, Trust \rangle$, 其中

G : 集合 $G = \{C, M, PSP, O, A, S\}$ 表示参与支付过程的主体集合。 C 代表顾客, M 代表商家, PSP 代表移动支付运营商, PSP 可以是银行、移动运营商、信用卡公司或者他们的联盟, O 代表顾客的开户银行, A 代表商家的存款银行, S 代表智能卡。

GE : 集合 $GE = \{MD, WN, FN\}$ 表示支付系统中的通信环境。其中 MD 代表移动设备, WN 代表无线网络, FN 代表固定网络。

PT : 表示支付系统使用的安全支付协议。本文的系统采用了脱线式的数字现金协议。协议包括取款、支付、存款 3 个子协议, 分别描述了现金的生成、流通和消亡的过程。

$Trust$: 表示 G 中主体存在的信任关系。假定 G 中主体存在如下信任关系: C 和 M 相信 O 、 A 和 PSP 不会泄露他们的私有信息并且遵守协议, 下面将 O 、 A 和 PSP 都用银行代替表示为 B 。 C 和 M 都相信智能卡遵守协议。 C 和 M 互不信任, 他们的任意一方可能会伪造消息或者抵赖。

安全移动支付系统包括 3 个独立的阶段^[6]: 身份认证、鉴别和安全实现。身份验证 (Identification): 移动设备通过个人密码或者声音验证合法用户身份。认证/鉴别 (Authentication): 交易提供商通过用户的身份 (如用户的移动电话号码) 或者密码机制 (数字签名或者安全协议, 如 WTLS) 认证用户的支付请求。安全实现 (Secure performance): 支付由交易提供商和商家通过执行安全支付协议 (iKP/SET) 完成。移动支付提供商与移动设备采用的通信协议无关。

图 1 所示的移动支付系统模型中, 顾客 C 使用 PIN 码通过移动设备 (手机) 的身份验证后, 移动设备在无线网络 WN 中发送顾客的支付请求, 无线网络运营商 PSP 收到请求并认证顾客的身份后, 将请求转交到固定网络 FN 的支付系统, 系统通过执行安全支付协议完成支付。

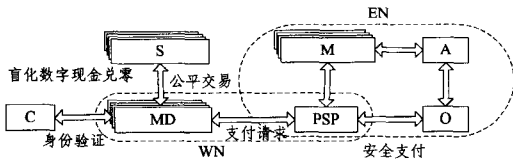


图 1 移动支付系统模型

智能卡 S 可以嵌入在移动设备中或者作为移动设备可配置的附件。智能卡 S 与商家 M 之间有特殊的接口通信。假定智能卡 S 和其他系统参与者之间的通信是安全的: 没有窃听、重放、伪造消息。智能卡用于分布匿名代理和公平交易, 由银行颁发给顾客。假定智能卡 S 应满足以下条件:

防篡改: 窃听者不能读取存储在智能卡上的敏感信息, 不能改变智能卡的行为。

消息的真实性: 智能卡嵌入有顾客的签名私钥, 能生成签名, 对应的公钥是经过银行认证的。同时智能卡嵌入认证机构的公钥, 用于验证与之通信的主体的公钥证书, 鉴别消息者的身份。

可靠状态信息: 智能卡存储交易的数据 (如商品和支付信息等) 即使断电也不会丢失信息。智能卡能发送交易状态的签名信息, 当恢复通信故障时智能卡能恢复故障发生时的状态信息。

3 基于智能卡的脱线式匿名数字现金协议

本文的支付系统所使用的安全支付协议是基于 Schnorr 不可抵赖签名算法提出的可追踪匿名的脱线式数字现金协议。该协议使用智能卡作为分布匿名代理实现数字现金动态匿名和兑零功能。可追踪匿名 (accountable anonymity)^[6] 指被合法使用的数字现金中隐藏的顾客身份信息不会泄露给商家和银行, 但是如果数字现金被重复使用, 则通过重用的数字现金可以追踪到隐藏的顾客身份信息。脱线式的数字现金协议是指商家不需要银行协助验证数字现金的有效性。动态匿名是指用户可以选择是否使用匿名数字现金。数字现金的兑零是指将数字现金转换为多个小面值的数字现金, 总的面值不变。

