基于角色限制条件的用户-角色指派研究

叶春晓[1,2] 符云清[3] 吴中福[1]

(重庆大学计算机学院 重庆 400044)[1] (重庆大学应用技术学院 重庆 400030)[2]

(重庆大学网络教育学院 重庆 400044)[3]

摘 要 URA97和URA02作为两个主要的用户-角色指派模型,得到广泛的应用。但这两个模型的指派先决条件较弱,不能满足一些对用户限制较强情况下的用户角色指派。本文认为同一角色下的不同用户之间存在差异,用户在指派某角色时除了常见的约束外,还要受到其他限制。提出了角色和用户属性概念,定义了角色限制条件角色资格条件,改进了指派先决条件,实现了指派先决条件的统一和更严格的用户角色指派限制。对RBAC96模型做了相应的修改。

关键词 访问控制,RBAC,用户角色指派,角色限制条件,角色资格条件

Research on User-Role Assignment Based on Role Restrictive Conditions

YE Chun-Xiao[1,2] FU Yun-Qing[3] WU Zhong-Fu[1]

(Computer School, Chongqing University, Chongqing 400044)[1]

(College of Applied Science and Technology, Chongqing University, Chongqing 400030)[2]

(College of Network Education, Chongqing University, Chongqing 400044)[3]

Abstract URA97 and URA02 as two major user-role assignment models, have gained wide application. But they are not suit for some more restrictive user-role assignment circumstance, due to weakness of their prerequisite conditions. This paper realizes that there exist differences among different users under the same role and some restrictions other than common constraints when assigning user to role. The paper proposes the idea of role and user attribute, defining role restrictive condition and role qualification condition, expanding the prerequisite condition of user-role assignment, unifying user-role prerequisite condition and a more strict restriction in user-role assignment. Make a corresponding modification on RBAC96 model.

Keywords Access control, RBAC, User-role assignment, Role restrictive condition, Role qualification condition

1 引言

访问控制作为信息系统的安全技术,获得了极大的发展。而基于角色的访问控制技术RBAC,作为信息安全领域的一种新技术,正不断受到重视。其中具有代表性的模型为Sandhu提出的RBAC96模型[1],该模型一经提出即受到瞩目,在此基础上人们又提出了许多补充和改进模型。相关的标准也在研究发布中[2]。

作为RBAC96的重要组成部分ARBAC97[3]由三部分构成,即URA97[4],PRA97,RRA97[5]。通过该三个模型,完成了对用户-角色指派,角色-权限指派和角色-角色指派的管理,使得整个管理过程分散为多个系统管理角色来完成,减轻了系统管理人员的负担。

在实际管理过程中,由于系统用户个数相对较多,一个用户可能会指派多个角色,因而用户-角色的指派过程相对繁琐和复杂。URA97提出了角色范围和指派先决条件的概念,用以减轻该过程的复杂程度。但URA97本身还存在一些问题,主要是指派先决条件中指派候选用户的选择与系统角色继承关系有关。作为对其的改进,URA02[6]保留了URA97的主要特点,重新定义了指派先决条件,将组织结构引入指派候选用户的选择过程中,避免URA97中用户角色指派与角色继承关系紧密相关的问题。

URA97和URA02模型的指派先决条件较弱,不能满足诸如CWSP等情况[7]。除此之外,在进行用户-角色指派时,对用户是否能够指派该角色的限制较弱。URA97中,指派先决条件与用户已经具有的角色有关。URA02中,指派先决条件与用户所在的组织结构有关,用户只要满足该指派先决条件就可完成指派。虽然指派过程是否成功还必须满足一些约束条件,但URA97和URA02中的指派约束条件更多地是考虑诸如SOD、角色基数、角色互斥[1]等方面,未考虑一些十分重要的因素如角色限制条件。角色限制条件的主要目的是对用户是否能够被指派角色的资格限制。本文的主要目的即是在用户-角色的指派过程中引入角色限制条件和角色资格条件概念,对已有的指派先决条件加以改进,使得在进行用户-角色指派过程中加强对用户的限制,实现指派先决条件的统一。

