计算机工程 2007 33 (22): 172-174,189 ISSN: 1000-3428 CN: 31-1289/TP 首页 当期目录 上一期 下一期

安全技术

适用于Smart Card的有效电子现金解决方案

吕敏芳，曹珍富

(上海交通大学计算机工程系可信任数字技术实验室，上海 200400)

收稿日期 修回日期 网络版发布日期 2007-11-19 接受日期

摘要 提出了一个可以在低计算能力、低存储量的硬件(如smart card)上实现的离线电子现金方案。该方案中，电子现金的存储量和效率都比一般的方案优很多，能满足电子现金所需要的安全特性，如匿名性、不可伪造性、多次消费检测等。该文还提出了一个类似的电子票据方案以及通过代理机构代理银行发布电子货币的方案。

关键词 电子现金；哈希树；Schnorr签名算法

分类号 TP309

DOI:

通讯作者:

作者个人主页: 吕敏芳;曹珍富