

基于可信第三方的可撤销匿名性的公平可分电子现金系统

胡泽军，吴中福，朱代华，朱兴亮
(重庆大学 计算机学院，重庆 400044)

摘要：第一次提出了一个实用的基于可信第三方的可分离线电子现金系统，该系统具有匿名性，以保护消费者的隐私；其匿名性是可撤销的，在必要的时候可以打击犯罪，以得到政府的使用许可；支付过程是公平的，防止某一交易方在交易中蒙受损失；电子现金是可分的，可以像现实货币一样按需要精确分割，用于精确支付。借鉴转换数字签名的思想，引入可信任的第三方，实现了交易过程的公平性和在必要时撤销匿名性，但只有在注册阶段、产生争议及撤销匿名性的时候才会涉及可信任的第三方。这种电子现金当然还可杜绝重复花费、防止超额支付及防伪。在支付协议中，该系统比目前基于二叉树的最快的可分电子现金计算量少 60 倍。

关键词：电子现金；可撤销匿名性；公平；可分；可信第三方

中图法分类号：TP309.2 文献标识码：A 文章编号：1001-3695(2004)10-0096-04

Trustee-based Anonymity-revocable Fair Divisible E-cash System

HU Ze-jun, WU Zhong-fu, ZHU Dai-hua, ZHU Xing-liang
(College of Computer Science, Chongqing University, Chongqing 400044, China)

Abstract: For the first time, this paper proposes a practical divisible off-line e-cash schema based on trustee. The anonymity, which the customer's privacy depend on, can be revoked whenever needed so as to punish crime and gain authorization of government. Fairness in the trade process prevents traders on both sides from loss. The divisible e-cash, which can be precisely divided like real cash, are paid in precision. By quoting the concept of digital signature transformation, introducing trustee, fairness in trade process and revocation of anonymity are realized. Trustee is only involved in during registration, disputation, revocation of anonymity. In addition, this kind of e-cash acts as a means to curb repetitive-spending, overdrawing, counterfeiting. Computation overhead of our system are 60 times less than the rapideast one at present based on binary-tree divisible e-cash system.

Key words: E-cash; Anonymity-revocable; Fair; Divisible; Trustee

电子现金由于其方便性和低成本必将成为未来的主要电子支付方式。匿名离线电子现金系统由 Chaum 提出^[1]，但该方案的电子现金不可分，实用性比较差。在实际交易中需要支付任意金额的现金（即可分性），有两种途径实现：一种类似于由 Okamoto 和 Ohta 在 1991 年首次提出的基于二叉树的可分数字现金系统，用户可将处于二叉树根节点的原始硬币分解成没有直系亲属关系的子节点进行支付，分割前后数字现金的总额相等^[2]。文献[3]第一次提出了有效的可分电子现金，系统的时间复杂度为 $O(\log N)$ ，此处 $N = (\text{总硬币价值}) / (\text{最小可分的现金单位})$ 。二是引入可信方，由可信方跟踪用户以防超额支付，但以前的方案一直存在的可分性和匿名性冲突或者通信量过大问题，不实用。为防止利用电子现金的匿名性进行犯罪活动，1995 年 Brichell 等提出了基于可信方的电子现金追踪技术；在可信方的帮助下，可以撤销某个特定的电子现金的匿名性，但由于可信方必须在线，效率不高。也可以利用可信方来实现公平交易^[4,5]，本方案也采用离线的可信方来实现公平交易。文献[6]也提出了一种基于可信方的可分电子现金方案，但用户的匿名性消失，未实现公平性。

本文基于目前最有效的 Brand 方案^[7]，引入可信方，同时实现电子现金的可分性、交易的公平性及可撤销匿名性，解决了基于可信方的电子现金可分性和匿名性冲突问题。本文涉及的电子现金有四个参与者：银行、用户、商家和可信任的第三方（以下简称可信方），有七个主要的处理协议：建立账户、取款、付款、存款、电子现金追踪、取款人追踪以及争议仲裁。本方案中，只有在注册阶段、产生争议及撤销匿名性的时候，可信方才参与交互，可信方在正常的交易过程中是离线的。同基于二叉树的方案比，本方案的显著特点是支付时只有一个现金，而不是多个硬币，因此支付过程十分高效。

