分级群签名*

李 敏, 王尚平, 马晓静, 秦 慧
(西安理工大学 理学院, 陕西 西安 710048)

摘 要: 现有的群签名方案均假设群成员具有相同的权限,首次提出分级群签名概念,并通过在一般的群签名中加入一个授权过程实现了分级群签名。该方案中,群成员具有不等的签名权限,任何群成员均不能对一个超出自己签名权限的消息产生有效的签名,验证者可以通过公开的消息权限标志来验证签名。

关键词: 知识签名; 双线性映射; 权限; 分级群签名
中图法分类号: TP391 文献标识码: A 文章编号: 1001-3695(2006)09-0088-04

Rank Group Signature

LI Min, WANG Shang-ping, MA Xiao-jing, QIN Hui
(College of Science, Xi'an University of Technology, Xi'an Shanxi 710048, China)

Abstract: The notion of rank group signature is proposed for the first time, and a concrete scheme is given as well. Different group members have different signing ability in the scheme, and no one can sign a message out of his purview. Meanwhile, the scheme satisfies ordinary security properties of group signature.

Key words: Signature of Knowledge; Bilinear Pairings; Purview; Rank Group Signature

群签名的概念最早由 Chaum 和 Heyst 于 1991 年在文献[1]中提出。一个群签名方案允许群成员以群组的名义对一个消息进行签名,任何人均可以使用群的公钥来验证签名的合法性,但是除了群主管之外的任何人都不能得到签名者的身份信息——匿名性,而且要判断两个群签名是否是同一个群成员签署的也是计算困难的——不可联系性。为了处理可能产生的纠纷,群主管利用自己拥有的秘密信息可以确定给定的群签名的签署者,从而为仲裁提供依据——实际责任的可追究性。

自从群签名的概念提出以来,许多群签名方案被提了出来,但是早期的方案都具有一些不期望的性质,如群公钥的长度或者签名的大小依赖于群成员个数的多少;要加入一个新的群成员,至少必须改变群的公钥等。这些方案在处理较大的群时效率很低。

直到 1997 年,文献[3]第一次提出了一个签名长度和公钥长度均为固定值的群签名方案,解决了上述两个不期望的性质。2000 年,文献[4]提出了一个高效的可证明抗联合攻击的群签名方案。之后有很多方案均利用双线性映射来构造群签名,同时期处理群成员删除问题的方案也被提出[5,6]。

在基于身份的密码系统中,由于用户的公钥及对应私钥由用户的身份信息通过密钥生成中心(PKG)产生,消除了通过认证机构如 CA 获得公钥证书的需求,同时也就消除了验证证书有效性的需要。因此很多密码系统转由以身份为基础来构建。基于身份的群签名方案首先在文献[7]中提出,此方案效率很低,而且后来被证明不能保证匿名性;文献[8]也提出了一个方案,但是被证明不具有不可伪造性,也不能抵抗联合攻击。后来,双线性对尤其是 Weil 对和 Tate 对的提出,为构造基于身份的系统提供了新的工具。2003 年,文献[2]利用双线性对构造了一个基于身份的群签名方案。该方案在一些合理的安全性假设下,满足对群签名的所有安全性要求,并且效率很高。

收稿日期: 2005-08-17; 修返日期: 2005-10-16
基金项目: 国家自然科学基金资助项目(60273089);陕西省自然科学研究计划资助项目(2003F37);陕西省教育厅自然科学研究计划资助项目(03JK165)

1 动机和想法

本文所使用的分级群签名和一般的群签名的不同之处在于: 在一般的群签名方案中,所有的群成员均具有同等的签名能力,任何合法群成员均可用群的名义对任何消息进行有效签名。这样实际上存在着一种不安全的因素,如一个群成员对超过自己权限的消息签名,验证方通过验证发现签名有效,认为整个群对消息认可。但是事实上是这个群成员滥用了匿名性,而且群主管并不是总能及时地发现这个成员的不诚实行为,即使后来被发现,群主管所能做的就是删除这个不诚实的群成员以及追究可能的法律责任,但是这个时候损害可能已经发生。考虑到现实世界中群成员一般并不具有同等的权限,他不能对超出自己权限的消息进行签名,即使签了名,也不会被认可。我们首次提出分级群签名的概念,并且在方案[2]的基础上提出了一个分级群签名方案。本文所提的方案中引入了一个消息等级表,它是一个消息等级的查询表,我们可以将一些预定义的需要受权限保护的消息及其对应级别存入这个表中。

