基于 ElGamal 体制的指定验证人多重数字签名

段昌敏[1],粟 栗[2]
DUAN Chang-min[1],SU Li[2]

1.湖北民族学院 信息工程学院,湖北 恩施 445000
2.华中科技大学 计算机学院,武汉 430074
1.School of Information Engineering,Hubei Institute for Nationalities,Enshi,Hubei 445000,China
2.College of Computer Science and Technology,Huazhong University of Science and Technology,Wuhan 430074,China
E-mail:bydht@163.com

DUAN Chang-min,SU Li.Designated verifier multisignature schemes based on ElGamal scheme.Computer Engineering and Applications,2007,43(36):153-156.

Abstract: Publicly verifiable multisignature makes the leakage of information,which is harmful to information security.Designated verifier multisignatures are privacy-oriented signatures that provide message authenticity only to specific receiver,which is suitable for some specific conditions.The paper proposes two designated verifier multisignature schemes based on ElGamal algorithm and designated verifier signature.One is a verifiably sequential multisignature,the other is a broadcasting multisignature.These multisignature schemes have the attribute of specified receiver,can avoid the leakage of information of both receiver and signatures,and resist forgery and coalition.The size of signature does not increase with signer number.These two schemes ensure the security of receiver and signatures.

Key words: disignated receiver multisignature;sequential multisignature;broadcasting multisignature

摘 要:通过分析指出公开可验证的多重签名会产生信息泄漏,危机信息安全,指出指定验证人多重签名能保护信息的安全性,并设计了两个基于 ElGamal 体制的方案:一种是可验证的按序多重签名,另一种是可抵制合谋攻击的广播多重签名。两种方案都具有指定验证人的特性,避免了签名者和接收者的信息泄漏,同时签名长度都不随签名者的人数增加而增长,并能抵制伪造和勾结攻击,能保障签名者和签名接收者的安全性。

关键词:指定验证人多重数字签名;按序多重签名;广播多重签名
文章编号:1002-8331(2007)36-0153-04 **文献标识码:**A **中图分类号:**TP309

1 前言

多重数字签名或门限多重签名适用于需要多个用户同时认证的需求,文献[1-4]中给出了不同的多重数字签名方案。任何人都可用签名者的公钥集验证多重签名的有效性,称文献[1-4]中的多重签名方案是公开可验证的。公开可验证的签名在特殊情况下也可能造成安全隐患, 例如涉及到私人财产或机密协议,任何人都可以通过签名公开示证;在分级授权系统中,也可以通过签名者的身份判断签名接收者的身份。

基于公开可验证签名引起的信息泄漏,Nyberg 等[5]提出认证加密和指定验证人签名,只有指定的接收者才能恢复和验证签名的密文或密文的签名。该性质能保护签名接收者信息的私密性, 攻击者从签名中不能获取签名者和接收者的相关信息。文献[6,7]对指定验证人签名的安全性进行了系统分析,证明了指定验证人签名具备理论上的完整性。文献[8]中设计了不需要使用随机预言机和零知识协议的安全指定验证人签名方案。文献[9,10]中设计了具有多个指定验证人的签名方案,并提出了指定验证人多重数字签名的思想。

本文首先对公开可验证的多重签名进行分析,指出其可能导致签名滥用、泄露用户私有信息等不安全因素。基于文献[9,10]中对适用于多个指定验证人的签名进行了讨论,提出基于 ElGamal 体制的指定验证人按序多重签名和指定验证人广播多重签名两种方案。两个方案中的签名都同时具备多重签名和指定验证人签名的性质:除签名者和接收者外,其他人不能验证和使用签名; 签名的长度不随签名人数的增加而增长;签名具有可验证性;签名不可伪造和抵赖,并能抵制勾结;即使攻击者截获签名,也不能加以验证,更不能向第三方验证签名的有效性,因此能更好地保护签名收发双方的安全性。

2 指定验证人多重数字签名

假定 SIG 是签名者 $U_1,\cdots,U_n$ 对信息 M 的多重签名,则任何人用签名者的公钥集$(y_1,\cdots,y_n)$对 SIG 加以认证,因而产生以下信息泄漏:

(1)多重签名可能被用于机密信息的公开验证。若任何人都可以对 SIG 的有效性加以验证,攻击者可以通过重签名知道信息 M 是否已经被签名者正确签名。例如双方希望秘密签署某个协议而不让外人知道工作进展(如商业收购、军事协定、匿

