App 控制锁具涉及的各种功能的方案（从 app 角度）

App 的密钥产生

方案 1：APP 的密钥每次随机产生。密钥算法为 RSA，长度 512 位。

方案 2：APP 的密钥初次登陆时随机产生，以文件形式保存在手机中。密钥算法为 RSA，长度 512 位。

锁的密钥产生

锁的密钥每次随机产生。密钥算法为 RC4，长度 64 位。

锁的复位

门锁内侧复位键长按 5 秒，锁内一切用户信息归 0，处于待接管状态。

初设管理员

用户进入 app 注册界面，填写管理员的用户信息（用户名、登录密码、开门密码），点击确认，app 将用户信息和国际移动用户识别码存入锁中。保存完，锁返回 app 重启以使注册生效的提示信息（消息框上有确定按钮）和锁的单片机芯片 ID。用户点击确定后，app 将存储锁的 ID。app 重启后进入登录界面，管理员用户进入登录界面便可以操作其它功能（例如：添加普通用户，临时用户等）。

注：注册完毕后，手机和锁中都存有共同的信息：手机的国际移动用户识别码和锁 ID，这相当于手机和锁相互绑定。

用户和锁建立连接通道

手机对锁的验证：

第一步：用户登录 app 前，选择要建立配对的蓝牙，点击连接按钮，手机产生一个随机数，并利用随机数生产公私钥；

第二步：手机将公钥、随机数、用户识别码明文发送给锁，锁接到后，将该随机数、用户识别码和锁 ID 作为输入，用我们事先烧录的算法计算，计算出一个数，并将该数值返回给手机；

第三步：手机接收锁的返回值（该步是不是要锁要先发送一个消息给手机，手机才能触发接收锁的返回值？是否可以用用户登录来触发），也用随机数、手机识别码和已存于其中的锁 ID，用我们事先写在 app 中的、和锁中一样的算法计算出一个数；如果两个数相等，则手机完成对锁的验证。

锁对手机的验证：

如果手机验证锁成功，用户登录，手机发送用户登录信息给锁，锁对用户名和登录密码进行验证，若正确，则随机产生对称的会话密钥，并用之前已接收到的手机公钥将会话密钥加密，密文返回给手机。

至此，手机和锁完成双向验证，手机获得锁的临时会话密钥，建立会话。用户进入功能选择界面。

注 1：管理员在建立普通用户时，不可能将普通用户手机识别码存于锁中，因此，普通用户在第一次登陆时，只采取锁对手机的验证。在首次登录后，以后每次登录再采取相互验证的方式。

注 2：当用户删除 app，锁的 id 也会被删除。为避免这种情况，可以将锁 id 保存在手机

中，当安装 app 后，自动导入回来。注意处理 1 个用户管理多把锁的情况。

管理员功能

管理员开锁：

- 管理员开锁：

  管理员在 APP 登录后，点击 APP 中的开门按键，APP 弹出要求输入开门密码的对话框；用户输完密码，点击确定，输入的密码会连同其他输入参数一起被用会话密钥加密，传输给门锁；门锁用会话密钥解密，审核用户的开门密码，根据审核结果执行操作，返回明文处理结果，并储存用户 ID+用户身份+开锁时间。

管理员管理其他用户：

- 管理员登录管理界面（读取用户信息）：

  管理员点击管理按钮后，弹出对话框要求输入登录密码，确认后进入用户信息列表（app 获取到除管理员之外的所有用户信息并以列表信息展示），长按其中一个用户信息弹出对话框（增加/删除），点击删除后会要求用户确认操作，app 将待删除的用户名及操作指令发送给锁，等待锁返回消息并进行界面更新。点击增加后，弹出增加用户信息填写界面，填写好信息后 app 将用户信息使用锁会话密钥进行加密传送，锁增加用户后返回成功或失败信息，用户界面进行更新。

- 增加用户：

  管理员进入增加用户的界面后发送一个准备注册用户的信息给锁，锁进入等待状态。注册界面有一个选项可以选择增加的是普通用户还是临时用户，注册界面的注册消息有用户名，密码，开锁密码，用户类型（普通用户，临时用户）。app 将用户注册消息发送给锁，锁储存完成后返回注册成功的信息

