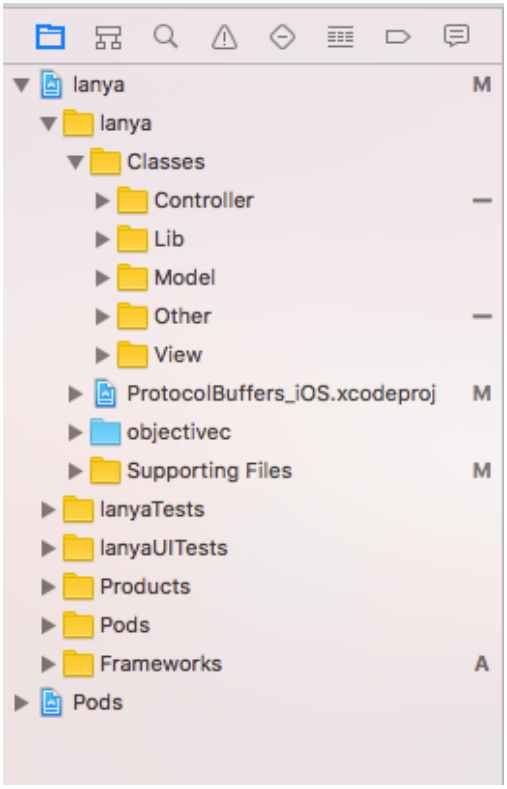
蓝牙聊天室项目小结

1.项目介绍

- 1.主要内容
  - 1.主要是实现老师论文中的用户认证和密钥协商协议
  - 2.所谓用户认证和密钥协商，是指在正式的通信之前，双方通过一些参数的交互，从而确定对方身份的合法性；同时，双发利用交换的参数建立起一把密钥，用于加密解密之后传递的信息
  - 3.这个协议是使用蓝牙作为通信载体的，具体的设想是这样的：通信的双发通过蓝牙发送一些认证参数，同时一方以二维码的方式生成另外一些参数提供给另一方扫描。这个协议适用于双发距离很近，但是又不得不用设备交流的环境。
- 2.项目过程中使用的知识
  - 1.椭圆曲线密码系统和双线性映射密码系统
  - 2.BLE通信
  - 3.ProtocolBuffer的使用

2.项目配置

- 项目的配置比较繁琐，尤其是要将Linux平台下的关于椭圆曲线和双线性映射的C代码移植到iPhone上
- 配置结束，大概是这个样子



3.登录界面

- 1.描述：用户在登录界面输入自己的名字，在蓝牙广播阶段会将用户的名字广播出去给周围的人。
- 2.登录界面的搭建如下所示（整个项目采用导航控制器管理各个子控制器，登录界面是导航控制器的根控制

器）：

- 3.登录界面的业务逻辑
  - 在viewDidLoad中要读入配置文件，根据配置文件中的信息决定相关控件状态
  - 点击登录的时候要讲用户的名字传递给蓝牙扫描界面（顺传 - 使用属性）
  - textField显示提示，并且编辑时候清除按钮可用
- 4.其他小的知识点：
  - 设置登录界面上头像的button为圆形，设置登录按钮为椭圆形

