分类号 TN918.1 密级 公开

重庆邮电大学硕士学位论文

论文题目 移动电子商务的数字签名和微支付协议研究

英文题目 Research of Digital Signature and Micropayment Protocol of Electronic Commerce in Mobile Communication

硕士研究生 卢霖

指导教师 李方伟 教授

学科专业 通信与信息系统

论文提交日期 2013.6.6 论文答辩日期 2013.6.5

论文评阅人 校内盲审

曾孝平 教授 重庆大学

答辩委员会主席 林金朝 教授 重庆邮电大学

2013 年 6 月 6 日

独 创 性 声 明

本人声明所呈交的学位论文是本人在导师指导下进行的研究工作及取得的研究成果。据我所知，除了文中特别加以标注和致谢的地方外，论文中不包含其他人已经发表或撰写过的研究成果，也不包含为获得 重庆邮电大学 或其他教育机构的学位或证书而使用过的材料。与我一同工作的同志对本研究所做的任何贡献均已在论文中作了明确的说明并表示谢意。

学位论文作者签名：[signature]　　签字日期：2013.6.8

学位论文版权使用授权书

本学位论文作者完全了解 重庆邮电大学 有关保留、使用学位论文的规定，有权保留并向国家有关部门或机构送交论文的复印件和磁盘，允许论文被查阅和借阅。本人授权 重庆邮电大学 可以将学位论文的全部或部分内容编入有关数据库进行检索，可以采用影印、缩印或扫描等复制手段保存、汇编学位论文。

（保密的学位论文在解密后适用本授权书）

学位论文作者签名：[signature]　　导师签名：[signature]

签字日期：2013.6.8　　签字日期：2013.6.8

摘要

随着网络、计算机以及信息技术的飞速发展，信息产品得到了越来越多人的关注。针对此类信息产品，我们将使用微支付(Micropayment)系统来对付费交易过程进行管理。微支付协议应满足这样的系统要求：在保证一定安全性的前提下，伴随着较低的管理要求和存储要求，并尽可能少的传输信息。

在常用的微支付系统中，Payword 协议是现如今比较流行的一种微支付协议。但同时，Payword 协议存在一些问题，比如安全性、公平性、消费额度和支付链交叉等。针对其中安全性问题，我们可以将数字签名技术引入到 Payword 协议中，加强用户在消息传递时的安全性。对于公平性来说，Hash 支付链的运用可以较好的保证参与双方平等公平地进行交易。对这样一些问题的改进，在移动电子商务中是非常有必要的。

所以本文重点研究了移动电子商务的安全性与支付协议的公平性等问题，主要工作内容包括：

1.针对原始 Payword 协议中存在的问题，本论文改进了一种基于 Payword 的匿名性微支付协议。协议特点如下：对于匿名性问题，经纪人提供匿名标识的方法，很好的对消费者的身份信息提供保护。并利用双线性对映射的原理，设计了一种参与者双方相互协商认证的密钥协商协议，得到了两者可以同时运用的共享密钥，防止了交易的不公平性。在协议的支付阶段，设计了一种双哈希支付对的方法，有效的防止了支付对的伪造，提高了系统安全性。同时，将双哈希支付对分配成 N 段，每一段支付对对映一个商家，不需要重复制造支付对，这又给消费者同时与多个商家交易提供了方便，节省了系统开销。

2. 由于移动电子商务通信时大多使用的是不安全信道，这将对系统产生很多负面影响，比如信息泄露和黑客攻击等。本论文将数字签名技术引入到电子商务微支付系统当中，不仅给系统提供了较好的安全性支持，还满足了用户的匿名性。并且在重复消费问题上，银行将用户的唯一身份标识存入数据库，一旦出现重复花费问题，银行便能够立刻识别该用户，避免了这一问题对用户的影响。同时本文将数字签名和 Hash 函数合理的配合，运用各自的特点，既满足了系统安全性又不影响系统的效率。

关键词：电子商务，微支付，Payword，hash 函数，数字签名

Abstract

As the rapid development of network, computer and information technology, information products have been getting more and more attentions. Aimed at this kind of information product, we will use micropayments system to manage the payment transaction. Micropayment protocols should meet the system requirements as follow: on the premise of guarantee of safety, with the lower managements requirements and storage requirements, make the transfer of information as little as possible.

In the normal micropayments system, Payword protocol is a kind of very popular micro payment protocols. But in the meanwhile, some problems exist in Payword protocol, such as security, fairness, consumer credit and payment chain cross, etc. For security issues, the digital signature technology can be introduced to Payword protocol, to strengthen the users' security in messaging. For the fairness issues, Hash chain can make the trade fairly both the equal participation sides. Working out these problems in the mobile e-business is very necessary.

So this thesis focuses on the security problems of mobile electronic commerce, such as fairness and Payword protocol, main work contents include:

1. For the problems existing in the original Payword protocol, this paper improves an anonymity micropayment protocols based on Payword. The features of the protocol proposed are as follows: for the anonymity problem, broker provides anonymous identification method, which is useful identity information to provide protection for consumers. And via using the principle of bilinear mapping, designs a protocol, in which both participants sides mutually authenticated and can use the Shared secret key at the same time, prevent the unfairness in trade. In the payment stage of protocol, designs a method of dual hash pay, effectively prevent the forge for paying, improve the security of system. In the meanwhile, the pair of hash- pay is decomposed into N pieces, each payment corresponds to a business, does not need to repeat manufacturing pay pair, which provides a convenient for consumers who is trading with several merchants at the same time, and saves system overhead.

Practically the channel used in mobile e-business communication is not secure, there will be many negative effects on the system, such as information leakage and hacker attacks, etc. In this paper, the digital signature technology is introduced into the micropayment system of electronic commerce, which not only provides the system better security support and also meets the users' anonymity. And on repeat purchases

issues, the bank save the only identity of users in the database, once spend is repeated, the bank can immediately identify the user, to avoid the influence of the problem to the user. At the same time, this article fits digital signatures with Hash function very well, using their own characteristics, both satisfied the system security and does not affect the efficiency of the system.

Keyword: E-commerce, Micropayments, Payword, Hash function, Digital signature

目录

第一章 绪论

1.1 课题研究背景及意义

1.1.1 移动电子商务研究背景

电子商务[1](Electronic Commerce)，EC 是 20 世纪 90 年代在美国等发达国家发展起来的一种企业模式。在计算机硬件、软件和网络的基础上，电子商务通过特定的协议组建起来一个电子网络环境，在该环境下进行各种商务活动。电子商务改变了传统交易方式，不需要买卖双方当面交易，打破了地理区域和时间的限制。同时随着现代信息技术的快速发展，电子商务的意义和作用也在不断的发展改变。

随着移动通信技术的发展以及移动终端的普及，一种崭新的电子商务模式也应运而生，那就是移动电子商务。移动电子商务指的是用户通过手机、掌上电脑、笔记本电脑等移动终端在无线上网技术的基础上形成的一种电子商务体系，它可以为用户提供多种多样的移动数据服务。而且由于移动终端本身的方便性与灵活性，使得用户可以在任何时间和地点进行移动电子交易。同时这些业务的开展也给移动运营商和设备商等通信企业提供了巨大的发展前景。

移动电子商务所具备的的最大特点就是“任何时间”、“任何地点”和“个性化”。用户可以随时随地得到想要的各种数据和服务，并且根据自己的意愿，个性化地定制服务内容。移动支付是用户对所购买信息和服务进行付款的方法，是移动电子商务的一个关键过程，用户通过自己的移动终端随时随地对电子商品进行支付。

但同时，在无线通信过程中，所有信息的传递都是在无线网络上完成的。而无线信道相比于有线信道，它是一类开放性的、安全性能低的信息通道，可能随时被他人窃听得到信道中的数据信息。如果传递的信息包括用户的身份或交易的秘密文件等重要数据信息，那么提高无线信道中信息传递的安全性就显得极其重要。

1.1.2 移动电子商务安全性问题研究现状

在移动电子商务中，认证与密钥协商协议和支付协议尤其关键，是移动电子商务系统中安全机制的核心部分。认证与密钥协议的主要任务是：确认交易双方的身份，并产生一个安全的会话密钥，可以使双方安全地进行通信，为交易提供一个安全可靠的通信环境；而支付协议的主要任务是，确保双方能够在交易完成

后进行公平的结算，并防止任何参与交易的一方出现恶意欺诈行为。如何针对无线信道的开放性以及移动通信宽带与设备受限等特点设计高效、安全、公平的认证与支付协议，是移动电子商务应用中的主要安全问题之一。

通常移动电子商务按照交易额的数量可分为：一、微支付[2-7](Micropayment)，交易数额较小，一般在$10 以下，主要是面向商家与消费者之间；二、宏支付，交易数额较大，一般在$10 以上，主要是面向个人与个人之间、商家与消费者之间和商家与商家之间，它对系统安全性要求更高，需要通过对金融机构进行交易鉴权。就目前来看，移动电子商务的交易内容主要是以小额交易为主，即微支付。微支付协议根据交易时网络的连接方式分为在线交易和离线交易，其中 Payword[8]、Millicent[9]和 MicroMint[10]等属于离线方式。对于微支付协议不同性能的研究开发，也产生了许多新的方向，如微支付协议的安全性研究、微支付协议的公平性研究和微支付协议的效率研究。目前以上而写的微支付协议的性能是发展的热点。本文中关于移动电子商务支付协议的研究都是基于 PayWord 的微支付协议。

目前，基于 PayWord 的微支付协议的研究主要集中在安全性、公平性和高效性三个方面，而安全性与公平性则是比较热门的两个方向，高效性的研究相对较少。安全性主要体现在认证与密钥协商协议中的认证和信息传输过程中的保密性及完整性；公平性则主要体现在支付协议中，有效防止恶意欺诈行为；高效性则贯穿于交易的整个流程中。无论是在安全性方面、公平性方面，亦或是高效性方面，相关研究都取得了一定的成果，但还存在着一些问题：认证与密钥协商协议过程中的消息上下文缺乏相关性和身份识别信息，容易被攻击者替换以及中间人攻击；商家与用户的交易过程中，总会有一方先提供商品或者电子货币，无法保证交易双方完全的公平性；交易商品还是以网络服务为主，实用性有待提高；目前讨论的移动电子商务微支付协议一般都牵涉到除用户、商家和移动网络运营商之外的银行，交易流程还是有第四方，影响了整个电子商务交易的效率。

1.1.3 移动支付的产业链

移动支付的产业链和传统行业的产业链是很不相同的，前者的结构更加的复杂。目前，移动支付产业链构造是由金融机构、移动服务提供商、商家、用户、移动设备提供商和运营商等多个环节构成的，其中掌握大量的用户资源和议价能力也基本相当的是金融机构和运营商。

且由于根据向移动用户提供移动支付的主体不同，其产业链的模式也不同，现可以分成三类，如表 1.1 所示：

表 1.1 中国移动支付产业链模式[11]

产业模式	提供移动支付服务
金融机构	即银联主导模：中国银联向移动用户提供移动支付服务，电信运营商只作为管道而存在，或者中国银联可以绕过电信运营商，直接向最终的客户提供移动支付业务
电信运营商	即运营商主导模式：电信运营商既是移动支付业务数据传输网络的提供者又是移动支付账户的管理者作为支付服务提供者存在
可信第三方	即第三方支付主导模式：独立于银行和移动电信运营商的可信任第三方支付向移动用户提供移动支付服务作为管道存在

目前，移动支付产业链的主导权争夺在我国国内非常激烈。在已有的支付技术中，中国电信和中国联通选择了 SIMPass 技术，而中国移动选择了 RFID-SIM 技术，中国银联却选择了智能 SD 卡，他们各方都在试图掌控了产业链的主导权。

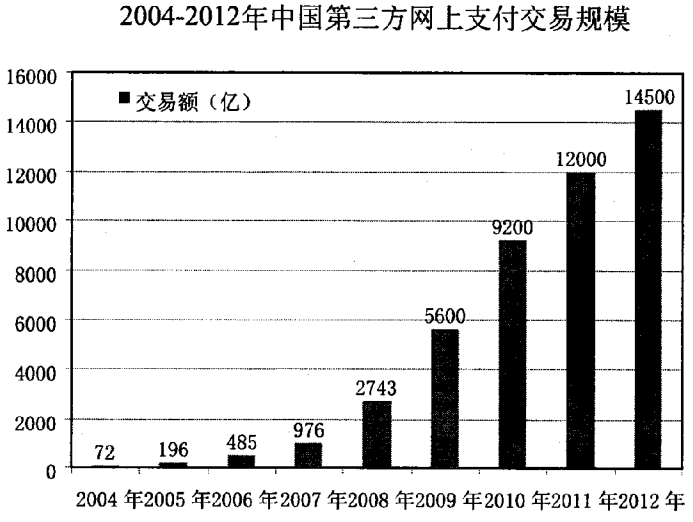

图 1.1 2004-2012 年中国第三方网上支付交易额

上图中数据显示出作为第三方交易模式的实体获取的利润很高，这会是一块人人想吃一口的“大蛋糕”，因此移动增值业务微支付中微支付协议的研究是一个发展前景很广的方向。

1.2 本文工作

移动电子商务微支付机制中的 Payword 协议的核心问题是匿名性与安全性等问题，因此本文的研究重点也在于此。结合移动网络环境和已有的微支付协议的

优缺点，如基于Hash链的Payword协议，基于数字签名Payword协议等等。如何采用有效的措施来实现微支付的公平性、安全性和匿名性将显得尤为重要也是本论文研究的重点。

作者于2011年2月进入移动安全项目组，参与的项目是国家自然科学基金《移动增值业务微支付系统中认证支付协议与签名技术的研究》(61071116)。经过两年多的学习，对移动电子商务中微支付协议进行了较深入的研究。本文所做的主要工作包括：

(1)对现有的移动电子商务安全体系(Payword协议)以及基于Payword的改进微支付协议进行了详细的分析、对比，指出各协议的优缺点，并按照改进方向进行归类总结，指明未来发展方向及前景。

(2)对电子商务微支付中的几种基本模型进行了详细介绍，分析了当前Payword协议的优点和存在的不足之处。对基于Hash链的Payword协议进行了改进研究，提出了一种基于双Hash链的微支付协议，通过验证分析，该协议保证了系统较高的的安全性、公平性和匿名性。同时最后对该协议进行了补充，使得系统能够拥有同时与多个商家交易的性能。

(3)对数字签名技术进行了较深入研究，分析了将数字签名技术应用于微支付协议中的必要性。设计出一种基于门限的具有追踪功能的民主群签名算法，并成功的将该算法引入了微支付协议中，提出了一种基于数字签名机制的微支付协议方案。通过理论分析，该方案在安全性和公平性上得到了较大的提高。

1.3 论文结构

本论文的撰写以及创新之处共分为5章节，各章内容安排如下：

第一章节介绍了电子商务的研究背景和现状。

第二章节简单介绍了一些电子商务的安全基础，和微支付基本框架。

第三章节提出了一种基于Hash链的微支付协议方案，并且改进后可以同时与多个商家交易。

第四章节将数字签名技术引入到微支付协议中，提出了一种基于门限的民主群签名方案，并详细研究和分析了数字签名在微支付中的运用。

第五章节对论文进行了总结，并提出了文章中的一些不足之处，和下一步将要进行的工作。

第二章 移动电子商务安全基础

由于微支付系统的安全性主要依赖于密码学理论，所以安全算法[12-17]是微支付协议的核心和基本。微支付协议理论基础是围绕现代密码技术而来的，所以在本章将重点介绍和研究微支付系统所涉及的数论基础、公开密钥算法和散列函数等相关问题。

2.1 电子商务的定义和分类

2.1.1 电子商务的定义

电子商务(Electronic Commerce)，EC 主要包括电子方式和商贸活动两个大方向。但现如今对电子商务并没有准确定义，不同的社会群体对电子商务都有不同程度的定义描述。如各国政府、学者、企业界人士都根据自己所处的地位和对电子商务的参与程度，给出了许多表述不同的定义。

1997 年 11 月，国际商会在法国巴黎举行了世界电子商务会议，会议中确定了电子商务的权威概念："电子商务是指对整个贸易活动实现电子化。从涵盖范围方面可以定义为：交易各方以电子交易方式而不是通过当面交换或直接面谈方式进行的任何形式的商业交易；从技术方面可以定义为：电子商务集合了多种技术，如数据交换、数据获取和数据自动捕获等。"

上海市电子商务安全证书管理中心给电子商务下的定义："电子商务是指采用数字化电子方式进行商务数据交换和开展商务业务活动。电子商务主要包括利用电子数据交换、电子邮件、电子资金转帐及 Internet 的主要技术在个人间、企业间和国家间进行无纸化的业务信息的交换。"