在本文提出的方案中,一个群的成员并不具有同等的签名能力,群成员的签名能力是在加入群的时候由群主管赋予的。一个群成员在对一个消息签名时,必须同时以零知识的方法证明他具有的签名权限。当一个验证者验证一个签名是否有效

时, 他首先要查询消息等级表获得消息等级标志, 然后对签名进行有效性验证。在这种情况下, 一个群成员对超出自己权限的消息的签名是不能通过验证算法的。

2　群签名定义及安全需求

定义 1　一个群数字签名方案包含以下五个步骤:

(1) 系统建立。一个概率性的算法生成公开参数, 包括共用参数、群的公开钥和群主管的一个秘密钥。

(2) 成员注册。一个概率性的用户与群主管之间的交互协议, 产生群成员的私钥和成员资格证书, 并注册新成员的身份。

(3) 签名。一个概率性的算法, 输入群公钥、成员证书及消息 m 和群成员的私钥 x, 产生一个消息 m 的签名。

(4) 验证。任何使用者均可以运行算法, 判断一个签名 sig 是否是群的合法成员签署的。

(5) 打开。一个算法, 可使群主管利用其拥有的秘密值获得给定消息的签名者的真实身份。

一个群签名方案必须满足如下的安全性需求:

(1) 正确性。合法群成员的任何签名必须都是有效的。

(2) 不可伪造性。只有合法的群成员才可以签名。

(3) 匿名性。给定一个群签名, 除群主管之外的任何人确定签名者的身份是计算困难的。

(4) 不可联系性。除群主管之外的任何人要判断两个签名是否是同一个成员签署的是计算困难的。

(5) 可追踪性。群主管总是可以打开一个有效的签名, 从而判定签名者的真实身份。

(6) 开脱性。群主管或者群成员合伙甚至他们联合起来均不能以另一个成员的名义签名, 即无陷害。也就是说, 一个群成员不能对事实上不是由他产生的签名负责。

(7) 抗联合攻击。群成员合伙甚至全部群成员联合起来也不能阻止一个有效签名的打开。

3　准备工作

3.1　双线性映射

设 G_1 是一个循环加法群, 它的阶为 q(素数), P 是其生成元。G_2 是循环乘法群, 其阶也为 q, a, b 是 Z_q^* 中的元素。我们假设离散对数问题(DLP) 在群 G_1 和群 G_2 中都是难解的。一个双线性映射是一个映射 $e: G_1 \times G_1 \rightarrow G_2$ 具有下列性质:

(1) 双线性。$e(aP, bQ) = e(P, Q)^{ab}$。

(2) 非退化。存在 $P, Q \in G_1$　满足: $e(P, Q) \neq 1$。

(3) 可计算性。对所有的 $P, Q \in G_1$, 存在高效的算法计算 $e(P, Q)$。

双线性对可以由 Weil 对或 Tate 对来构造[9,10]。

3.2　Gap Diffie-Hellman 群

设 G_1 是一个循环加法群, 它的阶为 q(素数), P 是其生成元。我们假设在群 G_1 中可以高效地计算逆元和乘法。

(1) 离散对数问题(DLP)。

给定两个元素 $P, Q \in G_1$, 求出 $n \in Z_q^*$, 使得 $Q = nP$。

(2) 计算性。Diffie-Hellman 问题(CDHP), 给定 P, aP, bP, $(a, b \in Z_q^*)$, 计算 abP。

(3) 判定性 Diffie-Hellman 问题(DDHP)。

给定: P, aP, bP, cP $(a, b, c \in Z_q^*)$

判定是否有 $c \equiv ab \bmod q$。

如果存在多项式时间算法可以解决群 G_1 中的 DDHP 问题, 但是不存在多项式时间算法以不可忽略的优势解决群 G_1 中的 CDHP 问题, 我们就称群 G_1 是一个 Gap Diffie-Hellman 群。

3.3　知识签名

许多群签名方案均使用了知识签名的概念。这个密码学工具允许一个实体向其他实体证明所拥有某个值, 同时没有泄漏关于该值的信息。下面介绍的方法是基于 Schnorr 签名方案[1,11]的结构, 这种知识签名在随机预言模型[12,13]下被证明是安全的且交互过程是零知识的。

