一个增强的有序多重签名方案①

张兴华

(廊坊师范学院 数学与信息科学学院, 廊坊 065000)

摘 要: 详细分析了王等人的多重数字签名方案和张等人的多重签名改进方案. 指出张等人的伪造攻击过程不成立, 并指出其参数设置错误, 并给出了详细证明. 基于离散对数问题的难解性, 采用改进原有方案的参数和增加新的参数 W 的方法, 提出一种新的增强的有序多重签名方案, 改进后的方案弥补了原方案参数设置错误的缺陷, 新的参数也使方案有了更强的安全性能, 新的方案可以抵抗伪造攻击, 可以抵抗公钥替换攻击, 满足不可抵赖性, 不可滥用性, 身份可识别性等特性, 新方案更加安全有效.

关键词: 多重签名; 伪造攻击; 数字签名

Improved Sequential Multi-signature Scheme

ZHANG Xing-Hua

(College of Mathematics and Information Science, Langfang Teacher's College, Langfang 065000, China)

Abstract: In this paper, a detailed analysis of the digital multi signature scheme and the improved multi signature scheme have been carried out. It points out that the forgery attack process which had been proposed by Zhang et al. cannot be established due to its parameter setting error, and the detailed proof has been demonstrated. A new sequential multi signature scheme enhancement is proposed by improving the existed parameters and adding new ones based on the intractability of discrete logarithm problem. A better security and effectiveness of this new scheme is presented in this paper as well, such as the resistance of forgery attack and the public key substitution attack, the satisfaction of non-repudiation and non-misuse, the property of identity identification, etc.

Key words: multi-signature; forgery attack; digital signature

为了防止消息发送者和接收者中任意一人的欺骗或者伪造, 常采用数字签名技术. 数字签名技术自产生以来, 已经十分广泛应用到现代人的工作和生活中, 像电子商务, 电子银行, 电子政务等. ElGamal 提出一个单个用户的签名方案[1],在此基础上又有了 Harn L,Xu Y 提出的完整且安全的 ElGamal 型数字签名方案[2]. 实际工作中, 当一份文件需要多个人对它进行签署才有效时, 通常采用多重数字签名技术, 每个签名人做部分签名, 一起生成最后的签名. Harn L 在 ElGamal 型数字签名方案基础上提出了多重数字签名方案[3]. 根据不同的签名过程, 多重签名方案包括两类: 有序多重数字签名方案和广播多重数字签名方案. 每种方案都有系统初始化、签名和验证这三个过程, 而且两个方案都包括消息发送者、消息签名者和签名验证者这三个对象, 文献[3]方案不能用于有序数字签名. 李子臣等设计了既适合于广播型数字签名, 又适合于有序型数字签名的新方案[4] (以下简称 L-Y 方案), 针对有序数字签名最近又提出了新的方案[5-8] . 王晓明[9] (以下简称 W 方案)提出 L-Y 方案在验证阶段没有对公钥进行验证, 所以存在伪造攻击, 并给出伪造过程证明, 经过分析, 其证明过程是正确的. 针对 L-Y 方案, 张骏等[10] (以下简称 Z 方案)又在 2009 年提出了和 W 方案相似的伪造攻击, 认为某个签名者获取了排在该签名者之前的任何签名者的签名, 并可以伪造多重签名. 通过对 Z 方案的伪造过程进行分析, 本文发现其中存在参数设置错误以及伪造过程不成立的问题,

① 基金项目:廊坊市科学技术研究与发展计划(2013011047)
收稿时间:2014-01-01;收到修改稿时间:2014-03-03

所以其证明过程是错误的.

基于前人的研究, 主要对 Z 方案存在的问题进行分析, 弥补 Z 方案存在的不足, 继而提出新的安全增强的有序多重签名方案, 新的方案对 Z 方案参数进行改正, 并设置了新的特征 W, 通过安全性分析, 新的方案相对于 Z 方案来说, 可以抵抗伪造攻击, 同时满足不可滥用、不可抵赖、可验证性、身份可识别性待特性, 实用性更强.

1 L-Y方案简介

初始化过程:

1)设 $U_i(i=1,2,...,n)$ 为签名者, U_S 为消息发送者, U_V 为消息接收者. M 为等待签名的消息, $h()$ 为单向并安全的哈希函数.

