蓝牙震动马达安全控制协议（V2.0）

> 基于 LE Secure Connections + Just-Works bonding

1 协议目标

- 链路强制加密（BT Security Level 4）
- 防重放、防篡改、防中间人
- 用户交互极简：首次 1 次系统弹窗，后续秒连
- 单包完成占空比设置

2 绑定与加密流程

步骤	动作	备注
1	玩具广播 `ADV_IND`	含 Flag LE General Discoverable
2	手机连接	任意中央设备
3	玩具立即调用 `bt_conn_set_security(conn, BT_SECURITY_L4)`	强制走 LESC
4	系统弹窗“是否配对 **××震动玩具**？”	Just-Works，无 6 位数字
5	配对成功 → 玩具把 `LTK/CSRK/Counter` 写入片内 Flash NVS	掉电不丢
6	后续再连	双方直接加密复用，**零弹窗**

3 GATT 服务定义

字段	值
Service UUID	`9A501A2D-594F-4E2B-B123-5F739A2D594F`
Char UUID	`9A511A2D-594F-4E2B-B123-5F739A2D594F`
Property	Write-Without-Response
MTU 需求	23 B 即可（包长 20 B）

4 数据包格式（手机 → 玩具）

固定 **20 B**，不足补 0x00

偏移	长度	名称	类型	说明
0	1	`cmd`	uint8	0x01 = 设置占空比
1	6	`counter`	uint48	单调递增，48 bit 小端
7	1	`duty`	uint8	0x00-0xFF → 0%-100%
8	8	`rsvd`	uint8[8]	预留，全 0x00
16	4	`mic`	uint32	AES-CMAC-32（前 16 B，CSRK）

偏移	长度	名称	类型	说明

5 计数器与重放保护

- 玩具维护 48 bit `last_counter`，**RAM 实时更新**
- 每收到 256 包 → 写片内 Flash NVS（磨损均衡, App 100 ms/包 → 25.6 s/次 → 每日 ≈3375 次 → 100 k 次寿命 Flash 可用约 29 年）
- 仅接受 `counter > last_counter` 且差值 < 2^{30}
- 溢出后主动 `bt_conn_disconnect`，清除 bonding，强制重新配对
- **掉电最多丢失 255 个序号**，仍在安全窗口内

6 设备端校验流程（伪代码）

```
if (len != 20) return ATT_ERR_INVALID_PDU;

uint48_t ctr = get_le48(&p[1]);
if (ctr <= last_counter) return ATT_ERR_VALUE_NOT_ALLOWED;

if (!aes_cmac_32_verify(p, 16, csrk, &p[16]))
    return ATT_ERR_AUTHENTICATION;

last_counter = ctr;        /* RAM 立即更新 */
counter_on_packet(ctr);    /* 累积 256 包再写 Flash */
set_pwm_duty(p[7]);
return 20;
```

7 安全声明

项目	实现
链路加密	AES-CCM，128 bit
密钥交换	P-256 ECDH（LESC）
认证方式	Just-Works（无 MITM）
重放保护	48 bit Counter
数据完整性	CMAC-MIC 32 bit
密钥存储	片内 Flash NVS，读保护开启

8 发布 checklist

- [ ] 固件打开 `CONFIG_BT_SMP_SC_ONLY=y`（仅 LESC）
- [ ] 关闭 `CONFIG_BT_USE_DEBUG_KEYS=n`
- [ ] 量产时开启芯片 RDP / APPROTECT
- [ ] App 端首次扫描过滤 Service UUID `9A501A2D-594F-4E2B-B123-5F739A2D594F`