无可信第三方的离线电子现金匿名性控制

李梦东[1],杨义先[2,3]

(1. 北京市丰台区富丰路 7 号,北京电子科技学院电子信息工程系,北京 100070;
2. 北京邮电大学信息安全中心 126 信箱,北京 100876;3. 北京邮电大学网络与交换国家重点实验室,北京 100876)

摘 要: 利用可信第三方的电子现金匿名性撤销方案增加了系统负担,并且可信第三方的跟踪是不确定的. 最近 Kulger 等提出了无可信第三方的可审计跟踪的电子现金方案,但需要用户事后审计检查. 结合 Camenisch 等的加标记跟踪及证明方法和 Abe 等部分盲签名方案,本文提出了一个无可信第三方的电子现金匿名性控制方案. 方案中银行只在需要跟踪时要求用户打开标记,从而进行用户和钱币的跟踪,这样跟踪时用户是知道的,因此简便实用地解决了无可信第三方情况下电子现金匿名性控制问题.

关键词: 电子现金; 匿名性控制; 限制性盲签名; 部分盲签名

中图分类号: TP309 **文献标识码**: A **文章编号**: 0372-2112 (2005) 03-0456-03

Revocable Anonymous Off-Line E-Cash Scheme Without TTP

LI Meng-dong[1], YANG Yi-xian[2,3]

(1. *Dept. of Electronic Information Engineering, Beijing Electronic Science and Technology Institute, Beijing* 100070, *China*;
2. *Information Security Center, Beijing Univ. of Posts and Telecomm., Beijing* 100876, *China*;
3. *State Laboratory of Networking and Switching, Beijing* 100876, *China*)

Abstract: The E-cash schemes that are revocable anonymous with the help of trusted third party cause additional costs and the level of anonymity is uncertain. Kulger *et al* adopted auditable tracing to control deanonymization without trusted third party (TTP), but the users have to audit the tracing frequently. Combining Camenisch *et al*'s method of inserting mark with proof and Abe *et al*'s partial blind signature, a new revocable anonymous off-line E-cash scheme without TTP is proposed. In this scheme the bank demands users to decrypt the mark of the coin when tracing is needed so that the user and coin can be linked together and then user is certain about tracing. So the scheme resolves the problem of the E-cash anonymity control without TTP simply and practically.

Key words: E-cash; anonymity control; restrictive blind signature; partial blind signature

1 引言

无条件匿名性的电子现金方案为"完美犯罪"提供了可乘之机,为此研究者引入了可信第三方[1~3],并强迫用户的加密信息中加入可信第三方(TTP)的跟踪公钥,用来认证取款协议或钱币,以便 TTP 利用陷门消息能够将存款协议和取款协议联系起来,从而实现用户或者钱币的跟踪. 这些协议一般是以 Schnorr 盲签名方案或 Brands 方案为基础,试图在用户的匿名性和认证性之间达到某种平衡或者说公平性[1,2].

但是 TTP 的加入增加了系统的负担,而且匿名性的控制程度是不确定的,也就是说 TTP 的跟踪是没有限制和不被检查的. 最近 Sander 等[4,5]提出不需 TTP 参与的可审计(Auditing)的电子现金方案,根据公共成员关系证明,保证银行的可审计性,同时保证用户的无条件匿名性. 由于不是基于盲签名的,因此不存在密钥的保护问题,可防止银行抢劫和敲诈行为. 但目前该方案并不实用,并且不能进行钱币或所有者跟踪. Kugler[6]在 Camenisch[1]基于盲签名的方案基础上,利用可审计跟踪方式取代了基于 TTP 的跟踪. 该方案中银行总是能够跟踪用户和钱币,但不合法的跟踪会被用户在其后的某个时间检查出来(即审计),这样就约束了银行的行为. 该协议是高效的,但存在的问题是用户必须不断做审计检查,这无疑增加了用户的负担.

