P2P电子支付理论与技术

P2P Electronic Payment—Theory and Technology

刘义春 著

電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

P2P 电子支付理论与技术

刘义春 著

電子工業出版社
Publishing House of Electronics Industry
北京 • BEIJING

内 容 简 介

本书描述了电子商务研究和应用中相关的密码学理论和信息安全技术，介绍了国内外电子现金技术的一些代表性研究成果，针对 P2P 交易环境提出了一类新的离线电子现金系统，先后针对 P2P 交易环境下简单交易模式、代理销售模式和多方分层支付模式等几种典型的 P2P 交易类型提出了相应的公平交易协议，并就存在 P2P 信任评估体系的情形分别针对几种交易模型给出了相应的基于信任的电子支付协议，此外还利用 Kailar 逻辑和串空间逻辑对所提出的几种支付协议分别进行了形式化分析。

本书可作为电子商务、信息安全等专业研究生和高年级本科生的教学参考书，也可作为现代密码学、电子商务、信息安全、计算机应用等领域研究人员和技术人员的参考资料。

图书在版编目（CIP）数据

P2P 电子支付理论与技术/刘义春著. —北京：电子工业出版社，2008.8
ISBN 978-7-121-06554-5

Ⅰ. P… Ⅱ. 刘… Ⅲ. 电子商务—支付方式 Ⅳ. F713.36

中国版本图书馆 CIP 数据核字（2008）第 057930 号

责任编辑：高买花　　特约编辑：陈宁辉
印　　刷：北京智力达印刷有限公司
装　　订：北京中新伟业印刷有限公司
出版发行：电子工业出版社
　　北京市海淀区万寿路 173 信箱　邮编　100036
开　　本：720×1000　1/16　印张：15.5　字数：312 千字
印　　次：2008 年 8 月第 1 次印刷
印　　数：3 000 册　定价：38.00 元

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：（010）88254888。

质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

服务热线：（010）88258888。

序　言

近年来，随着网络技术日益发展，新一代网络技术进入研究和应用领域，电子商务交易和网络支付成为商业活动的重要组成部分。P2P 网络作为一种新兴的分布式计算模式和交易环境，近几年来已成为人们广泛关注的热点。以往的电子商务研究一般集中在 C/S 模式，即客户通过支付数字现金或支票从商家购买商品或服务，商家提供商品或服务并获取支付。而在 P2P 支付模式中，每一成员既可以是客户，向其他成员支付数字现金等以购买商品或服务，又可以是商家，向其他成员提供商品或服务而获取支付。在 P2P 交易环境中，P2P 成员可能利用从其他成员处获得的数字现金或货币向另外一些商品或服务提供者进行支付，因此 P2P 支付工具必须是可流通的，即可在各交易者之间进行转移而无须银行介入。已有的电子支付系统大多面向简单交易情形，交易中只有单一的买方和单一的卖方。而在 P2P 交易情形中，普遍的情形是 P2P 成员从商品版权所有商或中间经纪商处获得商品或数字内容后再将其转卖给其他成员，从而获得中间人佣金。因此，在 P2P 支付系统中，除了对卖方的支付外，还应考虑对数字商品版权所有商甚至其他中间经纪商的支付。和一般的网络交易环境一样，P2P 系统成员可以利用 CA 认证机制认证其他 P2P 成员的身份，此外 P2P 成员还可利用 P2P 系统的信任机制，通过计算其他交易方的信任度来决定是否与其进行交易、以何种策略与其进行交易。

以往众多电子支付方案皆面向集中式 C/S 环境设计，支付仅在直接接触的买卖两方中进行，且采用的数字现金等支付工具为不可流通的、即收即兑的，显然不能很好地满足 P2P 支付环境的需要。因此，有必要根据 P2P 支付模式的特点，对 P2P 环境支付问题进行研究，并提出相应的支付体系和解决方案。

