基于椭圆曲线的多银行电子现金方案

孟显勇
(吉林大学 珠海学院 物流与信息管理系,广东 珠海 519000)

摘 要:目前安全移动终端设备广泛地应用于移动电子商务,但移动终端设备存储能力和处理能力都相对较低,不适合处理基于离散对数问题的电子现金系统。因此,论文基于Wang的方案。提出一个基于椭圆曲线的匿名可撤销的可分的多银行电子现金方案。由于椭圆曲线加密具有密钥强度高,并且椭圆曲线加密可以提高数字签名和认证的速度,因此,论文基于椭圆曲线的电子现金系统对资源和带宽占用率都很低,更适合于安全移动终端和各种嵌入式设备。

关键词:群盲签名;椭圆曲线加密;电子现金;多银行
中图分类号:TP309.2 **文献标识码**:A **文章编号**:1673-629X(2010)12-0221-04

Multi-Bank E-Cash Scheme Based on Elliptic Curve Cryptography

MENG Xian-yong
(Department of Logistics and Information Management, Zhuhai College of Jilin University, Zhuhai 519000, China)

Abstract: At present, the secure mobile terminal equipment is widespreadly applied to mobile electronic commerce, but storage and processing capability of mobile terminal equipment is much lower than those of traditional devices, it does not suit electronic cash system based on the discrete logarithms question. Therefore, this article based on the Wang's scheme proposes one anonymity-revocable divisible multi-bank e-cash system which is based on elliptic curve cryptography (ECC). Because ECC has high strength keys, and it can speed up digital signature and authentication, therefore, this scheme based on elliptic curve cryptography has low occupancy rate to the resources and the bandwidth, and it is more suitable for the safe mobile termination and all kinds of embedded equipment.

Key words: group blind signature; elliptic curve cryptography; electronic cash; multi-banks

0 引 言

随着3G移动业务的发展,促进了语音和视频业务的发展,进而也推动了移动电子商务的发展[1]。随着安全移动终端设备在移动电子商务的应用,需要建立一种安全强度高、系统资源占用率低和适合安全移动终端设备的电子现金系统[2]。

基于椭圆曲线的高效的移动安全电子现金系统尤其适合目前大量的基于智能卡的安全移动终端处理设备[3],并且与WPKI结合,可以构建安全高效的移动商务安全平台[4]。电子现金系统由Chaum[5]第一次提出,Chaum基于盲签名技术提出的电子现金系统为用户完全保护隐私的同时,也为不法分子利用电子现金的完全匿名性进行敲诈和洗钱等违法犯罪活动提供了便利。基于完全匿名电子现金系统的缺陷,Stadler[6]和Brickell[7]分别提出了匿名可撤销的电子现金系统,对于非法电子现金可以在可信第三方的协助下进行跟踪。因此条件匿名的电子现金系统,在保护用户的隐私的同时也防止犯罪分子敲诈和洗钱等违法活动。此后,Camenisch[8]等人和Frankel[9]等人分别提出了公平的离线的电子现金系统的概念,实现了交易双方的交易公平性;Okamoto和Ohta[10]提出了可分的电子现金系统,系统可以对电子现金进行任意地分割并进行灵活地支付,该系统的电子现金从可分性上更接近传统货币支付习惯;Brands[11]提出的一种利用Smart卡的电子支付系统,通过Smart卡保存和支付电子现金,实现电子现金的任意可分性。近年来,国内诸多学者在上述方案的基础上进一步改进,提出了公平的条件跟踪的多银行的电子现金方案。Wang提出了一个公正可分的多银行电子现金方案[12],Wang提出的方案是基于离散对数问题的,对于目前电子商务的一些安全移动终端设备来说,占用系统资源高、密码强度低、占用无线带宽高。

论文基于Wang的方案,提出一个基于椭圆曲线的公正的可分的多银行电子现金方案。由于椭圆曲线加密(Elliptic Curve Cryptography)具有密钥强度高,即

