基于混合离散对数的盲签名认证研究*)

李 波 邱小平

(重庆工学院计算机学院 重庆 400050)

摘 要 本文在分析混合系数的离散对数问题的基础上,提出了一种新的认证,这种认证比因式分解有更好的安全性,而且从证明者角度看来有更高的效率。最后我们得到一个基于信息不可识别性的安全性与因式分解相同的盲签名。

关键词 混合离散对数,认证,盲签名

Study About Blind Signature Authentication Based on Composite Discrete Logarithm

LI Bo QIU Xiao-Ping

(Department of Computer Science and Engineering, Chongqing Institute of Technology, Chongqing 400050)

Abstract A new authentication which security is better than factor has been given based on analysis to Composite Discrete Logarithm. High efficiency is the most peculiarity of the blind signature algorithm from the point of view of a prover. Finally an new blind signature scheme has been put forward, which security is based on unidentified information.

Keywords Composite discrete logarithm, Authentication, Blind signature

1 概述

在密码学中,可证明为安全的方案一直都是追求的一个重要目标。然而,效率一直就是一个难以实现的属性。即使在现在对于认证已经进行了广泛的研究,还是很少有方案能兼顾效率和安全性。其原因就是零知识协议的广泛应用。

对于所有的这些问题以及其他的在线认证,零知识证明理论成为一个非常强有力的工具。虽然其具有很高的安全性,却导致高负荷运算。最近发现信息不可分辨性是一个可以兼顾安全和效率的性质。Schnorr[1]提出了一个高效的基于素数阶子群离散对数问题的识别方案和签名方案的变种,这个以零知识闻名的方案为了抵抗主动攻击获得较高的安全性,使用了许多次固定长度的挑战应答交互。这样,高的安全性就需要很大的通信量和很大的存储空间存储预计算量。虽然没有提出安全的预处理方案,还是有许多应用中假定如果使用较大规模的挑战应答它的安全性与基本的三次通过协议相当。其安全性依赖于未经证明的假设,即假设这个方案是"信息隐藏"的。

在定义了信息隐藏和信息不可分辨属性以后,Brickell[2]提出了使用信息隐藏属性的 Schnorr 方案的一个变种。这些协议中有些是基于素数阶子群的离散对数问题,有的是基于 RSA 假设。但是所有这些方案都并不比原来的 Schnorr 方案更加有效。

1991 年,Grault 利用合数作为模代替素数,提出了 Schnorr 的一个变种,从证明者的角度来说提高了效率。Poupard[4]给出了这个方案的统计意义上的零知识属性的证明,证实了这个方案的安全性等价于合数的离散对数问题。然而,这个方案,对于高的安全性要求也需要许多次交互,而大的简化只能适用于大的不实用的数据。最近他们进行了简化,使其安全性仅仅等价于因数分解。这是仍在进行的一项工作。

然而这些方案的主要缺点是计算量大。至今,盲签名所面对的一个重要挑战是:从签名者角度看来,他们需要高效并且可证明是安全的签名,因为他们可能同时会有成千上万的签名。

本文研究混合系数的离散对数问题,也即信息不可识别性。我们提供一种新的认证,这种认证比因式分解有更好的安全性,而且从证明者角度看来有更高的效率。我们也降低了对 Schnorr[1]方案变形的实际安全参数的 Girault[3]的证明的开销。最后,基于信息不可识别性,我们得到一个安全性与因式分解相同的盲签名。

2 混合离散对数问题

Feige[5]已经证明,信息不可分辨属性对于识别协议来说已经足够提供用于抵抗主动攻击的安全性了。Pointcheval[6]进一步证明了盲签名的这一属性还提供了抵抗并行攻击下的多次伪装攻击的安全性。这是利用了函数 $f_{N,g}(x)=g^x \bmod N$,其中 N,g 是选择好的。下面我们定义一些有用的概念。

