

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

厦门大学博硕士学位论文摘要库

## 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

厦门大学博硕士学位论文摘要库

## 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

厦门大学博硕士学位论文摘要库

## 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

厦门大学博硕士学位论文摘要库



## 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 management 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

厦门大学博硕士学位论文摘要库

## 目 录

<b>第一章 引言</b> .....	<b>1</b>
<b>1.1 P2P 网络的安全问题</b> .....	<b>1</b>
<b>1.2 公钥密码学</b> .....	<b>2</b>
1.2.1 公钥基础设施 .....	3
1.2.2 基于身份的公钥密码体制 .....	4
1.2.3 无证书的公钥密码体制 .....	5
<b>1.3 本文的研究内容</b> .....	<b>6</b>
<b>1.4 本文的组织结构</b> .....	<b>8</b>
<b>第二章 P2P 网络体系结构与认证</b> .....	<b>11</b>
<b>2.1 P2P 的网络结构</b> .....	<b>11</b>
2.1.1 集中式 P2P 网络 .....	11
2.1.2 完全分布式非结构化 P2P 网络 .....	12
2.1.3 完全分布式结构化 P2P 网络 .....	12
2.1.4 混合式 P2P 网络 .....	13
<b>2.2 数学基础</b> .....	<b>14</b>
2.2.1 椭圆曲线离散对数问题 .....	14
2.2.2 双线性映射 .....	15
2.2.3 双线性 Diffie-Hellman 问题 .....	15
2.2.4 秘密共享方案 .....	15
2.2.5 哈希函数 .....	16
<b>2.3 CL-PKC 的研究现状</b> .....	<b>17</b>
2.3.1 无证书方案基本步骤 .....	17
2.3.2 信任模型 .....	18
<b>第三章 多可信中心的分布式密钥生成方案</b> .....	<b>19</b>
<b>3.1 设计目标与系统模型</b> .....	<b>19</b>

3.1.1 设计目标.....	19
3.1.2 系统模型.....	21
<b>3.2 基于无证书的多可信中心的分布式密钥生成方案 .....</b>	<b>22</b>
3.2.1 密钥分配方案.....	22
3.2.2 安全性分析.....	23
<b>3.3 (<math>\tau, N</math>) 门限的动态调整.....</b>	<b>24</b>
3.3.1 主密钥份额生成.....	24
3.3.2 主密钥份额更新.....	25
3.3.3 门限参数的选择.....	26
<b>3.4 节点密钥的撤销与更新 .....</b>	<b>27</b>
3.4.1 节点密钥的撤销.....	27
3.4.2 节点密钥的更新.....	28
<b>第四章 节点的会话密钥协商.....</b>	<b>31</b>
<b>4.1 密钥协商 .....</b>	<b>31</b>
4.1.1 非交互的域内密钥协商.....	31
4.1.2 非交互的跨域密钥协商.....	32
4.1.3 交互的域内密钥协商.....	33
4.1.4 交互的跨域密钥协商.....	34
<b>4.2 生成元不同的跨域密钥协商 .....</b>	<b>35</b>
4.2.1 系统模型.....	35
4.2.2 协议描述.....	35
4.2.3 安全性分析.....	36
<b>4.3 五个协议的分析与比较 .....</b>	<b>37</b>
4.3.1 安全性比较.....	37
4.3.2 计算效率比较.....	39
<b>第五章 P2P 网络密钥管理的设计与实现.....</b>	<b>41</b>
<b>5.1 系统方案选择 .....</b>	<b>41</b>
5.1.1 系统开发环境.....	41

5.1.2 椭圆曲线库 .....	41
5.1.3 类型说明 .....	42
<b>5.2 多可信中心的分布式密钥生成方案 .....</b>	<b>45</b>
5.2.1 系统设计与实现 .....	45
5.2.2 实验数据分析 .....	50
<b>5.3 节点的会话密钥协商 .....</b>	<b>51</b>
5.3.1 系统设计与实现 .....	51
5.3.2 实验数据分析 .....	51
<b>第六章 总结与展望 .....</b>	<b>53</b>
6.1 论文总结 .....	53
6.2 进一步的工作 .....	53
<b>参考文献 .....</b>	<b>55</b>
<b>攻读硕士学位期间的研究成果 .....</b>	<b>61</b>
<b>致谢 .....</b>	<b>62</b>

