计算机工程　2009 35 (24): 174-175　ISSN: 1000-3428　CN: 31-1289/TP　首页　当期目录　上一期

安全技术

密钥托管可控的跨域通信IBE模型

王 兴1，丁 宏1，李 欣2

(1. 杭州电子科技大学计算机学院，杭州 310018；2. 公安部第三研究所信息网络安全研发中心，上海 201204)

收稿日期　修回日期　网络版发布日期　接受日期

摘要　与传统的公钥密码体系相比，基于身份加密(IBE)具有许多优点，但目前提出的IBE模型都未能消除密钥托管。针对该问题，提出一种新的IBE模型，该模型可以控制密钥托管的范围或完全消除密钥托管，通过区域划分和域间互信，实现跨域互连，并给出在此基础上的对等密钥协商协议。分析结果表明，该模型未增加额外的结构，也未增加密钥协商的计算量或通信开销。

关键词　密钥管理；基于身份加密；密钥托管；密钥协商

分类号　TP309.2

DOI:

通讯作者:

作者个人主页: 王 兴1;丁 宏1;李 欣2