第 43 卷 第 7 期 计 算 机 工 程 2017 年 7 月
Vol. 43 No. 7 Computer Engineering July 2017

·体系结构与软件技术· 文章编号：1000-3428(2017)07-0054-06 文献标志码：A 中图分类号：TP301

具有射频识别功能的嵌入式低功耗智能钥匙设计

蒋存波，孔祥丽，金 红，焦 阳

（桂林理工大学 信息科学与工程学院，广西 桂林 541006）

摘 要：针对多把钥匙和多个锁的匹配性问题，设计一种用于主动身份认证的低功耗智能钥匙。使用授权注册和主动双向认证方式实现钥匙对多把锁的管理，采用密码词典加密和准动态密码索引字确保认证过程的可靠性。根据钥匙低功耗要求，提出 1 s 周期定时休眠与 0.005 s 唤醒机制，以尽可能降低身份认证卡的功耗。实验结果表明，该智能钥匙睡眠模式功耗小于 2 μA，且满足多把钥匙与多个锁之间相互匹配和安全认证的要求。

关键词：嵌入式系统；智能家居；无线身份认证；低功耗；安全性；无线射频识别

中文引用格式：蒋存波，孔祥丽，金 红，等. 具有射频识别功能的嵌入式低功耗智能钥匙设计[J]. 计算机工程，2017，43(7)：54-59.

英文引用格式：Jiang Cunbo，Kong Xiangli，Jin Hong，et al. Design of Embedded Low-power Intelligent Key with Function of Radio Frequency Identification[J]. Computer Engineering，2017，43(7)：54-59.

Design of Embedded Low-power Intelligent Key with Function of Radio Frequency Identification

JIANG Cunbo，KONG Xiangli，JIN Hong，JIAO Yang

（College of Information Science and Engineering，Guilin University of Technology，Guilin，Guangxi 541006，China）

【Abstract】For the matching of multiple locks and multiple keys，a low-power intelligent key which is applied to the active authentication with embedded radio frequency identification is designed. The management of multiple locks is realized by means of authorized registration and active two-way authentication，where password dictionary encryption and quasi dynamic password index are used to ensure that the authentication process is reliable. According to the low power requirement of the key，a 1 s periodic sleep with 0.005 s wakeup mechanism is proposed to reduce the power consumption of authentication card as much as possible. Experimental results show that，the power consumption of the intelligent key sleep mode is less than 2 μA，and it meets the requirement of matching and security authentication between multiple keys and multiple locks.

【Key words】embedded system；smart home；wireless identity authentication；low power consumption；security；radio frequency identification

DOI：10.3969/j.issn.1000-3428.2017.07.009

0 概述

嵌入式智能锁主要特点包括：一把钥匙能开多个门锁，门锁能够记录开锁钥匙编号和开锁时间；无线加密报文主动请求身份认证，直接通过门把手开门[1]；基于动态认证的 GPRS 短信息远程开锁和监测[2-3]。为了实现智能锁的功能，智能钥匙对应需要实现：一把钥匙管理多个门锁；使用无线通信报文通信，对身份认证请求识别并应答。同时由于智能钥匙独立门锁装置使用电池单独供电，需要低功耗设计以维持长时间使用，一块电池至少需要能够供电一年左右的时间。本文针对多把钥匙和多个锁的匹配性问题，设计一种基于嵌入式射频识别的低功耗智能钥匙。

1 硬件设计

使用 TI 公司的片上系统芯片 CC2530 作为核

基金项目：广西自然科学基金(2013GXNSFBA019250，2015GXNSFBA139250)；桂林理工大学重点实验室建设项目(桂理工科〔2014〕5 号)；广西发明专利倍增计划项目(KY2015ZL100)。

