维普资讯 http://www.cqvip.com

数字现金系统发展问题研究*)

肖 迪[1,2] 高婷婷[1] 王 磊[1] 廖晓峰[1]

(重庆大学计算机学院 重庆400044)[1] (重庆大学机械工程学院 重庆400044)[2]

摘 要 本文介绍了数字现金的关键技术、研究现状和应用现状,并指出了数字现金未来的发展方向。

关键词 数字现金,电子支付

Research on the Development of the Digital Cash System

XIAO Di[1,2] GAO Ting-Ting[1] WANG Lei[1] LIAO Xiao-Feng[1]

(College of Computer, Chongqing University, Chongqing 400044)[1]

(College of Mechanical Engineering, Chongqing University, Chongqing400044)[2]

Abstract In this article, we introduce the basic mode and properties of Digital Cash, and present the key techniques of Digital Cash with examples. The analysis of research and applying state of Digital Cash is made. The developing direction of Digital Cash is pointed out.

Keywords Digital cash, Electronic payment

1 引言

电子商务是将信息技术应用到商务领域中的产物,是未来社会的主流贸易方式。电子商务实现的关键是必须在确保交易各方安全的前提下高效地完成电子支付功能。电子支付方式主要分为:电子信用卡、电子支票和数字现金。其中,数字现金可以看作纸币的数字化形式,能够满足用户的匿名要求,特别适合于人们日常生活中经常进行的小额支付活动,所以它被认为是未来最有发展潜力的一种电子支付方式,成为当前学术界的一个研究热点。本文围绕数字现金的关键技术、研究现状和应用现状进行了深入论述,最后指出了数字现金未来的发展方向。

2 数字现金的基本概念

2.1 基本模式

一个典型的数字现金系统包括:用户、商人和银行三方和提款协议、支付协议、存款协议三协议,如图1所示。用户和银行执行提款协议,用户从银行提取数字现金,同时银行从用户的帐户上减去所提取的现金额;用户和商人执行支付协议,用户从商人处购买商品,同时将自己的数字现金支付给商人;商人和银行执行存款协议,商人把自己交易所得的数字现金传给银行,银行验证后在商人的帐户上加上相应的现金额。

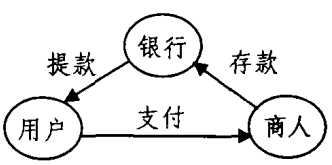

图1 数字现金的基本模式

2.2 理想的数字现金系统应具备的基本性质

(1)独立性:数字现金的安全性不依赖于任何物理位置,能通过计算机网络传送。

(2)安全性:数字现金不能被拷贝和重用。

(3)匿名性(不可追踪性):用户的隐私受到保护,没有人能追踪发现用户和他们的所购物品之间的关系。

(4)脱线付款:当一个用户用数字现金为所购物品付款时,用户和商家之间的协议是脱线执行的。即商家不必与一台主机相连以处理用户的付款。

(5)可转移性:数字现金可被转移给其他用户。

(6)可分性:给定数量的数字现金能被分成较小数额的几份数字现金。

(7)较高的处理效率:由于数字现金交易的实时性和频繁性,因此处理效率的高低成为一个数字现金系统能否广泛普及的一个重要因素。

3 数字现金系统的关键技术

要设计出一种理想的数字现金系统必须充分利用大量的高新技术,比如现代密码学中的几乎所有技术在这里都可以派上用场。本文仅介绍其中最为重要的几种。

3.1 分割选择/零知识证明技术(cut and choose /zero-knowledge proof)

该技术被证明者用来向验证者证明自己拥有或知道某一消息,但证明的过程不用向验证者泄露关于被证明消息的任何信息。在数字现金系统中,用户提取数字现金时,不能让银行知道数字现金的内容,但银行需要确定提取的数字现金是正确构造的。用户正确构造N个数字现金传给银行,银行随机地抽取其中的N-1个让用户给出其构造,若构造都是正确的,则银行就认为剩下的那个现金的构造也是正确的,并对它进行签名,这样用户得到数字现金。

3.2 盲签名技术(blind signature)

*)本文受国家自然科学基金(No:60271019)、教育部博士点专项基金(No:20020611007)和重庆市科委应用基础研究项目基金(No:7370)资助。

肖 迪 讲师,博士生,研究方向:制造业信息化、信息安全技术等。高婷婷 硕士生。王磊 硕士生。廖晓峰 教授,博士生导师。

维普资讯 http://www.cqvip.com

一般进行数字签名时，总是要先知道文件的内容而后才签署。但有时我们需要某人对一个文件签字，但又不让他知道文件的内容，这就需要盲签名技术。在数字现金系统中，盲签名是一个重要的模块，用来实现用户的匿名性。

