一种基于 CL 的新型可分电子现金系统

岳 璐,贾小珠,茹俊丽

(青岛大学 信息工程学院,山东 青岛 266071)

摘 要:基于 CL 签名给出了一种新型的可分电子现金系统,有效地将压缩支付和批处理支付加入到系统中,给出了实用的压缩可分电子现金方案,使得系统的效率较高。系统中无需可信第三方的参与,系统开销较小。方案的安全性基于 LRSW 假设、计算离散对数困难性假设以及单向散列函数存在性假设。

关键词:可分电子现金;常数级时间复杂度;压缩支付;双线性映射

中图分类号:TP393 **文献标识码**:A

A new divisible e-cash system based on CL

YUE Lu, JIA Xiao-zhu, RU Jun-li

(College of Information Engineering, Qingdao University, Qingdao 266071, China)

Abstract: Based on CL signature, this paper gives a new type of divisiable e-cash system, which constructs a security compact e-cash scheme of high efficiency by including compact spending and bactch spending. It reduces the costs of the system as it's without TTP. The security of the scheme is based on the assumptions of decision Diffie-Hellman, the hardness of calculating discrete logarithm and the LRSW assumptions.

Key words: divisible e-cash; constant complexity; compact spending; billinear pairings

可分电子现金一直是电子现金领域中的研究热点[1-4],目前,影响可分电子现金系统发展的问题主要有两方面:一是重复花费现象严重,二是效率低下。对于重复花费问题,许多学者提出多种追踪方案。但大多数都采用了引入可信第三方的方法[5-7],这种方法可有效地追踪非法用户,但在可信第三方面前,任何用户都不再具有匿名性,不能很好地满足合法用户的匿名性要求。而且,引入可信第三方,增加了系统开销,降低了系统效率。针对效率问题,CAMENISCH、HOHENBERGER 和 LYSYANSKAYA 在参考文献[6]中给出了离线的安全匿名的电子现金协议(CHL 协议),在此协议中,用户提取价值量为 k 的电子钱包,设系统的安全参数为 λ,则取款协议和支付协议的时间复杂度为 $O(\lambda+\log(k))$。M H Au 等人通过引入单向计数器提高了压缩的电子现金的效率[8]。在电子系统领域,由参考文献[9]可知,基于双曲线的 CL 更加高效,本文充分利用了这一优点,在参考文献[9]的基础上,提出通过加入两协议:批处理支付和压缩支付的方法,有效地解决了可分电子现金领域的效率问题。将系统的时间复杂度由 $O(\lambda+\log(k))$ 改进到 $O(\lambda)$。其中,批处理支付指用户支付给商家电子钱包中任意大小的货币,压缩支付指用户 1 次支付给商家整个电子钱包中的货币。另外,针对于可分电子现金领域中的重复花费问题,无须可信第三方的参与,系统在取款协议中加入了一个随机参数 y,每当用户执行压缩支付时,必须通过对 y 的计算才能得到相应的 C_i,从而计算 $T_i=g^u B_i^R$。如果用户重复使用电子现金,则通过 (s,t) 和 T_c 进行追踪,找出重复花费电子现金者。

1 预备知识

1.1 符号定义

设双曲线映射 $\hat{e}:G_1\times G_2\to G_T$。

其中:G_1、G_2 分别是基为素数 p 的循环群,它们可以相同也可以不同。

G_1、G_2、G_T 中的元素都有唯一的二进制表示。

g_0、h_0 分别是群 G_1、G_2 的生成元。

$\psi:G_2\to G_1$ 是同构体 G_2 到 G_1 的映射,满足 $\psi(h_0)=g_0$。

$\forall x \in G_1, x \in G_2, a, b \in Z_p$ 满足 $\hat{e}(x^a, y^b)=\hat{e}(x,y)^{ab}$。

g_0、h_0 满足 $\hat{e}(g_0, h_0) \neq 1$。

1.2 数学假设

1.2.1 DDH 假设

循环群 G 上的 DDH 假设为：给定 g, g^a, g^b, g^c，去判断 $g^{ab}=g^c$ 是否成立是困难的。其中，g 为 G 的生成元，a、b、c 为随机数，满足 $a, b, c \in \{0, 1, \cdots, q-1\}$。DDH 假设与解离散对数问题相关，因此，在循环群 G 中基于离散对数的困难性假设，DDH 假设是成立的。