作者简介：蒋存波(1962—)，男，教授，主研方向为嵌入式系统、自动检测与控制装置；孔祥丽(通信作者)，硕士研究生；金 红，副教授；焦 阳，硕士研究生。

收稿日期：2016-04-19 **修回日期：**2016-07-25 **E-mail：**1654646724@qq.com

心。CC2530 的特点是:1)整合了射频前端,具有无线信号收发功能[4-5]。在主动接收 RF 的情况下,功耗为 24 mA;在主动发送 RF 的情况下,功耗为 29 mA。2)有 5 种工作模式,可以在没有操作时进入低功耗或超低功耗状态,其中 PM2 模式下功耗为1 μA。智能钥匙原理如图 1 所示。

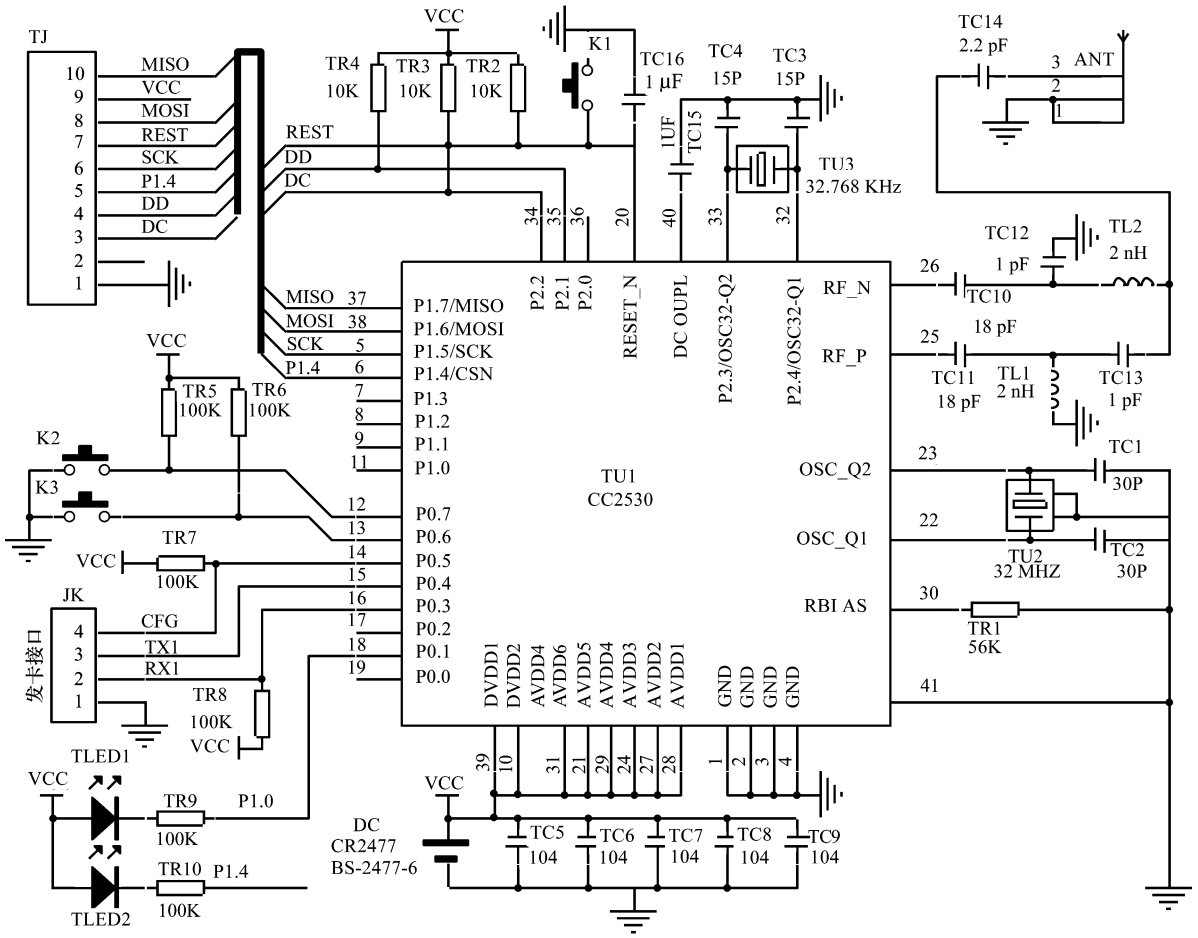


图 1　智能钥匙原理

在图 1 中,TJ 为程序下载与调试接口,JK 为工作于 UART 的有线方式发卡接口。将智能钥匙插入智能锁或专用发卡装置的发卡接口,使得 P0.5 = 0 进入发卡状态。在发卡状态,钥匙将对发卡器进行合法性识别,发卡器也将对钥匙进行合法性识别,通过识别后,钥匙将接收发卡命令,装入密码词典,将身份标识写入到身份标识表中。每个钥匙可以写入最多 8 个身份识别字以匹配本系列内的 8 个不同锁具,以减少携带钥匙的数量。按钮 K2 和 K3 用于钥匙主动开锁。

2　软件设计

为实现低功耗要求[6],采用周期性“睡眠(进入 PM2)-唤醒-睡眠”的工作方式。一个睡眠-唤醒周期约 1 s,唤醒后的持续工作时间 Ton 设定为约 5 ms,由定时器 Time1 控制。唤醒后启动无线电模块并进入 RF 接收状态,然后启动工作时间定时器 Time1 设定工作时间 Ton。在 Ton 时间内,如果收到智能锁的一个完整报文,则对报文进行有效性识别,并依据报文类型进行处理,处理完毕进入休眠状态;如果在 Ton 期间没有收到有效报文则定时进入休眠状态。当前 RF 认证报文主要使用身份认证请求、认证应答,认证报文使用 18 Byte 固定长度。配置钥匙(发卡)使用专门的配置接口,锁的 ID 与钥匙 ID 由发卡器生成。钥匙通过配置接口下载授权锁 ID、地址以及密码词典。