收稿日期:2010-04-19;**修回日期**:2010-07-21
基金项目:广东省粤港关键领域重点突破项目(2005A10 307005)
作者简介:孟显勇(1973-),男,内蒙古赤峰人,讲师,硕士,主要从事信息安全、电子支付、电子商务安全方面的研究。

在同等安全强度下密钥长度较短，160bit 的 ECC 可以提供与 1024bit 的 RSA 或 DSA 相当的安全性，并且椭圆曲线加密实现数字签名的产生与认证的速度要比 RSA 快，并能设计出密钥更短的公钥密码体制。因此，基于椭圆曲线的电子现金系统占用资源和带宽都较低，使系统更适合于安全移动终端和各种嵌入式设备。通过对论文电子现金系统的安全性、条件匿名性以及可跟踪性分析，证明该电子现金系统既具有简单性又具有高效性。

1 用于加密的有限域椭圆曲线的构造

1.1 椭圆曲线定义

将椭圆曲线(Elliptic Curve)应用于加密，是利用有限域上椭圆曲线的点构成的群实现离散对数加密。满足椭圆曲线方程的一个有序对偶称为一个点，常用 T、N 表示。T 的坐标为 $T=(x,y)$，x、y 属于该有限域。文中 T 的 x、y 坐标分别表示为 $R_x(T)$ 和 $R_y(T)$。

如果用 F 表示一个有限域，E 表示域 F 上的椭圆曲线，则 E 是一个点的集合：

$$E/F=\{y^2+a_1xy+a_3y=x^3+a_2x^2+a_4x+a_6,a_1,a_2,a_3,a_4,a_6,x,y\in K\}\cup\{O\}$$

用 O 来表示椭圆曲线上的无穷远点。

椭圆曲线 E 上的“+”运算定义，如果 T 和 S 是椭圆曲线上的两个点，求 $S=T+N$。S 表示通过曲线上的 T，N 两点的直线与曲线上的另外一点相交，然后作交点的关于 x 轴的对称点坐标。当 $T=N$ 时，S 表示过椭圆曲线上的 T 点求椭圆曲线在该点的切线与椭圆曲线上的另外一个点的交点关于 x 轴的对称点坐标。因此，由 $(E,+)$ 构成一个可交换 Abel 群，该 Abel 群上的加法单位元是 O。

椭圆曲线上的点乘运算是椭圆曲线密码系统的核心运算之一。椭圆曲线上的点乘运算定义如下：

$nT=T+T+\cdots+T$，表示 n 个 T 相加。即对于给定的一条椭圆曲线 E，在曲线 E 上的一点 T，对 T 点作 n 次加法运算所得的结果。点乘运算是椭圆曲线中的主要运算，点乘运算的速度会直接影响到椭圆曲线加密的速度。

椭圆曲线加密算法基于椭圆曲线离散对数运算的困难性。对于任意给定的椭圆曲线 E 求点乘运算 $nT=P$，并且 T 和 P 是椭圆曲线上的点。

椭圆曲线上离散对数的运算困难性是：已知 n 和椭圆曲线上的点 T，求 $P=nT$ 是容易的。反之，如果已知椭圆曲线上的点 T 和 P，求 n 满足 $nT=P$ 却是相当困难的。目前，椭圆曲线加密体制就是基于求解椭圆曲线上的离散对数的困难性的基础上设计的。

1.2 椭圆曲线选定

基于椭圆曲线的电子现金系统选择有限域 F 为素数域 $p=2^m$ 或 $p=q$，其中 q 为素数。如果选择硬件来实现电子现金系统，一般选择有限域为 $p=2^m$ 上的元素[13]。因为有限域 $p=2^m$ 的二进制的逻辑运算适合硬件实现。如果使用现有的处理软件实现电子现金系统，一般选择素数域上的元素。因为可以应用一些标准的运算模块来实现。文中选择的椭圆曲线为非超奇异椭圆曲线。因为，超奇异椭圆曲线存在亚指数算法，另外，并不是所有椭圆曲线都是安全的椭圆曲线，电子现金系统使用的椭圆曲线的阶必须为大素数或者含有大素数因子。安全的椭圆曲线才具有求解椭圆曲线上的离散对数的困难性，所以设计的电子现金系统前必须选择一个安全的椭圆曲线。