1.2.2 y-DDHI 假设[6,13]

素数循环群 G 上的 y-DDHI 假设指对于给定 $(y+2)$ 元组 $(g, g^x, g^{x^2}, \cdots, g^{x^y}, g^c) \in G^{y+2}$，判定 $c=1/x$ 是否成立是困难的。在离散对数困难性假设下，群 G 上的 y-DDHI 假设是成立的。

1.2.3 LRSW 假设[14]

设 $G=<g>$ 是以素数 p 为底的循环群，$u=g^x$，$v=g^y$，$O_{u,v}(\cdot)$ 满足对于 $a \in G, m \in Z_p$ 能够计算得到 (a^y, a^{x+mxy})。素数群 G 上的 LRSW 问题指：对于 $g, u, v, O_{u,v}(\cdot)$，求 (m, a, b, c) 满足 $m \neq 0 \wedge a \in G \wedge b=a^y \wedge c=a^{x+mxy}$，且 m 不是 $O_{u,v}(\cdot)$ 的输入。素数群 G 上的 LRSW 假设指素数群 G 上的 LRSW 问题是难解的。

2 基于 CL 签名的压缩电子现金方案

2.1 银行初始化

λ 为系统安全参数，(G_1, G_2) 是双线性群组，同构体 G_1、G_2 满足 $|G_1|=|G_2|=p$。

假设 G_p 是以 p 为底的群，且满足 DDH 假设。

设 $H: \{0,1\}^* \rightarrow Z_p$ 是加密哈希函数。

G_2 的生成元 h_0 满足 $\psi(h_0)=g_0$，G_1 的生成元 g_1、g_2、g_3，G_p 的生成元 u_1、u_0。银行随机选择 $\alpha, \beta, \gamma_1, \cdots, \gamma_4 \in {}_R G_p$，并计算 $X=h_0^\alpha$，$Y=h_0^\beta$，$Z_1=h_0^{\gamma_1}$，$\cdots$，$Z_4=h_0^{\gamma_4}$，$w_1=Y^{\gamma_1}$，$\cdots$，$w_4=Y^{\gamma_4}$。银行的私钥 $\mathrm{bsk}=(\alpha, \beta, \gamma_1, \cdots, \gamma_4)$，公钥 $(h_0, g_0, g_1, g_2, g_3, u_0, u_1, X, Y, Z_1, \cdots, Z_4, W_1, W_4)$。对于任意 $\alpha_r, \beta_r \in {}_R Z_p$，银行计算 $X_r=h_0^{\alpha_r}$，$Y_r=h_0^{\beta_r}$，然后，银行对 $i(i=1, \cdots, k)$ 计算 CL 型签名 $\sigma_i=(a_i, b_i, c_i)$，$(a_i, b_i, c_i)=(a_i, a_i^{\beta_r}, a_i^{\alpha_r+k\alpha_r\beta_r})$，其中 a_i 是随机产生的。

2.2 用户初始化

用户获得公私钥对 (u_0^x, x)。其中 $u_0^x \in G_p, x \in Z_p^*$。

2.3 取款协议

用户随机选择 $s, t, y, r \in {}_R Z_p$，运用公私钥对 (u_0^x, x)，计算 $C=h_0^s Z_1^t Z_2^x Z_3^y Z_4^r \in G_2$，$\Pi_0=PK\{(s,t,x,y,r): C=h_0^s Z_1^t Z_2^x Z_3^y Z_4^r \Lambda PK=u_0^x\}$，用户将 C 与 Π_0 发送给银行，银行检验 Π_0 是否正确，若正确，则随机选择 $d \in {}_R G_p$，计算 $a=h_0^d$，$A_1=a^{\gamma_1}$，$\cdots$，$A_4=a^{\gamma_4}$，然后计算 $b=a^\beta$，$B_1=A_1^\beta$，$\cdots$，$B_4=A_4^\beta$，$c=a^\alpha C^{d\alpha\beta}$。最后，银行将 $(a, b, c, A_1, A_2, A_3, A_4, B_1, B_2, B_3, B_4)$ 发送给用户，作为用户的电子钱包标志。对于 $i=1, \cdots, 4$，$\hat{e}(g,c)=\hat{e}(\psi(X), ab^s B_1^t B_2^x B_3^y B_4^r)$，银行检验 $\hat{e}(\psi(a), Z_i)=\hat{e}(g, A_i)$，$\hat{e}(\psi(a), Y)=\hat{e}(g, b)$，$\hat{e}(\psi(A_i), Y)=\hat{e}(g, B_i)$ 是否成立，若都成立则取款成功，将 $(a, b, c, A_1, A_2, A_3, A_4, B_1, B_2, B_3, B_4)$ 存入电子钱包。