定义 1(α-强素数) 如果一个素数 $p=2r+1$,其中 r 是一个大整数,其素数因子都大于 α,则称 p 是 α-强素数。

定义 2(α-强 RSA 模数) 如果 $N=pq$,并且 p 和 q 都是 α-强素数,N 就被称为 α 强 RSA 模数。

定义 3(不对称基) $N=pq$ 是一个 RSA 模数,在 Z_N^* 中的基 g 如果在 Z_p^* 和在 Z_q^* 中的 $Ord(g)$ 的奇偶性不一样,就说它是不对称基。也就是说,不对称基就是仅仅在 Z_p^* 和 Z_q^* 的两个子群其中之一的一个二次剩余。

定理 1 如果 $N=pq$ 是一个任意的 α-强 RSA 模数,对于

*)基金项目:教育部科技重点项目(03115),重庆市科委项目(2002C013)。李 波 博士后,研究方向:计算机网络,信息安全技术。邱小平 助教,研究方向:信息安全技术,数据库技术。

某些 $\alpha>2$，g 是一个阶大于 α 的在 Z_N^* 中的任意不对称基，那么定义为 $x->g^x \bmod N$ 的一个 $f_{N,g}()$ 的碰撞，可以将 N 分解。

证明：我们用 $2l$ 标记在 Z_N^* 中 g 的阶。可以认为这一阶就是偶数，因为它至少，并且恰在子群中的一个，例如 Z_p^* 中是偶数。而且，l 是奇数，并且大于 α，因为 l 大于 $\alpha/2>1$，$(p-1)/2$ 和 $(q-1)/2$ 的任何素数因子都是奇数，并且大于 α。因此，

$g^{2l}=1 \bmod p$，$g^{2l}=1 \bmod q$，但是 $g^l=-1 \bmod p$，

$g^l=1 \bmod q$.

让我们假设我们有一个 $x<y$ 的关于 $f_{N,g}()$ 的碰撞，也就是 $f_{N,g}(x)=f_{N,g}(y)$。如果我们定义 $L=y-x$，那么 $2l/L$。通过分解出 L 的奇数部分，$L=2^a b$，我们得到了 l 的倍数。那么，

$g^{2b}=1 \bmod p$，$g^{2b}=1 \bmod q$，但是 $g^b=-1 \bmod p$，$g^b=1 \bmod q$。

这样 g^b 就是 Z_N^* 中的 1 的一个不可忽略的平方根：$gcd(g^b,n)\in\{p,q\}$。

这样我们就得到了一个难题，两个不同的解提供了模数 N 的因式分解。

3 在密码协议中的应用

我们首先考虑识别协议，可以由此导出签名协议。然后我们考虑一个盲签名方案。

3.1 身份识别

描述：先回忆一下 Girault 的方案。如下所示：

$N=pq$ 是一个 RSA 模块，g 是属于 Z_N^* 的一个高阶元素。

私钥：s 属于 $\{0,\cdots,s-1\}$

公钥：$v=g^{-s} \bmod N$。

随机数：r 属于 $\{0,\cdots,R-1\}$

证明者		验证者
$x=g^r \bmod N$	→	
	←	$e\in\{0,\cdots,2^k-1\}$
$y=r+es$	→	
		$x=g^y v^e \bmod N$

我们有两个安全参数 k 和 k'，其中 k 代表了挑战的长度，k' 代表了泄漏的信息。还有私钥的一个范围。接着，我们定义 $R=2^{k+k'}S$。我们使用 RSA 模 $N=pq$ 以及属于 Z_N^* 的一个高阶元素。证明者随机地选择一个属于 $\{0,\cdots,S-1\}$ 的私钥 s，公布 $v=g^{-s} \bmod N$。

证明者选择一个随机数 r 属于 $\{0,\cdots,R-1\}$，发送数值 $x=g^r \bmod N$；验证者随机的选择一个挑战 e 属于 $\{0,\cdots 2^k-1\}$，送给证明者；最后，证明者计算并且发送 $y=r+es$；

验证者检验是否 $x=g^y v^e \bmod N$。

不能说这是知道基 g 模 N 中关于 v 的离散对数的证据，但是在特殊情况下，N 是一个 2^k-强 RSA 模数时（包括实际应用中典型的强 RSA 模数）可以应用下面的定理：

