可直接花费余额的电子支票系统

马春光[1,2],杨义先[1],胡正名[1],武 朋[2]
(1. 北京邮电大学信息安全中心,网络与交换国家重点实验室,北京 100876;2. 哈尔滨工程大学计算机科学与技术学院,黑龙江哈尔滨 150001)

摘 要: 首次将公平性引入电子支票中,描述了公平电子支票的模型,设计了一个可直接花费余额的公平电子支票系统. 系统使用基于 RSA 的部分盲签名技术实现了余额的直接花费,使用一个被动的 TTP 进行匿名撤销.

关键词: 密码学; 电子支票; 匿名撤销; 部分盲签名
中图分类号: TP309 **文献标识码**: A **文章编号**: 0372-2112 (2005) 09-1562-05

A Fair Electronic Check Systems with Reusable Refund

MA Chun-guang[1,2], YANG Yi-xian[1], HU Zheng-ming[1], WU Peng[2]
(1. *Information. Security Center, University of Posts and Telecommunications, Networking and Switching State Key Laboratories, Beijing* 100876, *China*;
2. *College of Computer Science and Technology, Harbin Engineering University, Harbin, Heilongjiang* 150001, *China*)

Abstract: The fairness is introduced to electronic check system for the first time, and the model of fair electronic check is discussed. A fair electronic check system with reusable refund is presented. In the system, the refund is reusable thanks to the RSA-based partially blind signature, and the anonymity revocation is achieved by employing a passive TTP short for trust third party. The system is efficient and meets all basic security requirements.

Key words: cryptography; electronic check; anonymity revocation; partially blind signature

1 引言

电子支票系统是比基于货币的电子现金系统(Coin-Based e-Cash System,简称电子货币)更有效的电子现金系统,最早由 Chaum[1,2]提出,它的设计初衷是集中物理现金的匿名性和物理支票的可精确花费性. 在电子支票系统中,用户用一张单一的支票来购买商品,然后得到具有支票面值和商品价格差价的余额. 只要商品的价格低于支票的面值,用户就可以用此支票进行支付,并且支付时的花费不依赖于支付金额.

最有效的电子现金系统应该具有这样的特征,即完成一次完整的交易,需要最少的取款次数和支付最少数目的货币. 为完成一次支付,电子货币系统[3,4]通常需要多次取款(因为一次取款只能提取一种面值的不可分货币),可分电子现金系统[5~8]和电子支票系统都只需要一次取款. 在支付时,电子货币系统和可分电子现金系统所支付的货币数量依赖于所购商品的金额,而电子支票每次购物只需支付一个支票. 可见,电子支票较其他的电子现金系统有着潜在的优势. 但是,对它的研究并没有电子货币和可分电子现金那么普遍,这是因为为电子支票系统(特别是离线系统)设计有效的可直接花费余额的机制是困难的. 在当前的电子支票系统[1,2,9~13]中,可以直接花费余额的离线电子支票系统还没有,在线系统中也只有 Chaum[1]系统和 Kim[13]系统可以直接花费余额. 其中 Chaum[1]系统的余额被限制在几种固定金额,使用有一定不便,Kim[13]系统的余额没有这种限制,并且当用户与一个商家进行多次交易时,银行可以离线,可行性和效率有了提高. 电子现金作为一种有效的支付手段,匿名性是最基本的安全要求,但是它也为敲诈、绑架、洗钱等完美犯罪[14]带来了便利. 完全匿名的电子现金系统是政府和银行不能接受的这障碍了电子现金的应用. 所以,近些年来密码学家们对可控匿名性(或称为公平性)进行了大量的研究,但是这些研究都是集中在电子货币系统[15~18]和可分电子现金系统[19]上,对电子支票的匿名控制问题在公开文献中还没有看到,当前的电子支票系统也都是完全匿名的. 本文首次将可控匿名的概念引入电子支票,讨论了公平电子支票模型,基于被动的可信第三方(TTP),应用部分盲签名技术设计了一个有效的可直接花费余额的公平电子支票系统,并对系统的安全性进行了分析. 本文的结构是:第 2 节讨论了公平电子支票模型,第 3 节对部分盲签名进行了介绍,第 4 节详细叙述了可直接花费余额的公平电子支票系统,第 5 节对系统的安全性行了分析,最后是总结和进一步的工作.