2.4 支付协议

设用户的电子钱包为 $(a, b, c, A_1, A_2, A_3, A_4, B_1, B_2, B_3, B_4, s, t, x, y, r, J)$，其中，$J \leqslant k$，商家身份为 I，并同意取款信息，计算 $R=H(\mathrm{info}, I)$。

2.4.1 单一货币的支付协议

用户计算 $S=u_1^{\frac{1}{s+J+1}}$，$T=u_0^x u_1^{\frac{R}{t+J+1}}$，任意选择 $r_1, r_2, r_3, r_4, r_5 \in Z_p$，计算 $A_T=g_1^J g_2^t g_3^{r_5}$，$\tilde{a}=a^{r_1}$，$\tilde{b}=b^{r_1}$，$\tilde{c}=c^{r_1}$，$\tilde{A}_i=A_i^{r_1}$，$\tilde{B}_i=B_i^{r_1}$，其中，$i=1, \cdots, 4$，并计算 $\hat{c}=\tilde{c}^{r_2}$，找到银行对 J 的 CL 签名 (a_J, b_J, c_J)，然后计算 $(\tilde{a}_J, \tilde{b}_J, \tilde{c}_J)=(a_J^{r_3}, b_J^{r_3}, c_J^{r_3 r_4})$，$\mathrm{SPK}\Pi_1$。为简便起见，令 $E_{\hat{c}}=\hat{e}(g_0, \hat{c})$，$E_{\tilde{a}}=\hat{e}(\psi(X), \tilde{a})$，$E_{\tilde{b}}=\hat{e}(\psi(X), \tilde{b})$，对于 $i=1, \cdots, 4$，$E_{\tilde{B}_i}=\hat{e}(\psi(X), \tilde{B}_i)$，$E_{\tilde{c}_j}=\hat{e}(g_0, \tilde{c}_j)$，$E_{\tilde{a}_j}=\hat{e}(\psi(X_r), \tilde{a}_J)$，$E_{\tilde{b}_j}=\hat{e}(\psi(X_r), \tilde{b}_J)$。

$$\Pi_1: SPK\{(s,t,x,y,r,\delta_2,J,\delta_4,r_5,\delta_J,\delta_t,\delta_5,): E_{\tilde{a}}=E_{\hat{c}}^{\delta_2} E_{\tilde{b}}^{-s} E_{\tilde{B}_1}^{-t} E_{\tilde{B}_2}^{-x} E_{\tilde{B}_3}^{-\gamma} E_{\tilde{B}_4}^{-r} \wedge E_{\tilde{a}_J}=E_{\hat{c}}^{\delta_4} E_{\tilde{b}_J}^{-J} \wedge \frac{u_1}{S}=S^J S^s \wedge A_T=g_1^J g_2^t g_3^{r_5} \wedge A_T^x=g_1^{\delta_J} g_2^{\delta_t} g_3^{\delta_5} \wedge \frac{u_1^R}{T}=T^J T^t u_0^{-\delta_J} u_0^{-\delta_t} u_0^{-x}\}(R)$$

其中，$\delta_2=1/r_2 \bmod p$，$\delta_4=1/r_4 \bmod p$，$\delta_J=Jx$，$\delta_5=r_5 x$，$\delta_t=tx$。

在支付货币时，用户将 $S, T, A_T, \tilde{a}, \tilde{b}, \tilde{c}, \tilde{A}_1, \tilde{B}_1, \cdots, \tilde{A}_4, \tilde{B}_4, \tilde{a}_J, \tilde{b}_J, \tilde{c}_J, \Pi_1$ 发送给商家，商家检验零知识证明 Π_1 的正确性，并对于 $i=1, \cdots, 4$ 检验 $\hat{e}(\psi(\tilde{a}), Z_i)=\hat{e}(g_0, \tilde{A}_i)$，$\hat{e}(\psi(\tilde{A}_i), Y)=\hat{e}(g_0, \tilde{B}_i)\hat{e}(\psi(\tilde{a}), Y)=\hat{e}(g_0, \tilde{b})$，$\hat{e}(\psi(\tilde{a}_J), Y_r)=\hat{e}(g_0, \tilde{b}_J)$ 是否正确，若都正确，则认为本次支付有效。

