电子支付研究综述

徐 明[1],张祥德[2]
(1.石家庄铁道学院 数理系,河北 石家庄 050043;
2.东北大学 理学院,辽宁 沈阳 110004)

摘 要:电子支付是电子商务的一个重要组成部分,它是指允许用户通过电脑、电话、传真机等途径完成支付的一种支付手段,如何安全可靠方便地实现电子支付,是电子商务发展中迫切需要解决的问题。介绍了电子支付制度的基本概念以及电子支付的一般模型,随后对电子支付制度做了分类,并深入探讨了各类电子支付系统的主要特点和相关实例,最后,基于对安全电子支付系统发展现状和未解决问题的分析,指出了今后该领域的研究方向。

关键词:电子支付;电子现金;盲签名;电子钱包
中图分类号:F724.6 **文献标识码**:A **文章编号**:1673-629X(2007)09-0213-04

Survey of Electronic Payment System

XU Ming[1], ZHANG Xiang-de[2]
(1. Department of Mathematics & Physics, Shijiazhuang Railway Institute, Shijiazhuang 050043, China;
2. School of Science, Northeastern University, Shenyang 110004, China)

Abstract: The electronic payment is an important part of E-commerce. It is such a payment means that people can pay for the goods by computer, telephone or fax. How to accomplish electronic payment securely and conveniently is a pressing problem to be solved in the development of E-commerce. In this paper, introduce the basic concept and the common model of the electronic payment scheme first, then classify the electronic payment schemes and probe into main characteristics and typical examples of all kinds of secure electronic payment systems. Furthermore, point out its development direction based on the analysis of status and problems remaining unsolved.

Key words: electronic payment; electronic cash; blind signature; electronic wallet

0 引 言

当前,人们作为顾客购买所需要的商品和服务的方式正在发生变化,随着网络的快速发展,出现了一种新的商业交易的方式:电子商务。

我们知道,信用卡与真实现金等支付手段在日常交易中具有重要地位,同样,电子支付也是电子商务的一个重要组成部分,同时也是电子商务发展的一个瓶颈,如何安全可靠方便地实现电子支付,成为电子商务发展中亟待解决的问题。近年来,人们根据不同的电子支付方式,运用密码学等先进技术,提出了诸多支付协议。但是,到目前为止,对于电子支付制度,还没有给出一个明确的分类。文中主要是在电子支付的安全需求的基础上对电子支付制度做了分类,并介绍各类电子支付系统的主要特点和相关实例。

收稿日期:2006-11-02
基金项目:辽宁省科学技术基金资助项目(002010)
作者简介:徐 明(1981-),女,河北衡水人,硕士研究生,研究方向为信息安全;张祥德,博士,教授,研究方向为组合数学与信息安全。

1 基本概念和一般模型

电子支付是指允许用户通过电脑、电话、传真机等途径完成支付的一种支付手段,一般的电子支付制度都具有这样一个模型——在电子支付制度中,存在三方:银行、用户和商家。用户与银行执行提款协议,提取所需的电子现金;用户与商家执行支付协议,将电子现金转移给商家;最后,商家与银行(可以不是提款协议中的那一家银行,但两家银行必须有业务联系)执行存款协议,将在支付协议中将所得的电子现金存入银行。

根据在支付协议中是否需要银行或一个公正的第三方的参与,所有的电子支付系统可以分为两大类:在线的电子支付系统与离线的电子支付系统。如果用户与商家在进行支付协议时,必须有银行或一个公正的第三方的参与,这个电子支付系统就称为在线的电子支付系统。与之相对应,如果用户与商家在进行支付协议时不需要有银行或公正的第三方参与,商家可以在一段时间以后再将支付协议的副本呈交给银行,完

成存款协议,这样的电子支付系统就称为离线的电子支付系统。与离线的电子支付系统相比,在线的电子支付系统具有较高的安全性与有效性,但同时也需要较大的花费,而且,支付过程必须有银行的参与,因此,它具有一定的局限性。文中重点介绍离线的电子支付系统上,最后简要介绍一下在线的电子支付系统。

2 离线的电子支付制度

2.1 电子支付基础——基本电子现金制度

对于一个最基本的电子现金制度,应该满足下面两个需要:

1) 安全性:在电子现金系统中的每一方的权益都应该受到保护,使之免受其它一方或多方的侵害。

2) 隐私性(不可追踪性):银行应该不具有这个能力:确定某个支付的支付者的身份,或进一步说,确定两个支付的支付者是否是同一人。

不可追踪性需要是从用户的利益角度来考虑的,不可追踪性主要是通过盲签名来实现的。所谓的盲签名,是指银行在签名的过程中得不到用户最终持有的银行签名的任何信息。大多数基本的电子现金制度都是基于这个意义上的盲签名而建立的;还有一些基本的电子现金制度,如文献[1,2],采用了比较特殊的盲签名:部分盲签名和前向安全的盲签名,与其它一般的基本电子现金制度相比,这些采用了特殊的盲签名的电子现金制度具有更强的隐私性。安全性需要是从银行的角度来考虑的,主要应该考虑下面两点:

