正则蕴涵算子族 $G-\lambda-R_0$ 的约束度理论相关研究

张 森,张兴芳
ZHANG Sen,ZHANG Xing-fang

聊城大学 数学科学学院,山东 聊城 252059
School of Mathematics Science,Liaocheng University,Liaocheng,Shandong 252059,China
E-mail:32415328@qq.com

ZHANG Sen,ZHANG Xing-fang.Analytical constraint degree and α-triple I method for fuzzy reasoning based on implication operators $G-\lambda-R_0$.Computer Engineering and Applications,2010,46(7):49-51.

Abstract: The theory of constraint degree of triple I method for fuzzy reasoning based on implication operators $G-\lambda-R_0$ is studied and its properties are analyzed.The general formulae of supremum(infimum) for solution of α-triple I method are obtained respectively.

Key words: fuzzy reasoning;implication operator $G-\lambda-R_0$;constraint degree;triple I method

摘 要: 研究了基于正则蕴涵算子 $G-\lambda-R_0$ 模糊推理的三 I 算法的约束度理论,分析了约束度的性质,给出了 α-三 I 算法的 FMP(FMT)上(下)确界的计算公式。

关键词: 模糊推理;$G-\lambda-R_0$ 蕴涵算子;约束度;三 I 约束算法
DOI: 10.3778/j.issn.1002-8331.2010.07.015 **文章编号:** 1002-8331(2010)07-0049-03 **文献标识码:** A **中图分类号:** O231

Zadeh[1]于 1973 年首先提出了模糊分离规则(简称 FMP 规则)的 CRI 算法(Compositional Rule of Inference)。针对 CRI 方法,人们进行了大量的研究并提出了许多新的派生推理方法。王国俊[2]首先指出了 CRI 方法的若干缺陷与不足,并基于逻辑语义蕴涵理论提出了模糊推理的全蕴涵三 I 算法。其基本思想为:已知 $A(B)\in F(X)(F(Y))$ 和 $A^*(B^*)\in F(X)(F(Y))$ 时寻求最优的 $B^*(A^*)=F(Y)(F(X))$ 使得 $A\to B$ 全力支持 $A^*\to B^*$,即

$$(A(x)\to B(y))\to(A^*(x)\to B^*(y)) \tag{1}$$

对一切 $x\in X,y\in Y$ 具有最大的可能值,其中 $F(X)$ 和 $F(Y)$ 分别表示 X 和 Y 上的模糊集全体。

文献[1](Klement 与 Navara)研究了基于参数的 T-范数——Frank T-范数的模糊逻辑系统,文献[3]研究了 Schweizer-Sklar T-范数导出的剩余蕴涵族,文献[4]讨论了带参数的 Kleene 系统。在此基础上,文献[5]提出了正则蕴涵算子族 $G-\lambda-R_0$,它具有一些良好的性质,是较理想的模糊蕴涵算子,因此有必要对这一蕴涵算子族关于三 I 方法进行深入的讨论。文献[2]中提出三 I 算法的支持度理论的一般形式化优化问题,然而对模糊控制系统进行模糊推理时,需考虑支持度理论的反问题,即已知 A,B 和 A^*(或 B^*),寻求最优的 B^*(或 A^*)使得

$$(A(x)\to_{G-\lambda-R_0}B(y))\to_{G-\lambda-R_0}(A^*(x)\to_{G-\lambda-R_0}B^*(y))\leqslant\alpha \tag{2}$$

对一切 $x\in X$ 和 $y\in Y$ 成立。该文的目的是基于正则蕴涵算子 $G-\lambda-R_0$ 对这一反问题进行了全面探讨,并研究了三 I 算法的约束度理论。

1 预备知识

定义 1 文献[5]给出了如下 t-模 $\otimes_{G-\lambda-R_0}$

$$x=y\otimes z=\begin{cases}y\wedge z,y\wedge z+\lambda(y\vee z-1)>0\\0,\text{其他情况}\end{cases} \tag{3}$$

