基于不可信赖托管者的公平电子现金 [1]

陈晓峰 王育民

(西安电子科技大学 ISN 国家重点实验室 西安 710071)

摘 要 利用 RSA 盲签名技术，给出了一种基于托管者的公平电子现金协议，重复花费者将以非常大的概率被托管者恢复出其身份．与以前协议不同的是：除非托管者与银行勾结，他无法提取用户的现金，而且托管者只能追踪银行要他追踪的现金，从而最大程度的保证了用户的隐私．该协议还可以追踪可疑的现金和用户，从而可防止和减少电子现金系统的犯罪活动——洗钱，勒索等．用户在提取现金时，托管者脱线提供服务，所以效率较高．

关键词 公平电子现金，匿名撤消，用户追踪

中图号 TN919.3

1 引 言

自从 Chaum[1] 引入电子现金概念以来，电子现金的研究已成为电子商务中的一个重要内容 [2,3]．通过电子现金人们可以在网上匿名购物，如同在超市使用货币和信用卡一样方便。一个理想的电子现金系统应具有以下的优点：

(1) 匿名性 如同现实世界，现金的使用不泄露用户的身份．

(2) 不可伪造性 用户不能伪造电子现金．

(3) 不可重复花费性 电子现金只能使用一次，重复花费将以很大的概率被发现．

(4) 可分性 电子现金可以分成更小数额的几份现金，但总金额保持不变。

(5) 可传递性 用户可以任意地将电子现金转借给别人，而不被追踪．

(6) 不可联接性 用户不同的电子现金不能被联接起来．

(7) 脱线支付 用户在支付电子现金时，商家不需要和银行进行联机验证。

最初的研究都着重于无条件匿名的电子现金，但是完全匿名的电子现金有可能被用于一些犯罪活动，如洗钱，勒索等 [4]．于是 Brickell[5] 与 Stadler[6] 分别独立地提出了基于托管者电子现金追踪的思想：在托管者的帮助下，银行可以对某特定的电子现金进行匿名撤消，从而可以防止利用电子现金的完全匿名性进行的犯罪活动。它包括两种模型：追踪现金的拥有者 (用户追踪) 及追踪用户的现金 (现金追踪)．

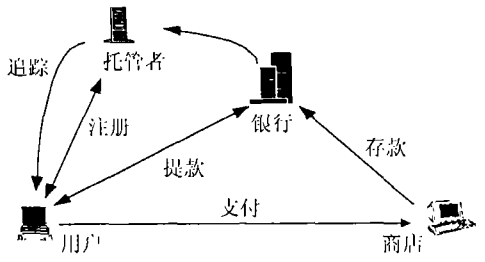

图 1 基于托管者的匿名可撤消电子现金系统

[1] 2001-03-30 收到，2001-09-10 定稿
国家自然科学基金资助课题 (60073052)

在 Brickell 与 Stadler 的协议中，都只实现了对用户的追踪，而且托管者都是在线提供服务，效率不高。后来 Camenish[7] 引入了对电子现金的追踪机制，与 Frankel[8] 分别独立地提出了公平脱线电子现金的概念，同时给出了两个方案。在他们的方案中，虽然托管者是完全脱线服务，但由于要进行复杂的模指数运算，所以效率也不高。 Juels[9] 利用一种所谓的 " trustee token " 提出了一种可行的高效的公平电子现金方案，但正如文中指出的它有两个缺点：首先是用户必须在托管方登记自己的账户，而且要存储一些认证的数据。其次，在有多个托管者的情况下，用户的隐私只能得到有限的保证。

在以前几乎所有的方案中，托管者可以无条件地实现追踪 (甚至不需要银行的协助和认可)，所以我们都假定托管者是可信赖的。但实际上我们找不到完全可信赖的第三方。为了防止恶意追踪和保护隐私，用户要求银行盲签名以实现电子现金的匿名性。但如何防止托管者的任意追踪目前尚未研究。也许采用秘密分享技术将用户的信息分配给多个托管者是一个解决的途径。但是，如何使托管者只能追踪银行或司法者要他追踪的现金仍是一个未解决的问题。