3.1 密码学基础和相关定义

离散对数假设 (DLA) 是假设离散对数问题的求解在多项式时间内不可计算的。Schnorr 的不可抵赖签名算法的安全性是基于 DLA 的。不可抵赖数字签名指签名验证 (鉴别) 需要签名者的合作, 其基本思想是签名者向验证者出示签名; 验证者产生一个随机询问因子给签名者; 签名者使用询问因子和私人密钥进行计算, 将计算结果送给验证者; 验证者确认结果。Schnorr 算法产生签名所需的大部分计算都可在预处理阶段完成, 对于相同的安全级, 它的签名长度比 RSA 和 ElGamal 短。Schnorr 鉴别和签名方案见表 1。

表 1 Schnorr 鉴别和签名方案

参数配置	选取两个素数 p 和 q , q 是 $p-1$ 的素数因子。然后选择 $g \in Z_p$ ($g \neq 1$) 满足 $g^q \equiv 1 \pmod{p}$, (p, q, g) 公开。签名者选择随机数即签名私钥 $sk \in Z_p$, 对应的公钥 $pk = g^{sk} \pmod{p}$
鉴别协议	假定签名者向验证者证明他的身份和签名一致, 则他们执行鉴别协议: 1. 签名者选取随机数 $r \in Z_p$, 计算 $x = g^r \pmod{p}$, 这是预处理步骤。 2. 签名者将 x 传送给验证者。 3. 验证者选择一个随机数 $e \in \{0, \dots, 2^t - 1\}$ 传送给签名者 (安全性基于参数 t , 破解该算法的难度大约是 2^t)。 4. 签名者计算 $y = r + se \pmod{q}$ 。然后将 y 传送给验证者。 5. 验证者确认 $x = g^y pk^e \pmod{p}$ 成立, 则接收签名的身份证明。
签名协议	假定签名者使用签名私钥 sk 对消息 m 进行签名, 他执行以下步骤: 1. 选取随机数 $r \in Z_p$, 计算 $x = g^r \pmod{p}$, 这是预处理步骤。 2. 计算 $e = H(m, x)$ 。 3. 计算 $y = r + se \pmod{q}$, e 和 y 即为签名。签名者将 e 和 y 传送给验证者。 4. 验证者计算 $x' = g^y pk^e \pmod{p}$, 然后确认 $e = H(m, x')$ 是否成立。如果成立则签名有效。

假定 p 和 q 是两个大素数, q 是 $p-1$ 的素数因子。选择 $g \in Z_p$ ($g \neq 1$) 满足 $g^q \equiv 1 \pmod{p}$ 。假定 Y 是银行的公钥, sk 是顾客的私钥, $I = g^{sk} \pmod{p}$ 是顾客的身份字。 $H(x, y)$ 是单向散列函数。 $a \in_R A$ 表示从集合 A 中随机选取元素 a 。下面

是数字现金协议中将用到的定义。

定义 1(数字现金) 数字现金 $c=(a=g^r, b=Y^r I^s)$ 。顾客随机选择 $r, s, s \in_R Z_p, s, sk$ 是顾客的私有信息。

定义 2(数字现金证书) 数字现金证书 $Cert_c$ 是一种用于验证数字现金的币值和授权的数字签名文件。签名文件包含有数字现金的币值和银行的授权信息等。

定义 3(匿名数字现金) 匿名数字现金 c' 是数字现金 c 的盲化。 $c'=(a'=g^{r'p}, b'=Y^{r'p} I^s)$ 。其中 $\rho \in_R Z_p$ 是顾客的私有信息。

定义 4(匿名数字现金与数字现金的等价性) 已知数字现金 c 和匿名数字现金 $c', m=h^e (h \in Z_p \text{ 公开})$, 则 c' 与 c 等价当且仅当 $\log_a m = \log_{g^a} (a'/a) = \log_y (b'/b)$, 其中 m 称为 c 和 c' 的等价因子。

定义 5(数字现金产权证书) 顾客选择随机数 $r \in Z_p$, 计算 $t=Y^k g^s \pmod p$ 和 $e=H(m, t)$, 其中 m 是 c 与系统当前时间值的组合, 计算 $u=k-re, v=s-sk * e$ 和 $t_1=g^{(s-1)*e} \pmod p$, 计算签名 $S=(e, u, v, t_1)$ 和 (m, t) , 则 (S, m, t) 称为数字现金 c 的产权证书 $Claim_c$ 。