1 记号与假设

用 ${}_R Z_q$ 表示在 Z_q 中随机地选择一个数，其中 Z_q 表示小于 q 的正整数； $||$ 表示连接操作； $|q|$ 表示数 q 的二进制位长度； $x \stackrel{?}{=} y$ 表示验证 x 是否等于 y ； $x \equiv y^a \pmod p$ 表示 x 与 y^a 模 p 同余，常简记为 $x = y^a$ ； $\text{sig}_u(A_1'; B_1'; M_T, d_t)$ 表示用户 U 用自己的私钥对元组 (A_1', B_1', M_T, d_t) 进行签名。

2 证明两个离散对数相等

文献[4]中提出了用“证明两个离散对数相等”来实现可

撤销电子现金的匿名性,它是基于 Schonorr的零知识证明方案构造的,可以形式地定义为:对于具有概率多项式计算时间的证明者 U 和验证者 V,给定某大素数 p, G_q 是乘法群 Z_p^* 的阶为素数 q 的子群, a, b 是子群 G_q 的生成元。

U 知道一个秘密数, $x \in_R Z_q, A \equiv a^x \pmod p, B \equiv bx^x \pmod p$, U 和 V 都知道 A, B, a, b。U 向 V 证明 $\log_a A = \log_b B^{[4]}$, 从而向 V 证明他知道秘密随机数 x。为减少 U 和 V 之间的通信量,可定义一 Hash 函数 $H: G_q \times G_q \times G_q \times G_q \times G_q \times G_q \rightarrow Z_q$, 用于计算随机访问因子 c, 证明过程如下:

- (1) U 选择 $y \in_R Z_q$, 计算 $A' = a^y \pmod p, B' = b^y \pmod p, c = H(A \parallel B \parallel A' \parallel B' \parallel a \parallel b), r = cx + y \pmod q$, 发送 A', B', r 给 V。
- (2) V 计算 $c = H(A \parallel B \parallel A' \parallel B' \parallel a \parallel b)$, 并验证 $a^r \equiv A^c \cdot A' \pmod p, b^r \equiv B^c \cdot B' \pmod p$ 。

3 实用的电子现金方案

我们的主要工作是基于 Brand 的电子现金方案^[7] (该方案是目前公认最有效的电子现金系统,但不可分),引入可信方解决电子现金的可分性和可撤销匿名性,借鉴转换数字签名的思想实现交易的公平性。该系统中可分电子现金的总额显式地表示在电子现金中(不同于已有的电子现金金额由银行密钥决定),支付金额显式地表示在支付信息中。

3.1 银行初始化

银行 B 选择两个大素数 p 及 q,使得 $|q| = \eta \times k, p = 2q + 1$,其中 η 为特定的常数, KE_1 为系统的安全系数。定义乘法群 Z_p^* 的阶为素数 q 的子群 G_q 以及 G_q 的生成元 g, g_1, g_2, g_3 ,使得求解各生成元的离散对数是困难的。选择密钥 $x_B \in_R Z_q$,定义单向随机 Hash 函数 H_1, H_2, H_3, H_4 。B 公开 p, q, g, $g_1, g_2, g_3, H_1, H_2, H_3$ 和其公钥 $h = g^{x_B}, h_1 = g_1^{x_B}, h_2 = g_2^{x_B}, h_3 = g_3^{x_B}$ 。

3.2 可信方初始化

为了在必要时进行现金追踪,可信方选择自己的私钥 $x_T \in_R Z_q$,计算并公开它的对应公钥 $h_T = g_2^{x_T}$;为了保证交易的公平性,用户 U 必须向可信方申请交易证书,可信方随机为 U 选取 t_c ,并计算 $(g_2)^{t_c} = T_c$,对 T_c 签名 $\text{sig}_T(T_c)$,并发送给 U,其中 t_c 为 U 的交易私钥。U 可以长期使用 t_c 及 $\text{sig}_T(T_c)$,同时可信方记录 t_c 及其对应的 T_c ,用于以后的交易争议仲裁。

3.3 用户初始化(开户)

用户初始化时选择 $u_1 \in_R Z_q$,以 $I \equiv g_1^{u_1} \pmod p$ 作为自己的身份字。在此, u_1 作为用户取款时的身份密码。