作者简介:段昌敏(1973-),男,硕士,讲师,主要研究领域为网络安全,计算机通信技术;粟栗(1981-),男,博士生,主要研究领域为公钥密码,网络安全。

名电子捐赠),用公开可验证的多重签名不能达到理想效果。

(2)泄漏用户的私有信息。譬如联合发布的证书,不同的发布者组合可能对应于不同的证书,在获取到请求者的重签名后,攻击者可以根据发布者的组合以一定概率判断请求者所得到的证书类型,从而判断请求者的私有信息;在多级安全系统授权中,授予的权限一般与授权者的身份对应,所以通过授权者的身份可以知道授予的权限,从而推断被授权者的身份。

可知,公开可验证的多重签名在特定情况下可能造成信息泄露。指定验证人签名中,只有签名接收者才能验证和向第三方证明签名的有效性,其他人不能验证或证明签名的有效性,也不能从签名中获取所有者或签发者的身份信息,较好地保护了签名收发双方的权利。在重签名中引入指定验证人功能,形成指定验证人多重签名[10]。

定义 1 指定验证人多重数字签名 若一个多重签名同时满足指定验证人签名的性质,则称该多重签名为指定验证人多重数字签名。指定验证人的多重签名满足以下性质:

(1)签名长度不随签名人数增加而变化;

(2)验证的计算复杂度不随签名人数增加而变化;

(3)除签名所有者或指定验证人外,其他人不能对签名的有效性加以验证。

采用指定验证人功能的重签名,即使攻击者截获签名,也不能加以验证,更不能向第三方验证签名的有效性,因此能更好地保护签名收发双方的安全性。

3 基于 ElGamal 体制的指定验证人按序多重签名

多重数字签名包括按序多重签名和广播多重签名两种形式。按序多重签名时,多个签名者必须按指定顺序签名;广播多重签名时,多个签名者是无序的。基于 ElGamal 签名体制分别设计两种指定接收人按序多重签名。

3.1 系统初始化

选择由可信中心发布大素数 p>512 bit,一个 p 阶生成元 $g\in Z_p^*$,一个无碰撞的单向散列函数 $h(\ )$。公开参数 $p,g,h(\ )$。假定有 n 个签名者 $U_1,\cdots,U_n$,他们分别拥有不同的私钥 $x_i\in_R Z_p^*$ $(1\leqslant i\leqslant n)$,并且公布其公钥 $y_i=g^{x_i} \bmod p$。签名的接收者拥有私钥 $x_R\in_R Z_p^*$,$y_R=g^{x_R} \bmod p$。M 表示需要签名的消息,$SigU_i$ 表示第 i 个签名者的签名。

3.2 指定验证人按序多重签名算法

签名接收者首先确定 n 个签名者 $U_1,\cdots,U_n$ 顺序对消息 M 进行签名,并公布签名顺序,然后将消息 M 秘密发送给 n 个签名者,n 个签名者按指定顺序对 M 进行签名。

(1)第一个签名者 U_1 执行如下的签名算法:

步骤 1 选取随机数 $k_1\in_R Z_p^*$,计算 $r_1=y_2^{k_1} \bmod p$,$e_1=h(r_1,M)$;

步骤 2 计算 $s_1=k_1e_1-x_1 \bmod (p-1)$;

步骤 3 置 $f_1=1$。

签名者 U_1 公布 f_1,并将签名的结果(r_1,s_1)发送给其他签名者。

(2)第 $i(1<i\leqslant n)$个签名者获得 U_{i-1} 的部分签名 $SigU_{i-1}$ 后,首先验证签名正确性,然后计算第 i 个部分签名。执行部分签名验证算法为:

步骤 1 计算 $t_{i-1}=g^{s_{i-1}}\cdot f_{i-1}\cdot\prod_{j=1}^{i-1}y_j$。验证 $t_{i-1}=1$ 是否成立,如果 $t_{i-1}\neq 1$ 则继续步骤 2,否则请求第 $i-1$ 个签名者重新签名,直到 $t_{i-1}\neq 1$;

步骤 2 验证 $r_{i-1}^{h(r_{i-1},M)}=t_{i-1}^{x_i} \bmod p$ 是否成立,如果成立则说明对消息 M 部分签名正确。

(3)如果验证签名者 U_{i-1} 的部分签名 $SigU_{i-1}$ 成立,则 U_i 计算部分签名 $SigU_i$ 如下:

步骤 1 选取随机数 $k_i\in_R Z_p^*$,计算 $r_i=y_{i+1}^{k_i} \bmod p$,$e_i=h(r_i,M)$;