2) P 为系统选择的大素数, g 是 $GF(P)$ 的本原元.

3) $U_i(i=1,2,...,n)$ 分别随机选取 $x_i\in[1,P]$, x_i 即为 U_i 的私钥, $y_i=g^{x_i}$ 为 U_i 的私钥. 其中 x_i 被 U_i 自己秘密保存起来, 只把 P,g,y_i 公开.

签名过程:

1)签名者中顺序排在第一的 U_1 随机选择 $k_1\in[1,P]$, 计算 $r_1=g^{k_1} \bmod p$ 和 $s_1=x_1h(m)-r_1k_1 \bmod p$

2) U_1 将 (r_1,s_1,m) 向他紧接着的后一个签名者发送, 与此同时, 广播 r_1 给所有的签名者.

3)签名者 $U_i(i=2,...,n)$ 按 $i=2,...,n$ 序号先后顺序随机选择 $k_i\in[1,P]$, 然后计算 $r_i=g^{k_i} \bmod p$ 和 $s_i=s_{i-1}+x_ih(m)-r_ik_i \bmod p$.

4) U_i 将 (r_i,s_i,m) 向他后一个签名者发送, 同时广播 r_i 给所有的签名者.

验证过程:

最后 U_n 将 (r_n,s_n,m) 发送给验收者 U_V, U_V 检查 $g^{s_n}\prod_{j=1}^{n}r_j^{r_j}=\prod_{j=1}^{n}(y_j)^{h(m)} \bmod p$ 是否成立, 若等式成立则签名有效, 否则说明以上签名结果是无效的, 不被认可.

2 L-Y方案的不足

W 方案提出在 L-Y 方案中, 一方面, $U_i(i=1,2,...,n)$ 中任意一人都能伪造 $U_i(i=1,2,...,n)$ 对消息 M 的签名; 另一方面, $U_i(i=1,2,...,n)$ 中排在后边的一人也可以伪造他前面的几个签名人对消息 M 的签名.

第一方面提出的伪造过程简介:

$U_i(i=1,2,...,n)$ 可以伪造 $U_1,U_2,...,U_n$, 对消息 M 的签名 (r_n,s_n,M), U_i 的操作如下:

1) U_i 随机选择 $x_i\in[1,P]$, 并设 $y_i^{'}=g^{x_i} \bmod p$ $y_i=\prod_{j=1}^{n}y_j^{-1}y_i^{'} \bmod p$ 公开 y_i.

2) 签名者 U_i 随机选择 $k_j\in[1,P-2]$, $r_j=g^{k_j} \bmod p(j=1to n)$, 并广播 $r_1,r_2,...,r_{n-1}$ 给验证人, 随之计算 $s_n=x_ih(M)-\sum_{j=1}^{n}r_jk_j \bmod(p-1)$, U_i 将 (r_n,s_n,M) 传送给验证人. 如果验证人验证 $g^{s_n}\prod_{j=1}^{n}r_j^{r_j}\stackrel{?}{=}\prod_{j=1}^{n}(y_j)^{h(M)} \bmod p$ 成立则伪造签名成功.

验证过程:

$$\prod_{j=1}^{n}y_j=y_1...y_{i-1}(y_i^{'}\prod_{j=1}^{n}y_j^{-1} \bmod p)y_{i+1}...y_n=y_i^{'} \bmod p$$

$$g^{s_{in}}g^{\sum_{j=1}^{n}r_jk_j}=(y_i^{'})^{h(M)} \bmod p$$

$$g^{s_n}\prod_{j=1}^{n}r_j^{r_j}=\prod_{j=1}^{i}(y_j)^{h(M)} \bmod p$$

由此可知, 验证等式成立, 伪造成功. 验证人认为 (r_n,s_n,M) 是 $U_1,U_2,...,U_n$ 对消息 M 的签名.

第二方面提出的伪造过程简介:

$U_i(i=1,2,...,n)$ 中排在后面的某个签名人可以伪造他前面的几个签名者对消息 M 的签名, 假设, $U_1,U_2,...,U_n$ 中有人预伪造 $U_1,U_2,...,U_{i-1}$ 对消息 M 的签名, U_i 的操作如下:

1) 随机选择并设 U_i 随机选择 $x_i\in[1,P]$, 并设 $y_i^{'}=g^{x_i} \bmod p$ $y_i=\prod_{j=1}^{i-1}y_j^{-1}y_i^{'} \bmod p$ 公开 y_i.