通过上述定义我们可以总结出，电子商务的定义可以通过以下几个方面来理解：第一，电子商务是对传统贸易活动的自动化和电子化；第二，在计算机软硬件与网络基础设施等基础上，用户间进行信息商品的传递、交换和获取，即电子商务活动；第三，对于传统商务活动中的每一个阶段，都是通过电子商务来完成，包括销售、支付、运输、信息交互、售后服务等等；第四，参与电子商务的群体包括消费者、供货商、企业员工、银行及政府等各种机构或个人，从而实现企业贸易活动的的高效率和低成本。

2.1.2 电子商务的分类

电子商务按照交易对象、支付发生情况、活动内容和使用网络类型等可以进行如下分类：

1 按照交易对象分类

(1)企业对消费者：B2C(Business to Customer)，是我国最早期的一种交易模式，现如今很多商务网站都是使用这一模式，如京东商城等。

(2)企业对企业：B2B(Business to Business)，企业之间通过网络进行商品和服务的交换，在以网络技术为基础的商务平台上进行消息供求、订货发货和支付等过程。

(3)企业对政府：B2G(Business to Government)，这种商务活动是企业与政府之间的商务模式，如海关保税平台、国税报税平台等。

2 按支付发生情况分类

(1)电子事务处理：如网上报税、网上办公等。

(2)电子贸易处理：如网上购物、网络缴费等。

3 按活动内容分类

(1)间接电子商务：这是对于有形实物来说的，如一本书、一件衣服等，并且需要通过物流公司来对物品的配送，最终必须送达消费者接收。

(2)直接电子商务：这是对于无形货物来说的，如应用软件、电子货币等，无需考虑配送的问题。

4 按使用网络类型分类

(1)EDI(电子数据交换)：主要运用在企业或者商家之间，相比较传统的交易方式，EDI 在效率和性能上为用户节省了大量时间和费用。

(2)互联网商务：主要以信息技术为基础，通过网络实现营销和购物等交易过程。具有少投入、成本低和库存小等特点。给消费者带来了很大的便利。

(3)Intranet 和 Extranet 商务：Extranet 是以 Internet 为基础建立起来的企业内部网，可以将公司各个分公司或部门联系在一起，提高了经营效益，减小了交易成本。

2.2 电子商务的安全需求

2.2.1 电子商务面临的安全威胁

在传统交易过程中，对于交易双方间的安全和信任关系，由于两者是面对面

的，因此很容易保证交易过程的安全性和建立信任关系。但在电子商务交易过程中，交易双方是通过网络来联系。订单信息、帐户信息等各种敏感信息都是通过公共的网络传输，使得电子商务的参与各方都面临着不同的安全威胁[19]。

1 商家（商品或服务的提供者）面临的安全威胁

(1)中央系统的安全性受到破坏：入侵者假冒成合法用户来改变客户数据（如改变商品的送达地址）、解除用户订单或生成虚假订单。

(2)竞争者检索商品的销售情况：恶意竞争者以他人名义来定购商品，从而了解有关商品的递送状况和货物的库存情况等商业信息。

(3)客户的资料被竞争者获取，为其所用。

(4)被他人假冒而损害公司的信誉，这种安全威胁主要有三种方式：建立与销售者服务器名字相同的另一个 www 服务器来假冒销售者；制造虚假订单；假冒成电子商务的参与方，以获得其他人的机密信息。

(5)消费者提交订单后不付款。

(6)虚假订单。

2 客户（商品或服务的购买者）所面临的安全威胁

(1)虚假订单。冒名者以其他客户的名义来定购商品，而且有可能收到商品，而被冒名的客户却被要求付款或返还商品。

(2)信用的威胁。购买者在付款后，收不到商品。

(3)机密性丧失。客户可能将秘密的个人数据或自己的身份数据（如 PIN，令等）发送给冒名为销售商的机构。同时，这些信息在传递的过程中也有可能受到窃听的威胁。

(4)拒绝服务。攻击者可能向销售商的服务器发送大量的虚假订单来挤占它的资源，从而使合法的用户得不到正常的服务。

2.2.2 电子商务的安全需求

在开放的 Internet 环境下进行电子商务，对电子商务提出了如下需求：

1 信息的保密性

电子商务中是在开放的网络环境上进行商务交易，而交易信息中都包含着客户、企业甚至国家机密，为避免恶意客户对信息的非法篡改、存取、窃取等非法操作和防止恶意客户窃取到原始信息数据后对其进行解读，因此对重要的信息必须进行加密处理。

2 数据的可靠性

数据的可靠性即为对方能及时地收到信息。只有保证电子商务的时效性和有

效性才能使完全暴露于网络环境上电子商务完全替代传统纸张上的贸易，所以要控制和预防网络故障、计算机软硬件错误，以保证电子商务的时效性和有效性。

3 数据的完整性

导致电子商务中交易各方信息产生差异原因可能是交易信息数据录入时发生意外差错、在传输时数据丢失以及信息传送的次序差异。因此，针对以上原因，需要防止对数据被非授权建立、修改和破坏，同时要保证在传送过程中数据的完整性和统一信息数据传送的次序。除此之外，电子商务系统应该具有一种检验数据完整性的方法。

4 可认证性

电子商务中应该具有一种对交易各方进行身份鉴别的方法，以确保此次贸易的安全的进行。在传统贸易中，贸易各方通过手写签字或者印章来鉴别对方身份，并通过此来建立贸易关系。但在电子商务中，数字签名与数字证书是交易中个人、企业或国家的唯一可靠的标识。因此可以通过结合数字签名与数字证书的认证方式对用户身份进行鉴别。

5 数据的不可否认性

在电子商务中，交易完成以后，按照交易的基本原则，参与交易的任何一方都不能再否认其交易行为，电子商务系统中交易方不能反悔或抵赖已经进行或完成的交易。

2.3 数论困难问题

现代的密码学算法的安全性基本都是依赖于数论中的难解问题[20-22]。如果不能再有限的计算时间和存储空间前提下计算出某一问题，则我们将其判定为难解问题[23]。虽然人们还不能完全肯定不存在某一种算法能够解出这种难题，但同样人们还无法找出这样一种算法，所以我们可以假设不存在某种有效算法可以解出这些困难问题。下面本文对几种数论的困难问题做相关定义和分析。

2.3.1 离散对数问题

定义 2.1 一个有限循环加法群 G，生成元为 g。存在元素 $a \in G$，整数 $x(0 \le X \le |G|)$ 是它的离散对数，且满足等式 $\mathrm{a} = g^x$，记为 $\log_g \mathrm{a}$。离散对数可以称为 a 的指数。

相对于普通对数的某些结论，在离散对数中也是成立的。比如，存在 $G = \langle g \rangle$ 是某一个阶为 n 的循环群，a、b、$c \in G$，有：

$$\log_g ab = \log_g a + \log_g b (\mathrm{mod}\ n) \tag{2.1}$$

同样的，对于$x>0$，有：

$$\log_g a^x = x \log_g a (\mathrm{mod}\ n) \tag{2.2}$$

定义 2.2 离散对数问题[24]:确定有限循环群G，生成元为 g，元素$a \in G$,要求计算得到正整数x，且满足$0 \le x \le Z_{ord(G)}$，同时有恒等式$a \equiv g^x$成立。

四种主要的离散对数算法和平均运算时间：(1)小步算法；(2)大步算法[25]：$O(n^{\frac{1}{2}} \log n)$；(3)Pohlig-Hellman 算法[26]：$O(\sum_{i=1}^{k} c_i(\log n + p_i^{\frac{1}{2}}))$；(4)Pollard 的算法[26]：$O(n^{\frac{1}{2}})$。除此之外，对于群$Z_p^*$还有专门的索引算法[27]。由于上述离散对数算法的运算时间与其群的阶数具有某种指数或亚指数关系，因此求解该类离散对数问题是很困难的[22]。所以得出离散对数问题的假设是在有限的资源空间内不存在任何算法能求解出离散对数问题。

2.3.2 表示问题

定义 2.3 设 G 是一有限循环群，阶为n，有生成元$g_1,\cdots,g_m \in G(g_i \neq g_j)$。m 元组：$x_1,\cdots,x_m$是$a \in G$的一个表示，且对于所有$i$、$x_i$:$1 \le i \le m, 0 \le x_i \le n\text{-}1$，满足：

$$a = \prod_{i=1}^{m} g_i^{x_i} \tag{2.3}$$

且存在$n^{m\text{-}1}$个$a \in G$对于$(g_1,\cdots,g_m)$的 m 元组表示。

定义 2.4 设一有限循环群 G,生成元组$(g_1,\cdots,g_m)$和元素a,找到整数组成的 m 元组$(x_1,\cdots,x_m)$，对所有$1 \le i \le m, 0 \le x_i \le n\text{-}1$，满足

$$a = \prod_{i=1}^{m} g_i^{x_i} \tag{2.4}$$

表示问题[29]是对离散对数问题的推广。如果随机选择一生成元组$(g_1,\cdots,g_m)$，则找到该元组的两个不同的表示在计算上是困难的。

2.3.3 Diffie-Hellman 问题

定义 2.5 Diffie-Hellman 问题：有一个有限循环群 G，g 是它的生成元，存在两个元素g^u，$g^v \in G$，能够得到g^{uv}。

在数论问题中，Diffie-Hellman 问题和离散对数问题是密切相关的。在多项式时间内要解出离散对数问题，必须先计算：

$$u = \log_g g^u \tag{2.5}$$

在此基础上再计算$(g^v)g^u$，则解出 Diffie-Hellman 问题。在一定的循环群中，两个困难问题的计算是相当的。

定义 2.6 Diffie-Hellman 确定问题[29]：给定一有限循环群 G，生成元为 g，任意选择三个元素 g^u、g^v、$g^w \in G$，能够确定元素 $g^w \stackrel{?}{=} g^{uv}$。

Brands 首先提出了 Diffie-Hellman 确定问题，在安全性方面，某些已有的密码协议[30][31]都是间接的建立在此基础上的。对于 Diffie-Hellman 确定问题，如果 Diffie-Hellman 困难问题能够解决，那么确定问题同样只需做出计算也能够得到解决。但同时两者的难解性是肯定的。

2.3.4 大数分解问题

定义 2.7 确定一个正整数 n，和某些不同的素数 p_i、正整数 e_i，能够计算得到式子 $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$，这就是大数分解问题。

随着计算能力和存储空间的不断提高，对于以前不能够完成的困难问题：因子分解又被得到了深入研究和应用，最新研究的多种分解整数 n 的算法[32]。同样凭借着计算机网络的分布式计算，费尔玛数 $F_9 = 2^{512}+1$ 已被分解成功。现如今主要的因子分解算法有：数域筛法[33][34]，二次筛法[35-37]、椭圆曲线法[38][39]、Pollard 的 $\rho, p-1$ 算法[40]、连分式算法[41][42]、试除法等。

2.4 公开密钥算法

对称密钥算法和非对称密钥算法是两类主要的加密算法。在对称密钥算法中，加密和解密的过程使用相同的密钥，因此在使用对称加密算法时通信双方需要提前互相告知其密钥。非对称密钥算法,又叫公开密钥算法，加密和解密的过程使用不同的密钥。加密密钥是公开的，所以也叫做公钥，而解密的密钥是不公开的，又叫做密钥。

Diffie 和 Hellman 于 1976 年在《密码学的新方向》[43]中第一次提出了公开密钥的概念以及陷门单向函数的概念。陷门单向函数的值很难计算，除非知道陷门。例如给定函数 $f: A \to B$，如果其陷门（往往将陷门作为私钥）存在，则该函数可作为公钥，从而对消息 $m \in A$ 的加密就是 $f(m)$，解密即为 $f^{-1}(f(m)) = m$。

除了应用于加密，陷门单向函数还可以实现数字签名。假设有一个消息 $m \in B$，其数字签名为 $s = f^{-1}(m)$，如果签名验证得到 $m = f(s)$，则签名有效。

2.4.1 Diffie-Hellman 密钥交换

Diffie-Hellman 密钥交换算法[43]是第一个公开密钥算法，主要作用于不加密信道上的密钥分配，却不能用于对信息的加密和解密。该算法的安全性是基于有限

域上离散对数问题的难解性。

例如：设 G 是一个有限循环群，q 为阶，生成元 $g \in G$，且在 G 中计算离散对数问题是困难的。现有 A 和 B 的私钥 x_A 和 x_B，公钥为 $y_A = g^{x_A}$ 和 $y_B = g^{x_B}$。A 和 B 在已有鉴别的信道上交换公钥，用自己的私钥为指数计算对方公钥的幂，则得到公共密钥 $k = y_A^{x_B} = y_B^{x_A} = y^{x_A x_B}$。

以上方案安全性是基于 Diffie-Hellman 问题的。假设发送者已知明文的离散对数，则该协议也能用作加密使用，如果 B 要把消息 $m = g^m$ 秘密地发送给 A，则 B 计算并发送 $c = y_A^m$ 给 A，然后 A 可以通过 $m = c^{1/x_A}$ 来解密。

2.4.2 RSA 加密算法

Diffie 和 Hellman 提出陷门单向函数[45][46]的概念后，1977 年由 Rvcest、Shamir 和 Adleman 提出了以他们三人名字首字母命名的 RSA 公钥密码算法[47]。RSA 算法的安全性基于大整数素因子分解的困难性。

其算法如下：设有两个大素数 p 和 q，其中 $p-1$ 和 $q-1$ 最少存在一个大的素因子，$n = pq$，有满足等式 $\gcd(e, \varphi(n)) = 1$ 的整数 e。接受者为 B，公钥 (n, e) 和私钥 (p, q, d)，且 d 满足 $de = 1 (\mathrm{mod}\, \varphi(n))$。

首先发送者 A 计算 $c = m^e (\mathrm{mod}\, n)$ 得到密文，并秘密发送给接受者 B，B 收到之后对秘文进行解密计算得到 $m = c^d (\mathrm{mod}\, n)$。

RSA 加密算法的难解性在于求解以合数 n 为模数的 e 次方根的困难性。但是，它的安全性在此系统中不能够得到绝对地保证。RSA 加密算法的安全性是基于大整数分解的困难性，即只需分解出 $n = p \times q$，就能够得到 $\varphi(n) = (p-1)(q-1)$，从而确定 e 的模 $\varphi(n)$ 乘法逆 d。

2.4.3 ElGamal 加密算法

ElGamal 加密算法[48]能够用于数据加密同时也能用于数字签名，其安全性主要依赖于计算有限域上离散对数这一难题。ElGamal 算法是 Diffie-Hellman 密钥交换的另一种应用。

其算法如下：p 是素数，α 是 Z_q 的本原元素，$\beta \in Z_p^*$，整数 a，$0 \le a \le p-2$，使得 $\alpha^a \equiv \beta \bmod p$，其中 p, α, β 是公开的，a 是秘密的。加密、解密算法为：

(1)加密算法：选择随机数 $k \in Z_{p-1}$，明文 x 的密文 $e_k(x, k) = (y_1, y_2)$，其中 $y_1 = \alpha^k \bmod p$，$y_2 = x\beta^k \bmod p$。

(2)解密算法：$d_k(y_1, y_2) = y_2 (y_1^a)^{-1} \bmod p$。

ElGamal 公钥密码系统是非确定的，它的密文依赖于明文 x 与加密者所选择的

的随机数 k。相同的明文加密得到的密文不一定相同。β^k 是明文 x 的掩码(masked)。显然 $d_k(e_k(x,k)) \equiv x \bmod p$。

攻破 ElGamal 公钥密码系统直接的方法是计算离散对数。当 $p-1$ 所有的因子都是小素数时可以采用 Pohlig-Hellman 算法。为此可以仿照因子分解算法引入因子库，先计算因子库中素数的离散对数，然后计算期望元素 β 的离散对数，这就是目前最有效的指标计算方法。

ElGamal 公钥密码系统可以在任何循环群上实现。选择群的标准是：群中的运算容易实现，以保证有效性；在群中离散对数问题在计算上是困难的，以保证安全性。

目前最受关注的群是 Z_q^* ， $Z_{2^m}^*$ 和定义在有限域上的椭圆曲线的点所构成的循环群。椭圆曲线公钥密码系统是当前替代RSA公钥密码系统的最佳选择。它比RSA和有限域上的公钥密码系统更加有效。因为要达到 1024 位 RSA 安全水平，椭圆曲线公钥密码系统只要 163 位数上的运算。虽然这里运算比素数域的模运算要复杂，但是密钥要短很多。椭圆曲线群的另一个特点是对同样的基域 F 可以选择不同的椭圆曲线，而这些不同的椭圆曲线可采用相同芯片实现域的运算。

2.5 散列函数

散列函数[49]是将一串任意长度的二进制码映射为固定长度的二进制串的函数，映射所得的二进制串称为散列值。散列函数应用非常广泛，其安全性是基于它的单向性和抗碰撞性，是实现数字签名的有效性、安全性的重要工具。

