

博士论文

基于DSA的扩展自证明签名方案

侍伟敏, 钮心忻, 杨义先, 高海英

(北京邮电大学信息安全中心, 北京 100876)

收稿日期 修回日期 网络版发布日期 2006-9-25 接受日期

**摘要** 自证明签名对验证者来说一次仅验证了两个签名,而在PMI系统中,验证者除了要认证用户身份,其中包括两个验证:一个是验证用户的签名,另一个是验证CA颁发的公钥证书,还需要验证AA颁发的属性证书。针对此问题,该文对自证明签名做了一定的扩展,提出了扩展自证明签名ESCS方案,ESCS由验证两个签名扩展到可同时验证3个签名,此后又对ESCS方案做了进一步的扩展,扩展后的ESCS方案可以同时验证多个签名。

**关键词** [扩展自证明签名](#) [DSA](#) [PMI](#) [PKI](#)

**分类号** [TP309.3](#)

**DOI:**

对应的英文版文章: [2006-19-002](#)

通讯作者:

作者个人主页: 侍伟敏; 钮心忻; 杨义先; 高海英

扩展功能

本文信息

- ▶ [Supporting info](#)
- ▶ [PDF\(107KB\)](#)
- ▶ [\[HTML全文\]\(0KB\)](#)
- ▶ [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“扩展自证明签名”的相关文章](#)
- ▶ [本文作者相关文章](#)

- [侍伟敏](#)
- [钮心忻](#)
- [杨义先](#)
- [高海英](#)