

## 高效的基于证书强指定验证者签名方案

翟正元\*, 高德智, 梁向前, 潘 帅

(山东科技大学 信息科学与工程学院, 山东 青岛 266590)

(\*通信作者电子邮箱 zhaiyuan1987@163.com)

**摘 要:**针对基于身份公钥密码系统下的强指定验证者签名中的第三方完全可信问题及已有签名方案效率不高的问题,利用基于证书密码系统中证书认证机构(CA)的信任级别低的优点,提出了一个新的强指定验证者签名方案。在随机预言模型下基于双线性 Diffie-Hellman (BDH) 问题假设给出了形式化的安全性分析。通过性能分析可看出:该方案能满足强指定验证者签名方案的所有性质,且签名长度仅为群中一个元素,具有较高的通信效率,适用于带宽受限的环境。

**关键词:**强指定验证者;证书认证机构;基于证书公钥密码系统;随机预言模型;双线性 Diffie-Hellman 问题

**中图分类号:** TP301.6; TP309.76 **文献标志码:** A

### Efficient certificate-based signature scheme with strong designated verifier

ZHAI Zhengyuan\*, GAO Dezhi, LIANG Xiangqian, PAN Shuai

(College of Information Science and Engineering, Shandong University of Science and Technology, Qingdao Shandong 266590, China)

**Abstract:** Concerning the flaw that it needs a fully credible third party in ID-based strong designated verifier signature and the low efficiency of existing schemes, taking the advantage of Certificate Authority (CA)'s low trust level in certificate-based public key cryptography, a new strong designated verifier signature scheme was proposed in this paper. Furthermore, the formal security analysis under assumed Bilinear Diffie-Hellman (BDH) problem in the random oracle model was presented. Performance analysis shows the scheme meets all properties of strong designated verifier signature schemes and enjoys higher correspondence efficiency used in bandwidth limited environment since the signature length is just one of the group elements.

**Key words:** strong designated verifier; Certificate Authority (CA); Certificate-Based Public Key Cryptography (CB-PKC); random oracle model; Bilinear Diffie-Hellman (BDH) problem

## 0 引言

2003 年, Gentry<sup>[1]</sup> 在欧洲密码学会议上首次提出基于证书公钥密码系统 (Certificate-Based Public Key Cryptography, CB-PKC) 的新概念, 该密码系统概念具有很强的应用背景。在 CB-PKC 中, 证书认证机构 (Certificate Authority, CA) 为用户的身份和公钥生成一个隐含证书, 用户使用自己的私钥和 CA 生成的证书来进行加密或签名。CA 不知道用户的私钥, 也就无法伪造用户的签名, 从而对 CA 的信任级别要求达到与传统公钥基础设施 (Public Key Infrastructure, PKI) 相同的级别。基于证书签名是基于证书公钥密码系统中的一个重要组成部分, 它是传统数字签名体制的一种有益扩展。2004 年, Kang 等<sup>[2]</sup> 首次给出了基于证书签名的概念和安全模型, 对该签名体制进行了比较系统的研究。现在基于证书签名体制的研究已经逐渐成为数字签名体制研究的热点, 文献[3–5]结合基于证书签名和一些具有特殊实用背景的数字签名体制进行了有益的探索, 获得了一些很有价值的研究成果。

在传统的数字签名中, 任何人只要知道签名者的公钥, 就可以验证签名的有效性。然而, 在一些特殊场合, 如电子选举、电子投票、软件认证等涉及到签名者的个人隐私时, 签名者希望只有指定的验证者才能验证签名的有效性。1996 年,