散列函数易于计算，可以将任意有限长度的二进制串映射为固定长度的二进制串的函数，如 $H:\{0,1\}^* \to \{0,1\}^l$，其中 l 是映射后的固定长度。密码散列函数的逆运算还应满足难解性，即弱无碰撞性、强无碰撞性和单向性。

(1)弱无碰撞性：已知某消息 x,确定一个 $x'(x \neq x')$使得等式 $H(x)=H(x')$ 成立在计算上是困难的。

(2)强无碰撞性：同时得到两个消息 x 和 $x'(x \neq x')$能够满足等式 $H(x)=H(x')$ 成立在计算上是困难的。

(3)单向性：给定 c，找到满足等式 $H(x)=c$ 的消息 x 在计算上是困难的。

MD5 哈希算法是 Ron Rivest 在麻省理工学院提出的，是最近几年应用最广的哈希算法之一[49]。

MD5 算法中，输入采用任意长度的消息文件，输出采用一个 128bit 的摘要。算法对消息的处理是需要分组进行的，通常每组按 512bit 进行分别处理。图 2.1

对 MD5 算法的整体运算工程进行了相关描述。在图中，HMD5 代表了单个 512bit 的 MD5 处理过程，也就是所说的 MD5 的压缩函数。MD5 算法由以下五个步骤组成：

(1)附加填充比特：填充输入消息，让消息的长度与 448 模 512 同余。比如消息为长度为 448bit，则需填充 512bit，让其称为 960bit 的比特串。在最高比特位处添加 1，其他位均为 0。

(2)附加长度值：可以用 64bit 的数字补充前消息的长度，在之前的补充后的比特串的后面附加这 64 个 bit 数字，因此，比特串的长度是 512 个 bit。扩展之后，比特串以每 512bit 为一个分组的形式形成序列 Y1Y2...YL，因此，整个比特串的长度为 L 个 512bit。

(3)对链接变量缓冲区初始化：可以将链接变量和哈希函数的最终输出结果储存在一个 128 位的链接变量缓冲区。一个 128 位的链接变量缓冲区可以用 4 个 32 为 bit 的寄存器来表示，分别由字母 A、B、C、D 来表示。将这些寄存器分别初始化为以下十六进制值：A=67452301、B=EFCDAB89、C=98BADCFE、D=10325476。这些寄存器的存储方式是低位在前、高位在后，即 A：01 23 45 67、B：89 AB CD EF、C：FE DC BA 98、D：76 54 32 10。

(4)利用 HMD5 算法依次对每一个 512 比特的消息分组进行处理，如果有 L 个消息比特串分组，那么就要执行 HMD5 算法 L 次。

(5)当处理完 L 个 512 比特的分组后，就输出由 128 个 bit 组成的 CVL。

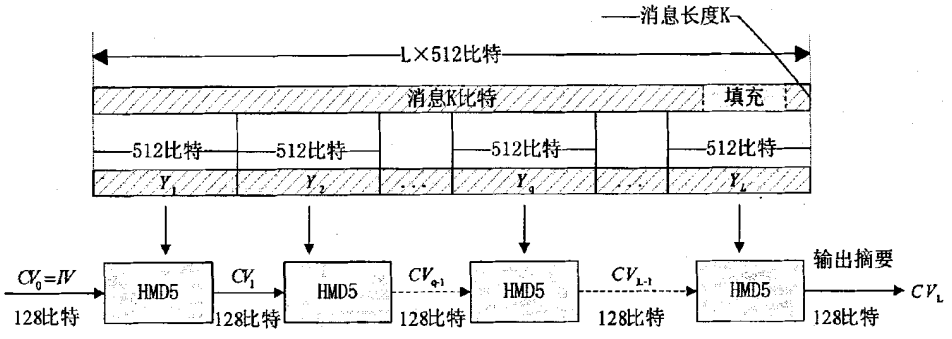

图 2.1 MD5 算法的整体描述

2.6 移动电子商务框架

移动电子商务系统因采用不同的核心技术、不同的应用领域和不同的市场定位而不同，图 2.2 为移动电子商务的一般框架，它主要包括用户级、开发者--提供者级。其中用户级主要由应用层、用户基础设施、无线和移动中间件、无线网络设施四部分组成。开发者--提供者级主要包括：应用开发者、内容提供者和服务提

供者三个部分，它们用于满足不同应用的需求和考虑。按照采用不同的核心技术分类，移动电子商务框架有如下三种：基于 SMS 的移动电子商务框架、基于 WAP 的移动电子商务框架和基于 Java 的移动电子商务框架。

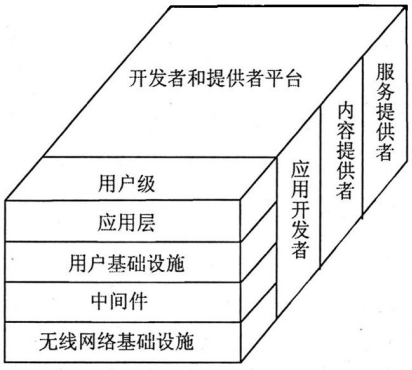

图 2.2 移动电子商务的一般框架

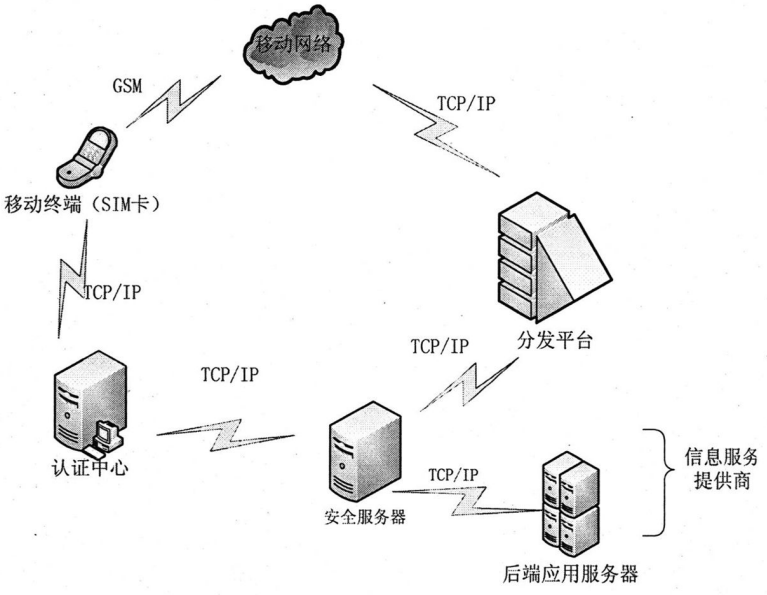

图 2.3 基于 SMS 的移动电子商务框架

图 2.3 为基于 SMS 的移动电子商务框架，包括了移动终端、移动网络、安全移动电子商务平台、应用服务提供商和认证中心五部分。其中安全移动电子商务平台主要有以下三个部分构成：SIM 卡、分发平台和安全服务器。其中 SIM 卡是客户端组件，提供了数据加密和签名功能；分发平台和安全服务器是服务器端组件，提供数据分发、数据加密和签名验证功能。移动终端与移动网络之间的通信是 GSM，其它几个部分之间的通信为 TCP/IP。

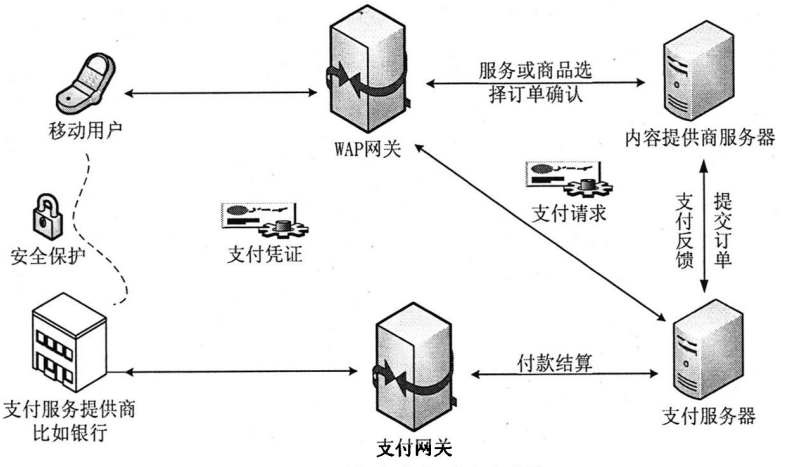

图 2.4 基于 WAP 的移动电子商务框架

图 2.4 为基于 WAP 的移动电子商务框架，它采用 WIM(WAP 用户识别模块)和智能卡技术来保证端到端的安全性和交易的不可否认性；可信移动终端能够保存证书且验证证书的有效性，确保了与移动电子商务应用系统、支付系统和安全基础结构之间通信的安全性，并能够对订单和支付信息签名，有效地保证了交易的真实性；移动终端和 WAP 网关之间采用 WTLS 协议加密；WAP 网关与商家 WAP 服务器采用 SSL 安全通道。

2.7 本章小结

本章首先介绍了电子商务的定义和分类，接着对目前移动电子商务中所存在的安全威胁和安全需求做了详细的阐述，然后给出了后续章节中电子商务微支付系统所依赖的各种难解问题；接着叙述了几种经典的公钥密码算法和后续章节中门限民主群签名方案中用到的散列函数。最后给出了移动电子商务的基本框架。

第三章 电子商务微支付系统研究

为了满足移动电子商务在各个方面的需求，首先必须保证电子商务中的安全性和公平性。现如今，对这些方面的研究虽然已经初现成果，如文献[52]、文献[53]和文献[54]等在安全性和公平性方面已经有了较大的提高。但是随着系统和用户需求的提高，现有的方案也出现了不足之处，如双向认证和 Hash 链交叉等问题。本章针对这些问题，提出了一种基于 Hash 链的微支付协议方案，并对该方案的安全性、公平性和效率进行了分析。

3.1 微支付协议模型

3.1.1 Millicent 协议

Compaq 和 Digital 于 1995 年联合开发出微支付系统 Millicent[50]。在小额付款中，Millicent 以其效率高、速度快得到了广泛的应用。其采用的保密技术没有涉及到公开密钥算法，只包含单向的 Hash 函数，这保证了他的快速计算能力，并加入“离线”支付验证方式，不仅降低了系统开销和运算成本，还保证了一定的安全性。

Millicent 系统主要包含：消费者(Customer)、商家(Vendor)和经纪人(Broker)。其中经纪人 B 在系统中起到了中间人的作用，也就是熟称的第三方。首先 C 必须与 B 签订一种类似于银行开户的合同，然后 B 通过买卖商家票据来为 C 和 V 提供服务。对于 C 来说，B 所持的票据可以用作购买 V 物品的通用货币；对于 V 来说，则用来返回未被使用的票据。不同于之前的中间服务器模式，在 Millicent 系统交易中，经纪人参与的部分很少，涉及到经纪人的交易量比较小，所以系统可以设置多个经纪人机构。

Millicent 使用的电子钱币是通过 Scrip 函数来制造的，其中每个用户使用的 Scrip 都有特别标识，只能本人使用，而且不同的 Scrip 不能在同一商家处使用。能够达到这些要求，都是因为系统用到了三种密钥方法：第一，消费者密钥(Customer-Secret)，消费者持有这个密钥来对 Scrip 加密，并证明自己拥有该 Scrip 的制造权限；第二，消费者控制密钥(Master-Customer-secret)，这个密钥是用作推导出第一个消费者密钥；第三，票据控制密钥(Master-Scrip-secret)，这个密钥是商家用来验证 Scrip 的真伪，防止消费者的欺诈。

图 3.1 为 Scrip 的示意图：

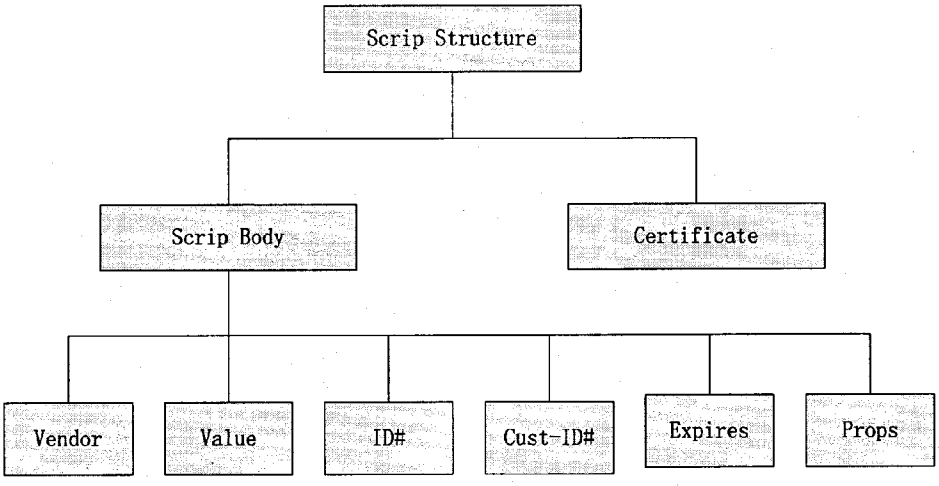

图 3.1 Scrip 格式图

上图中各个方框的含义：

(1)Vendor 表示该票据所对应的商家信息，消费者只能在此商家处使用该 Scrip；

(2)Value 表示该票据所包含的价值；

(3)ID# 显示该票据的唯一性，包含票据的识别码。它由 ID-series# 和 ID-sequence#两部分组成，其中 ID-series#的作用是当做商家 V 验证票据真伪时的依据；

(4)Cust-ID#表示消费者的身份 ID，即拥有该票据的消费者；

(5)Expires 表示票据的使用寿命，如果超过了这个时间限制，该票据则不法继续使用。

在 Millicent 系统中，Scrip 票据可以概括为两种，一种是 Vendor Scrip，另一种是 Broker Scrip。首先消费者先在经纪人 B 处购买 Broker Scrip，然后使用 Broker Scrip 在商家处购买由商家发行的 Vendor Scrip，最后消费者就可以使用 Vendor Scrip 与商家进行交易了。如下图 3.2、图 3.3 和图 3.4 为购买流程：

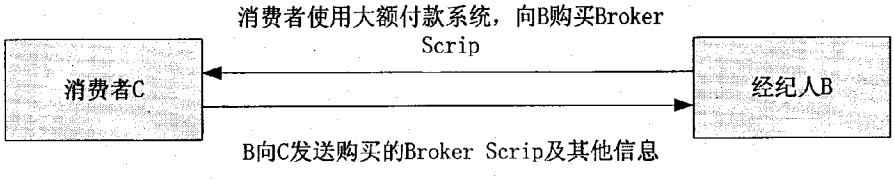

图 3.2 消费者购买 Broker Scrip

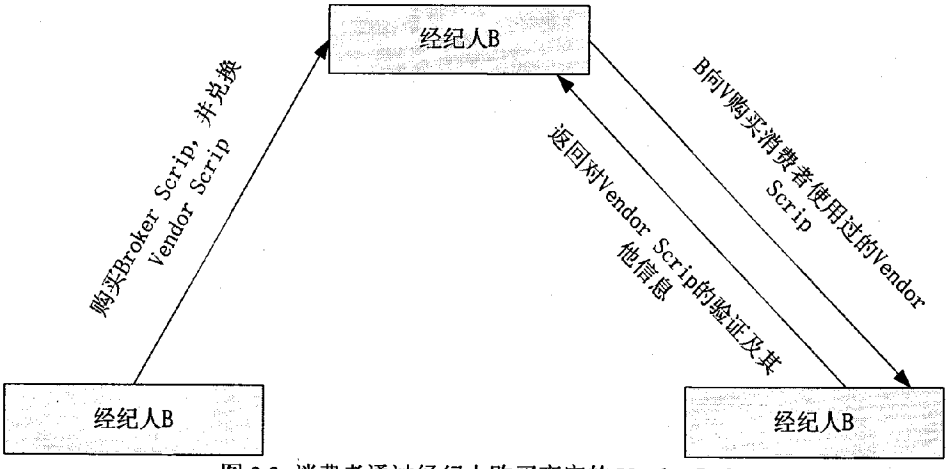

图 3.3 消费者通过经纪人购买商家的 Vendor Scrip

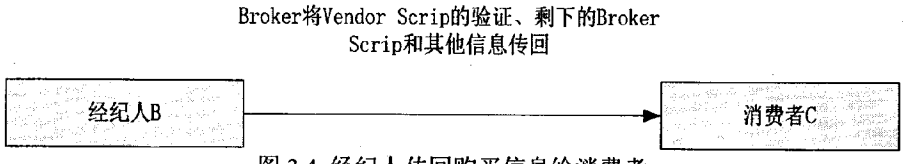

图 3.4 经纪人传回购买信息给消费者

Millicent 系统的交易流程：

消费者 C 方面：

(1)C 到 V 处选定商品，向 V 发出 Request(购物信息)，其中包括商品名、价格等信息；

(2)C 计算哈希函数 $H\{Customer\ Secret, Request, Scrip\}$，从而得到 Request-signature(摘要值)；

(3)C 把 Request、Request Signature、Vendor Scrip 和 Certificate 发送给 V，要求与 V 进行交易。

商家 V 方面：

(1)V 使用 Vendor Scrip 中的 ID 段查找对应的 Master-Scrip-Secret；

(2)V 计算哈希函数 $H\{Vendor\ Scrip,\ Master-Scrip-Secret\}$，从而得到 Vendor Scrip 的验证信息 Certificate。将此 Certificate 与从 C 中接收到的 Certificate 进行比较，如果相同，则可以进行交易，否则停止交易；