其中 $(y,z)\in[0,1]\times[0,1],\lambda\in[0,1]$。

其相应的伴随蕴涵算子为:

$$x=y\to z=\begin{cases}1,y\leqslant z\\z\vee[\lambda(1-y)\wedge y]\vee(1-\frac{y}{\lambda}),y>z\end{cases} \tag{4}$$

其中 $(y,z)\in[0,1]\times[0,1],\lambda\in(0,1]$。

注 1 由文献[5]知,此算子为正则蕴涵算子。

引理 t-模 $\otimes_{G-\lambda-R_0}$ 及其伴随蕴涵算子 $\to_{G-\lambda-R_0}$ 具有如下性质:

(1) $a\otimes_{G-\lambda-R_0}1=a$;

(2) $a\otimes_{G-\lambda-R_0}b=b\otimes_{G-\lambda-R_0}a$;

(3) $(a\otimes_{G-\lambda-R_0}b)\otimes_{G-\lambda-R_0}c=a\otimes_{G-\lambda-R_0}(b\otimes_{G-\lambda-R_0}c)$;

(4) 若 $a\leqslant c,b\leqslant d$,则 $a\otimes_{G-\lambda-R_0}b\leqslant c\otimes_{G-\lambda-R_0}d$;

(5) $b\to_{G-\lambda-R_0}c=1$ 当且仅当 $b\leqslant c$;

基金项目: 教育部科学技术研究重点项目(批准号:206089)。

作者简介: 张森(1986-),男,汉族,硕士研究生,研究方向为非经典数理逻辑;张兴芳(1957-),女,教授,研究生导师,主要研究方向为模糊推理,模糊逻辑,模糊信息处理等。

收稿日期: 2009-09-22 **修回日期:** 2009-12-21

(6)$a\leqslant b\rightarrow_{G\text{-}\lambda\text{-}R_0}c$ 当且仅当 $b\leqslant a\rightarrow_{G\text{-}\lambda\text{-}R_0}c$;

(7)$a\rightarrow_{G\text{-}\lambda\text{-}R_0}(b\rightarrow_{G\text{-}\lambda\text{-}R_0}c)=b\rightarrow_{G\text{-}\lambda\text{-}R_0}(a\rightarrow_{G\text{-}\lambda\text{-}R_0}c)$;

(8)$1\rightarrow_{G\text{-}\lambda\text{-}R_0}c=c$;

(9)$b\rightarrow_{G\text{-}\lambda\text{-}R_0}\bigwedge_{i\in I}c_i=\bigwedge_{i\in I}(b\rightarrow_{G\text{-}\lambda\text{-}R_0}c_i)$,$(\bigvee_{i\in I}b_i)\rightarrow_{G\text{-}\lambda\text{-}R_0}c=\bigwedge_{i\in I}(b_i\rightarrow_{G\text{-}\lambda\text{-}R_0}c)$;

(10)$b\rightarrow_{G\text{-}\lambda\text{-}R_0}c$ 关于 c 单调递增,关于 b 单调递减;

(11)$a\otimes_{G\text{-}\lambda\text{-}R_0}b\leqslant c$ 当且仅当 $a\leqslant b\rightarrow_{G\text{-}\lambda\text{-}R_0}c$。

2 约束度理论

定义 2(α-三 I FMP 原则) 设 X,Y 为非空集,$A(x)\in F(X)$,$A^*(x)\in F(X)$,$B(y)\in F(Y)$,则满足式(2)的 $F(Y)$中的模糊集 $B^*(y)$ 称为式(2)的三 I FMP α-解。

定义 3(α-三 I FMT 原则) 设 X,Y 为非空集,$A(x)\in F(X)$,$B(y),B^*(y)\in F(Y)$,则满足式(2)的 $F(X)$中的模糊集 $A^*(x)$称为式(2)的三 I FMT α-解。

定义 4(约束度) 设 Z 是非空集,$\alpha\in[0,1]$,$C,D\in F(Z)$,若

$$\sup\{C(z)\rightarrow D(z)|z\in Z\}=\alpha$$

则称 C 对 D 的约束度为 α,记为 $rest(C,D)=\alpha$。

注 2 显然,式(2)成立的充要条件是 $A\rightarrow B$ 对 $A^*\rightarrow B^*$ 的约束度小于或等于 α;对于 $\alpha\in[0,1]$,$rest(A,B)\leqslant\alpha$,成立的充要条件是 $A(z)>B(z)(\forall z\in Z)$,且 $A'(z)\leqslant\alpha,B(z)\leqslant\alpha$ 对任意 $z\in Z$ 成立,这里 $A'(z)=1-A(z)$。