本书在国内外现有研究成果的基础上，针对 P2P 支付模式的特点，从设计和分析两方面对 P2P 电子支付系统进行了研究。

本书第 1 章介绍了 P2P 网络的概念，描述了电子商务和电子支付系统的研

究现状。第 2 章介绍了电子商务研究和应用中相关的密码学理论和信息安全技术。第 3 章介绍了国内外电子现金技术的一些代表性研究成果，针对 P2P 交易环境提出了一类新的离线电子现金系统。第 4 章结合 P2P 交易环境特点，针对客户、商家两方交易情形，提出适用于一般 P2P 交易模式的公平支付协议，并利用 Kailar 逻辑和串空间逻辑对支付协议进行了形式化分析。第 5 章针对客户、代销商、商品版权所有商三方交易情形，提出适用于一般 P2P 交易模式的公平支付协议，利用 Kailar 逻辑和串空间逻辑对支付协议进行了形式化分析。第 6 章提出一种解决复杂交易情形的新模型——P2P 多方分层交易模型，给出了适用于 P2P 多方分层交易模型的公平支付协议，并利用 Kailar 逻辑和串空间逻辑对支付协议进行了形式化分析。

在本书付梓之际，特别感谢我的导师——中国密码学会理事、武汉大学张焕国教授，书中的研究成果正是在他的指导和帮助下完成的。本书编写工作中，广东省电子商务重点实验室的领导和同仁给予了大力支持，在此一并致以感谢。

本书的相关研究得到浙江省自然科学基金（No.Y106802）、广东省科技计划项目（No.2007B010200035）、浙江省教育厅科研项目（NO.20060239）的资助。

由于作者水平有限，书中难免存在疏漏和不妥之处，敬请读者批评指正。

作　者

2008 年 3 月

目　录

第1章

绪　论


研究背景


电子现金系统的研究


电子支付协议的研究


P2P 电子支付的研究


小结

1.1 研究背景

当今世界网络、通信和信息技术快速发展和日益融合，Internet 在全球迅速普及，促使电子商务蓬勃发展。所谓电子商务，是指商务活动的电子化实现，即通过电子化手段来实现传统的商务活动，如网上购物、网上订票、网上交费等。电子商务可降低商家的运营成本，提高其利润率；可以扩大商品销路，沟通企业与企业之间的联系渠道，为客户提供不间断的产品信息查询和定单处理等服务。

随着电子商务时代的到来，作为电子商务重要组成部分的支付问题就显得越来越突出了。电子商务的巨大潜力，为多种类型的电子支付方式提供了市场需求。Internet 将全世界的付款者和收款者联系在一起，他们可能来自不同的国家、不同的商业机构或社会组织，并且习惯于不同的支付方式。消费者选用何种支付工具进行支付、买卖双方按照什么工作流程进行支付是电子商务的核心工程。安全的电子支付是实现电子商务的关键环节。事实上，缺乏有效的电子支付的电子商务活动将是十分有限的，而不安全的电子支付是不能真正实现电子商务的。

电子商务支付系统是电子商务系统的重要组成部分，它指消费者、商家和金融机构之间使用安全电子手段交换商品或服务，即利用新型支付手段（包括电子现金、信用卡、智能卡等）把支付信息通过网络安全地传送到商家、银行或相应的处理机构，来实现电子支付，并获得定购的商品或应有的服务。

在传统的 C/S 网络模式中，服务器是网络的核心，所有事务都离不开服务器提供的服务。某一客户可离线或退出网络系统，但服务器必须在线提供服务。在 P2P 模式中，每一个成员既是客户方，又是服务器方；既从其他成员处获取资源，又向其他成员提供服务。在纯 P2P 网络中，每一成员退出系统都不影响整个系统的正常运转。P2P 网络排除了中央服务器成为网络服务瓶颈的可能性，与传统的 C/S 模式相比，显得更加廉价高效、安全可靠和具有更好的可扩展性。