(3)V 找出 Vendor Scrip 中的 Customer ID 段，然后查找其所对应的 Master-Customer-Secret，最后计算函数 $H\{Master-Customer-Secret, Customer-ID\}$ 得出 Customer-Secret；

(4)把上面(1)、(2)、(3)步得到的三个结果进行哈希函数计算 $H\{\text{Customer}-\text{Secret},\ \text{Vendor Scrip},\ \text{Request}\}$ 得到 Request-Signature，最后将其与

从 C 中的到的 Request-Signature 作比较，如果相等，则交易继续进行，否则交易停止；

(5)V 把 C 所买物品、剩余票据、Reply 和验证信息发还给 C。

具体交易流程如下图 3.5：

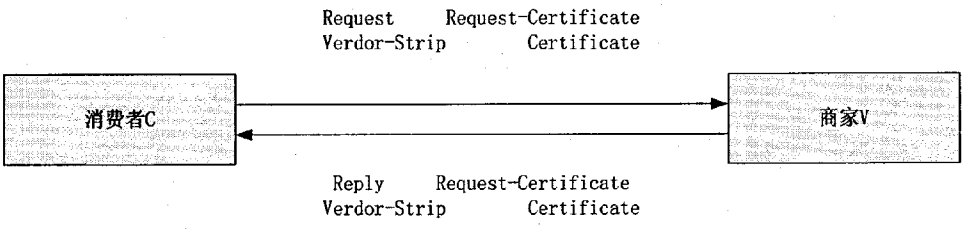

图 3.5 Millicent 系统消费者与商家的交易流程

Millicent 系统中，所流通的电子货币 Scrip 的制造和流通都是在经纪人、消费者和商家中进行。然而他们之间在交易阶段就已经完成了对 Scrip 的计算，商家收取该得的一部分，将剩余的发还给消费者，所以 Millicent 系统并不需要最后的结算阶段。

Millicent 系统分析：

(1)系统优势：1)使用了哈希函数计算，避免了第三者的伪造；2)使用可离线验证机制，提高系统效率；3)不需要复杂的加密技术，使用哈希函数计算，降低成本。

(2)系统劣势：1)系统中经纪人需要随时跟消费者和商家进行通信，情况复杂多变；2)消费者首次在经纪人处购买 Scrip 时，必须要在线交易，降低了系统效率；3)特定的 Scrip 只能在特定的商家处消费，这也加大了系统的通信量。

3.1.2 MicroMint 协议

MicroMint 是由 Ronald L.Riverst 和 Adi.Shamirt[51]所提出的一种微支付协议，与 Millicent 系统一样，也是由消费者 C、商家 V 和经纪人 B 三方组成，是一种基于唯一标识的离线电子现金形式，主要使用哈希函数的冲突原理而建立的，完全没有使用公开加密算法。

哈希函数的碰撞(电子货币的制造)：

MicroMint 协议中使用的电子货币是由哈希函数的碰撞产生的，也被称为 Hash Function Collisions。因为哈希函数可以把任意长度的输入经过计算(MD5)得到固定长度的输出，而且能够将输入缩减到一定长度，所以哈希函数可以进行多对一的计算。

现有哈希函数 h 对两个不同值 x_1 和 x_2 进行哈希运算得到一个相同的固定长度值 $y=h(x_1)=h(x_2)$，这就出现了一个哈希函数的碰撞。同样，如果输入 k 个不同

值 $x_1,x_2,\cdots,x_k$ 时，同时映射到一个 y 值上则产生一个 k 向哈希函数：$y=h(x_1)=h(x_2)=\cdots=h(x_k)$。在 MicroMint 协议中，是由 k(k 一般取 4)向哈希函数碰撞表示一个电子货币，即输入值为 x_1,x_2,x_3,x_4，并由组合 $M=\{x_1,x_2,x_3,x_4\}$ 表示一定数额的电子货币(如一分，一角等)。由此可知电子货币的制造是复杂的，但他的验证比较简单，只需要验证等式 $y=h(x_1)=h(x_2)=\cdots=h(x_k)$ 是否成立。

MicroMint 交易流程：

首先，经纪人 B 制造电子货币 M，需要确定多个不同的值 $x_1,x_2,\cdots,x_k$ 并拥有相同哈希值 y，其中 x 和 y 的长度决定了计算成本，而且电子货币的前期制造成本会更高一些，但随着电子货币的增加，成本又会慢慢降低。然后，消费者 C 从 B 处购买电子货币，与商家进行物品买卖。此时 V 需要验证 C 电子货币的正确性，首先检查 x_1,x_2,x_3,x_4 为四个不同值，并且同时映射到相同的 y 值上。同时系统也必须保证不会出现重复消费，所以经纪人为了以后核查需要保留使用过的电子货币的一个副本。和其他微支付系统一样，B 需要为 C 和 V 注册账号并维护，最后商家 V 和经纪人 B 同过离线方式进行结算。

MicroMint 协议分析：

MicroMint 协议与其他微支付系统相比具有以下特点：(1)采用多向哈希函数碰撞，杜绝了大规模的欺诈；(2)MicroMint 的电子货币可以面向多个商家，所以降低了计算消耗，消费者可以使用电子货币与多个商家进行交易；(3)消费者和商家都能够自行验证电子货币的真伪，不需要经纪人的参与，提到了交易效率；(4)未使用公钥密码技术，在安全方面有待提高。

3.2 Payword 协议模型分析

3.2.1 Payword 协议模型

Payword[51]协议由消费者(Consumer)、商家(Merchant)和经纪人(Broker)三方面组成。其中，C 在协议中的身份是普通消费者，主要向 M 购买商品并对其进行支付，M 则是向消费人群 C 提供商品，同时接受 C 的支付。C 和 M 都必须是经过 B 认证，并在 B 处建立自己的账号，B 对所建立账号进行维护、保障和转账。如图 3.6 所示，B 和 C、B 和 M 之间的虚线显示他们之间建立的联系是允许离线的，这保障了 C 和 M 之间的公平性。因为一般交易中 C 能够在购买商品后的一天或者一定时间内才向 M 进行支付。同时 C 和 M 之间必须是在线交易，这也是因为交易的公平性和高效性所考虑的。

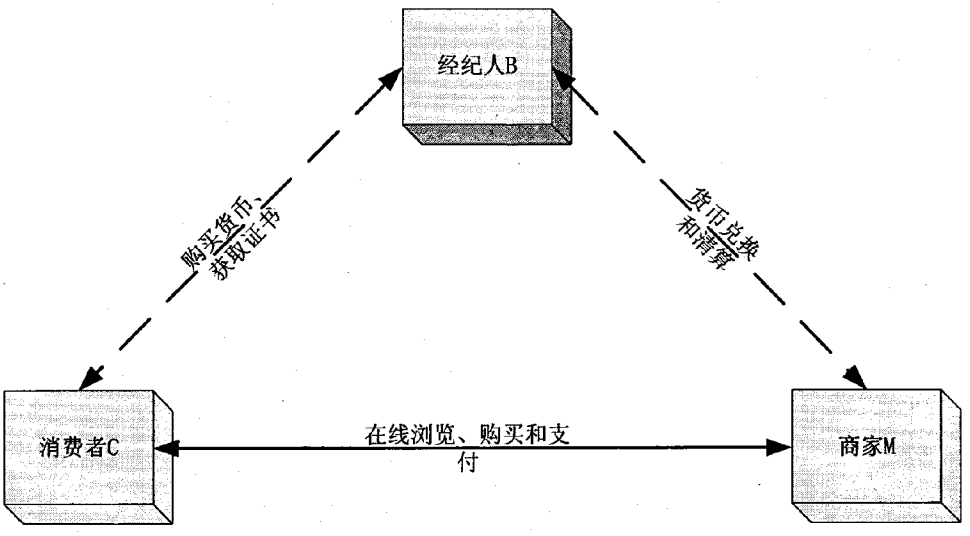

图 3.6 Payword 的协议模型

当 C 在 B 中建立自己账户时，B 需要给 C 提供一个 Payword 证书，该证书包含证书的有效期 D，这表示证书必须在规定时间到 B 处进行更新。当 C 获得证书后，则可以利用该证书制造购买商品所需的 Payword 链，利用支付链作为支付凭证提交给 M。M 接收到支付链后，经过验证通过之后 M 可以在规定时间向 B 提交支付对和消费者信息，从而得到所需价值的货币。具体操作如下：

(1)C 在 B 中注册之后，B 给 C 发送 Payword 证书 C_C，其中 PK_C 为 C 的公钥，ID_C 为 C 的身份信息，I_C 为附加信息，不包括消费者的身份信息。$B \to C : C_C = \{PK_C, ID_C, B, C, D, I_C\}$。

(2)C 根据证书 C_C 制造 Payword 链，如果 C 是第一次与 M 交易，则要先计算再签署对某一特定的 Payword 链 $w_1, w_2, \cdots, w_n$ 的承诺，即签名。首先选择一随机数 w_n，然后通过逆向计算出 Payword 链：$w_i = h(w_{i+1}), (i = n-1, n-1, \cdots, 0)$，所得的 w_0 用作支付根，不参与支付链。

(3)C 在 M 中选定要购买的物品，并向 M 发送商品信息、承诺、w_0 和支付对 (w_i, i)。$C \to M : ID$，商品，$C_C, w_0, (w_i, i)$。

(4)M 收到之后对其签名进行验证，并通过支付根 w_0 和承诺验证支付对，最后 M 在规定时刻向 B 提交支付对 (w_m, m) 和承诺，通过验证 B 扣除 C 相应的货币并发送到 M 的账户。

具体流程如图 3.7：

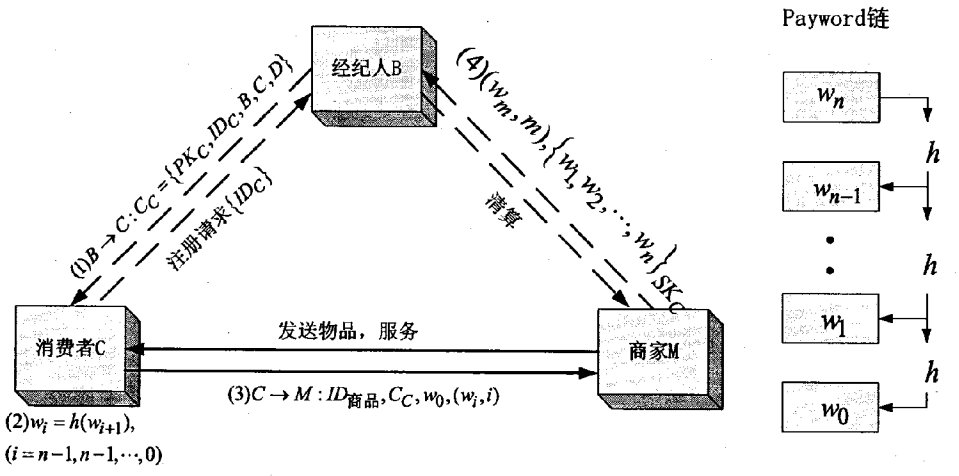

图 3.7 Payword 交易流程示意图

3.2.2 Payword 协议分析

Payword 协议通过给消费者颁发支付证书，使得消费者能够自行产生支付链，这在微支付系统中是独一无二的。当 C 在 B 中注册后，开始新的交易时不需要再通过 B 的认证和授权，只需要自己与 M 协商然后进行交易，最后没有使用的支付链也不需要返回给 B。在交易进行时，只存在 C 和 M 的相互验证，B 不用在其中过多参与，也不需要保留过多的用户或者商家的信息记录，这就为 C 的经常性访问提供了方便。因为在交易中 C 自行产生支付链并对 $w_1, w_2, \cdots, w_n$ 承诺，所以 C 知道自己所消费的额度，那些没有使用过的支付链被他人到处在计算上是困难的。当用户支付结束时，支付根 w_0 将会和 C 消费的支付链同时保存在数据库当中，如果用户使用相同的支付根再次支付则会得到提醒，防止 C 重复消费和 M 的重复兑换。

但同时，Payword 协议也存在一定的缺陷：

(1)双向认证问题：交易中 M 可以对 C 进行验证，但 C 没有对 M 进行验证，没有体现出公平性，C 可能受到不法商家的欺骗而损失利益。

(2)匿名性问题：在 $B \rightarrow C$ 和 $C \rightarrow M$ 过程中，用户的信息 ID_C 和 PK_C 多次出现在不安全信道当中很容易被他人截取，并用此来查看 C 的信息和交易内容，损害 C 的利益。

(3)公平性问题：消费者 C 在够买完商品完成支付后，商家 M 并没有给 C 一个支付凭据，当商家 M 拒绝给 C 提供相应商品时，消费者 C 无有效凭据。

(4)消费额度问题：由于在交易中，商家 M 并不知道 C 的存款，但是 C 可以一直进行支付链的制造，所以 M 发送服务给 C 但是却不确定能否得到相应的报酬。

(5)支付链交叉问题：消费者 A 和消费者 B 在同一商家购买物品时，有可能他们授权的支付链存在交叉，而商家正好可以利用这一漏洞对消费者进行欺诈。

(6)经纪人问题：交易过程中，经纪人起到一个第三方的角色，他可以给 C 和 M 提供一个平台，但是由于他的权限过大，如果他有欺诈行为，这将对消费者 C 和商家 M 造成极大的损失。

3.3 Payword 协议的改进工具

针对前一小节中协议存在的问题，下面介绍几种改进协议需要使用到的几种工具：

3.3.1 密钥协商协议

密钥协商[49]是指在参加与通信的双方之间建立共享密钥的过程，该过程主要涉及到两个不同用户之间共同协商得到一个共享密钥，并且任意一方事先都无法确定或者得到该共享密钥的值。ISO/IEC 11770-3 讲述了几种使用公钥密码技术的密钥协商机制，表 3.1 详细列出了这几种协商机制的特性。

表 3.1 几种使用公约密码技术的密钥协商机制特点比较

传输机制	1	2	3	4	5	6	7
传输回合数	0	1	1	2	2	2	3
密钥控制	A+B	A+B	A	A+B	A+B	A+B	A+B
密钥鉴别	A+B	B	A+B	--	A+B	A+B	A+B
密钥确认	--	--	B	--	--	--	A+B
实体鉴别	--	--	(A)	--	--	B	A+B

Diffie-Hellman 协议就是一种典型的协商机制，该机制是通过两回合的传输使得通信双方获得他们的共享密钥。由于协议必须保证通信双方中任何一方都不能单独获得密钥，所以 Diffie-Hellman 协议提供了一种联合的密钥控制，并且算法是建立在有限域中计算离散对数问题，这比单纯的计算指数问题困难的多。期间要算法如下：

(1)系统初始化：协议双方 A 和 B 确定两个大的质数 p 和 g，两者不是秘密值，且 g 是模数 p 的原根；

(2)A 随机选取一个任意大随机数 x，计算 $X = g^x \bmod p$ 并发送给 B；

(3)B 随机选取一个任意大随机数 y，计算 $Y = g^y \bmod p$ 并发送给 A；

(4)A 收到 Y 后计算 $m = Y^x \bmod p$；

(5)B 收到 X 后计算 $m' = X^y \bmod p$；

(6)验证等式 $m = m' = M$，如果成立则得到 A 和 B 的共享密钥 M，否则协议无效。

图 3.8 为 Diffie-Hellman 协商协议简图：

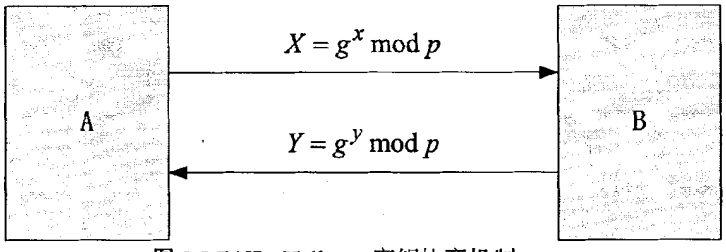

图 3.8 Diffie-Hellman 密钥协商机制

由于以上 Diffie-Hellman 协议的通信都是在透明信道上传输的，所以很容易受到第三方的恶意攻击，为了预付和避免这种攻击，一般可以使用公钥密码对消息进行签名然后再发送出去。协议假设 A 和 B 拥有各自的私钥和公钥 SK_A, SK_B, PK_A, PK_B，协议步骤如下：

