

一种新的公平有效的可分电子货币系统

潘剑峰,唐西林

(华南理工大学 理学院数学系,广东 广州 510640)

摘 要: 基于 schnorr 盲签名和非交互的零知识证明构造了一种新的公平有效的可分电子货币系统. 该系统中可分电子货币的计算利用了一重离散对数和抗强碰撞的 Hash 函数. 系统中使用了 C 值以界定其安全性. C 值可以是 C_1 , 也可以由 C_1, C_2 级联得到, 其中 C_1 可在发生多重消费时揭示用户身份, 而 C_1 和 C_2 结合则使得 B (银行)和 T (可信方)进行货币追踪和用户追踪简便易行. 此外, 该方案还能够实现多重花费和多重存款的追踪, 并通过限制 T 的权限, 有效防止 B 和 T 联合作弊.

关键词: 电子货币; 公平性; 可分性; 货币追踪和用户追踪

中图分类号: TP309.2

文献标识码: A

文章编号: 1000-7180(2010)06-0076-04

A Novel Fair and Efficient Divisible E-Cash System

PAN Jian-feng, TANG Xi-lin

(Dept. of Mathematics, South China University of Technology, Guangzhou 510640, China)

Abstract: A novel fair and efficient divisible E-Cash system based on the schnorr blind signature and non-interactive zero-knowledge proofs is proposed in this paper. In this system, both discrete logarithm and collision-resistance Hash function are used in the computation of divisible E-Cash. It contains the C value which defines the security. C can only be C_1 or be obtained by associated by C_1 and C_2 , where C_1 is able to disclose the users' ID when over-spending happened. Moreover, the combination of and can realized owner tracing and coin tracing through the cooperation of B and T more easily. The scheme can also realize overspending tracing and over-deposit user, furthermore, it can limit the power of T , avoid the possibility of the association guilt between B and T .

Key words: E-Cash; fairness; divisibility; owner tracing and coin tracing

1 引言

电子货币作为电子商务的关键技术已经越来越受到人们的关注. 目前为止所提出的电子货币系统, 可分为不包含 T (Trustee; 可信方)的电子货币系统和包含 T 的电子货币系统. 包含 T 的电子货币系统由于可以实现货币追踪和用户追踪, 从而可以追踪类似洗黑钱和完全犯罪的不法行为而备受人们青睐, 当然这种系统由于 T 的存在有时显得不够便捷. 同时根据实际中的需要, 部分电子货币量无需进行监控追踪, 只有在大笔的金融交易及特定情况下才需要监控, 所以应该把受监控的电子货币的数据

存放在可监控追踪的数据库中有选择地进行追踪. 当然, 一个好的电子货币系统还必须具有能防止 T 单独作弊, T 和 B 联合作弊等功能.

实际操作中, 消费者应该可以消费任意低于当前所拥有的从银行支取的电子货币, 即电子货币应该是可分的. 这样可以提供一种比重重复多次取款或支付更方便有效的电子货币. 已提出的电子货币系统的不足在于它们或者只是基于部分安全, 或者是非完全匿名, 或者货币间存在链接, 或者因为无 T 参与无法抗拒完全犯罪或洗黑钱等. 此外, 这些电子货币系统即使是完全匿名的, 由于计算基本上是基于高次数离散对数, 效率比较低. 目前, 公平有效的

可分电子货币系统还不多见。

文中提出一种公平的可分电子货币系统,该系统通过安全级联的安全 C 值限制 T 和 B 的权限,使得仅当 T 和 B 双方合作才能对电子货币进行追踪,保证了电子货币系统的安全性。进一步,通过门限技术本系统很容易实现多个 T 的扩展模型。

2 预备知识

2.1 可分电子货币的二叉树表示及相关要求

下面以文献[1]为基础(本文根据需要作了一些改动):

给定一棵 $L+2$ 层的二叉树,它代表价值为 2^L 的电子货币,以 $N(i, j)$ 表示树的第 i 层第 j 个结点。树的根节点属于第 0 层且标记为 $N(0, 0)$, 节点中包含经过银行盲签名的合法电子货币量的数据 S_p 。每一个子节点对应的电子货币价值是其父节点的一半,而且当节点对应的所有叶子有一个是死的情况下该节点不可用^[2-3]。

