# 树莓派项目

## 项目简介

使用python代码编写一个可抗密钥丢失的点对点通信协议

## 项目文档目录



## 状态机

获取初始key与seq

发送消息

ACK正确

更新文件中和程序key

与seq

超时／ACK错误

信息处理

准备发送

等待正确ack到来

准备发送下一个信息

发送

所有

消息

发送结束

**发送端状态机**

校验错误状态

等待消

息到来

HMAC

与SEQ

校验都

正确重

发正常

ACK包

重发上一个ACK包

获取初始key与seq

等待下一个消息来

校验正确状态

收到

end

消息

校验

错误

更新文件中和程序key与seq，并将消息写入缓存文件

显示整个过程收到的信息，并重置缓存文件和key、seq文件

**接受端状态机**

## 打包过程

message

message

Rand

Len8

Seq8

AESOUT

HMAC（32）

PACKET(512+32位)

包填充

AES加密

中1/3key

HAMC

前1/3key

打包

exchangge

ACK

HMAC

解包过程略

## 测试方案与测试结果

补充！！！！！

1. 发送方中断
2. 接收方中断
3. 发送方／接受方网络延迟
4. 网络延迟加中断
5. 多次中断
6. 两边均延迟
7. 两边均中断重启

## 版本缺陷

1. 在发送方，发送信息缓存文件的利用还未完全实现