目前的电子商务研究一般集中在 C/S 商务交易模式。客户用从银行获取的电子现金或支票，支付给商家用以购买商品；商家收到支付后将商品发给客户，随即到银行兑现所获支付。而在 P2P 支付模式中，每一成员既是客户，从其他成员处购买商品，又是商家，向其他成员提供内容服务。通常的 P2P 交易为网络上数字内容的交易，具有单次交易金额小、交易频繁的特点。

电子商务支付的关键问题是电子支付活动中的安全问题。常见的安全问题主要有：

- 以非法手段窃取信息，或对通信数据进行译码分析，使机密数据泄露给未经授权者；
- 篡改或删除通信信息中的数据以破坏支付信息的完整性；
- 由于系统故障、网络故障等造成电子商务交易过程中出现的通信中断或数据丢失，破坏支付过程的正常进行；
- 伪造身份参与交易以对支付协议进行攻击；
- 协议参与者利用过时的失效信息对协议进行攻击；
- 协议参与者利用协议漏洞让自己处于优势，而使其他参与方蒙受损失；
- 协议参与方对交易行为进行抵赖，否认交易结果。

为抵抗来自各方面的攻击和欺诈，必须确保电子支付系统的安全性、健壮性和完善性，主要措施包括：

- 保护机要数据不被非授权者泄露或窃取（数据机密性）；
- 保护机要数据不被篡改、删除（数据完整性）；
- 保护协议参与者身份、机要数据的可鉴别性及不可伪造性（数据真实性）；
- 使协议中一些特定信息仅在一定时间内有效，而不被日后用于攻击协议（时效性）；
- 协议参与方不能否认已发送或已接收的数据（不可否认性）；
- 保护诚实的协议参与方在协议执行的任何阶段都不让其他方处于劣势（公平性）；

● 保护系统和网络的稳定性和可靠性，以及系统的可恢复性。

在电子商务交易中，交易参与方除了关心自己的银行账户、口令、私钥、交易数据等机要信息不被泄露、窃获、删除、篡改外，最关心的问题是交易是否公平，其他交易方是否利用交易系统漏洞使自己占优势，或对交易环节进行抵赖，否认交易结果。一个完善的电子商务支付系统应满足安全性和公平性，能够防止一些常见的欺诈和攻击，且具有较高的交易效益。

电子商务交易实际上是指：客户使用某种电子支付工具，从商家购买所需商品，双方交易过程按具体的交易协议进行。电子支付系统的研究主要体现在两方面：电子现金等支付工具的研究、电子商务交易协议的研究。

1.2 电子现金系统的研究

1.2.1 电子现金的概念

货币是从商品世界中分离出来的，固定地充当一般等价物的特殊商品。随着社会的信息化、电子化以及贸易全球化，要求货币必须能通过网络进行流通，而传统的货币已显然不能适应这种要求。

电子货币是一种新的支付方式，是以电子化数字形式存在的货币，用户可以像使用纸币一样使用电子现金在网络上进行日常买卖。电子货币比现有的实际货币具有更多的优点：无须承担较大的存储风险、高昂传输费用、较大的安全保卫和防伪的投资。电子货币是在传统货币基础上发展起来的，与传统货币在本质、职能及作用等方面存在着许多共同之处。

当前广义的电子货币主要有三类：电子信用卡、电子支票和电子现金。电子信用卡不支持离线支付，在每次支付过程中必须实现客户、商家、银行和发卡机构的在线多方认证和数据的相互传送，这对小额支付来说代价太大；电子支票支持离线支付，既适合于小额支付，也适合于大额支付，但不能防止用户的拒绝支付和透支行为；电子现金则能较好地解决上述问题，既能用于大额支付，也能用于小额支付，而且还有保护用户支付行为

隐蔽性，防止拒绝支付和透支行为等诸多优点，因而更受商家和用户的青睐。

一个理想的电子现金机制，必须满足以下 6 个特性：

（1）独立性（Independence）：电子现金与任何网络、操作平台和物理存储无关，且能通过网络进行交易。

作为一种流通手段和支付工具，电子现金的用户具有多样性。因此，电子现金不能局限于特定的计算机系统、特定的网络体系和特定的存储介质，而必须能在 Internet 多种平台的用户间流通。