树的第 i 层有 2^i 个节点 $N(i, j)$, $1 \leq j \leq 2^i$, 每个节点对应着价值为 2^{L-i} 的电子货币(当有死叶子时,按照剩余的叶子数计算电子货币的价值);每个节点 $N(i, j)$ 包括叶子都含有一个特殊的 K 值,且每个电子货币都含有 C, S , 这些值的构成满足以下几个性质:

(1) 根节点的最终值必须是经过银行签名的(即从取款协议得到数据的一个或部分);

(2) 从根节点可轻松计算子节点的 K 值,而从子节点则无法计算与他没有后代关系的节点的 K ;

(3) S 值必须包含消费节点下一代两个后代的值,进而可计算其所有叶子的 S 值(用以判断重复消费行为);

(4) C, S 部分值必须只有 U 方可构造,当多重消费时, B 即可通过 C 值揭露用户身份,当需要追踪时, C 值则只能由 T 计算,然后发送计算结果给 B 进行追踪。

2.2 非交互的基于离散对数的零知识证明

非交互的零知识证明是由 Fiat-Shamir heuristic 提出的^[4]。本文涉及以下三类^[1,4]:

(1) 知道一个离散对数指数的证明: 记为 $PK\{\alpha, y = g^\alpha\}$;

(2) 证明两个离散对数指数相等的证明: 包括两种分别记为 $PK\{(\alpha_1, \alpha_2) : y = g^{\alpha_1} \wedge y = g^{\alpha_2}\}$ 和 $PK\{\alpha : y = g^{\alpha_1} \wedge y = g^{\alpha_2}\}$;

(3) 知道两个离散对数中一个是正确的证明:

记为 $PK\{(\alpha_1, \alpha_2), y = g^{\alpha_1} \vee y = g^{\alpha_2}\}$ 或者 $PK\{\alpha, y_1 = g^{\alpha_1} \vee y_2 = g^{\alpha_2}\}$ 。

此外,文中还用到双重离散对数的证明 $PK\{\alpha, y_1 = g^\alpha \vee y_2 = g^{\alpha_2}\}$ 以及由(2),(3)两种衍生出的 $PK\{\alpha, y_1 = g^{\alpha_1} \vee y_2 = g^{\alpha_2}\}$ 。

这种的非交互的零知识证明已经被证明在随机的 oracle 模型下是安全的。

3 公平可分电子货币系统(FDS)

我们提出的电子货币系统中,参与主体包含:银行 B ,可信方 T ,用户 U ,以及商家 M 。工作主体过程为: U 在 B 处支取相应额度的电子货币,接着在 M (商家)处根据需要使用该电子货币的一部分,当 M 商家积累了一部分电子货币之后,在 B 处存款,最后对以上过程出现的不合法行为进行相关追踪。

在花费电子货币时,该可分电子货币包含着一个正确的数据 S 用以判断用户是否多重消费;每消费一次需包含一个新鲜的随机值 R_0 用来判断 M 是否多次存款;同时还包含一个安全的 C 值用以多重消费时揭露用户身份以及需要时由 T 进行货币追踪和用户追踪。其中 C, S 必须是即使结合所有的合法的可分电子货币也无法透露用户信息的合理的值。

3.1 系统的建立

选定两个大素数 p, q , 其中, $2^{L-1} < p < 2^L$, L 是 64 的倍数, L 一般在 512 比特以上, q 是 $p-1$ 的素因子, $2^{159} < q < 2^{160}$ 即 q 是长为 160 比特。取 $g \in \mathbb{Z}_q^*$ 且 $g^q \equiv 1 \pmod{p}$ 。公开 g, p, q 。

系统由 T (可信方), U (用户), M (商家) 还有 B (银行) 构成, 他们有各自的私钥 x_t, x_u, x_m, x_b 以及相应的公钥 $y_t \equiv g^{x_t} \pmod{p}, y_u \equiv g^{x_u} \pmod{p}, y_m \equiv g^{x_m} \pmod{p}, y_b \equiv g^{x_b} \pmod{p}$, 并且 H_1, H_2, H 都是抗强碰撞的 Hash 函数。