2.1　多把锁管理方法

智能钥匙具有一把钥匙管理多个门锁的功能,锁和钥匙中分别存储对方的合法属性对[7]。钥匙中存储授权锁的属性集合,锁中存储开锁钥匙的属性集合。当钥匙中信息与锁中信息经双向认证确认匹配后才能启动开锁操作。锁和钥匙属性集数据结构如表 1 所示。钥匙属性由数据结构{KID,KA,LID,LA,RSSI}描述。其中,KID 和 LID 分别表示 4 Byte 的钥匙编号和锁编号,出厂时唯一确定;KA 和 LA 分别表示 1 Byte 的钥匙地址和锁地址,发卡时确定;

RSSI 可以反映钥匙与锁之间的距离,距离超过 1 m 则认定为不匹配。钥匙中保存已注册的锁属性集,锁属性由{LID,LA,KA,LPDI,RSSI}描述,LID 表示4 Byte的锁编号,LA 表示发卡时分配与钥匙对应的1 Byte锁地址,KA 表示发卡时分配的与锁对应的钥匙地址,LPDI 表示 4 bit 密码词典存储索引。钥匙将授权的锁属性集保存在 CC2530 内部 Flash 中,首地址为 0x3C800。锁属性集存储结构如图 2 所示。

表 1 锁/钥匙属性集数据结构

属性	(锁中)钥匙属性集					(钥匙中)锁属性集				
	KID	KA	LID	LA	RSSI	LID	LA	KA	LPDI	RSSI
含义	钥匙 ID	钥匙地址	锁 ID	锁地址	距离	锁 ID	锁地址	钥匙地址	锁的密码词典索引	距离
字节数	4	1	4	1	1	4	1	1	1	1

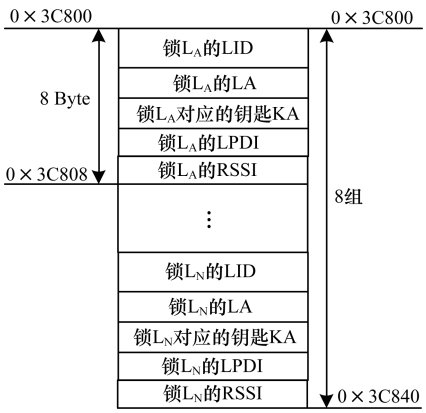


图 2 钥匙中锁属性集存储结构

2.2 多把锁认证过程

每个智能锁中含有一个特定的密码词典,锁在出厂时,密码词典通过专用随机数发生器唯一确定。同时,智能锁中存有至多 8 把授权钥匙的身份信息(ID 和地址信息,ID 为钥匙出厂固定信息,地址为发卡时随机分配的信息)。