本文第2部分分析现有的用户-角色指派模型。第3部分引入角色和用户属性概念,在此基础上提出角色限制条件和角色资格条件,给出相关的定义。第4部分同指派约束和已有指派模型进行对比。第5部分提出进一步的工作,最后是总结。

2 现有模型分析

2.1 URA97

URA97包括两部分:用户-角色指派和用户-角色撤消。

叶春晓 博士生,讲师,研究方向为网络安全,数据库技术,软件工程。**符云清** 博士,副教授,研究方向为现代远程教育技术,分布协同作业。**吴中福** 教授,博士生导师,研究方向为网络安全,现代远程教育技术。

在用户-角色指派过程中，URA97 引入了指派先决条件概念[3,4]。

定义 1 一个先决条件就是一个布尔表达式，用 $\wedge$ 和 $\vee$ 将 r 和 $\neg r$ 连接起来。其中 r 表示对于某个用户 u，$(\exists\ r' \geqslant r)(u,r') \in URA$，$\neg r$ 表示对于某个用户 u，$(\forall\ r' \geqslant r)(u,r') \notin URA$。

用户到角色的指派过程由 $can\text{-}assign(x,y,z)$[3,4]表示。其中，x 为系统安全员角色，y 为上述的指派先决条件，z 为可指派的角色集合。考虑图 1[6]和图 2[6]中的角色关系，$can\text{-}assign(PSO1,ED,\{E1\})$表示管理员 $PSO1$ 可为已经具有 ED 角色的某用户指派新的角色 $E1$，用户需要满足的条件是：该用户应当具有角色 ED。又如 $can\text{-}assign(PSO1,E2 \wedge \neg QE1,\{PE2\})$中，指派先决条件为 $E2 \wedge \neg QE1$，表示具有 $E2$ 角色且不具有 $QE1$ 角色。

URA97 中的撤消用 $can\text{-}revoke(x,z)$[3,4]表示。其中，x 表示管理员，z 表示被撤消的角色。如 $can\text{-}revoke(PSO1,\{PE2,QE2\})$表示管理员 $PSO1$ 可撤消某用户的角色 $PE2$，$QE2$。

该模型存在以下缺陷[6]：

· 当对某个用户指派高级角色时，在 URA97 中，需要按照角色继承关系从低到高依次进行。如在图 1 中，需要对用户 u 指派 $PL2$ 角色，则必须按以下步骤：1) u 指派 E 角色；2) u 指派 ED 角色；3) u 指派 $E2$ 角色；4) u 指派 $QE2$ 角色；5) u 指派 $PL2$ 角色。指派过程显得十分繁琐。

· 重复记录了用户-角色的指派过程。即上面的每一步骤均被记录下来，许多信息实际上并不需要。

· 先决条件决定了对需要指派的用户选择与系统角色继承关系有关，对需要灵活选择用户的场合不太适用。

· 授权过程的限制较弱，除了先决条件和静态、动态约束外，不存在该角色对用户的资格限制。

2.2 URA02

针对 URA97 的缺陷，在 URA02 中作了一定改进，主要是将先决条件中指派角色的用户选择与系统角色继承关系有关，改为与用户所处的组织结构有关。用户所处的组织结构由系统管理角色事先设置，其指派先决条件做了相应变化[6]：

定义 2 一个先决条件就是一个布尔表达式，用 $\wedge$ 和 $\vee$ 将 r 和 $\neg r$ 连接起来。对于某个用户 u 其中 r 表示：

情况 1：$r \in role$，$(\exists\ r' \geqslant r)(u,r') \in URA$

情况 2：$r \in OS\text{-}U$，$(\exists\ r' \leqslant r)(u,r') \in UUA$

$\neg r$ 表示：

情况 1：$r \in role$，$\neg(\exists\ r' \geqslant r)(u,r') \in URA$

情况 2：$r \in OS\text{-}U$，$\neg(\exists\ r' \leqslant r)(u,r') \in UUA$

其中 $OS\text{-}U$，URA，UUA 的含义见文[6]，指派过程也做了相应改进，在先决条件中加入了组织结构名。如，URA97 中的 $can\text{-}assign(PSO1,E1 \wedge \neg QE1,[PE1,PE1])$在 $URA02$ 中表示为：$can\text{-}assign(PSO1,@PJ1 \wedge \neg QE1,[PE1,PE1])$。其中的 $@PJ1$ 为图 3[6]组织结构名。URA02 的撤消过程同 URA97 模型相同。