本文利用 RSA 盲签名技术，给出了一种基于托管者的公平电子现金协议。与以前协议不同的是，即使托管者与银行勾结也无法花费用户的现金，而且托管者只能追踪银行要他追踪的现金，从而最大程度的保证了合法用户的隐私。我们的协议还可以用来追踪可疑的现金和用户，从而防止和减少电子现金系统的犯罪活动——洗钱，勒索等。

本文的安排如下：在第 2 节，我们将简单地介绍一下电子现金的基本性质和研究现状。第 3 节给出我们的公平电子现金方案，并分析了协议的效率。然后我们论证了协议的安全性，并讨论了电子现金系统中的各种犯罪行为。最后我们给出了结论和一些待解决的问题。

2 电子现金的性质和现状

2.1 电子现金的基本性质

电子现金在其周期中存在 4 个过程：注册账户，提取现金，支付现金，存储现金。它一般包括 3 个主体：用户 (B)，商家 (M)，银行 (bank)。在公平电子现金协议中我们还需要一个托管者 (Trustee，简称 T)。它的基本性质 [10] 如下：(1) 保护合法用户的匿名性。(2) 撤消匿名只能由托管者在必要的时候完成；而且只能撤消匿名，而不能伪造现金。(3) 银行 (与托管者，商家，其他用户相互勾结) 不能损坏用户的利益。(4) 撤消匿名性是可选的，即跟踪现金就不能跟踪该现金的用户。(5) 效率要高，托管者只是在必要的时候参与。(6) 防止犯罪：加入撤消匿名的体制不能导致更严重的犯罪。

2.2 电子现金的研究现状

目前，对电子现金的研究主要着重于匿名可撤消性，可分性，传递性，高效性。S. Brands[11] 的方案被认为是目前最有效的电子现金系统， Camenisch 和 Frankel 分别提出了基于该系统的可控制匿名的方案，前者的跟踪协议效率高出后者近一倍。但以上方案在用户提取电子现金时要求托管者在线服务，效率很低。

文献 [12] 基于证明离散对数相等和 Schnorr 盲签字提出另一个可控制匿名的电子现金，特点是托管者完全脱线，每个用户对应一个大素数，公共模是这些素数的乘积加 1，数学结构非常完美，只是表示电子现金的数据太长，目前还很难实用。

文献 [10] 提出了基于证明离散对数相等和 Schnorr 盲签字的托管者 (T) 脱线的可控制匿名的方案，效率有所提高。

Juels[9] 利用一种所谓的 " trustee token " 提出了一种可行的公平电子现金方案，是目前我们了解的比较有效的可控制匿名的电子现金方案. 然而，该方案给出了过强的用户追踪性质：托

管者不仅可以确定用户过去提取的所有电子现金，而且可以确定出用户将要提取的电子现金。当托管者不可信赖时，诚实用户的匿名信息就有可能被泄露。

3 基于托管者的公平电子现金

我们将根据 D. Chaum[2] 的方案 (然而我们不使用费时的选择——分割协议) 来构造基于托管者的公平电子现金，系统的安全性基于 RSA 体制 (即大整数分解是一个公开问题)．首先我们给出一些所要用到的符号．我们的协议包括 4 个主体：用户 (B)，商家 (M)，银行 (bank) 及托管者 (T)．

3.1 一些参数

银行：$n=pq$，其中 p,q 是两个大素数．$\phi(n)$ 没有小的奇因子。银行的私钥为 $\mathrm{sk}_{\mathrm{bank}}$，公钥为 $\mathrm{pk}_{\mathrm{bank}}$(在我们的协议中 $\mathrm{pk}_{\mathrm{bank}}$=3)．$\mathrm{pk}_{\mathrm{bank}}$ 公开，而其它参数保密。f,g 是两个无碰撞的函数并公开。