Jakobsson 等首次提出了指定验证者签名 (Designated Verifier Signature, DVS) 的概念<sup>[6]</sup>, 在 DVS 方案中只有指定验证者可以验证签名的有效性, 同时验证者自身也能够产生与签名者签名不可区分的副本, 使得任何第三方无法辨认签名者的签名。其特点是具有不可传递性, 可以有效地阻止签名的恶意传播, 保护签名者的隐私。指定验证者签名在电子商务、电子政务等实际活动中有许多重要用途, 得到研究者的重视。同年 Jakobsson 还引入了强指定验证者的签名 (Strong Designated Verifier Signature, SDVS) 的概念, 与 DVS 方案不同的是, 在 SDVS 方案中签名的验证过程要用到指定验证者的私钥, 对验证者提出了更高的要求。2003 年, Saeednia 等<sup>[7]</sup> 首先提出了一个基于签密思想的强指定验证者的签名方案, 并深入讨论了相关的安全概念, 拓宽了指定验证者签名方案的研究范围。2004 年, Susilo 等<sup>[8]</sup> 在 Saeednia 方案的基础上给出了第一个基于身份的强指定验证者签名方案, 比较遗憾的是该方案没有给出形式化的安全性证明。2008 年, Zhang 等<sup>[9]</sup> 给出一个随机预言模型中可证明安全的基于身份的强指定验证者签名方案, 但是后来 Kang 等<sup>[10]</sup> 指出该方案不满足不可伪造性。2009 年, 李明祥等<sup>[11]</sup> 提出一种高效的基于身份强指定验证者签名方案, 并给出严格的安全性证明, 完善了已有结果。2011 年, 孙士峰等<sup>[12]</sup> 指出文献[11]不满足强指定验证者签

收稿日期: 2012-09-14; 修回日期: 2012-10-28。

基金项目: 青岛市科技发展计划项目 (11-2-4-6-(1)-jch); 山东科技大学研究生创新基金资助项目 (YCA120340)。

作者简介: 翟正元 (1987–), 男, 山东费县人, 硕士研究生, 主要研究方向: 信息安全、密码学; 高德智 (1963–), 男, 山东青岛人, 教授, 博士, 主要研究方向: 应用泛函分析、密码学; 梁向前 (1969–), 男, 山东青岛人, 副教授, 博士, 主要研究方向: 信息安全、复分析; 潘帅 (1987–), 女, 山东青岛人, 硕士研究生, 主要研究方向: 信息安全、密码学。

名的第三方不可验证性,并对方案进行改进,进而提出了一个新的可证安全的强指定验证者签名方案。遗憾的是,在文献[8-12]的方案中,要求私钥生成中心(Private Key Generator, PKG)是完全可信的,否则PKG可以根据用户的私钥伪造用户的强指定验证者签名。事实上,在实际环境中要求PKG绝对可信是很难做到的,因此,上述方案在实际应用中仍然不够理想。

基于以上考虑,本文结合基于证书公钥密码体制的优点,利用双线性映射的特点设计了一个高效的基于证书强指定验证者签名方案。在随机预言模型下基于双线性Diffie-Hellman(Bilinear Diffie-Hellman, BDH)困难问题假设,本文证明了所给的方案是不可伪造的。该方案在签名过程和验证过程中只需要一次双线性对运算,减少了运算次数,与已有强指定验证者签名方案相比该方案具有签名长度短和效率高优点,实用性更强。

## 1 预备知识

### 1.1 双线性映射

**定义1** 假设 $G_1$ 是阶为素数 $q$ 的加法循环群, $G_2$ 为同阶的乘法循环群, $P$ 为 $G_1$ 的生成元。称映射 $e: G_1 \times G_1 \rightarrow G_2$ 为一个双线性映射,如果它满足如下特性:

- 1) 双线性性。 $\forall a, b \in \mathbb{Z}_q^*$  和  $P, Q \in G_1$ , 有
$$e(aP, bQ) = e(abP, Q) = e(P, abQ) = e(P, Q)^{ab}$$
- 2) 非退化性。存在 $P \in G_1$ , 满足 $e(P, P) \neq 1$ 。
- 3) 可计算性。对所有的 $P, Q \in G_1$ , 存在有效的算法计算 $e(P, Q)$ 。

### 1.2 困难性假设

本文提出的签名方案基于以下困难问题是安全的,目前为止还不存在多项式时间算法以不可忽略的优势解决下面问题:

**定义2** BDH问题。假设 $G_1$ 是一个阶为大素数 $q$ 的加法循环群, $P$ 是 $G_1$ 的生成元,给定 $\langle P, aP, bP, cP \rangle$  计算 $e(P, P)^{abc}$ ,其中 $a, b, c \in \mathbb{Z}_q^*$ 未知。

## 2 基于证书的强指定验证者签名

### 2.1 算法模型

一个基于证书的强指定验证者签名方案由三个实体:证书生成中心(CA)、原始签名者(A)、验证者(B)及以下五个算法组成:

- 1) Setup: 算法输入安全参数 $k$ , 输出系统参数 $params$ 、CA的主私钥 $msk$ 、主公钥 $mpk$ 。
- 2) UserKeyGen: 算法输入系统参数 $params$ , 输出用户ID的公私钥对 $(PK_{ID}, sk_{ID})$ 。
- 3) CertGen: 算法输入系统参数 $params$ 、CA的主私钥 $msk$ , 用户的身份ID及其公钥 $PK_{ID}$ , 输出用户的证书 $Cert_{ID}$ 。
- 4) Sign: 算法输入系统参数 $params$ , 消息 $m$ , 签名者A的私钥 $sk_A$ 、证书 $Cert_A$ 及验证者B的公钥 $PK_B$ , 输出消息 $m$ 的签名 $\sigma$ 。
- 5) Verify: 算法输入系统参数 $params$ , 消息 $m$ 的签名 $\sigma$ , 验证者B的私钥 $sk_B$ 、证书 $Cert_B$ 及签名者A的公钥 $PK_A$ , 输出“true”或“false”。

### 2.2 方案描述

- 1) Setup: 选择阶为素数 $q$ 的两个循环群 $G_1, G_2$ , 其中 $G_1$ 为

加法群,其生成元为 $P, G_2$ 为乘法群。 $e: G_1 \times G_1 \rightarrow G_2$ 为双线性映射。选择两个安全的Hash函数 $h_1: \{0, 1\}^* \times G_1 \rightarrow G_1, h_2: \{0, 1\}^* \times G_1 \rightarrow \mathbb{Z}_q^*$ 。CA随机选择 $s \in \mathbb{Z}_q^*$ 作为主私钥,并计算主公钥 $P_{pub} = sP$ ,最后公布系统参数 $params = (G_1, G_2, q, P, e, h_1, h_2, P_{pub})$ 。

2) UserKeyGen: 签名者A和验证者B分别随机选择 $x_A \in \mathbb{Z}_q^*, x_B \in \mathbb{Z}_q^*$ 作为自己的私钥,并计算相应的公钥 $PK_A = x_A P, PK_B = x_B P$ 。

3) CertGen: 签名者A向CA提交自己的身份 $ID_A$ 和公钥 $PK_A$ , CA计算对应的证书

$Cert_A = sh_1(ID_A, PK_A)$ , 并将 $Cert_A$ 发送给A。验证者B以同样的方法得到其证书 $Cert_B$ 。

4) Sign: 给定消息 $m \in \{0, 1\}^*$ , 签名者A计算

$$h = h_2(m, x_A PK_B)$$

$$Q_B = h_1(ID_B, PK_B)$$

$$\sigma = e(h Cert_A, Q_B)$$

则 $\sigma$ 即为消息 $m$ 的签名。

5) Verify: B收到A对消息 $m$ 的签名 $\sigma$ 后计算 $h' = h_2(m, x_B PK_A), Q_A = h_1(ID_A, PK_A)$ , 并验证 $\sigma = e(h' Q_A, Cert_B)$ 是否成立,如果成立则签名有效,输出“true”;否则输出“false”。