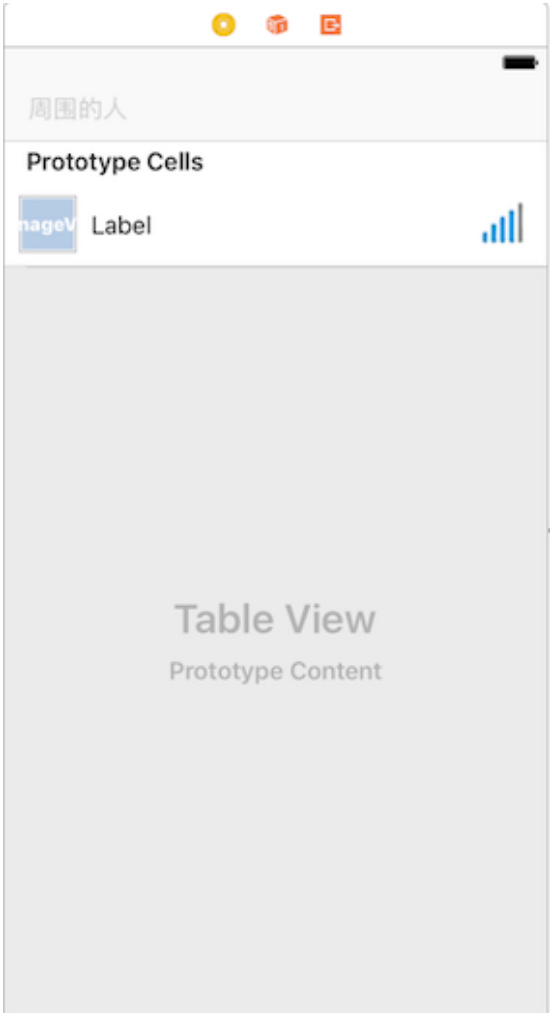
```
// 登录用户的头像显示为圆形
self.iconBtn.clipsToBounds=YES;
self.iconBtn.layer.cornerRadius=self.iconBtn.frame.size.height / 2;
// 设置登录按钮边框为椭圆形
self.loginBtn.clipsToBounds = YES;
self.loginBtn.layer.cornerRadius = 5;
```

  - 定义开发调试阶段的宏

```
// 定义调试阶段打印的宏，调试结束后，直接注释掉NSLog部分
#define XBLog(...) NSLog(__VA_ARGS__)
```

3.蓝牙扫描界面

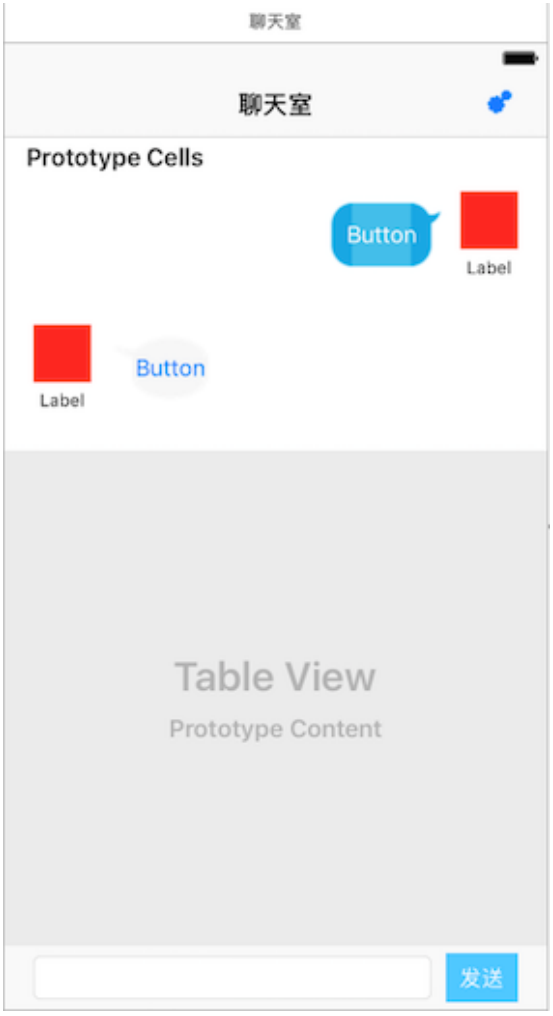
- 1.描述：当用户点击了登录之后，会跳转到蓝牙扫描界面。在这个界面中主要使用BLE建立会话密钥
- 2.蓝牙扫描阶段的界面搭建如下：



- 3.蓝牙扫描阶段的业务逻辑
    - 开启外设模式，广播自己构造的数据包。这个数据包中包含一个随机数，通过随机数值大小的比较，确定双方谁为中心，谁为外设
    - 开启中心管理者模式，扫描数据包，并通过数据包中随机数值的大小关系确定主从关系
    - 确定主从关系之后，互发认证信息，确定最终的会话密钥

4.聊天室界面

- 1.描述：在双发正确建立器加解密的密钥之后，双发就可以通过这个密钥来加解密传递的信息，这里利用tableview简单搭建了一个聊天室的界面
- 2.聊天室界面的搭建如下：



