# 蓝牙数据格式及加密处理

广播名称：3到5个字符 默认IB\_A3

数据格式：

|  |  |  |
| --- | --- | --- |
| 0:1 | 厂商ID | 0x17 0x28 |
| 2 | 协议版本号 | 0x00 |
| 3:4 | model号 | 0x02 0x03 蓝牙人体秤 |
| 5:10 | MAC地址 | 大端模式 |
| 11 | 随机数 | 随机生成（上一包的校验码） |
| 12 | 秤体模式 | 0x00 休眠  0x01 称重  0x02 平衡力  0x03 阻抗 |
| 13 | 标志位 | 称重模式  bit1:0 单位 00 kg, 01 lb, 10 st, 11 斤  bit3:2 分度 00 100g, 01 50g, 10 10g  bit4 稳定标志位  bit5 超载标志位  bit6 配网标志位  平衡力模式  bit1:0 状态 00 未开始, 01 进行中, 10 结束  阻抗模式  Bit0: 测值模式，0 直流，1 交流；  Bit1:阻抗测量状态，0阻抗测量进行中，1阻抗测量完成  Bit3:2阻抗值状态，00正常,01阻抗偏低/短路，02阻抗偏大/开路 |
| 14:15 | 重量/时间/阻抗 | 小端 x0.01kg/x0.1s/x 1阻抗单位（交流Ω，直流kΩ） |
| 16 | 广播包序号 | 每次发送累加1 |
| 17 | 校验和 | 累加校验[byte11 + ... + byte16] |

加密处理

数据发送时，秤体对协议中byte12至byte17部分做加密处理，加密因子初始值取决于byte11和byte12，每计算完一次后更新加密因子。密文及加密因子计算如下：

Xi: 第1位取秤体MAC地址的最后一位，后续通过计算得出；

Yi: 第1位取上一包蓝牙数据的校验和位，后续通过计算得出；

Di: 第i位明文；

Si: 第i位密文；

加密公式

Si = (Di xor Xi) + Yi;

Yi+1 = Xi xor Yi;

Xi+1 = Xi + Di;

解码公式

Di = (Si - Yi )xor Xi ,

Xi+1 = Xi + Di;

Yi+1 = Xi xor Yi;

例如

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 明文D | 17 | 28 | 00 | 02 | 03 | 18 | 72 | 93 | 65 | 48 | 6B | A5 | 01 | 10 | 4C | 1D | 20 | 48 |
| 密钥X |  |  |  |  |  |  |  |  |  |  |  |  | 6B | 6C | 7C | C8 | D5 | F5 |
| 密钥Y |  |  |  |  |  |  |  |  |  |  |  |  | A5 | CE | A2 | DE | A6 | 7B |
| 密文S | 17 | 28 | 00 | 02 | 03 | 18 | 72 | 93 | 65 | 48 | 6B | A5 | 0F | 4A | D2 | B3 | 9B | 38 |