2 电子支付协议

2.1 系统的初始化

2.1.1 可信第三方 TTP 设置

可信第三方 TTP 在有限素数域上选择一条安全的椭圆曲线 E。并且有限素数域的高阶基点分别是 $G_0,G_1,G_2\in E(F_p)$，设有限素数域 F 的高阶基点的阶为 N。可信第三方 TTP 选取 p 为大素数。设 $x\in_R Z_n^*$ ($x<N$，并且协议中以后产生的随机整数都小于阶 N)，点 G_0,G_1,G_2 为基点。设 $y=x\cdot G_0 \bmod p$，其中：$x\cdot G_0 \bmod p$ 的运算表示在椭圆曲线上完成 $x\cdot G_0$ 运算后，取 $(x\cdot G_0)$ 的 x 坐标值在模 p 的运算，即 $y=R_x(x\cdot G_0) \bmod p$，其中 $R_x(G)$ 表示取点 G 的 x 坐标，以后不作特殊声明均按此规则进行运算。选择安全的哈希函数 $H(.)$，公开 $\{E(F_p),G_0,G_1,G_2,H(.)\}$，可信第三方 TTP 随机选择私钥 $x_T\in_R Z_n^*$，公钥为 $f_2=x_T\cdot G_1 \bmod p$，并计算 $f_3=x_T^{-1}\cdot G_2 \bmod p$。

2.1.2 银行群 (B,B_i) 设置

每个分行 B_i 选取私钥 x_i，其公钥为 $y_i=x_i\cdot G_2 \bmod p$；总行 B 的私钥为 x_B；公钥为 $y_B=x_B\cdot G_2 \bmod p$；总行 B 负责为每个分行 B_i 颁发有权发行电子现金的证书 $\{r_i,s_i\}$，$k_i\in_R Z_n^*$。

$$r_i=(-k_i\cdot G_0+k_i\cdot y_i) \bmod p,\ s_i=k_i-r_i\cdot x_B\cdot \bmod p$$

2.1.3 用户 U 设置

用户 U 选择任意一家有发行电子现金权利的银行 B_i 并开户。用户在新开立的帐户中存取一定的额度的存款。用户 U 与银行 B_i 合作生成电子现金，用户 U 与银行 B_i 共同确定 INF = {endtime, M_T}，其中，endtime 是电子现金的有效期；M_T 是要取的币值；U 与

B_i 各自计算 $G_3 = H(\mathrm{INF}) \cdot G_0 \bmod p$。然后,U 随机选取 $u_1 \in_R Z_n^*$,计算 $I = u_1 \cdot G_3 \bmod p$,用户 U 将 I 作为身份证明信息发送给银行 B_i,银行 B_i 将身份证明信息 I 与用户 U 相关信息一起保存。

2.2 用户取款协议

2.2.1 用户零知识证明身份

用户 U 在不泄露 u_1 的前提下,通过零知识证明来向银行 B_i 证明自己确实掌握 u_i,证明过程如下:

1) 用户 U 在有限域 F 中随机选择 $w_1 \in_R Z_n^*$,计算 $T = w_1 \cdot G_3 \bmod p$,用户 U 将 T 发给银行 B_i;

2) B_i 计算 $c_B = H(T \| \text{date/time}) \bmod p$,并将 c_B 发送给用户 U;

3) 用户计算 $y = w_1 - c_B \cdot u_1 (\bmod p)$,将 y 发送给 B_i;

4) B_i 验证 $c_B = H(y \cdot G_3 + c_B \cdot I \| \text{date/time}) \bmod p$,若成立,说明用户的证明有效。