3.2 建立帐户

U, M 分别在银行中存入现金同时提交个人身份给银行 B , 当 B 验证通过后, 则为他们分别建立电子货币账户。

3.3 取款协议:

U 与 B 进行以下交互协议:

① U 需要在 B 处提取 2^L 元, 首先 U 发送 (s_u, m) 给 B , $m = w \cdot \text{Date} \cdot \text{Time} \cdot pk_u$, S_u 是 U 对 m 的 Schnorr 签名;

② B 计算 $\text{ver}(s_u, m) = 1$, 若成立随机选择 $l \in \mathbb{Z}_q^*, l \neq 1, R \equiv g^l \pmod{p}$, 并发送 R 给 U ;

③ U 随机选择 $\alpha, \beta \in \mathbf{Z}_q^*$, 计算 $R' \equiv Rg^{-\alpha}y_b^{-\beta}(\bmod) p; e' \equiv H(R' \oplus w)(\bmod) q, e \equiv e' + \beta(\bmod) q$, 并把 e 发送给 B;

④ B 计算 $S' \equiv l - x_e(\bmod) q$ 并发送给 U;

⑤ U 计算 $S_p \equiv S' - \alpha(\bmod) q$

协议结束 U 得到 (w, S_p, e') , U 计算 $g^{S_p}y_b^{e'} = R'$, 若成立则 (w, S_p, e') 就是经过 B 盲签名的合法电子货币, B 保留 (S_u, R) ;

3.4 支付协议

当 U 想要从可分的电子货币中支付给商家价值为 2^l 的一部分, $(l = L - i)$, 他要选择第 i 层一个还未花费的节点如 $N[i, j]$, 下述一个关于该节点的花费协议:

给定一个阶为 $o(G)$ 群 G, g, h 是他的随机选择的生成元, $G_1 = \langle g_1 \rangle$ 是 $\mathbf{Z}_{o(G)}^*$ 的子群, 而且每个 $G_i = \langle g_i \rangle$ 都是 $\mathbf{Z}_{o_{i+1}}^*$ 的子群, 这里 o_{i+1} 是 G_{i+1} 的阶. 例如可以选取 G_i 是 $\mathbf{Z}_{o_{i+1}}^*$ 的子群, 其中 $o_{i+1} = 2o_i + 1$ 对于 $\forall i$ 且每个都是素数. 然后 G_i 对应二叉树的第 i 层, 随机选择生成元 $g \in G, \forall i, g_{i,0}, g_{i,1}, g_1 \in G_i$, 所有这些都是公开的, 花费 $N(i, j)$ 执行协议:

① M 发送随机数 $R_0 = H(v \cdot \text{Date} \cdot \text{Time} \cdot pk_m)$ 其中 v 是双方购货的清单和金额;

② U 计算 $\tilde{K}_0 = g^{S_{h^r}}, K = g^{S_p}$,

当 $i = 0$, 则结束协议得到 $(\tilde{K}_0, K)$, 否则 j 从 1 到 i 做;

当 j 为 1 或偶数时, $\tilde{K}_j = g_j^K$, 当节点属于二叉树的左半部分时, $K = g_{j,0}^K$, 否则 $K = g_{j,1}^K$;

当 j 为大于 1 的奇数时, $\tilde{K}_j = H(K)$, 当节点属于二叉树的左半部分时, $K = H_1(K)$, 否则 $K = H_2(K)$;

③ 结束 ② 时 U 得到 $(\tilde{K}_0, \tilde{K}_1, \dots, \tilde{K}_i, K)$, 然后计算

$$S = LK \cdot RK,$$

$$\text{其中 } LK = \begin{cases} g_{i+1,0}^K & \text{当 } i = 0 \text{ 或 } i + 1 \bmod 2 = 0 \\ H_1(K) & \text{当 } i \geq 2 \text{ 且 } i + 1 \bmod 2 \neq 0 \end{cases},$$

$$RK = \begin{cases} g_{i+1,1}^K & \text{当 } i = 0 \text{ 或 } i + 1 \bmod 2 = 0 \\ H_2(K) & \text{当 } i \geq 2 \text{ 且 } i + 1 \bmod 2 \neq 0 \end{cases},$$

C 值:

$$C = C_1 \cdot C_2, C_1 = g^{S_p \cdot R_0}(S_u \cdot R), C_2 = y_b^{S_p \cdot R_0}(\text{当货币属于不被监督范围时, 不用提供 } C_2);$$

④ 同时 U 使用非交互的零知识证明基于离散对数的零知识证明向 M 证明 LK, RK, C, S 是由合

法的电子货币 (w, S_p, e') 正确计算而来的.

