doi:10.3969/j.issn.1000-436x.2013.09.017

应用规律下的 BLP 模型密级赋值方法

董婵[1]，范修斌[2]，李有文[1]，王建荣[3]
（1. 中北大学 理学院，山西 太原 030051；2. 中国科学院 软件研究所，北京 100080；
3. 北京科技大学 计算机与通信工程学院，北京 100083）

摘 要：根据信息系统的主客体访问属性规律，给出了一种可行的 BLP 模型密级赋值方法，提出了 2 个归并条件。继而给出了归并后的 BLP 模型下的主客体密级赋值的数学模型。证明了当条件解是非常值赋值解时，其扩张还原解不一定是全局解的结果，但由该解可以得到全局解的近似条件修改赋值解。利用近似条件修改赋值解，给出了某国家级信息系统 BLP 模型的密级具体赋值，解决了应用中的实际困难问题。
关键词：信息安全；BLP 模型；常值赋值；条件修改赋值；全局解；条件解
中图分类号：TP309 **文献标识码**：A **文章编号**：1000-436X(2013)09-0142-08

Secret level valuation method of BLP model based on some application properties

DONG Chan[1], FAN Xiu-bin[2], LI You-wen[1], WANG Jian-rong[3]
(1. School of Science, North University of China, Taiyuan 030051, China;
2. Institute of Software, Chinese Academy of Sciences, Beijing 100080, China;
3. School of Computer and Communication Engineering, University of Sciences and Technology Beijing, Beijing 100083, China)

Abstract: According to the access attribute properties between subjects and objects in the information system, a viable method of the BLP model secret level valuation was given, and two merging conditions were put forward. The mathematical model of subject-object secret level valuation under BLP model was established on the two merging conditions. When the condition solution was not the constant one, its expansion solution being not sure the global one was proved, but the approximate condition modification valuation solution could be obtained from it. Using the above results, one difficult problem from one national information system about the BLP model secret level valuation was solved.
Key words: information security; BLP model; constant valuation; condition modification valuation; global solution; condition solution

1 引言

访问控制通常用于系统管理员控制用户对服务器、目录、文件等网络资源的访问。它主要防止非法的主体访问受保护的网络资源；防止合法的用户对受保护的网络资源进行非授权的访问。通常实现访问控制的技术包括：自主访问控制、强制访问控制、基于角色的访问控制、基于客体的强制访问控制、基于任务的访问控制等。其中强制访问控制主要依据 BLP 模型或 Biba 模型来实现的。BLP 模型是在 1973 年由 D．Bell 和 J．LaPadula 提出并加以完善的[1~3]，它根据美国军方的安全政策设计，解决的本质问题是对具有密级划分信息的访问控制，是第一个比较完整地利用形式化方法对系统安全进行严格证明的数学模型，被广泛应用于描述计算机系统的安全问题。

BLP 模型从“访问控制”的角度研究如何既保证主体能有效地访问客体，又使得系统的安全性不致遭

收稿日期：2012-12-20；修回日期：2013-05-20
基金项目：保障技术重点实验室开放基金资助项目(KG-11-03)；国家自然科学基金资助项目(60833008, 60902024)
Foundation Items: The Opening Project of Key Laboratory of Guarantee Technology(KG-11-03); The National Natural Science Foundation of China (60833008, 60902024)

到破坏的性质和规则，是一种在计算机系统内实施多级安全策略的访问控制模型，通过制定主体对客体的访问规则和操作权限来保证系统的安全性。

BLP 模型有如下两大特点。

1) 简单安全特性（不向上读，即下读）：一个主体只能读一个低级别或相同安全级别的对象。

2) *特性（不向下写，即上写）：一个主体只能写一个高级别的或相同安全级别的对象。

从本质上来说，BLP 模型是一个状态机模型，它形式化地定义了系统、系统状态以及系统状态间的转换规则；定义了安全的概念，并制定了一组安全特性。以此对系统状态和状态转换规则进行限制和约束，使得对于一个系统，如果它的初始状态是安全的，并且所经过的一系列的规则都保持安全特性，那么可以证明该系统是安全的。当然该模型还要注意隐蔽信道的防范。

在实际工作中，人们进一步给出了各种扩展的 BLP 模型与分析[5~16]。BLP 模型以及扩展的 BLP 模型对进程或数据提供了多级机密性保护。在对隐蔽信道进行相应的防范后，基于 BLP 模型以及扩展的 BLP 模型都得到了相应的实际应用。

不论 BLP 模型还是扩展的 BLP 模型，都需要根据实际业务需求，对所有主客体进行赋值，为便于讨论仅对 BLP 模型的赋值进行分析。BLP 模型中主客体赋值结构由(l,c)组成，称之为安全级，其中 l 是密级，c 是范畴（部门或类别），即 $l\in L=\{l_0,l_1,\perp,l_{d-1}\},c\subset C$。一般情况下，主客体的密级集合 $L=\{0,1,2,3\}$，其中，0 表示可公开信息，1 表示秘密信息，2 表示机密信息，3 表示绝密信息。密级满足全序关系。所谓范畴是指信息系统中主客体所在的部门或类别等形成的集合，是所有部门或类别集合 C 的子集。范畴作为子集根据包含关系构成偏序关系[2]。信息系统中的任何主客体都对应着 C 的一个子集，即某个范畴。