当证明者要向验证者证明他能构造数字现金 c , 则只需要向验证者出示 c 的产权证书 $Claim_c$ 。验证者计算 $t'=Y^u g^{vb} \pmod p$ 后, 验证等式 $t'=tt_1 \pmod p$ 和 $e=H(m, t'/t_1)$, 如果成立, 则验证者认为证明者确实能构造 c 。

定义 2 的数字现金证书用于验证数字现金是否经过银行授权、数字现金的币值等。数字现金存储在电子钱包中。移动设备的防篡改硬件或者智能卡都可以充当电子钱包。定义 3 的匿名数字现金是确保在不透露私有信息的前提下顾客向商家和银行出示数字现金产权证书以证明其确实能构造该数字现金。

3.2 脱线式匿名数字现金协议

3.2.1 基本流程

数字现金协议包括取款、支付和存款等子协议, 描述如何构造、使用和销毁数字现金。如图 2 所示, 取款子协议由顾客发起, 顾客将构造的数字现金传给银行, 银行授权签署数字现金证书。如果顾客使用匿名数字现金, 请求匿名代理盲化数字现金, 用户与代理遵循盲化数字现金子协议。支付子协议由顾客发起, 顾客在商家处使用数字现金, 商家验证数字现金。实现脱线式数字现金要解决的主要问题是防止双重花费。在存款子协议中, 银行能通过重用的数字现金追踪双重花费者的身份, 从而防止双重花费。

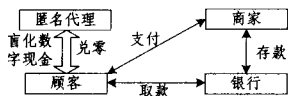


图 2 脱线式匿名数字现金协议

3.2.2 智能卡实现分布匿名代理 (Distributed Anonymity Provider Agent)

Wang 使用匿名代理服务器实现匿名代理。匿名代理是经过公正的可信任实体, 为顾客生成匿名数字现金证书。匿名代理服务器用于移动通信环境存在的问题是: (1) 匿名代理服务器可能成为瓶颈; (2) 固定服务器作为一个 TPE 需要严格的安全策略; (3) 匿名服务器与顾客之间通过移动网络连接, 网络可靠性不高; (4) 匿名代理服务器与银行联合, 能根据数字现金计算出顾客的身份字, 对顾客是潜在的风险。因此本节考虑将匿名代理的功能分散至各移动用户端, 使用智能

卡实现分布的匿名代理功能。智能卡接收顾客的匿名数字现金 c' 、数字现金 c , c' 与 c 的等价因子 $m=h^e (h \in Z_p \text{ 公开})$ 和 m 的 Schnorr 签名 S_m 。它验证 c' 和 c 等价后生成 c' 的数字证书 $Cert_{c'}$ 并传给顾客。智能卡实现匿名数字现金和兑零功能见表 2。

表 2 智能卡实现匿名数字现金和兑零

1	C→S	c, c', S_m, m
2	S	验证 c, c' 的等价性 $Cert_{c'}$ 或者 $(Cert_{c'}, Cert_{c'}, \dots, Cert_{c'})$ (n 代表将 c' 兑换的小面值的数字现金的个数, 每个数字现金的面值可以不同, 但是总额不变)
3	S→C	

智能卡实现分布匿名代理功能具有如下特点:

提高了移动设备与匿名代理之间通信可靠性, 移动设备与匿名代理服务器之间通过无线网络的通信由移动设备与本地智能卡之间的通信代替, 大大地提高了效率。

智能卡匿名代理只负责为单个用户构造匿名数字现金, 不会出现为多个用户构造匿名数字现金进行并行处理的现象, 解决了代理服务器的性能瓶颈问题。

智能卡使用防篡改技术, 因此匿名代理的私钥不会被读取和篡改。

3.2.3 脱线式匿名数字现金协议

表 3 给出了一个基于智能卡的脱线式匿名数字现金协议。

表 3 脱线式匿名数字现金协议

参数设置	选择两个大素数 p, q 使得 $ p-1 =\delta+k, p=\gamma q+1$, 其中 δ 是特定的常数, k 为系统的安全系数, γ 为一小整数。定义乘法群 Z_p^* 的阶为素数 q 的子群 G_q 以及 G_q 的生成元 g 。 $H: G_q \times G_q \rightarrow Z_p$ 是单向散列函数。 p, q, g, H 公开。
银行初始化	银行选取 $sk_B \in_R Z_q$ 作为私钥, 公钥 $Y=g^{sk_B} \pmod p$ 。银行建立三个数据库: 一是帐号数据库, 用于存储用户身份字及基本信息; 二是提款数据库, 用户存储用户的提款信息; 三是存款数据库, 用于存储用户的支付信息。银行选择卡密钥 $sk_S \in_R Z_q$, 计算并公布 $pk_S=g^{sk_S}$ 。
顾客初始化	顾客选取 $sk_U \in_R G_q$ 作为私钥, 将 $I=g^{sk_U} \pmod p$ 作为其与银行联系的身份字。银行发给顾客智能卡 S , S 中写有 sk_S 。
取款子协议	Step1. 顾客计算数字现金 $c=(a=g^r, b=Y^r I^s), r, s \in_R Z_p, s$ 是顾客的私有信息。 Step2. 顾客使用私钥 sk_U 对 (c, t) (t 是当前的系统时间值) 计算 Schnorr 签名 $S(c, t)$ 。 Step3. 顾客将 $(c, S(c, t), r, D)$ 传送给银行。 Step4. 银行验证 c 是正确构造后, 从顾客帐户划款, 然后将 c 的证书 $Cert_c$ 传送给顾客, 银行保存顾客的提款信息, 顾客保存 $(r, s, Cert_c)$ 。
盲化数字现金协议	Step1. 顾客选取随机数 $\rho \in_R Z_q$ 计算匿名数字现金 c' 。 Step2. 顾客使用私钥 sk_U 对消息 $m=h^e (h \in Z_q \text{ 公开})$ 计算 Schnorr 签名 S_m 。 Step3. 顾客将 (c, c', S_m, m) 传送给 S 。 Step4. S 验证 $Cert_c$ 和 m 的签名 S_m 有效, 并且验证 c 和 c' 等价后构造 c' 的数字证书 $Cert_{c'}$ 并传送给顾客。 S 保存 (c, c', S_m, m) , 顾客保存 $(r, s, c', Cert_{c'})$ 。
支付子协议	顾客将 $(c', Cert_{c'}, Claim_{c'})$ 传送给商家, 商家验证 $Cert_{c'}$ 和 $Claim_{c'}$ 。
存款子协议	商家将 $(c', Cert_{c'}, Claim_{c'})$ 传送给银行, 银行验证数字现金证书有效后, 查询支付信息数据库, 检测如果没有重复消费才为顾客存款。银行保存用户的支付信息。

3.3 匿名数字现金的安全性和可追踪匿名性分析

3.3.1 匿名数字现金安全性分析

脱线式匿名数字现金协议包括取款子协议、支付子协议和存款子协议。取款子协议在顾客 C 和银行 B 之间进行, 协议以输入顾客的身份字 I 开始, 以输出数字现金 τ 结束; 支付

子协议在 C 和 M 之间进行,协议以输入数字现金 τ 开始,以输出已经花费的数字现金 τ' 结束;存款子协议在 M 和 B 之间发生,以输入 τ' 开始,输出已存款的数字现金 τ'' 结束。数字现金是安全的当且仅当协议满足不可重用性、不可扩展性、不可伪造性和不可追踪性^[7]。

定义 6(安全数字现金) 数字现金是安全的当且仅当协议满足:

不可重用性(unreusable) 假定支付子协议中顾客 C 两次输入同一个数字现金 τ ,则 C 的身份信息 Id 在多项式时间内可以通过已存款的数字现金 τ_1 和 τ_2 计算出来。

不可扩展性(unexpandable) 假定顾客已经进行了 n 次取款,即已经获得了 n 个数字现金 τ ,则攻击者不可能单独在多项式时间内计算出第 $n+1$ 个数字现金。

不可伪造性(unforgeable) 银行、商家和代理不能在多项式时间内计算数字现金 τ 成功地用于支付。

不可追踪性(untraceable) 假定银行 B 和商家 V 分别在顾客 C_i 取款和支付子协议时获得的知识为 V_B^i 和 V_V^i ,则对任意 $i, j \in N$,银行和商家即使知道 V_B^i, V_B^j 和 $V_V^i \in_R \{V_V^i, V_V^j\}$,也不能在多项式时间内计算一个顾客的身份字 $l \in \{i, j\}$ 。