* 货币是不可伪造的;
* 货币不可重复支付。

货币的不可伪造性实质上是指银行签名的不可伪造性。为了实现这一性质,所有基本电子现金制度都利用了一些公认的密码学假设,即计算某些问题的困难性假设。根据这一点,所有的基本电子现金制度可分为两类:一类是基于计算 RSA 问题的困难性;另一类是基于计算离散对数问题的困难性。

在电子现金制度中,电子货币其实是由一系列的符号构成,因此,极容易被拷贝。又由于货币的不可追踪性,所以电子货币必须满足不可重复支付这一性质。货币的不可重复支付性是指同一货币不能被支付多次,否则,多次支付同一货币者的身份就会被揭露。为了防止在盲签名过程中用户的欺骗行为和抑制重复支付行为的发生,我们建立的电子现金制度必须采用一定的措施。根据所采取措施的不同,所有的基本电子现金制度又可分为两类:

(1)早期建立的基本电子现金制度,采用 cut - and - choose 技术来实现货币的不可重复支付性,因此是多单元的。

(2)后期实现的基本电子现金制度,不采用 cut - and - choose 技术,因此是单个单元的(single - term)。

2.2 带有"监视器"的电子支付制度——电子钱包

电子钱包的概念是由 D. Chaum 和 T. Pedersen 最早在文献[3]中提出的,电子钱包包括下面两部分:

(1) 一个由用户控制的电脑,用 C 来表示;

(2) 一个由特定组织或机构(在电子现金系统中,指银行)发给的防篡扰卡,用 T 来表示,一般采用智能卡。

要求 T 仅能与 C 交换数据,并不能与外界联系,为了达到这个目的,将 T 嵌入 C 内,这样 T 与组织交换的信息都必须经过 C。银行可以在 T 内存储一些秘密数据,如用户在提款协议中提取的货币。由于 T 也具有一定的计算、加解密的功能,因此,形象地说,这个防篡扰卡其实就是银行安插在用户端的一个监视器(Observer),它可以有效地提前制止用户重复支付同一货币或超额支付钱包中的货币。将电子钱包应用到电子现金系统中,可以保证对多重支付的提前抑制,而不是像前面介绍的基本电子现金系统那样,仅能在多重支付发生以后侦测并对多重支付者进行惩处来达到抑制多重支付的目的,而且即便是电子钱包的抗篡改装置遭到破坏,应用电子钱包的电子现金系统仍然可以对多重支付者的身份进行跟踪,从而达到与基本的电子现金系统相同的安全性。

2.3 公正的电子支付制度

在基本电子现金制度中,用户提取的电子货币是由用户产生的一系列符号构成,这个电子货币由银行进行盲签名,每一个签名代表一个特定的价值。这些货币可以在商店进行支付,商店使用银行的公开签名密钥验证这些货币的有效性。在这些系统中,将一个电子货币的提取与支付联系起来是不可行的,这将有利于一些非法的甚至是犯罪的活动,像洗黑钱、敲诈勒索等等。因此,有必要给基本的电子支付制度加入一些功能,如货币跟踪、用户跟踪,实现电子支付制度的公正性。为了解决这个问题,密码学家们提出了公正的电子现金制度这个概念,在公正的电子现金制度中,银行或其他人仍然不能将一个提款协议与相对应的支付协议联系起来。但是,如果银行侦测到货币的滥用,被信任的第三方能够帮助银行对某个账户进行查帐或找到某个特定交易中的购买者的身份,从而有助于阻止某些犯罪活动的进行。

2.4 可分割的电子支付制度

基本的电子支付制度有这样一个缺点:不能够完成精确的支付。为了解决这个问题,人们提出了可分

割的电子现金这一概念。称一个价值为$x的电子货币是可分割的,如果这个货币可以被消费多次,只要这个货币在参加的所有交易中的消费额不超过$x。货币的可分割性对于电子支付制度是非常有意义的,如果一个货币不可分割,那么顾客必须在需要消费的时候去银行提取合适面值的货币,这就在很大程度上造成了不方便,并且是很危险的(银行可以通过消费发生在提款之后这一特征将提款和支付联系起来,从而破坏了用户的匿名性)。或者,顾客事先提取各种面值的电子货币存放在自己的电子钱包里,这会给用户造成存储上的不方便。因此,在实际生活中,可分割性对电子现金系统来说是一个非常重要的性质。