本文主要研究根据实际需求对主体 s 或客体 o 的密级进行赋值的方法，并对其进行了分析。本文的研究方法同样可以应用到对改进的 BLP 模型以及对 Biba 模型[4]的赋值研究。

文献[17]指出了 BLP 模型的安全级赋值是 NP 完全问题，也就是说该类问题是困难的，该文也给出了基于层次聚类和遗传算法的近似最优化挖掘算法。本文在一定的实际应用规律下，给出了一种可行的赋值方法。本文将 BLP 模型严格化为 4 个公理，给出了常值赋值、条件修改赋值等概念。根据信息系统的主客体访问属性规律，给出了 2 个归并条件，继而给出了归并后的 BLP 模型下的主客体密级赋值的数学模型；上述 2 个归并条件，特别在代理信息系统中是很常见的。在此基础上，给出了全局解、条件解、扩张还原解以及近似条件修改赋值解的概念，得到了全局解为常值赋值解的充要条件是条件解为常值赋值解；证明了条件解是非常值赋值解时，其扩张还原解不一定是全局解，但由该解可以得到全局解的近似条件修改赋值解。本文的研究结果在某国家级大型信息系统 BLP 模型的密级赋值中得到了实际应用，解决了应用中的困难问题。

2　问题模型的建立

设信息系统参数如下。

所有主体的集合：$S=\{s_0,s_1,\perp,s_{n-1}\}$；

所有客体集合：$O=\{o_0,o_1,\perp,o_{m-1}\}$；

密级集合：$L=\{l_0,l_1,\perp,l_{d-1}\}$；

范畴集合：2^C，即集合 C 的幂集，所谓某集合的幂集即该集合的所有子集构成的集合。

主体访问客体的集合为：$A=\{N,R,W,RW\}$，其中，N 表示主体对客体不能进行读写操作，R 表示主体对客体仅可以进行读操作，W 表示主体对客体仅可以进行写操作，RW 表示主体对客体可进行读写操作。

易知，安全级的集合 $L\times 2^C$ 仍然满足偏序关系。不妨设 $t_s=(l_s,c_s),t_o=(l_o,c_o)$，$t_s,t_o\in L\times 2^C$。

当 $l_s\geq l_o,c_s\supseteq c_o$ 时，但 $l_s=l_o,c_s=c_o$ 不同时成立，则 $t_s>t_o$，即 $(l_s,c_s)>(l_o,c_o)$。当 $l_s\leq l_o,c_s\subseteq c_o$ 时，但 $l_s=l_o,c_s=c_o$ 不同时成立，则 $t_s>t_o$，即 $(l_s,c_s)>(l_o,c_o)$。当 $l_s=l_o,c_s=c_o$ 时，则 $t_s=t_o$，即 $(l_s,c_s)=(l_o,c_o)$。否则，t_s,t_o 之间没有序关系，简记为 $t_s\text{H}t_o$。

根据 BLP 模型[1~3]，严格细化为 4 个公理如下。

公理 1　若主体 $s\in S$ 的安全级为 (l_s,c_s)，客体 $o\in O$ 的安全级为 (l_o,c_o)，当 $(l_s,c_s)>(l_o,c_o)$ 时，则主体 s 对客体 o 可以进行读操作。记为 $A(s,o)=(1,0)=R$。

公理 2　若主体 $s\in S$ 的安全级为 (l_s,c_s)，客体 $o\in O$ 的安全级为 (l_o,c_o)，当 $(l_s,c_s)<(l_o,c_o)$ 时，则主体 s 对客体 o 可以进行写操作。记为 $A(s,o)=(0,1)=W$。

公理 3 若主体 $s\in S$ 的安全级为 (l_s,c_s)，客体 $o\in O$ 的安全级为 (l_o,c_o)，当 $(l_s,c_s)=(l_o,c_o)$ 时，当且仅当 $A(s,o)=(1,1)=RW$。

公理 4 若主体 $s\in S$ 的安全级为 (l_s,c_s)，客体 $o\in O$ 的安全级为 (l_o,c_o)，当 $(l_s,c_s)\#(l_o,c_o)$ 时，当且仅当 $A(s,o)=(0,0)=N$。

根据信息系统的实际需求，一般可先给出一个参数集合

$$A(S,O)=\{A(s,o)\mid \forall s\in S,o\in O\}$$

下面的研究问题是如何对信息系统中的主客体按照 BLP 模型公理 1~公理 4 进行赋值以满足实际需求的访问属性。

为了便于讨论，对 $\{(s,o)\mid s\in S,o\in O,A(s,o)=(0,0)=N\}$ 中 s,o 的范畴进行无序设置即可。对下述集合 $\{(s,o)\mid A(s,o)=R\}$，$\{(s,o)\mid A(s,o)=W\}$，$\{(s,o)\mid A(s,o)=RW\}$ 中的情况，不失一般性，认为主客体之间的范畴参数通过设置是满足偏序关系的，仅考察主客体的密级赋值即可。