而 U 的证明如下:

$$V_0 = \{(\alpha, \beta, S_p, e', \alpha_1, \alpha_2) : R' = Rg^{-\alpha}Y_b^{-\beta}$$

$$\wedge R' = g^{S_p}y_b^{e'} \wedge \tilde{K}_0 = g^{S_{h^r}} \wedge \tilde{K}_1 = g_{11}^{S_p} \wedge \tilde{K} = g_1^{\alpha_1}; \wedge (\tilde{K}_2 = g_2^{\alpha_{1,0}} \vee \tilde{K}_2 = g_2^{\alpha_{1,1}}) \wedge \tilde{K}_2 = g_2^{\alpha_2}\}$$

$$V_1 = \{(S_p, (S_u \cdot R)) : C_1 = g^{S_p \cdot R_0}(S_u \cdot R)$$

$$\wedge C_2 = y_b^{S_p \cdot R_0}\}$$

其中对电子货币合法性的验证也可以用签名的知识证明机制证明 S_p 是经过 B 盲签名的有效数据(合法货币);

$V = (V_0, V_1, \alpha_2)$, 而后的对 $\tilde{K}_3, \dots, \tilde{K}_i$ 以及 C, S 的验证则因有了 α_2 则可容易完成;

⑤ U 发送 (S, Π) 给 M, $\Pi = \{2^l, V, C, R_0, \tilde{K}_0, \tilde{K}_1, \dots, \tilde{K}_i\}$;

⑥ M 验证正确性, 若 V 正确则保存 (S, Π) 并结束协议.

3.5 存款协议

当 M 想存款 (S, Π) 时, 则把 (S, Π) 发送给 B, B 验证 V, C 的正确性, 同时通过数据库查看 R_0 是否是第一次接收的, 若不是说明 M 是进行第二次存款则拒绝, 若是则通过 S 计算出 2^l 个 $(S_{n_1}, \dots, S_{n_{2^l}})$, 这只需经过简单的计算即可. 这 l 个值分别对应 2^l 个叶子. 然后银行把 $(S_{n_j}, S, \Pi), j = 1, \dots, 2^l$ 与数据库 III (该数据库存放每次电子货币交易后形成 (S_{n_j}, S, Π) 的数据, 且用于发现并揭露多重消费的用户身份) 中数据进行比对, 若没有 (S_{n_j}, S', Π') 这样的数据存在, 则接收然后在 M 的帐户中存入 2^l 元, 并把含有 C_2 的和不含 C_2 分别存放在标记为 I, II 的两个数据库(数据库 I 含有可进行用户和货币追踪的数据的 C_2 , 而存在 II 中的电子货币则因为没有 C_2 而完全匿名), 否则仍在 M 中存入 2^l 元同时进行多重消费追踪.

3.6 多重消费追踪:

B 只需在数据库 III 中把 (S_{n_j}, S, Π) 和 (S_{n_j}, S', Π') 对应的 C_1 找出分别为 C_1 和 C'_1, R_0 分别为 R_1 和 R_2 , 计算 $(C_1^{R_1}/C_1'^{R_2})^{\frac{1}{R_1-R_2}} = (S_u \cdot R)$, 进而揭露用户身份.

3.7 用户追踪(只限于数据库 I 中的数据)

当怀疑某个用户进行敲诈、勒索等不法行为时, 则可以根据用户身份对其某次交易进行追踪, 用户

发送自己身份到B,B找出相应的 S_u 以及 S_u 对应的 R ,把 R 发送给T,T对数据库 I 中的货币数据计算

$\frac{C_1}{C_2^{x_i}}$ 是否等于 $S_u \cdot R$,若相等查 $\tilde{K}_0, \tilde{K}_1, \dots, \tilde{K}_i$;

$i = 0$,则已找到货币; $i = 1$,则需同样计算继续找出另一部分电子货币; $i \geq 2$,则由 V 中 a_2 得 $\tilde{K}_2 = H(g_{1,0}^{S_p})$ 或 $\tilde{K}_2 = H(g_{1,1}^{S_p})$,接着查看电子货币中是否等于以上两个值中得一个就可以找到全部得电子货币;

T结束查找过程则把查找到的货币数据发送给B,由B冻结这笔货币.

