一种安全公平的离线电子现金体制

徐 钊,杨义先
(北京邮电大学信息安全中心,北京 100876)

摘 要: 匿名的离线电子现金体制与实现中的现金一样,很好地保护了用户的稳私,但同时也使得司法部门难以追踪像勒索和洗钱这样的犯罪. 公平的离线电子现金体制对其进行了扩展,它允许可信方在必要时可以揭开用户的身份或追踪取出的电子钱币. 本文提出了一种电子钱币的不可伪造性和合法用户匿名性都可验证的公平离线电子现金体制.

关键词: 电子现金; 身份追踪; 钱币追踪
中图分类号: TN918 **文献标识码**: A **文章编号**: 0372-2112 (2003) 07-1078-02

A Secure Fair Off-Line E-Cash Scheme

XU Zhao, YANG Yi-xian
(Information Center, Bejing, University of Posts and Telecommunications, Beijing 10876, China)

Abstract: Anonymous off-line e-cash protects the customer's privacy as physical cash does. But it is impossible for a judge to investigate crimes such as blackmailing and money laundering. Fair off-line e-cash extends it by assigning trustees the abilities for identities revoking and coin tracing. A fair off-line e-cash scheme is proposed, in which both electronic coin's unforgeability and legitimate users' anonymity are provable.

Key words: e-cash; owner tracing; coin tracing

1 引言

匿名的离线电子现金体制是电子商务的重要组成部分,它很好地保护了用户的稳私,除非用户重复使用电子钱币,任何人无法对电子钱币进行追踪或获知用户的身份. 但这也给罪犯提供了可乘之机,例如罪犯可以勒索他人的电子钱币或进行洗钱活动. 公平的离线电子现金体制对其进行了扩展,它引入了可信方(如法院). 在一定的条件下,可信方在银行的配合下可以追踪可疑的电子钱币或揭开可疑用户的身份.

公平的离线电子现金体制是由 Y. Frankel 等[1]和 J. Camenisch 等[2]独立提出的. 后来,Y. Tsiounis 提出的公平离线电子现金体制[3]综合了文[1]和文[2]的优点,并证明了其匿名性是基于确定性 Diffie-Hellman 问题的难解性. 但以上几种体制所基于的盲签名体制的安全性都没有得到证明,因而这些体制中钱币的不可伪造性无法得到验证. 本文对 M. Abe 提出的可验证安全性的部分盲签名体制[4]加以改进,得到了可验证安全性的盲签名体制,在此基础上对文[3]中的公平离线电子现金体制进行了改进,得到了一种电子钱币的不可伪造性和合法用户的匿名性都可验证的公平的离线电子现金体制.

2 盲签名体制

设 n 为安全参数,p、q 为两个大素数,$q \mid p-1$,$g \in Z_p^*$ 且 g 的阶为 q. 设$\langle g\rangle$是 g 生成的循环群,它是 Z_p^* 的子群. H、H_1 为 hash 函数,H、$H_1: \{0,1\}^* \to Z_q$. 任选 $h \in \langle g\rangle$,rnd $\in \{0,1\}^*$. 签名者的私钥为 x,公开 g、h、y、w 和 $z = H_1(\text{rnd})$,且 $g^x = y \bmod p$,$h^x = w \bmod p$. 签名过程如下(以后计算中如无说明,都要 mod p):

(1) 签名者在 Z_q 中随机选择 u、s 和 d,计算 $a = g^u$,$b = h^u$ 和 $c = g^s z^d$,并将 a、b、c 传给用户;

(2) 用户在 Z_q 中随机选择 t、t_1、t_2、t_2、t_3、t_4,计算 $\xi = h^t$,$\zeta = w^t$,$\alpha = a g^{t_1} y^{t_2}$,$\beta = b^t \xi^{t_1} \zeta^{t_2}$,$\gamma = c g^{t_3} z^{t_4}$,$\varepsilon = H(\alpha \| \beta \| \gamma \| \xi \| \zeta \| m)$,$e = (\varepsilon - t_2 - t_4) \bmod q$. 并将 e 发送给签名者;

(3) 签名者计算 $r_1 = (e - d) \bmod q$,$r_2 = (u - r_1 x) \bmod q$,传 s、d、r_1、r_2 给用户;

(4) 用户计算 $\rho = (r_2 + t_1) \bmod q$,$\theta = (r_1 + t_2) \bmod q$,$\sigma = (s + t_3) \bmod q$,$\delta = (d + t_4) \bmod q$. 并验证 $\theta + \delta = H(g^\rho y^\theta \| \xi^\theta \zeta^\theta \| g^\sigma z^\delta \| \xi \| \zeta \| m)$ 是否成立,若是则得到签名 $(\rho, \theta, \sigma, \delta, \xi, \zeta, m)$;否则拒绝.