## 3 性能分析

### 3.1 安全性分析

下面从正确性、非传递性、第三方不可验证性和不可伪造性四个方面分析方案的安全性。

#### 3.1.1 正确性

正确性容易证明,这是因为如果 $\sigma$ 是A在签名阶段用自己的私钥 $x_A$ 和证书 $Cert_A$ 生成的,则有

$$\begin{aligned} h &= h_2(m, x_A PK_B) = h_2(m, x_A x_B P) = h_2(m, x_B PK_A) = h' \\ \sigma &= e(h Cert_A, Q_B) = e(h sh_1(ID_A, PK_A), h_1(ID_B, PK_B)) = \\ &= e(h' h_1(ID_A, PK_A), sh_1(ID_B, PK_B)) = \\ &= e(h' Q_A, Cert_B) \end{aligned}$$

#### 3.1.2 不可传递性

验证者B模拟签名者A对消息 $m$ 的签名,产生签名副本。B计算

$$h' = h_2(m, x_B PK_A)$$

$$Q_A = h_1(ID_A, PK_A)$$

$$\sigma' = e(Q_A, h' Cert_B)$$

则 $\sigma'$ 即是B对消息 $m$ 的签名副本。

显然 $\sigma' = e(h' Q_A, Cert_B)$ 能被验证算法接受,而且即使签名者和验证者的密钥泄露, $\sigma$ 与 $\sigma'$ 也是无法区分的。

#### 3.1.3 第三方不可验证性

在验证签名有效性的过程中,需要用到验证者B的私钥 $x_B$ 和证书 $Cert_B$ ,任何第三方(包括证书生产中心CA)都无法验证签名的有效性,也无法从验证等式中得到任何与签名者A有关的秘密信息,所以满足强指定验证者签名的第三方不可验证性。

#### 3.1.4 不可伪造性

下面从BDH假设出发,在随机预言模型下证明所给方案的不可伪造性。

**定理1** 如果存在敌手A能够在时间 $t$ 内以不可忽略的优势 $\varepsilon$ 在下面游戏中伪造强指定验证者签名,那么存在算法

能够以不可忽略的优势  $\xi$  解决 BDH 问题。

**证明** 下面通过挑战者  $C$  和敌手  $A$  之间的一个游戏证明如果  $A$  能够以不可忽略的优势  $\varepsilon$  伪造签名,那么  $C$  能够利用敌手  $A$  以优势  $\xi$  解决 BDH 问题。

在游戏中,  $A$  可以向  $C$  查询随机预言模型  $h_1, h_2$  的输出值。为了避免碰撞,  $C$  使用列表  $L_1, L_2$  来存储  $h_1, h_2$  的输出值。此外,它使用  $L_3$  来存储用户公私钥的查询值,  $L_4$  存储用户证书的查询值,  $L_5$  存储用户签名的查询值。挑战者  $C$  收到一个 BDH 问题实例  $(P, aP, bP, cP)$ , 其中  $P$  是  $G_1$  的生成元,  $C$  利用  $A$  通过下面的游戏计算  $e(P, P)^{abc}$ 。

1) 参数生成:  $C$  选择  $P_{\text{pub}} = cP$ , 生成系统参数  $params = (G_1, G_2, q, e, P, P_{\text{pub}})$ , 并将  $params$  发送给  $A$ 。

2)  $h_1$  询问<sup>[12]</sup>: 当敌手  $A$  对用户身份  $ID_i$  和公钥  $PK_i$  进行  $h_1$  询问时,  $C$  首先检查列表  $L_1$ , 如果  $(ID_i, PK_i, Q_i, c_i, \alpha_i)$  已经存在列表  $L_1$  中, 则将  $Q_i$  的值返回给  $A$ ; 否则  $C$  随机选择  $c_i \in \{0, 1, 2\}$  且  $\Pr[c_i = 0] = \delta, \Pr[c_i = 1] = \Pr[c_i = 2] = \frac{1-\delta}{2}$ ,

其中  $\delta$  的值待定。  $C$  随机选择  $\alpha_i \in \mathbb{Z}_q^*$ , 进行如下计算:

$$Q_i = h_1(ID_i, PK_i) = \begin{cases} \alpha_i P, & c_i = 0 \\ \alpha_i aP, & c_i = 1 \\ \alpha_i bP, & c_i = 2 \end{cases}$$