3.3 位承诺技术(bit commitment)

当 A 想向 B 承诺对未来将要发生的一个事件的预测，但在事件发生前不对其披露；而 B 又要求能确信 A 对其所要作的承诺不会变卦，这时就要用到位承诺技术。在数字现金系统中，位承诺技术可以在双方不信任的条件下完成认证，具有重要的应用。位承诺可以用多种技术来实现，如使用对称密码学、伪随机序列发生器、单向散列函数等。

3.4 关键技术在数字现金中的应用实例

现在我们应用上述关键技术来对 David Chaum[4]提出的一个数字现金系统加以实现。限于篇幅，我们在这里只介绍该系统中“提款协议”部分的实现过程。

系统设置：银行建立帐号数据库 ANDB(Account Number DataBase)记录用户帐号的存款金额，支票编号数据库 CNDB(Check Number DataBase)记录已经发行的支票号，已使用过的无效支票数据库 ICDB (Invalid Check DataBase)主要用于防止支票的重复使用。设用户和银行的 RSA 密钥分别是：(K-UPB，K-UPV)、(K-BPB，K-BPV)。“提款协议”实现如下：

(1)用户选择 k 个支票号。针对每个支票号 $X_i(1\leqslant i\leqslant k)$，填入支票金额 t_i 和 k 个鉴别字符串 $I_j(1\leqslant j\leqslant k)$。鉴别字符串主要用来对数字现金的重用进行事后检查。每个 I_j 是这样产生的：

用户选择随机数 a_j、c_j 和 d_j，计算 $x_j=g(a_j,c_j)$，$y_j=g(a_j\oplus u,d_j)$，$I_j=f(x_j,y_j)$，其中 f、g 是两参数的单向散列函数，u 为用户的帐号。这里实际上利用了单向函数来实现位承诺。

(2)用户选择随机数 $r_i(1\leqslant i\leqslant k)$，计算 $B_i=r_i^{K-BPB}(I_1\|I_2\|\cdots\|I_k\|X_i\|t_i)\bmod n$，‖表示间隔符。这一步开始利用盲签名技术。

(3)用户将$\{B_i\mid 1\leqslant i\leqslant k\}$分别用银行的公钥加密后发送给银行。

(4)根据分割选择/零知识证明技术的原理，银行在$\{B_i\mid 1\leqslant i\leqslant k\}$中随机选择 k－1个提出质疑，设为集合 $R=\{i_1,i_2,\cdots,i_{k-1}\}$。

(5)银行将 R 用用户的公钥加密后发送给用户。

(6)用户根据 R，加密传送相应的 r_i 和 a_j、c_j 和 $d_j(1\leqslant j\leqslant k)$及帐号 u 给银行。

(7)根据 R，银行用 r_i 解盲 B_i，若 $X_i\in$CNDB，且当 $i\neq j$ 时，有 $X_i\neq X_j$，$t_i=t_j=t$，那么银行根据提供的 r_i 和 a_j、c_j 和 $d_j(1\leqslant j\leqslant k)$重新计算 B_i'，若 $B_i'=B_i$，可以确定用户没有欺骗。

(8)银行确认用户没有欺骗以后，对剩下的那个未质疑的数字现金 B_p 进行签名：$C_p=B_p^{K-BPV}\bmod n$，并检查用户的帐号 u 中是否有足够的存款，如有则划去 t 元，否则终止协议。

(9)银行将$(C_p\|B_p)$用用户的公钥加密后传送给用户。

(10)用户除去盲因子 r_p，得到经过银行签名的金额为 t 元的数字现金(B，C)：$B=(I_1\|I_2\|\cdots\|I_k\|X_p\|t_p)\bmod n$，$C=B^{K-BPV}\bmod n$。

4 数字现金的研究现状

研究人员围绕着理想数字现金应该具备的各项基本性质进行了大量的研究，目前已提出了不少且各有侧重的数字现金方案。本文从数字现金基本性质的角度对各种具有代表性的数字现金方案的发展现状进行讨论。

