一个实用的 off-line 公平电子现金系统

高虎明,毛 剑,王育民
(西安电子科技大学 ISN 国家重点实验室,陕西西安 710071)

摘 要: 本文提出的 off-line 公平电子现金系统具有以下特点:能保护合法用户的匿名性;可追踪非法用户;非法者不能敲诈用户;他人获得合法用户的电子现金不可盗用;银行与用户之间发生重复花费的争议时可仲裁;银行与信任机构都是脱线的. 虽然信任机构要维护一个与银行相同数量级的数据库,但换来了申请、支付和存款的高效率.

关键词: 脱线公平电子现金; 广义 ElGamal 签字; eCash™
中图分类号: TB11 **文献标识码**: A **文章编号**: 0372-2112 (2003) 02-0196-03

A Practical Off-Line Fair Electronic Cash System

GAO Hu-ming, MAO Jian, WANG Yu-min
(National key laboratory of ISN, Xidian University, Xi'an, Shaanxi 710071, China)

Abstract: The future electronic cash should have all the advantages of note and not have the disadvantages of it. The system presented in the paper has following characteristics: revocable anonymity; off-line; as simple as eCash™ in application and payment processes; overcome the two flaws in the eCash™ system: 1. anyone who somehow observes the eCash™ Coins can spend them; 2. when the dispute about if one Coin has been doubly spent between Bank and a user takes place, it should be impossible for other person to arbitrate it. So the system should be one of the most practical systems proposed at present.

Key words: off-line fair electronic cash; the extending ElGamal signature; eCash™

1 引言

电子现金是特定银行发行的可作为货币支付的具有现金的匿名性特点的数据串. 著名密码学家 David Chaum 1982 年首次提出了利用盲签字实现电子现金的方法,基本模式如图 1 所示. eCash™是 DigiCash 开发的用软件实现的第一个完全匿名的在线电子现金系统,它的基本算法是 RSA 盲签字,1995 年 Mark Twain 银行就开始发行 Internet 网上电子现金,为了扩展业务,1998 年他们又成立了 eCash™ Technologies, INC. DigiCash 是 Divid Chaum 发起的提供电子支付系统的专业公司,建立于荷兰,现在总部设在美国,电子现金已由理论研究走向实用.

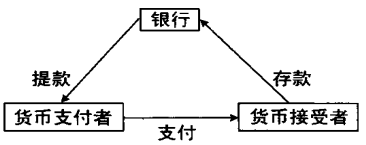


图 1 eCash™电子现金系统基本模型

1992 年 Von Solms B. 和 Naccache D. 指出完全匿名的电子现金像普通现金一样能被犯罪分子利用进行洗黑钱,勒索等犯罪活动. 我们希望未来的电子现金系统具有普通货币的优点克服它的缺点,1995 年,Stadler 和 Brickel 分别独立提出了可控制匿名的电子现金(或公平电子现金)的实现方案,为了解决保证合法用户的匿名性,同时避免敲诈和洗黑钱等违法活动及对用户进行有条件跟踪的矛盾引入了可信赖第三方,指出电子现金的基本模型如图 2,应该包含提款、支付、存款和追踪四个基本协议.

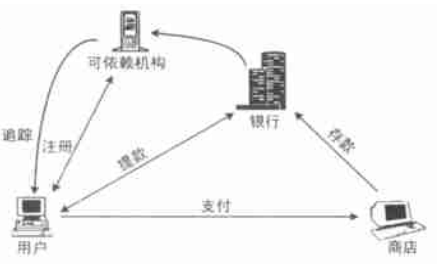


图 2 电子现金的基本模型

目前已有很多脱线的可控制匿名的电子现金方案,大部分或者使用分割选择技术,或者用零知识证明,或者表示电子现金的字符串太长,或者要求可信赖机构在线服务等等实用性较差. 我们了解的最有效的实现可控制匿名的电子现金方案是 Ari Juels1999 年提出的由 TTP 向用户发放"信任标志"(trustee token)的方法,"trustee token"是 TTP 的承诺,用来实现可控制匿名,可加在现有的完全匿名的电子现金系统的顶部,构成可控制匿名的电子现金系统.