(1)A 选取随机数 x，然后发送给 B；

(2)B 选取随机数 y，然后发送给 A；

(3)根据 Diffie-Hellman 协议计算出共享密钥 m，B 利用自己的私钥对消息 (x, y) 签名，再由 m 对其加密得到 $((x, y)_{sk_B})_{E_m}$，然后与 y 一起发送给 A；

(4)A 收到 B 发送的消息后对其进行解密，然后验证 B 的签名 $(x, y)_{sk_B}$，如果正确则 A 计算 $((x, y)_{sk_A})_{E_m}$ 并发送给 B；

(5)B 收到 A 发送的消息后对其进行解密，然后验证 A 的签名 $(x, y)_{sk_A}$，如果正确则协议完毕。

图 3.9 为端到端协商协议简图：

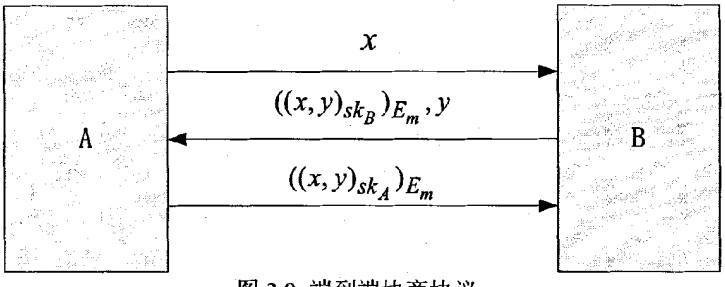

图 3.9 端到端协商协议

3.3.2 双线性对映射的定义

基于双线性对的密码体制是目前密码学界的一个研究热点[错误! 未找到引用源.]。目前为止，很多基于双线性对的方案都已被提出，这些方案涉及到的双线性对问题大多

是基于它的双线性和非退化性。下面简单介绍了一些双线性对的基本性质，及其计算方法。

双线性对是指在两个不同的循环群之间相对的线性映射关系。首先，确定一个大素数 q，设 G_1,G_2 是两个模为 P 的阶循环加法群。G_T 是一个 q 阶循环乘法群。然后，假设在 G_1,G_2,G_T 中，离散对数的计算问题是非常困难的。最后，定义一个双线性映射对 $e:G_1\times G_2\to G_T$，同时该线性对需要满足以下三个性质：

(1)双线性：随机选取三个成员 $P,R\in G_1,Q\in G_2$ 和两个随机数 $a,b\in Z_a^*$，有

1) $e(P+Q,R)=e(P,R)e(Q,R)$；

2) $e(P,Q+R)=e(P,Q)e(P,R)$；

3) $e(aP,bQ)=e(P,Q)^{ab}$。

(2)非退化性：存在成员 $P\in G_1,Q\in G_2$，使得 $e(P,Q)\neq 1\in G_T$。

(3)可计算性：对于成员 $P\in G_1,Q\in G_2$，存在有效多项式计算 $e(P,Q)$。

3.4 基于 Payword 的匿名性微支付协议

3.4.1 协议描述

在 3.2.2 节中，经过对 Payword 协议的分析，匿名性在协议中是一个短板。在协议产生的早期也未得到高度的认识，在实际操作中匿名性的问题将直接影响参与三方的切身利益。Ellis 提出的微支付协议对匿名性的定义是：参与者三方中的任意一方的 ID(身份标识)只要被别人窃取，则不具有匿名性。同时如果运用盲签名技术，则会大大增加协议的计算量，降低协议的效率，使得成本增加。

综合上述需求，本文提出了一种基于 Payword 的匿名性微支付协议。首先匿名性的实现是通过消费者在经纪人注册，经纪人提供一个匿名标识给消费者。然后消费者通过这一匿名标识与经纪人和商家进行交易。最后商家通过消费者支付的 Hash 链在经纪人处进行结算。该协议的唯一需要肯定的是经纪人必须消费者和商家可信的。

下面是一些协议使用的符号说明：

(1)消费者 C，商家 M，银行 B；

(2)Z：C，M，B 的任意一个实体；

(3) ID_Z：Z 的身份标识；

(4) PK_Z，SK_Z：Z 的公钥和私钥；

(5) $\{Data\}_{PK_Z}$：Z 对数据 Data 使用公钥加密；

(6) $H(Data)$：对数据 Data 进行哈希运算；

(7) $Sign_Z(Data)$：Z 使用私钥对数据 Data 进行数字签名；

(8) $A \rightarrow B:\{Data\}$：A 通过安全信道把数据 Data 发送给 B。

1 注册阶段

(1)消费者注册：

消费者将自己的身份信息(匿名)，地址及其他信息 I_C 进过公钥 PK_C 加密发送给银行：

$$C \rightarrow B:\{ID_C, I_C\}_{PK_C} \tag{3.1}$$

银行收到之后经过验证确定消费者的正确性，然后给消费者建立账户并分配一个匿名加密标识 $H(ID_C)$，该标识不含有消费者身份的任何信息。最后经过加密银行把证书发送给消费者：

$$B \rightarrow C:C_C = \{H(ID_C), ID_B, PK_C, I_C, E\}_{SK_B} \tag{3.2}$$

其中：E 是证书的有效期。

(2)商家注册：

商家将自己的营业许可证 ID_M 和网络地址 A_M 等信息经过公钥 PK_M 加密发送给银行：

$$M \rightarrow B:\{ID_M, A_M, I_M\}_{PK_M} \tag{3.3}$$

与消费者注册相似，银行经过验证后为商家建立账户并分配一个标识 ID_M，发送证书给商家：

$$B \rightarrow M:C_V = \{ID_M, ID_B, PK_M, A_M, I_M, E\}_{SK_B} \tag{3.4}$$

图 3.10 显示了消费者与商家的注册流程：

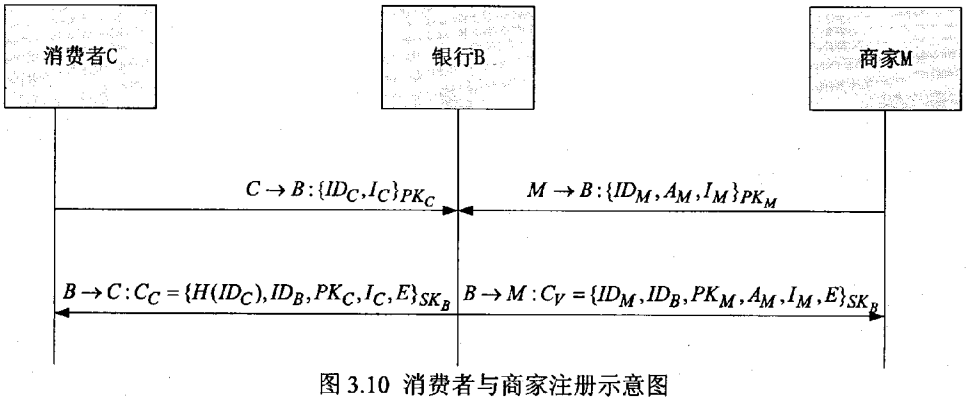

图 3.10 消费者与商家注册示意图

2 基于双线性对的密钥协商协议

微支付协议中，消费者与商家在交易之前需要通过协商、互相认证，确保安全之后才能进行通信，这样保证了消费者和商家之间的互相欺诈行为。密钥协商是一个协议，通过两个或者多个成员在一个公开的信道上通信联合地建立一个秘密密钥。在一个密钥协定方案中，密钥的值是某个函数值，其输入量由两个成员提供。消费者与商家通过密钥协商协议可以很好地保证通信的安全性。

(1) Setup

Setup 为系统初始化算法，令 q 为一个大素数，点 P 为 q 阶加法循环群 G_1 的生成元，G_2 为同阶的乘法循环群，存在双线性映射 $e:G_1\times G_1\to G_2$，$H_1:\{0,1\}^*\times G_1\to Z_q$，$H_2:\{0,1\}^*\to G_1$ 为两个哈希函数，选取随机数 $s\in Z_q$ 作为系统主密钥，令 $P_{pub}=sP$ 作为系统公钥。

(2) Extract

Extract 为私钥提取算法，给定一个身份信息 ID，PKG 计算 $d_{ID}=sH_2(ID)$，并将 d_{ID} 秘密发送给身份信息给 ID 的用户作为其私钥，同时 $Q_{ID}=H_2(ID)$ 为其公钥。

(3) Key agreement

Key agreement 为密钥协商协议，消费者 C 选择一个随机数 $r_c\in Z_q$，计算 $K_c=r_cH_2(ID_c)$，然后将 r_c,K_c 发送给商家 M；同样商家 M 选取随机数 $r_m\in Z_q$，计算 $K_m=r_mH_2(ID_m)$，然后将 r_m,K_m 发送给消费者 C；C 收到后计算得到 $L_c=r_cH_2(ID_m)$，B 收到后计算得到 $L_m=r_mH_2(ID_c)$；C 计算 $K_{cm}=e((K_m+L_c),Q_c)$；B 计算 $K_{mc}=e((K_c+L_m),Q_m)$；验证等式 $K_{cm}=K_{mc}$：

$$\begin{aligned}K_{cm}&=e(K_m+L_c,Q_c)\\&=e(r_mH_2(ID_m)+r_cH_2(ID_m),H_2(ID_c))\\&=e(H_2(ID_m),H_2(ID_c))^{r_m}e(H_2(ID_m),H_2(ID_c))^{r_c}\\&=e(r_cH_2(ID_c)+r_mH_2(ID_c),H_2(ID_m))\\&=e(K_c+L_m,Q_m)=K_{mc}\end{aligned}\tag{3.5}$$

由此得到双方的共享密钥 $K_{cm}=K_{mc}$(为方便计算后面都用 K_{cm} 表示)。图 3.11 表示密钥协商示意图：

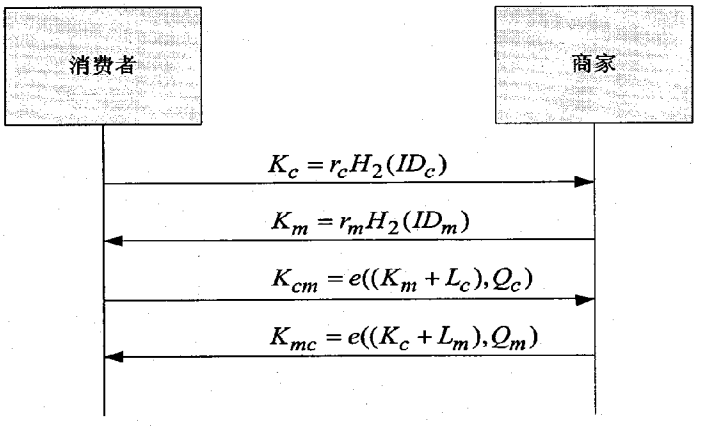

图 3.11 密钥协商示意图

3 支付协议

当不同参与者都完成协商之后，消费者就可以通过网页浏览商家的店铺，然

后选定自己需要购买的商品，然后确定商品价格 price 和订单信息I_{good}，加密后发送信息$\{ID_c, I_{good}, price, E\}_{K_{CB}}$给银行。其中 E 为订单有效期，$K_{CB}$为消费者与银行的共享密钥。银行用自己的密钥$K_{BC}$对消息验证后得到 price 等信息，然后对 C 账户余额进行查询，如果大于 price 则授权消费者制造支付链，并冻结 price 数额的金额，否则停止消费者的服务请求。

消费者获得交易的许可之后，随机选取一组随机数(w_{an}, w_{bn})，并用反向机制制造一组双 Hash 支付链：

1) 支付主链：$w_{a(i-1)} = H(w_{ai})(i = n, n-1, n-2, \cdots, 1)$，$\{w_{an}, w_{a(n-1)}, \cdots, w_{a0}\}$；

2) 支付从链：$w_{b(i-1)} = H(w_{bi})(i = n, n-1, n-2, \cdots, 1)$，$\{w_{bn}, w_{b(n-1)}, \cdots, w_{b0}\}$。

消费者制造出支付对之后，对其进行承诺，然后将第 i 个支付对(w_{ai}, w_{bi})、支付根(w_{a0}, w_{b0})和商品信息发送给商家(第 i 个支付对正好对应商品价格)：

$$C \to M : \{(w_{ai}, w_{bi}), (w_{a0}, w_{b0}), I_{good}, E, I_c\}_{K_{CM}} \tag{3.6}$$

其中I_c为交易的附加消息。商家收到消息后用共享密钥解密验证，得到支付对(w_{ai}, w_{bi})，通过计算得到$(w_{a0}, w_{b0})'$，与消费者发送过来的支付根(w_{a0}, w_{b0})对比验证是否相同，验证通过后商家即可以把商品发送给用户。

在现实生活中，消费者有可能需要同时与多个商家进行交易。在这种情况下，消费者每与一个商家交易就必须向银行提出一次交易请求和制造一次支付链，这大大降低了系统效率。为达到同时与多个商家进行交易的目的，消费者可以首先将多个订单消息和价格总和发送给银行，经过银行授权之后制造一条足够长的支付对，并将其分为 n 段，如图 3.12 所示。

$$\text{支付主链：}\quad \begin{aligned} & w_{a(i-1)} = H(w_{ai}) && \{w_{ai}, w_{a(n-1)}, \cdots, w_{a0}\} \\ & w_{a(2i-1)} = H(w_{a2i}) && \{w_{a2i}, w_{a(2i-1)}, \cdots, w_{a(i+1)}\} \\ & w_{a(ni-1)} = H(w_{ani}) && \{w_{ani}, w_{a(ni-1)}, \cdots, w_{a((n-1)i+1)}\} \\ & (i = n, n-1, n-2, \cdots, 1) \end{aligned} \tag{3.7}$$

$$\text{支付从链：}\quad \begin{aligned} & w_{b(i-1)} = H(w_{bi}) && \{w_{bi}, w_{b(n-1)}, \cdots, w_{b0}\} \\ & w_{b(2i-1)} = H(w_{b2i}) && \{w_{b2i}, w_{b(2i-1)}, \cdots, w_{b(i+1)}\} \\ & w_{a(ni-1)} = H(w_{ani}) && \{w_{bni}, w_{b(ni-1)}, \cdots, w_{b((n-1)i+1)}\} \\ & (i = n, n-1, n-2, \cdots, 1) \end{aligned} \tag{3.8}$$

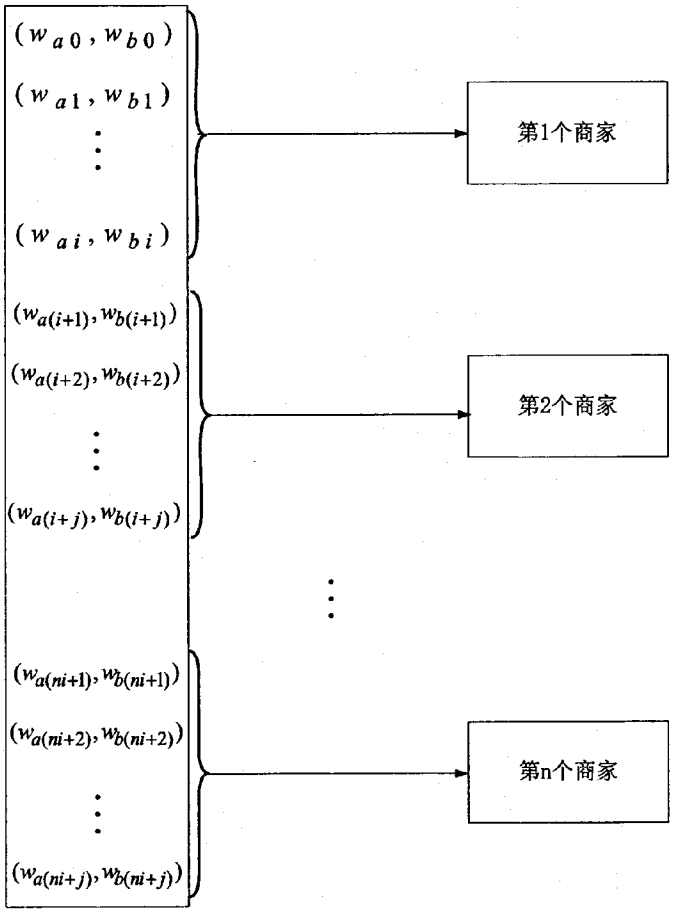

图 3.12 消费者同时与 n 个商家交易示意图

消费者将不同的支付对发送给不同的商家，然后和其进行交易，验证方法和前面一致。图 3.13 是支付协议示意图。

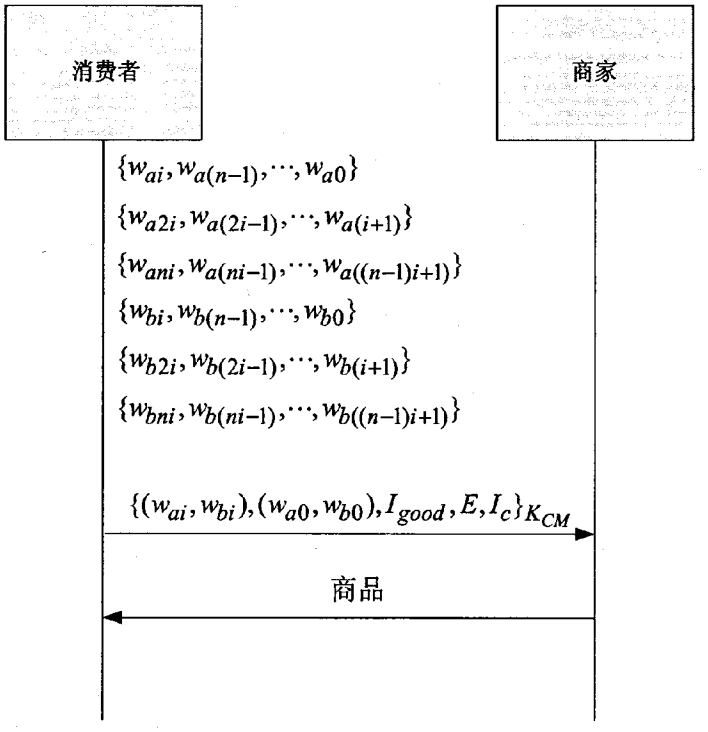

图 3.13 支付协议示意图

4 结算协议

消费者与商家交易结束后，商家给银行发送结算请求，将消费者支付给商家的支付对 (w_{ai}, w_{bi}) 和商家的凭证等信息发送给银行：$\{ID_M, (w_{ai}, w_{bi}), I_{good}, price, E\}$。银行收到之后对支付对进行验证。验证通过之后，银行将价值 price 的存款拨给商家，至此协议结束。