3.8 货币追踪(只限于数据库 I 中的数据)

B只需把货币中的 C_1 和 C_2 提交给T,T通过计算 $C_1/C_2/1/x_1 = S_u \cdot R$,然后把 $S_u \cdot R$ 发送给B即可找到相应的用户 pk_u .

4 安全性证明和有效性分析

考虑以下几个方面的安全性:

(1) 匿名性:电子货币是由B经过 schnorr 盲签名得到的,在支付给商家时(数据不包含 C_2),采用了非交互的零知识证明,而这种证明方式也完全没透露电子货币的任何数据以及电子货币与身份有关的任何消息(这是因为想从 $\tilde{K}_0$ 等数据中计算 S_p 等货币数据相当于求解离散对数问题,这是不可能的).所以在没有提供 C_2 的所有用户中,他们的电子货币是完全匿名的,而提供 C_2 的用户其匿名性则是可控的,即在有追踪需要时B可通过T找出被追踪者^[5-6];

(2) 对货币的多重存款和多重消费追踪,如3.5节及3.6节所述;

(3) 不可伪造性和安全性:T即使与B相勾结想要伪造用户U的合法的货币,相当于从 (S, Π) 计算出 S_p 或者通过旧的货币重组得到新货币,这是不可能的,这分别由 schnorr 盲签名以及离散对数和抗强碰撞的 Hash 函数的安全性保证,而这些安全性则是显然的,同时由每次交易的数据中都包含 R_0 ,且每次计算都包含有随机数 $\tilde{r}$ 来保证货币新鲜性;

需要指出的是,只有B和T合作才能完成货币追踪和用户追踪.T的权限还可通过门限化技术进

一步削弱.

5 结束语

FDS先基于离散对数达到匿名的效果,同时利用 Hash 函数简化了计算,具有下列优点:

(1) 可根据实际选择是否完全匿名,具有匿名的可控性,且可根据需要进行相关追踪;

(2) 已有的电子货币系统,电子货币至少包含四个数据量,FDS系统中货币基于 schnorr 盲签名,每个货币只有三个数据量,可比较快捷有效进行;

(3) 文中可分货币在验证上采用了非交互的零知识证明改变了已有的必须累次验证的方式而可采用并行多次验证大大提高了计算速度,优化了系统,在计算上则基于离散对数和 Hash 函数的交替进行,这就意味着每次的计算是同等长度的离散对数计算,保证了数据计算简便性.

参考文献:

- [1] Toru Nakanishi, Yuji Sugiyama. Unlinkable divisible electronic cash [C]//ISW 2000. Berlin: Springer, LNCS, 2002:121-134.
- [2] Sebastien Canard, Aline Gouget. Divisible E-cash systems can be truly anonymous [C]//EUROCRYPT 2007. Hance, LNCS, 2007:482-497.
- [3] Frankel Y D Y. Threshold cryptosystems [C]//Advances in Cryptology - CRYPTO'89. Milwaukee: University of Wisconsin Milwaukee, LNCS, 1989:307-315.
- [4] Fiat A, Shamir A. How to prove yourself: practical solutions to identification and signature problems [C]//Advances in Cryptology - CRYPTO'86. California, LNCS, 1986:186-194.
- [5] 刘义春.电子商务中信任机制的研究[J].微电子学与计算机,2008,25(3):122-125.
- [6] 文静华,张梅,张焕国.电子支付协议的博弈逻辑模型与形式化分析[J].微电子学与计算机,2007,24(9):113-115.

作者简介:

潘剑峰 男,(1985-),硕士研究生.研究方向为密码学与信息安全.

唐西林 男,(1962-),博士,教授.研究方向为密码学、代数学.