然后将  $Q_i$  的值返回给敌手  $A$ , 同时将  $(ID_i, PK_i, Q_i, c_i, \alpha_i)$  添加到列表  $L_1$  中。

3)  $h_2$  询问: 当敌手  $A$  对消息  $m_i$  和  $x_i PK_j$  进行  $h_2$  询问时,  $C$  首先检查列表  $L_2$ , 如果  $(m_i, x_i PK_j, \beta_i)$  已经存在列表  $L_2$  中, 则将  $\beta_i$  的值返回给  $A$ ; 否则  $C$  随机选择  $\beta_i \in \mathbb{Z}_q^*$  作为回答, 并将  $(m_i, x_i PK_j, \beta_i)$  添加到列表  $L_2$ 。

4) 用户密钥提取询问:  $A$  向  $C$  提交用户的身份  $ID_i$ ,  $C$  检查列表  $L_3$ , 如果  $ID_i$  不存在列表  $L_3$  中,  $C$  任意选择  $x_i \in \mathbb{Z}_q^*$  作为用户的私钥, 计算公钥  $PK_i = x_i P$ , 将  $(ID_i, c_i, x_i, PK_i)$  添加到列表  $L_3$  中, 并公布  $PK_i$ 。最后如果  $c_i = 0$ , 则将  $x_i$  的值返回给  $A$ ; 否则返回询问失败。

5) 用户证书询问:  $A$  向  $C$  提交用户的身份  $ID_i$  和公钥  $PK_i$ ,  $C$  检查列表  $L_4$ , 如果  $ID_i$  不存在列表中且列表  $L_1$  中  $c_i = 0$ ,  $C$  令  $Cert_i = \alpha_i P_{\text{pub}}$ , 并将  $(ID_i, PK_i, \alpha_i, Cert_i)$  添加到列表  $L_4$  中, 最后返回  $Cert_i$  的值。

6) 签名询问:  $A$  向  $C$  询问签名者  $ID_i$  对消息  $m_i$  的签名  $\sigma_i$  (强指定验证者为  $ID_j$ ),  $C$  首先检查列表  $L_1$  中  $(ID_i, PK_i, Q_i, c_i, \alpha_i), (ID_j, PK_j, Q_j, c_j, \alpha_j)$  的值, 若  $c_i = 0$ ,  $C$  计算  $h = h_1(m_i, x_i PK_j), \sigma_i = e(h\alpha_i cP, \alpha_j P)$ ; 若  $c_j = 0$ ,  $C$  计算

$$h = h_1(m_i, x_j PK_i) \\ \sigma_i = e(\alpha_i P, h\alpha_j cP)$$

则  $\sigma_i$  就是消息  $m_i$  的强指定验证者签名,  $C$  将  $\sigma_i$  的值返回给  $A$ ; 否则  $C$  退出游戏。

最后敌手  $A$  输出一个有效的强指定验证者签名  $(m^*, \sigma^*)$ , 其中签名者身份为  $ID_i^*$ , 指定验证者身份为  $ID_j^*$ 。  $C$  首先查询列表  $L_1$  中  $(ID_i, PK_i, Q_i, c_i, \alpha_i), (ID_j, PK_j, Q_j, c_j, \alpha_j)$  的值, 如果  $c_i = 1, c_j = 2$  或者  $c_i = 2, c_j = 1$ ,  $C$  继续游戏; 否则  $C$  退出游戏。

不妨假设  $c_i = 1, c_j = 2$ ,  $C$  查询列表  $L_2$  得到  $(m^*, x_i^* x_j^* P, \beta^*)$ , 那么  $C$  可通过如下等式来求解 BDH 问题:

$$\sigma^* = e(\beta^* \alpha_i^* a c P, \alpha_j^* b P) = e(ab P, c P)^{\beta^* \alpha_i^* \alpha_j^*}$$