3.4.2 安全性分析

(1)匿名性

因为在无线通信网络中进行的电子商务安全性不高，而用户在交易中传输的数据有可能会被泄露或遭到黑客攻击，导致用户私人信息被盗，所以保证用户的匿名信是协议迫切需要解决的问题，上述协议在交易的各个阶段都为用户提供了匿名信：

在注册阶段，消费者将身份信息 ID_c 发送给银行，银行经过 Hash 运算分配一个匿名标识 $H(ID_c)$ 返还给消费者。消费者在后面的交易阶段使用该匿名标识与商家进行交易。

在协商阶段，双方的私钥和公钥都必须先经过 Hash 运算得到，如消费者的公钥为 $H_2(ID)$。在消息的传递过程中用到的 $K_c = r_c H_2(ID_c)$，$L_c = r_c H_2(ID_m)$ 都是只包含 ID 的点映射，由于 Hash 函数的单向性，双方都不能从中获得对方的信息，

防止了身份的泄露，保证了用户的匿名性。

(2)双向认证

如果在用户交易中系统缺乏双向认证，将会出现交易一方被冒名顶替，给原交易双方造成损失。未解决这一问题以上协议增加了一项密钥协商协议，其中认证双方各选一随机数并计算 K_c、I_c和K_m、I_c，互相交换后得到各自的共享密钥 K_{cm}和K_{mc}，通过验证后得出结论$K_{cm}=K_{mc}$。这样使得交易中任何一方都能够保证是在与认证过的用户进行交易，避免了恶意用户的冒名顶替。

(3)Hash 链交叉

交易过程中，不同的消费者所产生的支付链可能存在着交叉问题(两条支付链中存在相同的支付对)，这会使得商家在结算时无法兑换自己应得的货币，损害商家利益。以上协议提供了一种双 Hash 链的支付方式，结算时商家将信息 $\{ID_M,(w_{ai},w_{bi}),I_{good},price,E\}$ 发送给银行(其中包括商品信息、价格、有效期、支付对等)。如果出现了两条支付对存在交叉，银行可以将交易开始时消费者发送给它的信息 $\{ID_c,I_{good},price,E\}_{K_{CB}}$ (其中包括商品信息、价格、有效期)与其对比，确定消费者身份和订单信息之后将价值 price 的货币拨给商家。这样一来，就不会因为支付对的交叉而损害商家的利益。

3.4.3 公平性分析

(1)重复消费

在交易中，消费者有可能将同一个支付对多次地发送给不同的商家，这使得在结算阶段不同商家间产生纠纷，破坏交易公平性。以上协议中要求银行保留每次消费完之后的支付根(w_{a0},w_{b0})和消费者凭证，如果有某个商家在要求清算时提供给银行相同的支付根，则银行可以查出该消费者并对其进行制裁，很好地避免了消费者的重复消费。

(2)恶意透支

如果消费者在银行的存款额少于所购买的商品价格，而消费者却能够制造支付对与商家进行交易，这就出现了恶意透支的现象。以上协议在支付阶段商家必须首先给银行发送信息 $\{ID_c,I_{good},price,E\}_{K_{CB}}$，银行解密之后查看消费者账户余额是否大于商品价格 price,如果大于则允许交易，否则拒绝交易请求，防止了消费者的恶意透支。

(3)商家欺诈

当消费者将支付对等信息发送给商家之后，如果商家拒绝发送商品给消费者，这样的欺诈行为将会对消费者造成巨大的损失。如果在以上协议出现这种问题，

消费者可以将本次服务的支付对(w_{ai}, w_{bi})和订单信息发送给银行，防止商家提前清算。如果商家已经清算，则银行可以要求商家发送交易收据给消费者，如果商家拒绝，则经纪人有权将该商家列入黑名单并追究其责任。

3.4.4 效率分析

对于 Payword 微支付系统而言，效率的高低是系统好坏的决定性因素。是否能够在支付和结算阶段以高效快捷、成本低廉、方便易用的方式进行支付交易，是判断一个系统优劣的重要因素。以上协议在支付阶段运用双Hash链的支付方式，消费者自行制作双支付链 (1) $w_{a(i-1)} = H(w_{ai})(i = n, n-1, n-2, \cdots, 1)$，(2) $w_{b(i-1)} = H(w_{bi})(i = n, n-1, n-2, \cdots, 1)$，以其非单元支付的方式减少了与服务器通信的次数。同时采用一条支付链分段支付的方式，降低了消费者制造 Hash 链的次数，节省了交易时间，提高了系统效率。

3.4.5 方案比较

经过上面的分析，相比较原来的 Payword 协议，不管从安全性、公平性和效率上，本协议都有了很大的提高。表 3.2 为改进后的 Payword 协议和其他微支付协议在一些性能上的比较：

表 3.2 改进协议性能比较

性能	Payword	文献[52]	文献[53]	文献[54]	改进协议
匿名性		√	√	√	√
双向认证					√
Hash 交叉			√		√
重复消费	√	√	√	√	√
恶意透支		√	√	√	√
商家欺骗	√	√	√	√	√
多商家					√

通过上述这些性质的比较，本文提出的改进微支付协议具有比较良好的性能。相比于 Payword 协议、文献[52]、文献[53]和文献[54]，本方案都具备比较明显的优势。

3.5 本章小结

本章介绍了几种微支付协议的模型，包括 Millicent、MicroMint 和 Payword 协议模型。针对现有微支付方案中存在的安全性、公平性较差和效率较低等问题，本章提出了一种改进的具有匿名性的 Payword 微支付协议方案。该方案中，双线性对的使用保证了方案具有较高的效率；双 Hash 链的使用可有效防止用户的重复消费和恶意透支等问题，保证了系统的公平性。另外，针对消费者可能同时与多个商家进行交易的情况，提出了一种新支付方法，用户只需要制造一条支付链便可完成和不同商家的同时交易，这较好地提高了系统的效率，降低了系统成本。本章节的研究是以 Hash 链为基础的微支付协议方案，而下一章的研究目标是在微支付协议中引入数字签名技术。

第四章 基于数字签名机制的微支付协议研究

现如今微支付协议中的信息传递都是在不安全信道中进行的，这也对信息的安全性提出了更大的挑战。数字签名能够实现身份认证、数据完整性、不可抵赖性等功能，是信息完整性和认证性的关键技术之一，也是电子商务及网络安全的关键技术之一。将数字签名技术运用于微支付系统可以大大提高信息传递的安全性，同时，计算量的多少是衡量一个方案的系统效率和可行性的重要因素。门限签名能够防止单点失效而产生的密钥丢失问题，本章提出了一种具有门限特性的民主群签名方案；由本文第三章可以看出，如果在微支付系统中使用Hash支付链，那么就能够保证系统有较高的效率。本章基于具有门限特性的民主群签名机制，结合Hash链提出一种新的微支付协议方案。该方案中，门限数字签名的使用保证了信息传递的完整性和可认证性，Hash链的使用在一定程度上提高了方案的效率。

4.1 数字签名

一切在计算机上生成和处理的文件，如图像、文档、软件和 Email 等都叫做电子文档。我们可以利用一种相对于日常生活中的手写签名的数字模拟手段一数字签名，来对电子文档进行签名。目前，最流行的电子签名依赖于公钥密码学架构。图 4.1 给出了数字签名方案的组成。

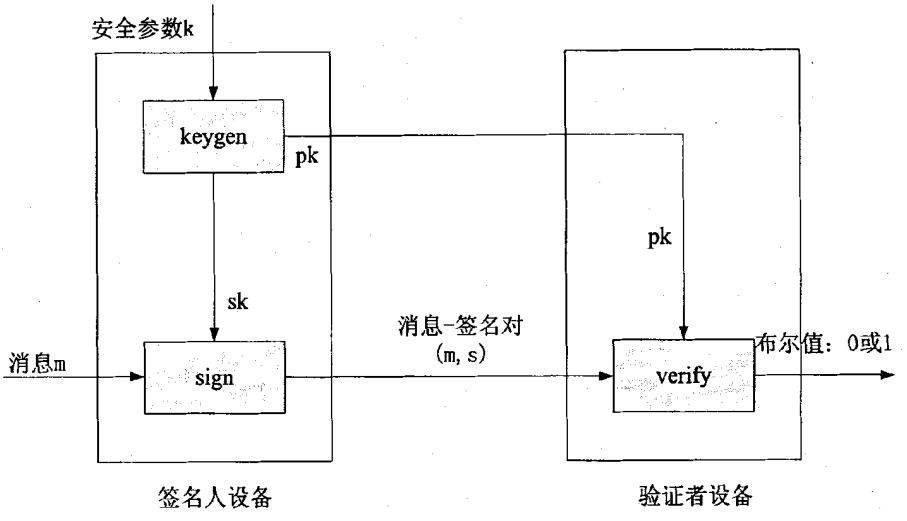

图 4.1 数字签名方案的架构

通常，一个数字签名方案包括密钥生成算法、签名算法和验证算法三个过程。同时，数字签名方案的安全性要求也是较高的，它必须能够保证在攻击者知道签名人的公钥和若干个有效的消息-签名对的情况下，也无法伪造该签名人的有效签名[49]。

数字签名技术作为信息安全的核心技术之一，能够提供认证性、完整性和不可否认性等安全服务，同样在安全电子商务和安全电子政务领域中也能起到关键作用。但是随着对数字签名研究的不断深入及电子商务、电子政务的快速发展，简单模拟手写签名的一般数字签名已不能完全满足现实中的应用需求。研究具有特殊性质或特殊功能的数字签名成为数字签名研究的主要方向。

4.2 身份识别

在微支付协议中，有两名参与者 Alice 和 Bob，Alice 知道一条重要的秘密信息，并且很想说服 Bob 相信自己确实知道这个消息。一个比较直接的做法显然是 Alice 将这个秘密消息告诉 Bob。但是这样一来，Bob 也知道了这个秘密，之后 Bob 可以告诉任何一个他想告诉的人，而 Alice 对此却毫无办法。一般来说，在密码体制中这里所说的秘密可以对应的是 Alice 的私钥 x，而 Bob 知道 Alice 的公钥 y。Alice 要让 Bob 确定自己拥有公钥 y 所对应的私钥 x，那么就意味着 Bob 承认了 Alice 的身份，这就是所谓的身份识别的过程。

在协议中要实现身份识别的方法一般采用交互式证明。即参与双方交互，一方知道秘密，称为示证者，另一方称为验证者。Alice 希望 Bob 相信自己的确知道某个秘密。交互证明可以有若干轮组成。在每一轮中，Alice 和 Bob 需要接收对方消息，然后加以计算，将计算结果发送给对方。一种比较典型的方式是挑战-应答式(challenge-response)，这是一个三段式的结构，如图 4.2 所示：

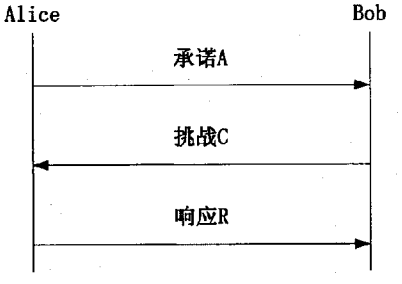

图 4.2 挑战-应答式协议

为了说服 Bob，Alice 需要首先选取随机数，利用该随机数作出一个承诺 A，将该承诺发送给 Bob；Bob 接收到 A 之后，经过计算会返回一个值 C 给 Alice，这

个值称为挑战；最后，Alice 需要利用自己的秘密 x 和收到的挑战作出响应，即发出响应值 R 给 Bob。Bob 会利用 Alice 的公钥 y 来检查所收到的承诺和响应值之间的关系是否一致，如果一致，则相信 Alice。如果不一致，Bob 就直接拒绝接受这个示证者[49]。

在微支付协议中参与者之间的身份认证可以通过这样一种方式来完成。比如 A 是消费者与商家 B 经过身份识别之后，A 就可以放心地在 B 处进行商品的选购和支付。由于微支付所要求的匿名性，我们在下节将提出了一种基于身份的数字签名方案。该方案不仅能够达到系统所要求的匿名性，并且还加入了门限技术，加强了方案的追踪能力。

4.3 基于门限的民主群签名方案

当微支付交易双方在完成身份识别之后，下一步就是通过通信信道传递购买信息和服务信息了。但现如今信道的安全威胁越来越大，用户必须采取安全有效的措施解决这一问题，不然既损失了双方利益还有可能暴露用户的身份信息，这些都是用户所不想看到的结果。经过对传递信息的综合分析，数字签名技术能够有效地解决这一安全性难题，下面本文提出了一种基于门限的民主群签名方案。

民主群签名的主要思想是使用群密钥协商协议来保证群成员动态变化后群公钥、群秘密的相应更新，协商后的群秘密用作追踪陷门，因此当前群体内任何成员均可对群签名执行追踪操作，不在该群体内的任意用户因不知群秘密而无法做到这一点。

为此，假设已经有一个安全的群密钥协商体制 GKA(S,J,L)，该体制包含三个算法：群体初始化算法 S、成员加入算法 J 和成员退出算法 L。算法 S 以当前群成员的公钥/私钥为输入，通过所有群成员的交互生成一个共享的群密钥；现有群成员与欲加入该群的新成员执行交互算法 J：原有群成员的输入包括自己的原签名私钥、全部原有群成员的公钥，新成员的输入包括自己的公钥/私钥，算法输出为更新后的共享群密钥和各成员公钥/私钥；算法 L 的输入包括剩余群成员的公钥/私钥、退出成员的公钥，输出为更新后的贡献群密钥和剩余各成员的公钥/私钥。

对这个群密钥协商体制的安全性要求是：

(1)协商出的群密钥只能有群成员掌握，不属于群体内的任何人都不知道该密钥的值；

(2)新加入群体的成员不知道他加入之前群体的群密钥；

(3)退出群体后的成员不知道他退出之后群体的群密钥。

满足这些条件的方案可用于下面提出的民主群签名方案中。方案具体描述如下。

4.3.1 方案描述

(1) 群体初始化

在群体初始化开始阶段，由可信中心生成系统参数，即通过给定的安全参数 λ，系统可信中心生成系统参数 G,q,g,h,H，其中，q 是一个长为 λ 比特的素数，G 为 q 阶乘法循环群，g 和 h 为 G 上的任意两个生成元，$H:\{0,1\}^* \to Z_q$ 为密码学意义上安全的哈希函数，其中 $Z_q=\{0,1,\cdots,q-1\}$，G,q,g,h,H 一起构成系统的公开参数。

(2) 密钥生成

密钥生成算法 KeyGen 生成用户公钥、私钥。假设 n 个用户构成一个群体，群成员 ID_i 选取随机数 $x_i \in Z_q$ 作为私钥，计算 $y_i=h^{x_i}$ 作为公钥，该用户将自己的公钥公开注册于可信中心，以便系统中其他用户可以在可信中心处检索。拥有公钥/私钥 $(x_i,y_i), i=1,\cdots,n$ 的 n 个用户构成一个群体 $U=\{ID_1,ID_2,\cdots,ID_n\}$，U 中的每个用户均有权以群体的名义对任意消息产生民主群签名。