定理 1 设 $rest(A,B)=\alpha$,$rest(B,C)=\beta$,则 $rest(A,C)\geqslant\alpha\otimes_{G\text{-}\lambda\text{-}R_0}\beta$。

证明 由已知及定义 4 得,对任意的 $z\in Z$,$A(z)\rightarrow_{G\text{-}\lambda\text{-}R_0}B(z)\leqslant\alpha$ 及 $B(z)\rightarrow_{G\text{-}\lambda\text{-}R_0}C(z)\leqslant\beta$ 成立。

由于 $a\otimes_{G\text{-}\lambda\text{-}R_0}b\leqslant c$ 当且仅当 $a\leqslant b\rightarrow_{G\text{-}\lambda\text{-}R_0}c$,所以

$$\alpha\otimes_{G\text{-}\lambda\text{-}R_0}A(z)\leqslant B(z),\beta\otimes_{G\text{-}\lambda\text{-}R_0}B(z)\leqslant C(z),\ \forall z\in Z$$

于是

$$(\alpha\otimes_{G\text{-}\lambda\text{-}R_0}\beta)\otimes_{G\text{-}\lambda\text{-}R_0}A(z)=\beta\otimes_{G\text{-}\lambda\text{-}R_0}(\alpha\otimes_{G\text{-}\lambda\text{-}R_0}A(z))\leqslant\beta\otimes_{G\text{-}\lambda\text{-}R_0}B(z)\leqslant C(z),\ \forall z\in Z$$

从而 $\alpha\otimes_{G\text{-}\lambda\text{-}R_0}\beta\leqslant A(z)\rightarrow_{G\text{-}\lambda\text{-}R_0}C(z),\ \forall z\in Z$。所以 $rest(A,C)\geqslant\alpha\otimes_{G\text{-}\lambda\text{-}R_0}\beta$。

注 3 若 $rest(A,B)=1$,$rest(B,C)=1$,则 $rest(A,C)=1$。

定理 2 设 $A,B,C\in F(Z)$,则

(1)$rest(A\vee B,C)=rest(A,C)\vee rest(B,C)$

(2)$rest(A,B\wedge C)=rest(A,B)\vee rest(A,C)$

证明(1)

$$rest(A,C)\vee rest(B,C)=\sup\{A(z)\rightarrow_{G\text{-}\lambda\text{-}R_0}C(z)\}\vee\sup\{B(z)\rightarrow_{G\text{-}\lambda\text{-}R_0}C(z)\}$$

$$\sup\{\sup\{A(z)\rightarrow_{G\text{-}\lambda\text{-}R_0}C(z)\},\sup\{B(z)\rightarrow_{G\text{-}\lambda\text{-}R_0}C(z)\}\}=\sup\{A(z)\vee B(z)\rightarrow_{G\text{-}\lambda\text{-}R_0}C(z)\}=rest(A\vee B,C)$$

其中 $z\in Z$。类似地可证明(2)。

推论 设 $A,B,A_i,B_i\in F(Z)(i\in I)$,则

(1)$rest(\bigvee_{i\in I}A_i,B)=\bigvee_{i\in I}rest(A_i,B)$

(2)$rest(A,\bigwedge_{i\in I}B_i)=\bigvee_{i\in I}rest(A,B_i)$

定理 3 设 $A,B,C\in F(Z)$,则

(1)$rest(A,B\rightarrow_{G\text{-}\lambda\text{-}R_0}C)=rest(B,A\rightarrow_{G\text{-}\lambda\text{-}R_0}C)$

(2)$rest(A,B\rightarrow_{G\text{-}\lambda\text{-}R_0}C)=rest(A,(1-C)\rightarrow_{G\text{-}\lambda\text{-}R_0}(1-B))$