每把智能钥匙中存有至多 8 把锁的密码词典和身份信息(ID 和地址信息,ID 为锁出厂固定信息,地址为发卡时随机分配的信息)。密码词典的物理存储结构如图 3 所示,首地址为 0x3C840。

图 3 钥匙中密码词典存储结构

在多对多配对的智能钥匙开锁中,使用双向身份认证和时间约束保证开锁的安全性。

认证过程为:在有开锁请求时,锁以广播方式主动向门锁附近发送开锁请求报文。钥匙收到请求报文后,首先依据明文 SID 字段顺序遍历锁属性表,判断是否存在 LID 与 SID 相同,存在说明该锁为授权锁,锁属性集存放首地址为 Address_LID。然后找到锁的 4 bit 密码词典索引存放地址为 Address_LPDI = Address_LID + 6,锁的密码词典存放地址为:Address_PD = 0x3C800 + (LPDI - 1) × 0x00401 +1。使用密码索引字 PI 从密码词典 PD 中确定一组密码字:$Address\_P_{DEC}$ = Address_PD + (PI - 1) ×0x00008,解密加密字段。然后判断明文身份信息与密文身份信息是否匹配,包括钥匙与锁地址、ID,同时取出请求报文发送时间。只有上述全部认证通过,才向锁发送混合明文与密文的认证应答报文。

锁针对应答报文,直接通过明文字段和自身密码词典解密报文,判断明文身份信息与密文身份信息的匹配性,然后判断应答时间是否在认证应答生命周期中。双向认证均通过再控制门开锁。

为提高安全性,认证应答过程具有生命周期。钥匙收到请求后立即启动定时器计时,得到生成应答报文的时间 *Ty*。应答报文发送时间 *Tack* = *Treq* + *Ty*,*Treq* 表示请求报文发送时间。锁发出含有 *Treq* 信息的请求报文后,也立即开启定时器计时,计算从发送请求到收到应答的延迟时间 *Td*。锁与钥匙间的通信距离为 0 m ~ 1 m 有效,单向射频通信延时 *Tc* ≈0.004 μs。若钥匙应答时间 *Tack* 满足 *Tack* + *Tc* ≤ *Treq* + *Td* ≤ 1 s,则应答报文在开锁认证应答生命周期内。

2.3 认证请求报文格式

当智能锁识别到有开锁请求时,发出加密的身份认证请求报文,等待智能钥匙用加密应答报文进行应答。智能钥匙收到请求报文后,判别{DA,FC,SA,DID}是否为请求报文指定信息,然后识别 SID 是否为合法授权门锁 ID[8]。如果是则组织发送加密认证应答报文,否则丢弃数据包。身份认证请求报文格式如表 2 所示。RSSI 值在接收缓存区数据域后 1 Byte 位置,由 CC2530 自动产生。表中 PD 表示锁对应的密码字典;P_{DEC} 表示解密密钥;P_{ENC} 表示加密密钥。

表 2　认证请求报文格式

功能	报文头				数据域			通信距离	校验字
	目的地址	功能编码	密码索引字	源 ID	源地址	目的 ID	请求时间		
字节数	1	1	1	4	1	4	3	1	2
字符值	DA	FC	PI	SID	SA	DID	T	RSSI	FCS
说明	广播地址 0xFF	0x05	用于从密码词典 PD 中寻找密钥 P_{DEC}	锁 ID(出厂唯一设定)	0x00	0xFF	锁发送认证请求报文的时间	CC2530 自动计算	CC2530 自动产生