(3) 群签名生成

在群签名生成算法 Sign 中，某一群成员 $ID_k(1\le k\le n)$ 作为签名人代表群体 U 对消息 m 产生民主群签名，具体步骤如下。

1) 计算秘密分享

签名人 ID_k 以秘密分发者的身份执行一个公开可验证的秘密分享方案，实现对秘密值 h^s 得 (t,n) 秘密分发，具体如下：

1、在集合 Z_q 中选择随机数 s，w_i，$1\le i\le n$ 和一个 q 元域上常数项为 s 的 $(t-1)$ 次随机多项式 $p(x)=\sum_{j=0}^{t-1}\alpha_j x^j$，满足条件 $\alpha_0=s$，签名人 ID_k 计算并广播自己对该多项式的承诺，即 $\tau=g^{\alpha_0}$，$\tau_j=g^{\alpha_j}$，$1\le j\le t-1$，利用这些承诺值计算 $\chi_i=\prod_{j=0}^{t-1}\tau_j^{i^j}$，$i=1,2,\cdots,n$，式中 $\tau_0=\tau$；

2、为使群成员最终能够恢复出秘密值 h^s，该签名人计算多项式值 $p(i)$ 并用该值加密第 i 个成员的公钥，即计算并公布 $\eta_i=y_i^{p(i)}$，$1\le i\le n$；

3、利用所选择的随机数、所有群成员的公钥及公开参数计算 $a_{i1}=g^{w_i}$，$a_{i2}=y_i^{w_i}$，利用所选择的哈希函数计算哈希值 $e=H(\chi_1,\cdots,\chi_n,\eta_1,\cdots,\eta_n,a_{11},\cdots,a_{n1},a_{12},\cdots,a_{n2})$ 并由该哈希值和多项式值获得响应值 $r_i=w_i-p(i)e$，$1\le i\le n$；

4、作为秘密分享部分的输出，签名人置 $share=(\tau,\tau_1,\cdots,\tau_{t-1},\eta_1,\cdots,\eta_n,e,r_1,\cdots,r_n)$。

此处，签名人对不同的消息执行民主群签名操作时需要使用不同的随机数 s，以便在群体 U 中分发不同的秘密值 h^s，若分发相同的秘密值，将可能导致意想不到的潜在威胁。

任何人在收到 share 后都能够确信秘密分发是正确地产生了其输出结果，秘密分发者要想欺骗秘密接受者接受一个假秘密值在计算上是困难的。

2) 计算数字签名

签名者利用所分发的秘密和自己的私钥对消息 m 产生数字签名，具体如下：

1、计算 $\gamma = g^{x_k}$， $c = h^s y_k$；

2、选择随机数 $r_{k1}, r_{k2}, z_{i1}, z_{i2}, \rho_i = {}_R Z_q, i = 1,2,\cdots,n, i \neq k$，并计算 $l_{i1} = H(m, \tau, \frac{c}{y_i})$，$l_{i2} = H(m, \gamma, y_i)$， $u_{i1} = (g^{l_{i1}} h)^{z_{i1}} (\tau^{l_{i1}} \frac{c}{y_i})^{\rho_i}$， $u_{i2} = (h^{l_{i1}} g)^{z_{i2}} (y_i^{l_{i1}} \gamma)^{\rho_i}$， $i = 1,2,\cdots,n, i \neq k$；

3、选择 $l_{k1} = H(m, \tau, h^s)$， $l_{k2} = H(m, \gamma, y_k)$， $u_{k1} = (g^{l_{k1}} h)^{r_{k1}}$， $u_{k2} = (h^{l_{k2}} g)^{r_{k2}}$，$\rho_k = H(m, t, c, g, u_{11}, \cdots, u_{n1}, u_{12}, \cdots, u_{n2}) - \sum_{j \neq k} \rho_j$ ， $z_{k1} = r_{k1} - \rho_k s$， $z_{k2} = r_{k2} - \rho_k x_k$；

4、输出 $sign = (\gamma, c, \rho_1, \cdots, \rho_n, z_{11}, \cdots, z_{n1}, z_{12}, \cdots, z_{n2})$。

签名人在群体 U 中分发的秘密值 h^s 及其中的随机数 s 在签名过程中均被使用到，对不同的消息执行签名时使用的整数 s 应该是随机的，否则公开可验证秘密分享部分与签名人使用自己的私钥计算签名部分就是相互孤立开来的，这很容易带来潜在攻击。

签名人以自己的私钥和群体 U 中所有成员的公钥计算出签名部分 sig，这种方法使任意签名接受者获得签名 sig 后都能够确定是群体 U 产生了该签名，但是要想精确知晓群体 U 中那个成员产生了 sig 在计算上是不可行的。由于签名人在计算中使用了自己的私钥，而这个私钥只有他自己才知道，所以不知道该私钥的人无法产生这样的签名。

3) 输出民主群签名

将秘密分享部分和数字签名部分组成的一个二元组(share，sig)作为群成员 ID_k 代表群体 U 对消息 m 最终产生的民主群签名。

(4) 群签名验证

在群签名验证算法中，任何人均可以判定给定的民主群签名是否确实是由群体 U 中的某个成员代表整个群体 U 产生的，具体方法如下。

1) 验证秘密分享部分是否有效：计算 $\chi_i = \prod_{j=0}^{t-1} \tau_j^{i^j}$， $i = 1,2,\cdots,n$，式中 $\tau_0 = \tau$，进而重构 $a_{i1} = g^{r_i} \chi_i^e$，$a_{i2} = y_i^{r_i} \eta_i^e$，验证 $e = H(\chi_1, \cdots, \chi_n, \eta_1, \cdots, \eta_n, a_{11}, \cdots, a_{n1}, a_{12}, \cdots, a_{n2})$ 是否成立，如果不成立，则意味着原签名人对 h^s 的秘密分享不正确，从而拒绝该签

名，否则继续执行。

2) 验证数字签名部分是否有效：计算哈希值$l_{i1}=H(m,\tau,\frac{c}{y_i})$，$l_{i2}=H(m,\gamma,y_i)$，进而重构值$u_{i1}=(g^{l_{i1}}h)^{z_{i1}}(\tau^{l_{i1}}\frac{c}{y_i})^{\rho_i}$，$u_{i2}=(h^{l_{i2}}g)^{z_{i2}}\cdot(y_i^{l_{i2}}\gamma)^{\rho_i}$，$i=1,2,\cdots,n$，最后检查等式$\sum_{i=1}^{n}\rho_i=H(m,\tau,c,\gamma,u_{11},\cdots,u_{n1},u_{12},\cdots,u_{n2})$是否成立，如果不成立，则拒绝该签名；否则接受该民主群签名为有效。

由于只有群体 U 中的所有成员的公钥才能够使得第二步中最后要检查的等式成立，通过这样的计算，验证者能够确信签名来自群体 U。但是，由于这一验证过程中群体 U 中所有成员的地位都是对称的，所以，验证者并不能确切地知道群体 U 中的哪个成员产生了这个签名。这正是本方案能够提供签名者匿名性的原因。

(5) 追踪算法

签名人追踪算法使得在发生争端的情况下(如一个签名通过签名验证检验过程，但是群体 U 中的所有成员均否认自己产生了该签名)由群体 U 中不少于 t 个成员一起执行本操作，以自己的私钥为输入，揭晓产生该签名的签名人的真实身份，具体方法如下。

1) 验证民主群签名是否有效：t 个成员$\{ID_1,ID_2,\cdots,ID_t\}$以签名验证者的身份验证该签名是否有效，如果该签名无效，则意味着该签名不是群体 U 产生的，所以不需要由群体 U 执行任何追踪计算，否则继续下面步骤。

2) 重构秘密：群成员$ID_i(i=1,\cdots,t)$利用自己的私钥为输入计算并公布$\xi_i=\eta_i^{x_i^{-1}}$；参与运算的群成员根据这些节点广播的数据ξ_i执行拉格朗日插值运算，即计算$\lambda_i=\prod_{j=1,\cdots,t,j\neq i}\frac{j}{j-i},i=1,\cdots,t$，继而重构出由签名人分发的秘密值$\mu=\prod_{i=1}^{t}\xi_i^{\lambda_i}$。

3) 恢复签名人身份：利用重构的秘密之执行解密运算并恢复出签名人身份。所述的解密运算及利用恢复出的秘密值的逆元μ^{-1}与密文c做乘积运算$y=c\mu^{-1}$，在群体$U=\{ID_1,ID_2,\cdots,ID_n\}$中查找公钥等于 v 的群成员即为产生该签名的真正签名人。

4.3.2 方案安全性分析

判断一个群签名方案的必须满足可验证性、不可伪造性、可追踪性和匿名性。下面是从群签名的特性来对本文提出的群签名方案进行分析。

(1)可验证性

民主群签名的可验证性体现在两个方面，一个是秘密分享部分的可验证性，另一个是群签名的可验证性：

1)秘密分享部分

在群签名验证阶段，首先通过签名对(share，sig)计算出结果χ_i，然后重构得到a_{i1}和a_{i2}，通过这些值计算出$a_{i1}=g^{r_i}\chi_i^e$和$a_{i2}=y_i^{r_i}\eta_i^e$，与之前计算出的$a_{i1}=g^{w_i}$和$a_{i2}=y_i^{w_i}$进行对比，如果所得结果相同这证明秘密共享是正确的。

2)数字签名部分

在群验证阶段，首先计算l_{i1}和l_{i2}的值，进而重构出值u_{i1}和u_{i2}，最后检查出结果$\sum_{i=1}^{n}\rho_i=H(m,\tau,c,\gamma,u_{11},\cdots,u_{n1},u_{12},\cdots,u_{n2})$，则确定签名是正确的。

(2)不可伪造性

群加入算法和离开算法保证了用户在加入群之后才能得到群密钥，退出后得不到群新密钥，这也就保证了群体之外的人无法产生一个能够通过签名验证算法的数字签名。

(3)可追踪性

如果群体中的某个成员对一个消息产生了群签名，则他必定会被群体中任意一个其他成员通过签名追踪算法追踪出来。任何群成员，如ID_i，要对某消息产生一个群签名$\sigma=(share,sig)$，首先验证其有效性，无效则判定为非本群成员的签名，有效则对其进行秘密重构然后恢复出签名人身份。

(4)匿名性

给定一个民主群签名，该方案保证了不知道追踪陷门的任何验证者都无法确定出产生该签名的群成员的身份。

通过对以上几个性质的分析，本方案能够对信息进行数字签名，并达到较好的保密性。

对基于数字签名的微支付协议来说，理想的状态是达到下面六个标准：

(1)独立性：电子现金方案应包括银行的数字签名，并且该方案是独立的，跟任何网络或存储设备无关。

(2)安全性：电子现金方案应具备不可伪造性和不可重用性。不可伪造性保证了银行签名方案的安全性，即电子现金是不可伪造的。不可重用性能够控制和检测重复花费或重复报账。

(3)离线性：商家在清算阶段不需要在线与银行交互。

取款：客户在银行取走一定面值的电子货币，该客户账户就应相应地减去这一定面值的存款。

付款：客户向商店付款时需要提供付款信息，以便验证电子货币的面值和合法性。

拨款：商店把这些信息提供给银行以便验证，如果验证通过则将该电子货币

转到商店的账户上。

(4)匿名性：消费者在交易过程中的消费情况应具有不可跟踪性和不可联系性。不可跟踪即无论银行还是商店都不能跟踪用户的消费情况；不可联系即指在同一账户中提取的电子现金是不能联系的。通过数字签名技术实现其匿名性，使得电子现金中不包含面值及其他有效信息。

(5)可分性：一定面值的电子货币可以分成多次花费，但必须保证花费总额不大于电子货币的面值。

(6)可转移性：客户的电子货币可以转移给同一类型的其他客户使用。

基于这六个标准，我们将上面提出的民主群签名方案运用于电子支付微支付系统，下面是本文提出的一种基于数字签名的微支付协议。

4.4 基于数字签名的的微支付协议

相对于第三章中所提出的微支付协议方案，使用的是Hsah支付链的货币方式。本节将运用数字签名来构建电子货币，实现货币的完整性和健壮性，方案如下所示：

(1)系统初始化

银行B随即产生群G的生成元组$\{g,g_1,g_2\}$和私钥$x\in Z_q^*$。选择两个碰撞散列函数H，H_0，其中H用于产生银行签名和验证，H_0用于付款协议中口令的确定。银行公开$p,q,\{g,g_1,g_2\},H,H_0$和银行公钥$h=g^x \bmod p$，对私钥x保密。

银行对$(A,B)\in G^2$的数字签名$Sig(A,B)=(z,a,b,r)$，其中$g^r=h^{H(A,B,z,a,b)}a, A^r=z^{H(A,B,z,a,b)}b$。一元硬币是三重组$(A,B,Sig(A,B))$。

银行有用户账号数据库。每个商店有唯一标识符I_S，将I_S和交易日期/时间输入到H_0产生商店口令不同，相同商店的不同交易口令也不同。

(2)注册协议

银行B在用户C开账号时，首先验证用户C的身份。

C随即选择$u_1\in Z_q^*$，计算$I=g_1^{u_1} \bmod q$。如果$g_1^{u_1}g_2\neq 1 \bmod q$，则秘密保存$u_1$并将$ID_U$，$I$发送给银行B。

银行B判断ID_U的唯一性后将I存入数据库，I就是C的唯一账号。C账号的作用是在出现重复消费时，银行能唯一的识别C。银行计算对Ig_2的签名$z=(I\cdot g_2)^x \bmod q$发送给用户C。C保存u_1,z(其中z中嵌入了用户C的身份信息)，z的表示为(u_1x,x)。

(3)交易协议

用户 C 要从银行 B 取一单元货币时，银行 B 首先检查用户身份 ID_U，I 的合法性。然后银行 B 与用户 C 执行下面操作：

1)B 随即为用户 C 选择盲化因子 $w \in Z^q$，计算 $a = g^w \bmod q, b = (I \cdot g_2)^w \bmod q$ (在 b 中嵌入了用户 C 的身份信息)，将 a,b 发送给 C；

2)C 随机取 $s \in Z_q^*, x_1, x_2 \in Z_q$，计算 $A = (I \cdot g_2)^s, z' = z^s \bmod q, B = g_1^{x_1} g_2^{x_2} \bmod q$。C 再随机选择 $u, v \in Z_q$，计算 $a' = a^u g^v \bmod q$，$b' = b^{su} A^v \bmod q$，$c' = H(A, B, z', a', b')$，$c = (c'/u) \bmod q$。C 将口令 c 发送给银行 B；

3)B 计算 $r = (c \cdot x + w) \bmod q$ 发送给 C，并从 C 的账号上减掉一货币金额；

4)C 为了核实银行计算，证明银行知道私钥 x，需要验证 $g^r = a \cdot h^c \bmod q$ 且 $(I \cdot g_2)^r = b \cdot z^c \bmod q$。若验证成功，则计算 $r' = (r \cdot u + v) \bmod q$。这时 $Sig(A,B) = (z', a', b', r')$ 是 (A,B) 的一个数字签名。$(A, B, Sig(A,B))$ 就是一单位货币。

用户 C 与商家 M 协商好之后向 M 付款，操作如下：

1)C 将 $(A, B, Sig(A,B))$ 发送给 M；

2)如果 $A \neq 1$，则 M 计算口令 $d = H_0(A, B, I_M, date/time)$ 并将 d 发送给 C，其中 I_M 是商店的标识号，data/time 是这笔交易的日期和时间；

3)C 计算 $r_1 = (d \cdot u_1 \cdot s + x_1) \bmod q, r_2 = (d \cdot s + x_2) \bmod q$ 并发送给 M；

4)若 $Sig(A,B) = (z', a', b', r')$ 是合法签名，而且验证 C 知道 A,B 的表示，即 $g_1^{r_1} g_2^{r_2} = A^d B$，则 M 接收该货币。

(4)结算协议

商店定期将所有的支付记录 $(A, B, Sig(A,B)), r_1, r_2$ 及相应的时间日期发送给银行(如果 A=1，则银行不予受理)。银行 B 将商店 M 收到的货款拨入商店账号，操作如下：

1)银行由支付记录 $(A, B, Sig(A,B)), r_1, r_2$ 及相应的时间日期计算 $d = H_0(A, B, I_M, date/time)$；

