

研究简报

利用身份证进行密钥分配的新方案

杨义先

北京邮电学院信息工程系 北京

收稿日期 1987-4-27 修回日期 1987-9-7 网络版发布日期 2010-4-13 接受日期

摘要

本文给出了两类利用身份证进行密钥分配的新方案,并将它们推广到会议密钥分配方案中去。

关键词 [密码](#) [密钥分配](#) [保密通信](#) [身份证](#) [会议密钥](#)

分类号

NEW SCHEMES FOR IDENTITY-BASED KEY DISTRIBUTION

Yang Yixian

Beijing University of Posts and Telecommunications Beijing

Abstract

Two classes of identity-based key distribution schemes and the corresponding conference key distribution schemes are proposed in this paper.

Key words [Cryptography](#) [Key distribution](#) [Privacy communication](#) [Conference key](#) [Identity](#)

DOI:

扩展功能

本文信息

▶ [Supporting info](#)

▶ [PDF\(695KB\)](#)

▶ [参考文献\[PDF\]](#)

▶ [参考文献](#)

服务与反馈

▶ [把本文推荐给朋友](#)

▶ [加入我的书架](#)

▶ [加入引用管理器](#)

▶ [复制索引](#)

▶ [Email Alert](#)

相关信息

▶ [本刊中 包含“密码”的 相关文章](#)

▶ 本文作者相关文章

· [杨义先](#)

通讯作者

作者个人主

页