本文提出的方案是基于 Ari Juels 的思想的,但是简单实用存在以下两个漏洞: (1) 万一用户丢失电子现金,可被他人使用; (2) 银行与用户之间争议关于某个电子现金是否已经花费时无法仲裁. 我们的电子现金形式是 $\{g^x, h(g^x)^d\}$,基本想

收稿日期:2001-07-12;修回日期:2002-04-28
基金项目:国家自然科学基金(No. 60073052)

法是可信任机构有存储 g^x 的数据库,用来追踪实现可控制匿名,银行签发电子现金用 RSA 盲签字,用户支付用广义 ElGamal签子,x 为用户的秘密信息,他人不知道 x,即使有 $\{g^x, h(g^x)^d\}$也无法使用从而避免了上述两漏洞.

我们的系统与 eCash™ 比除了增加可信任机构和一个 ElGamal签字系统外,并没有增加额外的通信、存储和运算开支,是一个很有实用价值的脱线的可控制匿名的电子现金系统.提款和支付的效率和复杂度与 eCash™ 基本相同,为了实现公平性增加可信任机构的开支是不可避免的,与别的方案比只是增加了可信任机构的数据库维护量,但由于是脱线服务不会影响使用效率具有很强的实用性.

2　系统的建立

2.1　系统使用的基本密码工具

(1) hash 函数:hash 函数是将任意长的数字串 M 映射成一个较短的定长输出数字串的函数,一般用表 $h(\cdot)$ 表示.说一个 hash 函数是安全的是指给定函数值求自变量困难,例如 MD-4,MD-5,SHA 等是安全的 hash 函数.

(2) RSA 盲签字算法:设 B 的公钥为 e 密钥 d,模为 $n=pq$, p, q 为两个安全大素数, $h(\cdot)$ 是安全 hash 函数. A 要得到 B 对 m 的盲签字,有以下几种形式:

(a) A 任选 $1<k<n$,计算 $t=(h(m))\,k^e \bmod n$ $\xrightarrow{t}$ B;

(b) B 计算 $S'=t^d=(h(m)\,k^e)^d \bmod n$ $\xrightarrow{S'}$ A;

(c) A 计算 $S=S'/k=h(m)^d \bmod n$. S 为 B 对 $h(m)$ 的 RSA 签字.

验证过程 $S^e=h(m)$

(3)广义 ElGamal 签字算法:设 g 是乘法群 G 的生成员, G 上求离散对数难. $|G|=P$, x_i 为私钥, $y_i=g^{x_i}$公钥, $y=y_1y_2\cdots y_k$, $i=1,2,\cdots k$,于是有 $y=g^{(x_1+x_2+\cdots x_k)}$.

对 M 的签字过程:随机选取 $t\in_R(0,m)$,计算 $r=g^t$, $s=(h(M)-(x_1+x_2+\cdots+x_k)\,r)\,t^{-1}$,$(r\parallel s)$ 为对 M 的签字.

验证过程: $y^r r^s=g^{h(M)}$.

定理　广义 ElGamal 签字与 ElGamal 签字具有相同的安全性.

证明　令 $x=(x_1+x_2+\cdots+x_k)$, $y=y_1y_2\cdots y_k=g^{(x_1x_2\cdots x_k)}=g^x$,由于 $x_1, x_2, \cdots, x_k$是用户的秘密信息,所以 x 也是用户的秘密信息; $y_1, y_2, \cdots, y_k$ 是公开的,于是 y 也是公开的.那么广义 ElGamal 签字与已知私钥为 x,公钥为 (g, y) 的 ElGamal 签字相同,即它们具有相同的安全性.

2.2　系统初始化

假定银行 bank、信任机构 TTP(third trust party)、支付者 payer、接受者 payee 各自的计算机通过 Internet 互联.

(1)银行的初始化

银行:
(a)随机选择大的安全素数 p, q,计算 $n=p*q$, $\phi(n)=(p-1)*(q-1)$;
随机选择 $0<e<n$,计算 $d=e^{-1} \bmod \phi(n)$;
(b)选择群 G, $|G|=P$ 是素数, g 是生成元,使得在 G 上求离散对数困难;
(c)选择安全 hash 函数 $h(\cdot)$.

银行公布 $(n, e; G, g)$ 和 $h(\cdot)$

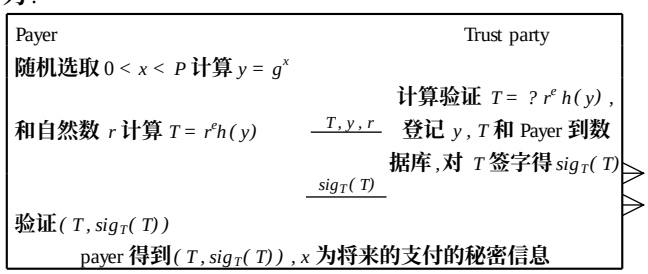
(2)可信任机构的初始化

选择签字体制,生成自己的公私钥 (S_T, P_T),公布签字验证公钥 P_T.