用户：其私钥为 sk_{B}，公钥为 pk_{B}．其身份记为 ID_{B}．

商家：其私钥为 sk_{M}，公钥为 pk_{M}．

不可信赖的托管者：其私钥为 sk_{T}，公钥为 pk_{T}．$H(x)$ 是一个安全的 hash 函数。

3.2 公平电子现金协议

我们的协议包括以下几个子协议：

3.2.1 注册协议 (图 2) B 提交自己的身份信息 ID_{B} 给 T，T 验证无误后产生两个随机数 m, r_j (T 通过 m 来追踪 B)．B 发送 $(r_i, f(x_1,x_2,\cdots,x_k))$ 给 T，其中 r_i 是随机数，$x_u=(g(a_u,b_u),g(c_u,d_u))$，$a_u,b_u,c_u,d_u$ 是 B 选取的秘密随机数，$1\le u\le k$．然后 T 发送 (r_j,m) 及其签名 $\mathrm{sk}_{\mathrm{T}}[r_i^3 f(x_1,x_2,\cdots,x_k)r_j^3 H(m)]$ 给 B．

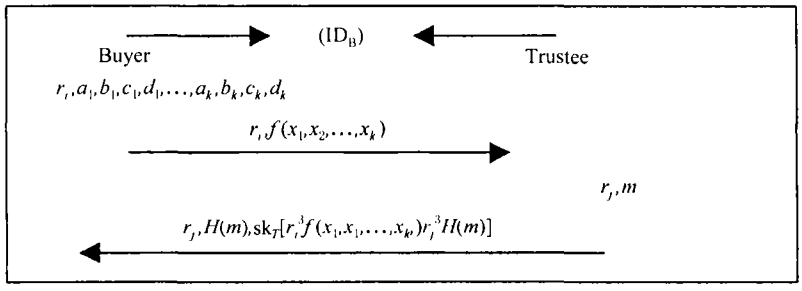

图 2 注册协议

3.2.2 提取协议 协议中所有的运算都是基于模 n，为简便起见，我们略去 mod$n$．我们假定用户在银行有一个账户，并且他和银行共享一个秘密．通过共享的秘密用户就可以从某一特定 (自己) 的账户上取电子现金。

步骤 1 B 提交 $(r_i^3, f(x_1,x_2,\cdots,x_k), r_j^3 H(m))$ 和 $\mathrm{sk}_{\mathrm{T}}[r_i^3 f(x_1,x_2,\cdots,x_k)r_j^3 H(m)]$ 给银行。

步骤 2 银行首先验证 T 的签名。若签名无误，则对数据 $(r_i^3 f(x_1,x_2,\cdots,x_k), r_j^3 H(m))$ 盲签名得到 $[r_i^3 f(x_1,x_2,\cdots,x_k)r_j^3 H(m)]^{1/3}$ 并发送给 B．

步骤 3 B 去掉盲因子后得到电子现金：$\mathrm{coin}=f^{1/3}(x_1,x_2,\cdots,x_k)H^{1/3}(m)$．

步骤 4 银行从 B 的账户上减去相应的数额。

3.2.3 支付协议 (图 3) B 将 $\mathrm{coin}=f^{1/3}(x_1,x_2,\cdots,x_k)H^{1/3}(m)$ 交给 M，M 选择一个随机的验证比特串：$z_1,z_2,\cdots,z_k$．B 发送 m 给 M 并做出如下的响应：