（2）安全性（Security）：能防止电子现金的复制、伪造和重复使用。

传统货币的安全性是由货币的物理难伪造性来保证的，由于纸币采用特殊的纸张和特殊的制造手段，使得货币的伪造困难很大且易于辨别。由于电子现金极易复制，其安全性无法依赖于任何物理条件，而只能从数学上来保证，所以必须采取一定的密码学技术来保证电子货币的安全性。

（3）匿名性即不可追踪性，也就是说电子现金的用户和他的购买行为无法被跟踪。

电子现金应该保证用户的身份匿名性和不可追踪性，即保证买卖双方的自由不受到干涉。银行不能追踪顾客的开支情况，不能知道顾客把现金给了谁，购买了什么东西。目前解决这个问题的核心技术是盲签名。

（4）离线支付（Off-line Payment）：当一个用户在使用电子现金时，用户和商店的交易过程是以离线方式进行的，并没有银行在线参加。

在线电子货币要求进行每次支付时都要有银行参加，能防止重复花费和超额消费，但通信代价高，且会导致银行因频繁参与交易而成为交易瓶颈，降低交易效率。使用离线电子货币时银行无须卷入支付过程，交易效率较高，通信成本低，但需解决重复花费问题。

（5）可迁移性（Transferability）：电子现金可以在用户之间任意转让、流通。

如同传统的货币一样，电子现金应该能在银行兑付之前在多个用户之间迁移、流通，流通期间银行不应知道现金开支情况。

（6）可分性（Divisibility）：要能够处理各种不同货币单位和货币种类

的交易，允许进行等值交换，以大换小或以小换大。

一般来说，一个实用的电子现金系统应该根据需要满足上述几个性质中的部分性质。

1.2.2 电子现金技术研究现状

1982 年 David Chaum 等利用 RSA 盲签名算法构造了最早的电子现金方案[1]。该方案通过对包含用户信息的签名内容进行盲化处理，使签名银行签名时无法解读被签内容中用户信息，确保电子现金的用户和他的购买行为无法被跟踪，从而首次解决了电子现金的匿名性。该方案被用于建立最早也是最著名的商业化电子现金系统 DigiCash。David Chaum 又于 1990 年改进该方案后重新设计了离线匿名的电子现金系统[2]，在提款和支付电子现金时采用分割选择技术以确保所提交签名的电子现金的正确性，防止现金提取中出现欺诈行为，然后利用 RSA 盲签名技术对所提交货币进行盲签名。

1991 年 T. Okamoto 提出了一个基于 RSA 盲签名的可分电子现金系统[3, 4]。该方案基于 RSA、Hash 函数和多次盲签名，将每次提取现金时都进行用户身份信息的隐匿改为在账户建立时进行隐匿，提高了系统效率，降低了用户被跟踪的可能性。同时用户可将现金分成任意金额进行支付，直至将现金金额支付完毕。这是第一个可分的电子现金系统。

以后 S. Brand 和 M. Frankelin 先后利用 Schnorr 签名和素数阶群的计算，分别提出了基于离散对数在线和脱机的电子现金方案[5, 6, 7]，其安全性基于 Schnorr 签名和素数阶群上的表示问题。该类方案皆具有较高的计算效率，且银行无须在线参与交易，因此消除了银行成为交易瓶颈的可能性。S. Brand 的电子现金方案已成为一个经典的电子现金方案，现在大多数电子现金系统都来源于 S. Brand 方案的改进。

Markus Stadler 等利用不经意传输技术，实现对信息的盲签名，必要时可通过一个外部仲裁者撤销签名的匿名性[8]。Van Bjerre Damgard [9]利用一种可验证安全性的签名技术[10]，通过对签名的变换执行一个双方计