URA02 克服了 URA97 的前三个缺陷，但仍然存在以下缺陷：

· URA02 建立在一个假设基础上，即用户在指派前就已经被设置到合适的组织结构中，这需要系统管理角色了解组织结构和进行预先的设置工作。一旦指派策略发生变化，需要系统管理角色将用户重新设置到合适的组织结构中。

· 同 URA97 一样，授权过程的约束较弱，不存在角色对用户的资格限制。

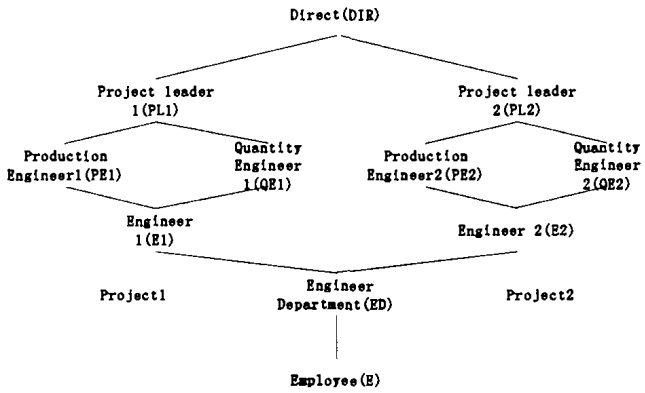

图 1 角色继承关系

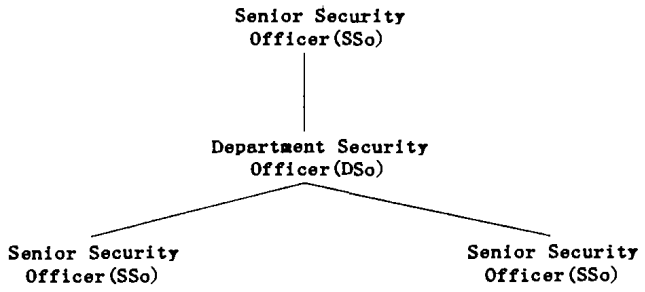

图 2 管理角色继承关系

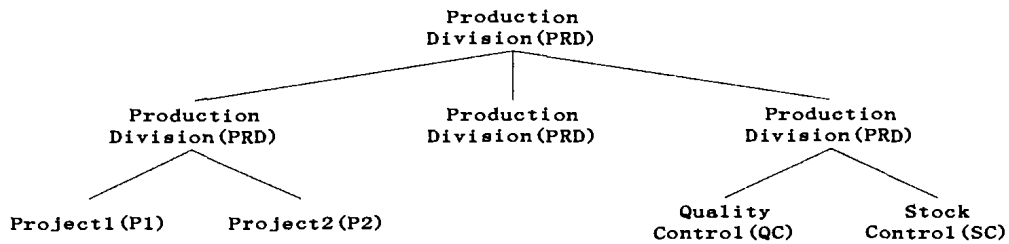

图 3 用户组织结构

3 基于角色限制条件的用户-角色指派

3.1 概述

URA97 和 URA02 指派过程中，指派先决条件的一个作用在于指定用户需要满足的限制条件。由上可知，URA97 和 URA02 模型在指派时，用户除了需要满足先决条件外，还需要满足相关的约束条件（主要是 SOD，角色基数，角色互斥等），但忽视了一个十分重要的问题，即用户是否满足该角色的某些限制条件（主要是对指派为该角色的用户资格限制）。如在招聘广告中常见的系统分析员需要有一定的工作经历和资格要求。

指派先决条件的另一个作用也就是限制了需要指派角色的用户选择范围。在URA97中,对角色的选择是在指派先决角色范围内,与角色继承关系有关,因而会引起多步指派问题。URA02中,角色指派先决条件与用户所处的组织结构有关,在指派前必须将用户分配到合适的组织结构中。一旦授权策略变化后,需要重新将用户分配到合适的组织结构中。