2) 签名者 U_i 随机选择 $k_j\in[1,P]$, $r_j=g^{k_j} \bmod p(j=1toi)$, 并广播 $r_1,r_2,...,r_{i-1}$ 给验证人, 随之计算 $s_i=x_ih(M)-\sum_{j=1}^{i}r_jk_j \bmod(p-1)$, U_i 将 (r_i,s_i,M) 向后一个签名者发送. 将 r_i 传送给 U_i 后面的签名人 U_{i+1} 和验证人. 如果 U_{i+1} 验证 $g^{s_i}\prod_{j=1}^{i}r_j^{r_j}\stackrel{?}{=}\prod_{j=1}^{i}(y_j)^{h(M)} \bmod p$ 成立则伪造签名成功.

验证过程:

$$\prod_{j=1}^{i}y_j=y_1...y_{i-1}(y_i^{'}\prod_{j=1}^{i-1}y_j^{-1} \bmod p)=y_i^{'} \bmod p$$

$$g^{s_i} g^{\sum_{j=1}^{i} r_j k_j} = (y_i')^{h(M)} \bmod p$$

$$g^{s_i} \prod_{j=1}^{i} r_j^{r_j} = \prod_{j=1}^{i} (y_j)^{h(M)} \bmod p$$

由此可知, 验证等式成立, 伪造成功. U_{i+1} 认为 (r_i, s_i, M) 是 $U_1, U_2, ..., U_{i-1}$ 对消息 M 的签名.

W 方案提出的第一方面的伪造攻击经分析是正确的, 合理的.

Z 方案提出 W 方案提出的第二方面的伪造攻击仍然可以得到扩展.

3　分析Z方案提出的伪造攻击

Z 方案提出: 设 $U_f (1 \le f < i)$ 是被 U_i 截取签名的 U_i 之前的任意一个签名者, 则 U_i 可以伪造 $U_f, U_{f+1}, ..., U_i$ 对消息 M 的签名. 并进行了以下证明:

1) 设 U_i 随机选择 $x_i \in [1, P]$, 并设

$$y_i' = g^{x_i} \bmod p \quad y_i = \prod_{j=f}^{i-1} y_i^{-1} y_i' \bmod p \tag{1}$$

公开 y_i.

2) 签名者 U_i 随机选择 $k_j \in [1, P]$, $r_j = g^{k_j} \bmod p (j = f to i)$, 并广播 r_j, 计算 $s_i = s_{f-1} + x_i h(M) - \sum_{j=f}^{i} r_f k_f \bmod (p-1)$, U_i 将 (r_i, s_i, M) 向后一个签名者发送.

3) Z 方案提出只要通过以下验证等式就能成功进行伪造:

$$g^{s_i} \prod_{j=1}^{i} r_j^{r_j} = \prod_{j=1}^{i} (y_j)^{h(M)} \bmod p \tag{2}$$

4) Z 方案的证明过程如下:

首先由已知 $s_i = s_{f-1} + x_i h(M) - \sum_{j=f}^{i} r_f k_f \bmod (p-1)$ 计算

$$g^{s_i} = g^{s_{f-1} + x_i h(M) - \sum_{j=f}^{i} r_j k_j} \bmod p$$

$$= g^{x_i h(M)} \cdot g^{s_{f-1} - \sum_{j=f}^{i} r_j k_j} \bmod p$$

$$= g^{x_i h(M)} \cdot g^{s_{f-1}} / g^{\sum_{j=f}^{i} r_j k_j} \bmod p$$

其次计算 $\prod_{j=1}^{i} r_j^{r_j} = \prod_{j=1}^{f-1} r_j^{r_j} \cdot \prod_{j=f}^{i} r_j^{r_j}$

$$= \prod_{j=1}^{f-1} r_j^{r_j} \cdot \prod_{j=f}^{i} (g^{k_j})^{r_j} \bmod p$$

$$= \prod_{j=1}^{f-1} r_j^{r_j} \cdot g^{\sum_{j=f}^{i} r_j k_j} \bmod p$$

最后计算 $g^{s_i} \prod_{j=1}^{i} r_j^{r_j} = g^{x_i h(M)} \cdot g^{s_{f-1}} / g^{\sum_{j=f}^{i} r_j k_j}$