算协议[11]，来实现一种盲签名技术。Birgit Pfitzmann 和 Michael Waidner 分析了 Damgard 的盲签名方案，指出 Damgard 系统实际上不是不可追踪的，并给出了破解 Damgard 系统的途径和增强现金系统安全性的一般方法[12]。

Yi Mu 等利用 Nyberg-Rueppel 的可恢复消息的签名技术，提出了一个公平的电子现金方案[13]，在提取现金时使用一个可信机构的公钥，使可信机构必要时能使用其私钥撤销现金的匿名性。韩国的 Hyung-Woo Lee 和 Tai-Yun Kim 结合不经意传输技术和 Nyberg-Rueppel 的可恢复消息的签名，提出了一种可撤销匿名性的电子现金方案[14]。Hua Wang 等通过对交易各方赋予不同的角色，授予不同的权限，利用基于角色的访问控制技术建立一个不可追踪的电子现金支付方案[15]。Zhong 利用零知识证明方法设计了一个可撤销匿名性的单项可分电子现金系统 ZCash[16]，Shingo Miyazaki 提出基于离散对数问题的部分签名方案的匿名的电子现金方案[17]，但该系统不能防止对电子现金的重复花费，当然是不切实际的。Moses Liskov 针对电子支付的分期偿付问题，在 Okamoto 的可分电子现金体系基础上提出一个分期偿付的电子现金方案[18]。Tomas Sander 等利用 Hash 树和 Hash 链技术，基于银行数据库管理体系提出了一个不依赖于公钥签名体系的可查证的匿名电子现金系统[19]。Greg Maitland 和 Colin Boyd 利用群签名技术实现电子现金的不可追踪性，提出了一个基于群签名技术的匿名电子现金系统[20]。

在 1995 年由 Digital 公司开发的 Millicent 微支付系统[21]，利用一个密钥控制的单向散列函数来认证和验证支付票据，一个票据代表了商家给顾客建立的一个账号，在任何给定的有效期内，顾客都可以利用该票据购买商家的服务。在 Millicent 中，没有使用公钥技术，而采用效率更高的 Hash 函数，部分采用了对称加密算法。单向 Hash 函数中使用的密钥只有凭据发行者和要验证并最终接收此凭据的商家才知道，所以，可以有效防止票据的伪造。

R. L.Rivest 和 A. Shamir 在 Hash 函数冲突原理基础之上提出一种离线微支付系统 MicroMint[22]。单向 Hash 函数 H 把 x 映射到另一具有固定长度的 y=H(x)值。当两个不同的值 x_1 和 x_2 都被 H 映射到同一个值 y 时，即

$H(x_1)=H(x_2)=y$，则出现了 Hash 函数 H 的一个双向冲突。一般情况下，当 k 个不同输入值 x_1，x_2，…，x_k 都被 H 映射到同一个值 y 时，即 $H(x_1)=H(x_2)=\cdots=H(x_k)=y$，则会出现一个 k 向 Hash 函数。一个 MicroMint 货币由一个四向 Hash 函数冲突来代表，即由 4 个具有相同 Hash 值的输入值 x_1，x_2，x_3，x_4 组成 $C=\{x_1, x_2, x_3, x_4\}$，它代表一定数量的小额单元钱，如一分等。MicroMint 没有采用公钥和对称加密技术，但由于采用了四向 Hash 函数冲突，大规模的欺骗在计算上是不可行的。

Ronald L. Rivest 和 Adi Shamir 还提出了另一种微支付体制 PayWord[22]。与 MicroMint 不同，它基于 Hash 链技术，是一种典型的基于信用的离线微支付机制。同典型的 Hash 链支付机制相同，用户 C 在银行 B 处建立完账户以后，由 B 给 C 发一个 PayWord 证书。利用 PayWord 证书，B 授权 C 制造 PayWord 链，以作为支付凭证提交给商家 M，M 可在以后通过 B 进行兑换。在第一次支付请求时，C 计算并签署对某一特定 PayWord 链的承诺，即对包含 PayWord 根和其他附加信息的签名。C 随机提取某一个 PayWord ω_n，并在此基础上以相反的顺序创建 PayWord Hash 链$\{\omega_i\}$，其中$\omega_i=h(\omega_{i+1})$。ω_0 不是用于支付的 PayWord 本身，而是该链的根。C 把承诺、ω_0 和第 i 个支付对(i, ω_i)一同发送给 M，M 对承诺中签名进行验证，然后利用ω_0 和承诺来验证支付对。