定理 2 假设 N 是一个 2^k-强 RSA 模数，如果存在一个攻击者 A，其运行时间界定为 T，对于不可忽略的小量 v，能够以大于 2×2^{-k} 的概率 ε 被接受，那么基 g 模 N 的离散对数可以在界定为 $4T/\varepsilon\times S/Ord(g)$ 的时间内被计算出来。

证明：用古典的开方技术，我们能够得到两个对于同一个声明 x 的有效证明，一对 (α,β) 使得 $v^\alpha=b^\beta \bmod N$，其中 $0<\alpha<2^t$。而且，这些可以在期望的时间 $4T/\varepsilon$ 内被完成。

如果首先进行化简 $v=g^\gamma \bmod N$，对于一个随机选择的小于 S 的 γ，那么可以得到 (α_1,β_1) 使得

$L=\alpha_1\gamma-\beta_1=0 \bmod Ord(g)$，它非零的概率大于 $(S/Ord(g)-1)^{-1}$。

然后用想知道其离散对数 x 的 v 来进行这样的化简，得到 (α_2,β_2)。让我们用 l_0 初始化上面得到的 L，接着递归的计算 $l_{i+1}=l_i/\gcd(\alpha_2,l_i)$，直到 gcd 等于 1。极限用 l 来标记。既然 $\alpha_2<2^t$，小于 $\lambda(N)$ 的所有奇素因子，那么 $2l$ 仍然是 $Ord(g)$ 倍数。然后我们计算 $y=\beta\alpha_2^{-1} \bmod l$，得到 $x=y+cl \bmod Ord(g)$，其中 $c\in\{0,1\}$。我们只需要检查一下 c 的正确值。

可以认为在特殊情况下，g 是 $\lambda(N)$ 的最大的阶，$Ord(g)=\lambda(N)$ 的倍数导致了 N 的分解。

定理 3 这一协议在统计意义上是零知识的。

证明：可以参考 Poupard[6] 的论文。

要指出的是，交互验证知识协议的零知识属性对于识别协议来说是一个足够强大的属性，主要的缺点是基础方案为了达到高的安全性所需要的一系列的交互。这样信息不可分辨属性也就足够确保抵抗主动攻击的安全性，而提供一个更加有效率的方案。

定理 4 这一协议是统计意义上信息不可分辨的。

证明：我们必须证明即使对于一个不诚实的验证者来说，证明者所用的私钥也是独立于所发布的信息的。令 $s_1<s_2$，是 $\{0,\cdots,S-1\}$ 中的两个不同的私钥，并且

$g^{-s1}=g^{-s2}=v \bmod N$.

我们可以证明下面的发布信息是不可识别的，假设 r 是在 $\{1,\cdots R-1\}$ 中随机选择的，S 表示攻击者以可能的概率用某种方式得到 x 的挑战 e。那么：

$\delta 1=\{(x=g^r \bmod N,e,y)\mid y=r+s1e,e=S(x)\}$，

$\delta 2=\{(x=g^r \bmod N,e,y)\mid y=r+s2e,e=S(x)\}$

事实上，如果对任何三元组 (α,β,γ)，对应 $\alpha=g^\gamma v^\beta \bmod N$，我们定义 $pi(\alpha,\beta,\gamma)=Pr[(x,e,y)=(\alpha,\beta,\gamma)]$，对 $I=1,2$。$(x,e,y)\in\delta i$。

我们用 $p_{\alpha,\beta}$ 表示对于方法 S 来说，输入为 α，输出为 β 的概率，δ 是一个布尔函数，定义为 $\delta(\text{true})=1$，$\delta(\text{false})=0$，这样我们得到：

$$\begin{aligned}pi(\alpha,\beta,\gamma)&=Pr[\alpha=g^r \bmod N,\beta=S(\alpha),\gamma=r+si\beta]\\&=Pr[\alpha=g^r \bmod N]*p_{\alpha,\beta}*Pr[\gamma=r+si\beta\mid\gamma\\&=r+si\beta \bmod Ord(g)]\\&=(1/Ord(g))*p_{\alpha,\beta}*\delta(0=<\gamma-si\beta<=R)*Ord(g)/R。\end{aligned}$$