在上述假设下，给出函数 $T(s,o)$

$$T(s,o)=\begin{cases}1,\ \text{如果}\ A(s,o)=R, & l_s>l_o\\ 0,\ \text{如果}\ A(s,o)=R, & l_s=l_o\\ 0,\ \text{如果}\ A(s,o)=R, & l_s<l_o\\ 0,\ \text{如果}\ A(s,o)=W, & l_s>l_o\\ 0,\ \text{如果}\ A(s,o)=W, & l_s=l_o\\ 1,\ \text{如果}\ A(s,o)=W, & l_s<l_o\\ 0,\ \text{如果}\ A(s,o)=RW, & l_s>l_o\\ 1,\ \text{如果}\ A(s,o)=RW, & l_s=l_o\\ 0,\ \text{如果}\ A(s,o)=RW, & l_s<l_o\end{cases}$$

记：$l_S=\{(l_{s_0},l_{s_1},\cdots,l_{s_{n-1}})\mid l_{s_i}\in L,i=0,\cdots,n-1\}$

$$l_O=\{(l_{o_0},l_{o_1},\cdots,l_{o_{n-1}})\mid l_{o_j}\in L,j=0,\cdots,m-1\}$$

称 $l_S\times l_O$ 为信息系统的密级赋值空间，即

$$l_S\times l_O=\{((l_{s_0},\cdots,l_{s_{n-1}}),(l_{o_0},\cdots,l_{o_{n-1}}))\mid l_{s_i}\in L,i=0,\cdots,n-1,\ l_{o_j}\in L,j=0,\cdots,m-1\}$$

赋值空间 $l_S\times l_O$ 中的每个具体元素称为一个具体赋值，简称赋值。

问题的数学模型为

$$H=\max_{l_S\times l_O}\sum_{s\in S,o\in O}T(s,o)\tag{1}$$

即求使 $\sum_{s\in S,o\in O}T(s,o)$ 达到最大的赋值，称之为问题（1）。

定义 1 问题（1）的解称为全局最大赋值解，或简称全局解。

该模型等价于文献[17]中的模型。由文献[17]可知，该问题为 NP 完全问题，也就是说该类问题的求解一般是困难的。

定义 2 若

$$\max_{l_S\times l_O}\sum_{s\in S,o\in O}T(s,o)=\#(S\times O)-\#\{(s,o)\mid A(s,o)=N\},$$

则存在主客体的固定赋值满足实际需求，这样的赋值叫做主客体密级常值赋值，简称常值赋值。否则，称之为非常值赋值。在非常值赋值的情况下可以通过一定条件下的赋值修改，借以满足实际需求的访问属性，称之为条件修改赋值。

注释 设 *Set* 为某一有限集合，*#Set* 表示集合中元素的个数。

定理 1 基于枚举方法，问题（1）的求解计算复杂度为 $(mn)d^{m+n}$。

证明 对于每个主客体，其密级赋值有 d 种可能，所以主客体的总枚举量为 d^{m+n}。又因为每次枚举所统计的表量为 mn，所以其计算复杂度为 $(mn)d^{m+n}$。

一般情况下问题（1）的求解虽然是困难的，但是信息系统的主客体之间访问属性存在着一定的规律，可以根据这些规律归并，给出应用规律下的问题（1）的近似解。

3 一定条件下的问题的求解

在实际信息系统中，可能存在着一类主体对同类客体具有相同的访问属性或者存在一类客体对同类主体有着相同的被访问属性，分别定义如下。

条件 1 一类主体对同类客体具有相同的访问属性。

条件 2 一类客体对同类主体具有相同的被访问属性。

在信息系统中形成上述 2 个条件是很普遍的，原因如下。

在信息系统中，访问属性的集合为 $\{r,w,e,a,c\}$，其中，r 为只读，w 为读写，e 为运行，a 为添加，c 为控制。该集合中仅有 5 个元素。针对某客体，

所有主体的访问属性最多分为 5 类。再由于信息系统中的若干客体在应用上功能相似，例如各种日志类等；若干主体的需求相似，例如查询服务等，所以信息系统中普遍存在着上述 2 个条件。因此研究 2 个条件下的 BLP 模型安全级赋值具有普遍意义和实际价值。