本文提出一种不需 TTP 的电子现金匿名性控制方案. 该方案取款时用户将电子现金的秘密值加密作为标记,和其有效性证明一起交给银行,这样做并不失去匿名性. 需要跟踪时银行要求用户解密标记,由于用户身份与标记是相联系的,银行便可以跟踪到用户支付的现金;为了实现所有者跟踪,银行采用部分盲签名,使电子现金保持一个非盲的时间戳,只需要这个时间戳范围内取款的用户打开标记,撤销其电子现金的匿名性. 这样银行的跟踪是明确的,而用户又可保持一定的匿名性,因此简单实用地解决了无 TTP 的电子现金匿名性控制问题.

2 基本工具

2.1 限制性盲签名和已知离散对数的知识证明

Brands[7]采用限制性盲签名的方法,在盲签名中嵌入身份,用以实现防止重复花费. 为了能够撤销匿名性,Camenese[1]方案在文献[7]基础上增加了标记 d,采用 TTP 的跟踪公钥作为指数运算的底,并给出标记的一个知识证明;

收稿日期:2003-11-17;修回日期:2004-06-19
基金项目:国家"973"项目(NO. G1999035804);国家自然科学基金项目(No. 60372094,90204017)

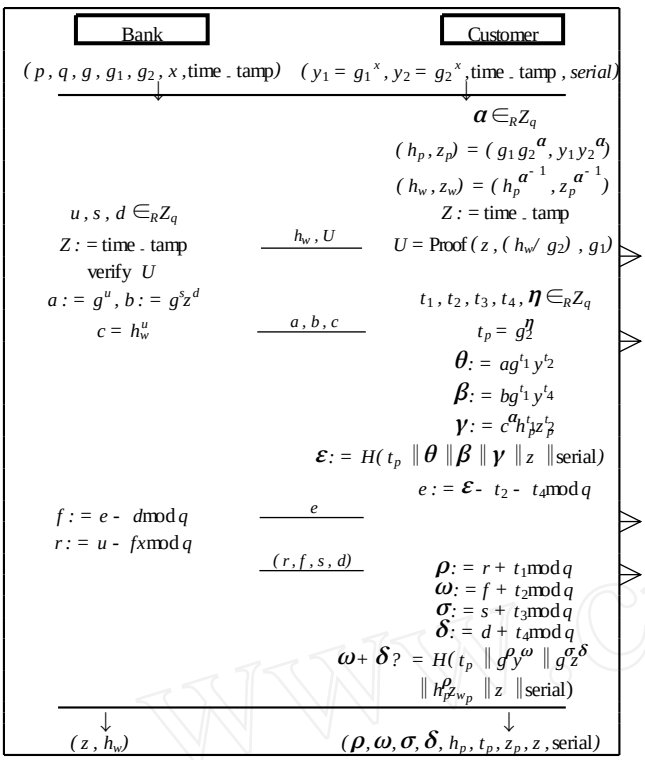

图 1　取款协议

Kulger[6]为了不使用 TTP,采用银行选择跟踪公钥作为标记的底,用户事后审计;我们的方案是用户选择标记的底,且仅利用如下简单的已知离散对数的知识证明方案[1].

如果证明者知道群成员 h 以 g 为底的离散对数 x,他随机选一个 r,作如下证明 PROOF,证明是诚实验证者零知识的. 其中 $H:\{0,1\}^* \rightarrow Z_q$ 是单向 hash 函数.

$$c = H(m \| g \| h \| g^r),\ s = r - cx$$

$$\mathrm{PROOF}(m, g, h) = (c, s),\ c = H(m \| g \| h \| g^s h^c)$$

2.2　WF-Schnorr 部分盲签名方案

Abe 等在文献[8]中提出 WF-Schnorr 部分盲签名方案,是基于离散对数困难问题,并在随机预言模型下证明了该方案是证据不可分辨的知识证明,满足不可伪造性和部分盲性. 具体协议详见文献[8].