简单地化简可以得到 $p_{\alpha,\beta}/R\times\delta(0=<\gamma-si\beta<=R)$。这样发布信息 $\delta 1$ 和 $\delta 2$ 之间的距离就是所有的三元组 (α,β,γ) 使得 $\gamma=\log\alpha-s1\beta \bmod Ord(g)$：

$$\begin{aligned}sum&=\Sigma p_{\alpha,\beta}*2(s2-s1)\beta/R*Ord(g)\\&=<(2S*\Sigma\beta p_{\alpha,\beta})/R*ord(g).\end{aligned}$$

通过定义概率 $p_{\alpha,\beta}$，显然对于任何 α，$\Sigma\beta p_{\alpha,\beta}=1$。对于所有可能的 α 之和，等于 $Ord(g)$。既然 $\beta<2^t$，$R=2^{t+k'}S$，我们得到：

$sum=<2S*2^t/R=2/2^{k'}$.

由于它的信息不可分辨性，使得我们获得一个经过三次互通就可以实现的高效的安全的识别协议。

定理 5 N 是一个 2^t－强 RSA 模数，g 是在 Z_N^* 中的一个高阶不对称基，如果 $S>=2\times Ord(g)$，这一协议抵抗主动攻击的安全性是等价于分解 N 的。

证明：为了证明这个识别方案的安全性能够抵抗主动攻击，我们选择一个随机的私钥 $s<S$，让攻击者验证一些交互。然后我们假定她能够以概率 ε 成功的进行扮演。利用在定理 2 证明中的第一步，就可以得到一个乘数 L，其阶为 g 的概率是大于一半的。然后，就像在定理 1 中的证明一样，既然 g 是一个非对称基，那么她就可以成功的得到 N 的因式分解。

这样我们就可以对原来的识别协议进行修改。修改后的协议如下所述。

$N=pq$ 是一个 2^k-强 RSA 模块，g 是属于 Z_N^* 的一个不对称基元素，阶高于 2^k。

H 是一个超过 80 位的哈希函数。

私钥：s 属于 $\{0,\cdots,s-1\}$

公钥：$v=g^{-s} \bmod N$。

随机数：r 属于 $\{0,\cdots,R-1\}$

证明者		验证者
$x=g^r \bmod N$		
$h=H(x)$	→	
	←	$<e\in\{0,\cdots,2^k-1\}$
$y=r+es$	→	
		$h=H(g^y v^e \bmod N)$?

尽管如此，当我们有了 N 的因式分解，剩下的安全性就完全等价于 Schnorr 识别方案，可以预见，素数阶子群的离散对数问题仍然难以解决。

而且，即使为了高的安全性级别而提高挑战程度，安全性仍然保持，而基于零知识属性的协议就不具备这种特点。

3.2 签名

我们当然可以将前面的识别协议转换为签名协议，只要使用一个哈希函数产生一个随机的挑战就可以了。这一方案介绍如下：

初始化。$N=pq$ 是一个 2^k-强 RSA 模块，g 是属于 Z_N^* 的一个不对称基元素，阶高于 2^k。

H 是一个哈希函数。

产生密钥。私钥：s 属于 $\{0,\cdots,s-1\}$

公钥：$v=g^{-s} \bmod N$。

对消息 m 签名。产生随机数：r 属于 $\{0,\cdots,R-1\}$，计算 $x=g^r \bmod N$，得到 $e=H(m,x)$，在计算 $y=r+es$，签名就是：

$\Sigma(e,y)$；

验证 (m,e,y)：$e=H(m,g^y v^e \bmod N)$?