2 公平电子支票模型

一个公平的电子支票系统包括四个主体:银行,TTP,用户和商家. 每个用户和商家在银行都有一个帐号. 一个可直接花

收稿日期:2003-09-19;修回日期:2005-05-12
基金项目:国家重点基础研究发展规划(973 计划)项目(No. 1999035804);国家自然科学基金(No. 90204017, No. 60372094);

费余额的公平电子支票有五个协议:取款协议,支付协议,存款协议,余额存储协议,匿名撤销协议(包括支票追踪和用户追踪).

用户通过取款协议从银行提取电子支票,然后通过支付协议将电子支票支付给商家并得到相应的余额支票,商家可以将得到的支票通过存款协议存到自己的帐户(如果是在线系统,存款可在支付同时完成).用户执行支付后的余额可以再次通过支付协议进行支付,也可以通过余额存储协议将其直接存储到银行.在支票追踪协议中,银行将某个支票的取款视给 TTP,TTP 返回一些特殊信息,通过这些信息,银行可以在存款阶段发现这个支票.在用户追踪协议中,银行将某个支票的存款视给 TTP,TTP 返回一些特殊信息,通过这些信息,银行可以借助用户帐户数据库发现支票的拥有者.通过支票追踪协议,TTP 可以追踪可疑支票的目的地(非法货币存到谁的银行帐户),进而减少敲诈等犯罪活动.通过用户追踪协议,TTP 可以追踪可疑支票的提取者(谁从银行提取了这个支票),进而减少洗钱等犯罪活动.

公平电子支票应该具有以下性质:

(1)不可伪造性、匿名性、不可双重花费性(这是所有电子现金都有的属性);

(2)可任意精确花费性(这是电子支票区别于其他电子现金系统的本质特征);

(3)余额可直接花费性,余额不可连接性;

(4)可撤销匿名性(包括支票追踪和用户追踪),并且匿名撤销只能由 TTP 完成;

(5)TTP 安全性:TTP 只能撤消匿名,不能伪造电子现金,并且应该保护合法用户的匿名性;

本文设计了一个满足以上性质的在线的公平电子支票系统.

3　部分盲签名

部分盲签名是由 Abe 和 Fujisaki[20]提出的一种特殊的盲签名技术.部分盲签名 Sign(m, c)是对两部分消息的签名,c 被称为可见部分,是在签名生成前双方协商的,对签名者来说是可见的,m 称为致盲部分,对签名者来说是不可见的.部分盲签名可以自然地用于电子支票,m 可用来表示电子支票的序列号,c 可用来表示电子支票的面值、有效期等.Abe 和 Camenisch[21]给出了基于 RSA 和基于 DLP 的部分盲签名方案,其中基于 RSA 的部分盲签名方案如图 1 所示,本文将在取款协议中使用这个方案,以实现余额支票的直接花费.

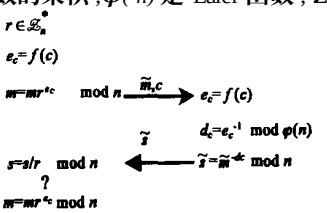

图 1　基于 RSA 的部分盲签名

方案中,n 是两个大素数的乘积,$\varphi(n)$ 是 Euler 函数,$\mathbf{Z}_n^*$ 是模 n 乘法群,r 是致盲因子,f 是公钥生成函数,e_c 是 f 以 c 为输入得到的 RSA 公钥,d_c 是对应的 RSA 私钥.部分盲签名的安全性很大程度上依赖于公钥生成函数 f,Abe 和 Camenisch[21]对于 f 的安全需求、构造方法等进行了详细的分析,指出得到满足安全需求的有效的 f 并不困难.本文不对 f 的具体构造进行讨论,假设已经选择了安全的 f,细节可参阅文献[12].

