**华 中 科 技 大 学**

**网络空间安全学院**

本科：《网络安全程序设计》报告

题目：基于OpenSSL的安全聊天系统

姓 名 邬雪菲

班 级 网安2104

学 号 U202112131

联系方式 18172029686

分 数

评 分 人

2024年11月30日

**报告要求**

**1. 报告不可以抄袭，发现雷同者记为0分。**

**2. 报告中不可以只粘贴大段代码，应是文字与图、表结合的，需要说明流程的时候，也应该用流程图或者伪代码来说明；如果发现有大段代码粘贴者，报告需重写。**

**3. 报告格式严格按照要求规范，并作为评分标准。**

**报告评分表**

|  |  |  |  |
| --- | --- | --- | --- |
| **评分项目** | **分值** | **评分标准** | **得分** |
| 设计原理 | 15 | 15-13：统流程清晰，报文处理过程描述清楚；  12-10：系统流程比较清晰，报文处理过程描述比较清楚；  9-0：描述简单 |  |
| 系统设计 | 15 | 15-13：系统结构设计描述详细、清楚、完整，前后关系清晰；  12-10：系统结构设计比较清楚，关键模块、流程等都进行了描述；  9-0：系统结构设计描述比较简单或不完整 |  |
| 详细设计与实现 | 15 | 15-13：关键模块设计描述详细、清楚、完整，前后关系清晰；  12-10：关键模块设计比较清楚，关键模块、流程等都进行了描述；  9-0：关键模块设计描述比较简单或不完整 |  |
| 问题分析与解决 | 20 | 20-16：问题描述准确，原因分析清晰，解决方法正确；  15-12：问题描述较准确，原因分析较清晰，解决方法较合理；  11-0：问题描述简单，原因分析不清，解决方法不合理； |  |
| 系统测试 | 15 | 15-13：任务完成，针对任务点的测试，对结果有分析  12-10：针对任务点的测试截图，没分析  9-0：测试很简单，没有覆盖任务点 |  |
| 心得体会 | 10 | 10-8：体会真实具体  7-5：体会比较空洞  4-0：没有写什么体会 |  |
| 格式规范 | 10 | 依据标题、正文、图、表、目录格式符合规范的程度评分 |  |
| **总 分** | | |  |
| **评分人：** | | | |

目 录

[1 设计目的和要求 1](#_Toc182238935)

[1.1 设计目的 1](#_Toc182238936)

[1.2 设计要求 1](#_Toc182238937)

[2 设计原理 2](#_Toc182238938)

[2.1 技术原理 2](#_Toc182238939)

[2.2 环境与工具 2](#_Toc182238940)

[3 系统设计 3](#_Toc182238941)

[3.1 系统结构设计 3](#_Toc182238942)

[3.2 核心数据流程 3](#_Toc182238943)

[4 详细设计与实现 4](#_Toc182238944)

[4.1 关键模块流程 4](#_Toc182238945)

[4.2 关键数据结构 4](#_Toc182238946)

[4.3 模块接口设计 4](#_Toc182238947)

[5 问题分析与解决 5](#_Toc182238948)

[5.1 XXX问题 5](#_Toc182238949)

[6 系统测试 6](#_Toc182238950)

[6.1 测试环境 6](#_Toc182238951)

[6.2 功能测试 6](#_Toc182238952)

[6.3 性能测试 6](#_Toc182238953)

[7 心得体会及意见建议 7](#_Toc182238954)

# 设计目的和要求

## 设计目的

1. 通过课程学习，使学生以 Linux 操作系统为对象，从整体上认识网络通信从应用层 API 到内核协议栈的层次结构、工作原理和运行机制，了解网络通信面临的安全威胁，建立网络安全程序设计的思想；
2. 通过实践，让学生了解主要的网络安全程序设计技术及解决安全威胁的技术思路，使学生能够将安全理论应用于实践，培养相应的程序设计能力，提升工程实践能力；
3. 通过课堂讲授与课外文献检索阅读，使学生了解与本课程相关的计算机领域的前沿发展；
4. 通过规范化的文献阅读报告以及课外实践报告，培养学生良好的文档习惯以及撰写规范文档的能力。

