通信学报
Journal on Communications
主管单位：中国科学技术协会
主办单位：中国通信学会

于义科,郑雪峰.标准模型下基于身份的高效动态门限代理签名方案[J].通信学报,2011,(8):55~63

标准模型下基于身份的高效动态门限代理签名方案

DOI：

中文关键词：

英文关键词：

基金项目：

作者	单位
于义科	
郑雪峰	

中文摘要：

基于身份的门限代理签名方案大都是在随机预言模型下进行安全证明,并且方案中每个代理人的代理签名密钥在有效期内都是固定不变的。在Li和Jiang提出的基于身份的签名方案基础上,利用可公开验证秘密分享技术提出了一个在标准模型下可证安全的基于身份的(t,n)-动态门限代理签名方案。方案中代理人的代理签名密钥可以定期更新,而且代理签名验证过程只需要常数个双线性对运算，因此方案具有更好的动态安全性和较高的效率。

英文摘要：