- 删除，查询用户：

  管理员进入查询用户的界面后发送查询用户信息给锁，app 进入等待锁返回消息的状态。锁返回除管理员之外的用户信息（用户账户名，密码），app 以列表形式显示。用户点击列表中的一条信息后弹出菜单栏（删除），点击删除选项后弹出一个确认删除的对话框。确认后发送带有该条用户信息及删除命令的消息给锁，锁进行解析进行删除，返回是否成功的状态。

- 查询开锁记录：

  App 发送一条带有查询开锁记录的消息给锁，等待锁返回开锁记录，以列表形式展现。

普通用户功能：

- 开锁：点击开锁按钮后弹出一条对话框要求输入该用户的开锁密码，app 将消息发送给锁，锁进行验证开锁后返回是否成功的状态，app 进行显示
- 修改自身开锁密码：点击修改按钮后要求输入当前开锁密码，app 发送修改开锁消息（带有当前开锁密码）给锁，锁进行验证后并进行修改，返回是否修改成功的消息给 app，app 并进行展示。

注：普通用户修改开锁密码是为租房用户考虑，当管理员在普通用户修改了密码后，管理员再一次登录时，app 会在查询用户功能键处提示更新信息。

临时用户功能：

- 开锁：点击开锁按钮后弹出一条对话框要求输入该用户的开锁密码，app 将消息发送给锁，锁进行验证开锁后返回是否成功的状态，app 进行显示，锁删除该临时用户。

(临时用户只给一次开锁次数或限定开锁时间)

1. 接口定义

1.1 初设管理员（管理员和锁建立初次连接通道）

接口	初始化设备（指令字：0x01）
功能描述	在锁复位时确定锁的主人（管理员注册）
输入参数	手机的公钥（？字节） 管理员用户名（8 个字节）管理员登录 app 密码（8 个字节） 开锁密码（8 个字节）手机识别码（？字节）效验字（1 字节）效验采用异或效验 验证解密是否正确 不是报文结尾的效验字
输出参数	处理结果（成功：锁的蓝牙设备号、锁 ID；失败：0）
接收方	电控锁
发送方	APP
通信加密方式及验证过程	手机将自己公钥传给锁，锁接到手机公钥后，用手机公钥加密会话密钥，将该密文传给手机，手机用自己私钥解密，获得锁的会话密钥。手机用锁的会话密钥加密输入参数，将该密文传给锁，锁用会话密钥解密，存储管理员的用户名、登录密码、开锁密码、身份标识、手机识别码，并密文返回锁 id。手机解密密文，存储锁的蓝牙设备号、锁 ID。

注明：

- 这一步只发生在锁被复位，管理员注册时。
- 校验字是为了验证发送的数据包的正确性
- 手机存锁的蓝牙设备号是为了以防一个手机对应多把锁。

1.2 普通用户、临时用户和锁建立初次连接通道

接口	普通用户初始化（指令字：0x02）
功能描述	手机不验证锁，只是锁验证手机。通过验证，获取锁会话密钥，为加密通讯做准备
输入参数	用户名、登录密码、手机识别码、App 的公钥
输出参数	处理结果（成功：公钥加密会话密钥、锁的蓝牙设备号、锁 ID；失败：0）
接收方	电控锁
发送方	APP
通信加密方式及验证过程	App 蓝牙和锁的蓝牙连接，App 向锁发送公钥。锁接到公钥，随机产生会话密钥，并用公钥加密会话密钥传给手机。手机用私钥解密，获得会话密钥。手机用会话密钥加密用户名、登录密码、手机识别码。锁解密密文，对用户名和登录密码审核，审核通过，追加用户名对应的手机的识别