4　公平电子支票系统

4.1　系统设置

银行选择安全的 RSA 模 $n = pq$,以及合适的公钥生成函数 f,这些将用于部分盲签名,签发电子支票.银行选择另一个安全的 RSA 模 $n_b = p_b q_b$,生成 RSA 密钥对 (e_b, d_b),选择密码学安全的 Hash 函数 H.银行公开 (n, f)、(n_b, e_b) 和 H.TTP 选择安全的 RSA 模 $n_T = p_T q_T$,生成 RSA 密钥对 (e_T, d_T),公开 (n_T, e_T).用户选择安全的 RSA 模 $n_u = p_u q_u$,生成 RSA 密钥对 (e_u, d_u),公开 (n_u, e_u).商家选择安全的 RSA 模 $n_s = p_s q_s$,,生成 RSA 密钥对 (e_s, d_s),公开 (n_s, e_s).用户和商家分别将其公钥发给银行,建立帐户 acct_u 和 acct_s.

另外,系统选择一个对称加密方案(例如 DES、AES 等),确定密钥空间 K.本文中将使用两个对称密钥 K_b, K_s,分别用于用户与商家及用户与银行间的保密数据传送.

4.2　注册协议

用户和 TTP 执行图 2 所示的协议,得到追踪标记 K_T 和 TTP 对它的签名 $\mathrm{Sig}_{d_T}(K_T)$,同时,TTP 将追踪标记 K_T 和用户公钥 e_u 对应,存入数据库.

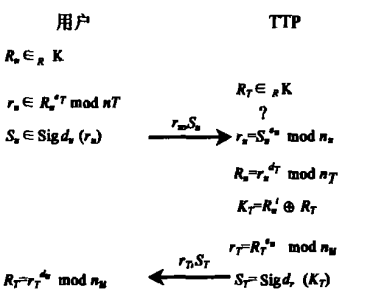

图 2　注册协议

4.3　取款协议

用户和银行执行图 3 所示的协议,完成初始电子支票的提取.协议结束时,银行从用户帐户中扣除相应金额,即从帐户 acct_u 中扣除 $c.V$.协议的实质就是用户得到银行的部分盲签名.用户将帐户 acct_u、致盲消息 $\tilde{m}$、$\mathrm{Sig}_{d_u}(\tilde{m} \| c \| T_u)$ 一起传给银行,其中 T_u 为时间戳,用于防止重传攻击;银行对致盲消息 $\tilde{m}$ 签名,并将签名 $\tilde{s}$ 传给用户;用户对 $\tilde{s}$ 脱盲,得到初始电子支票 (s, c),其中 $s = (H(K_b) \| H(K_s) \| K_T)^{d_c} \bmod n$, $c = V \| T.c.V$ 表示支票的面值,$c.T$ 表示支票的有效期;K_b 为唯一标识支票的序列号,同时也作为用户和银行的通信密钥,将用于双方间保密数据传送;K_s 是用户和商家的通信密钥,将用于双方间保密数据传送;K_T 是用户在 TTP 处注册的追踪标记,将它嵌入支票中可以在需要时完成匿名撤销.

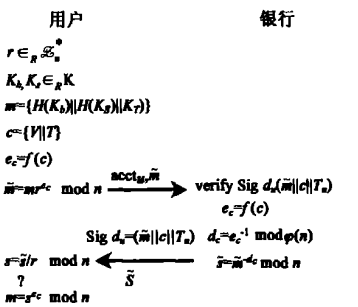

图 3　取款协议

4.4　支付协议

用户、商家、银行通过如下三轮交互协议,可以完成在线

支付.

4.4.1 第一轮交互(用户与商家) 用户进行:

(1) 选择 $r' \in_R \mathbf{Z}_n^*$, K_b', $K_s' \in_R K$;

(2) 计算 $m' = \{H(K_b') \| H(K_s') \| K_T\}$, $e_c' = f(c')$, $\tilde{m} = m' r'^{e_c} \bmod n$,这些将用于构造余额支票;

(3) 分别用银行和商家的 RSA 公钥加密 K_b 和 K_s, $k_b = K_b^{e_b}$, $k_s = K_s^{e_s}$;

(4) 计算 $t_s = \{K_T \| \mathrm{Sig}_{d_s}(K_T)\}_{K_s}$, $t_b = \{K_T \| \mathrm{Sig}_{d_S}(K_T)\}_{K_b}$;

(5) 传送初始支票 (s, c),验证数据 $(k_s, H(K_S), k_b, H(K_b), t_s, t_b)$,购买项目标识号 I 等给商家;

商家进行:

(1) 计算 $K_s = k_s^{d_s} \bmod n_s$,并用 K_s 解密 t_s;

(2) 验证支票(包括合法性、面值和有效期): $K_T \stackrel{?}{=} (\mathrm{Sig}_{d_T}(K_T))^{e_T} \bmod n_T$, $e_c = f(c)$, $m = \{H(K_b) \| H(K_s) \| K_T\}$, $m \stackrel{?}{=} s^{e_c} \bmod n$, $c.V \stackrel{?}{\geq} \mathrm{price}_s$, $c.T \stackrel{?}{\leq} \mathrm{CurrentDate}$;其中 CurrentDate 表示当前日期.