如果 $z_i = 1$，则 B 发送 $a_i, b_i, g(c_i, d_i)$ 给 M；

如果 $z_i = 0$，则 B 发送 $g(a_i, b_i), c_i, d_i$ 给 M．

如果 M 验证 B 的响应符合电子现金，则接受现金并交给 B 货物，否则拒收现金．

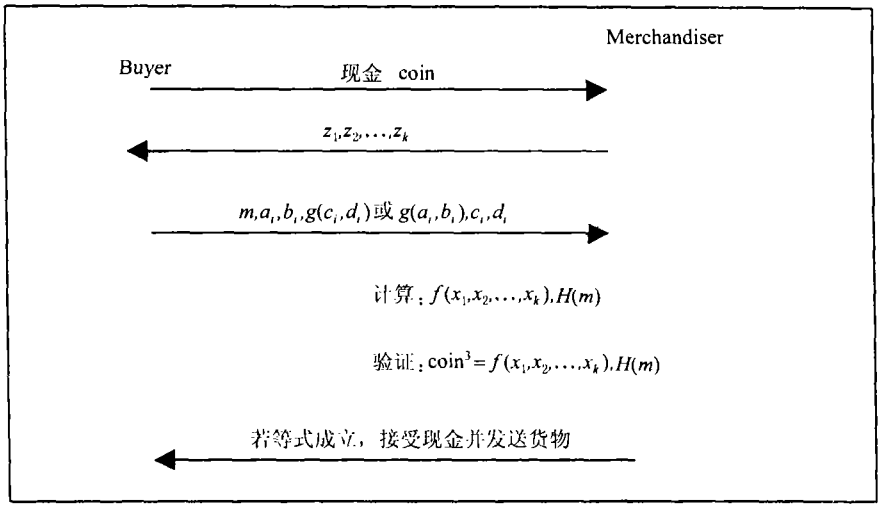

图 3　支付协议

3.2.4 *存储协议*　M 提交电子现金和对应的响应给银行，银行验证成立后将现金加到 M 的账户上．

3.3 协议的分析

如果银行发现某笔电子现金重复出现，而且验证比特串相同，则断定 M 重复存储；如果验证比特串不同，则断定 B 重复花费，他提交该现金给 T，T 由随机数恢复出 B 的身份．这样，我们就阻止了重复花费而且实现了追踪现金．如果银行要追踪用户，他发送该用户的身份给 T，T 计算出所有该用户使用的 m 给银行，这样就追踪出该用户提取的所有现金．当然，除非与银行勾结，任何人无法窃取用户的现金．然而，可以 T 构造一个“陷害”某用户的现金——他利用该用户的 m 从自己的账户上提取现金，追踪该现金就无法追踪到 T，这个问题文献 [9] 也没有给出完善解决的办法，也许可以采用非对称指纹 [13] 的技术来解决这个问题．而且，为了防止 T 任意追踪现金和用户，即他只能在银行的协助下进行追踪，我们给出下面改进的协议：

步骤 1　B 选择秘密的随机数 m_j，令 $M_i = m||m_i, 1 \le i \le t$．然后选取随机数 r_i 并发送 $r_i^3 M_i^9$，$r_i^3 H(M_i^3)$ 给 T．T 使用选择——分割协议检验其中 $t-1$ 个数据的正确性后，对余下的数据 (不妨设为 $r_1^3 M_1^9$，$r_1^3 H(M_1^3)$) 签名：$\text{sk}_\text{T}[r_1^3 M_1^9]$，$\text{sk}_\text{T}[r_1^3 H(M_1^3)]$．

步骤 2　B 发送 $r_1^3 M_1^9$，$r_1^3 H(M_1^3)$，$s_1^3 f(x_1, x_2, \cdots, x_k)$ 及签名 $\text{sk}_\text{T}[r_1^3 M_1^9]$，$\text{sk}_\text{T}[r_1^3 H(M_1^3)]$ 给银行，银行首先验证签名的正确性，并存储该数据和签名．然后对 $r_1^3 M_1^9$，$r_1^3 H(M_1^3)$，$s_1^3 f(x_1, x_2, \cdots, x_k)$ 盲签名．

步骤 3　B 去掉盲因子得到：$\text{coin} = (L_1, L_2) = (M_1^3, f^{1/3}(x_1, x_2, \cdots, x_k) H^{1/3}(M_1^3))$ 在支付协议中商家验证：$L_2^3 = f(x_1, x_2, \cdots, x_k) H(L_1)$，存储协议我们就不再给出．

分析：如果银行要追踪可疑的现金，他首先计算出 M_1，然后 T 可根据 M_1 恢复出提取现金者；而 T 单独无法追踪现金 (T 无法得到 M_1)．使用限制性的盲签名协议保证了用户必须诚实地提交数据 M_i．