2.4.2 压缩支付协议

为支付完整个电子钱包里的货币，用户计算 $T_c=u_0^x u_1^{\frac{R}{y+1}}$，对于 $r_1, r_2, r_3 \in {}_R Z_p$ 计算 $A_T=g_1^y g_2^{r_3}$，$\tilde{a}=a^{r_1}$，$\tilde{b}=b^{r_1}$，

$\tilde{c}=c^{r_1}$，$\tilde{A}_i=A_i^{r_1}$，$\tilde{B}_i=B_i^{r_1}$，其中，$i=1,\cdots,4$，并计算 $SPK\Pi_2$。

$$\Pi_2:SPK\{(x,y,r,\delta_2,r_3,\delta_y,\delta_3):\frac{E_{\tilde{a}}}{E_{\tilde{b}}^{s}E_{\tilde{B}_1}^{t}}=E_{\tilde{c}}^{\delta_2}E_{\tilde{B}_2}^{-x}E_{\tilde{B}_3}^{-y}E_{\tilde{B}_4}^{-r}\wedge A_T=g_1^{y}g_2^{r_3}\wedge A_T^{x}=g_1^{\delta_y}g_1^{\delta_3}\wedge\frac{u_1^{R}}{T}=T_c^{y}u_0^{-\delta_y}u_0^{-x}\}(R)$$

其中，$\delta_2=1/r_2 \bmod p$，$\delta_y=yx$，$\delta_3=r_3x$。

在支付货币时，用户将 $s,t,T_c,A_T,\tilde{a},\tilde{b},\tilde{c},\tilde{A}_1,\tilde{B}_1,\cdots,\tilde{A}_4,\tilde{B}_4,\Pi_2$ 发送给商家，商家对于 $i=1,\cdots,4$ 检验 $\hat{e}(\psi(\tilde{a}),Z_i)=\hat{e}(g_0,\tilde{A}_i)$，$\hat{e}(\psi(\tilde{A}_i),Y)=\hat{e}(g_0,\tilde{B}_i)\hat{e}(\psi(\tilde{a}),Y)=\hat{e}(g_0,\tilde{b})$ 是否成立，并检验 Π_2 是否正确，若都正确，则认为本次支付有效。

2.4.3 批处理支付

对于需支付 n 个货币的情况 $J+n-1\leqslant k$，对于 $i=1,\cdots,n$，用户计算 $S_i=u_1^{\frac{1}{s+J+i}}$，$T_i=u_0^{x}u_1^{\frac{R}{t+J+i}}$，令 $I=J+n-1$，对于 $r_1,r_2,r_3,r_4,r_5,r_6,r_7\in_R Z_p$ 用户计算：

$A_T=g_1^{J}g_2^{t}g_3^{r_7}$，$\tilde{a}=a^{r_1}$，$\tilde{b}=b^{r_1}$，$\tilde{c}=c^{r_1}$，$\tilde{A}_i=A_i^{r_1}$，$\tilde{B}_i=B_i^{r_1}$，其中，$i=1,\cdots,4$，$\tilde{c}=c^{r_2}$，用户找出银行分别对 J、I 的 CL 签名 $(a_J,b_J,c_J),(a_I,b_I,c_I)$，并计算 $(\tilde{a}_J,\tilde{b}_J,\tilde{c}_J)=(a_J^{r_5},b_J^{r_5},c_J^{r_5r_6r_7})$，$(a_I,b_I,c_I)=(a_I^{r_5},b_I^{r_5},c_J^{r_5r_6})$ 和 $SPK\Pi_3$。