根据安全数字现金定义,下面对本文提出的匿名数字现金协议进行安全性分析。

定理 1 匿名数字现金满足不可重用性。

证明:假定商家在两次支付中收到匿名数字现金 c' , $Claim_{c'}$ 和 c' , $Claim_{c'}$, $S_1 = (e_1, u_1, v_1, t_{11})$, $S_2 = (e_2, u_2, v_2, t_{12})$,其中

$$u_1 = k_1 - re_1 \pmod{q}, v_1 = s - sk_U * e_1 \pmod{q}$$

$$u_2 = k_2 - re_2 \pmod{q}, v_2 = s - sk_U * e_2 \pmod{q}$$

当商家将这两个匿名数字现金存入银行时,银行计算 $(v_2 - v_1)/(e_1 - e_2) = sk_U$, sk_U 是顾客的私钥。因此如果数字现金 c' 被重复使用,则银行能在多项式时间内计算出顾客的私钥 sk_U 。

定理 2 匿名数字现金满足不可扩展性。

证明:由于顾客在整个协议过程中不会出示私钥 sk_U 和随机数 s ,并且顾客构造的不同数字现金对应的随机数 s 的值不同。因此即使伪造者看到了 n 个合法数字现金,他也不知道顾客的私钥和 s ,从而无法构造第 $n+1$ 个合法的数字现金。

定理 3 匿名数字现金满足不可伪造性。

证明:构造有效的数字现金包括构造数字现金 $c = (a = g^r, b = Y^r I)$ 和 c 的 Schnor 签名 $S_{(c, I)}$ 两个部分。虽然银行知道 I 能够构造 c ,但是银行不知道顾客的私钥 sk_U ,因此不能构造 $S_{(c, I)}$ 。同理匿名代理和商家也不能构造有效的数字现金。系统执行完取款子协议后,银行和匿名代理可能拥有有效的数字现金,但是他们不能使用,因为在支付子协议中,还需要顾客提供产权证书 $Claim_c$ 或 $Claim_{c'}$,构造 $Claim_c$ 或 $Claim_{c'}$ 需要顾客的私钥。同理商家也无法构造数字现金。

定理 4 匿名数字现金满足不可追踪性。

证明:通过提款子协议,银行拥有数字现金 c 、数字现金证书 $Cert_c$ 、随机数 r 和顾客身份字 I 。通过支付子协议,商家拥有匿名数字现金 c' 、数字现金证书 $Cert_{c'}$ 和产权证书 $Claim_{c'}$ 。假定银行与顾客 C_1 和 C_2 执行取款子协议后分别拥有的知识为 $(c_1, Cert_{c_1}, r_1, I_1)$ 和 $(c_2, Cert_{c_2}, r_2, I_2)$,商家与顾客 C_1 和 C_2 执行支付子协议后分别拥有的知识分别为 $(c_1', Cert_{c_1'}, Claim_{c_1'})$ 和 $(c_2', Cert_{c_2'}, Claim_{c_2'})$ 。由于银行和商

家不能在多项式时间内根据 $(c, Cert_c, r, I)$ 和 $(c', Cert_{c'}, S, m, t)$ 计算用户构造数字现金的私钥 sk_U 和 s ,因此他们即使获得了 C_1 和 C_2 的取款信息和两个顾客的支付信息,也不能在多项式时间内计算出是顾客 C_1 或者 C_2 的支付信息。因此数字现金满足不可追踪性。

3.3.2 匿名数字现金的可追踪匿名性

若匿名数字现金被正确使用,则其隐藏的客户身份信息不会泄露给商家和银行,但是如果被重复使用,则它隐藏的身份信息可被追踪。

定理 5 匿名数字现金满足可追踪匿名性。

证明:首先证明如果匿名数字现金被正确使用,则匿名数字现金中隐藏的客户身份字不会泄露给商家和银行。在支付子协议中,商家收到 $(c', Cert_{c'}, Claim_{c'})$ 。基于 DLA,商家不能在多项式时间内由 c' 计算出顾客的私钥 sk_U 和 s ,因此商家不能计算顾客的身份字。银行在取款协议后拥有 $(c, Cert_c, r, I)$,在存款协议后拥有 $(c', Cert_{c'}, Claim_{c'})$,根据定理 4,银行不能将顾客的支付信息和提款信息对应起来,因此银行也不能从 $(c', Cert_{c'}, Claim_{c'})$ 获知顾客的身份字。然后证明如果重复使用匿名数字现金,则匿名数字现金中顾客的身份字可被追踪,见定理 1 的证明。