## 设计要求

实现一款基于OpenSSL的安全聊天系统，满足以下要求：

1. Windows或Linux平台均可
2. 点到点模式
3. 基于OpenSSL的安全套接字通信
4. 客户端服务器双向认证
5. 聊天记录本地加密存储，输入正确口令可查看

# 设计原理

## 技术原理

### SSL/TLS协议

SSL（Secure Sockets Layer）和TLS（Transport Layer Security）协议是用于在网络上进行安全通信的协议，它们在传输层对数据进行加密，以防止数据在传输过程中被截获或篡改。协议的工作流程主要包括以下几个步骤：

1. 握手过程：在数据传输开始之前，客户端和服务器通过一系列的消息交换来协商加密算法、生成会话密钥，并进行身份验证。
2. 密钥交换：使用公钥加密技术，客户端和服务器交换密钥信息，以确保密钥的安全传输。
3. 数据加密：一旦密钥交换完成，双方使用协商的密钥对数据进行加密和解密，确保数据的机密性。

在本次实验中，借助了OpenSSL来实现SSL协议。OpenSSL是一个强大的开源工具包，广泛应用于实现安全通信，支持SSL和TLS协议，同时提供了丰富的加密算法、协议实现以及证书管理功能，使得开发者能够轻松地在应用程序中集成安全通信功能。

### AES算法

AES（Advanced Encryption Standard）作为一种广泛采用的对称加密算法，其设计初衷是为了提供一种高效且安全的加密手段，用于保护敏感数据。AES算法的加密过程涉及一系列复杂的数学运算，包括字节替换、行移位、列混淆和轮密钥加，这些步骤在多轮迭代中执行，每一轮都利用密钥的不同部分来增强加密的复杂度和安全性。这种多轮加密的设计显著增加了破解的难度，因为攻击者需要尝试的密钥组合数量呈指数级增长。

为实现安全性，对本地存储的聊天记录采用PyCryptodome 库中的 AES算法来加密，采用ECB（Electronic Codebook）模式。ECB模式是一种简易的加密模式，每个块独立加密，这种模式的优势在于其加密过程的并行性，即不同的数据块可以同时被加密，更适用于对处理速度要求高的系统。

### 数字证书和双向认证

数字证书由可信的证书颁发机构（CA）签发，这些CA是经过权威认证的机构，负责验证申请证书的实体的身份，并为它们颁发数字证书。这些证书包含了实体的公钥、身份信息以及CA的数字签名等。

在双向认证中，客户端和服务器都需要向对方提供数字证书以证明其身份。这个过程包括证书验证和身份验证两个过程。

证书验证是双向认证中的一个核心环节。它确保了证书的签发者是可信的，证书没有过期，且未被列入撤销列表。这一过程通过检查证书中的签发者信息、有效期、撤销状态和路径验证来完成。一旦证书被验证为有效，通信双方就会使用证书中的公钥来加密一个预主密钥，并在握手过程中交换这个密钥。这个预主密钥随后用于生成用于加密通信的对称密钥，从而确保了通信的机密性和完整性。

身份验证通过证书中的公钥来实现。在SSL/TLS握手过程中，服务器首先使用客户端的公钥加密一个随机生成的预主密钥，并发送给客户端。客户端随后使用自己的私钥解密这个预主密钥，得到用于加密通信的对称密钥。这一过程不仅验证了服务器的身份，也确保了客户端的身份被服务器所认可。

双向认证的实施显著提高了通信的安全性。它防止了中间人攻击，因为攻击者无法提供有效的数字证书来冒充合法的通信方。

## 环境与工具

主机：Windows 11 Home, 64-bit (Build 22631.4460) 10.0.22631

集成开发环境：Visual Studio Code 1.90.1 (user setup)

虚拟机：

VMware Workstation 17 Pro 17.0.0 build-20800274

操作系统：Ubuntu 20.04.1 LTS 内核版本：5.4.0-54-generic

依赖工具包：

Python 3.8.10

cryptography 44.0.0

pycryptodome 3.9.9

# 系统设计

## 系统结构设计

由于本实验要求实现点到点通信，故每个节点即可以为服务器也可以是客户端，不需要一个公共服务器进行通信转发，而是每个节点之间直接连接。但是注意到即使是p2p模式，也需要有一个发送方主动发起连接到接收方的监听端口，而不是两者同时监听和发送连接。故程序需要有一段主控代码来设置客户端的模式。