在条件 1 下，可以把这类主体定义为等价主体；在条件 2 下，可以把这类客体定义为等价客体。可以把等价主体归并简化为一个主体，把等价客体归并简化为一个客体。

例如，某信息系统的实际需求访问属性如表 1 所示。

在实际需求表 1 下，根据规律 1 和 2，归并主客体。

在归并后下，把对表 1 的问题求解转化为对表 2 的问题求解。

设归并转化后的主体集合为 S'，转化后的客体集合为 O'。例如上例中的转化后的主客体集合分别为

$$S'=\{s_0,s_3,s_7\},O'=\{o_0,o_1,o_{12},o_{16},o_{23},o_{27},o_{32},o_{38}\}$$

问题 1 的数学模型转化为如下

$$H'=\max_{l_{S'}\times l_{O'}}\sum_{s\in S',o\in O'}T(s,o) \tag{2}$$

即求使 $\sum_{s\in S',o\in O'}T(s,o)$ 达到最大的赋值，称之为问题（2）。

设 $\#S'=n',\#O'=m'$，则由定理 1 可知问题（2）的枚举计算复杂度为 $(m'n')d^{m'+n'}$。

定义 3　问题（2）的解称为条件最大赋值解，或简称为条件解。

为方便问题讨论并不失一般性，以下令 $L=\{0,1,2,3\}$。

在问题（1）中，变量的个数为 $\#S+\#O$，每个变元的密级取值范围为 $L=\{0,1,2,3\}$，在公理 1~4 的条件下，因其变元量大，具体求全局解的难度还很大。例如表 1 中的变元个数为 $\#S+\#O=10+42=52$，则枚举计算复杂度为 $420\cdot 4^{52}=1.64\times 2^{112}$，求全局解就比较困难。

在条件 1 和 2 下，把问题（1）转化为问题（2）后，问题（2）中，每个变元的密级取值范围仍为 $L=\{0,1,2,3\}$，但是变元量转化为 $\#S'+\#O'$，当 $\#S'+\#O'$ 较小的情况下，是可以具体给出问题（2）的解。

表 1　某信息系统的实际需求访问属性

o	s									
	s_0	s_1	s_2	s_3	s_4	s_5	s_6	s_7	s_8	s_9
o_0	N	N	N	RW	RW	RW	RW	N	N	N
o_1	R	R	R	RW	RW	RW	RW	N	N	N
o_2	R	R	R	RW	RW	RW	RW	N	N	N
o_3	R	R	R	RW	RW	RW	RW	N	N	N
o_4	R	R	R	RW	RW	RW	RW	N	N	N
o_5	R	R	R	RW	RW	RW	RW	N	N	N
o_6	R	R	R	RW	RW	RW	RW	N	N	N
o_7	R	R	R	RW	RW	RW	RW	N	N	N
o_8	R	R	R	RW	RW	RW	RW	N	N	N
o_9	R	R	R	RW	RW	RW	RW	N	N	N
o_{10}	R	R	R	RW	RW	RW	RW	N	N	N
o_{11}	R	R	R	RW	RW	RW	RW	N	N	N
o_{12}	RW	RW	RW	RW	RW	RW	RW	N	N	N
o_{13}	RW	RW	RW	RW	RW	RW	RW	N	N	N
o_{14}	RW	RW	RW	RW	RW	RW	RW	N	N	N
o_{15}	RW	RW	RW	RW	RW	RW	RW	N	N	N
o_{16}	RW	RW	RW	RW	RW	RW	RW	RW	RW	RW
o_{17}	RW	RW	RW	RW	RW	RW	RW	RW	RW	RW
o_{18}	RW	RW	RW	RW	RW	RW	RW	RW	RW	RW
o_{19}	RW	RW	RW	RW	RW	RW	RW	RW	RW	RW
o_{20}	RW	RW	RW	RW	RW	RW	RW	RW	RW	RW
o_{21}	RW	RW	RW	RW	RW	RW	RW	RW	RW	RW
o_{22}	RW	RW	RW	RW	RW	RW	RW	RW	RW	RW
o_{23}	R	R	R	R	R	R	R	RW	RW	RW
o_{24}	R	R	R	R	R	R	R	RW	RW	RW
o_{25}	R	R	R	R	R	R	R	RW	RW	RW
o_{26}	R	R	R	R	R	R	R	RW	RW	RW
o_{27}	N	N	N	R	R	R	R	RW	RW	RW
o_{28}	N	N	N	R	R	R	R	RW	RW	RW
o_{29}	N	N	N	R	R	R	R	RW	RW	RW
o_{30}	N	N	N	R	R	R	R	RW	RW	RW
o_{31}	N	N	N	R	R	R	R	RW	RW	RW
o_{32}	N	N	N	N	N	N	N	R	R	R
o_{33}	N	N	N	N	N	N	N	R	R	R
o_{34}	N	N	N	N	N	N	N	R	R	R
o_{35}	N	N	N	N	N	N	N	R	R	R
o_{36}	N	N	N	N	N	N	N	R	R	R
o_{37}	N	N	N	N	N	N	N	R	R	R
o_{38}	R	R	R	N	N	N	N	R	R	R
o_{39}	R	R	R	N	N	N	N	R	R	R
o_{40}	R	R	R	N	N	N	N	R	R	R
o_{41}	R	R	R	N	N	N	N	R	R	R

例如表 2 中的变元量为 $\#S'+\#O'=3+8=11$，则枚举计算复杂度为 $24\cdot 4^{11}=1.5\times 2^{26}$，这种情况就

可以枚举求解，其求解结果为 $H'=14<16$，即问题（2）不存在常值赋值，其非常值赋值解如下。

表 2 某信息系统的实际需求访问属性归并

o	s		
	s_0	s_3	s_7
o_0	N	RW	N
o_1	R	RW	N
o_{12}	RW	RW	N
o_{16}	RW	RW	RW
o_{23}	R	R	RW
o_{27}	N	R	RW
o_{32}	N	N	R
o_{38}	R	N	R