2.4　认证应答报文格式

应答报文由智能钥匙发出,智能锁接收。钥匙收到 FC = 0x05 认证请求报文后,从接收缓存区读取 RSSI 进行距离识别、确认与授权门锁信息匹配后则组织发送应答报文。应答报文 8 Byte 数据域进行加密处理,PI 是应答装置产生的随机数,T 是与请求报文匹配的应答报文时间戳。智能钥匙的密码词典与智能锁配对,门锁对距离和应答报文的{SID,SA,DA,DID,T}字段进行匹配性识别。报文格式如表 3 所示。在认证请求报文格式和认证应答报文格式中,报文头不加密;数据域的 X 和 K 为 8 Byte,采用加解密算法,$Y = X \oplus P_{ENC}$;通信距离和校验字部分都不加密。

表 3　认证应答报文格式

功能	报文头				数据域			通信距离	校验字
	目的地址	功能编码	密码索引字	源 ID	源地址	目的 ID	请求时间		
字节数	1	1	1	4	1	4	3	1	2
字符值	DA	FC	PI	SID	SA	DID	T	RSSI	FCS
说明	锁的地址(发卡设定)	0x06	用于从密码字典 PD 中寻找密钥 P_{DEC}	钥匙 ID(出厂唯一设定)	钥匙的地址	锁 ID(出厂唯一设定)	钥匙发送认证应答报文时间	CC2530 自动计算	CC2530 自动产生

2.5　发卡报文格式

使用 UART 接口有线连接进行钥匙配置(发卡)。在智能锁上设置配置接口,智能钥匙插入配置接口,从管理员用户登录[9]后可进行钥匙的配置(发卡)和注销已发卡等操作。一旦钥匙插入配置接口,则只能执行发卡功能 HCfg_Key( )。也可以通过无线方式实现软发卡,钥匙收到发卡请求报文并通过身份验证后,关闭睡眠功能运行无线发卡功能 SCfg_Key( )。根据功能编码的不同,0x10 ~ 0x16 发卡通信报文分别代表发卡请求报文、初始化钥匙报文、发卡请求应答报文、执行结束应答报文、配置地址码报文、配置密码词典报文和注销钥匙报文。发卡通信报文格式如表 4 所示,共 2 + n + 2 Byte。

表 4　发卡通信报文格式

功能	起始标志	功能编码	数据域	校验字
字节数	1	1	n	2
字符值	:	FC	DATA	LRC
值和说明	0x3A	0x10 ~ 0x16 其他非法	依据 FC 具有不同长度 n 和不同内容	软件计算

2.6　密码词典与加解密方法

CC2530 内部 FLASH 存储 8 个锁的密码字典,每个密码字典与授权锁一一对应,每个密码词典 PD 存储结构为:{1 Byte 锁地址 LA,128 × 8 Byte 密码字典 PD}。密码字典保存 128 个 64 bit 长的密码字,双方通过动态密码索引字 PI 的传递进行密码同步。智能钥匙收到合法认证请求报文后,经由 SID 确定锁属性集合,然后通过锁属性集合中 LPDI 找到授权锁对应的 128 × 64 bit 的密码词典。请求报文中 PI 字段由锁装置通过实时时钟产生一个 7 bit 随机数,随机数值决定报文使用密码词典 128 个密钥当中的哪个。智能钥匙通过 PI 和 PD 找到 P_{DEC},解密请求报文的加密字段,判断数据域的合法性。钥匙通过 CC2530 内部随机数产生装置产生一个 7 bit 随机数,从同一个 PD 中确定对称密钥 P_{ENC},加密认证应答报文的数据域字段。