证明 (1)由于 $(a\rightarrow_{G\text{-}\lambda\text{-}R_0}(b\rightarrow_{G\text{-}\lambda\text{-}R_0}c)\otimes_{G\text{-}\lambda\text{-}R_0}b)\otimes_{G\text{-}\lambda\text{-}R_0}a=(a\rightarrow_{G\text{-}\lambda\text{-}R_0}(b\rightarrow_{G\text{-}\lambda\text{-}R_0}c)\otimes_{G\text{-}\lambda\text{-}R_0}a)\otimes_{G\text{-}\lambda\text{-}R_0}b\leqslant(b\rightarrow_{G\text{-}\lambda\text{-}R_0}c)\otimes_{G\text{-}\lambda\text{-}R_0}b\leqslant c$,所以 $a\rightarrow_{G\text{-}\lambda\text{-}R_0}(b\rightarrow_{G\text{-}\lambda\text{-}R_0}c)\leqslant b\rightarrow_{G\text{-}\lambda\text{-}R_0}(a\rightarrow_{G\text{-}\lambda\text{-}R_0}c)$。

同理可得 $a\rightarrow_{G\text{-}\lambda\text{-}R_0}(b\rightarrow_{G\text{-}\lambda\text{-}R_0}c)\geqslant b\rightarrow_{G\text{-}\lambda\text{-}R_0}(a\rightarrow_{G\text{-}\lambda\text{-}R_0}c)$,从而 $a\rightarrow_{G\text{-}\lambda\text{-}R_0}(b\rightarrow_{G\text{-}\lambda\text{-}R_0}c)=b\rightarrow_{G\text{-}\lambda\text{-}R_0}(a\rightarrow_{G\text{-}\lambda\text{-}R_0}c)$。

由约束度的定义即可得(1)。

类似地可证明(2)。

定理 4 设 $A,B,C,D\in F(Z)$,则

(1)$rest(A,B\wedge C\rightarrow_{G\text{-}\lambda\text{-}R_0}D)=rest(A,B\rightarrow_{G\text{-}\lambda\text{-}R_0}D)\vee rest(A,C\rightarrow_{G\text{-}\lambda\text{-}R_0}D)$。

(2)$rest(A,B\rightarrow_{G\text{-}\lambda\text{-}R_0}C\vee D)=rest(A,B\rightarrow_{G\text{-}\lambda\text{-}R_0}C)\vee rest(A,B\rightarrow_{G\text{-}\lambda\text{-}R_0}D)$。

证明 (1)由定理 2 和定理 3 得

$$rest(A,B\wedge C\rightarrow_{G\text{-}\lambda\text{-}R_0}D)=rest(B\wedge C,A\rightarrow_{G\text{-}\lambda\text{-}R_0}D)=rest(B,A\rightarrow_{G\text{-}\lambda\text{-}R_0}D)\vee rest(C,A\rightarrow_{G\text{-}\lambda\text{-}R_0}D)=rest(A,B\rightarrow_{G\text{-}\lambda\text{-}R_0}D)\vee rest(A,C\rightarrow_{G\text{-}\lambda\text{-}R_0}D)$$

(2)由定理 2、定理 3 及 De Morgan 对偶律得

$$rest(A,B\rightarrow_{G\text{-}\lambda\text{-}R_0}C\vee D)=rest(A,\neg(C\wedge D)\rightarrow_{G\text{-}\lambda\text{-}R_0}\neg B)=rest(A,\neg C\vee\neg D\rightarrow_{G\text{-}\lambda\text{-}R_0}\neg B)=rest(\neg C\vee\neg D,A\rightarrow_{G\text{-}\lambda\text{-}R_0}\neg B)=rest(\neg C,A\rightarrow_{G\text{-}\lambda\text{-}R_0}\neg B)\vee rest(\neg D,A\rightarrow_{G\text{-}\lambda\text{-}R_0}\neg B)=rest(A,\neg C\rightarrow_{G\text{-}\lambda\text{-}R_0}\neg B)\vee rest(A,\neg D\rightarrow_{G\text{-}\lambda\text{-}R_0}\neg B)=rest(A,B\rightarrow_{G\text{-}\lambda\text{-}R_0}C)\vee rest(A,B\rightarrow_{G\text{-}\lambda\text{-}R_0}\neg D)$$