(3) 生成购买项目的加密密钥: $K' \in_R K$, $K_I = K' \oplus K_S$;

(4) 生成收据: $\mathrm{Receipt} = \mathrm{Sig}_{d_u}(\{\mathrm{item}\}_{K_I} \| I \| \mathrm{price}_s \| s)$;

(5) 传送加密项目 $\{\mathrm{item}\}_{K_I}$ 和收据 $\{\mathrm{Receipt}$ 给用户;

用户进行:

(1) 验证收据 Receipt;

(2) 构造余额请求 $O_u = \{\mathrm{price}_u \| \mathrm{acct}_s \| \tilde{m}\}_{K_b}$,并将其传给商家;

4.4.2 第二轮交互(商家与银行) 商家进行:

(1) 构造存款请求 $O_s = \mathrm{Sig}_{d_s}(\mathrm{price}_s \| s)$;

(2) 传送 (s, c)、$(k_b, H(K_s), t_b)$、O_u、O_s、price_s、acct_s 给银行;银行进行:

(1) 计算 $K_b = k_b^{d_b} \bmod n_b$,并用 K_b 解密 t_b;

(2) 验证支票: $K_T \stackrel{?}{=} (\mathrm{Sig}_{d_T}(K_T))^{e_T} \bmod n_T$, $e_c = f(c)$, $m = \{H(K_b) \| H(K_s) \| K_T\}$, $m \stackrel{?}{=} s^{e_c} \bmod n$, $c.T \stackrel{?}{\geq} \mathrm{CurrentDate}$;

(3) 以支票序列号 K_b 为关键字在存储已花费支票的数据库中查找,如果没有重复花费,存储花费记录: $(s, c, K_b, \mathrm{acct}_s, \mathrm{Sig}_{d_T}(K_T))$;

(4) 验证 O_u、O_s,并验证 $\mathrm{price}_u + \mathrm{price}_s \stackrel{?}{=} c.V$.

(5) 对余额支票进行盲签名: $c''.V = c.V - \mathrm{price}_s$, $c''.T = c.T$, $c' = c''.V \| c''.T$, $e_c' = f(c')$, $d_c' = e_c'^{-1} \bmod \phi(n)$, $\tilde{s} = \tilde{m}^{d_c'}$;

(6) 构造支付证书: $\mathrm{PayCert} = \mathrm{Sig}_{d_b}(\mathrm{price}_s \| \mathrm{acct}_s \| s)$;

(7) 存储相应金额 (price_s) 到商家帐户 (acct_s),并将盲签名 $\tilde{s}$ 和支付证书 PayCert 传送给商家;商家验证支付证书 PayCert.

4.4.3 第三轮交互(商家与用户) 商家将银行的盲签名 $\tilde{s}$ 和 K 传给用户.

用户进行:

(1) 脱盲得到余额支票 (s', c'): $s' = \tilde{s} / r' \bmod n$, $m' \stackrel{?}{=} s'^{e_c'}$;

(2) 计算密钥 $K_I = K_S \oplus K'$,解密 $\{\mathrm{item}\}_{K_I}$ 得到所购项目 item.

4.5 余额存储协议

如果用户在有效期内没有花费原始支票或余额支票,或者由于其他原因以后不想花费支票,那么它可以通过如下的交互协议直接将未花费的支票存储到自己的帐户.