设 $G = < g >$ 是阶为 n 的循环群, g 是 G 的生成元, y 是 G 中一个元素。以 g 为基的 y 的离散对数是使得 $g^x = y$ 成立的最小正整数 x。

定义 2　满足 $c = H(m \| y \| g \| g^s y^c)$ 的对 $(c, s) \in \{0, 1\}^k \times Z_n^*$, 称为元素 $y \in G$ 的以 g 为基的关于消息 m 的离散对数知识签名, 表示为

$$SKREP[(\alpha): y = g^{\alpha}](m)$$

如果秘密值 $x = \log_g(y)$ 已知, 则这样的签名是容易计算的。从 Z_n^* 中随机地选择 r, c 和 s 可以这样计算

$$c := H(m \| y \| g \| g^r)$$

$$s := r - cx \pmod n$$

但是如果不具有秘密值 $x = \log_g(y)$, 则计算这样的知识签名是困难的。所以, 拥有秘密值的一个实体可以提供这样的离散对数知识签名来证明自己具有该秘密值, 同时没有泄露该值。本文将利用知识签名来证明一个群成员具有的权限。

3.4　成员权限及消息等级的划分

成员权限的划分: 一个群可以设想为一个机构或组织, 具有客观上的等级划分, 这种权限划分在一个机构或组织内是相对固定的, 我们可以根据这种客观的等级来构造一棵树。树的每一个节点代表一种权限而不是一个成员, 也就是说不同的成员可以有相同的权限。不同的等级反映到树中就是树的一层, 上下级关系映射为树的父子关系。

权限标志的生成: 我们称负责产生权限和权限分发以及消息等级划分的实体为权限管理者, 他可以是群主管, 也可以是独立的第三方。我们假定群中共有 s 种权限, 设循环群 G, 阶为 q, g 是一个随机选取的 G 的生成元。权限管理者随机从 z_q^* 选择不相等的数 $x_1, x_2, \cdots, x_s$, 计算 $g^{x_i} = p_i$ $(i = 1, 2, \cdots, s)$。将这 s 个数与权限一一对应起来, 当一个成员注册的时候, 权限管理者根据成员的实际权限来分配他适当的 x_i 作为其权限。

消息等级的划分: 消息等级的划分与权限的划分密切相关, 即如果一个群成员具有权限标志 x_i, 那么他可以签署的所有消息等级标志均为 $p_i = g^{x_i}$。消息区分表是一些数据记录, 保存着消息特征及其对应等级的信息。签名的验证者可以访问这些数据记录获得消息的等级。简单的示意图如图 1 所示。

图 1 是一个简单的权限树。我们假设第一等级的权限为 x_1, 第二等级的权限为 x_2, 第三等级的权限为 x_3, 则在本文提出的群签名方案中, 只有具有第一等级权限的成员(拥有 x_1) 可以对消息 m_{1_i} 产生有效签名。

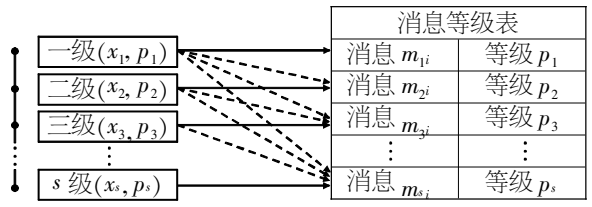

图 1 消息区分表

需要说明的是在这个示意图中,具有较高等级权限的成员也不能对等级较低的消息签名,如即使第一等级的成员也不能对第三等级的消息 m_{3_i}签名。这是由权限的分配方法决定的。另外一种可选的权限分配方法是等级较高的成员可以获得所有低于自己等级的权限。仍以图 1 为例,第一等级的成员不但可以获得 x_1,而且可以获得 x_2, x_3,在这种分配方法下,等级较高的成员可以对等级较低的消息签名(图 1 中用虚线表示)。可以根据实际需要来选择一种分配方法。

4 分级群签名方案

我们的群签名方案是基于文献[2]方案的。此方案是一个基于身份的群签名方案,在基于身份的系统中有一个密钥生成中心(PKG),在本文中,群管理同时也是 PKG。

(1) 系统建立

G_1 是一个阶为 q(素数)的 Gap Diffie-Hellman 群, P 是其生成元, G_2 是循环乘法群,其阶也为 q, g, h 均是其生成元,设 h 以 g 为基的离散对数未知。 e: $G_1 \times G_1 \rightarrow G_2$ 是一个双线性映射。定义两个哈希函数:

$H_1: \{0,1\}^* \times G_1 \rightarrow Z_q$

$H_2: \{0,1\}^* \times G_1 \rightarrow G_1$

群管理随机选择 $s \in Z_q^*$,计算 $P_{pub} = sP$,系统公开参数为 $\{G_1, G_2, e, q, P, P_{pub}, H_1, H_2\}$, s 是群主管的主密钥(保密)。

群主管按第 3.4 节的方法划分权限,并得到三元组的集合。

(2) 密钥提取

用户随机选择 $r \in Z_q^*$,发送 rP 及身份信息 ID 给群主管,群主管通过秘密信道返回给用户 $S_{ID} = sH_2(ID, rP)$,用户的私钥为 (r, S_{ID}),公钥为 $Q_{ID} = H_2(ID, rP)$。

(3) 成员注册

用户随机选择 $z \in Z_q^*$,然后发送 rzP, zP, rP, ID 给群主管,其中 ID 是用户的身份信息。群主管验证 $S_{ID} = sH_2(ID, rp)$, $e(rzP, P) = e(zP, rP)$,如果均成立,群主管根据用户身份标志 ID 通过秘密信道返回用户成员证书 (S, rzP),其中 $S = sH_2(ID, rzP)$,用户保密 (z, rz, zp),同时返回一个适当的二元组 (x_i, p_i) 作为用户的权限,其中 $p_i = g^{x_i}$。群主管将 rzP, zP, rP, ID, (x_i, p_i) 存入成员列表。

(4) 签名

假设消息 m 的等级为 p_i,为了给一个消息 m 签名,群成员根据自己的成员证书和权限执行下面的运算:

$U = k_1 rzP$ $k_1 \in_R Z_q^*$ 随机选择

$W = (q - k_1) zp$

$R = k_2 H_2(ID, rzp)$

$k_2 \in_R Z_q^* \setminus \{k_1\}$ 随机选择

$h = H_1(m, U + W)$

$V = hk_2 s + k_1 rzH_2(m, U + W + R)$

$SK = \mathrm{SKREP}[(\alpha): p_i = g^{\alpha}](m \| U \| W \| R \| V)$

对消息 m 的签名是 (U, W, R, V, SK)。

(5) 验证

验证者查询消息等级表获得消息 m 的等级标志 p_i。

验证者计算 $\bar{k} = H_1(m, U + W)$

如果

$$e(V, P) = e(R, P_{pub})^{\bar{k}} \times e(H_2(m, U + W + R), U)$$

且 $c = H(m \| p_i \| g \| g^s p_i^c)$,则签名有效。

(6) 打开

给定一个签名,群主管可以根据成员列表判断是否有

$$e(rzP, P) = e(V, P) \times e(W, rp)$$

如果找到一组 (rzp, rp) 满足上式,则可以确定签名者的身份,并可以提供如下的证据:

$$e(rzP, P) = e(V, P) \times e(W, rp)$$

$$e(S, P) = e(H_2(ID, rzp), P_{pub})$$

$$e(S_{ID}, P) = e(H_2(ID, rP), P_{pub})$$

5 安全性分析

群签名方案[2]满足在第 2 节提出的对群签名的安全性要求,而且克服了密钥生成中心(本方案中也为群主管)可以伪造成员签名的缺陷。本文提出的分级群签名方案是文献[2]方案的扩展,在其基础上增加了权限管理产生权限的过程以及在签名中加入了一个知识签名。本文所提方案的安全性与文献[2]中的结论相同。下面只简要给出方案的安全性结论,证明过程可以参考文献[2]。

结论 1 如果存在敌手 A 能以不可忽略的概率 ε伪造五元组 (ID, rp, rxp, S_{ID}, S),则可以以同样的概率 ε解决群 G_1 中的计算性 Diffie-Hellman 问题(CDHP)。