$$\Pi_3:SPK\{(s,t,x,y,r,\delta_2,J,\delta_4,\delta_6,r_7,\delta_J,\delta_t,\delta_7):E_{\tilde{a}}=E_{\tilde{c}}^{\delta_2}E_{\tilde{b}}^{-s}E_{\tilde{B}_1}^{-t}E_{\tilde{B}_2}^{-x}E_{\tilde{B}_3}^{-y}E_{\tilde{B}_4}^{-r}\wedge E_{\tilde{a}_J}=E_{c_J}^{\delta_4}E_{b_J}^{-J}\wedge\frac{E_{\tilde{a}}}{E_{\tilde{b}_{n-1}}}=E_{c_I}^{\delta_6}E_{b_I}^{-J}\wedge\frac{u_1}{S_1^{J}S_1}\wedge\cdots\wedge\frac{u_1}{S_n^{J}S_n}\wedge A_T=g_1^{J}g_2^{t}g_3^{r_7}\wedge A_T^{x}=g_1^{\delta_J}g_2^{\delta_t}g_3^{\delta_7}\wedge\frac{u_1^{R}}{T}=T_1^{J}T_1^{t}u_0^{-\delta_J}u_0^{-\delta_t}(u_0)^{-x}\wedge\cdots\wedge\frac{u_1^{R}}{T_n^{R}}=T_n^{J}T_n^{t}u_0^{-\delta_J}u_0^{-\delta_t}(u_0)^{n-x}\}(R)$$

其中，$\delta_2=1/r_2 \bmod p$，$\delta_4=1/r_4 \bmod p$，$\delta_6=1/r_6$，$\delta_J=Jx$，$\delta_t=tx$，$\delta_7=r_7x$。

在支付货币时，用户将 $A_T,S_1,T_1,\cdots,S_n,T_n,\tilde{a},\tilde{b},\tilde{c},\tilde{A}_1,\tilde{B}_1,\cdots,\tilde{A}_4,\tilde{B}_4,\tilde{a}_J,\tilde{b}_J,\tilde{c}_J,\tilde{a}_I,\tilde{b}_I,\tilde{c}_I,\Pi_3$ 发送给商家，商家检验 $\hat{e}(\psi(\tilde{a}),Z_i)=\hat{e}(g_0,\tilde{A}_i)$，$\hat{e}(\psi(\tilde{A}_i),Y)=\hat{e}(g_0,\tilde{B}_i)$，$\Pi_3$ 是否正确，其中 $i=1,\cdots,4$，$\hat{e}(\psi(\tilde{a}),Y)=\hat{e}(g_0,\tilde{b})$，$\hat{e}(\psi(\tilde{a}_J),Y_r)=\hat{e}(g_0,\tilde{b}_J)$，$\hat{e}(\psi(\tilde{a}_I),Y_r)=\hat{e}(g_0,\tilde{b}_I)$，若都正确，则认为本次支付有效。

2.5 存款协议

商家发送给银行支付协议的复本，银行检验商家与用户交易的复本的正确性，为了防止用户和商家串通起来进行联合欺骗，银行需检验商家的身份 I，确认 $R=H(\text{info},I)$ 没有被使用过，防止电子现金的重复花费。同时为了防止商家将 1 次交易的复本提交给银行 2 次，在确认 $R=H(\text{info},I)$ 没有被使用过以后，银行将 S,T,R 存入自己的数据库。(如果是压缩支付，则银行对于 $i=1,\cdots,k$，计算 $S_i=\text{Ved}(s,i)$，并将所有的 $(S,T,R),(S,T_c,s,t,R)$ 存入相应的数据库)。

3 非法用户的追踪

对于重复花费者的追踪：当银行收到一个新的支付协议的复本时，银行首先检查数据库中是否存在 S，如果有，则说明重复花费了电子现金，银行对重复花费者按以下方式进行追踪。

(1)单个电子现金的重复花费

设银行数据库中的记录为 (S,T',R')，当前提交的新的复本为 (S,T,R)，银行计算 $PK=(\frac{T^{R'}}{T'^{R}})^{1/(R'-R)}$，找出非法用户身份，进行惩罚。

(2)压缩支付中和单个电子现金重复

设银行数据库中的记录为 (S,T_c,s,t)，当前提交的新的复本为 (S,T,R)，银行确认 i 满足 $S_i=\text{Vrf}(s,i)$，并计算 $PK=T/(\text{Vrf}(t,i)^{R})$，找出非法用户，并进行惩罚。

(3)重复压缩支付

设银行数据库中的记录为 (s,t,T_c,R)，当前提交的新的复本为 (s,t,T'_c,R')，银行计算 $PK=(\frac{T_c^{R'}}{T_c'^{R}})^{1/(R'-R)}$，找出非法用户并进行惩罚。