3　本文方案

3.1　系统建立

设 p, q 是两个大素数,且 $q \mid p-1$, g 是 Z_p^* 的一个阶为 q 的元素, $G = \langle g \rangle$ 是 g 生成的 Z_p^* 的子集,并假设在 Z_q 解 $\log_g h$ 是困难的. 银行选择 G 中元素 g_1, g_2,选择签名私钥 $x \in_R Z_q$,计算 $y = x^x$, $y_1 = g_1^x$, $y_2 = g_2^x$. 公开 $G, p, q, g, g_1, g_2, y, y_1, y_2$.

3.2　取款协议

首先消费者向银行证明自己的身份,银行公布此时的时间戳 time_stamp,消费者交给银行一个标记 h_w,并做一个关于秘密 α 的知识证明 $U = \mathrm{Proof}(\mathrm{time\_stamp}, (h_w / g_2), g_1)$

之后银行作部分盲签名,并将 h_w 嵌入签名中.

协议结束时,电子现金即钱币为 $(\rho, \omega, \sigma, \delta, h_p, t_p, z_p, z, \mathrm{serial})$,银行记录该用户此次取款的时间戳 z 和标记值 h_w,在消费者的帐户中减去一项. 取款协议过程见图 1. 其中 t_p 作为防止重复花费之用.

3.3　支付协议

商家将 $m = \mathrm{ID\_Merchant} \| \mathrm{Counter}$(身份和计数值)交给消费者,向消费者证明自己的身份. 消费者将钱币 $(\rho, \omega, \sigma, \delta, h_p, t_p, z_p, z, \mathrm{serial})$ 交给商家,并对作一个 Schnorr 签名 c_p, s_p,商家验证钱币的有效性和签名的有效性. 商家最后得到的电子现金形式为 $:(\rho, \omega, \sigma, \delta, h_p, z_p, c_p, s_p, m, z, \mathrm{serial})$. 支付协议过程见图 2.

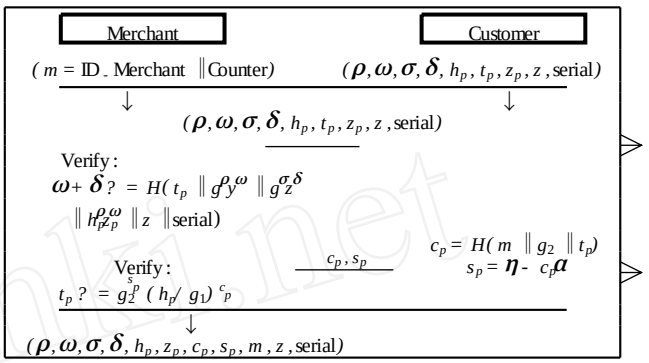

图 2　支付协议

3.4　存款协议

商家向银行证明自己的身份,将电子现金 $(\rho, \omega, \sigma, \delta, h_p, z_p, c_p, s_p, m, z, \mathrm{serial})$ 交给银行,银行与支付协议中的商家类似,检查商家身份和电子现金的有效性,检查是否重复花费即检查现金中的 (c_p, s_p) 是否重复. 如上述步骤都通过,在商家的帐户上增加一个钱币,并记录该电子现金及其时间戳. 将同一时间戳的电子现金列表存储.

3.5　匿名性撤销

(1) 当进行钱币(coin)跟踪,即由用户身份跟踪钱币时,银行根据司法部门提供的线索和凭证,确定跟踪某一消费者,则在取款协议中要求该用户提交秘密 α,银行验证 h_w 并可计算 h_p,从而在存款协议中可确定相应的电子现金;

(2) 当进行所有者跟踪,即由钱币跟踪用户身份时,银行根据司法部门的凭据,确定所需撤销匿名性的电子现金的时间戳,如时间 T. 银行要求该时间戳 T 的电子现金的取款用户打开取款时的秘密值 α,银行计算 h_p,验证 h_w 正确性后,在该时间戳 T 存款的电子现金中查找 h_p,从而确定用户和电子现金的联系,即实现该电子现金匿名性的撤销.