3.4 取款协议

在该系统中,银行的一对现金密钥可以用于提取任意金额的电子现金,这与现有的其他电子现金系统中提取不同金额的电子现金使用不同的密钥是不相同的,有利于简化系统的构造及管理维护。在现金提取协议开始时,首先通过可信信道向银行证明自己的身份 I(也就是提取人知道 u_1),银行检查之后,如果同意提取则向 U 确认。然后 U 与 B 执行类似 Brand 方案^[7]中的现金提取协议(注意:这里必须将提取金额信息通过 hash 函数 H 嵌入到提取的电子现金中)。取款协议执行的结果:得到并保存一个关于 A, M_T, d_t 的盲 Schnorr 型数字签字: $\text{BlindSig}(A, M_T, d_t) = (z, a, b, r_1)$,即, $g^{r_1} \equiv h_a^c \pmod p, A^{r_1} = Z^c b \pmod p$ 。

(1) 用户 U 选择 $s \in_R Z_q, M_T$ 为取款额, $d_t = H_1(\text{drawdate})$,其中 drawdate 为取款日期。

(2) 用户计算: $A_1' = g_3^{(s^{-1})}, B_1' = h_T^s, h_t = g_2^{d_t}$,并用自己的通信私钥对元组 (A_1', B_1', M_T, d_t) 进行签名。将 $A_1', B_1', M_T, d_t, \text{drawdate}$ 及其签名 $\text{sig}_u(A_1', B_1', M_T, d_t)$ 发送给银行。

(3) 用户 U 向银行 B 证明: $\log_{A_1'} g_3 = \log_{h_T} B_1'$,如果 A_1', B_1' 不满足等式,则 B 中止协议。

(4) 银行 B 断定 drawdate 真实有效后,选择 $w \in_R Z_q$,计算 $d_t = H_1(\text{drawdate}), h_1 = g_2^{d_t}, a' = g^w, b' = (h_t A_1')^{-w}$ 后,将 a', b' 发送给用户 U。

(5) 用户 U 计算 $A = (h_t A_1')^s = h_t^s g_3, Z' = h_2^{d_t} h_3^{(s^{-1})}, Z = Z^s = h_2^{d_t s} h_3$,选择 $u, v \in_R Z_q$,然后计算 $a = a^u g^v, b = b^u A^v, c = H_2(A, Z, a, b, M_T, d_t)$ 及 $c' = (c/u) \pmod q$,并将 c 发送给银行 B。

(6) 银行返回 $r_1' = c x_B + w$,并从用户 U 的对应账户减去相应的取款额。B 得到并保存: d_t, A_1', B_1', M_T, w 。

(7) 用户 U 验证: $g^{r_1'} \stackrel{?}{=} h^c a', (h_t A_1')^{r_1'} \stackrel{?}{=} Z^c b'$;如果通过验证,则计算 $r_1 = (r_1' u + v) \pmod q, \text{Balance} = M_T$,U 得到并保存: s, $\text{Balance} = M_T, \text{BlindSig}(A, M_T, d_t) = (z, a, b, r_1)$,也即满足: $g^{r_1} = h^c a \pmod p, A^{r_1} = Z^c b \pmod p$;如果未通过验证,则请求银行重新计算。

以上取款协议中: s 作为现金的密码, (A, M_T, d_t) 作为现金标志, $\text{BlindSig}(A, M_T, d_t) = (z, a, b, r_1)$ 是从银行取得的盲签名,作为现金防伪, Balance 是账户余额。

3.5 支付协议

(1) 用户 U 首先检查自己的电子现金的余额是否足够本次支付额 M_p 及电子现金是否过期,如果 $\text{Balance} < M_p$ 或者电子现金已过期则终止,否则将 A, $M_T, Z, a, b, r, \text{drawdate}, d_t$ 发送给商家 V。

(2) V 验证: $\text{BlindSig}(A, M_T, d_t) \stackrel{?}{=} (z, a, b, r_1)$ 及电子现金未过期,其中 $d_t = H_1(\text{drawdate})$ 。若验证通过,则返回确认信息,否则中止协议。

(3) U 选择 $S_1 \in_R Z_q$,并计算 $c_2 = H_3(A, B, M_T, M_p, \text{datetime1})$,其中 $B = h_t^{s_1}, \text{datetime1}$ 为当前时间,最后 B, $\text{datetime1}, M_p$ 将发送给商家 V。