	码，并返回会话密钥加密的锁的 ID。App 接到密文，用会话密钥解密，获得锁的会话密钥和锁 ID。手机存储锁蓝牙设备号和锁 ID。

注：临时用户考虑退出时删除锁 ID，以免锁 ID 外泄

1.3 用户和锁建立连接通道（非初次）

接口	获得门锁会话密钥（指令字：0x03）
功能描述	通过相互验证，获取锁产生的会话密钥，为加密通讯做准备
输入参数	App 的公钥、用户名（8 字节）、登录密码（8 字节）、app 产生的随机数（8 字节）
输出参数	审核通过，则返回公钥加密会话密钥的密文； 审核失败，返回失败。
接收方	电控锁
发送方	APP
通信加密方式及验证过程	App 蓝牙和锁的蓝牙连接，App 向锁发送随机数，锁返回验证计算结果，手机核对计算结果。如果通过审核，手机发送用户名和登录密码密文、App 的公钥给锁，锁用公钥解密并审核用户，若审核通过，则锁用该公钥加密会话密钥，返回密文给 app。App 接到密文，用私钥解密，获得锁的会话密钥。

注：手机和锁须双相验证

1.4 开锁（所以用户都有该权限）

接口	开锁（指令字：0x04）
功能描述	用户开锁
输入参数	用户名（8 个字节）开锁密码（8 个字节）效验字（1 字节）效验采用异或效验 验证解密是否正确 不是报文结尾的效验字
输出参数	处理结果（1 字节，1：成功 0：失败）
接收方	电控锁
发送方	APP
通信加密方式及验证过程	输入参数使用会话密钥加密，锁接到密文用会话密钥解密。锁验证用户名、开锁密码，若正确，则执行开锁，存储用户名+用户身份+开锁时间；不正确，则不开锁、不

	存储。输出参数明文传输。

1.5 读取用户信息（仅限管理员权限）

接口	读取用户信息（指令字：0x05）
功能描述	管理员登录用户管理界面，获得用户信息
输入参数	用户名（8 个字节）登录密码（8 个字节）效验字（1 字节）效验采用异或效验 验证解密是否正确 不是报文结尾的效验字
输出参数	输出所用用户的用户名、用户标识、登录密码、开锁密码
接收方	电控锁
发送方	APP
通信加密方式及验证过程	输入参数使用会话密钥加密，锁接到密文用会话密钥解密。锁验证用户名、登录密码，若正确，则向手机发出所有用户的用户名、用户标识、登录密码、开锁密码。输出参数用会话密钥加密。App 用会话密钥解密。

注明：当用户看到该记录时，初次只看到用户名，身份标识。用户再次做出修改选择，则弹出完整的用户名、用户标识、登录密码、开锁密码对话框。

1.6 增加用户（仅限管理员权限）

接口	增加用户（指令字：0x06）
功能描述	在管理员登录条件下，增加普通用户或临时用户
输入参数	增加的用户名（8 个字节）身份标识（1 字节）登录密码（8 个字节）开锁密码（8 个字节）效验字（1 字节）效验采用异或效验 验证解密是否正确 不是报文结尾的效验字
输出参数	处理结果（1 字节，1：成功 2：已安装 0：失败）
接收方	电控锁
发送方	APP
通信加密方式及验证过程	输入参数使用会话密钥加密，锁接到密文用会话密钥解密。检测用户名，若已存在，则提示用户名已安装。若不重名，则锁存储用户名+身份标识+登录密码+开锁密码。输出为明文（例如提示录入成功）。

1.7 删除用户（仅限管理员权限）

接口	增加用户（指令字：0x07）
功能描述	在管理员登录条件下，删除用户
输入参数	用户名（8 个字节） 效验字（1 字节）效验采用异或效验 验证解密是否正确 不是报文结尾的效验字
输出参数	处理结果（1 字节，1：成功 0：失败）
接收方	电控锁

发送方	APP
通信加密方式及验证过程	输入参数使用明文。输出参数使用明文。

1.8 用户修改自己的开锁密码（管理员和普通用户权限）

接口	增加用户（指令字：0x08）
功能描述	用户登录条件下修改自己的开锁密码
输入参数	用户名（8 个字节） 开锁原密码（8 字节）开锁新密码（8 字节）效验字（1 字节）效验采用异或效验 验证解密是否正确 不是报文结尾的效验字
输出参数	处理结果（1 字节，1：成功 0：失败）
接收方	电控锁
发送方	APP
通信加密方式及验证过程	输入参数使用会话密码加密，锁核对用户名和用户开锁原密码。核对正确，用新密码代替旧密码；核对错误，返回失败信号。输出参数使用明文。

流程接口及定义（待定）