<<基于身份的公钥密码体制的研究>>

图书基本信息

书名：<<基于身份的公钥密码体制的研究>>

13位ISBN编号：9787564711184

10位ISBN编号：7564711183

出版时间：2012-4

出版时间：电子科技大学出版社

作者：杨浩淼，邱乐德 著

页数：260

内容概要

在传统的公钥密码学中，公钥是与身份无关的随机字符串，公钥基础设施(PKI)通过签证中心颁发公钥证书来绑定公钥和身份。
而在基于身份密码学(IBC)中，公钥是代表用户身份的任意字符串，可以直接从身份中提取，则证书和公钥目录是不必要的，因此简化了公钥的管理，并由此带来了不需要密钥信道的非交互式通信以及不需要证书校验，节约了计算和通信成本。
尽管IBC简化了公钥和证书的管理，相比较传统的PKI有着天然的优势，但是具体的基于身份密码系统在实施中存在一些公开问题，例如缺乏有效的非交互式密钥吊销的完整解决方案，缺乏有效的可验证加密签名方案，这些问题不解决，基于身份密码系统在实践中的应用将受到很大限制。
另一方面，双线性映射和基于标准模型的可证明安全是近几年密码学界的研究热点。

<<基于身份的公钥密码体制的研究>>

书籍目录

编辑推荐

《基于身份的公钥密码体制的研究》著获得国家自然科学基金资助，四川省2012年度第一批图书出版重点规划项目。

版权说明