那么系统结构可分为客户端、服务器以及消息查看这三个主要部分，两者仅在监听和发送连接请求方面有所不同，都支持SSL/TLS连接、收发消息、消息加密存储等功能。

系统的结构设计图如图3-1所示：

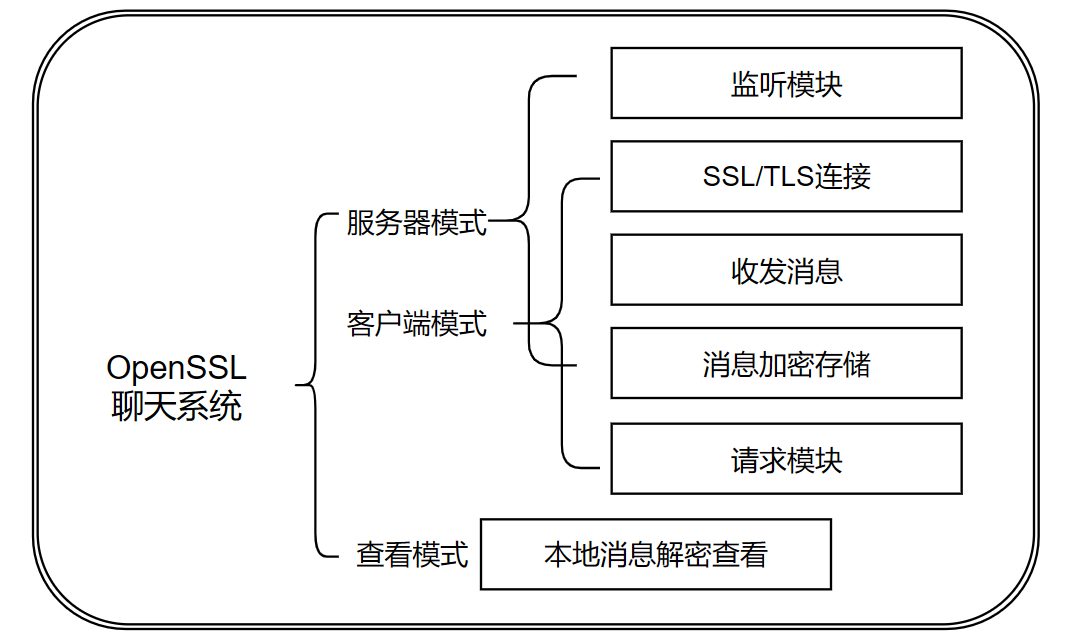


图3-1 系统结构设计图

## 核心数据流程

在聊天进行时，需要两个节点程序分别启动服务器模式和客户端模式以进行通信。两者的通信流程如下：

1. 服务器端开始监听指定端口；
2. 客户端向目标服务器IP和端口发送连接请求；
3. 服务器监听到连接请求，返回服务器证书并请求客户端证书；
4. 客户端验证服务器发送的证书是否有效/正确；
5. 客户端向服务器交换密钥信息；
6. 客户端向服务器发送客户端证书；
7. 服务器验证客户端的证书；
8. 双方确认连接；
9. 双方开始使用共享密钥通信。