这一方案抵抗伪装者使用零消息攻击的安全性在随机 Oracle 模型中表现的十分清楚。由于信息不可分辨属性，我们不需要进行伪装以抵抗动态选择消息攻击。事实上，我们可以利用一个有私钥 s_1 的签名者，使用分支引理或者 ID 化简引理，分离出第二个私钥。正如前述，只要 $S>=2Ord(g)$，我们就能以很高的概率得到模数 N。

定理 6 如果 $S>=2Ord(g)$，使用动态选择消息攻击的潜在伪装者攻击这个方案的难度要高于因式分解。

3.3 盲签名

现在，我们考虑一个基于前面所述问题的盲签名方案。如下所示：

$N=pq$ 是一个 2^k-强 RSA 模块，g 是属于 Z_N^* 的一个不对称基元素，阶高于 2^k。

私钥：s 属于 $\{0,\cdots,s^{-1}\}$

公钥：$v=g^{-s} \bmod N$。

随机数：r 属于 $\{0,\cdots,R-1\}$

银行		用户
$x=g^r \bmod N$	……	→
		$\beta\in\{0,\cdots,M-1\}$，
		$h=g^\beta \bmod N$，
		$\gamma\in\{-2^k,\cdots,2^{k-1},\}$
		$\alpha=xhv^\gamma \bmod N$
		$\varepsilon=f(m,\alpha)$
		$e=\varepsilon-\gamma$
	←	直到 $e\in\{0,\cdots,2^k-1\}$
$y=r+es$	→	
		$x=g^\gamma v^e \bmod N$?
		$u=y+\beta$

$\alpha=g^u v^e \bmod N$?

盲签名方案并不是那么简单，因为这一方案的初始化需要仔细地选择安全参数。然而，所产生的方案从银行的角度来说很有用。事实上，它的计算量是很小的。

由于上面所述的信息不可分辨属性，我们希望得到一个至少比因式分解的安全性更高的盲签名方案。其中，k 是安全参数，k' 是泄漏信息参数，我们定义 $R=2^{k+k'}S$ 和 $M=2^{k+2k'}S$，其中 $S>=2Ord(g)$，定义了私钥的范围。

首先我们要证明这个方案是盲的。例如，即使是一个不诚实的银行，也无法在以后将一个用户和一个消息签名对联系起来。这是匿名协议非常重要的一个属性。我们想要银行无法认出用户，即使拥有了消息和签名对。

定理 7 这一方案是统计上的盲签名方案。

证明：这一协议的输出的签名在前面已经经过了讨论，已证明了是安全的。现在我们只要证明它是盲的就可以了。

令 $(m,\alpha,\varepsilon,\rho)$ 是在执行完一次盲签名方案，经过两次交互 $(x1,e1,y1),(x2,e2,y2)$。所得到的签名。要看是否有可能知道它是来自那一次的结果。这样，我们就要研究下面的一些可能性。对于 $i=1,2$：

$pi(\alpha,\varepsilon,\rho)=Pr[\alpha=xig^\beta v^\gamma,$

$\varepsilon=ei+\gamma,\rho=yi+\beta|0=<\varepsilon-\gamma=<2^k-1]$

对于 i 的两个值，有：

$pi(\alpha,\varepsilon,\rho)=Pr[\gamma=\varepsilon-ei,\beta=\rho-yi|0=<\varepsilon-\gamma=<2^k-1]$

$=\delta(0=<\rho-yi=<M-1)*2^{-k}/M$

那么两个发布消息的距离等于

$sun=\Sigma 2|y2-y1|/2^k M=<2\Sigma 2^k S(1+2^{k'})/2^k M=<2*(1+2^{k'})/2^{2k'}=<3/2^{k'}$

相对于泄漏参数 k' 的信息这一距离可以忽略。

4 安全性和高效性分析

从应用的角度来说，选择一个 1024 位的模数 N 和 160 位长的不对称基 g 为阶更加方便。泄漏信息参数 k' 可以被固定在 64 位长，安全参数可以根据情况选择 24 位到 128 位。这样其安全性可以证明是等价于 1024 位模数的因式分解。一旦发现一种新的有效的算法对大数进行因式分解，其安全级别就一下子降到了 Schnorr 方案的程度，素数阶子群的离散对数问题。（对于识别协议未经证明为安全，但是对签名方案证明是安全的）。从证明这的角度来说，这些协议是非常有效地。事实上，如果我们仅仅考虑所需要进行的实时的运算，仅包括自然整数 N 上的一次乘法和一次加法。而且使用的数字非常小。

在表 1 中，我们对算法的效率进行了直观的分析。

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