定理 1 该签名是盲签名体制.

定理 2 该体制是证据不可分的.

易知签名者用证据 $k(g^k = z)$ 而不用 x 进行签名时,只需修改(1)、(3):

(1′) $a = g^{r_2} y^{r_1}$,$b = h^{r_2} w^{r_1}$,$c = g^v$.

(3′) $d = (e - r_1) \bmod q$,$s = (v - dk) \bmod q$

收稿日期:2001-11-28;修回日期:2002-03-16
基金项目:国家自然科学基金(No. 90204017)

用户观察值的分布不变,因而用户无法知道签名者是用 x 还是用 k 进行签名的.

定理 3　该体制在签名的个数小于 $poly(\log(n))$ 时是不可伪造的,其中 n 是安全参数, $poly(x)$ 为 x 的多项式.

详细的证明见文[4].这里就不细述了.

3　对数相等的知识证明

对数相等的知识证明是公平的离线电子现金体制中一个基本的工具.用 $Eq\log[(A, a), G_1; (B, b), G_2]$ 来表示 $A = a^x G_1^w$, $B = b^x G_2^w$,其中, G_1、G_2 是 Z_q 的生成元.具体方法参见文[3].

类似地,用 $Eg\log[(A, g_1, g_2, g_3); (B, h_1, h_2, h_3)]$ 来表示 $A = g_1^x g_2^y g_3^z$ 和 $B = h_1^x h_2^y h_3^z$.

4　公平的离线电子现金体制

4.1　初始化

银行:选择两个大素数 p、q, $q \mid p-1$, $g \in Z_p^*$ 且 g 的阶为 q,设$\langle g\rangle$是 g 生成的循环群,它是 Z_p^* 的子群. g_1、g_2、g_3、g_4 也是$\langle g\rangle$的生成元.私钥为 x_B, H、H_1 为 hash 函数, H、$H_1: \{0,1\}^* \to Z_q$.公开 p、q、g、g_1、g_2、g_3、g_4 和 H、H_1,以及公钥 $y = g^{x_B} \bmod p$, $h_1 = g_1^{x_B} \bmod p$, $h_2 = g_2^{x_B} \bmod p$, $h_3 = g_3^{x_B} \bmod p$, $h_4 = g_4^{x_B} \bmod p$, $z = H_1(rnd)$, $rnd \in \{0,1\}^*$.

可信方:私钥为 x_T,公钥为 $f_2 = g_2^{x_T} \bmod p$, $f_3 = g_3^{x_T} \bmod p$.

用户:随机选择 $u_1 \in Z_q$,且 $g_1^{u_1} g_2 \neq 1$.银行将 $I = g_1^{u_1}$ 作为用户的身份,且用户必须向银行证明他知道 I 等于 g_1 的多少次方(用 Schnorr 身份认证体制).

4.2　取款

(1)用户随机选择 t, τ_1, $\tau_2 \in Z_q$,计算 $I' = I^{t^{-1}} g_3^{t^{-1}} g_4^{\tau_2}$, $W = h_1^{u_1 t^{-1}} h_3^{t^{-1}} h_4^{\tau_2}$, $E_1 = g_2^t f_3^{\tau_1}$, $E_2 = g_3^{\tau_1}$, $V_1 = Eq\log[(E_1, f_3), g_2; (E_2, g_3), nil]$, $V_2 = Eq\log[(g_3, I'), (g_1, g_4); (E_1, g_2), f_3; (I, I'), (g_3, g_4)]$, $V_3 = Eg\log[(I', g_1, g_3, g_4); (W, h_1, h_3, h_4)]$,这里 V_3 用来证明 I 和 W 满足关系 $W = (I')^{x_B} \bmod p$.