$$\cdot \prod_{j=1}^{f-1} r_j^{r_j} \cdot g^{\sum_{j=f}^{i} r_j k_j} \bmod p$$

$$= \prod_{j=1}^{f-1} r_j^{r_j} \cdot g^{s_{f-1}} \cdot g^{x_i h(M)} \bmod p \tag{3}$$

$$= g^{x_i h(M)} \cdot \prod_{j=1}^{f-1} (y_j)^{h(M)} \tag{4}$$

$$= y_i' \prod_{j=1}^{f-1} y_j^{h(M)} \bmod p$$

按 Z 方案介绍,上式联合式(1)可以得出式(2).

但是本文发现 Z 方案存在以下缺陷:

1)参数选择 $s_i = s_{f-1} + x_i h(M) - \sum_{j=f}^{i} r_f k_f \bmod (p-1)$ 有误,应该选择 $s_i = s_{f-1} + x_i h(M) - \sum_{j=f}^{i} r_j k_j \bmod (p-1)$.

2)即使假设参数正确,选择 $s_i = s_{f-1} + x_i h(M) - \sum_{j=f}^{i} r_j k_j \bmod (p-1)$, 由式(3)推导出式(4),要用到式(2),不能用结论证明结论,所以由式(3)推导出式(4)步骤不可行.

3)按照已知假设式(1),从式(3)开始推导如下:

$$g^{s_i} \prod_{j=1}^{i} r_j^{r_j} = g^{x_i h(M)} \cdot g^{s_{f-1}} / g^{\sum_{j=f}^{i} r_j k_j}$$

$$\cdot \prod_{j=1}^{f-1} r_j^{r_j} \cdot g^{\sum_{j=f}^{i} r_j k_j} \bmod p$$

$$= \prod_{j=1}^{f-1} r_j^{r_j} \cdot g^{s_{f-1}} \cdot g^{x_i h(M)} \bmod p \tag{3}$$

$$= \prod_{j=1}^{f-1} r_j^{r_j} \cdot g^{s_{f-1}} \cdot (y_i')^{h(M)} \bmod p$$

$$\ne \prod_{j=1}^{i} (y_j)^{h(M)} \bmod p$$

因为验证等式不成立,所以伪造过程证明不成立,也就不能证明方案可以被伪造.

总的来说,Z 方案提出的扩展改进思路是正确的,只是部分参数设置欠合理,如 s_i, 推导过程欠合理,如由式(3)推导出式(4),要用到式(2),不能用结论证明结论.

4　新的增强的有序多重签名方案

在以上几个方案基础上,本节提出一种新的增强的可以抵抗伪造攻击的有序多重签名方案,新的方案改进了 Z 方案的参数,改进的参数弥补原方案的不足,设置合理,推导正确. 相比于以上方案,又增加了新的参数 W. 新的方案系统建立和 Z 方案基本相同,除了在 Z 方案的基础上改进了一些参数外, 新增加的参数 W 中规定了 $U_i (i = 1,2,...,n)$ 的签名顺序为 $U_1, U_2, ..., U_n$, 使签名者很难进行伪造,还包括签名者的公钥等信息,使签名者不能任意调换公钥.

4.1 签名方案

签名过程:

1)签名者U_1随机选择$k_1 \in [1,P]$,计算

$r_1 = g^{k_1} \bmod p$和$s_1 = x_1 y_1 h(M,W) - r_1 k_1 \bmod p$

2)第一个签名者U_1将(r_1, s_1, W, M)向后一个签名者发送,广播r_1给所有的签名者.

3)签名者$U_i (i = 2,...,n)$按i序号先后顺序随机选择$k_i \in [1,P]$,计算

$r_i = g^{k_i} \bmod p, s_i = s_{i-1} + x_i y_i h(M,W) - r_i k_i \bmod p$

4)U_i将(r_i, s_i, W, M)向后一个签名者发送,广播r_i给所有的签名者.

验证过程:

U_n将(r_n, s_n, W, M)发送给U_V,U_V检查$g^{s_n} \prod_{j=1}^{n} r_j^{r_j} = \prod_{j=1}^{n} (y_j^{y_j})^{h(M,W)} \bmod p$是否成立,等式成立则签名有效,否则签名不被承认.