结论 2 一个群成员无论是否与 PKG 勾结,均不能以不可忽略的概率陷害另一个群成员。

结论 3 如果在群 G_1 中离散对数问题难解,则 PKG 不能伪造一个群成员的签名。

我们下面讨论一个群成员能不能对一个超出自己权限的消息产生有效的签名。显然他面临的问题是产生正确的知识签名 SK,如果 G_1 中离散对数问题难解,则知识签名在随机预言模型[12,13]下被证明是安全的。再来看群成员勾结在一起的情况。需注意的一点是群成员不能与权限管理者勾结,否则他能够获得足够高的权限来对任何消息签名。我们要讨论的问题是群成员勾结起来能不能得到比他们当中任何人的权限都高的权限。由于权限是权限管理者随机选取的 Z_p^* 中的元素,显然群成员联合起来并不能降低问题的难度,因此本文的方案并没有降低原方案的安全性。

6 结论

考虑到现实世界中一个机构或群体内部各成员并不一定具有同等权限,本文通过扩展群签名方案[2]提出一个分级群签名方案。除了具有一般群签名的特征之外,本文中所提群签名方案为每个成员赋予一定的权限,任何群成员均不能对一个超出自己权限的消息产生有效的签名,只能对符合自己权限以及低于自己权限的消息进行签名,防止了群成员滥用匿名性而导致发生无法补救的损害,提高了安全性。方案中用到了离散

对数知识签名,同时需要维护消息等级表,这在一定程度上降低了方案的效率。

参考文献:

[1] avid Chaum, E van Heyst. Group Signatures[C]. Proceedings of EUROCRYPT '91, LNCS 547, Springer-Verlag, 1991. 257-265.

[2] Zuo-wen Tan, Zhuo-Jun Liu. A Novel Identity-based Group Signature Scheme from Bilinear Maps[C]. MM Research Preprints, 2003. 250-255.

[3] Jan Camenisch, Markus Stadler. Efficient Group Signature Schemes for Large Groups[C]. Advance in Cryptology-EUROCRYPT '97, LNCS1294, Springer-Verlag, 1997. 410-424.

[4] Guiseppe Ateniese, Jan Camenisch, *et al*. A Practical and Provably Secure Group Signature Scheme[C]. Proceedings of CRYPTO '00, LNCS1880, Springer-Verlag, 2000. 255-270.

[5] Jan Camenisch, Anna Lysyanskaya. Dynamic Accumulators and Application to Efficient Revocation of Anonymous Credentials[C]. Proceedings of CRYPTO '02, LNCS2442, Springer-Verlag, 2002. 61-76.

[6] Emmanuel Bresson, Jacques Stern. Group Signatures with Efficient Revocation[C]. Proceedings of the 4th International Workshop on Practiceand Theory in Public Key Cryptography, PKC2001, LNCS1992, Springer-Verlag, 2001. 190-206.

[7] S Park, S Kim, D Won. ID-based Group Signature[J]. Electronics Letters, 1997, 33(19): 1616-1617.

[8] Y Tseng, J Jan. A Novel ID-based Group Signature[C]. International Computer Symposium, Workshop on Cryptology and Information Security, 1998. 159-164.

[9] F Hess. Efficient Identity Based Signature Schemes Based on Pairings [C]. Proc. of the 9th Workshop on Selected Areas in Cryptography-SAC 2002, LNCS 2595, Springer-Verlag, 2002. 310-324.

[10] J Cha, J H Cheon. An Identity-based Signature from Gap Diffie-Hellman Groups[C]. Public Key Cryptography-PKC 2003, LNCS 2567, Springer-Verlag, 2003. 18-30.

[11] Chen L, Pedersen T. New Group Signature Schemes[C]. Advance in Cryptology-EUROCRYPT '94, LNCS950, Springer-Verlag, 1995. 171-181.

[12] I B Damgard. Practical and Provable Secure Release of a Secret and Exchange of Signature[C]. Advances in Cryptology- CRYPTO '93, LNCS765, Springer-Verlag, 1994. 200-217.

[13] T E L Gamal. A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms[C]. Advances in Cryptology- CRYPTO '84, LNCS196, Springer-Verlag, 1985. 10-18.