如果银行规定一个数据 m 只能提取一笔电子现金，则 T 就无法陷害用户。如果银行发现用户提交的数据和签名已经存储过，则拒绝为该数据签名。这样一旦有两笔不同现金中的 L_1 对应同一个相同 m，则必定是 T 在陷害用户。

4 安全性分析

(1) 银行　银行的安全性基于 RSA 体制。伪造现金就相当于对大数模 n 的分解，这是一个困难问题。采用无碰撞的函数保证了用户必须诚实地构造现金。借助 T 的帮助银行可以容易地追踪现金或用户。当然，我们不考虑银行提取用户的现金，首先银行要考虑自己的信用，其次，一般假定银行随意地控制用户的账号，他必须被信任 [9]。

(2) 用户　采用盲签名技术，银行无法从现金中得到用户的身份信息，从而保证了现金的匿名性；而重复花费的用户则一定可以被追踪。由于采用了无碰撞函数，其它用户无法冒充现金的提取者重复花费这笔现金。

(3) 商家　商家只能存储现金，而不能冒充用户重复花费。其次，即使商家从现金中得到某用户使用的 $m, f(x_1, x_2, \cdots, x_k)$ 但他无法伪造 T 的签名，所以他也无法伪造一个追踪该用户的现金，他更无法提取该用户的现金。这样，就保证了合法用户的利益不受损失。

(4) 托管者　他只能在银行的授权下追踪用户和现金。而且 T 无法冒充某用户提取现金，也不能“陷害”某用户。

5 攻击分析

这一节我们来分析电子现金系统中的各种犯罪行为及恶意攻击 [14,15] 以及如何利用现有的方法来防止这些攻击。

(1) 银行抢劫攻击　这种攻击首先由文献 [16] 提出：如果银行用来签名的密钥泄露，就会受到毁灭性的“抢劫”攻击，因为此时攻击者能够伪造现金。除非银行发现现金的存储量超过提取量，他无法发现这种攻击。所以就像现实中银行遭受抢劫而破产一样，电子现金的系统一旦受到这种攻击就会崩溃。对这种攻击没有好的办法，银行只能妥善保管密钥，而且定期更换密钥。

(2) 洗钱攻击　不法分子通过贩卖毒品或军火获得高额利润，然后设法将这些钱合法化。文献 [14] 提出了流量控制的思想，使得大笔现金无法转移。而司法者 (或银行) 一旦发现可疑的用户和现金，则可以通过用户追踪和现金追踪恢复罪犯的身份。

(3) 行贿受贿　对于无转移性的现金，行贿者必须“花费”这笔钱给受贿者 (当然他从受贿者处得到特殊的“商品”)。而只要司法者 (反贪部门) 检查到受贿者有来历不明的巨额资产，同样可以追踪出该现金的提取者。一般来说，具有用户追踪和现金追踪性质的现金系统，都可以防止这种犯罪行为，前提是司法者的有效和公正性。

(4) 不法交易　比如司法者当场抓获某些贩毒交易者，可通过现金追踪得到操纵交易的幕后者 (比如 EVE) 的身份，然后再通过用户追踪得到 EVE 所提取的所有的现金，就可发现 EVE 进行的所有交易。

(5) 匿名敲诈　绑架者可以敲诈人质 (或其家属) 要求提供巨额电子现金。当然，在保证人质人身安全的前提下，被敲诈者可以将此现金告诉给银行和司法者，通过在线现金追踪就可以得到罪犯的行踪 (正如现实世界中司法者在被敲诈者提供现金的地点抓获罪犯一样)。被敲诈者甚至可以在人质安全后通过银行宣布他被敲诈的现金，这样罪犯就无法花费。当然，如何保证人质人身安全也是一个复杂的问题，我们这里就不再讨论。

对于广义的匿名敲诈 [6] 问题，目前尚无解决的方法。我们利用本文中的协议对这个问题做一讨论：

绑架者 (简称 K) 挟持人质要求政府 (简称 G) 提交一笔电子现金，首先 K 提交数据 $r_1^3M^9$, $r_1^3H(M^3)$, $s_1^3f(x_1,x_2,\cdots,x_k)$ 给银行要求盲签名。然后 K 去掉盲因子后就得到现金 coin $=(M^3,f^{1/3}(x_1,x_2,\cdots,x_k)H^{1/3}(M^3))$。这样 K 就可以随意的花掉这笔钱 (注意到 K 的账户上并没有减少相应的数额)。