2.2.2 生成电子现金

用户与银行 B_i 交互执行下面的协议:

step1　B_i 随机选择 $a, b, d \in_R Z_n^*$,然后计算 $A = a \cdot r_i \bmod p$, $B = a \cdot s_i - b \cdot H(A \| C \| D \| E) \bmod p$, $C = r_i \cdot a - d \bmod p$, $D = b \cdot G_0 \bmod p$, $E = d \cdot y_B \bmod p$, $\alpha_i = B \cdot G_0 + C \cdot y_B + E + H(A \| C \| D \| E) \cdot D (\bmod p)$

step2　用户 U 随机选择 $r, s \in_R Z_n^*$,然后计算 $I' = u_1 \cdot s^{-1} \cdot G_3 + s^{-1} \cdot G_2 (\bmod p)$, $E_1 = s \cdot G_1 + r \cdot f_3 (\bmod p)$, $E_2 = r \cdot G_2 \bmod p$, $m = s \cdot (I' + G_1) \bmod p$,并将 E_1, E_2, m 传送给银行 B_i;

step3　B_i 验证其正确性,并保存 E_1, E_2, m 同时计算 $R = t \cdot \alpha_i \bmod p$, $t \in_R Z_n^*$ 并发送 R 给用户 U;

step4　用户 U 收到 R 计算 $z = s \cdot R \bmod p$,并计算出 $e = H(\mathrm{INF} \| z) \bmod p$,将 e 发送给 B_i;

step5　银行 B_i 求解方程 $e = x_i \cdot R + t \cdot S \bmod p$,计算出参数 S, $S = t^{-1} \cdot (e - x_i \cdot R) \bmod p$,银行将生成的电子现金标记为:e_ cash $= \{A, B, C, D, E, R, S, e, m$ INF$\}$。

step6　银行 B_i 将电子现金 e_ cash 发送给用户 U,用户 U 对电子现金的有效性进行验证。用户 U 验证等式 $e \cdot \alpha_i = R \cdot (\alpha_i + A) + S \cdot R (\bmod p)$ 的正确性,如果验证正确,用户 U 接受银行发送的电子现金 e_ cash,并修改电子现金的余额为 blance $= M_T$。

2.3 支付协议

在交易过程中,若用户 U 选购价格为 M_p 的商品,需要支付金额为 M_p 的电子现金。用户 U 首先检查支付卡中的账户余额 balance,如果 balance $< M_p$ 证明用户 U 余额不足,系统会自动终止协议。否则电子现金系统执行如下协议:

step1　用户 U 计算 $A_1 = u_1 \cdot G_3 + s \cdot G_1 (\bmod p)$, $A_2 = s \cdot f_2 (\bmod p)$,并将自己的 e_ cash 和 A_1, A_2, M_p 发送给商家。

step2　商家收到 e_ cash 和 A_1, A_2, M_p,对其进行验证,商家计算:

$\alpha_i = B \cdot G_0 + C \cdot y_B + E + H(A \| C \| D \| E) \cdot D (\bmod p)$ 并验证:

$e \cdot \alpha_i = R \cdot (\alpha_i + A) + S \cdot R (\bmod p)$ 的正确性,若未通过验证拒绝用户支付,否则接收用户支付,并计算:$G_3 = H(\mathrm{INF}) \cdot G_0 \bmod p$,

$d = H(A_1 \| A_2 \| I_s \| \text{paytime})$

商家发送 d 给用户。其中,I_S 表示商家在银行的账号。

step3　用户 U 选择 $s_1 \in_R Z_n^*$, $B_0 = u_1 \cdot s \cdot G_3 \bmod p$ 计算 $h = H(A_1 \| A_2 \| M_T \| M_P, \text{paytime})$, $n_1 = h \cdot s_1 \cdot G_3 \bmod p$, $r_1 = d \cdot u_1 \cdot s + s_1 (\bmod p)$,将 n_1, h, r_1 发给商家。

step4　商家检验如下等式是否成立 $h = H(A_1 \| A_2 \| M_T \| M_P, \text{paytime})$, $r_1 \cdot G_3 \bmod p = d \cdot B_0 + h^{-1} \cdot n_1 (\bmod p)$,若成立,则接受 e_ cash,并保存 e_ cash, A_1, A_2, M_p, n_1, r_1, paytime, d 而用户则保存 balance = balance $- M_P$。