4　安全性和效率分析

本文协议是结合加入标记、证明机制的盲签名方案和部分盲签名方案而成的,其安全性依赖于二者的安全性,并保证了两方案的安全性互不影响. 标记及其证明的加入并不影响部分盲签名的匿名性和不可伪造性.

4.1　协议的正确性

定理 1　对于诚实的双方,取款协议中电子现金的验证方程成立.

证明　原验证方程即

$$\omega + \delta = f + d + t_2 + t_2 \pmod q = e - d + d + t_1 + t_2 \pmod q = \varepsilon$$

因此即证: $g^\rho y^\omega = a g^{t_1} y^{t_2}$; $g^\sigma z^\delta = b g^{t_3} z^{t_4}$; $h_p^\rho z_p^\omega = c^\alpha h_p^{t_1} z_p^{t_2}$;

由于 $g^{\rho}y^{\omega} = g^{r+t_1}g^{x(f+t_2)} = g^{r+xf}g^{t_1}g^{xt_2} = g^{u}g^{t_1}y^{t_2} = ag^{t_1}y^{t_2}$

$g^{\sigma}z^{\delta} = g^{s+t_3}z^{d+t_4} = g^{t_3}g^{s}z^{d}z^{t_4} = bg^{t_3}z^{t_4}$

$h_p^{\rho}z_p^{\omega} = h_p^{r+t_1}z_p^{f+t_2} = h_p^{u}h_p^{t_1}z_p^{t_2} = C^{\alpha}h_p^{t_1}z_p^{t_2}$ 证毕.

定理 2 对于诚实的双方,支付协议中消费者对于消息 m 的签名验证方程成立.

证明 $g_2^{s_p}(h_p/g_1)^{c_p} = g_2^{\eta-c_p\alpha}(g_1g_2^{\alpha}/g_1)^{c_p} = g_2^{\eta} = t_p$ 证毕.

4.2 匿名性

本文协议的匿名性依赖于文献[8]中部分盲签名方案的部分匿名性.原协议是在随机预言模型下的基于离散对数困难性,为证据不可分辨的知识证明.

与原部分盲签名相比较,本文取款协议中增加了消费者交给银行的 h_w 和证明 U,与文献[1]加入标记的情况一样,这两项并不影响原部分盲签名的性质,可保证用户在不跟踪时的匿名性.消费者在银行的记录为:(身份,时间戳 z, h_w,证明 U),银行保证标记 h_w 绑定在电子现金中.标记 h_w 不暴露取款者的秘密 α,是基于离散对数问题的;证明 U 是诚实验证者的零知识证明.因此本协议的匿名性等同于文[8]的部分匿名性.

4.3 不可伪造性

本方案是基于文[8]方案的部分盲签名的不可伪造性.文献[8]方案是在随机预言模型下基于离散对数困难问题的.本方案取款协议中银行交给取款者的 c,并不暴露银行的秘密 u,因为这是离散对数困难问题.

4.4 防止重复花费

如果重复花费发生,银行可以确定企图重复花费者的身份.对于一次取款,银行收到两对 (c_p, s_p), (c_p', s_p'),可得

$$s_p = \eta - c_p\alpha \bmod q \qquad s_p' = \eta - c_p'\alpha \bmod q$$

解方程组得 $\alpha = (s_p - s_p')/(c_p' - c_p) \bmod q$,银行可计算 $h_w = g_1^{\alpha^{-1}}g_2$,便可判断重复花费者的身份.

4.5 匿名性控制

协议中银行可以根据司法部门提供的授权,撤销用户的匿名性,并且这种跟踪或者说撤销匿名性是明确的,要求用户知晓和配合.跟踪时银行需要用户解密标记 h_w,(而不使用跟踪公钥).钱币跟踪过程为:用户提交 α,银行计算: $h_p = g_1g_2^{\alpha}$,验证 α 是否满足 $h_w = g_1^{\alpha^{-1}}g_2$,如果成立,查找存款协议中含有 h_p 的电子现金,从而确定取款者的身份.如果不成立,说明用户在欺骗;所有者跟踪过程为:银行要求某一时间戳取款的用户提交 α,银行分别计算各个 h_p,验证 α 是否满足 $h_w = g_1^{\alpha^{-1}}g_2$,如果成立,在这一时间戳内存款的电子现金中进行匹配,从而确定钱币的所有者.协议中加标记是为了防止用户冒认现金,而证明 U 保证这个标记嵌入到电子现金中.