$l_{s_0}=2,l_{s_3}=2,l_{s_7}=1,l_{o_0}=2,l_{o_1}=0,l_{o_{12}}=2,$
$l_{o_{16}}=2,l_{o_{23}}=1,l_{o_{27}}=1,l_{o_{32}}=0,l_{o_{38}}=0;$
$l_{s_0}=2,l_{s_3}=2,l_{s_7}=1,l_{o_0}=2,l_{o_1}=1,l_{o_{12}}=2,$
$l_{o_{16}}=2,l_{o_{23}}=1,l_{o_{27}}=1,l_{o_{32}}=0,l_{o_{38}}=0;$
$l_{s_0}=2,l_{s_3}=2,l_{s_7}=1,l_{o_0}=2,l_{o_1}=2,l_{o_{12}}=2,$
$l_{o_{16}}=2,l_{o_{23}}=1,l_{o_{27}}=1,l_{o_{32}}=0,l_{o_{38}}=0;$
$l_{s_0}=3,l_{s_3}=3,l_{s_7}=1,l_{o_0}=3,l_{o_1}=0,l_{o_{12}}=3,$
$l_{o_{16}}=3,l_{o_{23}}=1,l_{o_{27}}=1,l_{o_{32}}=0,l_{o_{38}}=0;$
$l_{s_0}=3,l_{s_3}=3,l_{s_7}=1,l_{o_0}=3,l_{o_1}=1,l_{o_{12}}=3,$
$l_{o_{16}}=3,l_{o_{23}}=1,l_{o_{27}}=1,l_{o_{32}}=0,l_{o_{38}}=0;$
$l_{s_0}=3,l_{s_3}=3,l_{s_7}=1,l_{o_0}=3,l_{o_1}=2,l_{o_{12}}=3,$
$l_{o_{16}}=3,l_{o_{23}}=2,l_{o_{27}}=2,l_{o_{32}}=0,l_{o_{38}}=0;$
$l_{s_0}=3,l_{s_3}=3,l_{s_7}=2,l_{o_0}=3,l_{o_1}=0,l_{o_{12}}=3,$
$l_{o_{16}}=3,l_{o_{23}}=2,l_{o_{27}}=2,l_{o_{32}}=0,l_{o_{38}}=1;$
$l_{s_0}=3,l_{s_3}=3,l_{s_7}=2,l_{o_0}=3,l_{o_1}=0,l_{o_{12}}=3,$
$l_{o_{16}}=3,l_{o_{23}}=2,l_{o_{27}}=2,l_{o_{32}}=1,l_{o_{38}}=0;$
$l_{s_0}=3,l_{s_3}=3,l_{s_7}=2,l_{o_0}=3,l_{o_1}=1,l_{o_{12}}=3,$
$l_{o_{16}}=3,l_{o_{23}}=2,l_{o_{27}}=2,l_{o_{32}}=1,l_{o_{38}}=1;$
$l_{s_0}=3,l_{s_3}=3,l_{s_7}=2,l_{o_0}=3,l_{o_1}=2,l_{o_{12}}=3,$
$l_{o_{16}}=3,l_{o_{23}}=2,l_{o_{27}}=2,l_{o_{32}}=0,l_{o_{38}}=0;$
$l_{s_0}=3,l_{s_3}=3,l_{s_7}=2,l_{o_0}=3,l_{o_1}=2,l_{o_{12}}=3,$
$l_{o_{16}}=3,l_{o_{23}}=2,l_{o_{27}}=2,l_{o_{32}}=0,l_{o_{38}}=1;$
$l_{s_0}=3,l_{s_3}=3,l_{s_7}=2,l_{o_0}=3,l_{o_1}=2,l_{o_{12}}=3,$
$l_{o_{16}}=3,l_{o_{23}}=2,l_{o_{27}}=2,l_{o_{32}}=1,l_{o_{38}}=0;$
$l_{s_0}=3,l_{s_3}=3,l_{s_7}=2,l_{o_0}=3,l_{o_1}=2,l_{o_{12}}=3,$
$l_{o_{16}}=3,l_{o_{23}}=2,l_{o_{27}}=2,l_{o_{32}}=1,l_{o_{38}}=1;$
$l_{s_0}=3,l_{s_3}=3,l_{s_7}=2,l_{o_0}=2,l_{o_1}=3,l_{o_{12}}=3,$
$l_{o_{16}}=3,l_{o_{23}}=2,l_{o_{27}}=2,l_{o_{32}}=0,l_{o_{38}}=0;$
$l_{s_0}=3,l_{s_3}=3,l_{s_7}=2,l_{o_0}=2,l_{o_1}=3,l_{o_{12}}=3,$
$l_{o_{16}}=3,l_{o_{23}}=2,l_{o_{27}}=2,l_{o_{32}}=0,l_{o_{38}}=1;$
$l_{s_0}=3,l_{s_3}=3,l_{s_7}=2,l_{o_0}=2,l_{o_1}=3,l_{o_{12}}=3,$
$l_{o_{16}}=3,l_{o_{23}}=2,l_{o_{27}}=2,l_{o_{32}}=1,l_{o_{38}}=0;$
$l_{s_0}=3,l_{s_3}=3,l_{s_7}=2,l_{o_0}=2,l_{o_1}=3,l_{o_{12}}=3,$
$l_{o_{16}}=3,l_{o_{23}}=2,l_{o_{27}}=2,l_{o_{32}}=1,l_{o_{38}}=1$。

