电子现金技术*)

李继国[1] 曹珍富[2] 李建中[1]

(哈尔滨工业大学计算学院 哈尔滨 150001)[1] (上海交通大学计算机系 上海 200030)[2]

摘 要 本文首先介绍电子现金产生的背景、概念、研究思路、国内外现状与进展。然后介绍了电子现金系统的模型、分类、关键技术、存在的问题及述评。最后对电子现金技术的未来进行展望。目的在于让广大读者了解电子现金的发展和重要意义,激发读者积极参与电子现金技术的研究,促进我国电子商务的发展。

关键词 电子现金,盲签名,匿名性,可分性

E-Cash Technology

LI Ji-Guo[1] CAO Zhen-Fu[2] Li Jian-Zhong[1]

(School of Computer Science & Technology, Harbin Institute of Technology, Harbin 150001, China)[1]

(Department of Computer Science & Technology, Shanghai Jiao Tong University, Shanghai 200030, China)[2]

Abstract This paper firstly introduces background, conception, research idea, present situation and progress at home and abroad of e-cash technology. Then we introduce models, categories, key technologies, open problems and remarks of e-cash system. Finally, we look into the future of e-cash technology. We want to make most readers learn about progress and significance of e-cash technology, to encourage readers to participant the research of e-cash technology, and to accelerate development of e-commerce in our country.

Keywords E-cash, Blind signature, Anonymity, Divisibility

1. 引言

随着 Internet 网络技术的飞速发展,建立在 Internet 网络技术基础之上的电子商务正在逐渐走进我们的生活。人们对方便、快捷、安全的电子支付技术的需求越来越迫切,而电子现金(E-Cash)就是一种非常重要的安全电子支付系统,电子现金正是在这样的背景下应运而生的。商家希望通过 Internet 来销售其商品,顾客也希望能够通过 Internet 方便而安全地购买物品。这一切,既为 Internet 技术的发展提供了新的动力,同时也使其面临着巨大的挑战。这是因为,电子商务的发展离不开电子化的交易手段,而 Internet 却缺乏标准的安全机制,难以保证在电子化交易中交易双方的身份认证、交易数据的保密性、匿名性、不可否认性以及交易的公平性。

为了解决这些问题,计算机专家和密码学专家们利用密码技术,在 Internet 标准协议基础之上进行了深入的探讨与研究,提出了许多电子现金方案[1~17]。电子现金(E-Cash)又称电子货币(E-money/coin),数字现金(Digital cash/money),它可以看作是现实纸币的电子或数字模拟,但比现实纸币更方便经济,它是一种重要的电子支付系统。它的最简单形式包括三个主体和四个安全协议过程:商店,用户,银行;注册协议,提款协议,支付协议,存款协议。第一个电子现金方案由 Chaum[1]在 1982 年提出,他利用盲签名技术,可以完全保护用户的隐私权。根据电子现金在花费时是否与银行进联机验证,分为在线电子现金系统和离线电子现金系统。尽管在线电子现金系统有非常好的安全性,但巨大的通信量和验证中心的瓶颈会使得系统的效率极低。而离线电子现金系统对用户的重复花费都是进行事后检测,又由于电子现金非常容易拷贝,因此重复花费不可避免,并且事后检查出的重复花费所造成的损失如何挽回也是尚待解决的问题。完全匿名的电子现金系统[1]可使不法分子进行"完美犯罪"[8],如敲诈、勒索、非法购买、行贿受贿等。于是基于密钥托管[18,19]、公平盲签名[9]和间接论述证明[20](indirect discourse proofs)等思想的匿名撤销的离线电子现金方案[10~12,21]和公平离线电子现金方案[20,22]成为研究的热点。针对在线和离线电子现金系统的优缺点,陈恺,张玉清和肖国镇[23]给出一种概率验证方案,建立了一个联机和脱机相结合的匿名可分电子现金系统。一个理想的电子现金系统应具有如下性质:

独立性:电子现金的安全性不依赖于任何物理位置,电子现金能通过计算机网络传送。

条件匿名性:现金的使用不泄露合法用户的身份,在必要时(如用户被怀疑敲诈、勒索等)可借助可信第三方撤销匿名性。

不可伪造性:除了银行合法发行电子现金外,任何人都不能伪造电子现金。

不可重复花费性:电子现金只能使用一次,重复花费将以很大的概率被发现。

可分性:电子现金可以分成更小数额的几份现金,但总金额保持不变。

可传递性:用户可以任意地将电子现金转借给别人,而不被追踪。

不可连接性:用户不同的电子现金不能被联系起来。

离线支付:用户在支付电子现金时,商店不需要和银行进行联机验证。

目前世界上已投入使用的电子现金系统有 Netcash[24]电

*)国家自然科学基金(No. 60072018),国家杰出青年科学基金资助项目(60225007),教育部高等学校博士学科点专项基金(20020248024)。李继国 博士生,主要研究方向为密码学理论与技术、电子商务等;曹珍富 教授,博士生导师,主要研究方向为数论与现代密码算法理论、信息安全的理论与技术、密码协议与网络安全、电子商务等;李建中 教授,博士生导师,主要研究领域为数据库系统技术,并行计算技术。