于是  $e(P, P)^{abc} = \sigma^*^{-\beta^* \alpha_i^* \alpha_j^*}$ 。

下面分析  $C$  利用敌手  $A$  解决 BDH 问题的优势  $\xi$ 。假定  $A$  可以向  $C$  最多提交  $q_{h_1}$  次  $h_1$  查询、 $q_{h_2}$  次  $h_2$  查询、 $q_k$  次密钥查询、 $q_c$  次证书查询以及  $q_s$  次签名查询,  $A$  成功伪造关于消息  $m^*$ , 签名者  $ID_i^*$ , 验证者  $ID_j^*$  的指定验证者签名, 需要满足以下条件:

①  $A$  在密钥查询阶段没有查询签名者  $ID_i^*$ , 验证者  $ID_j^*$  的密钥, 记此事件为  $E_1$ , 则  $\Pr[E_1] = \delta^{q_k}$ 。

②  $A$  在证书查询阶段没有查询签名者  $ID_i^*$ , 验证者  $ID_j^*$  的证书, 记此事件为  $E_2$ , 则  $\Pr[E_2] = \delta^{q_c} (1 - \delta)^{q_{h_1} - q_c}$ 。

③  $A$  在签名查询阶段,  $C$  没有失败而退出且  $A$  没有查询关于消息  $m^*$ , 签名者  $ID_i^*$ , 验证者  $ID_j^*$  的签名, 记此事件为  $E_3$ , 则  $\Pr[E_3] = (\delta - \delta^2)^{q_s}$ 。

故  $C$  利用敌手  $A$  解决 BDH 问题的优势

$$\xi = \Pr[E_1] \Pr[E_2] \Pr[E_3] \left( \frac{1-\delta}{2} \right)^2 \varepsilon = \delta^{q_k} \delta^{q_c} (1-\delta)^{q_{h_1}-q_c} (\delta - \delta^2)^{q_s} \left( \frac{1-\delta}{2} \right)^2 \varepsilon \geq$$

$$\left( \frac{q_s + q_{h_1} - q_c}{q_k + q_{h_1} + 2q_s} \right)^{q_k + q_c + q_s} \left( \frac{q_k + q_s + q_c}{q_k + q_{h_1} + 2q_s} \right)^{q_{h_1} + q_s - q_c + 2} \frac{\varepsilon}{4}$$

当且仅当  $\delta = \frac{q_k + q_{h_1} - q_c}{q_k + q_{h_1} + 2q_s}$  时, 不等号成立。

所以, 如果存在敌手  $A$  能够以不可忽略的优势  $\varepsilon$  伪造强指定验证者签名, 那么  $C$  能够以不可忽略的优势  $\xi$  解决 BDH 问题。

### 3.2 效率分析

本文方案与文献[8, 11-12] 方案的效率比较如表 1 所示。为了方便比较, 本文用  $C$  表示加法循环群  $G_1$  上的数量乘法运算,  $C_+$  表示加法循环群  $G_1$  上的加法运算,  $C_p$  表示双线性对运算,  $C_h$  表示哈希函数运算,  $G_1$  中元素的比特长度为  $|G_1|$  且  $|G_1| = |G_2|$ 。

表 1 方案效率比较

方案	签名阶段	验证阶段	签名长度
文献[8] 方案	$C_p + 2C_+ + 2C_h + C_+$	$2C_p + C_+ + 2C_h + 2C_+$	$2 G_1 $
文献[11] 方案	$C_p + 2C_+ + 2C_h + C_+$	$2C_p + 2C_h$	$2 G_1 $
文献[12] 方案	$C_p + 2C_+ + 2C_h + C_+$	$C_p + C_+ + 2C_h + C_+$	$2 G_1 $
本文方案	$C_p + 2C_+ + 2C_h$	$C_p + 2C_+ + 2C_h$	$ G_1 $

从表 1 可以看出本文方案在签名阶段和验证阶段的运算量相同, 都仅需一次双线性对运算、两次数乘运算和两次哈希运算, 且签名长度仅为  $G_2$  中一个元素的比特长度。与同类方案相比, 具有更高的计算效率和通信效率, 适合用于电子拍卖、电子投票及软件认证等实际活动。