双方在SSL/TLS下的通信时序图如图3-2所示：

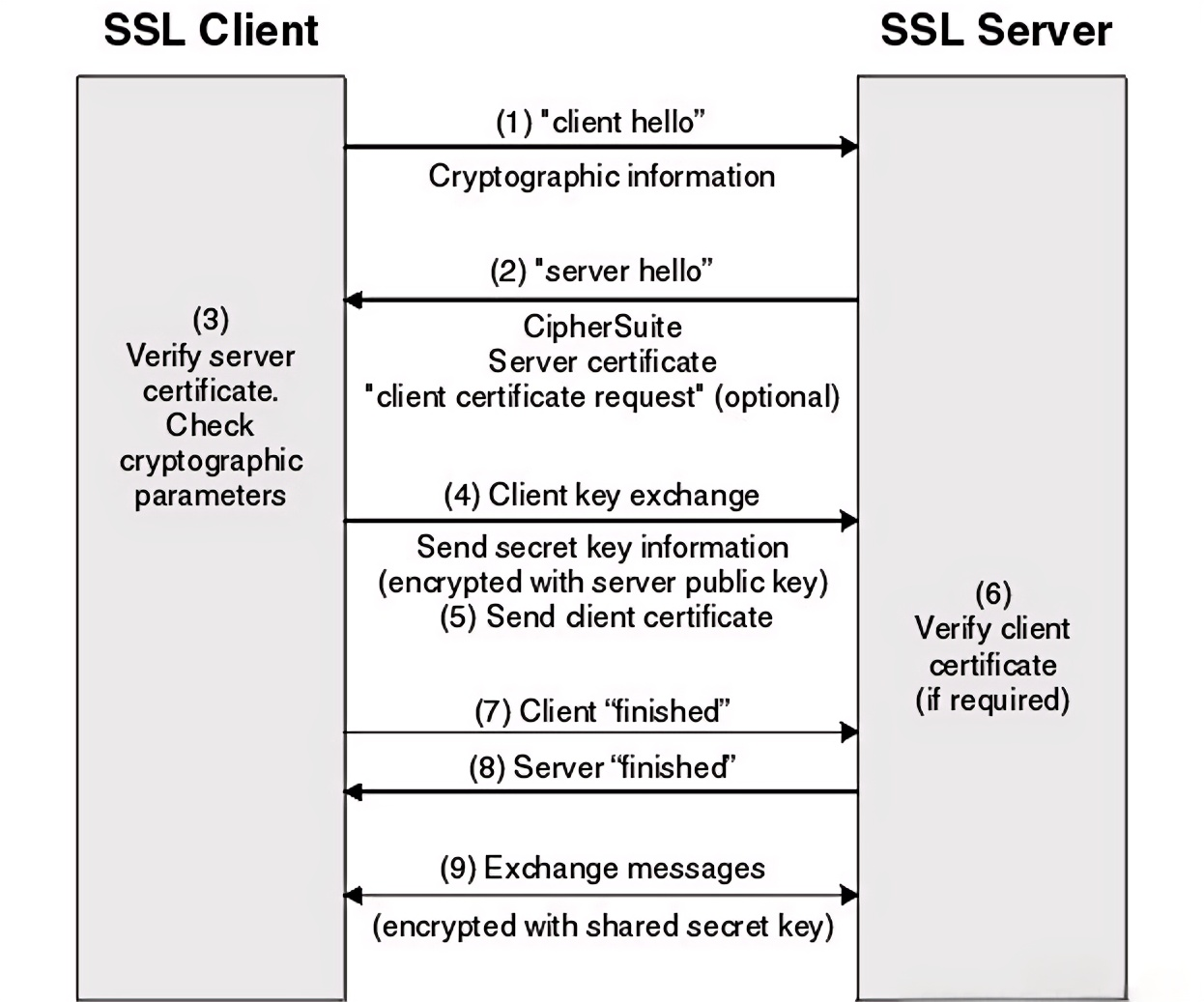


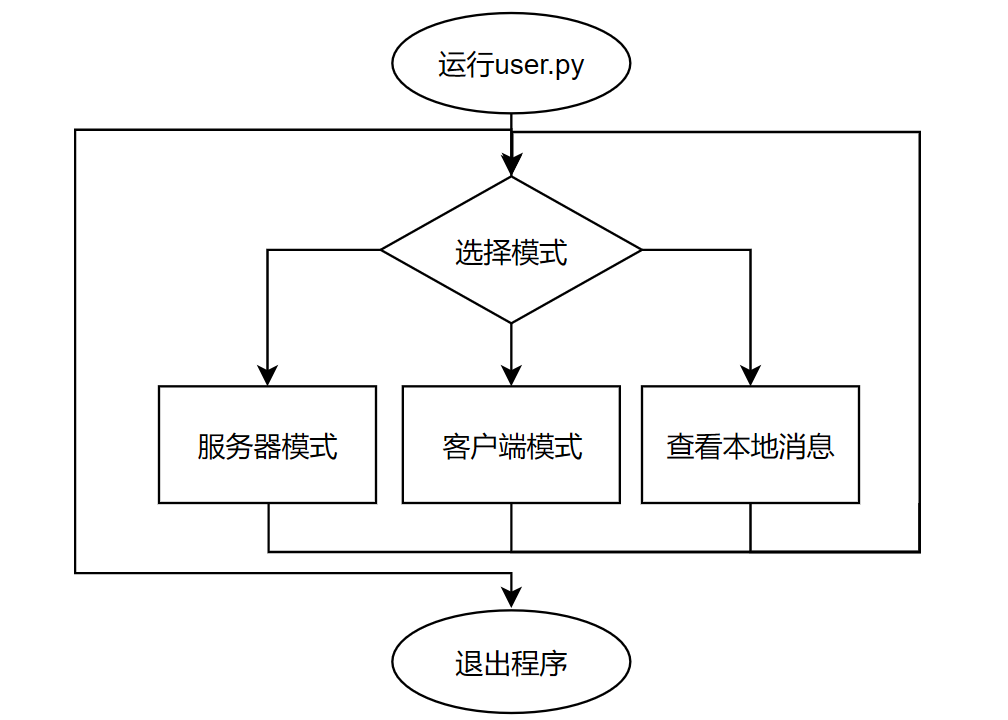
图3-2 SSL/TLS通信时序图

# 详细设计与实现

## 关键模块流程

### 主要控制模块

python启动程序后，将进入功能选择循环，用户可以根据提示进入不同的模式，程序流程如图4-1所示：



4-1 main函数流程图

### 服务器模式

服务器模式启动后，首先接受用户输入的端口和密钥信息，然后开始准备连接：

1. 在目标端口设置监听套接字

### 客户端模式

### 查看消息模式

## 关键数据结构

系统关键数据结构的设计及相关说明。包括：连接表结构、主要协议（TCP、UDP、ICMP）的状态机实现机制等。

## 模块接口设计

系统关键接口的设计及相关说明。

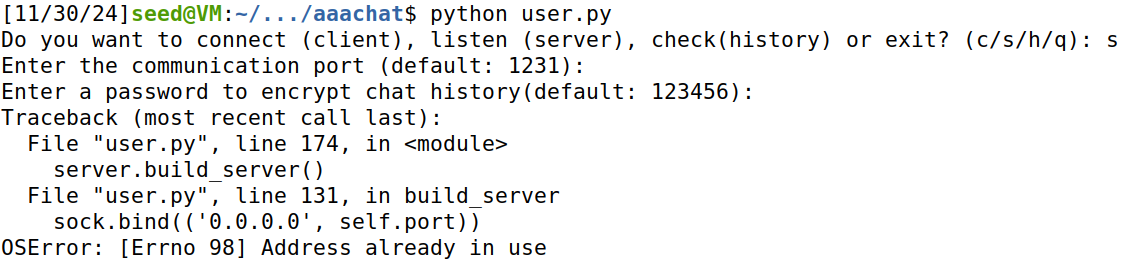
# 问题分析与解决

针对设计开发中碰到的重要技术问题，详细说明问题产生的原因、解决的方案、代码的实现。

## 端口释放问题

### 问题描述

多次测试客户端，每当服务端强制断开后重启，系统显示地址已经被占用，无法启动。