2.4 存款协议

商家 S 将得到的电子现金 e_ cash,以及支付信息 e_ cash, A_1, A_2, M_p, n_1, r_1, paytime, d 发送给银行 B_i,银行 B_i 验证有效性。

首先,银行 B_i 检验电子现金是否在有效期内,若在有效期内则验证等式:$e \cdot \alpha_i = R \cdot (\alpha_i + A) + S \cdot R (\bmod p)$ 的正确性,若未通过验证,证明商家有伪造行为。

然后,银行在"已支付 e_ cash"的银行数据库中检索,若检索到,证明商家重复存款,否则接收商家存款。中央银行 B 会定期地公布已花费电子现金表,每个发币银行 B_i 都会拥有一个在线的已花费电子现金数据库支持存款阶段电子现金有效性的验证。

3 方案的安全性分析

3.1 可追踪性

1) 可疑用户的追踪。

TTP 与 B_i 合作,TTP 接受 B_i 发过来的 A_1, A_2,并计算 $I = A_1 - x_T^{-1} \cdot A_2 (\bmod p)$,通过 I 来确认用户 U 的身份。

2) 可疑货币的追踪。

TTP 与银行 B 合作，TTP 接受银行 B 发过来的 I，E_1, E_2，并计算 $m = I + (E_1 - x_T^{-1} \cdot E_2) + G_2 \bmod p$。TTP 将计算得到的 m 发送给银行 B，银行 B 对 m 进行跟踪，当存款时 m 会出现，B 可以在支付或存款时跟踪识别可疑电子现金。

3) 发币银行确认。

总行 B 可以确认电子现金的发币银行，通过验证以下等式：

$$x_B \cdot r_i \cdot \alpha_i \cdot G_0 \bmod p = k_i \cdot (C \cdot y_B \cdot G_0 + E) \bmod p$$

如果等式成立，那么相应的 r_i 对应的那个成员就是发币者 B_i。

3.2 方案的安全性

3.2.1 银行 B 无法伪造签名

群权威 B 知道 $\{r_i, s_i, k_i\}$，要伪造签名必须知道 x_i，要获得 B_i 私钥只能通过 y_i 求解 x_i，由椭圆曲线加密知道其困难性相当于求解椭圆曲线离散对数。

3.2.2 用户无法识别签名身份

由 (A, B, C, D, E) 得到 $\{r_i, s_i, k_i\}$ 的困难性也相当于求解椭圆曲线离散对数的困难性，所以用户无法识别签名者的身份。

3.2.3 B_i 签名无法伪造

每次签名过程中，群成员 B_i 选择不同的 a, b, d, t，故伪造签名必须解决椭圆曲线离散对数问题。

3.2.4 防止重复花费

若商家重复存款电子货币，银行在存款前对电子货币进行验证，到银行数据库检索，若检索到电子货币存在，并且 paytime 与数据库电子货币相同，说明支付时间相同，证明是商家重复存款，而不是用户重复支付。

若用户重复支付电子货币，B_i 将 A_1, A_2 发送给 TTP，TTP 计算 $I = A_1 - x_T^{-1} \cdot A_2 (\bmod p)$，即得该用户的身份。

3.2.5 防止伪造

若用户要伪造电子现金 e_cash = $\{A, B, C, D, E, R, S, e, m$ INF$\}$，必须可以伪造电子货币里的 S，因为商家在接收电子现金前要对等式 $e \cdot \alpha_i = R \cdot (\alpha_i + A) + S \cdot R (\bmod p)$ 进行有效性验证。而 $S = t^{-1} \cdot (e - x_i \cdot R) \bmod p$ 是银行 B 的签名，每次生成电子现金时 t 是由 B_i 随机选择，并且 x_i 为银行 B_i 的私钥，因此，伪造 e_cash 里的 S 的困难性相当于求解椭圆曲线上离散对数。