步骤 2 计算 $s_i=s_{i-1}+k_ie_i-x_i \bmod (p-1)$;

步骤 3 计算 $f_i=f_{i-1}\cdot(r_{i-1}')^{-e_{i-1}'\cdot x_i^{-1}} \bmod p$;

步骤 4 公布 f_i,并将签名(r_i,s_i)发送给第 $i+1$ 个签名者,直到第 n 个签名者。

第 n 个签名者的签名发往接收者,所以他以 y_R 为底计算 $r_n=y_R^{k_n} \bmod p$,并计算出相应的 r_n、s_n 和 f_n。公布 f_n,将签名(r_n,s_n)发送给签名接收者,接收者采用自己的私钥对签名进行认证。

3.3 按序多重签名的验证和使用

3.3.1 验证过程

当需要使用签名时,签名接收者通过向第三方出示签名(r_n,s_n)和 f_n,并配合第三方验证该签名是由签名者 $U_1,\cdots,U_n$ 共同签发的。验证过程为:

(1)第三方首先计算 $y=\prod_{j=1}^{n}y_j \bmod p$ 和 $e_n=h(r_n,M)$;

(2)第三方计算 $t_n=g^{s_n}\cdot f_n\cdot y \bmod p$ 并验证 $t_n\neq 1$;

(3)签名所有者通过文献[6]中交互式离散对数零知识证明协议向第三方证明自己拥有 x_R,使得等式 $r_n^{h(r_n,M)}=t_n^{x_R} \bmod p$ 和 $g^{x_R}=y_R$ 成立来证明签名有效,且是发给该接收者的。

3.3.2 正确性证明

若已知签名(r_n,s_n)和 f_n 以及 n 个签名者 $U_1,\cdots,U_n$ 的顺序,则计算 $t_n=g^{s_n}\cdot f_n\cdot\prod_{j=1}^{n}y_j \bmod p$,若 $r_n^{h(r_n,M)}=t_n^{x_R} \bmod p$ 成立说明签名有效。

证明 由签名过程可知

$$g^{s_n}=g^{(k_1e_1+k_2e_2+\cdots+k_ne_n)-(x_1+x_2+\cdots+x_n) \bmod (p-1)} \bmod p\equiv g^{\sum_{i=1}^{n}k_ie_i}\cdot\prod_{j=1}^{n}-y_j \bmod p$$

$$f_n\equiv f_{n-1}r_{n-1}^{-e_{n-1}\cdot x_n^{-1}}\equiv\prod_{j=1}^{n-1}g^{-k_je_j}\cdot \bmod p\equiv g^{-\sum_{j=1}^{n-1}k_j} \bmod p$$

$$t_n^{x_R}\equiv(g^{s_n}\cdot f_n\cdot\prod_{j=1}^{n}y_j)^{x_R}\equiv(g^{\sum_{j=1}^{n}k_je_j}\cdot\prod_{j=1}^{n}-y_j\cdot g^{-\sum_{j=1}^{n-1}k_je_j}\cdot\prod_{j=1}^{n}y_j)^{x_R}\equiv y_R^{k_ne_n}\equiv r_n^{h(r_n,M)} \bmod p$$

因此,验证等式 $r_n^{h(r_n,M)}=t_n^{x_R} \bmod p$ 成立则签名有效。

3.4 按序多重签名的安全性分析

(1)机密性。即使攻击者获得了签名,由于验证要求 $t_{i-1}=g^{s_{i-1}}\cdot f_{i-1}\cdot\prod_{j=1}^{i-1}y_j$ 和 $r_{i-1}^{h(r_{i-1},M)?}=t_{i-1}^{x_i} \bmod p$,而攻击者不知道 x_i,他不能验证签名,也不能向第三方证明签名的有效性。

(2)签名不能伪造。每个签名者 U_i 生成部分签名时计算 $r_i=$

$y_{i+1}^{k_i}=g^{(x_{i+1}\cdot k_i)} \bmod p$,相当于选取了随机数 $x_{i+1}\cdot k_i$,与 ElGamal 方案相比,其他步骤均无变化。由于随机数的选取方式不影响安全性,故每个部分签名的不可伪造性等同于 ElGamal 签名。

(3)签名者不能否认自己的签名。因为在签名 s 使用了签名接收者私钥,并采用该签名者的公钥验证,而签名者的公钥与签名者是唯一对应的,所以签名者不能否认自己的签名。