### 原因分析

设计程序时设置服务器模式下持续监听目标端口，而当连接需要断开时，虽然客户端可以轻松地关闭连接，但是服务器端仍然陷入监听循环，如果采用ctrl+z强制终止程序，操作系统并不会立即释放端口，从而导致重新在该端口上启动服务时会出现地址已被使用的错误提示。

### 解决方法

有多种解决方法，可以直接使用命令终止进程以释放端口，但为了简化测试流程也为了更合理的程序设计，我选择在原始程序上进行修改。

首先是在绑定套接字之前，可以设置SO\_REUSEADDR选项，这允许服务器在前一个使用该端口的进程终止后立即重用该端口，使用方法如下：

sock.setsockopt(socket.SOL\_SOCKET, socket.SO\_REUSEADDR, 1)

同时修改服务器模式逻辑，收到连接断开的信号后，如果不需要再等待客户端连接，用户可ctrl+c发送SIGINT信号，程序将释放套接字并退出监听以及服务器模式，而不是继续监听。若要重新启动服务器模式，可以在主程序的选择大循环中重新开启，如此可更节约系统资源。

# 系统测试

## 测试环境

主要描述系统测试拓扑，网络设置等。

## 功能测试

本节主要描述系统功能的测试过程和结果。

## 性能测试

本节主要描述系统性能的测试过程和结果。

# 心得体会及意见建议

在本次网络安全程序设计课程中，我有幸深入探索并实践了网络通信安全的核心原理与技术。通过开发一个基于OpenSSL的安全聊天系统，我不仅将理论知识与实践技能相结合，而且对国家网络安全战略有了更深刻的认识和理解。