## 4 结语

本文针对基于身份的强指定验证者签名方案不能有效抵抗 PKG 中心的伪造攻击, 要求 PKG 中心完全可信的缺陷, 结合基于证书公钥密码系统的优点和强指定验证者签名方案的特点, 构造了一个高效的基于证书强指定验证者签名方案。最后对方案进行安全性及性能分析, 分析结果表明方案能够满足强指定验证者签名方案所具有的性质, 是一种高效、安全的签名方案。

(下转第 813 页)



CSA 的各个算子,证明 Multi-CSA 中的各个算子满足进化算法收敛的两个充分条件(选择采用基于杰出者的机制),从而证明 Multi-CSA 是收敛的。本文还通过实验直观阐述在各种

参数值组合的情况,Multi-CSA 收敛的情况。这些分析在理论和应用上均证明了 Multi-CSA 是收敛的,完善了该改进算法,具有一定的实用意义。

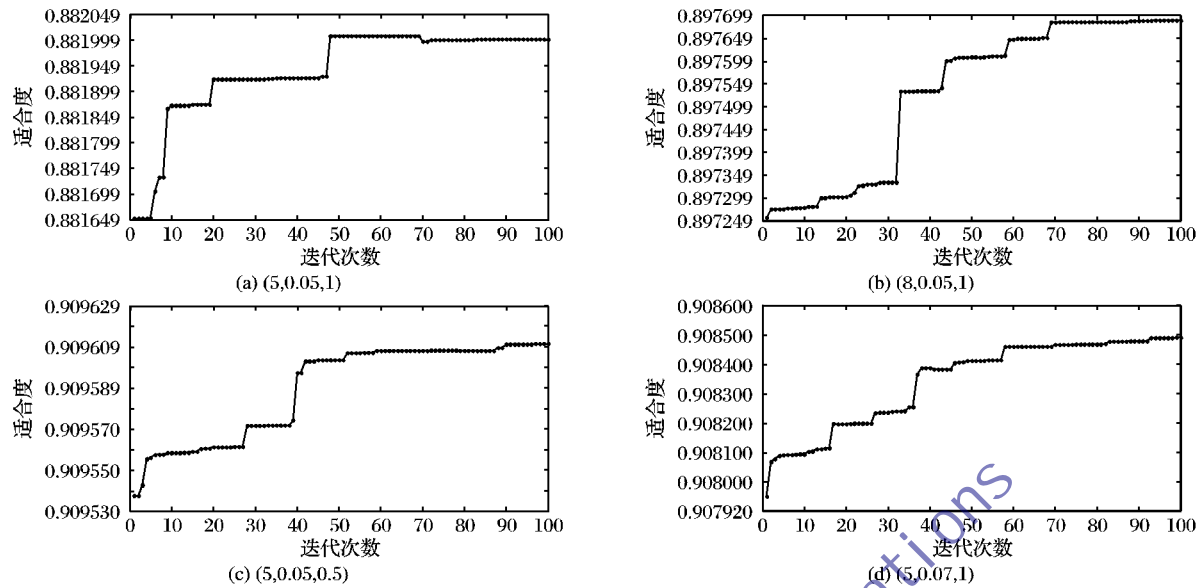


图3 不同参数组合时种群适合度情况

#### 参考文献:

- [1] 于瀛,侯朝桢.一种克隆选择算法的收敛性分析[J].计算机应用,2006,26(6):96-98.
- [2] 洪露,纪志成,龚成龙.一类克隆选择算法的收敛性方法研究[J].信息与控制,2011,40(2):232-236.
- [3] VILLALOBOS-ARIAS M, COELLO C A C, HEMANDEZ-LEMA O. Convergence analysis of a multi-objective artificial immune system algorithm[C]// Proceedings of the 3rd International Conference on AIS. Berlin: Springer-Verlag, 2004: 226-235.
- [4] CUTELLO V, NICOSIA G, ROMEO M, et al. On the convergence of immune algorithm[C]// Proceedings of IEEE Symposium on Foundations of Computational Intelligence. Washington, DC: IEEE Computer Society, 2007: 409-415.
- [5] CLARK E, HONE A, TIMMIS J. A Markov chain model of the B-cell algorithm[C]// Proceedings of the 4th International Conference on Artificial Immune Systems. Berlin: Springer, 2005: 318-330.
- [6] 方贤进,幕学海,刘凌冰,等.基于B细胞算法的克隆选择算法的收敛性分析[J].计算机应用,2010,30(3):772-775.
- [7] 焦李成,杜海峰,刘芳,等.免疫优化计算、学习与识别[M].北京:科学出版社,2006.
- [8] 马力,焦李成,白琳,等.自适应多克隆聚类算法及其收敛性分析[J].模式识别与人工智能,2008,21(1):72-81.
- [9] 吴秋逸,焦李成,李阳阳,等.自适应量子免疫克隆算法及其收敛性分析[J].模式识别与人工智能,2008,21(5):592-597.
- [10] RUDOLPH G. Finite Markov chain results in evolutionary computation: a tour d'hORIZON[J]. Fundamenta Informaticae, 1998, 35(14): 67-89.
- [11] 郑仙花,骆炎民.基于多类数据分类的改进克隆选择算法[J].计算机应用,2012,32(11):3201-3205.
- [12] GREENHALGH D, MARSHALL S. Convergence criteria for genetic algorithms[J]. SIAM Journal on Computing, 2000, 30(1): 269-282.

(上接第761页)