3　基本协议描述

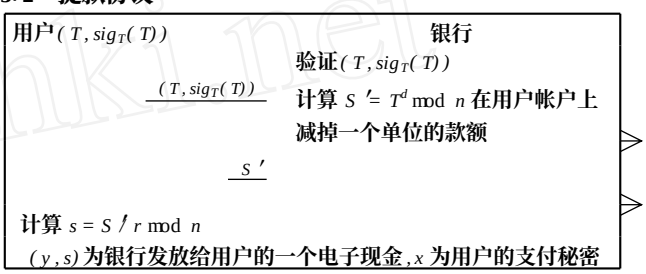
3.1　信任符 T 的申请协议

用户 payer 在信任机构注册,记录包括银行帐户等足够信息以备将来能追踪到用户 payer.申请一个信任符 T 的协议为:



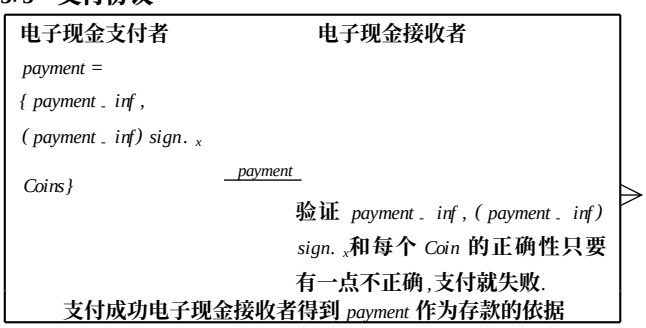
我们只描述了申请一个 T 的情形.事实上,很容易扩展的一次申请多个 T 的情形.

3.2　提款协议



(y, s) 为一电子现金,满足 $s^e=h(y) \bmod n$,其中 $y=g^x$, x 为用户的支付秘密.当然用户利用多个 T 可以一次申请多个 (y, s).

3.3　支付协议



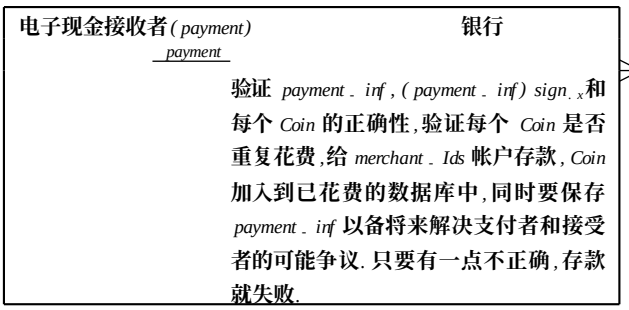
$(m)\,sign._x$ 代表对 m 的广义 ElGamal 签字.

假定电子现金支付者和接收者商定了支付银行 *bankID*、支付金额 *amount*、币种 *currency*、电子现金数量 *nCoins*、时戳 *timestamp*、接收者身份 *merchant_Ids* 与其银行帐户对应,交易描述 *description* 以备将来解决支付者和接收者的可能争议.

$payment\_inf=\{bankID, amount, currency, nCoins, timestamp, merchant\_Ids, H(description)\}$

具体算法如上表.

3.4 存款协议



3.5 追踪协议

从理论上讲追踪分为两种:已知电子现金 (y,s) 找出它的申请者,称它为向后追踪;已知申请者 payer 找出他申请的所有电子现金称为向前追踪.

3.5.1 向后追踪 政法部门有时要了解某笔交易的真相,如防止洗黑钱等,或者是要找出重复花费者时想发现它的申请人,此时他知道 (y,s),通过把 (y,s) 递交给可信赖机构查寻数据库,即可找出对应申请者 payer.

3.5.2 向前追踪协议 当需要追踪某个用户申请到的电子现金时,如该用户被敲诈,要追回被敲诈的电子现金.按照法律程序由银行和信任机构配合,通过查找各自的数据库即可得到他特定时间申请到的电子现金 (y,s).