我们给出如下的解决方法：

银行发送 $\{\mathrm{A},\mathrm{B}\}=\{[r_1^3M^9\|r_1^3s_1^3f(x_1,x_2,\cdots,x_k)H(M^3)]^{1/3},\mathrm{coin}\}$ 给用户 i。在正常情况下，用户只须发送电子现金 coin 给商家，并证明银行签名的成立。银行在遭受敲诈后，在线提供验证。所有用户还要提交验证数据 $\{[r_1^3M^9\|r_1^3s_1^3f(x_1,x_2,\cdots,x_k)H(M^3)]^{1/3},r_1,s_1\}$ 给银行。银行首先检验验证数据中签名的正确性，若不成立，则不接受此现金。然后再比较验证数据是否等于敲诈数据。若相等，也不接受此现金。

除非银行一开始就保存所有用户的验证数据并与 T 勾结，否则合法用户的身份信息不会泄露。而且用户只有在银行遭受敲诈时 (政府此时介入) 才提交验证数据。所以，合法用户的信息不会泄露。

敲诈者想出了如下的方法：

首先他合法地提取 100 美元的电子现金，发送 $(r_1^3M^9,r_1^3H(M^3),s_1^3f(x_1,x_2,\cdots,x_k))$ 给银行，并提交托管者的签名。银行验证成立后对该数据盲签名，并发送验证数据给 K。

然后 K 敲诈银行 100000 美元的电子现金，他发送 $(s_u^3f(x_1,x_2,\cdots,x_k),r_v^3M^9,r_v^3H(M^3))$ 给银行要求盲签名。他得到现金 $(M^3,f^{1/3}(x_1,x_2,\cdots,x_k)H^{1/3}(M^3))$。然后他花费该现金，并提交验证数据 $\{[r_1^3M^9\|r_1^3s_1^3f(x_1,x_2,\cdots,x_k)H(M^3)]^{1/3},r_1,s_1\}$。这样，敲诈者就成功地将 100 美元“变成”了 100000 美元。

银行可用多公钥的思想解决这个问题 [9]。比如说 $(M\|f^{1/3}(x_1,x_2,\cdots,x_k)H^{1/3}(M))^3$ 代表 100 美元，而 $(M\|f^{1/17}(x_1,x_2,\cdots,x_k)H^{1/17}(M))^{17}$ 代表 10000 美元。这样，敲诈者要敲诈一笔现金，他必须提取相同数额的合法现金，而且无法花费这笔合法现金 (否则就相当于重复花费)。

当然，广义的敲诈问题至今仍是一个困难问题，它涉及到社会，政治，经济等一系列复杂的问题。也许，解决敲诈问题的“最好”方法是：消灭敲诈。

6 结　论

本文我们利用 RSA 盲签名技术，给出了一种基于托管者的公平电子现金协议。与以前协议不同的是，我们对托管者的信任度可以达到最小。即使托管者与银行勾结也无法花费用户的现金，而且托管者只能追踪银行要他追踪的现金，从而最大程度的保证了合法用户的隐私。我们的协议还可以用来追踪可疑的现金和用户，从而防止和减少电子现金系统的犯罪活动如洗钱、勒索等。

当然，如何解决广义的敲诈问题，提高电子系统的效率需要进一步的工作。其次，在匿名可撤消的公平电子现金系统中防止新的犯罪是一个必须解决的问题 [10]。而且，我们的协议采用的是 RSA 盲签名技术，为了保证长期的安全，其密钥长度至少为 1024bit。而 160bit 的椭圆曲线密码体制就可以提供同等的安全强度，所以采用 ECC 盲签名技术可以大大地提高该协议的效率。

参　考　文　献

[1] D. Chaum, Blind Signature for Untraceable Payments, Eurocrypt' 82, Plenum Press, 1983, 199-203.