2)验证 $g_1^{r_1} g_2^{r_2} = A^d B$，$Sig(A,B) = (z', a', b', r')$ 是对(A,B)的合法签名；

3)银行查询自己的数据库。若 A 没有相应项，则以商店的名义将 $(A, I_S, date/time, r_1, r_2)$ 存入数据库，银行接收商店的支付记录并在商店账号中加入一单位货币，否则进入分析阶段。若数据库中已经有完全相同的项，则肯定是商店企图重复入账；若数据库中有 $(A, date'/time', r_1', r_2')$ 而且 $g_1^{r_1'} g_2^{r_2'} = A^{d'} B$ (其中 $d' = H_0(A, B, I_S, date'/time')$)，则是用户 C 重复消费。这里两次口令 d, d' 不同，计算出 (d, r_1, r_2) 与 (d', r_1', r_2') 不同。银行将 $b = g_1^{r_1'} g_2^{r_2'} A^{-d'}$ 代入等式 $g_1^{r_1} g_2^{r_2} = A^d B$，得到 $g_1^{r_1 - r_1'} g_2^{r_2 - r_2'} = (I \cdot g_2)^{sd - sd'}$，又从交易协议中 r_2 的定义知 $s \cdot d - s \cdot d' = r_2 - r_2'$，从而 $g^{r_1 - r_1'} = I^{r_2 - r_2'}$。这时银行就能计算 $I = g_1^{(r_1 - r_1')/(r_2 - r_2')}$，再从数据库查找该账号的拥有者 ID_A 就是重复花费者。

当有重复消费情况出现时，该方案能够通过运算揭示重复花费者身份，以此对重复花费有威慑作用。

4.5 安全性分析

(1)匿名性分析：在用户 C 开户阶段，用户可以在银行得到一个唯一标识 $I = g_1^{u_1} \bmod q$ 用于后面交易阶段。取款时用户可以运用 I 计算得到 A 和 B，然后 A 和 B 进行签名得到货币 $(A, B, Sig(A, B))$，并在于商家进行交易时使用到，其中并不保护用户的身份信息 ID_U，从而保障了用户的匿名性。

(2)相互认证：通过 4.2 节的身份识别协议，参与双方可以安全的进行认证，保障各自权益。

4.6 公平性分析

(1)重复消费：在开户阶段，银行将用户的唯一标识 I 保存在数据库中，以保证在商家的清算阶段能够发现某一相同用户的 I 是否有重复消费现象。

(2)恶意透支：本方案在交易阶段分为了取款和付款两个阶段。如果某一用户需要与某一商家进行交易时，用户必须首先在银行处取款，得到所需要的电子货币单位 $(A, B, Sig(A, B))$，然后再与商家进行电子货币和商品的兑换，有效的防止了用户的恶意透支。

4.7 效率分析

系统建立初期，银行选择了具有高效性的两个碰撞散列函数 H 和 H_0，其中 H 用于银行的数字签名，后者用于交易阶段中的付款协议中口令的确定。用户的开户阶段也是只是进行了几次模运算 $I = g_1^{u_1} \bmod q$ 和 $z = (I \cdot g_2)^x \bmod q$，在不影响系统性能的情况下保证了系统的效率。在交易阶段，银行和用户分别进行了两次和五次模运算，尽量简化运算次数并保证结果的正确性。

通过以上安全性、公平性和效率的分析，确定本方案在性能上满足了系统的要求，具有较好的性能。

4.8 本章小结

本章研究了数字签名技术和身份识别技术，并阐述了其在微支付系统中的作用。提出了一种基于门限的民主群签名方案。在该签名方案中，每个用户具有相同级别的权限，各用户共享方案的群密钥，解决了普通数字签名方案中存在的权力过分集中问题。基于本章提出的门限民主群签名方案并结合 hash 链提出了一种基于新的微支付协议方案。分析表明，新协议能够保证用户的安全性，匿名性和身份认证性。另外，通过理论分析可以看出，新方案具有较高的效率，同时也可有效防止消费者的重复消费现象，能够保证交易过程中的公平性。

第五章 总结与展望

5.1 全文工作总结

全文工作是在国家自然科学基金项目《移动增值业务微支付系统中认证支付协议与签名技术的研究》(项目编号：61071116)的资助下完成的，本论文主要完成了以下几个方面的工作：

(1)对移动电子商务安全基础进行了深入的研究，包括移动电子商务的实现技术、安全技术以及几种移动电子商务框架，分析了移动电子商务所面临的安全威胁以及安全需求。

(2)对几种电子商务微支付协议进行了研究分析(Millicent、MicroMint 和 Payword)，指出了各自的优缺点。同时针对目前 Payword 协议所存在的安全性、匿名性以及公平性等问题，提出了一种新型电子商务微支付方案，并对该方案进行了全面的分析。该方案运用了双 Hash 支付链，并且能够让消费者同时与多个商家进行交易，在安全性上得到了满足，并且实现了交易的匿名性，保证了协议的公平性。

(3)对数字签名技术进行了分析研究，提出一中具有追踪功能的基于门限的民主群签名方案。该方案有效的实现了群体 U 中所有成员的公平性，在比如合资公司所要求的公平性能够得到很好地运用。针对这一特点，本文将数字签名技术运用于微支付系统当中，提高了系统的安全性。

5.2 展望

本文在基金项目的支持下做出了一些成果，但是在实际操作中还是存在一些问题：

(1)对本文提出的基于双 Hash 支付对的微支付改进协议中，虽然在安全性、公平性等性能上得到了很大的提高，但同时对于系统的运算能力提出了相当的要求。如何在实际操作中实现性能的满足和运算能力的保证将是下一步工作的重点。

(2)微支付系统要求的是高效快速的实现交易，Hash 链的运用使得这一要求得到了满足。但是如果单纯的使用 Hash 链并不能满足系统的其他一系列的要求，所以在此基础上对系统进行改进，并加入数字签名技术。虽然在安全性、公平性和高效性上达到了要求，但数字签名的计算还是比较复杂的，所以如何使微支付系统在高效性和安全性之间达到一个平衡将是下一步工作的又一个重点。

致谢

时光飞逝，三年研究生生涯即将结束。回想三年来经过的点点滴滴，其中有欢笑有失落，有成长有收获。研究生三年的学习和生活，将会是我一生中最美好的回忆。

首先，我最需要感谢的是我研究生导师李方伟教授。在研究生三年的科研工作中，李老师提供给我一个非常好的平台，并拥有机会参与到科研项目当中，是李老师让我不断进步。在学习生活中，李老师时时刻刻都在教育我们如何成为一名合格的研究人员，并传授我们很多做人做事的道理，这将是我们终身的财富。在此，我想对李老师说一声：谢谢您。

我要感谢团队老师陈善学老师和朱江老师对我学习生活中的帮助。还有就是在我刚进入课题组时曾经给予过帮助的师兄师姐，在此，感谢他们在学术上对我的指导和建议。还要感谢刘涛、龙吟、宋捷、李映虎、沈爱国和孟令文几位同学以及11、12级的师弟师妹，是他们让我的研究生生活更精彩。并祝愿他们在以后的工作生活当中身体健康，工作顺利。

感谢我的父母，是你们给我提供的物质和精神条件，让我能在学习生涯中不断进取，谢谢你们。

最后，对所有参加论文评审和对本文提出宝贵意见的各位专家、教授、老师表示感谢，请接受我最诚挚的谢意。

参考文献

[1] 吴志平.ERP 与电子商务的相关性研究[D].湘潭:湘潭大学,2004.

[2] Rivest R L. Electronic lottery tickets as micropayments[C]//Financial Cryptography. Springer Berlin Heidelberg, 1997: 307-314.

[3] Geer D. E-micropayments sweat the small stuff [J]. Computer, 2004, 37(8): 19-22.

[4] Adachi N, Aoki S, Komano Y, et al. The security problems of Rivest and Shamir's PayWord scheme[C]//E-Commerce, 2003. CEC 2003. IEEE International Conference on. IEEE, 2003: 20-23.

[5] Kienreich W, Tochtermann K, Oswald E. Micropayment in the context of distributed digital libraries [J]. WSEAS Transactions on Information Science and Applications, 2005, 2(7): 934-944.

[6] Mallat N, Rossi M, Tuunainen V K. Mobile banking services [J]. Communications of the ACM, 2004, 47(5): 42-46.

[7] Day Greg. Mobile Commerce- An Emerging Opportunity [J]. Telecommunication Journal of Australia, March 2005, 5(3):5-14.

[8] Rivest R L, Shamir A. PayWord and MicroMint: Two simple micropayment schemes[C]//Security Protocols. Springer Berlin Heidelberg, 1997: 69-87.

[9] Burstein J. An implementation of MicroMint [D]. Massachusetts Institute of Technology, 1998.

[10]Herzberg A, Yochai H. MiniPay: charging per click on the Web [J]. Computer Networks and ISDN Systems, 1997, 29(8): 939-951.

[11]罗少贤.对移动通信网中的安全问题的探讨[J].中山大学研究生学刊(自然科学,医学版), 2004, 3: 009.

[12]Koblitz N. A course in number theory and cryptography [M]. Springer, 1994.

[13]Menezes A J, Van Oorschot P C, Vanstone S A. Handbook of applied cryptography[M]. CRC press, 2010.

[14]Schneier B,吴世忠.应用密码学——协议,算法与 C 源程序[J].机械工业出版社,北京, 2000.

[15]王育民,电信技术,刘建伟,等.通信网的安全: 理论与技术[M]. 西安电子科技大学出版社, 1999.

[16]冯登国, 裴定一.密码学导引(第一版)[M].北京:科学出版社,1999.

[17]卢开澄. 计算机密码学: 计算机网络中的数据保密与安全[M]. 清华大学出版

社, 2003..

[18]王大飞.移动电子商务安全研究[J]. 2011.

[19]徐国爱,李中献,詹榜华,等.电子商务安全体系结构[J]. 通信保密, 2000, 22(4).

[20]Garey M. andD. Johnson (1979): Computers and Intractability–A Guide to the Theory of Incompleteness [J]. San Francisco, New York: Freeman Company, 1979.

[21]Goldreich O, Micali S, Wigderson A. How to prove all NP statements in zero-knowledge and a methodology of cryptographic protocol design[C]//Advances in Cryptology—CRYPTO'86. Springer Berlin Heidelberg, 1987: 171-185.

[22]Odlyzko A M. Discrete logarithms and smooth polynomials [J]. Contemporary Mathematics, 1994, 168: 269-269.

[23]Gill J. Computational complexity of probabilistic Turing machines [J]. SIAM Journal on Computing, 1977, 6(4): 675-695.

[24]Pomerance C, Goldwasser S. Cryptology and Computational Number Theory: Lecture Notes [M]. American Mathematical Soc., 1990, 42(3): 49-74.

[25]Donald E K. The art of computer programming [J]. Sorting and searching, 1999, 3: 426-458.

[26]Pohlig S, Hellman M. An improved algorithm for computing logarithms over information theory, IEEE Transactions on, 1978, 24(1): 106-110.

[27]Pollard J M. Pollard J M. Monte Carlo methods for index computation [J]. Mathematics of computation, 1978, 32(143): 918-924.

[28]Adleman L. A subexponential algorithm for the discrete logarithm problem with applications to cryptography[C]//Foundations of Computer Science, 20th Annual Symposium on. IEEE, 1979: 55-60.

[29]Brands S. Brands S A. An efficient off-line electronic cash system based on the representation problem [J]. Sorting and searching, 1993, 24-67.

[30]Jakobsson M, Yung M. Distributed magic ink signatures[C]//Proceedings of the 16th annual international conference on Theory and application of cryptographic techniques. Springer-Verlag, 1997: 450-464.

[31]DeSantis A. Advances in Cryptology-EUROCRYPT'94: Workshop on the Theory and Application of Cryptographic Techniques, Perugia, Italy, May 9-12, 1994. Proceedings [M]. Springer Verlag, 1995: 257-265.

[32]Odlyzko A M. The future of integer factorization [J]. CryptoBytes (The technical newsletter of RSA Laboratories), 1995, 1(2): 5-12.

[33]Lenstra A K, Lenstra Jr H W, Manasse M S, et al. The number field sieve[M]//The

development of the number field sieve. Springer Berlin Heidelberg, 1993: 11-42.

[34]Lenstra A K, Lenstra H W, Manasse M S, et al. The factorization of the ninth Fermat number [J]. Mathematics of Computation, 1993, 61(203): 319-349.

[35]Pomerance C. The quadratic sieve factoring algorithm[C]//Advances in cryptology. Springer Berlin Heidelberg, 1985: 169-182.

[36]Pomerance C, Smith J W and Tuler R. Pipe-line Architecture for Factoring Large Integers with the Quadratic Sieve Algorithm. SIAM Journal on Computing, April 1988, 17(2): 387-403.

[37]Siverman R D. The Multiple Polynomial Quadratic Sieves. Mathematics of Computation, January 1987, 48(177): 329-339.

[38]Odlyzko A M. Discrete logarithms in finite fields and their cryptographic significance[C]//Advances in cryptology. Springer Berlin Heidelberg, 1985: 224-314.

[39]Montgomery P L. Speeding the Pollard and elliptic curve methods of factorization [J]. Mathematics of computation, 1987, 48(177): 243-264.

[40]Donald E K. The art of computer programming [J]. Sorting and searching, 1999, 3: 426-458.

[41]Morrison M A, Brillhart J. A method of factoring and the factorization of F7 [J]. Mathematics of Computation, 1975, 29(129): 183-205.

[42]Poet R. The Design of Special Purpose Hardware to Factor Large Integers [J]. Computer Physics Communications, 1985, 37(2): 337-341.

[43]Whitfield Diffle and Martin E Hellman. New Directions in Cryptography[C]// Transactions on Information Theory, IEEE November 1976:644-654.

[44]Rivest R L, Shamir A, Adleman L. A method for obtaining digital signatures and public-key cryptosystems [J]. Communications of the ACM, 1978, 21(2): 120-126.

[45]Diffie W, Hellman M E. Multiuser cryptographic techniques[C]//Proceedings of the June 7-10, 1976, national computer conference and exposition. ACM, 1976: 109-112.

[46]Diffie W, Hellman M. New directions in cryptography [J]. Information Theory, IEEE Transactions on, 1976, 22(6): 644-654.

[47]Merkle R C. Protocols for public key cryptosystems[C]//IEEE Symposium on Security and privacy. 1980, 1109: 122-134.

[48]ElGamal T. A public key cryptosystem and a signature scheme based on discrete logarithms[C]//Advances in Cryptology. Springer Berlin Heidelberg, 1985: 10-18.

[49]郑东, 李祥学, 黄征. 密码学——密码算法与协议[J]. 2009.

[50]Glassman S. The Millicent protocol for inexpensive electronic commerce [J]. http://www. research. digital. com/SRC/millicent, 1995..

[51]Rivest R L, Shamir A. PayWord and MicroMint: Two simple micropayment schemes[C]//Security Protocols. Springer Berlin Heidelberg, 1997: 69-87.

[52]姬东耀, 王育民. 移动计算网络环境中的认证与小额支付协议[J]. 电子学报, 2002, 30(4): 495-498.

[53]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.

[54]李明柱, 李志江, 杨义先. 移动通信增值服务认证和支付研究[J]. 通信学报, 2003, 24(4): 123-127.

[55]李凌春. PayWord 微支付系统的安全性分析及其改进研究[J]. 大众科技, 2008 (11):23-24.

[56]王志恒, 谷大武, 白英彩. 种新型小额电子支付协议的研究与设计[J]. 计算机工程 与应用, 2001 (17):51-53.

[57]曹华, 金瓯, 贺建飚. 基于双哈希链的公平移动支付协议的设计和分析[J]. 计算机测量与控制, 2007, 15(1): 117-119.

[58]郎为民. 微支付协议研究[D]. 武汉: 华中科技大学, 2005:15-21.

[59]孟健, 杨阳. 基于 PayWord 的自更新 Hash 链微支付协议[J]. 计算机工程, 2009 (35):63-6 5.

[60]李方伟, 孙逊. 移动电子商务微支付协议的改进[J]. 重庆邮电大学学报(自然科学版), 2009 (6):815-818.

[61]卿丽研. 基于 Pay Word 的微支付系统 NPAY 设计与研究[J]. 商场现代化,2008(1):34-35.

[62]谭运猛, 付雄, 朗为民. 基于多 Pay Word 链的新型高效微支付方案[J]. 华中科技大学学报, 2004.32(5):29-31.

附录

攻读硕士学位期间参加的科研项目

(1)移动增值业务微支付系统中认证支付协议与签名技术的研究（61071116）国家自然科学基金

(2)移动通信系统认证协议和密钥算法研究（2007BB2388） 重庆市自然科学基金

攻读硕士学位期间发表的主要论文

[1]卢霖,李方伟.基于双 Hash 链的 Payword 改进协议安全性研究[J].电子技术应用，2013.6

[2]Lin Lu, Fangwei Li. Micro-payment Mechanism and Improved Analysis Based on Pay Word[C]. FSKD 2012.2715-2718.

[3]李映虎,李方伟,卢霖.具有易追踪性的无可信中心门限签名方案[J].电子技术应用,2012,38(10): 146-149.