子现金构架，欧盟 ESPRIT 计划研制的 CAFE[25](Conditional Access for Europe)系统，D. Chaum 建立的 E-Cash[26]系统以及 CyberCash[27]等电子现金系统。而国内在电子现金设计方面的工作仅限于理论研究，暂时还没有安全、有效、实用的电子现金系统。尽管各国都在积极地研究电子现金技术，但出于安全和效率等多方面的技术原因，真正实用的大规模电子现金系统尚不多见。

2. 主要电子现金模型

本文总结出四个常用的电子现金模型如图 1～4。

图 1 是电子现金的基本模型，包括三个主体和四个安全协议过程：商店 S，用户 U，银行 B；一个取款协议，用户 U 从银行 B 提取电子现金，这时他的帐户被记入借方；一个支付协议，用户 U 支付电子现金给商店 S；一个存款协议，商店 S 把电子现金存入银行 B，这时它的帐户被记入贷方。

在离线电子现金系统中，同一电子现金两次花费能被检查，但不能防止。针对这一问题，1992 年 D. Chaum 和 T. P. Pedersen[5]利用防窜扰设备(如 smart 卡)解决了这一问题，并给出了具有电子钱包的电子现金模型(如图 2 所示)。在该模型中，Smart 卡与用户相互制约防止用户两次花费同一电子现金。即如果用户删除对 Smart 卡不利的信息或两次花费同一电子现金，则 Smart 卡不工作。另一方面，Smart 卡不能直接向外部发送或从外部接收信息，而必须通过用户进行，以防止 Smart 卡将用户的保密信息(如身份等)泄露出去。其它工作过程如基本模型。

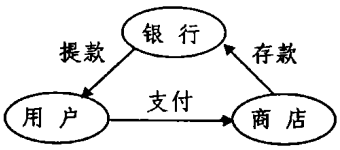

图 1

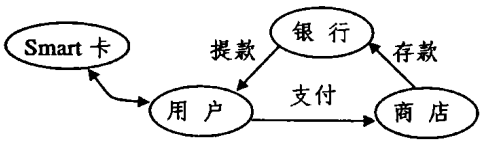

图 2

J. Camenisch，U. Maurer，M. Stadler[10]提出的公平离线电子现金模型(如图 3 所示)扩展了上述两个模型的功能。除了具有基本模型的全部功能外，它还可利用可信第三方 T 来进行用户跟踪和货币跟踪。用户跟踪协议跟踪指定货币的用户身份。在这个协议中 B 把存款协议的信息提供给 T。T 返回一个包含验证信息的串，通过它 B 由帐户数据库验证用户的身份。

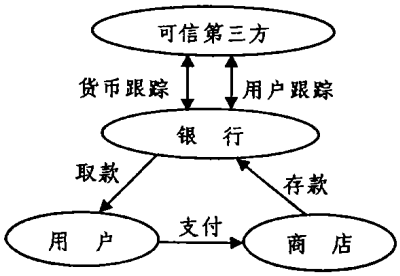

图 3 公平离线电子现金模型

货币跟踪协议跟踪货币取款的来源。在这个协议中，T 根据来自 B 的取款协议信息返回取款来源信息。B 能通过访问它的存款协议信息使用 T 的返回值来发现货币。

用户跟踪协议允许授权机构阻止洗黑钱，因为他们能发现可疑货币的来源。它也允许授权机构发现使用匿名服务的顾客的身份，而对合法用户仍然提供匿名性。

货币跟踪协议允许授权机构发现可疑取款的目的地。这能解决勒索问题[8]：一名顾客被勒索并且强迫匿名提取电子货币，以至勒索者能不被验证身份地使用这些货币，实际上进行着“完美犯罪”，当然不幸者不得不抱怨并且要求继续跟踪取款。当可疑用户取款时，该机制也能跟踪他的活动。

张方国、张福泰、王育民[17]首次提出了多银行电子现金模型，如图 4 所示，这些银行形成一个群体，受中央管理，每个银行都可以发行电子现金。这个系统的参与主体有：中央银行 B，各地分行 B_i，可信第三方 T，某个用户 U(他有自己的银行 B_i)，商店(他有自己的银行 B_j)。工作过程如下：

注册：用户 U 首先在可信第三方建立起身份与化名，或身份与匿名的身份号的联系，使得以后可信第三方通过这些联系能够实现用户的匿名撤销，同时用户也得到了可信第三方发给他的可以证明已经注册的合法证书。

开户：用户 U 在自己的银行 B_i 有帐号。

提款：用户 U 从自己的银行 B_i 提取一笔电子现金。

支付：用户 U 在商店买了东西，将现金支付给商店。

存款：商店在自己的银行 B_j 将得到的电子现金存入自己的帐号。

追踪：银行 B_j 发现这笔电子现金有问题时，由中央银行找到银行 B_i，然后借助可信第三方追踪到用户 U。

为了减轻商店的工作量，使得商店可方便地验证任意一笔电子现金的合法性，假定所有银行形成一个群体，各银行利用群盲签名技术发行电子现金[15]。

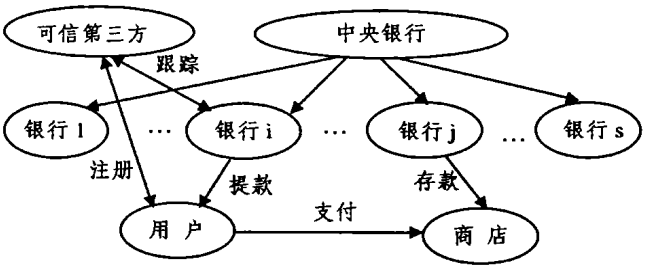

图 4 多银行公平电子现金模型

3. 电子现金的关键技术

3.1 盲签名技术

1982 年，Chaum[1]首次提出盲签名概念，并利用盲签名技术提出了第一个电子现金方案。利用盲签名技术可以完全保护用户的隐私权，因此，盲签名技术仍在诸多电子现金方案[2~7]中广泛使用。