引入角色限制条件后,一方面指派过程中角色对用户的约束更强;另一方面,对用户的选择与角色继承关系和用户组织结构无关,只要满足角色约束条件的用户均在选择范围内。即使角色继承关系、用户组织结构发生变化后,用户的选择范围也只与角色限制条件有关。即使指派策略发生变化后,也不用象URA02那样,需要系统管理角色重新分配用户到新的组织结构中。并且,在后续部分可看到,引入角色限制条件后可实现URA97和URA02模型中指派先决条件的统一。

以现实生活为例,高校的职称从低到高依次为助教、讲师、副教授、教授,可分别看作角色 $asst$,$instr$,ap,$prof$。考虑两个拥有 $instr$ 角色的计算机系教师 T_a,T_b,用户的部分状态如下表:

表1 用户部分状态

姓名	教龄	学位	年科研经费(万元)
T_a	10	博士	10.5
T_b	8	硕士	5

虽然 T_a,T_b 均拥有角色 $instr$,但两个用户的目前状态并不相同。

假设副教授对用户的限制条件可描述为"教龄10年以上且拥有博士学位且年科研经费不少于10万元",显然 T_b 不具有晋升副教授的资格,即 T_b 不能被指派 ap 角色。

在URA97中,指派副教授角色的过程可表示为 $can\text{-}assign(sa, inst \wedge \neg ap, \{ap\})$,其指派先决条件为"$inst \wedge \neg ap$",显然 T_b 满足该先决条件可被指派 ap 角色,但这违反了 ap 角色的限制条件要求。

在URA02中,指派副教授角色的过程可表示为 $can\text{-}assign(sa, @计算机系 \wedge \neg ap, \{ap\})$,其指派先决条件为@计算机系 $\wedge \neg ap$,显然 T_b 满足该先决条件可被指派 ap 角色,但这同样违反了 ap 角色的资质条件要求。

为了表达角色限制条件,本文将引入角色属性和用户属性的概念。角色限制条件实际上就是角色属性表达式。

通过上面的分析,我们可将URA97和URA02存在的主要缺陷归纳为以下三点:

1)同一角色下或同一组织结构内的不同用户无差异,即不同用户的属性值相同。

2)否认用户属性值的可变性。即用户的状态不发生改变。

3)除了指派时的先决条件和静态约束、动态约束外,角色对用户的限制很少。

因此,本文从以上两个方面着手,考虑如下改进:

1)同一角色下或同一组织结构内的不同用户存在差异,即不同用户的属性值不同。

2)用户属性值可变。即用户的状态会随着时间推移而发生变化。

3)除了指派时的先决条件和静态约束、动态约束外,角色对用户还存在其他限制(主要是资格限制)条件。

3.2 定义

定义3 UCA 为能够满足指派过程中系统角色对用户限制描述需要的用户最小公共属性集合,$uca[1],\cdots,uca[t] \in UCA$,$uca[t](1 \leqslant t \leqslant n, n$ 为 UCA 所有属性数)是其第 t 个属性。

系统中的用户实际上具有两种类型的属性:一种是每个用户都具有的公共属性,公共属性用来对目前用户的状态进行描述,该状态可用于表达角色限制条件。另一种是每个用户均不同的私有属性,私有属性起补充描述作用,在角色限制条件中不起作用。

系统中的角色也拥有同用户相同的用以描述限制条件的属性集,即 UCA。

定义4 一个角色 r 第 t 个属性的属性表达式 $ae_r[t](1 \leqslant t \leqslant m)$ 可表示为:$ae_r[t] = uca[t]\ aop\ ac$。其中,$aop$ 为 $>$,$<$,$\geqslant$,$\leqslant$,$=$,$\neq$ 6种常见的比较运算符。ac 为属性表达式常量,由字符串,数字,字符等简单数据类型构成。

