>> 首页
>> 被收录信息
>> 投 稿 须 知
>> 模 板 下 载
>> 信 息 发 布
>> 常见问题及解答
>> 合 作 单 位
>> 产 品 介 绍
>> 编委会/董事会
>> 关 于 我 们
>> 网 上 订 阅
>> 友 情 链 接

友情链接
>> 中国期刊网
>> 万方数据资源库
>> 台湾中文电子期刊
>> 四川省计算应用研究中心
>> 维普资讯网

# 基于RSA的证实数字签名方案*

## A Confirmer Signature Scheme Based on RSA



中文关键词：证实数字签名；不可否认签名；RSA；数字签名

英文关键词：Confirmer Signature;Undeniable Signature;RSA;Digital Signature

基金项目：国家自然科学基金资助项目(10471078)；教育部高等学校博士学科点专项科研基金资助项目(20040422004)；曲阜师范大学博士科研基金资助项目

| 作者 | 单位 |
| --- | --- |
| 鞠宏伟1，李凤银2，禹继国2，曹宝香2 | (1.曲阜师范大学 资产管理处，山东 日照 276826；2.曲阜师范大学 计算机科学学院，山东 日照 276826) |

中文摘要：

验证者要知道一个证实数字签名的有效性，必须得到一个称为证实者的第三方的帮助与合作，签名者的安全性和证实签名的不可见性是一个证实数字签名方案必须具备的两个重要特性。提出了一种完全基于RSA的证实数字签名方案，分析表明，该方案是一种安全而高效的证实数字签名实现方案。

英文摘要：

Without the help and cooperation of a designated confirmer, a verifier cannot determine the validity of a confirmer signature. The subscriber’s security and the confirmer signature invisibility are characteristic to a confirmer signature scheme. A confirmer signature scheme based on RSA is proposed. It is showed that the new scheme is an implementation of secure and efficient confirmer signature.

关闭