盲签名：一个盲签名方案包括两个实体，消息发送者和签名者。它允许发送者让签名者对给定的消息签名，并且没有泄露关于消息和消息签名的任何信息。

为了说明盲签名的基本概念，我们设 A 为发送者 B 为签名者。A 从 B 处获得盲签名一般来说有如下几个步骤：

(1)A 将消息 m 乘一个随机数得 m'，这个随机数通常称为盲因子，A 将盲消息 m' 送给 B。

(2)B 对 m' 签名后，将其签名 $sig(m')$ 送给 A。

(3)A 通过除去盲因子可从 B 关于 m' 的签名 $sig(m')$ 中得到 B 关于原始消息 m 的签名 $sig(m)$。

但遗憾的是 S. vanSolms, D. Naccade[8]指出盲签名在完全保护用户隐私的同时,也为许多不法分子提供了方便。他们利用电子现金的完全匿名性进行一些违法犯罪活动,如敲诈勒索、洗钱、贪污、非法购买等。出于这个原因,1995 年,M. Stadler, J-M. Piveteau 和 J. Camenisch[9]提出了公平盲签名的概念,可用于条件匿名支付系统[10~12]。公平盲签名模型包括发送者、签名者、可信第三方(如法官)和两个协议(发送者和签名者之间的签名协议、签名者和可信第三方之间的连接恢复协议)(见图 5)。

通过执行签名协议,发送者获得他所选择消息的有效签名,使得签名者不能把他看到的盲消息签名对与原始消息签名对联系起来。通过运行连接恢复协议,签名者从法官获得信息,使他能识别出相应的盲消息签名对和原始消息签名对。根据连接恢复协议中法官从签名者获得的消息,可把公平盲签名方案分为两种类型:

类型 I:给定签名者的盲消息签名对,法官发送信息使签名者能有效地认出相应的原始消息签名对。

类型 II:给定原始消息签名对,法官发送信息使签名者能有效地识别相应的原始消息的发送者或发现相应的盲消息签名对。

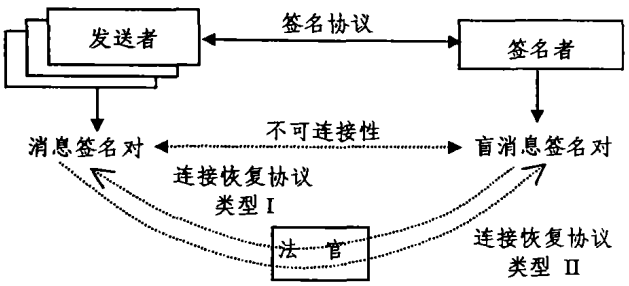

图 5 公平盲签名

公平盲签名主要有两方面的应用。一方面,在匿名支付系统中为防止洗钱提供工具。在基于类型 I 的支付系统中,可信第三方能发现可疑取款的目的地,而在基于类型 II 的支付系统中,他们能确定可疑现金源。另一方面,它能防止文[8]中提出的"完美犯罪"方案:即一个用户被敲诈并强迫他匿名提取现金。如果使用公平盲签名方案类型 I,在给定银行取款协议中所看到的信息后,可信第三方能跟踪被敲诈的电子现金。

注 1:公平盲签名技术不能解决广义敲诈问题,即不法分子强迫银行使用完全盲签名协议,则无法跟踪该不法分子。M. Stadler, J-M. Piveteau 和 J. Camenisch[9]提出了两种公平盲签名方案。一种是基于 Chaum[1]盲签名方案和分割选择方法[1,4],另一种是基于 Fiat-Shamir[28]方案的变形和不经意传输概念[29]。前者在签名协议中需要大量的数据交换,而且签名较长,后者虽然签名非常短但签名协议效率低,两者都不适合于实际应用。因此,高效的公平盲签名方案尚待进一步研究。

在现有的公平电子现金系统中,商家和用户必需使用同一银行,这一要求使电子现金的广泛使用受到一定程度的限制。1998 年,A. Lysyanskaya 和 Z. Ramzan[15]扩展了 J. Camenisch 和 M. Stadler[30]的群签名方案,提出了群盲签名方案,并指出如何利用群盲签名方案构造多银行电子现金思想。最近,张方国、张福泰、王育民[17]首次提出了多银行电子现金模型,并设计了一个可跟踪用户的多银行电子现金方案。

