# 无感蓝牙锁

## 一、整体功能流程

### 1. 设备上电默认行为（首次使用 / 未绑定）

- 默认进入 **配置模式**（BLE Peripheral）
- 开启 BLE 广播，等待 App 连接绑定
- 绑定成功后保存绑定信息，后续上电进入 **HOST 模式**

### 2. 已绑定后的行为（正常使用流程）

- 上电自动进入 **HOST 模式**
- 作为 BLE 主机，主动扫描广播
- 检测目标设备广播后执行鉴权，通过后可响应用户按键开锁请求

### 3. 无感开锁整体流程

- 主动扫描 → 发现目标广播 → **解析并验证内容**
- 执行鉴权 → 用户按键触发开锁
- 控制电机解锁 → 蜂鸣器反馈操作结果

## 二、设备端功能需求

### 1. BLE 配置模式（默认上电模式）

- 条件：首次使用 / 未绑定
- 行为：
  - BLE 从设备广播，包含设备名、MAC、固件版本等信息
  - 提供 GATT 服务供 App 连接绑定，写入密钥、用户标识等
  - 成功后保存绑定信息至 Flash，下次上电进入 HOST 模式

### 2. BLE HOST 模式（绑定成功后默认工作模式）

- 条件：已绑定
- 行为：
  - 作为 BLE 主机，定时或连续扫描特定格式广播
  - 广播中提取 App ID、随机数、签名等信息
  - 验证 App 身份后进入监听按键状态

## 三、电机控制模块

### 控制逻辑

- GPIO 控制电机驱动（MOS / 电机芯片）
- 鉴权成功 + 按键触发 → 电机通电工作（约 300ms）
- 定时关闭，防止卡顿或过热

## 四、按键行为逻辑

| 操作 | 当前状态 | 功能 | 蜂鸣器反馈 |
| --- | --- | --- | --- |
| 短按 1 次 | 鉴权成功 | 控制电机开锁 | 成功：短滴1声；失败：短滴2声 |
| 长按 3 秒 | 任意状态 | 关机 | 长鸣1秒 |
| 短按 1 次 | 关机状态 | 开机 | 短滴1声 |
| 连按 3 次 + 长按 | 任意状态 | 进入配置模式 | 长鸣后启动广播 |
| 上电默认 | 未绑定 | 配置模式（广播+绑定） | —— |
| 上电默认 | 已绑定 | HOST 模式（扫描） | —— |

## 五、广播内容格式设计

- 广播数据包含字段：

    - 固定前缀 + 设备类型标识
    - 当前设备状态（绑定状态、加密模式）
    - 可选加密 Token（防重放攻击）
- 广播结构示例：

```
Byte[0]   : Frame Type (0xAA)
Byte[1-2] : Device Type + Version
Byte[3-8] : 设备唯一 ID（加密）
Byte[9-14]: Rolling Token（可变随机数）
Byte[15-] : CRC / MAC / 签名
```

# 六、加解密与鉴权流程设计

## 鉴权算法设计

- 推荐方案：**AES-GCM + HMAC-SHA256**
- 双向认证：广播中带有签名，设备验证通过后返回确认广播或允许用户按键解锁
- 加密使用设备密钥（App 绑定时下发）

## 加解密流程

- App 生成随机 Token，广播时包含该 Token
- 设备解析 Token，使用密钥 + nonce 进行 HMAC 校验
- 校验通过 → 接受用户按键开锁命令
- 若需要通信加密，使用 AES-GCM 加解密报文内容

# 七、App 通信通道设计

- 配置模式下，App 通过 BLE 连接设备 GATT 服务，主要用于：
    - 获取设备信息
    - 写入绑定凭据（加密密钥、App ID）
    - 升级配置项（如广播频率、电机参数等）
- 通信通道需定义：
    - 绑定服务 UUID

- 鉴权验证服务 UUID
- 命令控制服务 UUID（如：远程解锁、配置修改）

# 八、详细开发任务拆解

| 模块 | 子任务 | 说明 | 状态 |
| --- | --- | --- | --- |
| **BLE 配置模式** | 启动广播 + GATT 服务注册 | 设备首次上电或解绑后进入 | ☐ |
| | 接收绑定指令并保存信息 | Flash 保存绑定用户、密钥、状态等 | ☐ |
| **绑定状态判断** | 判断绑定状态并切换工作模式 | 上电初始化时区分配置 / 主机模式 | ☐ |
| **HOST 模式** | 扫描广播 + 过滤解析广播内容 | 解析广播中 App ID + Token 等字段 | ☐ |
| | 执行鉴权流程（Token 校验） | HMAC-SHA256 校验 / AES-GCM 解密验证 | ☐ |
| | 等待按键触发解锁 | 鉴权成功后监听按键 | ☐ |
| **电机模块** | GPIO 控制电机开关 | 保护电路控制，时序精确 | ☐ |
| **按键逻辑** | 实现按键状态机 / 多次操作识别 | 区分短按、长按、连击等操作 | ☐ |
| **加密模块** | AES-GCM 加密解密流程封装 | 与 App 交互密钥、Nonce 同步 | ☐ |
| | HMAC-SHA256 校验 | 校验 App 广播数据合法性 | ☐ |
| **广播内容设计** | 广播结构格式规范、CRC 校验等设计 | 统一格式，App/设备都能解析 | ☐ |
| **通信通道设计** | 配置 GATT 服务（绑定 / 配置 / 控制） | 设计 UUID 和通信协议 | ☐ |