在数字现金的早期研究中，人们主要侧重于对“匿名性”和“脱线付款”的研究，由此形成一种“匿名脱线不可分数字现金系统”的数字现金类型。该类型的数字现金方案最早是由 Chaum，Fiat 和 Naor[4]提出的，其方案的安全性主要基于 RSA，Hash 函数和随机性假设，提款和支付时采用分割选择技术，虽然该方案很不实用，但是它为以后的研究工作奠定了基础。Okamoto 和 Ohta[5]对该方案进行了改进，将提款协议中用户身份的零知识证明部分改到在申请建立帐户阶段来进行，使系统的效率有所提高。Franklin 和 Yung[6]提出了第一个基于离散对数假设的脱线数字现金方案，从而为数字现金的发展开辟了除 RSA 以外的另一条道路。1993年 Brands[7]提出了一种单个现金方案，该方案的安全性基于 Schnorr 签名和素数阶群上的表示问题(即 Brands 假设)，效率较高，已经成为一个经典的数字现金方案。

数字现金的“可分性”也是一个研究的重点，由此形成了一类“匿名脱线可分数字现金系统”。可分数字现金的实现技术主要有两条途径：一是由 Okamoto 和 Ohta[8]提出的数字现金金额的二叉树表示方法，目前很多的“可分数字现金系统”都采用了该方法，但是该方法实现复杂，运算量大，不利于实际推广应用；另外一条技术途径是设想在提取现金时取出适量面额不等的数字现金，而支付时则以这些数字现金的子集来完成等额支付。

人们对于数字现金的“匿名性”的态度也有一个逐渐成熟的过程，由于数字现金的完全匿名性可能被用于犯罪活动，所以现在人们提出了一类在一定条件下“可撤消匿名性的数字现金系统”。这种类型的数字现金系统一般需要在普通数字现金系统的基础上增加一个可信的仲裁方和现金提取人跟踪协议和现金跟踪协议，以实现对现金提款人和现金的跟踪。该类型的数字现金中比较有代表性的方案有：Camenisch[9]提出的可信方除了用户登记和跟踪以外均脱线的可撤消匿名性的数字现金方案。

在脱线数字现金系统中，对用户的重复花费都是在事后检查，事后检查出的重复花费损失如何挽回是很棘手的。而在线数字现金系统虽然有很好的安全性，但是巨大的通信量和银行验证时可能形成的瓶颈又使得这种系统效率低下，无法实用化。针对上述问题，人们提出了一类将在线和脱线验证结合起来的“基于概率验证的数字现金系统”，即通过加入一个概率算法来决定对用户支付的数字现金是采用在线方式由银行来验证还是采用脱线方式直接由商家验证。该类型的数字现金中比较有代表性的方案有：陈恺[10]和史国庆[11]分别独立提出的加入概率验证的数字现金系统。

为了防止用户在脱线支付时重复花费数字现金，人们提出了一类“基于智能卡的数字现金系统”，通过在防窜扰的智能卡中去掉已花费过的数字现金可以在一定条件下实现对重复花费的防止功能。陈恺[12]和王常吉[13]基于 Brands 体制分别独立提出了利用电子钱包和智能卡的可撤消匿名性的数字现金方案。

通过对现有某数字现金方案进行局部改进来提高其处理效率的情况在人们对数字现金进行研究的过程中很常见，比如：谭运猛[14]针对 Brands 提款协议中的大量模指数运算严重降低用户端的在线处理速度的问题提出了预处理算法；王

(下转第79页)

维普资讯 http://www.cqvip.com

表3 算法精确性的比较

支持度	3%	2%	1.5%	1%
Aprior 算法	47%	57%	79%	92%
GSP 算法	44%	57%	78%	85%
SPM-ID 算法	54%	67%	90%	98%

表4 可扩展性分析(1%,2%,2s)

数据量	71.4M	71.4 * 2M	71.4 * 4M
Aprior 算法	154s	337s	613s
GSP 算法	143s	335s	550s
SPM-ID 算法	134s	210s	374s

我们在 AIX4.0,ReadHat7.2,Win2000Server 下的实验结果如表5所示,结果数据表明 SPM-ID 算法在不同的环境下有较好适应性。

表5 可适应性分析(数据库大小71.4M,(1%,2%,2s))

环境	Unix	Linux	Win2000
Aprior 算法	154s	187s	188s
GSP 算法	143s	145s	177s
SPM-ID 算法	134s	134s	137s

参 考 文 献

1 Denning D E. An intrusion detection model. IEEE Trans on Software Engineering, 1987, 13(2): 222~232

2 Lee W, Stoifo S J. Data mining approaches for intrusion detection. In: Proc. of the 7th USENIX Security Symposium. San Antonio, TX. Jan. 1998

