计算机应用研究
Application Research Of Computers

一种改进的椭圆曲线安全代理签名方案*

Improved secure proxy signature scheme based on elliptic curve

中文关键词：代理签名 椭圆曲线 椭圆曲线离散对数问题

英文关键词：proxy signature elliptic curve elliptic curve discrete logarithm problem (ECDLP)

基金项目：国家“973”计划资助项目（2007CB310704）；国家自然科学基金资助项目（90718001，60821001，U0835001）

作者	单位
胡兰兰a,b,c， 郑康锋a,b,c， 李剑a，b，胡正名a,b,c， 杨义先a,b,c	(北京邮电大学 a.网络与交换技术国家重点实验室 信息安全中心； b.网络与信息攻防技术教育部重点实验室； c.灾备技术国家工程实验室，北京 100876)

中文摘要：

为解决基于椭圆曲线的代理签名方案的安全问题，提出一种改进的抗伪造攻击的代理签名方案。该方案通过改进代理签名私钥生成方式和相应的代理签名验证等式的方法，提高了基于椭圆曲线的代理签名方案的安全性。分析表明，新方案解决了以往方案中存在的原始签名者伪造问题，满足强代理签名方案所必须的六种性质，具有无须安全通道的优点并且更为高效。分析结果说明，新方案比以往方案具有更好的安全性和更高的实用性。

英文摘要：

To overcome the secure weakness of the existing proxy signature scheme based on elliptic curve, this paper presented an improved proxy signature scheme that could avoid forgery attack. Enhanced the security of the proxy signature scheme based on elliptic curve by improving on the generate form of the private key and the corresponding verification equation of proxy signature. The analysis showed that the new scheme resolved secure problems in the former schemes, met the six aspects of security features needed by strong proxy signature scheme, did not need the support of the secure channel, and was more efficient. The analytic results prove that the new scheme is more secure and practicable.