(4)签名方案能抵制勾结。在按序签名方案中,若 k 个攻击者期望通过勾结来否认他们产生的部分签名,必须将原签名传递给后续的签名者 U_i,并通过认证。其难度相当于不使用自己的私钥并构造一个 ElGamal 签名,基于签名的不可伪造性是不可实现的。

4　指定验证人广播多重签名

4.1　指定验证人广播多重签名

指定验证人广播多重数字签名的系统初始化与按序多重签名方案相同。由于广播多重签名的无序性,n 个签名者 $U_1,\cdots,U_n$ 签名的过程相同,以第 i 个签名者为例:

(1)签名接收者选择随机数 n 个随机数 $k_{R1},\cdots,k_{Rn}$,其中 $k_{Ri}\in_R Z_p^*(1\leqslant i\leqslant n)$,计算 $K_{Ri}=g^{k_{Ri}} \bmod p$,并计算 $K_R=K_{R1}\cdot K_{R2},\cdots,K_{Rn}$,公布 K_R;

(2)签名接收者将 k_{Ri} 和需要签名的消息 M 一起安全发送给签名者 U_i;

(3)U_i 选取随机数 $k_i\in_R Z_p^*$,计算 $r_i=y_R^{k_i} \bmod p$,并发送给签名接收者;

(4)签名接收者收集到 n 个 r_i,计算 $r=r_1\cdot r_2,\cdots,r_n \bmod p$,并计算 $e=h(r,M)$,公开 e;

(5)签名者计算 $s_i=(k_i-k_{Ri})e-x_i \bmod (p-1)$,并将 s_i 发送给签名接收者;

(6)签名接收者得到 n 个签名者产生的 s_i 后,首先计算 $s=\sum_{i=1}^{n}s_i \bmod q$,然后验证 s 是否满足等式:$(g^s\cdot\prod_{i=1}^{n}y_i\cdot K_R^e)^{x_R} \bmod p=r^e$,若等式成立,则$(e,s,K_R)$为消息 M 的 n 重签名;否则说明有不正确的 s_i,逐一用等式$(g^{s_i}\cdot y_i\cdot K_{Ri}^e)^{x_R} \bmod p=r_i^e$对签名进行检验,找出不正确的 s_i 值,请求该签名者重新签名,直到正确为止。

4.2　广播多重签名的验证和使用

4.2.1　签名的验证过程

当签名接收者使用重签名时,他需要向第三方(验证者)出示签名(e,s,K_R),并配合第三方验证该签名是由签名者 $U_1,\cdots,U_n$ 共同签发的。验证签名的过程为:

(1)验证者计算 $y=y_1\cdot y_2,\cdots,y_n \bmod p$,$h(r,M)=e$;

(2)验证者计算 $t=g^s\cdot y\cdot K_R^e \bmod p$,将 t 发送给签名接收者;

(3)签名接收者通过文献[6]中的交互式零知识证明协议向验证者证明自己拥有 x_R;签名接收者通过计算 $t^{x_R} \bmod p=r^e$,同时 $g^{x_R}=y_R$ 说明签名(r,s,K_R)是由签名者 $U_1,\cdots,U_n$ 联合对 M 签发的,且是发给他的。

4.2.2　正确性证明

若已知签名(r,s,K_R)和 n 个签名者 $U_1,\cdots,U_n$ 的公钥乘积 y,则等式 $h(r,M)=e$,$(g^s\cdot y\cdot K_R^e)^{x_R} \bmod p=r^e$ 成立说明签名有效。

证明　由签名过程知

$$s\equiv s_1+s_2+\cdots+s_n\equiv\sum_{j=1}^{n}k_j\cdot e+\sum_{j=1}^{n}k_{Rj}\cdot e-\sum_{j=1}^{n}x_j \bmod (p-1)$$

$$g^s\equiv g^{\sum_{i=1}^{n}k_ie}\cdot g^{-\sum_{i=1}^{n}k_{Ri}e}\cdot\prod_{i=1}^{n}y_i^{-1}\equiv g^{\sum_{i=1}^{n}k_ie}\cdot y^{-1}\cdot K_R^{-e} \bmod p$$

$$(g^s\cdot y\cdot K_R^e)^{x_R}\equiv(g^{\sum_{i=1}^{n}k_ie}\cdot y^{-1}\cdot K_R^{-e}\cdot y\cdot K_R^e)^{x_R}\equiv(g^{\sum_{i=1}^{n}k_ie})^{x_R}\equiv$$