用户:

(1) 构造存储请求: $R_u = \{\mathrm{acct}_u \| c \| K_S \| K_T \| \mathrm{Sig}_{d_T}(K_T)\}_{K_b}$;

(2) 用银行的 RSA 公钥加密支票序列号: $k_b = K_b^{e_b} \bmod n_b$;

(3) 传送 (k_b, R_u, s) 给银行;

银行:

(1) 计算 $K_b = k_b^{d_b} \bmod n_b$,并用 K_b 解密 R_u;

(2) 验证支票: $K_T \stackrel{?}{=} (\mathrm{Sig}_{d_T}(K_T))^{e_T} \bmod n_T$, $e_c = f(c)$, $m = \{H(K_b) \| H(K_s) \| K_T\}$, $m \stackrel{?}{=} s^{e_c} \bmod n$, $c.T \stackrel{?}{=} \mathrm{CurrentDate}$;

(3) 检查双重花费,存储记录 $(s, c, K_b, \mathrm{acct}_u, \mathrm{Sig}_{d_T}(K_T))$;

(4) 存储 $c.V$ 到用户帐户 acct_u;

(5) 构造存款证书 $\mathrm{DepCert} = \mathrm{Sig}_{d_b}(c.V \| \mathrm{acct}_u \| s)$,并传送给用户用户验证存款证书 DepCert,完成存储.

4.6 匿名撤销协议

4.6.1 支票追踪

(1) 银行构造追踪请求 $O_b = (e_u \| \mathrm{Sig}\, d_b(e_u))^{e_T} \bmod n_T$ 并传送给 TTP;

(2) TTP 首先解密 O_b,并验证签名,然后在其数据库中查找与 e_u 对应的追踪标记 K_T,生成追踪证书 $\mathrm{TraceCert} = \mathrm{Sig}_{d_T}\{K_T \| e_u\}$;

(3) TTP 计算 $k_T = K_T^{e_b} \bmod n_b$,并将 k_T、TraceCert 一起传给银行;

(4) 银行解密 k_T,得到 K_T,并验证 TraceCert;

(5) 银行通过 K_T 在存款数据库(即已花费支票数据库)中找到对应的电子支票.

4.6.2 用户追踪

(1) 银行构造追踪请求 $O_b = (K_T \| \mathrm{Sig}_{d_b}(K_T))^{e_T}$,并传送给 TTP;

(2) TTP 首先解密 O_b,并验证银行签名,然后在其数据库中查找与追踪标记 K_T 对应的 e_u,生成追踪证书 $\mathrm{TracCert} = \mathrm{Sig}_{d_T}\{K_T \| e_u\}$;

(3) TTP 计算 $E = e_u^{e_b} \bmod n_b$,并将 E、TracCert 一起传给银行;

(4) 银行解密 E,得到 e_u,并验证 TracCert;

5 安全性分析

本系统的安全性基于三个假设:RSA 签名体制的安全性、基于 RSA 的部分盲签名的安全性、Hash 函数 H 的安全性.

不可伪造性 因为只有银行知道 n 的素数分解,所以伪造合法的电子支票是不可行的.另外,只要 RSA 签名体制是安全的(可以抵抗选择明文攻击),通过与银行执行 k 次取款

协议,得不到 k 个以上的合法电子支票.

匿名性　只要基于 RSA 的部分盲签名是安全的,取款用户的匿名性就可以保持.

不可双重花费性　系统中的电子支票是关于 $m = \{H(K_b) \| H(K_s) \| K_T\}$ 的签名.如果用户可以找到不同的两组数据 $(K_b, K_s) \neq (K_b, K_S')$,满足 $H(K_b) \| H(K_S) = H(K_b) \| H(K_S')$,则用户就可以双重花费电子支票.但是,Hash 函数的安全性(单向、无碰撞)使得这是不可行的.另外,因为我们的系统是在线系统,所以其他形式的双重花费可由银行在支付时立即发现.

可任意精确花费性　我们采用 RSA 部分盲签名将面值作为可见部分嵌入电子支票中,只要所购项目的价格不大于支票面值,用户就可以用此支票在支付协议中实现精确花费,并得到相应余额支票.

余额可直接花费性　在我们的系统中,余额支票和初始支票具有相同的结构,所以对支付双方(用户和商家)来讲,余额支票可以与初始支票一样直接用于支付.

余额不可连接性　余额支票和原始支票的序列号(K_b、K_b')是用户在不同时间随机选取的(K_b 在取款时选取,K_b' 在支付时选取),二者在统计上是无关的,所以余额支票和原始支票是不可连接的.同样的原因,同一用户提取的不同初始电子支票也是不可连接的.