4.2 方案性能分析

4.2.1 正确性分析

由

$s_1 = x_1 y_1 h(M,W) - r_1 k_1 \bmod p$

$s_i = s_{i-1} + x_i y_i h(M,W) - r_i k_i \bmod p$可知:

$s_2 = s_1 + x_2 y_2 h(M,W) - r_2 k_2 \bmod p$

$= x_1 y_1 h(M,W) - r_1 k_1 + x_2 y_2 h(M,W) - r_2 k_2 \bmod p$

$= (x_1 y_1 + x_2 y_2) h(M,W) - (r_1 k_1 + r_2 k_2) \bmod p$

……

$s_n = s_{n-1} + x_n y_n h(M,W) - r_n k_n \bmod p$

$= x_1 y_1 h(M,W) - r_1 k_1 + x_2 y_2 h(M,W) - r_2 k_2 + ...$

$+ x_n y_n h(M,W) - r_n k_n \bmod p$

$= (x_1 y_1 + x_2 y_2 + ... + x_n y_n) h(M,W) - (r_1 k_1 + r_2 k_2 + ... + r_n k_n) \bmod p$

下面证明验证等式的成立:

$$g^{s_n} \prod_{j=1}^{n} r_j^{r_j} = \prod_{j=1}^{n} (y_j^{y_j})^{h(M,W)} \bmod p$$

左边$= g^{s_n} \prod_{j=1}^{n} r_j^{r_j}$

$= g^{(x_1 y_1 + x_2 y_2 + ... + x_n y_n) h(M,W) - (r_1 k_1 + r_2 k_2 + ... + r_n k_n)} \prod_{j=1}^{n} r_j^{r_j}$

$= ((g^{x_1})^{y_1} . (g^{x2})^{y2} ... (g^{xn})^{yn})^{h(M,W)} / g^{\sum_{j=1}^{n} r_j k_j} . \prod_{j=1}^{n} r_j^{r_j}$

$= ((y_1)^{y_1} . (y_2)^{y2} ... (y_n)^{yn})^{h(M,W)} / g^{\sum_{j=1}^{n} r_j k_j} . \prod_{j=1}^{n} r_j^{r_j}$

$= ((y_1)^{y_1} . (y_2)^{y2} ... (y_n)^{yn})^{h(M,W)} / \prod_{j=1}^{n} (g^{k_j})^{r_j} . \prod_{j=1}^{n} r_j^{r_j}$

$= ((y_1)^{y_1} . (y_2)^{y2} ... (y_n)^{yn})^{h(M,W)} / \prod_{j=1}^{n} (r_j)^{r_j} . \prod_{j=1}^{n} r_j^{r_j}$

$= ((y_1)^{y_1} . (y_2)^{y2} ... (y_n)^{yn})^{h(M,W)}$

右边$= \prod_{j=1}^{n} (y_j^{y_j})^{h(M,W)}$

$= ((y_1)^{y_1} . (y_2)^{y2} ... (y_n)^{yn})^{h(M,W)}$

通过证明可知验证等式左右相等,所以验证等式是正确的,可以得出签名有效的结论,说明提出的新方案是个正确的方案.

4.2.2 安全性分析

同样假设$U_f (1 \le f < i)$是被U_i截取签名的U_i之前的任意一个签名者,则U_i不能伪造$U_f, U_{f+1}, ..., U_i$对消息 M 的签名. 证明:

1) 签名者U_i随机选择$x_i \in [1,P]$,并设

$y_i' = g^{x_i} \bmod p$, $y_i = \prod_{j=f}^{i-1} y_i^{-1} y_i' \bmod p$

2) 签名者U_i计算$r_j = g^{kj} \bmod p (j = ftoi)$和

$s_i = s_{f-1} + x_i y_i h(M,W) - \sum_{j=f}^{i} r_j k_j \bmod (p-1)$

3) 签名者U_i发送(M, r_i, W, s_j)给U_{i+1}.