厦门大学博硕士学位论文摘要库

## Contents

<b>Chapter1 Introduction.....</b>	<b>1</b>
<b>1.1 Security Problems in P2P Networks .....</b>	<b>1</b>
<b>1.2 Public Key Cryptography .....</b>	<b>2</b>
1.2.1 Public Key Infrastructure .....	3
1.2.2 Identity-Based Cryptography .....	4
1.2.3 Certificateless Public Key Cryptography.....	5
<b>1.3 Research and Innovation .....</b>	<b>6</b>
<b>1.4 Structure of Thesis.....</b>	<b>8</b>
<b>Chapter2 Architecture and Authentication in P2P Networks .....</b>	<b>11</b>
<b>2.1 Architecture of P2P Networks .....</b>	<b>11</b>
2.1.1 Centralized P2P Networks .....	11
2.1.2 Decentralized Structured P2P Networks.....	12
2.1.3 Decentralized Unstructured P2P Networks.....	12
2.1.4 Hybrid P2P Networks .....	13
<b>2.2 Basic Mathematics Knowledge.....</b>	<b>14</b>
2.2.1 The Discrete Logarithm Problem on Elliptic Curve Groups .....	14
2.2.2 Bilinear Pairing .....	15
2.2.3 The Bilinear Diffie-Hellman Problem .....	15
2.2.4 Secret Sharing Schemes .....	15
2.2.5 Hash Functions.....	16
<b>2.3 Research Status of CL-PKC .....</b>	<b>17</b>
2.3.1 Basic Steps of Certificateless Schemes.....	17
2.3.2 Trust Model.....	18
<b>Chapter3 The Key Distribution Scheme with Multiple Trusted</b>	

<b>Centers .....</b>	<b>19</b>
<b>3.1 Design Target and System Model.....</b>	<b>19</b>
3.1.1 Design Target .....	19
3.1.2 System Model .....	21
<b>3.2 A Certificateless-Based Key Distribution Scheme with Multiple KGCs .....</b>	<b>22</b>
3.2.1 The Key Distribution Scheme.....	22
3.2.2 Security Analysis .....	23
<b>3.3 Dynamic Adjustment of (t,n)-Threshold .....</b>	<b>24</b>
3.3.1 Generate Master Key Share .....	24
3.3.2 Renew Master Key Share.....	25
3.3.3 Selection of Threshold Parameters .....	26
<b>3.4 Revocation and Renovation of Private Keys.....</b>	<b>27</b>
3.4.1 Revocation of Private Keys .....	27
3.4.2 Renovation of Private Keys .....	28
<b>Chapter4 Key Agreement Protocol .....</b>	<b>31</b>
<b>4.1 Key Agreement.....</b>	<b>31</b>
4.1.1 Non-interactive Key Agreement in One Domain.....	31
4.1.2 Non-interactive Key Agreement across Multiple Domains.....	32
4.1.3 Interactive Key Agreement in One Domain.....	33
4.1.4 Interactive Key Agreement across Multiple Domains.....	34
<b>4.2 Key Agreement across Multiple Domains with Different Generators.....</b>	<b>35</b>
4.2.1 System Model .....	35
4.2.2 Protocol Discription .....	35
4.2.3 Security Analysis .....	36
<b>4.3 Analysis and Comparison of Protocols .....</b>	<b>37</b>
4.3.1 Comparison of Security .....	37
4.3.2 Comparison of Computational Efficiency .....	39
<b>Chapter5 Implementation of Key Management in P2P Networks ...</b>	<b>41</b>



Degree papers are in the "[Xiamen University Electronic Theses and Dissertations Database](#)". Full texts are available in the following ways:

1. If your library is a CALIS member libraries, please log on <http://etd.calis.edu.cn/> and submit requests online, or consult the interlibrary loan department in your library.
2. For users of non-CALIS member libraries, please mail to [etd@xmu.edu.cn](mailto:etd@xmu.edu.cn) for delivery details.

厦门大学博硕士论文摘要库