3.4 协议的效率分析

用户期望提交购买请求到收到商品的这段时间即支付处理的时间尽可能短。支付处理速度与计算代价和通信开销有关。计算代价是考虑签名、验证签名、加解密和哈希等密码运算消耗的资源,其中以签名和验证签名最为消耗资源,本节以这两种运算的次数衡量计算代价。通信开销用传送消息数目衡量。在本文的支付子协议中,计算代价是商家验证数字现金证书和产权证书两次验证签名运算,顾客没有计算负荷,也没有通信开销。与 Chaum 的盲签名数字现金相比,它适合计算力差的移动顾客的支付处理。顾客可以在空闲时间预先计算数字现金产权证书。为了减少去银行取款的次数,顾客可以预先一次性购买大面值的数字现金,然后使用时再到匿名代理处兑零,减少了与银行的通信开销。由于顾客和智能卡之间的通信没有网络延迟,因此提高了取款的效率。Wang 实现匿名数字现金的方法中,顾客和匿名代理服务器之间有网络通信延迟,而且当大量顾客同时向服务器发送请求时,会降低服务器的性能。由于移动顾客与网络断连的情况时常发生,使用 Wang 的方法实现匿名数字现金的效率低。本文方法使用智能卡来实现匿名代理,增加了匿名代理和顾客之间通信的可靠性,即使顾客断连也不会影响生成匿名数字现金的效率。

因此本文提出的用智能卡在不降低安全性的前提下,减小了通信开销和避免了处理瓶颈,提高了协议的效率。

4 基于智能卡的匿名公平支付系统

4.1 公平移动支付系统

移动支付系统中,非面对面的顾客和商家是互不信任的,系统中的任意一方总担心另一方在支付过程中处于比自己更加有利的位置,从而使自己蒙受损失。公平的移动电子支付方案和协议就是为解决这类问题而设计的。本节在 Vogt 的基础上提出了一个可以使用匿名数字现金购买时间敏感商品和一般商品的公平移动支付系统方案。

时间敏感商品是指商品具有保质期的商品,超过保质期

后商品就失去了其使用价值,例如股票交易等实时数据、与移动设备位置相关的数据。假定某人 A 想在东风路住宿,因此用手机查询这条街道上的旅馆信息,然而当他走到五一路才收到东风路的旅馆信息,这时他已经不想回到东风路了,因此收到的东风路的旅馆信息对他没有用处。无线网络由于可靠性低,因此可能延迟商品传送的时间,当顾客收到商品时,商品已经过期。这对顾客是不公平的。这时顾客可以通过请求取消或完成该交易恢复公平性。当出现争议时,通过可信任第三方(Trusted Third Part, TTP)作为仲裁者加以解决,本文考虑让银行担当 TTP 功能。TTP 由于只在出现争议时才使用,在支付过程中不涉及,因此是乐观意义上的公平交易。

顾客 C 首先发起主协议,他将数字现金及验证信息等传送智能卡 S;智能卡转交给商家 V;商家验证数字现金有效后才将商品传送给智能卡;智能卡收到商品后询问顾客是否过期;若没有过期顾客通知智能卡继续交易;智能卡将商品传送给顾客;顾客验证商品。如果商品过期,或者商品经过验证不是顾客期望的或者顾客长时间未收到商品,对顾客都是不公平的。这时顾客通过发起撤销协议来恢复他的公平性。顾客向智能卡发送撤销交易请求,这时智能卡可能:1. 还没有将支付传送给商家,智能卡只需删除数字现金和商品等信息,将交易状态重置为初始状态;2. 已经将商品传送给顾客则忽略顾客请求;3. 其他的情况下,请求银行撤销顾客的支付,智能卡将其当前记录的状态信息传送给银行,状态信息证明他还没有将商品项传送给顾客,这样才能保证公平性。银行取消顾客的支付后通知智能卡,智能卡重置状态,如取消存储的商品。基于数字现金的公平支付主协议和撤销协议分别见表 4 和表 5。在支付系统中,顾客可以根据自己的需要来选择是否使用匿名的数字现金。

表 4 基于数字现金的公平支付主协议

1	V→S	数字现金,证书,产权证书
2	S→V	数字现金,证书,产权证书
3	V	验证数字现金
4	V→S	时间敏感商品,商品校验信息
5	S→C	询问顾客商品过期
6	C→S	商品仍在保质期内顾客同意继续交易
7	S→C	传送商品和商品验证信息
8	C	验证商品