$$(y_R^{\sum_{j=1}^{n}k_j})^e\equiv r^e \bmod p$$

因此,等式$(g^s\cdot y\cdot K_R^e)^{x_R} \bmod p=r^e$ 成立说明签名有效。

4.3　广播多重签名的安全性分析

广播多重签名的机密性、不可伪造性和不可否认性均与按序多重签名一致,仅因部分签名的无序性使合谋攻击方式有所不同。文献[11]中指出 t 个恶意的签名者合谋攻击的必要条件是适当各自的私钥和随机数,满足 $\sum_{i=1}^{t}x_i=0 \bmod (p-1)$和 $\sum_{i=1}^{t}k_i=0 \bmod (p-1)$。这将产生与他们私有信息 x 和 k 无关的结果,合谋攻击成功。

文献[12]中指出安全的方案中应该由签名接收者和签名者共同生成参数,且签名者应该在签名接收者发送参数前对自己的公钥做出承诺,使得签名者不能随意修改和选择公私钥,构造合谋攻击。本文的广播签名方案中,要求签名者先公布自己的公钥,如果需要修改公钥,则由签名接收者重新生成随机数。由于签名接收者和签名者共同生成密钥,破坏了合谋攻击的必要条件,所以签名者不能形成勾结。

5　性能分析

(1)两个方案产生的签名长度不随签名人数的增加而增长。

(2)具备指定验证人签名性质。在本文的两个方案中,采用下一个签名者或签名接收者的公钥为底数计算签名项 r,除使用该公钥对应的私钥外,都不能有效地验证该签名,也无法向第三方证明签名的有效性。满足了指定验证的性质,保护了签名接收者信息不被泄漏。

(3)签名者的机密性。两个方案中,除指定签名接收者外,攻击者并不能正确地解开签名,而在签名中,也没有签名者的直接身份信息,所以不能识别签名者的身份。方案同时保证了签名收发双方身份的机密性。

(4)签名可以验证。按序多重签名中每一个签名者都必须首先验证上一个签名的正确性,才能执行下一个签名,从而传递地验证了签名;广播多重签名中签名接收者可以对单个签名者产生的签名加以验证。

(5)计算量和通信量。定义 T_h、T_{exp}、T_{mul} 分别表示一次模 p 的散列运算、幂运算和乘运算的时间。按序签名方案所需要的计算包括验证上一个部分签名和计算部分签名。验证签名时间固定为 $3T_{exp}+2T_{mul}+T_h$,不随签名人数的变化而变化。计算部分签名的时间为 $2T_{exp}+3T_{mul}+T_h$,总计算量为 $5T_{exp}+5T_{mul}+2T_h$。签名过程中与接收者交互 2 次。

广播多重签名中,n 个签名者执行签名共需要 $n(T_{exp}+T_{mul})$,签名接收者在签名生成过程中需要 $nT_{exp}+(2n-2)T_{mul}+T_h$,验证 n 重签名需要 $4T_{exp}+(n+1)T_{mul}$,在签名过程中 n 个签名者共与签名接收者交互 $4n$ 次。

6 总结

本文对公开可验证的重签名产生的信息泄漏进行了分析，并设计了两个基于 ElGamal 体制的指定验证人多重签名方案解决安全隐患。二个方案中的签名同时具备指定验证人签名和多重签名的性质，签名的长度和验证计算量不随签名人数的增加而增长；签名除指定验证人外，其他人不能从签名中获得收发双方的信息，也不能验证和使用签名。分析指出，指定验证人多重数字签名能更好地保护签名接收者和签名者的隐私，为系统提供了更高的安全性。（收稿日期：2007 年 7 月）

参考文献：

[1] Harn L,Lin C Y,Wu T C.Structured multisignature algorithms[J].IEE Proceedings of Computers and Digital Techniques,2004,151:231-234.

[2] Tada M.An order-specified multisignature scheme secure against active insider attacks[C]//LNCS 2384:Information Security and Privacy,ACISP 2002,2002:328-345.

[3] Wang Y L,Wang L H.A new type of digital multisignature[C]//Proceedings of the 9th International Conference on Computer Supported Cooperative Work in Design 2005.United States:IEEE Computer Society Press,2005,2:750-754.

[4] 陆浪如，曾俊杰，张白愚.基于离散对数多重签名体制的改进[J].通信学报，2002,23(6):1-5.

[5] Nyberg K,Ruppel R A.Message recovery for signature scheme based on discrete logarithm problem[J].Designs Codes and Cryptography,1996,7:61-81.