本文只讨论了最基本的比较运算和常见的简单数据类型。对复杂的集合运算如 in,not in 等,复杂的数据类型如构造类型、集合类型可作为进一步的工作。

定义5 对角色 r,其角色限制条件 qc_r 可表示为:$qc_r = ae_r[1]\ lop\ ae_r[2]\cdots lop\ ae_r[t], 1 \leqslant t \leqslant m$。其中 lop 为 $\wedge$ 或 $\vee$ 运算。

定义6表明角色限制条件为用 $\wedge$ 或 $\vee$ 连接的多个角色属性表达式。

实际上,上面给出的角色限制条件定义隐含了URA97和URA02的指派先决条件部分。广义地讲,URA97的指派先决角色和URA02的指派先决条件中的用户组织结构也可看作角色限制条件的一部分。只要在指定角色限制条件时包含相关的属性,就可以将几种指派先决条件统一起来。因而需要定义角色资格条件。

定义6 对角色 r,其角色资格条件 $qa_r = ae_r[1]\ lop\ ae_r[2]\cdots lop\ ae_r[t], 1 \leqslant t \leqslant m$。其中 lop 为 $\wedge$ 或 $\vee$ 运算。$ae_r[t]$ 不属于角色 r 中与用来表示用户当前角色和用户当前组织结构的相关属性所构成的集合。

推论1 对于角色 r,有 $qa_r\ qc_r$。即角色资格条件是角色限制条件的子集。

由定义5和定义6知推论1显然成立。

定义7 一个先决条件就是一个用 $\wedge$ 和 $\vee$ 将 qc_r 或 qa_r 两者之一和 $\neg r$ 连接起来的布尔表达式。其中 qc_r 表示角色 r 的角色限制条件,qa_r 表示角色 r 的角色资格条件,$\neg r$ 表示对于某个用户 u,$(\forall r' \geqslant r)(u, r') \notin URA$。

定义8表明,加入角色限制条件和角色资格条件后,若先决条件中只有角色资格条件 qa_r,用户只要满足由该资格条件构成的先决条件即可,因而实现了用户选择与角色继承关系和用户所处的组织结构无关;若先决条件中为角色限制条件 qc_r,则可实现先决条件的统一。并且,先决条件加强了对指派该角色的用户的资格限制,用户只有满足该角色资格条件对其的资格要求后,才能被指派该角色。

定义8(用户角色指派判定) $can\text{-}assign \subseteq AR \times CR \times 2^R$。其中 AR 为管理角色集合,CR 所有先决条件集合,R 为角色集合。

用户角色指派判定的形式同URA97和URA02相同,但其中的CR的含义同已有模型不同。

定义9(用户角色撤消判定) $can\text{-}revoke \subseteq AR \times 2^R$。$AR$ 和 R 的含义同上。

3.3 用户选择

有了角色限制条件后，就可实现多种用户选择方式，实现表达方式的统一。

1. URA97 方式　对 URA97 的指派先决角色部分，在角色限制条件中只包含“当前角色”属性，不包含其他属性即可实现 URA97 的指派先决条件。假设角色中用来表示用户的“当前角色”属性为 *curole*，则指派副教授角色的判定 *can-assign*(*sa*, *inst* ∧ ¬*ap*, {*ap*}) 可改写为 *can-assign*(*sa*, *curole* = '*inst*' ∧ ¬*ap*, {*ap*})。

2. URA02 方式　对 URA02 的指派先决条件，在角色限制条件中只包含“当前组织结构”属性，不包含其他属性即可实现 URA02 的指派先决条件。假设角色中用来表示用户的“当前组织结构”属性为 *urunit*，则指派判定 *can-assign*(*sa*, @计算机系 ∧ ¬*ap*, {*ap*}) 可改写为 *can-assign*(*sa*, *curunit* = '计算机系' ∧ ¬*ap*, {*ap*})

3. 全选择　此方式下，指派先决条件只包含角色限制条件的资格条件部分。此时，只要满足该限制条件的用户即可进行角色指派，用户的选择范围为整个系统，与角色继承关系和用户组织结构无关。如，*can-assign*(*sa*, (教龄≥10 年 ∧ 学位 = “博士” ∧ 年科研经费≥10) ¬*ap*, {*ap*})。

