基于身份的强指定验证人签名方案*

Identity-based strong designated verifier signature schemes

中文关键词：基于身份的签名 指定验证人签名 代理签名 双线性对

英文关键词：identity-based signature designated verifier signature proxy signature bilinear pairings

基金项目：国家自然科学基金资助项目（60873119）；陕西省自然科学基础研究计划资助项目（2007A06）

作者	单位
毛卫霞，李志慧 ，薛婷	（陕西师范大学 数学与信息科学学院，西安 710062）

中文摘要：

在有些情况下，需要将验证者限定为某一个人。 利用基于身份的密码体制，提出了一种强指定验证人签名和一种强指定验证人多重代理签名，并对其安全性进行了分析。 在签名代价和验证代价上，提出的强指定验证人签名比Kang等人的方案要低。提出的强指定验证人多重代理签名可以同时授权给n个代理人，可以有效防止代理签名人对签名权的滥用。

英文摘要：

We should specify a verifier in some circumstances. Using identity-based cryptography, this paper proposed a strong designated verifier signature and a strong designated verifier multi-proxy signature. It also analyzed the proposed schemes. The proposed strong designated verifier signature scheme was lower than Kang et al.’s scheme in the signing cost and verifying cost. The proposed strong designated verifier multi-proxy signature scheme could delegate n proxy signers. Thus it could prevent proxy signers abusing signing authority.