[6] Kim S J,Park S J,Won D H.Zero-knowledge nominative signatures[C]//International Conference on the Theory and Applications of Cryptology,Process of PragoCrypt'96.Prague,Czech:Technical Publishing House,1996,1:380-392.

[7] Gentry C,Molnar D,Ramzan Z.Efficient designated confirmer signatures without random oracles or general zero-knowledge proofs[C]//LNCS 3788:Advances in Cryptology,ASIACRYPT 2005,2005:662-681.

[8] Lipmaa H,Wang G L,Bao F.Designated verifier signature schemes:attacks,new security notions and a new construction [C]//LNCS 3580:Proceedings of 32nd International Colloquium on Automata,Languages and Programming,2005:459-471.

[9] Chow S S M.Identity-based strong multi-designated verifiers signatures[C]//LNCS 4043:Third European PKI Workshop:Theory and Practice,2006:257-263.

[10] Laguillaumie F,Vergnaud D.Multi-designated verifiers signatures:anonymity without encryption[J].Information Processing Letters,2007,102:127-132.

[11] Wu T,Chou S.Two-based multisignatures protocols for sequential and broadcasting architecture[J].Computer Communication,1996,19:851-856.

[12] 韩小西，王贵林，鲍丰.针对基于离散对数多重签名方案的一种攻击[J].计算机学报，2004,27(8):1147-1152.

（上接 76 页）

表 3 负荷预测结果

日期	实际值	本文算法		GA 算法		SA 算法	
		预测值	误差	预测值	误差	预测值	误差
6 月 16 日	801.070 0	800.511 5	−0.069 8	786.345 6	−1.872 5	805.311 3	0.526 7
6 月 23 日	805.010 0	810.661 8	0.697 2	793.850 1	−1.405 8	796.316 5	−1.091 7
6 月 30 日	815.080 0	816.464 7	0.157 4	795.158 0	1.612 6	787.283 7	−3.543 4
7 月 6 日	832.250 0	830.292 4	−0.235 8	803.876 2	−3.529 6	810.536 2	−2.678 9
7 月 13 日	818.210 0	821.137 7	0.356 5	800.145 2	−2.257 7	805.353 1	−1.596 4
7 月 20 日	836.980 0	835.197 0	−0.213 5	819.603 1	−2.120 2	818.409 8	−2.269 1
7 月 27 日	843.950 0	846.949 0	0.354 1	8 824.880 6	−2.311 8	831.640 4	−1.480 2
绝对平均误差			0.297 8		2.158 6		1.883 8

结构和权值的算法，它是在遗传算法中对控制码和权值域分别引进算子。在交叉过程中，对权值应用自适应交叉和变异率，引入向适应度高的方向进化的交叉算子，对控制基因用两点交叉。在变异时，对控制基因采用基本变异算子，之后将中间种群中的适应度高的个体在其周围进行模拟退火，这样充分发挥了遗传算法和模拟退火算法的优点，克服了遗传算法在神经网络优化过程中存在的不足。表 2 说明，本文算法确实有效地使神经网络的结构和权值同时得到了优化；表 3 说明将本文算法优化神经网络应用于预测，确实提高了收敛速度，得到了较高的预测精度。（收稿日期：2007 年 7 月）

参考文献：

[1] 高大文，王鹏.人工神经网络中隐含层节点与训练次数的优化[J].哈尔滨工业大学学报，2003,35(2):207-209.

[2] 金朝红，吴汉松，李腊梅，等.一种基于自适应遗传算法的神经网络学习算法[J].微计算机信息，2005,21:49-51.

[3] 田旭光，宋彤，刘宇新.结合遗传算法优化 BP 神经网络的结构和参数[J].计算机应用与软件，2004,21(6):69-71.

[4] Holland J H.Adaptation in natural and artificial systems[D].Ann Arbor University of Michigan Pre,1975.

[5] 叶德谦，康建红，杨樱.实数编码遗传算法的前向神经网络优化设计[J].计算机工程，2005,31(16):163-164.

[6] Metropolis N.Equations of state calculations by fast computing machines[J].J Chem Phys,1953(21):1087-1091.

[7] Kirkpatrick S,Gelatt C D,Vechi Jr M P.Optimization by simulated annealing[J].Science,1983(220):671-680.

[8] 王凌.智能优化算法[M].北京：清华大学出版社；施普林格出版社，2001.

[9] 曹军，苏建民.遗传算法与模拟退火算法在神经网络优化中的性能分析[J].东北林业大学学报，2002,30(6):26-28.