可撤销匿名性　在需要的时候,银行可以向 TTP 提出支票追踪或用户追踪请求,从而撤销匿名.追踪协议中,追踪请求 O_b 和追踪结果都以密文的形式(分别用 TTP 的 RSA 公钥和银行的 RSA 公钥加密)传送,这保证了双方间的保密通信.另外,只有 TTP 掌握追踪标识 K_T 和用户公钥 e_u 的对应关系,并且每次追踪银行都得到 TTP 颁发的追踪证书 TracCert,所以除了 TTP 外的任何人都不能进行匿名撤销或假冒 TTP 与银行执行追踪协议.关于匿名撤销,一个问题是,如果用户进行支票余额存储,则在其向银行提交的存储请求 R_u 中包含了其帐号 acct_u 和追踪标记 K_T,这样银行结合开户时得到的用户公钥与帐号的对应关系 (e_u, acct_u),就可以"部分的"撤销了用户的匿名性.对这个问题一个折衷的办法是,在在支付时,将"很小的"余额先"保存"在商家,由商家给用户开据"零头收据".当零头积累到一定数目时(可以进行一次支付),可以在另一次的支付时,花费到商家.这个解决办法的关键是,在进行"零头积攒"的过程中,如何保证这些零头的不可连接性.我们认为,对此问题更本质的一个解决办法是,在余额存储时用户可以向银行以零知识的方式证明余额支票中已嵌入了"正确"的追踪标记 K_T,细节问题将是我们下一步的研究内容.

TTP 安全性　TTP 不能伪造电子支票,因为它既不知道 n 的素分解也不能打破 RSA 签名体制.另外,匿名撤销需要银行和 TTP 共同参与,所以,除非银行和 TTP 勾结,否则合法用户的匿名性会得到保持.另外,我们的系统有这样一个特点:在取款时用户不需要向银行证明电子支票中嵌入了追踪标记 K_T,但是,在支付时没有正确嵌入追踪标记的支票将被视为非法支票而不被接受.利用这个性质,我们可以对系统稍加改动,以便更大程度上保护诚实用户的匿名性.具体做法是:

(1)银行以适当的方式定期公布不诚实用户的黑名单;

(2)取款时,不在黑名单中的用户不用将追踪标记嵌入电子支票中;

(3)支付时,商家和银行先检查黑名单.如果用户在黑名单中,那么没有嵌入追踪标记的支票将被视为非法支票,而没有在黑名单中的用户则只需要证明支票构造的正确性就可以.

这样,对诚实用户的匿名性是无条件保持的,而对于不诚实用户(在黑名单中)的匿名性总是可以撤销.另外,如果诚实用户受到敲诈,他可以在取款时主动地将追踪标记嵌入支票中,这样在支付时银行便会实时地检测到追踪标记.

6　结束语

本文将公平性引入电子支票,并设计了一个基于被动 TTP 的公平电子支票系统,这使得电子支票系统更加实用,更能被政府和银行接受.另外,系统支持余额的直接花费和存储,这方便了用户的使用.系统中使用对称加密体制进行保密消息的传送,这提高了系统的效率.

系统的一个缺点是,当进行支票追踪时,银行可以追踪到此用户所有的支票(甚至是以后要提取的),而不单单是一次交易的支票,这对银行和政府来说是欢迎的,但对用户来说是对匿名性的一种侵犯.一种改进的方法是,用户定期向 TTP 注册新的追踪标记,这样可以避免对以后提取的电子支票的滥用追踪.产生这类问题的本质原因是由于系统假设 TTP(一般是政府和法律部门)是可信的,而如果 TTP 是不诚实的(尽管这种情况很少),他和银行勾结就可以滥用匿名撤销,所以更彻底的解决方法是设计不使用 TTP(例如基于审计机制)的公平电子支票系统,这将是我们进一步的研究内容.另外,设计一个公平的可直接花费余额的离线电子支票系统也是我们所感兴趣的.

致谢:特别感谢审稿老师认真细致的审阅,以及编辑老师辛劳的工作.

参考文献:

[1] Chaum D. Online cash checks[A]. Proceedings of EuroCrypt '89[C]. Germany: Springer-Verlag, 1990. 288 - 293.

[2] Chaum D, Boer B, Heyst E, Mjolsnes S, Steenbeek A. Efficient offline electronic checks[A]. Proceedings of EuroCrypt '89[C]. Germany: Springer-Verlag, 1990. 294 - 301.