作者简介:

李敏(1982-),男,河北邢台人,硕士研究生,主要研究方向为密码理论与网络安全;王尚平,男,陕西扶风人,教授,博士,主要研究方向为密码理论与网络安全;马晓静(1981-),女,江苏淮安人,硕士研究生,主要研究方向为密码理论与网络安全;秦慧(1979-),女,湖北十堰人,硕士研究生,主要研究方向为密码理论与网络安全。

(上接第 66 页)

[5] hen L, Song Z J, Liavas B. Master Assembly Model for Real-time Multi-user Collaborative Assembly Modeling on the Internet[C]. Montreal, Canada: Proceedings of the ASME Design Technical Conferences and Computers and Information in Engineering Conference, DETC/CIE-34456, 2002.

[6] Chen L, Song Z J, Feng L. Internet-enabled Real-time Collaborative Assembly Modeling via an E-assembly System: Status and Promise [J]. Computer-Aided Design, 2004, 36(9): 835-847.

[7] 董兴辉,童秉枢,高陆,等. 基于 Web 的协同装配系统及其关键技术研究[J]. 计算机集成制造系统, 2003, 9(1): 20-24.

[8] 李雄伟,刘继红,王俊峰. 基于 Web 的协同装配规划[J]. 计算机辅助设计与图形学学报, 2003, 15(3): 348-354.

[9] 王俊峰,刘继红,钟毅芳. Web 环境下的协同装配规划系统[J]. 计算机集成制造系统, 2004, 10(1): 83-87.

[10] Shyamsundar N, Gadh R. Internet-based Collaborative Product Design with Assembly Features and Virtual Design Spaces[J]. Computer-Aided Design, 2001, 33(9): 637-651.

[11] Singh P, Betting B. Port-compatibility and Connectability Based Assembly Design[J]. Journal of Computing and Information Science in Engineering, 2004, 4(3): 197-205.

[12] Fuh J Y H, Li W D. Advances in Collaborative CAD: The-State-of-The Art[J]. Computer-Aided Design, 2005, 37(5): 571-581.

[13] Li W D, Lu W F, Fuh J Y H, *et al*. Collaborative Computer-Aided Design-research and Development Status[EB/OL]. http://www.cadconferences.com, 2004.

[14] Nof S Y, Chen J. Assembly and Disassembly: An Overview and Framework for Cooperation Requirement Planning with Conflict Resolution[J]. Journal of Intelligent and Robotic Systems, 2003, 37(3): 307-320.

[15] Wang L H, Shen W M, Xie H, *et al*. Collaborative Conceptual Design— State of the Art and Future Trends[J]. Computer-Aided Design, 2002, 34(13): 981-996.

[16] 董兴辉. 协同环境下预装配方法与装配规划的研究[M]. 北京: 清华大学出版社, 2003.

[17] Xie N, Blackhurst J, Wu T. Design and Implementation of a Distributed Information System for Collaborative Product Development[J]. Journal of Computing and Information Science in Engineering, 2004, 4(4): 281-293.

[18] Zhou S Q, Chin K S, Xie Y B, et al. Internet-based Distributive Knowledge Integrated System for Product Design[J]. Computers in Industry, 2003, 50(2): 195-205.

[19] Zha X F. A Knowledge Intensive Multi-agent Framework for Cooperative/Collaborative Design Modeling and Decision Support of Assemblies[J]. Knowledge-based Systems, 2002, 15(8): 493-506.

[20] Zha X F, Lim S Y E, Lu W F. A Knowledge Intensive Multi-Agent System for Cooperative/Collaborative Assembly Modeling and Process Planning[J]. Journal of Integrated Design and Process Science, 2003, 7(1): 99-122.

[21] 董兴辉,高陆,徐晓慧,等. 协同装配信息集成建模及装配顺序规划研究[J]. 计算机辅助设计与图形学学报, 2003, 15(7): 823-827.

[22] 董兴辉,徐晓慧,田凌,等. 面向协同装配设计的信息建模[J]. 清华大学学报(自然科学版), 2004, 44(5): 620-624.

[23] Huang G Q, Mak K L. Design for Manufacture and Assembly on the Internet[J]. Computer in Industry, 1999, 38(1): 17-30.

[24] Xie S Q, Tu P L, Zhou Z D. Internet-based DFX for Rapid and Economical Tool/Mould Making[J]. Int. J. Adv. Manuf. Technol., 2004, 24: 821-829.

作者简介:

徐翱(1982-),男,硕士研究生,主要研究方向为产品协同装配设计;邱浩波(1974-),男;刘琼(1965-),女,副教授,博士;高亮(1974-),男,副教授,博士。