[2] D. Chaum, A. Fiat, M. Naor, Untraceable Electronic Cash, Crypto' 88, LNCS 1000, Berlin, Springer-Verlag, 1996, 84-95.

[3] S. Brands, Untraceable Off-line Cash in Wallet with Observes, Crypto'93, LNCS 773, Springer-Verlag, Berlin, 1994, 302–318.

[4] B. von Solms, D. Naccache, On blind signatures and perfect crimes, Computers and Security, 1992, 11(6), 581–583.

[5] E. Brickell, P.Gemmell, D. Kravitz, Trustee-based tracing extension to anonymous cash and the marking of anonymous change, Proc. 6-th Annual ACM-SIAM Symposium on Discrete Algorithms (SODA), 1995, 457–466.

[6] M. Stadler, J. M. Piveteau, Jan. Camenisch, Fair blind signatures, Eurocrypt' 95, LNCS 921, Springer-Verlag, 1995, 209–219.

[7] J. Camenisch, U. Maurer, M. Stadle, Digital payment systems with passive anonymity-revoking trustees, Computer Security Esorics' 96, LNCS 1146, Springer-Verlag, 1996, 33–43.

[8] Y. Frankel, Y. Tsiounis, M. Yung, Indirect discourse proofs: Achieving fair off-line E-cash Asiacrypt' 96, LNCS 1163, Springer-Verlag, 1996, 286–300.

[9] A. Juels, Trustee Tokens: Simple and practical anonymous digital coin tracing, Financial Cryptography '99, LNCS 1648, Springer-Verlag, 1999, 33–43.

[10] G. Davida, Y. Frankel, Y. Tsiounis, M. Yung, Anonymity control in E-cash systems, Financial Cryptography'97, LNCS 1318, Springer-Verlag, 1997, 1–16.

[11] S. Brands, Untraceable off-line cash in wallets with observers, Crypto'93, LNCS 839, Berlin, Springer-Verlag, 1993, 302–318.

[12] Feng Bao, R. H. Deng, A New type of " magic ink " signature towards transcript-irrelevant anonymity revocation, Asiacrypt'98, Springer-Velag, 1998, 1–11.

[13] B. Pfitzmann, M. Schunter, Asymmetric fingerprinting, Eurocrypt'96, LNCS 1070, Berlin, Springer-Verlag, 1996, 84–95.

[14] T. Sander, A. Ta-Shma, Flow control: A new approach for anonymity control in electronic systems, Financial Cryptography '99, LNCS 1648, Springer-Verlag, 1999, 46–61.

[15] T. Sander, A. Ta-Shma, Auditable, anonymous electronic cash, Crypto '99, LNCS 1648, Springer-Verlag, 1999, 555–572.

[16] M. Jackbosson, M. Yung, Revokable and versatile electronic money, In 3^{rd} ACM Conference on Computer and Communications security, India, ACM press, 1996, 76–87.

FAIR ELECTRONIC CASH BASED ON UNTRUSTWORTHY TRUSTEE

Chen Xiaofeng Wang Yumin

(*National Key Laboratory on ISN, Xidian University, Xi'an* 710071, *China*)

Abstract A fair electronic cash protocol based on trustee is presented by using RSA blind signature technique in this paper, the identity of multi-spender will be revealed by trustee with very high probability. Contrasting with the previous protocol, the user's money cannot be withdrawn unless the trustee is in collusion with the bank, and the trustee can only trace the money that the bank asked him to trace. So the privacy of the user can be ensured to the maximum limit. Also this protocol can be used to trace the dubious cash and the owner, thereby it may be exploited to decrease the crimes like money laundering, blackmailing, etc. in the electronic cash system. This protocol requires off-line participation of trustee when users withdraw the cash, so it is efficient for implementation.

Key words Fair electronic cash, Anonymity revocation, User tracing

陈晓峰： 男， 1976 年生，博士生，研究方向为电子商务，椭圆曲线密码.

王育民： 男， 1936 年生，教授，博士生导师，研究领域为信息理论，编码及密码理论.