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

田有亮,马建峰,彭长根,陈 曦.椭圆曲线上的信息论安全的可验证秘密共享方案[J].通信学报,2011,(12):96~102

椭圆曲线上的信息论安全的可验证秘密共享方案

DOI：

中文关键词：

英文关键词：

基金项目：

作者 **单位**

田有亮，马建峰，彭长根，陈 曦

中文摘要：

基于椭圆曲线上的双线性对技术，构造一种可验证秘密共享方案。该方案的信息率为2/3，与Pederson的方案(Crypto91)及相关方案相比，本文方案在相同的安全级别下有较高的信息率，从而提高了秘密共享协议的效率。同时，理论上证明该方案是信息论安全的。最后，将上述方案推广到无可信中心的情况，设计了无可信中心的秘密共享方案。经分析表明，所提方案具有更高的安全性和有效性，能更好地满足应用需求。

英文摘要：

查看全文 查看/发表评论 下载PDF阅读器

关闭