同理，若商家伪造电子现金 e_cash = $\{A, B, C, D, E, R, S, e, m$ INF$\}$，也需要能伪造出电子现金里的 S，而 $S = t^{-1} \cdot (e - x_i \cdot R) \bmod p$ 是银行 B 的签名，每次生成电子现金时 t 是由 B_i 随机选择，并且 x_i 为银行 B_i 的私钥，因此，伪造 e_cash 里的 S 的困难性相当于求解椭圆曲线上离散对数。

4 结束语

论文基于 Wang 的方案，提出一个基于椭圆曲线的匿名可撤销的可分的多银行电子现金方案。由于椭圆曲线加密具有密钥强度高，并且椭圆曲线加密实现数字签名的产生与认证速度快，因此，论文基于椭圆曲线的电子现金系统对资源和带宽占用率都很低，更适合于安全移动终端和各种嵌入式设备。通过对论文电子现金系统的安全性、条件匿名性以及可跟踪性分析，证明该电子现金系统既具有简单性又具有高效性。

参考文献：

[1] 张方国，张福泰，王育民. 多银行电子现金系统[J]. 计算机学报，2001，24(5)：455－462.

[2] 王天银，蔡晓秋，张建中. 基于椭圆曲线的离线多银行电子现金系统[J]. 计算机工程，2007，33(15)：155－157.

[3] 蔡庆华. 一个基于椭圆曲线的前向安全的签密方案[J]. 计算机技术与发展，2007，17(12)：132－135.

[4] 周红生，王 斌，铁 玲，等. 基于代理签名的多银行电子现金系统[J]. 上海交通大学学报，2004，38(1)：79－82.

[5] Chaum D. Blind Signature for Untraceable Payments[C]// Advances in Cryptology－Crypto'82. Berlin: Springer－Verlag, 1983: 199－203.

[6] Stadler M M, Piveteau J, Camenisch J. Fair Blind Signatures [C]//Advanced in Cryptology EUROCRYPT'95. [s. l.]: Springer Verlag, 1995: 209－219.

[7] Brickell E, Gemmell P, Kravitz D. Trustee－based Tracing Extension to Anonymous Cash and the Marking of Anonymous Change[C]//Proc. 6th Annual ACM－SIAM Symposium on Discrete Algorithms (SODA). [s. l.]: [s. n.], 1995: 157－166.

[8] Camenisch J L, Piveteau J M, Stadler M A. Digital Payment Systems with Passive Anonymity Revoking Trustees [J]. Journal of Computer Security, 1997, 5(1): 69－89.

[9] Frankel Y, Tsiounis Y, Yung M. Indirect Discourse Proofs: Acheieving Efficient Fair Off－line E－cash[C]//Advanced in Cryptology ASIACRYPT'96. [s. l.]: Springer Verlag, 1996: 286－300.

[10] Okamoto T, Ohta K. Universal Electronic Cash[C]//Advances in Cryptology Crypto'91, Lecture Notes in Computer Science. [s. l.]: Springer－Verlag, 1992: 324－337.

(下转第 254 页)

对数据进行必要的验证和转换。在业务层,Spring 管理服务层组件,并负责向 Action 提供调用业务模型组件和 DAO 组件以完成业务逻辑,并提供事务处理、缓冲池等容器组件以保证数据的完整性和提高系统性能。在数据持久层,Hibernate 则根据模块需要的各种持久化操作,确定对应的 DAO 操作,并利用其对象化映射和数据库交互,分析模块所涉及的表,确定表之间的关系,并处理 DAO 组件请求的数据,返回处理结果。整个业务逻辑层使用整合 SSH 架构[8~12],即除了包含 Spring 外,还包括 Struts 和 Hibernate 的一部分,如图 3 中的虚线。采用 SSH 整合开发模型,不仅实现了业务逻辑层与数据持久层的分离,还实现了视图、控制器与模型的分离,而且数据库的变化也不会影响前端,从而大大提高了系统的可重用性。

