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

罗长远,霍士伟,邢洪智.普适环境中基于身份的跨域认证方案[J].通信学报,2011,(9):111~115

普适环境中基于身份的跨域认证方案

DOI：

中文关键词：

英文关键词：

基金项目：

作者	单位
罗长远	
霍士伟	
邢洪智	

中文摘要：

利用椭圆曲线加法群提出了一种基于身份的签名算法，算法中签名的验证结果相对于签名者身份是一个常量，该算法可保证跨域认证中用户身份的匿名性，并且避免了复杂的双线性对运算。基于该算法设计了一种普适环境中的跨域认证方案，方案中用户利用该算法对时戳签名作为认证信息，在实现安全跨域认证的同时实现了用户匿名性。分析表明，该方案同时具有安全和效率上的优势，更加适合在普适环境下应用。

英文摘要：

查看全文 查看/发表评论 下载PDF阅读器

关闭