定该签名是PKG伪造的，则该群成员不必为他人产生的群签名承担责任。

(5)可跟踪性：PKG可以打开任何有效的群签名以确定签名者的身份，签名者不能否认他的签名。因为PKG能提供证据证明该签名的确是该群成员的签名，因为：

$e(rx_iP,P)=e(x_iP,rP)$；

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

(6)防合谋攻击：群管理员PKG知道所有群成员的私钥，群成员合谋子集不能产生一个有效的群签名，使得群管理员不能将签名与其中的一个群成员的身份联系起来。

(7)效率：传统的群签名方案中，群公钥的大小和群签名的长度与群成员的数量成正比，因此对于比较大的群或动态性很强的群效率很低。而本方案中群公钥的大小和群签名的长度是常数，不依赖于群成员的数量，群签名的算法和协议是有效的。

结论 基于身份的密码系统可以简化基于证书的密码系统繁琐的密钥管理过程。本文是在基于身份的数字签名方案的基础上，利用双线性映射的特殊性质，构造了一种新的基于身份的群签名方案，该方案是安全有效的。基于身份的签名方案能够降低证书管理开销，具有较高的执行效率，因此具有更广泛的现实意义。

参 考 文 献

1 Shamir A. Identity-based cryptosystems and signature schemes. Advances in Cryptology-Crypto 1984, LNCS 196, Springer-Verlag, 1984. 47～53

2 Boneh D, Franklin M. Identity-based encryption from the Weil pairing. Advances in Cryptology-Crypto 2001, LNCS 2139, Springer-Verlag, 2001. 213～229

3 Cha J, Cheon J H. An identity-based signature from gap Diffie-Hellman groups. Public Key Cryptography-PKC 2003, LNCS 2567, Springer-Verlag, 2003. 18～30

4 Hess F. Exponent Group Signature Schemes and Efficient Identity Based Signature Schemes Based on Pairings. Cryptology ePrint Archive, Report 2002/012

5 Chen Xiaofeng, Zhang Fangguo, Kim K. A New ID-based Group Signature Scheme from Bilinear Pairings. Cryptology ePrint Archive, Report 2003/116

6 Bellare M, Namprempre C, Neven G. Security Proofs for Identity-Based Identification and Signature Schemes. Advances in Cryptology-Eurocrypt 2004, LNCS 3027, Springer-Verlag, 2004. 268～286

7 Xu Jing, Zhang Zhenfeng, Feng Dengguo. ID-Based Proxy Signature Using Bilinear Pairings. Cryptology ePrint Archive, Report 2004/206

第六届中国Rough集与软计算学术研讨会（CRSSC2006）

征 文 通 知

由中国人工智能学会粗糙集与软计算专业委员会和中国计算机学会人工智能与模式识别专业委员会主办、浙江师范大学承办的“第六届中国Rough集与软计算学术研讨会”(CRSSC2006)拟定于2006年10月30日至11月3日在浙江金华召开。

Rough集理论自1982年由波兰数学家Zdzisław Pawlak教授提出以来，其理论模型得到不断完善和发展，并渗透到很多学科，成为研究数据挖掘、知识约简和粒计算的理论基础。Rough集理论自身也已成为完整、独立的科学领域。此外，Rough集理论与其它一些软计算理论，诸如Fuzzy集、粒计算、神经网络、遗传算法等均已经成为当前国内计算机及相关专业的研究热点。

自2001年在重庆成功召开“第一届中国Rough集与软计算学术研讨会(CRSSC2001)”以来，我国每年的CRSSC系列研讨会在规模和质量上均呈良好的增长趋势，在此领域的研究工作发展很快。2003年成立了中国人工智能学会粗糙集与软计算专业委会，Rough集的研究队伍也更加壮大，研究成果在深度和广度上有了更大的发展。

现将有关征文事宜通知如下，欢迎各界人士踊跃投稿。

一、征文范围

Rough集理论及应用；计算智能；机器学习；文字计算；Fuzzy集理论及应用；粒计算；软计算及其应用；演化计算；Petri网；软计算的逻辑基础；非经典逻辑；神经网络；计算复杂性；空间推理；统计与概率推理；智能Agent；多准则决策分析；决策支持系统；知识发现与数据挖掘；多Agent技术；近似推理与不确定性推理；网络智能；集成智能系统；数据仓库；模式识别与图像处理生物信息与生物计算；认知信息学；其他有关领域

二、征文要求

a) 未公开发表过，一般不超过6000字。

b) 论文包括中英文题目，作者姓名、单位、地址、邮编、E-mail地址、联系电话，中英文摘要（一般不超过200字）、关键词、正文和参考文献。

c) 论文请用Word排版，A4纸打印，一式两份，欢迎通过会议网站在线投稿或通过EMAIL投稿。

d) 录用论文将由《计算机科学》杂志专辑出版。

e) 征文请寄：浙江省金华市浙江师范大学信息科学与工程学院 吴小红 收 邮政编码：321004，
电子版投稿请送：crssc2006@zjnu.cn 会议网站：http://cs.cqupt.edu.cn/crssc/crssc2006

三、重要日期 截稿日期（收到）：2006年4月31日 录用日期（发出）：2006年6月10日
论文清样付印和论文注册截止日期（收到）：2006年7月10日

四、联系方式 联系人(联系电话)：梁久祯(0579-2298258)；王基一(0579-2283436)；吴小红(0579-2298903)
电子信箱：liangjz@zjnu.cn（梁久祯），xx51@zjnu.cn（王基一）