盲签名方案是匿名电子现金的基础。但是,如果单纯地使用目前流行的各种盲签名方案,则无法获取有关待签名的盲签名候选的任何信息,因此必需使用"分割选择"技术来检查盲签名候选的内容,这极大地降低了电子现金的效率。1996 年,M. Abe, E. Fujisaki[31]针对在线电子现金系统银行数据库无限增长问题提出的部分盲签名概念为此问题的解决提供了思路。钟鸣、杨义先[32]提出了一个部分盲签名方案,签名者在签名消息中加入某种身份信息,无需使用"分割选择"方法来检查盲签名候选的内容,并且在此基础上给出了一个基于比特承诺的有效、不可连接、可分电子现金方案[33],这极大地提高了电子现金的效率。S. Miyazaki 和 K. Sakurai[34]也利用部分盲签名方案设计了一个切实可行的电子现金系统。文[35~37]中提出的部分盲签名方案和门限部分盲签名方案也能很容易地运用到目前的电子现金方案中。

3.2 分割选择技术

分割选择技术是密码学的重要技术之一,在电子现金系统[4,7,38,39]中有重要的应用。在取款阶段用户向银行发送 2n 条"盲候选"(其中 n 是安全参数),银行随机选择其中的 n 条盲候选要求用户泄露盲候选的内部结构,银行验证它们的正确性并对剩余的 n 条盲候选进行盲签名。在支付阶段类似的分割选择技术被商店利用来验证用户身份的"线索"(hint),使得如果用户两次花费,则商店通过两条线索识别用户。由此可见,分割选择技术是验证货币正确性的零知识证明的一个工具。因此,它保持了用户的匿名性。显然,分割选择技术导致通信、计算和存储开支的过分浪费,因为在每个阶段都有 k 个货币传输、存储和验证。因此,使用分割选择技术的电子现金系统效率低,后来这种技术逐步被其它技术所取代,如部分盲签名[32,35,36]技术,电子钱包技术[5,40~43]等。

3.3 比特承诺技术

所谓比特承诺,简单地说就是证明者 P 想对验证者 V 承诺一个预测(即 1 比特或比特序列),但直到某个时间后才揭示他的预测。另一方面,V 想确信 P 承诺了他的预测后,他没有改变他的想法。T. Okamoto[44]首先提出检查使用离散对数承诺的数是否在指定的区间这一思想,并应用到电子现金系统中。后来 A. Chan, Y. Frankel, Y. Tsiounis[45]改进了 T. Okamoto 方案,降低了计算复杂性和通信量,并且他们的方案可以方便地使用文[10,11,20]中的跟踪方法。最近,钟鸣,杨义先[33]也利用文[44]中的比特承诺技术给出了一个有效的不可连接电子现金方案。比特承诺技术在电子现金系统中发挥着重要作用。因此,在某种程度上说能否设计出安全、高效、实用的电子现金系统关键在于能否设计出高效的比特承诺方案。

3.4 一次零知识认证技术

T. Okamoto 和 K. Ohta[46]提出了一个新型认证技术,一次零知识认证系统。通俗地说,在这个认证系统,两次使用同一认证被阻止。基于这种技术和分割选择技术,他们提出了一个新的满足不可跟踪性和不可再次花费性的不可跟踪电子现金方案,并进一步探讨了电子现金的可传递性和可分性。下面我们给出一次零知识认证的定义和存在性定理。

一次零知识认证:认证系统 $(A,\{P_i,V_i\})$ 是一次零知识的,如果满足如下条件:

• 零知识性:对任意 V_i,I 和 t,存在一个概率多项式时间图灵机 $M_{V_i}^{*}$ 使得 $M_{V_i}^{*}(I,t)$ 和 $((C,X),(\tilde{P}_i(S),V_i(t)))(I)$ 是多项式不可区分的。

• 一次性:存在一个概率多项式时间图灵机 M_{V_i} 使得如果 $\tilde{P}_i$ 的认证以同一 (C,X) 被 $\tilde{V}_i$ 两次接受,那么对于输入 I

由 Mv_i 产生的输出以压倒多数的概率满足关系 R。

下面定理说明一次零知识认证系统是存在的

定理 如果存在一个安全比特承诺方案(或单向函数)和安全数字签名方案,那么一次零知识认证系统能使用 NP 完全关系来构造。

注 2:通俗地说,零知识性意味着当有效的证明者 $\overline{P}_i$ 的认证以同一(C,X)执行一次,则不会泄露关于秘密信息 S 的任何知识。一次性意味着当有效的证明者 $\overline{P}_i$ 的认证以同一(C,X)执行两次,则秘密信息 S 会被验证者泄露。

3.5 证明对数等式技术

证明对数等式技术主要用于电子现金系统[14,20,43,47]的跟踪。用户和货币跟踪的一个基本工具是对数等式的有效盲证明。这种证明或者孤立地用在公平离线电子现金系统(FOLC),或者作为构造非交互间接论述证明的一个块,它能够提供 FOLC 所必需的一些功能。