于是可以对其进行条件修改赋值。

例如，当 $l_{s_0}=2,l_{s_3}=2,l_{s_7}=1,l_{o_0}=2,l_{o_1}=0,l_{o_{12}}=2,l_{o_{16}}=2,l_{o_{23}}=1,l_{o_{27}}=1,l_{o_{32}}=0,l_{o_{38}}=0$ 时，没有通过的主客体实际需求访问属性的点为：$(s_3,o_1),(s_7,o_{16})$。也就是说

$$A(s_3,o_1)=RW,A(s_7,o_{16})=RW$$

是不满足的，因为 $(l_{s_3},l_{o_1})=(2,0),(l_{s_7},l_{o_{16}})=(1,2)$。

下面给出其条件修改赋值如下：

在访问控制时，先判别主客体的编号，若主客体为 (s_3,o_1)，则令 $A(s_3,o_1)=RW$；若主客体为 (s_7,o_{16})，则令 $A(s_7,o_{16})=RW$。

在条件修改赋值下，实现的 BLP 模型与表 2 的实际需求访问属性相符合。

但是在实际操作时，需要查询条件修改的主客体的编号和访问属性表。实际上问题（2）的解也是针对最小查询的条件修改表量给出的。

问题（2）的解是条件解，需要将其按照条件 1 和 2，还原为问题（1）的解或近似解，为此给出如下定义。

定义 4　由问题 (2) 的解，扩张还原为问题 (1) 的解或近似解，称之为扩张还原解。

为讨论扩张还原解，下面讨论条件解与全局解的关系。

4　全局解与条件解的关系分析

定理 2　问题（1）存在常值赋值解的充要条件为问题（2）存在常值赋值解。

证明　若问题（1）存在常值赋值解，则满足

$$\max_{l_S\times l_O}\sum_{s\in S,o\in O}T(s,o)=\#(S\times O)-\#\{(s,o)\mid A(s,o)=N\}$$

按照条件 1 和条件 2 归并后仍满足

$$\max_{l_{S'}\times l_{O'}}\sum_{s\in S',o\in O'}T(s,o)=\#(S'\times O')-\#\{(s,o)\mid s\in S',o\in O',A(s,o)=N\}$$

于是问题（2）存在常值赋值解。

若问题（2）存在常值赋值解，则满足

$$\max_{l_{S'}\times l_{O'}}\sum_{s\in S',o\in O'}T(s,o)=\#(S'\times O')-\#\{(s,o)\mid s\in S',o\in O',A(s,o)=N\}$$

把按照条件 2 归并的结果扩张还原，满足

$$\max_{l_{S'}\times l_{O}}\sum_{s\in S',o\in O}T(s,o)=\#(S'\times O)-\#\{(s,o)\mid s\in S',o\in O,A(s,o)=N\}$$

在还原按照条件 2 归并结果的基础上，按照条件 1 归并的结果扩张还原，满足

$$\max_{l_S\times l_O}\sum_{s\in S,o\in O}T(s,o)=\#(S\times O)-\#\{(s,o)\mid A(s,o)=N\}$$

于是问题（1）存在常值赋值解。因此定理得证。

由定理 2 知，因为表 2 没有常值赋值解，所以表 1 也没有常值赋值解。

性质 1　对于单一主体，存在常值赋值解满足该主体对所有客体的访问属性。

证明　对于单一主体 s，不妨把所有客体分为 4 类 $\{o_0,o_1,o_2,o_3\}$，那么

$$A(s,0_0)=N,A(s,0_1)=R,A(s,0_2)=W,A(s,0_3)=RW$$

由公理 1~4 可得

$$\max_{l_S\times l_O}\sum_{s\in S,o\in O}T(s,o)=\#(S\times O)-\#\{(s,o)\mid A(s,o)=N\}$$