4) 检验$g^{S_i} \prod_{j=1}^{i} r_j^{r_j} \stackrel{?}{=} \prod_{j=1}^{i} r_j^{r_j} (y_j^{y_j})^{h(M,W)} \bmod p$

5) $g^{S_i} = g^{s_{f-1} + x_i y_i h(M,W) - \sum_{j=f}^{i} r_j k_j \bmod (p-1)} \bmod p$

$= g^{x_i y_i h(M,W)} \cdot g^{s_{f-1} - \sum_{j=f}^{i} r_j k_j \bmod (p-1)} \bmod p$

$= g^{x_i y_i h(M,W)} \cdot g^{s_{f-1}} / g^{\sum_{j=f}^{i} r_j k_j} \bmod p$

6) $\prod_{j=1}^{i} r_j^{r_j} = \prod_{j=1}^{f-1} r_j^{r_j} \cdot \prod_{j=f}^{i} r_j^{r_j}$

$= \prod_{j=1}^{f-1} r_j^{r_j} \cdot \prod_{j=f}^{i} (g^{k_j})^{r_j} \bmod p$

$= \prod_{j=1}^{f-1} r_j^{r_j} \cdot g^{\sum_{j=f}^{i} r_j k_j} \bmod p$

7) $g^{S_i} \prod_{j=1}^{i} r_j^{r_j} = g^{x_i y_i h(M,W)} \cdot g^{s_{f-1}} / g^{\sum_{j=f}^{i} r_j k_j}$

$\cdot \prod_{j=1}^{f-1} r_j^{r_j} \cdot g^{\sum_{j=f}^{i} r_j k_j} \bmod p$

$= \prod_{j=1}^{f-1} r_j^{r_j} \cdot g^{s_{f-1}} \cdot g^{x_i y_i h(M,W)} \bmod p$

$= \prod_{j=1}^{f-1} r_j^{r_j} \cdot g^{s_{f-1}} \cdot (y_i')^{y_i h(M,W)} \bmod p$

$\neq \prod_{j=1}^{n} (y_j^{y_j})^{h(M,W)} \bmod p$

由于等式不成立, 所以伪造攻击不成立, 方案满足不可伪造性, 可以抵抗公钥替换攻击, 方案是安全的.

此外还满足以下安全性质:

1)不可滥用: W 规定了签名的范围, 任何签名人都不能超过规定的范围.

2)可验证性: 验证人可以验证签名是否有效, 而且可以确定签名的顺序.

3)不可抵赖: 规定了签名的顺序和签名人的公钥, 签名生成后, 任何签名人不能抵赖.

4)身份可识别性: W 中有签名人的公钥, 任何人可以从中识别签名人的身份.

5 结语

在需要多个人签署一个文件, 这个文件才有效时, 而且是一个签名者必须在他前面的一个或者多个签名者都按顺序签名后他才能签名的情况下, 例如总经理只有看到其他相关部门经理签名后, 才能放心的签名. 这就用到有序多重签名方案.

本文在研究多种有序多重签名方案的基础上, 提出 Z 方案存在缺陷, 针对 Z 方案进行分析和改进, 新的方案改进了 Z 方案的参数并在 Z 方案基础上增加了新的安全参数, 改进后的方案满足原有方案基本的安全特性, 又有了新安全特性, 新的方案更加强健、安全, 适用性更强.

参考文献

1 ElGamal TA. Public cryptosystem and signature scheme based on discrete logarithms. IEEE Trans, 1985, IT-31(14): 469–472.

2 Harn L, Xu Y. Design of generalised ElGamal type digital signature schemes based on the discrete ogarithms. Electronics Letters, 1994, 30(24): 2025–2026.

3 Harn L. New digital signature scheme based on discrete logarithm, Electronics Letters, 1994, 30(5): 396–398.

4 李子臣,杨义先.ElGamal 多重数字签名方案.北京:北京邮电大学学报,1999,22:30–34.

5 秦艳琳,吴晓平.高效的无证书有序多重签名方案.通信学报,2013,(7):105–110.

6 焦阳,傅德胜.基于 ElGamal 的有序多重数字签名方案.四川大学学报(自然科学版),2013,50(4):757–759.

7 李沛,王天芹.基于身份的代理签名方案.计算机技术与发展,2011,21(5):155–162.

8 高雪寒.RSA 数字签名解决短信欺骗.计算机技术与发展,2013,23(1):161–164.

9 王晓明.一种多重数字签名方案的安全性分析.南开大学学报(自然科学版),2006,36:33–38.

10 张骏,陈力群.一种改进的 Elgamal 有序多重签名方案.计算机应用与软件,2009,26(3):258–259.