[3] Chaum D, Fiat A, Naor M. Untraceable electronic cash[A]. Proceedings of Crypto '89[C]. Germay: Springer-Verlag, 1990. 319 - 327.

[4] Brands S. Untraceable off-line cash in wallets with observers[A]. Proceedings of Crypto '93[C]. Germany: Springer-Verlag, 1993. 302 - 318.

[5] Okamoto T, Ohta K. Universal electronic cash[A]. Proceedings of Crypto '91[C]. Germany: Springer-Verlag, 1993. 324 - 337.

[6] Okamoto T. An efficient divisible electronic cash scheme[A]. Proceedings of Crypto '95[C]. Germany: Springer-Verlag, 1995. 438 - 451.

[7] Chan A, Frankel Y, Tsiounis Y. Easy come-easy go divisible cash[A]. Proceedings of EuroCrypt '98[C]. Germany: Springer-Verlag, 1998. 561

- 575.
[8] Nakanishi T, Sugiyama Y. Unlinkable divisible electronic cash[A]. Proceedings of ISW2000[C]. Germany: Springer-Verlag, 2000. 121 - 134.
[9] Brands S. An efficient of-line electronic cash system based on representation problem[R]. Netherlands: CWI, 1993. CS - R9323.
[10] Hirschfeild R. Making electronic refunds safer[A]. Proceedings of Crypto '92[C]. Germany: Springer-Verlag, 1993. 106 - 112.
[11] Solage A, Traore J. An efficient fair off-line electronic cash system with extensions to checks and wallets with observers[A]. Proceedings of FC '98[C]. Germany: Springer-Verlag, 1998. 275 - 295.
[12] Deng R, Han Y, Jeng A, Ngair T. A new on-line cash check scheme[A]. Proceedings of 4th ACM Conference on Computer and Communication Security[C]. USA: ACM Press, 1997. 111 - 116.
[13] Kim S, Oh H. A new electronic check system with reusable refund[J]. International Journal of Information Security, 2002, 1(3): 175 - 188.
[14] Solms von B, Naccache D. On blind signature and perfect crimes[J]. Computer and Security, 1992, 11(6): 581 - 583.
[15] Frankel Y, Tsiounis Y, Yung M. Indirect Discourse Proofs: Achieving Efficient Fair Off-Line E-Cash[A]. Proceedings of AsiaCrypt '96[C]. Germany: Springer-Verlag, 1996. 16 - 30.
[16] Camenisch J, Maurer U, Stadler M. Digital Payment Systems with Passive Anonymity-Revoking Trustees[A]. Proceedings of ESORICS '96[C]. Germany: Springer-Verlag, 1996. 33 - 43.
[17] Davida G, Frankel Y, Tsiounis Y, Yung M. Anonymity Control in E-Cash Systems[A]. Proceedings of FC '98[C]. Germany: Springer-Verlag, 1998. 1 - 16.
[18] Jacbosson M, Yung M. Revokable and versatile electronic money[A]. Proceedings of 3rd ACM Conference on Computer and Communication Security[C]. USA: ACM press, 1996. 76 - 87.
[19] Tsiounis S Y. Efficient electronic cash: new notions and techniques[D]. USA: Northeastern University, 1997.
[20] Abe M, Fujisaki E. How to date blind signatures[A]. Proceedings of AnsiaCrypt '96[C]. Germany: Springer-Verlag, 1996. 244 - 251.
[21] Abe M, Camenisch J. Partially blind signature schemes[A]. Proceedings of 1997 Symposium on Cryptography and Information Security[C]. SCIS97-33D, Fukuoka, Japan, 1997.

作者简介:

马春光 男,1974 年 1 月出生于黑龙江省双鸭山市,现为哈尔滨工程大学计算机科学与技术学院副教授,北京邮电大学信息安全中心在读博士. 主要研究方向为密码学、信息安全、网络安全、电子支付等. E-mail: cgma@163.com.

杨义先 男,1961 年 3 月生于四川盐亭,博士,教授,北京邮电大学博士生导师,全国政协委员,国家有突出贡献的中青年专家,首届政府特殊津贴获得者,主要研究方向为密码学、网络安全、信息安全、信号与信息处理等. E-mail: yxyang@bupt.edu.cn.