3 http://www.cs.msstate.edu/~secrutiy/iids/publications/citss_ids.pdf

4 周斌,吴泉源. 序列模式挖掘的一种渐进算法[J]. 计算机学报, 1999,22(8):882~887

5 Joshi M, Karypis G. A Universal Formulation of Sequential Patterns: [Technical Report No. 99-021]. Department of Computer Science, University of Minnesota, 1999

6 Mannila H, Tovonen H. Discovering generalized episodes using minimal occurrences. In: Proc. of the 2nd Intl. Conf. on Knowledge Discovery in Databases and Data Mining, Portland, Oregon, Aug. 1996

(上接第68页)

常吉[15]则通过在 Brands 数字现金方案中嵌入由银行规定的数字现金的有效期来防止银行检察现金重用性的数据库的无限增长。

5 数字现金的应用现状

目前在国外已有一些数字现金系统在实际使用或试用。下面是两种比较有代表性的基于智能卡的数字现金系统:

VisaCash 是一个储值支付品牌,由 Visa 提供,消费者的智能卡跟踪保持在银行的现金帐户的金额,为付款者提供脱线的支付担保。商家收集所有支付,统一在银行进行批存款操作,一旦通过银行内部网络进行资金结算,这些收款者的资金有效。

Mondex electronic cash 与 VisaCash 不同,就像一个现金替代物。智能卡代表现金,资金可以从付款者的卡直接转到收款者,收款者重复接收资金而不需要在银行存放。在 Mondex 和普通货币之间转换需要内部金融网络,但不进行结算存款。

数字现金在欧洲和日本比较普及,主要用于小金额的购买活动,如:自动售货机、Internet 上的微支付等。但是由于数字现金的某些关键技术并未彻底解决,再加上存在一些相互竞争的技术而没有统一的数字现金系统的标准,从而给数字现金的进一步推广应用造成了困难。

结论 由于数字现金具有极为广泛的应用前景,因此对它的研究已成为当前学术界的一个热点。但是,在迄今人们已提出的各种数字现金方案中还没有一个方案可以真正地同时满足理想数字现金的各种性质要求。我们认为,数字现金未来的研究发展方向应该集中在如何解决其可分性、可传递性和如何提高其执行效率上,这样才有可能把数字现金真正推向实用化。

参 考 文 献

1 Schneier B(美). 应用密码学. 北京. 机械工业出版社,2000

2 杨义先,等. 信息安全新技术. 北京. 北京邮电大学出版社,2002

3 卿斯汉. 密码学与计算机网络安全. 北京:清华大学出版社,2001

4 Chaum D, Fiat A, Naor M. Untraceable Electronic Cash. Advances in Cryptology-Crypto'88, 1990. 319~327

5 Okamoto T, Ohta K. Disposable Zero-knowledge Authentication and Their Applications to Untraceable Electronic Cash. Advances in Cryptology, Proceedings of Crypto'89 (Lecture Notes in Computer Science), 1990. 481~496

6 Franklin M, Yung M. Secure and Efficient Off-line Digital Money. In: Proc. ICALP'93 LNCS 700, Springer-verlag, 1993. 265~276

7 Brands S. Untraceable Off-Line Cash in Wallets with Observers. Advances in Cryptology-Crypto'93, 1993. 302~318

8 Okamoto T, Ohta K. Universal Electronic Cash. Advances in Cryptology-Crypto'91. 1992. 324~337

9 Camenisch J, Maurer U, Stadler M. Digital Payment Systems with Passive Anonymity-Revoking Trustees. Esorics'96. Italy. Springer-verlag, 1996. 33~44

10 陈恺,等. 基于概率验证的可分电子现金系统. 计算机研究与发展, 2000.6

11 史国庆,等. 加入概率验证的 Brands 数字现金改进方案算法. 计算机工程与科学,2001.6

12 陈恺,等. 可撤消匿名性的可分电子现金系统. 西安电子科技大学学报,2001.1

13 王常吉,等. 一个新的利用 Smart 卡的公正的电子现金系统. 计算机学报,2001,12

14 谭运猛,等. 针对 Brands 电子现金支付协议的预处理算法. 通信学报,2002.2

15 王常吉,等. 一个改进的基于限制性盲签名的电子现金系统. 电子学报,2002,7

16 Yu H-C, His K-H, Kuo P-J. Electronic payment systems: an analysis and comparison of types. Technology in Society, 2002, 24:331~347

17 陈恺,等. 电子现金系统的研究与发展. 西安电子科技大学学报, 2000,4