学校编码：10384　　分类号_____密级_____
学　　号：23020071151271　　UDC _____

厦门大学

硕　士　学　位　论　文

P2P 网络中基于无证书的分布式密钥管理

Certificateless-Based Distributed Key Management In P2P Networks

梁 晨

指导教师姓名：黎忠文　　教授
专　业　名　称：计算机系统结构
论文提交日期：2010 年　5　月
论文答辩时间：2010 年　6　月
学位授予日期：2010 年　　月

答辩委员会主席：_____
评　　阅　　人：_____

2010 年 6 月

厦门大学学位论文原创性声明

本人呈交的学位论文是本人在导师指导下，独立完成的研究成果。本人在论文写作中参考其他个人或集体已经发表的研究成果，均在文中以适当方式明确标明，并符合法律规范和《厦门大学研究生学术活动规范（试行）》。

另外，该学位论文为（　　）课题（组）的研究成果，获得（　　）课题（组）经费或实验室的资助，在（　　）实验室完成。（请在以上括号内填写课题或课题组负责人或实验室名称，未有此项声明内容的，可以不作特别声明。）

声明人（签名）：

年　　月　　日

厦门大学学位论文著作权使用声明

本人同意厦门大学根据《中华人民共和国学位条例暂行实施办法》等规定保留和使用此学位论文，并向主管部门或其指定机构送交学位论文（包括纸质版和电子版），允许学位论文进入厦门大学图书馆及其数据库被查阅、借阅。本人同意厦门大学将学位论文加入全国博士、硕士学位论文共建单位数据库进行检索，将学位论文的标题和摘要汇编出版，采用影印、缩印或者其它方式合理复制学位论文。

本学位论文属于：

（　　）1.经厦门大学保密委员会审查核定的保密学位论文，于　　年　　月　　日解密，解密后适用上述授权。

（　　）2.不保密，适用上述授权。

（请在以上相应括号内打“√”或填上相应内容。保密学位论文应是已经厦门大学保密委员会审定过的学位论文，未经厦门大学保密委员会审定的学位论文均为公开学位论文。此声明栏不填写的，默认为公开学位论文，均适用上述授权。）

声明人（签名）：

年　　月　　日

摘　要

目前，P2P 网络的应用越来越广泛，P2P 技术已经对互联网产生了深刻的影响。但 P2P 网络具有分散性、自治性和动态性等特点，这些特点带来的安全问题已严重影响到 P2P 网络的进一步发展，因此 P2P 网络的安全问题受到越来越多的重视。传统的公钥基础设施（PKI）需要用证书来绑定身份和公钥，这使得 PKI 的证书管理十分复杂，包括证书的分发、存储、验证、更新以及撤销，这些问题妨碍了 PKI 在 P2P 网络中实施的高效性。基于身份的公钥密码体制（ID-PKC）虽然摒弃了证书，但由于其固有的密钥托管性质，使得私钥生成中心（PKG）可能伪造节点的签名，或者解密节点的加密信息，因此 ID-PKC 很难为 P2P 网络提供足够的安全性。为了适应 P2P 网络的特点，本文对基于无证书公钥密码体制（CL-PKC）的密钥管理方案进行了研究，主要做了以下几点工作：

（1）提出了一种适应 P2P 网络特点的基于无证书的多可信中心密钥生成方案，并分析了该方案的安全性。我们的方案引入了门限技术，利用混合 P2P 网络中的超级节点担任密钥生成中心（KGC, Key Generate Center），即符合混合 P2P 网络的特点，又能有效地避免单可信中心存在的单点失效以及主密钥泄露等危险。

（2）提出了一种改进的交互的跨域密钥协商协议，并在安全性和计算效率方面，与现有的几种密钥协商协议进行了比较。本文提出的协议允许不同域的公共参数中的生成元参数可以不同，具有更好的适用性。

（3）对提出的密钥管理方案进行具体设计与实现，验证这些方案的正确性，并测试它们的计算效率。本文的系统模型将主密钥份额管理和节点密钥管理结合起来，构造了一个完整的基于无证书的密钥管理模型，为解决 P2P 网络安全的问题进行了尝试性的探索。

关键词：P2P 网络；无证书公钥密码体制；密钥管理；会话密钥

Abstract

Nowadays, the application of P2P networks becomes more and more extensive. P2P technology has already had a profound impact on the Internet. However, P2P networks have characteristics of decentralization, autonomy and dynamicity. The security problems caused by these characteristics have seriously affected further development of P2P networks. Therefore, the security problem of P2P networks attracts more and more attention. Traditional Public Key Infrastructure (PKI) needs a certificate to bind an identity and its public key, and certificate management in PKI is very complicated, including certificate distribution, certificate storage, certificate verification, certificate update, and certificate revocation. These problems prevent implementing PKI in the P2P network efficiently. Although Identity-Based Public Key Cryptography (ID-PKC) abandons certificates, because of its inherent nature of key escrow, Private Key Generator (PKG) can not only forge the signature of any entity, but also decrypt any encrypted message. So, ID-PKC can not supply efficient security for P2P networks. In order to fit the characteristics of P2P networks, we do research on Certificateless-based (CL-PKC) key management schemes. The specific tasks consist of the following:

（1）We proposed a certificateless-based key distribution scheme with multiple trusted centers that fits the characteristics of P2P networks, and analysed its security. The proposed scheme introduced the threshold technology, and uses super nodes in hybrid P2P network as Key Generation Center (KGC). So it does not only fit the characteristics of P2P networks, but also avoids risks of single-point failure and master key leaking in one trusted center model.

（2）We proposed an improved interactive key agreement protocol across multiple domains, and then compared it with some existing key agreement protocol from aspects of security and computational efficiency. The proposed scheme allows different generators in common parameters of different domains.

（3）We implemented the proposed key management schemes, then verified their

correctness and tested their computational efficiency. Combined master key share management and key managenment of nodes, this system constructed a complete certificateless-based key management model, which is an exploration to solve security problems in P2P networks.

Keywords：P2P Networks；CL-PKC；Key Management；Session Key

目 录

Contents