

安全技术

DSS签字标准在密钥交换协议中的应用研究

程 辉<sup>1</sup>, 欧阳旦<sup>2</sup>

(1. 解放军信息工程大学电子技术学院, 郑州 450004; 2. 空军电子技术研究所, 北京 100089)

收稿日期 修回日期 网络版发布日期 2006-10-16 接受日期

**摘要** 密钥的安全分配是采用密码技术保证通信安全的重要环节, 文章介绍了一种将DSS签字标准与Diffie-Hellman协议相结合的密钥交换协议, 指出其在前向安全性上的不足。在此基础上, 提出了一种密钥交换协议设计方案, 并对其安全和计算量作了简要分析。

**关键词** [密钥交换](#) [数字签名](#) [数字签字标准](#) [离散对数](#)

分类号

**DOI:**

对应的英文版文章: [2006-20-061](#)

通讯作者:

作者个人主页: [程 辉<sup>1</sup>](#); [欧阳旦<sup>2</sup>](#)

扩展功能

本文信息

- ▶ [Supporting info](#)
- ▶ [PDF \(106KB\)](#)
- ▶ [\[HTML全文\] \(0KB\)](#)
- ▶ [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](#)
- ▶ [引用本文](#)
- ▶ [Email Alert](#)
- ▶ [文章反馈](#)
- ▶ [浏览反馈信息](#)

相关信息

- ▶ [本刊中 包含“密钥交换”的 相关文章](#)
- ▶ 本文作者相关文章
  - [程 辉](#)
  - [欧阳旦](#)