(4) V 验证 datetime1 的有效性(就是 datetime1 在合理范围内),计算 $c_2 = H_3(A, B, M_T, M_p, \text{datetime1})$ 及 $d = H_4(A, B, I_v, \text{datetime2})$,其中 datetime2 为选取的另一合理时间值, I_v 是商家的身份字,最后将 d 返回给 U。

(5) U 计算: $r = ds + c_2 S_1$ 。

(6) U 选择 $s_2 \in_R Z_q$,计算: $r' = r + t_c + s_2, t = s_2^{-1} + t_c, Y_1 = g_2^{s_2}, Y_2 = g_2^{(s_2^{-1})}$,并将 $r', t, Y_1, Y_2, \text{sig}_T(T_c)$ 传送给 V。

(7) U 向 V 证明 $\log_{g_2} Y_1 = \log_{Y_2} g_2$,V 验证 U 的证明信息,如果真实则继续下一步,否则中止协议。

(8) V 验证: $h_t^{r'} (g_3)^d \stackrel{?}{=} (A^d B^{c_2}) (Y_1 \cdot T_c)^{d_t}, g_2^t \stackrel{?}{=} Y_2 \cdot T_c$,如果通过验证则继续下一步。

(9) V 向用户供货后,U 向 V 传送 r,并计算 $\text{Balance} = \text{Balance} - M_p$ 。

(10) V 验证: $h_1^{r'} (g_3)^d \stackrel{?}{=} A^d B^{c_2}$,如果通过验证则接收现金,否则依据供货信息向可信方请求仲裁。

在支付协议中,所有的随机数都用于扰乱作用。

3.6 存款协议

银行从商家处接收: A, M_T, Z, a, b, r₁, d₁, B, drawdate, date-time1, datetime2, Mp, d, c₂, r 等信息,首先根据 drawdate 断定电子现金没有过期,否则中止协议,然后验证:

- (1) BlindSig(A, M_T, d₁) $\stackrel{?}{=}$ (z, a, b, r₁)。
- (2) h_t^r(g₃)^d $\stackrel{?}{=}$ A^dB^{c₂}。
- (3) datetime1, datetime2, d, c₂ 的正确性。

若以上验证结果正确,则查看电子现金(A, M_T, d₁) 是否已有相同的存款记录存在(也就是对于合法的存款,datetime1, datetime2, c₂, r 应当不同),如果有表明商家企图将同一笔现金存入两次,予以拒绝;否则,在存款数据库中查询(A, M_T, d₁) 的存款额是否超过 M_T,如果未超过,银行接受存款;否则表明现金持有者企图超额支付,银行予以拒绝,并根据存款信息向可信方请求追踪提款人(现金持有者)。

4 效率

我们检验了当 δ=688, k=1, |q|=688, |p|=689(为便于同文献[8] 相比较) 的效率情况(假定随机哈希函数足够快)。除非特别指明,没有假定的预处理,事实上有几个步骤可以进行预处理的。下面我们把文献[3, 8] 的情况同系统进行比较,考虑相同的基准,使用大于 512 位素数模与 512 位的指数进行幂运算。

4.1 存储需求

本方案,用户 U 需要为一个硬币存储 540 字节(s, M_T, Z, a, b, r₁), 银行要为一个硬币存储 400 字节(d₁, A₁ ', B₁ ', M_T, w)。在相同参数被使用时,相比而言,文献[8] 的硬币大小是 323 ~495 字节,文献[3] 的硬币大小是 264 字节。可见,本方案存储需求比文献[8] 的略大。

4.2 计算量

(1) 在本方案取款协议中用户的模指数运算量为 15. 5 次,银行是七次(幂乘按 1. 5 次计算);文献[8] 取款协议中 U 和 B 执行相当于 22 次完全模 N(512 位) 的求幂运算;文献[3] 中,为了达到相同的功能(即获得硬币间的不相关性),用户每次取款时都进行初始化,U 需要执行超过 4 000 次幂运算,对 512 位的基准,这等于大约 32 000 乘幂运算。因此,取款协议中,本方案计算量与文献[8] 相当,远小于文献[3]。