于是性质成立。

同理，由性质 1 可得：

性质 2　对于单一客体，存在常值赋值满足该客体被所有主体访问的属性。

当 $n>1,m>1$ 时，因为主客体赋值存在相互制约，一般是不存在常值赋值解的。

下面讨论非常值赋值解情况。

为便于讨论，可以根据实际需求访问属性表对等价的主体进行连续排列，对等价的客体进行连续排列，并对主客体根据新的排列进行自然编序。如表 3 所示。

表 3　访问属性

o	s			
	s_0	s_1	s_2	s_3
o_0	RW	RW	R	RW
o_1	RW	R	W	RW
o_2	R	W	RW	R
o_2	RW	R	W	RW

重新排列后如表 4 所示。

不失一般性，下文中讨论的问题都是重新排列后的访问属性表。

定理 3　存在着问题（2）的所有非常值赋值解的扩张还原解都不是问题（1）的非常值赋值解的情况。

证明　不妨设实际需求访问表为表 4。按照条件 1 和条件 2 可归并为表 5。

表 4　重新排列后的访问属性

o	s			
	s_0	s_1	s_2	s_3
o_0	RW	RW	RW	R
o_1	RW	RW	R	W
o_2	RW	RW	R	W
o_3	R	R	W	RW

表 5　访问属性归并

o	s		
	s_0	s_2	s_3
o_0	RW	RW	R
o_1	RW	R	W
o_3	R	W	RW

由公理 3，$l_{s_0}=l_{o_0},l_{s_0}=l_{o_1},l_{s_1}=l_{o_0}$，即 $l_{s_1}=l_{o_1}$ 与 $A(s_1,o_1)=R$ 矛盾，由定理 2 知，表 4 和表 5 都没有常值赋值解。

表 4 的非常值赋值解为

$H=13$，

$l_{s_0}=1,l_{s_1}=1,l_{s_2}=2,l_{s_3}=0,l_{o_0}=1,l_{o_1}=1,l_{o_2}=1,l_{o_3}=0;$

$l_{s_0}=1,l_{s_1}=1,l_{s_2}=3,l_{s_3}=0,l_{o_0}=1,l_{o_1}=1,l_{o_2}=1,l_{o_3}=0;$

$l_{s_0}=2,l_{s_1}=2,l_{s_2}=3,l_{s_3}=0,l_{o_0}=2,l_{o_1}=2,l_{o_2}=2,l_{o_3}=0;$

$l_{s_0}=2,l_{s_1}=2,l_{s_2}=3,l_{s_3}=1,l_{o_0}=2,l_{o_1}=2,l_{o_2}=2,l_{o_3}=1$。

表 5 的非常值赋值解为

$H'=7$，

$l_{s_0}=2,l_{s_2}=0,l_{s_3}=1,l_{o_0}=0,l_{o_1}=2,l_{o_3}=1;$

$l_{s_0}=3,l_{s_2}=0,l_{s_3}=1,l_{o_0}=0,l_{o_1}=3,l_{o_3}=1;$

$l_{s_0}=3,l_{s_2}=0,l_{s_3}=2,l_{o_0}=0,l_{o_1}=3,l_{o_3}=2;$

$l_{s_0}=3,l_{s_2}=1,l_{s_3}=2,l_{o_0}=1,l_{o_1}=3,l_{o_3}=2$。

由于表 4 和表 5 的非常值赋值解中只有 $l_{s_0}=2$ 是两者都有的，表 5 的非常值赋值解中当 $l_{s_0}=2$ 时，$l_{s_2}=0$，但是表 4 非常值赋值解中，$l_{s_2}=3$，故定理成立。

由定理 3 可知，问题（2）的非常值赋值解，其扩张还原解不一定是问题（1）非常值赋值解，但可以认为是问题（1）较优的解。

定义 5 在问题（2）的非常值赋值解的扩张还原解基础上，通过条件修改给出的满足实际需求访问属性问题（1）的解，称为近似条件修改赋值解。

例如，根据表 2 的解，可以给出表 1 的近似条件修改赋值解如下

在 $l_{s_0}=2,l_{s_3}=2,l_{s_7}=1,l_{o_0}=2,l_{o_1}=0,l_{o_{12}}=2,l_{o_{16}}=2,\ l_{o_{23}}=1,l_{o_{27}}=1,l_{o_{32}}=0,l_{o_{38}}=0$ 下，令

$$\begin{cases} A(s_i,o_j)=RW, i=3,4,5,6,\ j=1,2,\cdots,11 \\ A(s_i,o_j)=RW, i=7,8,9,\ j=16,17,\cdots,22 \end{cases}$$

其他的主客体访问遵循公理 1~4。

表 1 是某实际信息系统的访问属性表，上述给出了其赋值，并得到实际应用。

在表 1 的近似条件修改赋值解下，不符合 BLP 模型的点数为 $4\times11+3\times7=65$，此数量比 $n\times m=10\times42=420$ 小很多。

还可以从表 2 的 23 个解中求出其所有的扩张还原解，继而给出所有的近似条件修改赋值解。在实际工作中可以使用最小的修改解。

由表 1 的近似条件修改赋值解，易得如下定理。

定理 4 根据问题（2）的条件解得到的近似条件修改赋值解中修改的单点还原的结果，行列具有顺序性，访问属性具有一致性。

证明 根据实际需求访问属性表重新排列的结果，问题（2）中修改的单点按行列是顺序拉开的，拉开的点的访问属性是修改的单点访问属性的一致派生，故定理得证。

由定理 4 可知，在问题（1）的近似条件修改赋值解判别条件中，修改点的判别简单，属性统一。

5 结束语

本文得到了 BLP 赋值的全局解为常值赋值解的充要条件是条件解为常值赋值解；证明了条件解是非常值赋值解时，其扩张还原解不一定是全局解，但由该解可以得到全局解的近似条件修改赋值解。利用近似条件修改赋值解，给出了某实际信息系统的 BLP 模型密级赋值方法，解决了应用中的实际问题。在以后的工作中，可以利用快速数论变换[18]来进一步研究问题（2）的计算复杂度。

参考文献：

[1] BELL D E, LAPADULA L J, Secure Computer Systems: Unified Exposition and Multics Interpretation[R]. Bedford, MA: The MITRE Corporation, 1976.