本系统的设计遵循了点到点通信的基本原则，确保了数据传输的安全性和隐私性。通过实现基于OpenSSL的安全套接字通信，我深入理解了SSL/TLS协议的工作原理，包括握手过程、密钥交换和数据加密等关键环节。此外，系统还支持客户端与服务器之间的双向认证，这一特性对于防止身份伪造和中间人攻击至关重要。

在实现过程中，我采用了Python作为开发语言，这得益于其丰富的标准库和第三方库，为OpenSSL的安全套接字通信提供了直观而强大的支持。通过使用Python，我能够高效地处理双向认证、套接字加密等复杂操作，这不仅提升了开发效率，也加深了我对网络安全编程的理解。此外，系统还具备聊天记录本地加密存储功能，用户需输入正确的口令才能查看，这一设计进一步增强了数据的安全性。通过这一功能，我不仅巩固了对加密算法和数据保护策略的知识，也提高了对用户隐私保护的意识。

当然，对于课程设计我也有一些建议。首先是课程的理论和实践结合不足，课程讲授没有配备相应的实验，而是直接让学生选题进行开发，这样虽给了学生很大的自由发挥空间，但是在完成任务的过程中理论转化为实践的门槛升高，需要更多时间自行了解编程过程。而且，实验提供的参考资料过少，虽锻炼了学生的信息检索能力，但如果能提供一些参考程序或推荐书籍会让学生更好地理解课题。

通过本次课程设计，我的编程能力、系统设计能力以及对Python API的熟练度都有了显著提升。我深刻体会到，网络安全不仅仅是技术问题，更是国家战略的重要组成部分。在未来的学习和工作中，我将继续致力于网络安全领域的研究与实践，为维护国家网络安全贡献自己的力量。

|  |
| --- |
| 原创性声明 |
| 本人郑重声明本报告内容，是由作者本人独立完成的。有关观点、方法、数据和文献等的引用已在文中指出。除文中已注明引用的内容外，本报告不包含任何其他个人或集体已经公开发表的作品成果，不存在剽窃、抄袭行为。  已阅读并同意以下内容。  判定为不合格的一些情形：  （1）请人代做或冒名顶替者；  （2）替人做且不听劝告者；  （3）实验报告内容抄袭或雷同者；  （4）实验报告内容与实际实验内容不一致者；  （5）实验代码抄袭者。  **作者签名：** |

***以下内容提交时删除！！！***

附件I 实验报告规范化要求

目□□录（黑体小2号加粗居中）

**1□□□**×××实验 1

1.1□□×××××× 1

1.2□□×××××× 3

1.2.1□□×××××× 7

1.3□□×××××× 10

（章为宋体小4号加粗，其余宋体小4号，字母、阿拉伯数字为Time New Roman小4号）

1□×××实验（黑体小2加粗居中）

**1.1□××××××**（黑体4号加粗，字母、阿拉伯数字为Time New Roman4号加粗）

×××××××××××××××××××××××

（宋体小4号，行间距固定1.5倍行距，字符间距为标准）

.......

.......

.......

**1.2.1□××××××**（黑体小4号加粗，字母、阿拉伯数字为Time New Roman小4号加粗）

**1.2.1.1□××××××**（黑体小4号加粗，字母、阿拉伯数字为Time New Roman小4号加粗）

××××××××××××××××××××××

.......

.......

--------章与章之间插入分页符----------

表3-1□××××××××××

|  |  |  |  |
| --- | --- | --- | --- |
| ××××× | ××× | ××× | ××× |
| ××××× | ×× | ×× | ×× |
| ××××× | ×× | ×× | ×× |
| ××××× | ×× | ×× | ×× |
| ××××× | ×× | ×× | ×× |

（表标题：位于表格上方，黑体小4号，字母、阿拉伯数字为Time New Roman小4号，表内容：宋体5号，字母、阿拉伯数字为Time New Roman 5号）

×××××××××××××××××××××××××××（如图3-1所示）。



图3-1□××××××××××

（图标题：位于图下方，黑体小4号，字母、阿拉伯数字为Time New Roman小4号）

.......