设置:一个概率多项式时间($p.p.t.$)证明者 P 和一个 $p.p.t.$ 验证者 V。一般输入是 A,B,a,b,G_1,G_2,G_3,其中 a,b,G_1,G_2,G_3 是素阶子群 G_q 的生成元,$q\in Z_p^*$,p 是大素数,Z_p^* 是乘群。假定证明者不知道与 a,b,G_1,G_2,G_3 相对应的离散对数。向 P 秘密输入 x,v,w 使得 $A\equiv a^xG_1^v(\bmod p)$,$B\equiv b^xG_2^w(\bmod p)$。符号:EqLog$[(A,a),G_1,(B,b),G_2]$表示 $A\equiv a^xG_1^v(\bmod p)$,$B\equiv b^xG_2^w(\bmod p)$,其中 $x\in G_q,G_1,G_2$ 是 G_q 的生成元。人们直觉地认为 $\log_aA=\log_bB$((计算总是模 p)证明如图 6 所示。

EqLog$[(A,a),G_1,(B,b),G_2]$

输入:A,B

P 证明 $A\equiv a^xG_1^v(\bmod p)$,$B\equiv b^xG_2^w(\bmod p)$,即 $\log_aA=\log_bB$:

P		V
$y,s_1,s_2,s_3\in_R Z_q$		
$A'=a^yG_1^{s_1}$,$B'=b^yG_2^{s_2}$		
	A',B' →	$c\in_R Z_q$ 或
	← c	$c=H(A,A',a,G_1,B,B',b,G_2,Info)$
$r=c\cdot x+y$		
$r_1=c\cdot v+s_1$,$r_2=c\cdot w+s_2$	r,r_1,r_2 →	Verify:
		$a^r\cdot G_1^{r_1}\ ?\ A^c\cdot A'$ 和 $b^r\cdot G_2^{r_2}\ ?\ B^c\cdot B'$

图 6 对数等式的证明

4. 电子现金的分类

电子现金技术经过 20 年的发展,已取得了丰硕的成果。到目前为止,仍没有十分系统的分类。H. Petersen 和 G. Poupard[48]根据电子现金系统的功能、性质、效率和安全性等综合考虑,给出了较为系统的分类,如图 7、图 8 所示。

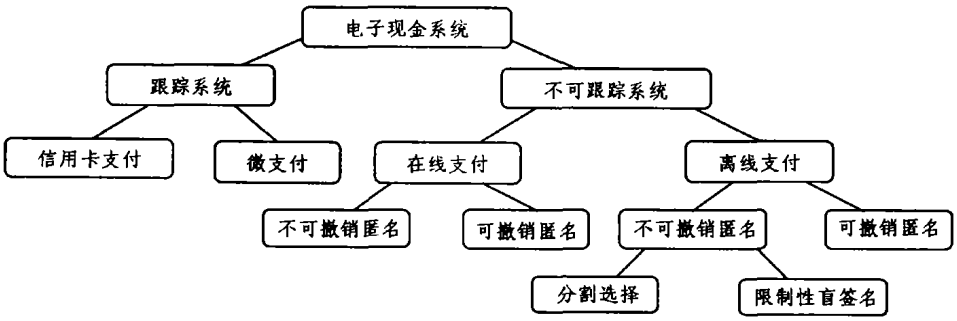

图 7 电子现金系统的分类

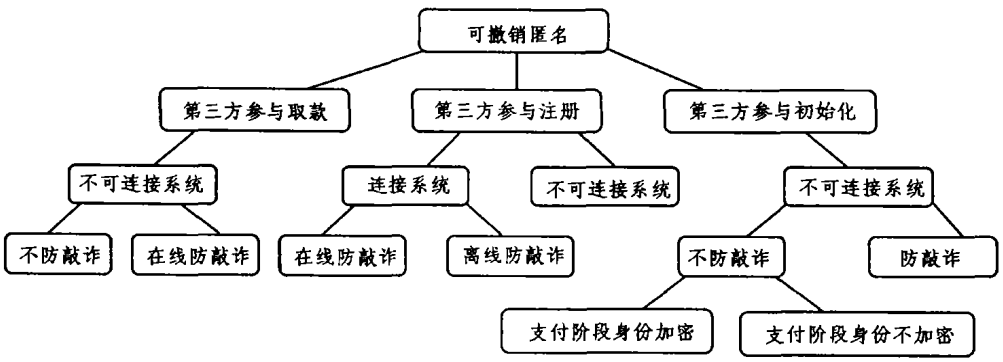

图 8 公平电子现金系统的分类

5. 可能的攻击

不诚实的用户

· 透支(overspending):用户花费的现金值超出了它的允许值。

不诚实的商店

· 冒充(impersonation):商店多次重复花费或重复存储用户支付的现金。

·洗钱(money laundry):商店通过非法活动获得电子现金,为了隐藏货币的来源,商店设法将这些钱合法化。

不诚实的银行

·跟踪用户:银行跟踪电子现金与用户之间的关系。

·借助第三方跟踪用户:银行向第三方谎称电子现金已透支,在借助第三方跟踪该现金的诚实用户的身份后,指控该用户。

·诬陷用户:银行虚假地指控用户透支现金。

·诬陷商店:银行虚假地指控商店两次向银行存同一个有效的电子现金。

·透支后伪造现金:银行对一个已经透支的现金产生虚假的支付文本,以获取过多地赔偿。

不诚实的可信第三方

·诬陷用户:可信第三方虚假地识别一个诚实的用户,因此银行可能会毫无理由地指控该用户。

不诚实的局外人 不诚实的局外人是一个实体,它可能向可信第三方注册(但不是必须的)或者有一个银行帐户。

·伪造现金 对于伪造现金有三种不同的攻击:

一般伪造(universal forgery):一个实体为了获得有效的电子现金,在已知公开参数和过去的支付文本的情况下,伪造银行的签名。

多次取款伪造(one-more forge):一个实体参与n次取款协议后,能获得第n+1次的有效电子现金。

透支伪造:一个实体知道几个透支的支付文本产生新鲜现金文本,并且能够存入银行。

·现金或假名的窃听:一个消极的攻击者窃听取款、支付或存款的通信以获得可花费的现金,一个积极的窃听者可扮作中间人并且修改协议数据。同样的攻击也可应用在注册阶段获取签名的假名。

·窃取或敲诈用户的现金:攻击者可能从用户的设备(如Smart卡)窃取现金文本或强迫用户从他的帐户取款,并且把它们转移到攻击者的设备,使得他以后能花费这笔现金。

·窃取或敲诈商店的现金:攻击者或者窃取商店设备中尚未存入银行的支付文本,或者强迫商店泄露它们。

·窃取或敲诈秘密钥:攻击者或者窃取银行(用户/商店)的秘密钥,例如,黑客攻击进入系统或者强迫泄露秘密钥。

·广义敲诈(blindfolding):攻击者强迫银行(可信第三方)使用完全盲签名协议,以获得电子现金并且他能成功地花费而不被跟踪。

6. 存在的问题及述评

(1)一个尚未解决的问题是基于密码学假定(例如,离散对数)的有效电子现金方案的安全性证明。因为安全性是电子现金系统得以实际应用的一个重要保障,它涉及到用户、商家及银行的风险问题。目前几乎所有的电子现金方案都没有从理论上给出严格的安全性证明,值得庆幸的是这一问题已引起国内外密码学者的高度重视。Pointcheval 和 Stern[49,50]在这方面的研究取得了一定的进展并给出了一些签名方案的安全性证明,指出 Brands[2]方案的安全性证明是可行的。但是为了证明现存的各种电子现金方案的安全性,仍有一些数论问题尚待解决。进一步,目前所有实用的电子现金方案都是建立在存在随机 Oracle 模型假定之上,这是一个非常强的假定,因此如果能弱化或回避这一假定也是一项非常有趣且值得进一步研究的问题。

(2)另外一个值得注意的问题是:往往一个理论上被证明非常安全的电子现金系统可能由于通信代价和计算复杂度过高导致在实践中是不可行的。因此在电子现金系统的安全性问题上,如何在理论证明与实际应用之间寻求一种妥协也是值得探讨的问题。

(3)可分性是电子现金的重要性质,其中最重要的是提供精确支付问题。非可分电子现金方案[51]限制了可分精度和精确支付的次数。可分电子现金方案一般采用二叉树方法[7,33,44],但它允许同一电子硬币的不同支付之间的可连接性,这就影响了用户支付的匿名性。因此寻求一种新的有效可分电子现金的表示方法,使得电子现金具有不可连接性和无限可分精度仍是一个尚未解决的问题[23,47]。

(4)在文[17]中给出了两个尚未解决的问题:一是设计一个实用的多银行电子现金方案不一定利用群签名技术;二是设计一个可废除群成员的群签名方案,这也是群签名方案的一个公开问题,若设计出可废除群成员的群签名方案,则可克服文[17,52]中的电子现金方案的缺点。本文作者认为使用向前安全的数字签名方案[53,54]结合文[17]中的思想可解决第二个尚未解决的问题。

(5)尽管国内外学者对电子现金系统中的敲诈问题进行了深入地探讨与研究。但到目前为止,由 S. van Solms, D. Naccade[8]提出的广义敲诈问题(即不法分子强迫银行使用完全盲签名协议匿名地提取电子现金而无有效方法跟踪不法分子)仍没有得到彻底解决。

(6)目前所有的公平电子现金方案都借助可信第三方(即密钥托管的思想[18,19])来实现对可疑用户和现金进行跟踪。这样就存在两个问题:一是可信第三方权力过大,它只要与银行合谋就能随意地跟踪合法的用户和现金,侵犯了用户的隐私权。二是可信第三方无条件可信这个条件过强。本文作者认为对于前者可通过秘密分享思想[55]加以解决,对于后者采用半可信第三方的思想[56,57]似乎更为合理。另一方面,现有的电子现金方案都是单银行发行电子现金,一旦银行的密钥泄露或被攻击者窃取,那将是灾难性的。因为攻击者能够伪造电子现金且很难发现,对于这种情况作者认为如果采用公平门限盲签名[9]或部分门限盲签名技术[36],多个银行对电子现金进行盲签名,即使攻击者得到一个或几个(小于门限值)银行的签名密钥仍无法伪造合法的电子现金。同时银行定期更换密钥,这能极大提高系统的安全性,当然这也会相应地增加计算量和通信代价。

结论与展望 随着信息技术的突飞猛进,电子支付的革命使得传统商业银行迅速向综合服务机构转变,业务范围扩展至社会生活每一角落,如财务咨询、委托理财、外汇、代理税收、代收工资费用等,以及通过网络进一步提供旅游、信息服务、交通和娱乐等全方位的公共服务,成为电子商务不可或缺的媒介,作为电子商务关键技术之一的电子现金系统将在未来的电子支付手段中占主导地位。因此,对安全、高效、可分的公平离线电子现金系统的研究不仅具有重要的科研学术价值,而且对国家电子商务、金融体系机构的信息化建设和国民经济的发展具有重大的意义。