推论 设 $A,B,C,A_i,B_i,C_i\in F(Z)(i\in I)$,则

(1)$rest(A,\bigwedge_{i\in I}B_i\rightarrow_{G\text{-}\lambda\text{-}R_0}C)=\bigvee_{i\in I}rest(A,B_i\rightarrow_{G\text{-}\lambda\text{-}R_0}C)$

(2)$rest(A,B\rightarrow_{G\text{-}\lambda\text{-}R_0}\bigvee_{i\in I}C_i)=\bigvee_{i\in I}rest(A,B\rightarrow_{G\text{-}\lambda\text{-}R_0}C_i)$

3 α-三 I 算法的 FMP(FMT)上(下)确界

定理 5(α-三 IFMP 算法) 设 X,Y 为非空集,$A(x),A^*(x)\in F(X)$,$B(y)\in F(Y)$,$0\leqslant\alpha\leqslant1$,则式(2)的三 I FMP α-解,即 $F(Y)$中使式(2)成立的最大模糊集 $B^*(y)$的算法为:

$$B^*(y)=\inf_{x\in E_y\cap K_y}\{\alpha\otimes_{G\text{-}\lambda\text{-}R_0}(A^*(x)\otimes_{G\text{-}\lambda\text{-}R_0}R_{G\text{-}\lambda\text{-}R_0}(A(x),B(y)))\}\quad(5)$$

其中 $E_y=\{x\in X|A^*(x)+R_{G\text{-}\lambda\text{-}R_0}(A(x),B(y))>1\}$,$K_y=\{x\in X|\alpha+A^*(x)\wedge R_{G\text{-}\lambda\text{-}R_0}(A(x),B(y))\geqslant1\}$。

证明 首先,证明对 $\forall x\in X$,式(5)成立。事实上,一方面

$$(A(x)\rightarrow_{G\text{-}\lambda\text{-}R_0}B(y))\rightarrow_{G\text{-}\lambda\text{-}R_0}(A^*(x)\rightarrow_{G\text{-}\lambda\text{-}R_0}B^*(y))\leqslant(A(x)\rightarrow_{G\text{-}\lambda\text{-}R_0}B(y))\rightarrow_{G\text{-}\lambda\text{-}R_0}(A^*(x)\rightarrow_{G\text{-}\lambda\text{-}R_0}(\alpha\otimes_{G\text{-}\lambda\text{-}R_0}(A^*(x)\otimes_{G\text{-}\lambda\text{-}R_0}R_{G\text{-}\lambda\text{-}R_0}(A(x),B(y)))))=(A(x)\rightarrow_{G\text{-}\lambda\text{-}R_0}B(y))\rightarrow_{G\text{-}\lambda\text{-}R_0}(A^*(x)\rightarrow_{G\text{-}\lambda\text{-}R_0}(A^*(x)\otimes_{G\text{-}\lambda\text{-}R_0}(\alpha\otimes_{G\text{-}\lambda\text{-}R_0}R_{G\text{-}\lambda\text{-}R_0}(A(x),B(y)))))\leqslant(A(x)\rightarrow_{G\text{-}\lambda\text{-}R_0}B(y))\rightarrow_{G\text{-}\lambda\text{-}R_0}(\alpha\otimes_{G\text{-}\lambda\text{-}R_0}R_{G\text{-}\lambda\text{-}R_0}(A(x),B(y)))\leqslant\alpha$$

即 $B^*(y)$是式(2)的解。

另一方面,设 $D(y)\in F(Y)$,且存在 $y_0\in Y$ 使得 $D(y_0)>B^*(y_0)$,则

$$D(y_0)>\alpha\otimes_{G\text{-}\lambda\text{-}R_0}(A^*(x)\otimes_{G\text{-}\lambda\text{-}R_0}R_{G\text{-}\lambda\text{-}R_0}(A(x),B(y)))$$