4 SSH 整合框架在网络教学平台中的应用

下面是以网络教学平台的用户身份认证系统来说明 SSH 框架的实现。

用户身份认证是指用户登录网络教学平台时的身份验证过程。在本网络教学平台中,用户身份有管理员、教师和学生三种。用户首先从 logon.jsp 页面输入登陆信息,并通过 struts 调用 staticsQueryAction 的 createOperateLog()方法获取用户输入信息,以便判断登录用户类型是管理员、教师还是学生,再通过不同方法调用数据访问层中的 DAO 从而获取登录用户的具体信息。然后利用 Hibernate 访问具体的数据表来获取持久化对象,并处理 DAO 中的具体数据,从而实现从 java 类到数据表之间的映射,stasticsQueryAction 将返回的登录用户对象放到 session 会话上,以便检查用户是否登录,再通过 struts 返回到 logon.jsp 页面。

在设计用户身份认证系统的查询与统计功能时,采用 spring 的 ioc 框架定义接口变量和变量所对应的 setter 方法,而实例化对象的具体操作则由 spring 完成,即 spring 在运行时读取配置文件来完成对象实例化。在查询时,先利用 spring 创建 bean,应用业务注入实现数据持久层的通信,并配置注入 DWR 所需要的且能供 DWR 框架将 Java 代码编译成 Js 时使用的 DAO;然后,设置 hibernate 的属性,并确定 hibernate 使用的数据库语句;最后配置 struts 中 action 所需要使用的 DAO 和 service。

5 结束语

基于 MVC 模式的网络教学平台运用多种模式的设计,采用松散耦合的编程体系结构,分离了业务逻辑层、数据持久层和表示层,有效地减少了远程调用的次数,提高了系统响应速度。实践证明,本平台采用了先进的 MVC 模式开发、分层架构,简化了 Web 应用程序的开发过程,提高开发效率,缩短开发周期,提高了系统的可扩展性;同时,对数据对象的封装存储,有效地屏蔽了后台数据库的数据结构,提高了系统的安全性。

参考文献:

[1] 袁守华.基于 Web 的课程网络教学网站的开发与应用[J].中原工学院学报,2004,15(1):49-53.

[2] 邱旭东,刘文浩.基于 JSP 的 MVC 改进模式研究及应用[J].计算机技术与发展,2006,16(8):134-136.

[3] Davis M,Consultant. Struts, an open-source MVC implementation[EB/OL]. 2001. http://www.ibm.com/developerworks/java/library/j-struts/index.html.

[4] Harrop R. Spring 专业开发指南[M].成都:电子工业出版社,2006.

[5] Johnson R,Hoeller J. The Spring Framework Reference Documentation[EB/OL]. 2008. http://static.springframework.org/spring/docs/2.5.x/reference/.

[6] Hibernate Reference Documentation 3.5.1[EB/OL]. 2007. http://docs.jboss.org/hibernate/stable/core/reference/en/pdf/hibernate-reference.pdf.

[7] Alur D, Crupi J, Malks D. Core J2EE Patterns: Best Practices and Design Strategies[M]. American: Prentice Hall, 2003.

[8] 韩义亭,张成宇.SSH 架构及其在 Web 开发中的应用[J].网络安全技术与应用,2007(10):72-74.

[9] 李腊元,徐 鹏.基于 MVC 模式的 JSF,Spring 和 Hibernate 整合[J].计算机技术与发展,2008,18(3):46-49.

[10] 廖胜军.基于 SSH 整合架构的应用研究[D].武汉:武汉理工大学,2008.

[11] 张 飞,张 建.基于 Spring 与 Hibernate 的数据库访问技术研究[J].计算机工程与设计,2009,30(7):1668-1670.

[12] 李 宁.Java Web 开发技术大全—JSP + Servlet + Struts 2 + Hibernate + Spring + AJAX[M].北京:清华大学出版社,2009.

(上接第 224 页)

[11] Brands S. Untraceable off-line cash in wallets with observers [C]//Advanced in Cryptology CRYPTO'93. [s.l.]: Springer-Verlag,1993:302-318.

[12] 王大星,杜育松,沈 静.公正可分的多银行电子现金支付方案[J].计算机工程,2007,33(16):126-127.

[13] 邹候文,王 峰,唐 屹.椭圆曲线点乘 IP 核的设计与实现[J].计算机应用,2006,26(9):2131-2136.