4 特性分析

(1)公平性。用户不可伪造电子现金欺骗商家，以单一货币的支付为例，用户不能伪造关于消息 (s,t,x,y,r) 的 CL 签名以及关于 j 的 CL 签名 $S=u_1^{\frac{1}{j+s+1}}$。因为以上的签名和计算基于 k-DDHI 假设和离散对数很困难，因此，用户不可能成功伪造电子现金进行欺骗。

商家不可能伪造电子现金欺骗银行，因为只有合法的 T 与 S 满足 $T=u_0^{x}S^{R}$，而且 R 是随机产生的，在离散对数的困难性假设前提下无法取出 R。其他情况下类似。

(2)可分性。用户 1 次从银行取得 n 个电子现金放入自己的电子钱包，每当有支付请求时，取 i 个总和满足支付请求的电子现金进行支付，满足 1 次取款多次支付的要求，从而达到可分。

(3)高效性。系统基于 CHL 协议的设计思想，当用户能够计算得到 S_i 和 T_i，则直接提交相应的 s 和 t。充分利用了 CL 签名的优点，除批处理支付协议外，其他协议均为常数级时间复杂度，而且，批处理支付协议的时间复杂度也与花费的电子现金的数目线性相关。因此，

系统整体效率较高。

本文将压缩支付和批处理支付的思想融入到压缩型电子现金系统中，给出了运用这种思想的可靠电子现金方案，基于CL签名构建了一种安全高效的可分电子现金系统。但是，CL签名不支持并发签名，所以，提款协议必须按序进行。目前，在安全的压缩型电子现金系统中，设计并行取款的新型系统是下一步研究方向。

参考文献

[1] NAKANISHI T, SHIOTA M, SUGIYAMA Y. An unlinkable divisible electronic cash with user's less computations using active trustees[C]. ISITA 2002, 2002.

[2] CANARD S, GOUGET A, HUFSCHMITT E. A handy multi-coupon system[J]. Applied Cryptography and Network Security-ACNS 2006, LNCS, 2006(3989):66-81.

[3] 李梦东，杨义先.无可信第三方的离线电子现金匿名性控制[J].电子学报，2005，33(3):456-458.

[4] 费雄伟，李乔良.一个新的安全且高效的电子现金系统[J].计算机应用研究，2008，25(5):1543-1545.

[5] BRICKELL E, GEMMELL P, KRAVITZ D. Trustee-based tracing extensions to anonymous cash and the making of anonymous change [C]. In SODA '95, Proceedings of the Sixth Annual ACM-SIAM Symposium on Discrete Algorithms. Society for Industrial and Applied Mathematics, 1995:457-466.

[6] CAMENISCH J, HOHENBERGER S, LYSYANSKAYA A. Compact e-cash [J]. In EUROCRYPT, LNCS, 2005(3494):302-321.

[7] CANARD S, TRAOR'E J. On fair e-cash systems based on group signature schemes. In ACISP, 2003:237-248.

[8] AU M H, WU Q, SUSILO W, et al. Compact e-cash from bounded accumulator. In CT-RAS, 2007.

[9] TERANISHI I, SAKO K. K-times anonymous authentication with a constant proving cost. In Public Key Cryptography, 2006.

[10] CAMENISCHAND J, LYSYANSKAYA A. Signature schemesand anonymous credentials from bilinear maps [J]. In CRYPTO, 2004(3152):56-72.

[11] AU M H, SUSILO W, MU Y. Constant-size Dynamic k-TAA [C]. In SCN 2006, volume 4116 of LNCS. Springer-Verlag, 2006.

[12] BONEH D, BOYEN X. Short signatures without random oracles [C]. In EUROCRYPT 2004, Berlin, LNCS 3027, Springer-Verlag, 2004.

[13] DODIS Y, YAMPOLSKIY A. A verifiable random function with short proofs and keys[J]. In PKC 2005, volume 3386 of LNCS, 2005:416-431.

[14] LYSYANSKAYA A, RIVEST R L, SAHAI A, et al. Pseudonym systems. In Selected Areas in Cryptography[J], Lecture Notes in Computer Science, 1999(1758):184-199.

(收稿日期：2009-09-06)

作者简介：

岳璐，女，1985年生，硕士研究生，主要研究方向：信息安全。

贾小珠，男，1963年生，教授，主要研究方向：信息安全，计算机辅助教育。

茹俊丽，女，1970年生，讲师，主要研究方向：计算机及其应用。