表 5 基于数字现金的公平支付撤销协议

7'	C→S	撤销请求
8'	S→B	状态信息
9'	B	验证状态撤销支付
10'	B→S	撤销支付
11'	S	重置状态

4.2 效率及公平性分析

顾客与智能卡之间的通信没有网络通信延迟,因此顾客向智能卡传送数字现金,智能卡向顾客传送商品所需的时间通信时间很短,所以在效率上几乎等同于商家和顾客之间的直接交易。引入智能卡充当交易中介,避免了使用全局同步时钟和时间戳,减小了系统的开销。如果不使用智能卡充当中介,则顾客声明其收到的商品过期,需要提供证据证明其何时收到商品,因为不诚实的顾客可能会故意撒谎说是在保质期后收到的商品,这样需要引入时间戳和全局同步时钟,从而增加系统的开销。

协议对顾客是公平的,只要顾客还没有收到商品或者收到的商品过期,或者商品不符合顾客的期望,他可以发起撤销

协议来收回他的支付。协议对商家是公平的,只有当顾客没有收到商品时,支付才可能被撤销。由于使用脱线式的数字现金支付协议,商家验证数字现金不需要与银行联系。因此商家只有收到了有效的支付后才会传送商品,保证了对商家的公平性。如果数字现金被重复使用,商家存款时,银行能够检测顾客的身份。银行强制顾客付款恢复商家的公平性。

该方案也适用于一般商品的公平交易。它使用智能卡实现交易中介功能,减少了使用时间戳和全局统一时钟的代价,通过分析证明系统满足公平性。

结束语 本文给出了一种基于智能卡的匿名公平移动支付系统。提出了一个匿名的脱线式数字现金协议,即将智能卡作为分布匿名代理实现数字现金的动态匿名和兑零功能。证明了该数字现金是安全的且满足可追踪匿名性,与 Chaum 和 Wang 的数字现金比较,效率更高,移动顾客承担的计算负荷更小,降低了通信开销和避免了处理瓶颈,可以应用于移动环境下的匿名支付。提出了一个关于时间敏感商品的公平移动支付方案,即使用智能卡实现交易中介功能,以减少使用时间戳和全局统一时钟的代价。通过分析证明系统是公平的,可以用于移动环境下的时间敏感商品和一般商品的公平交易。

参 考 文 献

[1] Chaum D. Blind Signature for Untraceable Payments[C]//Proceedings of Advances in Cryptology. 1983;199-203

[2] Chan A, Frankel Y, Tsionis Y. An Efficient Off-Line Electronic Cash Scheme as Secure as RSA[R]. NU-CCS 96-03. Northeastern Univ., 1995

[3] Wang H, Cao J, Zhang Y. A Flexible Payment Scheme and Its Role-Based Access Control[J]. IEEE Transactions Knowledge and Data Engineer, 2005, 17(3):425-436

[4] Vogt H, Gärtner F C, Pagnia H. Supporting Fair Exchange in Mobile Environments[J]. Journal on Mobile Networks and Applications, Kluwer Academic Publishers, 2003, 8(2):127-136

[5] Herzberg A. Payments and banking with mobile personal devices[J]. Communications of the ACM, 2003, 46(5):53-58

[6] Nambiar S, Lu C T, Liang L R. Analysis of Payment Transaction Security in Mobile Commerce[C]//Proceedings of the 2004 IEEE International Conference on Information Reuse and Integration (IEEE IRI-2004). 2004;475-480

[7] Franklin M K, Yung M. Secure and Efficient Off-line Digital Money[C]//ICALP'93 LNCS 700. Springer Verlag, 1993

[8] Qing S H, Li G C. A formal model of fair exchange protocols [J]. Science in China Series F-Information Sciences, 2005, 48(4):499-512

[9] Asokan N. Fairness in Electronic Commerce[D]. University of Waterloo, Ontario, Canada, 1998

[10] Kremer S, Markowitch O. Fair multi-party Non-repudiation Protocols[J]. International Journal on Information Security, 2003, 1(4):223-235

[11] Zhou J, Gollmann D. A Fair Non-repudiation Protocol [C]//Proc. IEEE Symposium on Security and Privacy. 1996;55-61

[12] 邓所云, 詹榜华, 胡正民, 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

[13] 陈恺, 杨波, 王育民, 等. 利用电子钱包的有效的公正支付系统[J]. 计算机学报, 2001, 24(11):1-5

[14] Karjoth G, Lange D B, Oshima M. A security model for aglets [J]. Lecture Notes in Computer Science, 1998, 1419:188-205