(2) 在支付协议中,本方案的用户只执行五次的模指数运算,商家执行 15 模指数运算;文献[8] 支付时有 5 + n(5L + 2) 次模指数运算,此处 n 是支付的节点数,L 是支付节点的深度;而文献[3] 求幂次数大约为文献[8] 的六倍。文献[8] 支付时平均有九个节点,二叉树最深为 13(将百元钞分割为分计),平均按七层计算,则支付运算量为 5 + 9(5 ×7 + 2) =338 次模指数运算,最多达 608 次。总之,本方案的用户只执行五次的模指数运算,为文献[8] 的 1/66,商家执行 15 次模指数运算,计算量只有文献[8] 的 1/22。

4.3 通信量

在取款协议中,本方案用户发送数据量约为 480 字节,接收数据量约为 260 字节,与文献[8] 相当。在支付协议中,本

方案与文献[8] 比较,客户 U 平均少向商家 V 传送 1 152 字节的数据。

5 安全性及公正性

5.1 安全性

取款协议的安全性同于 Schonorr 签名方案。下面重点讨论支付协议的安全性。电子现金以(A, M_T, d₁) 作为标志,由支付协议验证盲签名 BlindSig(A, M_T, d₁) , = (z, a, b, r₁) ,可保证(A, M_T, d₁) 是来自银行的电子现金。电子现金以(B, datetime1, datetime2, c₂, r) 作为支付标志。

(1) 若 h_t^r(g₃)^d = A^dB^{c₂}, 则 r = ds + c₂s₁。

证:由取款协议的结论可知: A = h_t^sg₃, 设 B = h_t^{s₁}, 则 A^dB^{c₂} = h_t^{ds + c₂s₁}g₃^d, 由离散对数求解困难假设知: r = ds + c₂s₁, 得证。

所以由验证条件 h_t^r(g₃)^d = A^dB^{c₂}, 可防止电子现金拥有者伪造无效的支付信息 r。

(2) 即使向商家支付多笔电子现金,商家不能伪造有效的支付信息。

证:由于商家接收 r = ds + c₂s₁, 对于不同的支付, s 相同,但 s₁ 由客户选取每次不同。则 m 次支付可获得 m 个方程组,但有 m + 1 个未知数,所以商家不可能求解出 s。又由于 d 和 c₂ 是一个哈希值,所以方程组间不满足线性关系,商家就不能组合出支付信息,故商家不能伪造有效的支付信息。

5.2 可信方仲裁协议

在本方案的支付协议过程中, 如果商家在提供货物给客户之前任何时候中止协议,双方都没有损失:一方面, U 没有得到货物;另一方面, V 即使得到 r ', 对他也毫无用处,因为他无法从 r 获得有效的支付信息 r。同样,对于其他任何人,有关 r ' 的数据也是毫无用处的。 如果商家收到了现金,而且客户收到了货物,则交易显然是公平的。 如果客户收到货物,但未能将有效的支付信息 r 传给商家,则此时商家可以凭收货回执向可信方申请获取 r 的信息。可信方根据 T_c 的信息查找到相应的 t_c, 首先计算 s₂⁻¹ = t - t_c, 进而得到 s₂。利用商家提供的 r 计算 r = r ' - t_c - s₂, 最后将 r 返给商家(由于有收货回执,可认为客户已经收到货物)。可见,在这种情况下,对交易双方是公平的,能保证两者都得到互换物,商家收取现金,客户取得货物。综上所述,支付方案在任何状况下都具有公平性。另外,在正常的支付过程中只涉及交易双方,并不需要可信任的第三方介入,所以本方案是一个优化意义上的支付方案。

正确性证明:

(1) r 是正确构造的。sig_T(T_c) 是可信方的签名,从而保证有(g₂)^{t_c} = T_c; 由 5. 1 节结论可知: h_t^r(g₃)^d = A^dB^{c₂}, 不妨设 Y₁ = g₂^a, 且 h_t = g₂^{d_t}, 可以得: (A^dB^{c₂}) · (Y₁ · T)^{d_t} = h_t^{r + t_c + a}g₃^d; 由支付协议验证条件有: h_t^r(g₃)^d = (A^dB^{c₂}) · (Y₁ · T)^{d_t}, 根据求解离散对数难假设,可以认为只可能 r ' = r + t_c + a。从而得证: 对付款方而言,不可能伪造无效的 r 来蒙骗商家。