与文献[6]相比,本文方案对用户来说跟踪是明确的,不需要事后审计检查,更符合事件调查的步骤,因此更具有公平性.如果用户拒不打开承诺,则银行和司法部门将对其采取惩罚措施.为防止用户将自己的帐户现金金额化完后,拒不打开承诺,银行可对余额做出限制.

4.6 方案效率分析

本文方案是不需要 TTP 的,因此节省了系统负担.与 Kulger[6]方案相比,本文方案省去了加入跟踪公钥过程,用户不需事后检查跟踪的合法性,只需要记录和必要时提交一个电子现金的秘密,因此比较简单实用地解决了无 TTP 的跟踪问题,提高了效率.

5 结论

本文针对文献[6]方案需要用户事后审计的问题,提出了一种无 TTP 的电子现金匿名性控制方案,结合文献[1]在电子现金加标记的方法和文献[8]部分盲签名方案,在本方案中银行根据司法部门提供的线索或凭证,可撤销某时间戳的电子现金匿名性.实际上本方案的作用是审计用户,合法用户应该提供正确的秘密.这样做的代价是:可能会使同一时间戳的一部分诚实用户失去匿名性,但这类似于司法调查方式,不失为一种实用的选择.为进一步提高跟踪效率,银行可以限制每次时间戳的电子现金数量.

参考文献:

[1] J Camenisch, U Maurer, M Stadler. Digital payment systems with passive anonymity-revoking trustees[A]. Computer Security-ESORICS'96, volume 1146 of Lecture Notes in Computer Science[C]. Berlin: Springer-Verlag, 1996. 31 - 43.

[2] G Davida, Y Trankel, et al. Anonymity control in e-cash systems[A]. FinancialCryptography-FC'97, volume of 1318 of Lecture Notes in Computer Science[C]. Berlin: Springer-Verlag, 1997. 1 - 16.

[3] Y Frankel, Y Tsiounis, M Yung. "Indirect discourse proofs": Achieving efficient fair off-line e-cash[A]. Advances in Cryptology-ASIACRYPT'96[C]. Berlin: Springer-Verlag, 1996. 286 - 300.

[4] T Sander, A Ta-Shma. Auditable, anonymous electronic cash[A]. Advance in Cryptology-CRYPTO'99[C]. Berlin: Springer-Verlag, 1999. 555 - 572.

[5] T Sander, Blind. Auditable membership proof[A]. Financial cryptography-FC'00, vol 1962 of LNCS[C]. Berlin: Springer-Verlag, 2000. 53 - 71.

[6] D Kulger, H Vogt. Off-line payment with auditable tracing[A]. Financial cryptography-FC'2002[C]. Berlin: Springer-Verlag, 2002. 42 - 55.

[7] S Brands. Untraceable off-line cash in wallet with observer[A]. Advance in Cryptology-CRYPTO'93[C]. Berlin: Springer-Verlag, 1993. 302 - 318.

[8] M Abe, T Okamoto. Provably secure partially blind signatures[A]. Advances in Cryptology-CRYPTO'2000[C]. Berlin: Springer-Verlag, 2000. 271 - 286.

[9] D Pointcheval, J Stern. Security arguments for signatures and blind signatures[J]. Journal of Cryptography, 2000, 13(3): 361 - 396.

作者简介:

李梦东 男,1964 年 9 月出生于北京市,博士,2002 年 8 月至 2004 年 7 月在北京邮电大学信息安全中心作博士后研究,现在北京电子科技学院工作,主要研究方向为密码学与信息安全.

E-mail: lmd@besti.edu.cn