- 3.聊天室的业务逻辑
- 关于BLE信息的发送和接收都在蓝牙扫描的那个界面中，所以这个通过代理方式，将自己要发送的信息通知那个界面；同时在接收到别人发送的信息的时候，调用这个控制器的显示数据方法，显示数据。
- 4.其他小的知识点：
    - tableview上的两个cell公用一个类，因为数量完全一样，就只有约束不一样
    - 点击文本框时，文本框弹出，tableview要上移，使用约束控制（也可以使用transform）
    - 点击某一个cell的时，退出编辑，tableview要下移

5.设置界面

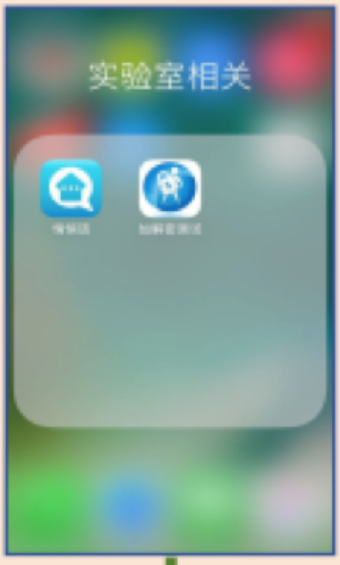
- 1.描述：点击聊天室右上角的设置按钮，来到设置界面，这里可以设置相关的用户状态信息
- 2.设置界面的搭建如下：

- 3.设置界面的逻辑业务
- 如果自动登录开启，那么记住用户名开启
- 如果记住用户名关闭，那么自动登录关闭

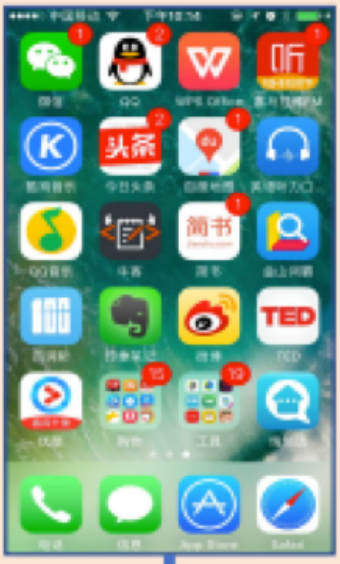
6.效果图

设备 A

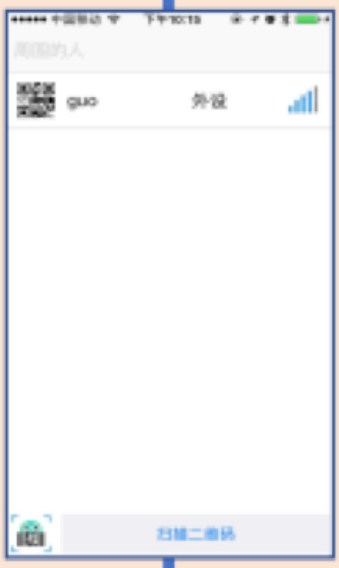
设备 B



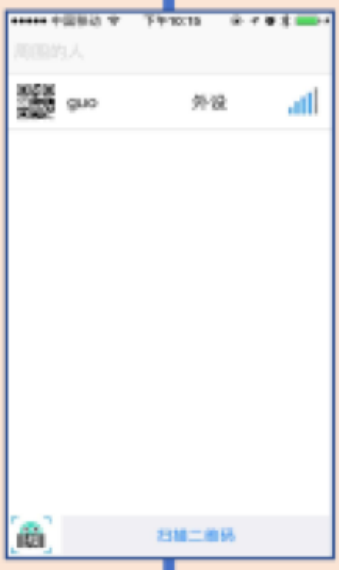
点击 “悄悄话 “app，启动聊天室系统



蓝牙会自动扫描到附近的人，显示在列表中



点击设备 A 中某一个列表设备，A 会通过蓝牙发送一部分认证参数给，同时生产二维码



设备 A

设备 B

设备 B 点击“扫描二维码“，扫描设备 A；此时点击”否“，表示此次仅两方通信

双方计算并生成会话密钥，点击“好的，知道了“，进入聊天室

此时双发聊天发送的信息是使用上述会话密钥加密的