(2)银行验证 V_1、V_2 和 V_3,若成立,则在 Z_q 中随机选择 u、s 和 d,计算 $a = g^u$, $b_1 = (I' g_2)^u$, $b_2 = g_4^u$ 和 $c = g^s z^d$,并将 a, b_1、b_2、c 传给用户;

(3)用户在 Z_q 中随机选择 t_1、t_2、t_3、t_4、x_1 和 x_2,计算 $\xi = (I' g_2 g_4^{-\tau_2})^t$, $\zeta = (W h_2 h_4^{-\tau_2})^t$, $\alpha = a g^{t_1} y^{t_2}$, $\beta = (b_1 b_2^{-\tau_2})^t \xi^{t_1} \zeta^{t_2}$, $\gamma = c g^{t_3} z^{t_4}$, $\eta = g_1^{x_1} g_2^{x_2}$, $\varepsilon = H(\alpha \| \beta \| \gamma \| \xi \| \zeta \| \eta \| m)$, $e = (\varepsilon - t_2 - t_4) \bmod q$.并将 e 发送给银行.

(4)银行计算 $r_1 = (e - d) \bmod q$, $r_2 = (u - r_1 x) \bmod q$,传 s、d、r_1、r_2 给用户.

(5)用户计算 $\rho = (r_2 + t_1) \bmod q$, $\theta = (r_1 + t_2) \bmod q$, $\sigma = (s + t_3) \bmod q$, $\delta = (d + t_4) \bmod q$.并验证 $\theta + \delta = H(g^{\rho} y^{\theta} \| \xi^{\rho} \zeta^{\theta} \| g^{\sigma} z^{\delta} \| \xi \| \zeta \| \eta \| m)$ 是否成立,若是则得到电子钱币 $(\rho, \theta, \sigma, \delta, \xi, \zeta, m)$;否则拒绝.

4.3　付款、存款、身份追踪和钱币追踪

文[3]有详细论述.

5　安全性分析

5.1　不可伪造

由于该体制是建立在第 2 节的盲签名体制上的,所作的一些小改动并不影响其安全性.具体地讲,取款协议中第一步只是用户向银行出示的一些认证信息,以便可信方在以后可对用户身份或钱币进行追踪,真正的签名是从第二步开始的.在第三步中用户多计算的 η 也只是为了支付时使用,对用户伪造签名没有帮助.

5.2　不可重用、可追踪与合法用户的匿名性

文[3]有详细论述.

6　结束语

本文提出了一种可验证安全性的盲签名体制,并在此协议的基础上对文[3]中的公平离线电子现金体制进行了改进.与其它的公平的电子现金体制相比,新体制可以证明钱币不可伪造性和合法用户的匿名性.此外,本文的盲签名体制能安全地签出对数个(关于安全参数)签名,但我们可用同样的方法对文[5]中的盲签名体制进行改造,得到能安全地签多项式个签名的盲签名体制,并构造相应的公平离线电子现金体制.但这样的取款协议比较复杂.

参考文献:

[1] Y Frankel, Y Tsiounis, M Yung. Indirect discourse proofs: achieving fair off-line e-cash [A]. In Advances in Cryptology, Proc of Asiacrypt'96 [C]. Kyongju, South Kerea: Asiacrypt, 1996. 286 - 300

[2] J Camenisch, U Maurer, M Stadler. Digital payment systems with passive anonymity-revoking trustees [A]. In Esorics'96 [C]. Italy: Esorics, 1996. 33 - 43.

[3] Y Tsiounis. Fair off-line cash made easy [A]. In Advances in Cryptology, Proc of Asiacrypt'98 [C]. Beijing China: Asiacrypt, 1998.

[4] M Abe, T Okamoto. Provably secure partially blind signatures [A]. In Advances in Cryptology, Proc of Crypto'2000 [C]. 2000.

[5] M Abe. Asecure three-move blind signature scheme for polynomially many signatures [A]. In Advances in Cryptology: Eurocrypto'2001 [C]. 2001.

作者简介:

徐　钊　男,1968 年生于四川省蓬溪县,硕士,研究方向为密码算法和协议、电子支付等.

杨义先　男,1961 年生于四川盐亭,博士,北京邮电大学教授,博士生导师,研究方向为密码学、网络安全与信息安全等.