可分割性概念是由T.Okamoto和K.Ohta于1992年在文献[4]中最早提出的。在文献[4]中,T.Okamoto和K.Ohta提出了用二叉树的方法实现货币的可分割性,后来出现的关于可分割性的文章大多沿用了这一方法。但也有一些文章从其它角度出发,实现货币的可分割性[5~7]。其中,文献[5]的核心思想是n次支付过程中用户使用的是同一形式的货币,因而具有可链接性。文献[6]介绍的是电子支票,它只能被用户使用一次,然后将余额存入银行。文献[7]的核心思想则是把一个大面值的货币分割成若干"相等"的子部分,因此又称为电子债券(electronic coupon)。文献[5~7]都不是严格意义上的可分割货币,但它们都具有与可分割货币类似的性质,因此,把它们也看作是可分割的货币。

2.5 可让渡的电子现金制度

可让渡性是指被接收到的货币还可以支付给其他人,并且在这个过程中不需要银行或公正的第三方的参与。也就是说,这个过程是离线的。

具有可让渡性的电子现金系统称为是可让渡的电子现金系统。在可让渡的电子现金系统中,被多次让渡的电子现金的所有忠实用户的身份必须保持匿名性。

在现实世界中,真实的货币都具有可让渡性。而设计一个电子现金系统的标准就是使电子货币的性质尽可能接近于真实的货币。因此,可让渡性就成了电子现金的一个非常重要的性质。

在实现可让渡性的文章中,采用的方法大致可分为三类:一类是使用名义货币这个概念来实现可让渡性;第二类利用了匿名的公开密钥来实现可让渡性;第三类则是利用群签名来实现可让渡性。

在第一类可让渡的电子现金系统中,使用了名义货币,即没有价值的货币。如果用户想要支付自己已经接收到的货币,必须事先提取一个没有价值的货币,即名义货币。然后,将接收到的货币与名义货币一起使用。这无疑增大了数据的流通量与储存量。

在第二类可让渡的电子现金系统中,使用了匿名的公开密钥,在让渡货币时,用户使用该公开密钥进行签名,因此,同一公开密钥对应的交易是可链接的。为了避免链接,可以采用用户在不同的交易中使用不同的公开密钥这一方案,但这会增加与匿名性服务中心的数据交流量。此外,当侦测到多重支付时,银行需要与匿名性服务中心联系来恢复多重支付者的身份。

第三类可让渡的电子现金系统使用了群签名。所谓的群签名,是指这样一个制度:它允许一个群的成员以群的名义来对某个消息进行签名。签名者的身份在一般情况下不可知,但验证者可用群的公开密钥对签名进行验证。在特殊情况下(如出现争议),群的管理者可以识别出某个群签名的签名者的身份。在第三类可让渡的电子现金系统中,如文献[8],使用群签名和盲签名将用户信息嵌入到电子现金中,由于群签名和盲签名都是匿名的和不可链接的,从而使得电子现金制度也具有匿名性和不可链接性,并且相对于第一类可让渡的电子现金制度,没有使用名义货币,避免了庞大的数据交流量和存储量,因此,效率更高。

3 在线的电子支付制度

在此之前介绍的电子现金系统都有一个共同特征:离线(off-line)。所谓的离线的电子现金系统是在支付阶段不需要第三方(常指银行)的参与。与此相对的便是在线的电子现金系统:在支付阶段需要一个第三方的参与,来确保交易中的电子货币的有效性。

电子现金的概念最早是由David Chaum提出的。其实,早期的一些关于电子现金的文章中建立的电子现金系统都是在线的。

后来,人们发现在线的电子现金系统具有这样一个缺点:由于在支付过程中需要一个在线的第三方来验证货币的有效性,这就给第三方(或者是银行或者是货币发行中心)造成极大的负担,形成了一个瓶颈。于是,人们把注意力转移到离线的电子现金系统的研究上,出现了大量的关于离线的电子现金系统的文章。

最近,随着网络技术的快速发展,网络分布的区域变广,网络中数据传送的速度变快,这给在线的电子现金系统提供了一个很大的发展空间,相继又出现了一些关于在线的电子现金系统研究的文章。其实,相对于离线的电子支付制度而言,在线的电子支付制度具有更高的效率与安全性,如果能够解决前面提到的那些制约因素,在线的电子支付制度将会有更广阔的发展前景。

4 安全电子支付制度的研究方向

文中仅仅介绍了电子支付制度的理论部分,并没有论述这些电子支付制度在实际中是如何实现的。其实,在实际应用中,这些电子支付制度的实现还是存在很多问题的。目前已开发出多种电子支付制度,然而多数都是在封闭的专用网络上运行的。虽然它们在某一国家或者某一地区具有一定的市场,但从总的来看,仍然存在着如下亟待解决的实际问题:

(1) 没有一种电子支付的完整解决方案、支付模型与体系结构。尽管一些系统正逐渐成为标准,但仅有很少几个标准的 API。从开放市场的角度来看,协议间的通用 API 和网关是绝对需要的。

(2) 大多数电子支付系统都是封闭式的,即使用专有技术,仅支持一些特定集合的协议和机制。这些支付系统通常需要一个中央服务器作为所有参与者的可信第三方,有的甚至要求使用特定的服务器或浏览器。

(3) 尽管大多数方案都使用了公钥密码,但多方安全受到的关注远远不够,消费者的匿名性和隐私也还未得到充分的考虑,大多数系统都限制为两方,因此难于集成一个安全的联结到第三方,并且没有建立一种解决争议的决策程序。

5 结 论

随着网络的发展,电子商务越来越受到人们的关注。作为电子商务的核心技术,电子支付也越来越得到人们的重视。电子支付是指允许用户通过电脑、电话、传真机等途径完成支付的一种支付手段。如何安全可靠方便地实现电子支付,是电子商务发展中迫切需要解决的问题,近几十年来,许多学者都致力于这方面的研究。文中主要是从密码学的角度出发,介绍电子现金制度的发展现状并对现有的电子支付制度作了一下分类。

目前,存在着许多电子支付制度,它们具有着这样或那样的性质。但迄今为止,还没有出现一个完善的制度,满足既具备所有必需的性质又具有较高的使用效率。因此,要想实现电子支付在现实生活中的推广和普及,仍然需要广大学者的继续努力。

电子支付作为电子商务的重要组成部分,在今后必将得到更大的发展。

参考文献:

[1] Miyazaki S, Sakurai K. A more efficient untraceable e-cash system with partially blind signatures based on the discrete logarithm problem[C]// In: FC'98. Berlin: Springer-Verlag, 1998:296-307.

[2] Duc D N, Chen J H, Kim K. A forward secure blind signature scheme based on the strong RSA assumption[C]// In: ICICS 2003. Berlin: Springer-Verlag, 2003:11-21.

[3] Chaum D, Pedersen T. Wallet Databases with Observers[C]// In: Advances in Cryptology - CRYPTO'92. Berlin: Springer-Verlag, 1993:89-105.

[4] Okamoto T. An Efficient Divisible Electronic Cash Scheme [C]// In: Advances in Cryptology - CRYPTO'95. Berlin: Springer-Verlag, 1992:438-451.

[5] Eng' T, Okamoto T. Single-Term Divisible Electronic Coins[C]// In: Advances in Cryptology - CRYPTO'91. Berlin: Springer-Verlag, 1993:356-378.

[6] Nakanishi T, Haruna N, Sugiyama Y. Unlinkable Electronic coupon protocol with Anonymity control[C]// In: ISW'99. Berlin: Springer-Verlag, 1999:37-46.

[7] Solages A D, Traore J. An Efficient Fair Offline Electronic Cash System with Extensions to Checks and Wallets with Observes[C]// In: FC'98. Berlin: Springer-Verlag, 1998:275-295.

[8] Maitland G, Boyd C. Fair Electronic Cash Based on a Group Signature Scheme[C]// In: ICICS 2001. Berlin: Springer-Verlag, 2001:461-465.

(上接第 212 页)

需要渗入产品的 GUI,形成其独特的产品魅力。手机界面的设计规范很多,但基本的都是符合软件行业的设计标准,也符合人类的审美观念,只有设计好的 GUI,才能让用户和谐地使用手机游戏。

参考文献:

[1] 饶 威. 浅谈中国手机游戏的发展[J]. 科教文汇,2006(2):159-160.

[2] 王 森. JAVA 手机和 PDA 程序设计入门[M]. 第 3 版. 北京:电子工业出版社,2005.

[3] 惠 志. 一个基于 3D 游戏引擎的虚拟展示方案[J]. 微机发展,2005,15(4):95-97.

[4] 涂 超. 基于 Morfit 3D 引擎的三维游戏开发研究[J]. 微机发展,2005,15(10):70-73.

[5] Boll S, Wasch J. A Java application programming interface to a multimedia enhanced object-oriented DBMS[C]//In First International Workshop on Persistence and Java(PJ1). Glasgow, Scotland: [s.n.], 1996.

[6] Mynatt E D, Edwards W K. Mapping GUIs to auditory interfaces[C]//Proceedings of the Fifth Annual Symposium on User Interface Software and Technology (UIST '92). New York: ACM, 1992:61-70.