(2) 商家在最后接收到 r ', r 后仍不能计算出 t_c。 r ' = r + t_c + s₂, 由于 s₂ 是随机选取的,商家不能从 Y₁ = g₂^{s₂}中求解 s₂, 因而商家不能从 r ', r, Y₁ 计算出 t_c; 得证: 商家不能从 r ', r 计算 t_c。

(3) 商家在收到 r 后,不能不付货而计算出 r。由(2) 知即

使商家以前同该客户有过交易也不可能计算出客户的交易私钥 t_c , 并且商家也不能从 $Y_2 = g_2^{(s_2^{-1})}$, 计算出 s_2 , 因而商家不可能根据 $r' = r + t_c + s_2$, 在仅知道 r 条件下计算 r , 也就是商家不可能在不送货的情况下获得有效的支付信息 r 。

综上所述, 可信方仲裁协议是安全的。

5.3 犯罪追踪协议

(1) 前向追踪。由检察机关提出请求, 根据提供的取款信息中的 B_1 和 d_t , 由可信方计算: $A = (B_1)^{(x_T)^{-1} \cdot d_t} \cdot g_3$, 从而追踪现金的花费。

(2) 后向追踪。可信中间人根据检察机关提供的支付信息中的 A 和 d_t 计算: $D = A / g_3$, $D^{d_t^{-1} \cdot x_T} = g_2^{(s \cdot d_t \cdot d_t^{-1} \cdot x_T)} = g_2^{s \cdot x_T} = h_T^s = B_1$; 从而根据取款记录查到相应的取款人。

正确性证明: 在取款协议中, 用户 U 向银行 B 证明: $\log_{A_1} g_3 = \log_{h_T} B_1$; 所以不妨设 $A_1' = g_3^{(s^{-1})}$, $B_1' = h_T^s$ 。由 Schonorr 盲签名协议可知: $A = (h_t A_1')^s = h_t^s g_3$, 所以 $(B_1')^{(x_T)^{-1} \cdot d_t} \cdot g_3 = (g_2)^{x_T(s(x_T)^{-1} \cdot d_t)} \cdot g_3 = g_2^{s \cdot d_t} \cdot g_3 = A$, 因此有结论一: $A = (B_1')^{(x_T)^{-1} \cdot d_t} \cdot g_3$; 显然 $(A / g_3)^{d_t^{-1} \cdot x_T} = g_2^{(s \cdot d_t \cdot d_t^{-1} \cdot x_T)} = g_2^{s \cdot x_T} = h_t^s = B_1$; 故有结论二: $(A / g_3)^{d_t^{-1} \cdot x_T} = B_1$ 。

5.4 超额支付追踪

如果银行证明某个现金(A, M_T, d_t) 的支付额大于本身币值时, 可信方根据支付信息, 用同犯罪追踪协议一样的方法可以找出现金的拥有者。

5.5 匿名性保证

用户提取现金 $A, M_T, Z, a, b, r_1, d_t$, 银行 B 得到并保存: $d_t, A_1'; B_1'; M_t, w$ 。显然, 银行不可以从 $d_t, A_1'; B_1'; M_t, w$ 中获取有关 A, M_T, Z, a, b, r_1 的信息, 即银行不能从用户的取款信息中获取数字现金的信息。在支付过程中, 商家不能取得任何有关用户身份的证明, 只能断定某用户支付一笔现金给自己, 现金是真实的。在存款过程中, 银行为数字现金 $A, M_t, Z, a, b, r_1, d_t$ 建立记录, 并监控存入的数字现金是否超出提取的数字现金, 其中 d_t , drawdate 用于保证电子现金的时间有效性(电子现金是有时间限制的, 必须在一定时间内使用和存入银行, 如五年), 显然银行也不能从电子现金的信息推导出取款人的身份信息。同样从币值揭示信息 $B, datetime1, datetime2, M_p, d$,

c_2, r 也不能获取取款人信息。在几个协议中出现了 d_t, d_t 为三方所共知, 但由于 d_t 只是取款日期, 所以许多用户都可以使用相同的 d_t 而不会对用户的匿名性造成威胁。总之银行联同商家也不能获取用户信息, 因此电子现金是匿名的。