联机电子现金方案能及时避免用户重复花费电子现金，但代价是系统负担大大增加，银行可能成为瓶颈。脱机电子现金系统不能及时检测用户的重复花费，需滞后一定时间才能发现货币的重复花费，从而可能造成商家和银行的损失。为平衡上述两种情形，1997 年 Jarechi 等介于在线支付和离线支付之间，提出概率投票（Probabilistic Polling ）技术[23]，商家根据一个概率值来判断是否要同银行进行交互，以验证客户是否有足够的能力来进行支付，以减少不诚实用户重复花费所带来的损失。

微电子彩票是一种基于概率的微支付机制[24]，彩票的面值一般较小，不需要银行处理每一次的微支付货币，只需处理中奖的彩票即可，可以提供更高的匿名性和私有性，使银行端的处理效率极大提高。在微支付过程中（以信息浏览为例），彩票购买者 C 首先从彩票发行者 B 处购买微彩票

（也可以经授权自己产生微彩票），然后浏览收费网页，此时将用彩票向彩票接收者 M 支付，M 根据中奖号指示器和票号来判断所接收的彩票是否中奖。如果判断中奖，M 则在线（或一定时期离线）把中奖的彩票提交给银行（即支付者，可以为其他第三方）进行兑现。由于只把中奖的彩票提交给银行进行兑现，所以，对银行而言，微电子彩票支付具有很高的效率。由于概率的原因，微电子彩票支付方法可以为用户提供更高的匿名性和私有性，适合用户对某些特定商家的固定或重复性消费，对频繁更换商家的支付中，要求彩票接收商承担一定的风险。

除 DigiCash 外，著名的商业化电子现金系统还有 CyberCash 公司的 CyberCash 系统[25]、南加州大学提出的 NetCash 系统[26]、First Virtual 公司的 First Virtual 系统[27]、卡内基梅隆大学的 NetBill 系统[28]及 IBM 的 iKP 系统[29, 30]。

国内对电子现金的研究也成绩斐然。杨波、王育民使用基于概率的分割选择技术提出了一种新的电子货币系统[31]；陈恺、肖国镇通过概率验证，决定匿名可分电子现金在支付时采用联机还是脱机验证，提出一种基于概率验证的可分电子现金系统[32]；钟鸣、杨义先提出一种基于盲签名和任意零知识证明的电子现金方案[33]；祁明等通过加入概率检验算法改进 Brands 数字现金方案[34]；陈恺、胡予濮等通过引入可信方提出一种可撤销匿名性的可分电子现金系统[35]；张方国、王育民等利用群签名算法和群盲签名算法提出一种可跟踪用户的多银行电子现金系统[36]；王常吉、裴定一通过嵌入有由银行规定的电子现金的有效期，改进了 Brands 的基于限制性盲签名的电子现金系统[37]；王常吉、裴定一还通过改进 Brands 系统，提出了一个利用防窜扰的 Smart 卡的公正、离线的电子现金系统[38]；陈晓峰、王育民等利用指纹的技术和离线可信第三方，给出了一种脱线的匿名可控制电子现金方案[39]；高虎明、王育民通过在现金支付时增加 ElGamal 签名，对 eCash 电子现金系统进行了改进，使之可仲裁、不可盗用[40, 41]；郭涛、李之棠基于椭圆曲线的盲签名方案，利用 Brands 的受限盲签名技术构建了一个离线电子现金协议[42]；蔡满春、杨义先利用基于椭圆曲线密码体制的签名和盲签名算法以及分割选择技术，提出一种离线电子现金方案[43]；陈少真、李