4. 混合方式　此方式可分为两种：URA97 混合方式和 URA02 混合方式。

1) URA97 混合方式下，指派先决条件既可包含 URA97 的先决角色，也包含角色限制条件中的资格条件部分。对 URA97 的先决条件进行了加强，用户不但必须拥有先决角色，还要满足资格条件的限制。

2) URA02 混合方式下，指派先决条件既可包含 URA02 的组织结构，也包含角色限制条件中的资格条件部分。对 URA02 的先决条件进行了加强，用户不但在指定的组织结构中，还要满足资格条件的限制。

3.4　用户-角色指派

1. 角色集合只有一个角色　此时，用户只能指派一个角色。假设有 *can-assign*(*x*, *y*, {*z*}) 指派判定，此种指派中，角色集合中只有一个角色，因而指派先决条件 *y* 中的角色限制条件实际上就是角色 *z* 的限制条件 qc_z。

2. 角色集合中有多个角色　此时，用户可被管理角色指派候选角色集合中的角色之一。假设有 *can-assign*(*x*, *y*, {*a*, *b*, *c*}) 判定，此种指派中，候选角色集合中有多个角色，且角色之间为 *or* 关系。此时指派先决条件 *y* 的构成相对复杂。设角色 *a*, *b*, *c* 的限制条件分别为 qc_a, qc_b, qc_c，*a*, *b*, *c* 之间为 *or* 关系，则指派先决条件 *y* 的角色约束条件部分应表示为 $qc_a \vee qc_b \vee qc_c$。则整个指派先决条件 *y* 可表示为 $(qc_a \vee qc_b \vee qc_c) \wedge \neg R$，*R* 为先决角色集合。

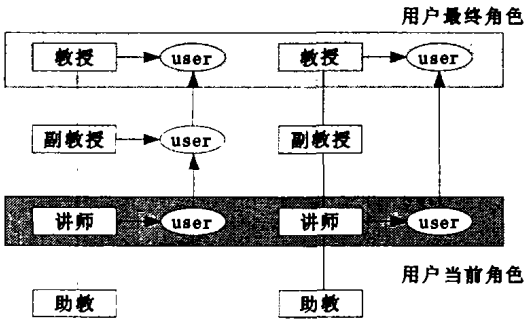

图 4　指派过程比较

3. 单步指派　URA97 在指派用户更高级角色时，需要按照角色继承关系由低到高依次进行，指派过程步骤增加，特别是在跨角色继承层次指派时。如某人原来为讲师，破格提拔为教授，URA97 指派时就先要指派副教授角色，然后再指派教授角色，这显然与实际情况不符。本方法中，采用 3.3 节中第三种方式进行指派时，用户只要满足教授的限制条件，就可直接将该用户指派为教授角色，不需要中间步骤。

4. 撤消　撤消用户角色时，由于 URA97 和 URA02 中均未考虑撤消先决条件，本文亦未讨论撤消先决条件，其基本过程同已有的两个模型，不详细说明。

4　比较

4.1　与指派约束比较

URA97 和 URA02 模型中，指派过程还需要满足相关约束。约束可分两类：静态约束和动态约束。

对静态约束而言，主要是在角色被指派给用户时的限制。动态约束条件比静态约束弱，主要是角色被激活时应满足的限制条件，本处只讨论静态约束。URA97 和 URA02 中的静态约束主要体现在如数目限制、角色互斥、先决角色等方面。

可见，现有模型中的约束条件十分简单，并不涉及到角色对用户的资格限制。当然，角色限制条件也可以用静态约束来表示，但将角色限制条件包含在指派先决条件中，有如下优点：

1. 同静态约束中的数目限制和角色互斥相比较，角色限制条件更能体现指派时对用户的资格限制本质，即从角色的角度出发设置限制条件，用户必须满足该角色对用户的限制条件（主要是资格条件）。