4 系统特性和安全性分析

系统的优点是用户申请电子现金时 TTP 脱线,支付时银行脱线,提高了效率;支付和存款的通信与计算复杂度与 eCash™基本相同,对合法用户而言,具有与已有的在线完全匿名的电子现金系统相同的效率.系统的缺点是为了实现可追踪性,TTP 要维护与银行相同数量级的数据库.

系统的安全是建立在 hash 函数、RSA 公钥体制以及乘法群 G 上求离散对数难度之上的.

用户支付匿名性是电子现金系统的基本要求,本系统的电子现金形式是 $\{g^x, h^d(g^x)\}$,d 为银行的秘密钥,r 是用户的秘密随机数,银行单独无法建立 $h(g^x)r^e$ 与 $\{g^x, h^d(g^x)\}$ 的对应,以及用户和 coin 的对应,支付时用户对银行是完全匿名的,银行不能跟踪用户窥探用户的个人隐私.

伪造电子现金是不可能的,其难度相当于攻破 TTP 的签字体制、RSA 公钥体制、hash 函数 $h(\cdot)$ 或求的乘法群 G 上的离散对数.

可追踪非法用户、非法者不能敲诈用户,TTP 保存有 $(g^x$,用户$)$,给定 $\{g^x, h^d(g^x)\}$,TTP 随时能通过 g^x 找到它的申请者;给定用户 TTP 能找到他申请的所有电子现金.用户想得到完全不可追踪的电子现金,要伪造 TTP 签字的 trustee token,相当于攻破 TTP 的签字算法;或者伪造银行的 RSA 签字.

他人获得合法用户的电子现金不可盗用、银行与用户之间发生重复花费的争议时可仲裁,x 是用户秘密信息,别人无法对 payment_inf 签字,即使看到 $\{g^x, h^d(g^x)\}$ 也不能进行支付,其难度是求乘法群 G 上的离散对数.

5 结束语

简便有效、实用是新技术推广的一个重要前提,虽然近年来学术界提出了很多的电子现金方案,有在线的、脱线的、完全匿名的、可撤消匿名的、可分的、可传递的等等.我们认为目前最有效的实现可控制匿名的电子现金方案是 Ari Juels,1999 年提出的由 TTP 向用户发放"信任标志"(trustee token)的思想,"trustee token"是 TTP 的承诺,用来实现可控制匿名,可加在现有的完全匿名的电子现金系统的顶部,构成可控制匿名的电子现金系统.本文给出了基于 eCash™的用 trustee token 思想实现的脱线的可控制匿名的系统,我们的电子现金形式与 eCash™不同,从而克服了 eCash™的两个缺点:(1)他人获得合法用户的电子现金可盗用;(2)银行与用户之间发现电子现金是否被重复花费的争议时无法仲裁.同时对合法用户来说使用效率和复杂度与 eCash™基本相同.这样我们的系统有很强的实用性,当然实现时具体细节要进一步完善,如安全参数的选定,乘法群 G 的选择,对 g^x 取 hash 是否要填充,如何填充等要具体分析研究.

参考文献:

[1] http://www.ecashtechnologies.com.

[2] D Chaum, A Fiat, M Naor. Untraceable electronic cash[A]. advances in cryptology. Proc. of Crypto'88[C]. Springer-Verlag, Berlin: Crypto, 1990. 319 - 327.

[3] T ElGamal. A public-key cryptosystem and a signature scheme based on discrete logarithms[J]. IEEE. Trans on Information Theory, 1985: 469 - 472.

[4] Donal O'Mahony. Michael Peirce, Hitesh Tewari. Electronic Payment Systems[M]. Artech House, INC. 1997.

[5] Davida G, Tsiounis Y, Moti Yung. Anonymity control in e-cash systems [A]. Financial Cryptography, First International Conference, FC'97 [C]. Springer-Verlag, Berlin: FC, 1997. 1 - 16.

[6] Ari Juels. Trustee tokens: Simple and practical anonymous digital coin tracing[A]. Financial Cryptography, FC'1999 [C]. Springer-Verlag, Berlin: FC, 1999. 29 - 45.

作者简介:

高虎明 男,1963 年 1 月生于山西省距史县,西安电子科技大学博士生,副教授,主要研究方向:密码学及其应用,电子商务和网络安全.e-mail: gaohuming@263.net

毛 剑 女,1978 年 2 月生于陕西省西安省,西安电子科技大学博士生,主要研究方向:密码学及其应用,电子商务和网络安全.

王育民 男,1936 年生于北京,西安电子科技大学教授,博士生导师,研究领域为信息理论,编码及密码理论.