参 考 文 献

1 Chaum D. Blind signature for untraceable payment. Advances in Cryptology- Eurocrypt'82 Proceedings, Plenum Press, 1983. 199～203

2 Brands S. Untraceable off-line cash in wallets with observers. In Advances in Cryptology- Crypto'93 Proceedings, Lecture Notes in Computer Science 773, Springer-Verlag, 1993. 302～318

3 Jakobsson M. Mini-Cash: A minimalistic approach to E-Commerce. In: Second Intl. Workshop on Practice and Theory in Public Key Cryptography, PKC'99, Lecture Notes in Computer Science 1560, Springer-Verlag, 1999. 122～135

4 Chaum D, Fiat A, Naor M. Untraceable electronic cash. In: Proc. of Crypto'88, Lecture Notes in Computer Science 403, Springer-Verlag, 1990. 319～327

5 Chaum D, Pedersen T. Wallet databases with observers. In:

Proc. of Crypto'92, Lecture Notes in Computer Science 740, Springer-Verlag, 89～105
6 Ferguson N. Single term off-line coins. In: Proc. of Eurocrypto'93, Lecture Notes in Computer Science 765, Springer-Verlag, 318～328
7 Okamoto T, Ohta K. Universal electronic cash. In: Proc. of Crypto'91, Lecture Notes in Computer Science 576, Springer-Verlag, 324～337
8 van Solms S, Naccade D. On blind signatures and perfect crimes. Computers and Security, 1992, 11(6): 581～583
9 Stadler M, Piveteau J M, Camenisch J. Fair blind signature. In: Proc. of Eurocrypt'95, Lecture Notes in Computer Science, Springer-Verlag, 1995, 921: 209～219
10 Camenisch J, Maurer U, Stadler M. Digital payment systems with passive anoymity- revoking trustee. In Esorics'96, Lecture Notes in Computer Science 1146, Springer-Verlag, Italy 1996. 33～43
11 Davida G, Frankel Y, Tsiounis Y, Yung M. Anonymity control in e-cash. In: Proc. of the 1st Financial Cryptography Conf. Lecture Notes in Computer Science 1318, Anguilla, BWI, Springer-Verlag, Feb. 1997. 24～28
12 Claessens J, Preneel B, Vandewalle J. Anonymity controlled electronic payment system. In: Proc. 20th Symposium on Information Theory in the Benclux, Haasrode, Belgium, 1999. 109～116
13 钟鸣，杨义先．一种基于 RSA 盲签名和二次剩余的电子现金方案．北京邮电大学学报，2000，23(3)：87～90
14 王常吉，裴定一．一类公正的离线的电子现金方案．计算机应用，2001，21(3)：9～10
15 Lysyanskaya A, Ramzan Z. Group blind signatures: A scalable solutions to electronic cash. In: Hirschfeld R ed. Lecture Notes in Computer Science 1465, Berlin: Springer-Verlag, 1998. 184～197
16 左英男，戴英侠，许剑卓．一种安全的 Internet 小额交易协议分析．计算机工程，2000，26(7)：136～138
17 张方国，张福泰，王育民．多银行电子现金系统．计算机学报，2001，21(5)：454～462
18 曹珍富．基于公钥密码系统的门限密钥托管方案．中国科学 E 辑，2000，30(4)：360～366
19 曹珍富，李继国．基于 ElGamal 体制的门限密钥托管方案．计算机学报，2002，25(4)：346～350
20 Frankel Y, Tsiounis Y, Yung M. Indirect discourse proofs: Achieving fair off-line e-cash. Advances in Cryptology. In: Proc. of Asiacrypt'96, Lecture Notes in Computer Science 1163, Kyongju, South Korea, Nov. Springer-Verlag, 1996. 286～300
21 Jakobsson M, Yung M. Revokable and versatile electronic money. In: Proc. of the 3rd ACM Conf. on Computer Communication Security, ACM Press, 1996. 76～87
22 Solages D, Traore J. An efficient fair off-line electronic cash system with extensions to checks and wallets with observers. In: Proc. of the 1st Financial Cryptography Conference, Anguilla, BWI, Springer- Verlag, 1998
23 陈恺，张玉清，肖国镇．基于概率验证的可分电子现金系统．计算机研究与发展，2000，37(6)：752～757
24 Medvinsky G, Neuman B C. Netcash: A design for practical electronic currency on the Internet. In: Proc. of the 1st Annual ACM Conf. on Computer and Communications Security, ACM Press, 1993, 102～106
25 Camenisch J L, Piveteau J-M, Stadler M. An efficient payment system protecting privacy. In: Proc. of ESORICS'94, Lecture Notes in Computer Science 875, Springer-Verlag, 1994. 207～215
26 eCash Technologies, 2000. http://www.digicash.com/
27 CyberCash, Inc, 1999. http://www.cybercash.com
28 Fiat A, Shamir A. How to prove yourself: Practical solutions to identification and signature problems. In: Proc. of Crypto'86, Lecture Notes in Computer Science 263, Springer-Verlag, 186～194
29 Even S, Goldreich O, Lempel A. A randomized protocol for signing contracts. Communications of the ACM, 1985, 28: 637～647