2. 有利于将角色限制条件同具体角色结合起来，将角色限制条件作为角色本身的固有属性，如同对象的属性一样，符合认识习惯。

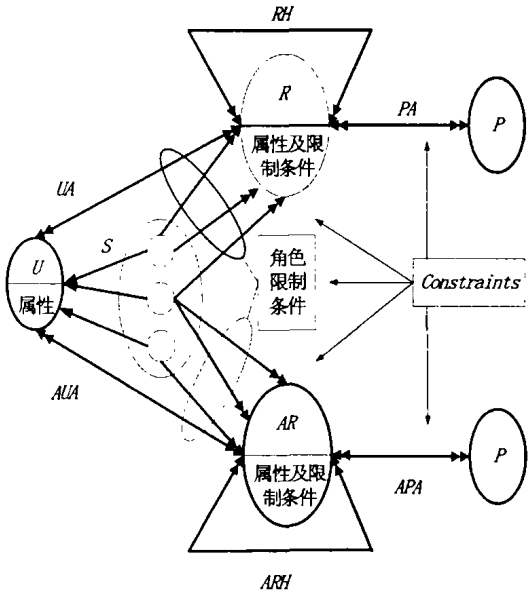

图 5　加入属性和限制条件后的 RBAC96 模型

3. 有利于对角色限制条件的管理。对于存在继承关系的角色来说，其限制条件往往存在一定的相似性或包含关系。如，对助教-讲师-副教授-教授这一角色继承关系来说，讲师对用户的限制条件强于助教对用户的限制条件，副教授的限制条件又强于讲师的限制条件。限制条件之间可用类似角色和权限继承的方式进行管理。而静态限制条件和规则不便于

（下转第 83 页）

表 1

方案	识别	签名	盲签名
模	$\|N\|=1024$ 位；$\|p\|=\|q\|=512$ 位		
$Ord(g)$	160 位		
安全参数	$k=24$	$K=128$	
消息泄漏参数	$K'=64$		
$\|S\|(>\|Ord(g)\|)$	168 位		
$\|R\|(=\|S\|+k+k')$	256 位	360 位	
$\|M\|(=\|S\|+k+2k')$			424 位
在线花费(证明者)	Mult(24,168) +Add(256,192)	Mult(128,168) +Add(360,296)	
通信	360 位(45 字节)		
签名大小		488 位 (61 字节)	552 位(69 字节)

可以看到，既然声明可以预先计算，在一次证明中证明者只要进行一次加法和一次乘法。对于一个使用推荐的参数的盲签名来说，银行只要将 128 位的整数与 168 位的相乘，然后加上一个 360 位的整数。与 Shnorr 方案相比，最重要的受益是对于模数化简的压缩。

然后花少量的存储空间，银行就可以每秒盲签成千上万的消息。而且由它的安全性，也可以安全地执行并行的撤销操作。

参 考 文 献

1 Schnorr, Guillou. Quistquater Composite discrete logarithm and secure authentication. In: Third Intl. Workshop on Practice and Theory in Public Key Cryptosystems, PKC2000

2 Brickell E F, McCurley K S. An interactive identification scheme based on discrete logarithm and factoring …, Advances in Cryptology- Eurocrypt'90, LNCS 473, Springer-Verlag, pp. 481～486

3 Girault M. An identity-based identification scheme based on discrete logarithms modulo a composite number Advances in Cryptology- Eurocrypt'90, LNCS 473, Springer-Verlag, pp. 581～586

4 Poupard. Practical multi-candidate election system. PODC 2001. 274～283

5 Feige U, Shamir A. Zero knowledge proofs of identity. In: Proc. of the Nineteenth Annual ACM Symposium on Theory of Computing, New York City, May 1987. 210～217

6 Pointcheval. Provably Secure Blind Signature Schemes (1996) David. ASIACRYPT: Advances in Cryptology -- International Conference on the Theory and Application of Cryptology

7 Girault M, Stern J. On the Length of Cryptographic Hash-Values used in Identification Schemes. Identification schemes. In: Proc. of Crypto 94, Lecture Notes in Computer Science 839, 202～215

(上接第 76 页)