[2] BELL DE, LAPADULA L J, Secure Computer Systems: Mathematical Foundations[R]. Bedford, MA: Electronic Systems Division, Air Force System Command Corporation, Hanscom AFB,1973.

[3] BELL DE, LAPADULA L J, Secure Computer Systems: a Mathematical Model[R]. Bedford, MA: Electronic Systems Division, Air Force System Command Corporation, Hanscom AFB,1973.

[4] BIBA K J. Integrity Considerations for Secure Computer Systems[R]. Bedford, MA: USAF Electronic Systems Division, Hanscom AFB,1977.

[5] BRANSTAD D. Data categorization and labeling (executive summary)[A]. Proceedings of the 13th National Computer Security Conference[C]. Washington: NIST Press, USA, 1990.32-33.

[6] Department of Defense Computer Security Center. Department of Defense Trusted Computer System Evaluation Criteria[S]. Fort George G. Meade, MD 20755,1983.

[7] GLIGOR V D, BURCH E L, CHANDERSEKARAN C S. On the design and the implementation of secure Xenix workstation[A]. Proceedings of the 1986 IEEE Symposium on Security and Privacy[C]. IEEE Computer Society,1986.102-117.

[8] LANDWEHR CE, HEITMEYER CL, MCLEAN J. A security model for military message systems[J]. ACM Transactions on Computer Systems, 1984, 9(3):198-222.

[9] MCILROY M D, REEDS J A. Multilevel security in the UNIX tradition[J]. Software Practice and Experience,1992, 22(8):673-694.

[10] 费稼轩,张涛,林为民等.基于动态可信度量的敏感信息安全控制模型[J].计算机技术与发展,2012, 22(5):237-241.
FEI J X,ZHANG T,LIN W M, *et al*. Secure control model of sensitive information based on dynamic trust measurement[J]. Computer Technology and Development,2012, 22(5):237-241.

[11] 石文昌,孙玉芳,梁洪亮.经典 BLP 安全公理的一种适应性标记实施方法及其正确性[J].计算机研究与发展,2001,38(11):1366-1372.
SHI W C, SUN Y F, LIANG H L. An adaptable labeling enforcement approach and its correctness for the classical BLP security axioms[J]. Computer Research and Development, 2001, 38(11):1366-1372.

[12] 梁洪亮,孙玉芳,赵庆松.一个安全标记公共框架的设计与实现[J].软件学报,2003, 14(3):547-552.
LIANG H L, SUN Y F, ZHAO Q S. Design and implementation of a security label common framework[J]. Journal of Software, 2003, 14(3): 547-552.

[13] 李益发,沈昌祥.一种新的操作系统安全模型[J].中国科学 E 辑,2006,36(4):37-356.
LI Y F, SHEN C X. A new kind of operating system security model[J]. Science in China Ser E, 2006,36(4):37-356.

[14] 马新强,黄羿,李丹宁.基于扩充敏感标记的格理论模型研究[J].计算机工程,2009,35(21):171-173.
MA X Q, HUANG Y, LI D N. Research on lattice theoretical model based on extended sensitivity label[J].Computer Engineering,2009, 35(21):171-173.

[15] 刘彦明,董庆宽,李小平.BLP 模型的完整性增强研究[J].通信学报,2010,31(2):100-106.
LIU Y M, DONG Q K, LI X P. Study on enhancing integrity for BLP model[J]. Journal on Communications,2010,31(2):100-106.

[16] 池亚平,樊结,程代伟.基于可信等级的 BLP 改进模型[J].计算机工程,2012,38(8):117-119.
CHI Y P,FAN J,CHENG D W. Improved BLP model based on trusted level[J].Computer Engineering, 2012,38(8):117-119.

[17] 杨智,金舒原,段洣毅等.多级安全中敏感标记的最优化挖掘[J].软件学报,2011,22(5):1020-1030.
YANG Z,JIN S Y,DUAN M Y, *et al*. Optimal mining on security labels in multilevel security system[J]. Journal of Software, 2011,22(5): 1020-1030.

[18] 孙琦,郑德勋,沈仲琦.快速数论变换[M].北京:科学出版社,1980.
SUN Q, ZHENG D X, SHEN Z Q. Fast Number Theory Transform[M]. Beijing: Science Press,1980.

作者简介：

董婵（1989-），女，山西芮城人，中北大学硕士生，主要研究方向为最优化方法及其应用。

范修斌（1966-），男，山东新泰人，中国科学院研究员，主要研究方向为数学、密码学、信息安全。

李有文[通信作者]（1967-），男，山西盂县人，中北大学副教授，主要研究方向为最优化方法及其应用。E-mail: youli@huc.edu.cn。

王建荣（1986-），男，山西吕梁人，北京科技大学博士生，主要研究方向为通信与信息系统。