#### 参考文献:

- [1] GENTRY C. Certificate-based encryption and the certificate revocation problem [C]// Proceedings of EUROCRYPT 2003. Berlin: Springer-Verlag, 2003: 272-293.
- [2] KANG B G, PARK J H, HAHN S G. A certificate-based signature scheme[C]// Proceedings of CT-RSA 2004. Berlin: Springer-Verlag, 2004: 99-111.
- [3] LI J G, HUANG X Y, MU Y, et al. Certificate-based signature: security model and efficient construction [C]// Proceedings of EuroPKI 2007. Berlin: Springer-Verlag, 2007: 110-125.
- [4] LI J G, XU L Z, ZHANG Y C. Provably secure certificate-based proxy signature schemes [J]. Journal of Computers, 2009, 4(6): 444-452.
- [5] LI J G, HUANG X Y, ZHANG Y C, et al. An efficient short certificate-based signature scheme [J]. The Journal of Systems and Software, 2012, 85(12): 314-322.
- [6] JAKOBSSON M, SAKO K, IMPAGLIAZZO R. Designated verifier proofs and their applications [C]// Proceedings of EUROCRYPT 1996. Berlin: Springer-Verlag, 1996: 143-154.
- [7] SAEEDNIA S, KREMER S, MARKOWITZ O. An efficient strong designated verifier signature scheme [C]// Proceedings of ICISC '2003. Berlin: Springer-Verlag, 2004: 40-54.
- [8] SUSILO W, ZHANG F T, MU Y. Identity-based strong designated verifier signature schemes[C]// Proceedings of ACISP '2004. Berlin: Springer-Verlag, 2004: 313-324.
- [9] ZHANG J, MAO J. A novel ID-based designated verifier signature scheme [J]. Information Sciences, 2008, 178(3): 766-773.
- [10] KANG B Y, BOYD C, DAWSON E. Identity-based strong designated verifier signature schemes: Attacks and new construction [J]. Computers and Electrical Engineering, 2009, 35(1): 49-53.
- [11] 李明洋,郑雪峰,朱建勇,等.一种高效的基于身份的强指定验证者签名方案[J].四川大学学报:工程科学版,2009,41(4): 176-180.
- [12] 孙士峰,温巧燕,金正平,等.对一类强指定验证者签名方案的分析与改进[J].四川大学学报:工程科学版,2011,43(1): 91-96.
- [13] 张永洁,王彩芬,张玉磊.两个指定验证者签名方案的分析与改进[J].计算机应用,2010,30(5): 1227-1229.