利用类似继承的方式进行管理。

4.2 与现有模型比较

和现有的 URA97, URA02 模型相比，本方法的主要改进在于将指派先决条件加以扩展，引入了角色限制条件和角色资格条件概念，具有以下优点：

①形式统一。在表达 URA97 和 URA02 模型的先决条件时，可通过在角色限制条件中只包含与用户当前角色和当前组织结构有关的属性来实现。

若先决条件只包含角色资格条件时，又可实现本文的方法。达到表达形式上的统一。

②实现一步指派。同 URA02 一样，采用 3.3 节第三种用户选择方式进行指派时，只要用户满足角色资格条件，就可直接指派该角色，不需要中间过程，达到一步指派。

③对用户-角色指派的限制加强。用户必须具备相应的资格后才能被指派相关角色。URA97 与 URA02 对用户的限制较弱，否认用户个体差异的存在，不符合现实世界真实情况。本方法加强了指派过程中对用户的限制。

④可实现自动指派和撤消。当用户不再满足当前角色限制条件后，系统可根据用户当前情况，自动将用户指派给满足其限制条件的新角色。同样，角色限制条件发生变化后，系统也可自动将满足该限制条件的用户指派给该角色，将不满足该限制条件的用户撤消其角色。实现自动指派和撤消比较复杂，可做进一步的研究，此处显示了其可能性。

5 进一步工作

1. 角色限制条件的表达。本文为说明思想，对角色限制条件只讨论了相对简单的情形，属性表达式运算和属性表达式常量均较简单。对运算，可进一步考虑集合运算；对表达式常量，可进一步考虑其他数据类型，如集合和构造类型等。

2. 自动指派和撤消。自动指派和撤消有助于简化用户-角色的指派过程，简化管理角色的工作。并可在用户角色变化频繁的环境如 CSCW 中得到很好地应用。在某些对用户角色改变要求及时的场合，由系统自动进行指派和撤消可实时反映用户当前实际状态。

3. 多级角色限制条件继承。由上述可知，上级角色的限制条件同下级角色的限制条件之间存在类似继承的关系。因而，考虑在角色继承环境下上下级各个角色限制条件的表达时，可采用角色限制条件的上下级继承方式进行处理。同时，指派先决条件的表达也需要改进以适应角色限制条件的继承情况。

总结 本文着眼于用户-角色指派问题。首先分析了 URA97 和 URA02 两种常见的指派模型，指出其指派先决条件只与角色和组织结构有关的缺陷。仔细分析了现实世界中用户-角色指派时实际存在的角色对用户的资格限制，定义了角色和用户属性，对指派先决条件进行改进，提出了在其中包含角色限制条件和角色资格条件的思想，并给出相关的定义和做了详细的阐述。将对用户的资格限制，用角色限制条件实现和用指派约束实现两种方式做了对比，说明了采用前者的优点。本文也对在角色-用户指派中引入角色限制条件后与 URA97 和 URA02 模型中的角色-用户指派做了比较，最后提出进一步工作的方向。

分析表明，采用基于角色限制条件的用户-角色指派，将有效地避免 URA97 和 URA02 模型对用户限制较弱的问题，更符合现实世界实际情况，也有助于系统管理角色的管理工作。

参 考 文 献

1 Sandhu R S, et al. Role-based access control models. IEEE Computer, 1996, 29(2): 38～47

2 Ferraiolo D F, Sandhu R S. A proposed standard for role-based access control. ACM trans. on information and System Security, 2001, 4(3): 25～29

3 Sandhu R S, Bhamidipati V, et al. The ARBAC97 model for role-based administration of roles. TISSEC, 1999, 2(1): 105～135

4 Sandhu R S, Bhamidipati V. The URA97 for Role-based User-Role Assignment. In: Proc. of IFIP WG 11.3 workshop on database security, lake tahoe, California, Aug. 1997

5 Sandhu R, Munawer Q. The ARBAC99 model for administration of roles. In: Proc. of the Annual Computer Security Applications Conf. 1999

6 Oh S, Sandhu R. A Model for Role Administration Using Organization Structure. SACMAT'02, Monterey, California, USA, 2002

7 赵青松，孙玉芳，孙波. 基于系统先决条件的授权模型研究. 计算机研究与发展, 2003, 40(3): 406～412

8 Goh C, Baldwin A. Towards a More Complete Model of Role. Internet Business Management Department HP Laboratories Bristol HPL-98-92 May, 1998