30 Camenisch J, Stadler M. Efficient group signature schemes for large groups. In: Kaliski Jr B S, ed. Lecture Notes in Computer Science 1294, Berlin: Springer-Verlag, 1997. 410～424
31 Abe M, Fujisaki E. How to date blind signatures. Advances in Cryptology-Asiacrypt'96 , Lecture Notes in Computer Science 11631, Springer, New York, 1996. 244～251
32 Zhong Ming, Yang Yixian. Partial blind signature based on bit commitment. Chinese Journal of Electronics, 2000, 9(3): 284～286
33 Zhong Ming, Yang Yixian. An efficient unlinkable electronic cash based on bit commitment. Chinese Journal of Electronics, 2001, 10(2): 255～258
34 Miyazaki S, Sakurai K. A practical off-line digital money system with partially blind signatures based on the discrete logarithm problem. IEICE Trans. Fundamentals, 2000, E83-A(1): 106～108
35 Abe M, Camenisch J. Partially blind signature schemes. SCIS97, 1997
36 Juang W-S, Lei C-L. Partially blind threshold signatures based on the discrete logarithm. Compuer Communications 1999, 22: 73～86
37 Juang W-S, Lei C-L, Liaw H T. Fair blind threshold signatures based on the discrete logarithm. Compuer Systems Science & Engineering, 2001, 6: 371～379
38 Franklin M, Yung M. Secure and Efficient Off-line Digital Money. In: Proc. of the twentieth international Colloquium on Automata, Languages and Programming (ICALP 1993), Lund, Sweden, (Lecture Notes in Computer Science 700), Springer-Verlag, 1993. 265～276
39 Pailles J C. New protocols for electronic money. In: Proc. of Ausicrypt'92, 263～274
40 Camer R, Pedersen T. Improved privacy in wallets with observers. In Advances in Cryptology, Proc. of Eurocrypto'93, Lecture Notes in Computer Science 765, Springer-Verlag, 1993. 329～343
41 杨波，刘胜利，王育民．利用 Smart 卡的可撤销匿名性的电子支付系统．电子学报，1999，27(10)：792～796
42 杨波，王育民．利用电子钱包的公正支付系统．计算机学报，1999，22(8)：792～796
43 陈恺，杨波，王育民，肖国镇．利用电子钱包的有效的公正支付系统．计算机学报，2001，24(11)：1191～1195
44 Okamoto T. An efficient divisible electronic cash scheme. In Don Coppersmith, ed. Advances in Cryptology, Proc. of Crypto'95, Lecture Notes in Computer Science 963, Springer-Verlag, Santa Barbara, California, U. S. A, 1995. 27～31
45 Chan A, Frankel Y, Tsiounis Y. Easy come-easy go divisible cash. In: Advances in Cryptology-Eurocrypto'98. Espoo, Finland: Springer-Verlag, 1998. 561～575
46 Okamoto T, Ohta K. One-time zero-knowledge authentications and their applications to untraceable electronic cash. IEICE Trans. Fundamentals, 1998, E81-A(1): 2～10
47 Tsiounis Y. Efficient electronic cash: New notions and techniques: [PhD Thesis]. College of Computer Science, Northeastern University Boston, Massachusetts, 1997
48 Petersen H, Poupard G. Efficient scalable fair cash with off-line extortion prevention. Lecture Notes in Computer Science, 1997, 1334: 463～495
49 Poincheval D, Stern. Provably secure blind signature schemes. In Advances in Cryptology. In: Proc. of Asiacrypt'96, Lecture Notes in Computer Science 1163, Kyongju, South Korea, Springer-Verlag Nov. 1996
50 Poincheval D, Stern. Security proofs for signature schemes. In Advances in Cryptology, Proc. of Eurocrypt'96, Zaragoza, Spain, Springer-Verlag, 1996. 387～398
51 Kozen D, Zaks S. Optimal bounds for the change-making problem. Theoretical Computer Science, 1994, 123: 377～388
52 Traore. Group signature and their relevance to privacy-protecting off-line electronic cash systems. In: Proc. 4th Australian Conf. on Information Security and Privacy, Australia, 1999. 228～243
53 Abdalla M, Reyzin L. A new forward-secure digital signature scheme. In Advances in Cryptology, Proc. of Asiacrypt'2000, Lecture Notes in Computer Science Springer-Verlag, 2000
54 Bellare M, Miner S. A forward-secure digital signature scheme. Advances in Cryptology, Proc. of Crypt'96, Lecture Notes in Computer Science 1666, M. Wiener ed. , Springer-Verlag, 1999
55 Shamir A. How to share a secret. Commun. ACM, 1979, 24 (11): 612～613
56 蒋晓宁，叶澄清，潘雪增．基于半可信离线第三方的公平交易协议．计算机研究与发展，2001，38(4)：502～508
57 Franklin M K, Reiter M K. Fair exchange with a semi-trusted third party. In: proc. of 4th ACM Conf on Conputer and Communication Security, Zurich: ACM Press, 1997. 1～5