又由于

$$(A(x)\to_{G\text{-}\lambda\text{-}R_0}B(y_0))\to_{G\text{-}\lambda\text{-}R_0}(A^*(x)\to_{G\text{-}\lambda\text{-}R_0}D(y_0))=$$

$$\inf\{c|c\otimes_{G\text{-}\lambda\text{-}R_0}R_{G\text{-}\lambda\text{-}R_0}(A(x),B(y_0))\geqslant A^*(x)\to_{G\text{-}\lambda\text{-}R_0}D(y_0)\}=$$

$$\inf\{c|A^*(x)\otimes_{G\text{-}\lambda\text{-}R_0}(c\otimes_{G\text{-}\lambda\text{-}R_0}R_{G\text{-}\lambda\text{-}R_0}(A(x),B(y_0)))\geqslant D(y_0)\}=$$

$$\inf\{c|(c\otimes_{G\text{-}\lambda\text{-}R_0}R_{G\text{-}\lambda\text{-}R_0}(A(x),B(y_0)))\otimes_{G\text{-}\lambda\text{-}R_0}A^*(x)\geqslant D(y_0)\}$$

所以 $c\otimes_{G\text{-}\lambda\text{-}R_0}R_{G\text{-}\lambda\text{-}R_0}(A(x),B(y_0))>\alpha\otimes_{G\text{-}\lambda\text{-}R_0}R_{G\text{-}\lambda\text{-}R_0}(A(x),B(y))$。即得 $c>\alpha$。从而$(A(x)\to_{G\text{-}\lambda\text{-}R_0}B(y_0))\to_{G\text{-}\lambda\text{-}R_0}(A^*(x)\to_{G\text{-}\lambda\text{-}R_0}D(y_0))>\alpha$。这就证明了对$\forall x\in X$，$B^*(y)$是使式(2)成立的最大模糊集。

此外，容易验证：当 $x\in(E_y\cap K_y)^c$ 时，$B^*(y)=0$。所以

$$B^*(y)=\inf_{x\in E_y\cap K_y}\{\alpha\otimes_{G\text{-}\lambda\text{-}R_0}(A^*(x)\otimes_{G\text{-}\lambda\text{-}R_0}R_{G\text{-}\lambda\text{-}R_0}(A(x),B(y)))\}\vee$$

$$\inf_{x\in(E_y\cap K_y)^c}\{\alpha\otimes_{G\text{-}\lambda\text{-}R_0}(A^*(x)\otimes_{G\text{-}\lambda\text{-}R_0}R_{G\text{-}\lambda\text{-}R_0}(A(x),B(y)))\}=$$

$$\inf_{x\in E_y\cap K_y}\{\alpha\otimes_{G\text{-}\lambda\text{-}R_0}(A^*(x)\otimes_{G\text{-}\lambda\text{-}R_0}R_{G\text{-}\lambda\text{-}R_0}(A(x),B(y)))\}\vee 0=$$

$$\inf_{x\in E_y\cap K_y}\{\alpha\otimes_{G\text{-}\lambda\text{-}R_0}(A^*(x)\otimes_{G\text{-}\lambda\text{-}R_0}R_{G\text{-}\lambda\text{-}R_0}(A(x),B(y)))\}$$

即为式(5)。

注 4　仅对 α-三 IFMP 算法进行了详细讨论，α-三 IFMT 算法有类似的方法。

4　结束语

采用了具有良好性质的正则蕴涵算子 G-λ-R_0，主要分析了三 I 方法的 G-λ-R_0型约束度理论，给出了一般化的 α-三 I 方法的 FMP 公式。所得结果进一步完善和丰富了三 I 方法的理论，进而可望为实现新型模糊控制器的某些性能指标提供必要的理论依据。

参考文献：

[1] Klement E P，Navara M.Propositional fuzzy logics based on Frank t-norms：A comparison[M]//Dubois D.Fuzzy Sets，Logics and Reasoning about Knowledge.[S.l.]：Kluwer Academic Publishers，1999.

[2] 王国俊.模糊推理的全蕴涵三 I 算法[J].中国科学：E 辑，1999，29(1)：43-53.

[3] Whale T.Parameterized R-implications[J].Fuzzy Sets and Systems，2003，134：231-281.