6 结论

论文提出一个紧密联系的协议群, 第一次实现了一个基于可信方的实用离线电子现金系统。该系统具有可撤销的匿名性, 电子现金可分, 支付过程公平且高效。该方案涉及到一个可信方, 但只有在注册阶段和产生争议以及撤销匿名性的时候才涉及, 在正常的支付过程中可信方是离线的。这种电子现金在支付协议中比目前基于二叉树的最快的电子现金的计算量小 60 倍, 并且可以在现有配置的微机上进行适时支付, 是一种高效实用的电子现金。

参考文献:

[1] Chaum, et al. Untraceable Electronic Cash[C]. Advances in Cryptology- Crypto ' 88, German: Springer- Verlag, 1990. 319-327.
[2] T Okamoto, K Ohta. Universal Electronic Cash [C]. Advances in Cryptology- Crypto ' 91, German: Springer- Verlag, 1992. 324-337.
[3] T Okamoto. An Efficient Divisible Electronic Cash Scheme[C]. Advances in Cryptology- Crypto ' 95, German: Springer- Verlag, 1995. 438-451.
[4] Y Frankel, et al. Indirect Discourse Proof: Achieving Fair Off-line E-cash[C]. Proc. Asiacrypt '96. German: Springer- Verlag, 1996. 286-300.
[5] 邓所云, 詹榜华, 等. 一个优化的公平的电子支付方案[J]. 计算机学报, 2002, 25(10): 1094-1098.
[6] 陈恺, 胡予濮, 等. 可撤销匿名性的可分电子现金系统[J]. 西安电子科技大学学报(自然科学版), 2001, 28(1): 57-61.
[7] S Brands. Untraceable Off-line Cash in Wallets with Observers[C]. Advances in Cryptology- Crypto ' 93, German: Springer- Verlag, 1993. 302-318.
[8] A Chan, Y Frankel, Y Tsiounis. Easy Come- easy Go Divisible Cash [C]. Advances in Cryptology- proceedings of Eurocrypt '98. Espoo, Finland: Springer- Verlag, 1998. 561-575.

作者简介:

胡泽军(1972-), 男, 四川资中人, 硕士生, 主要研究方向为电子商务、计算机网络与通信、计算机安全; 吴中福(1941-), 男, 四川内江人, 教授, 博士生导师, 主要研究方向为电子商务、计算机网络与通信、计算机安全; 朱代华(1974-), 四川隆昌人, 硕士生, 主要研究方向为电子商务、远程教育。

(上接第 57 页)

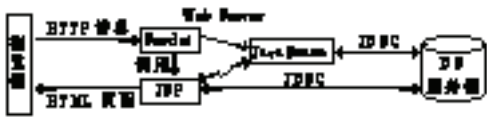


图 5 利用 JSP/Servlet 实现数据库访问

在 Web 服务器所在的主机上驻留了多个 Servlet, 针对每个数据库都有一个 Servlet 专门用来负责对该数据库的访问, 其他 Servlet 可以利用这些 Servlet 提供的方法来访问不同的数据库。这样, 所有的客户端都能透明地访问分布在不同数据库中的数据。

5 结束语

中间件技术改变了传统的 C/S 应用模式, 在客户端和服务端之间加入了中间件, 构成了三层或多层应用模式。本文分

析了众多的 Web 服务器与数据库连接的方案, 由于 Java 技术本身的优势, Servlet/JSP 具有动态、高效、简洁、与平台无关的特点, 适合于开发包含复杂逻辑处理功能的 Web 应用系统, 必将推动数据库应用技术的发展。

参考文献:

[1] 雨阳隆春. 深入 JSP 网络编程[M]. 北京: 清华大学出版社, 2001.
[2] 谢天保, 雷西玲, 张景. 基于 Web 的数据库访问模式的研究[J]. 计算机应用研究, 2002, 19(8): 75-76, 110.
[3] 徐琨, 刘志镜, 来琳涵. Web 数据库访问的中间件技术分析研究[J]. 计算机工程与科学, 2002, 24(4): 54-56.
[4] Sun Java Servlet API Specification[EB/OL]. http: // java. sun. com, 1998.

作者简介:

杜小丹(1972-), 女, 讲师, 硕士, 主要从事计算机应用技术的教学与科研; 张凤荔, 副教授, 主要研究方向为时空数据库和信息安全; 周明天, 教授, 博士生导师, 主要研究方向为网络计算和安全; 于洪(1972-), 男, 计算机辅助教学教研室主任, 讲师。