[4] 吴洪博.修正的 Kleene 系统中的广义重言式理论[J].中国科学：E 辑，2002，32(2).

[5] 张森，李成允，张兴芳.正则蕴涵算子族 G-λ-R_0 及其三 I 支持算法[J].计算机工程与应用，2009，45(22)：29-31.

[6] 王琼.基于剩余蕴涵的模糊三 I 方法的支持度[J].西南交通大学学报，2004(4).

[7] 袁和军，李骏.推广形式下的三 I 算法[J].陕西师范大学学报，2002(2).

[8] 王国俊.非经典数理逻辑与近似推理[M].北京：科学出版社，2000.

[9] 吴望名.参数 Kleene 系统中的广义重言式[J].模糊系统与数学，2000，14(1)：1-7.

[10] 王国俊.模糊推理的一个新方法[J].模糊系统与数学，1999，13(3)：1-9.

[11] 王国俊.一种新型的三 I 算法及其逻辑基础[J].自然科学进展，2003，13(6).

(上接 28 页)

表 2　计算量比较

方案	计算操作		
	对运算	点乘运算	指数运算
WCD-1	1	0	4
WCD-2	1	0	5
WCX	1	0	6
新方案	1	0	5*

注：$T_{A3}=g_T^{r_A}$ 可以预计算，从而在线指数运算次数可以减少到 5。

6　结束语

基于身份的认证密钥协商协议应尽量满足已知的安全属性。对三个基于 Gentry 加密方案的认证密钥协商协议进行了方案安全分析，指出他们都不满足已知会话相关临时秘密信息安全性的要求。通过改进，给出一个完善安全性的基于身份的认证密钥协商协议。分析表明新方案满足目前已知的几乎所有的认证密钥协商协议安全属性。

参考文献：

[1] Blake-wilson S，Johnson D，Menezes A.Key agreement protocols and their security analysis[C]//LNCS 1355：Proc of the 6th IMA International Conference on Cryptography and Coding.Berlin：Springer-Verlag，1997：30-45.

[2] Shamir A.Identity-based cryptosystems and signature schemes[C]//LNCS 196：Proc of Advances in Cryptology-Crypto 1984.Berlin：Springer-Verlag，1984：47-53.

[3] Shim K.Efficient ID-based authenticated key agreement protocol based on the Weil pairing[J].IEE Electronics Letters，2003，39(8)：653-654.

[4] Sun H，Hsieh B.Security analysis of Shim's authenticated key agreement protocols from pairings[EB/OL].http://eprint.iacr.org/2003/113.

[5] Mccullagh N，Barreto P.A new two party identity-based authenticated key agreement[C]//LNCS 3376：Proc of the 2005 RSA Conference.Berlin：Springer-Verlag，2005：262-274.

[6] Xie G H.Cryptanalysis of the Noel McCullagh and Paulo S.L.M.Barreto's two party identity-based key agreement[EB/OL].http://eprint.iacr.org/2004/343.

[7] Chen L，Kudla C.Identity based authenticated key agreement protocols from pairing[C]//Proc of the 16th IEEE Computer Security Foundations Workshop.Pacific，New York：IEEE Computer Society，2003：219-213.

[8] Bellare M，Rogaway P.Random oracles are practical：a paradigm for designing efficient protocols[C]//Proc of the First ACM Conference on Computer and Communication Security.New York：ACM Press，1993：62-73.

[9] Gentry C.Practical identity-based encryption without random oracles [C]//LNCS 4004：Proc of Advances in Cryptology Eurocrypt 2006.Berlin：Springer-Verlag，2006：445-464.

[10] 王圣宝，曹珍富，董晓蕾.标准模型下可证安全的身份基认证密钥协商协议[J].计算机学报，2007，30(10)：1842-1854.

[11] 汪小芬，陈原，肖国镇.基于身份的认证密钥协商协议的安全分析与改进[J].通信学报，2008，29(12)：16-21.

[12] Canetti R，Krawczyk H.Analysis of key exchange protocols and their use for building secure channels[C]//LNCS 2045：Proc of Advances in Cryptology-Eurocrypt 2001.Berlin：Springer-Verlag，2001：453-474.