为尽可能降低身份认证卡的功耗,结合用户对智能锁系统的安全要求,本文设计未使用 CC2530 的 AES 功能,而是用以下的加密方法。智能锁系统和智能钥匙仅对报文的{SA,DID,T}字段加密,其他字段不加密。加密过程为:产生一个 7 位随机数填入报文 PI 字段,利用 PI 从 PD 中获得一个加密密码 P_{ENC},对 64 位的 X = {SA,DID,T}字段进行加密,加密算法 $Y = X \oplus P_{ENC}$。解密过程为:利用报文 PI 从配对的 PD 中获得解密密钥 P_{DEC},执行 $X = Y \oplus P_{DEC}$ 进行解密[10-11]。密码字长度 64 位,动态密码索引字 7 位,密码词典索引 4 位,综合密码二进制位数达到 75 位,再加上认证时间 T 的时效作用[12],这种加密方式可以满足智能门锁密码安全需要[13]。

2.7　睡眠-唤醒机制

智能锁与钥匙工作在 CC2530 点对点透传方式,

传输距离(有效识别距离)为门外 0 m ~ 0.8 m 时,无线传输速率可达 B = 100 Kb/s ~ 250 Kb/s[4-5]。物理层传输还需要增加 6 Byte 帧头,与 MPDU 负载共计字节数 n = 24 Byte。当波特率为 B Kb/s,1 位起始位、1 位停止位、无奇偶校验时,发送 n 个字节需要的时间 $T_{TX} = 10 \times n/B$ ms。若 B = 100 Kb/s,在近距离发送一个 24 Byte 报文需要 $T_{TX} = 10 \times 24/100 = 2.4$ ms。考虑钥匙唤醒后可能要发送 2 个认证请求报文钥匙才能收报一个完整的报文,即接收认证请求报文的时间 $T_{REQ} = 2T_{TX}$。钥匙发送应答报文时间 $T_{ACK} = T_{TX}$,CPU 处理信息时间 $TA < 1$ ms,启动发送和接收均需要 0.192 ms 延时。在需要应答时,钥匙唤醒后需要 $T_W = T_{REQ} + T_{ACK} + 1 + 2 \times 0.192 \approx 8.584$ ms,如果没收到认证请求报文不需要应答,则只需要工作时间 $T_W = T_{REQ} + 0.192 = 4.992$ ms。设定唤醒后的定时时间 Ton = 5 ms,如果有认证请求,则不理会 Ton 标识待处理完毕并发出应答后再进入 PM2 状态,如果无有效的认证请求报文则检测 Ton 标识置位就进入休眠(PM2)状态。

CC2530 运行过程的功耗:R_X 期间(8.2 - 2.4 = 5.8 ms)为 24 mA,T_X 期间(2.4 ms)为 29 mA,PM2 = 1 μA。通常情况下绝大多时间是工作在无认证请求的空闲状态,一个睡眠-唤醒周期的平均工作电流可以用下式近似估算:

$$I_{VAR} = \frac{(T_{REQ} + 0.192) \times I_{RX} + (T_{SLEEP} - T_{REQ}) \times I_{PM2}}{T_{SLEEP}}$$

其中,T_{SLEEP}是睡眠周期。选择 T_{SLEEP} = 1 000 ms,则一个睡眠周期的平均电流:

$$I_{VAR} = \frac{(T_{REQ} + 0.192) \times I_{RX} + (T_{SLEEP} - T_{REQ}) \times I_{PM2}}{T_{SLEEP}} = 0.120\ 8 \text{ mA}$$

要工作一年时间,需要的电池容量 $I_H = 365 \times 25 \times I_{AVR} = 87\ 60 \times 0.120\ 8 \approx 1\ 058$ mAH,一粒 CR2477 约 950 mAH。选择 CR2477 电池可工作时间为 $t = I_{HE}/(I_{AVR} \times 24) = 950/(0.120\ 8 \times 24) \approx 327$ d(约 10 个月)。如果 CC2530 的无线传输速率能工作在 B = 200 Kb/s,这时 T_{TX} = 1.2 ms,一粒 CR2477 约 950 mAH,大约可工作时间为 626 d(约 20 个月)。

结论:选择 Time1 作为工作时间定时器,选择定时值 $Ton \geqslant T_{REQ} + 0.2$ ms = 5.0 ms,允许中断,在中断服务程序设置 Ton 标识。设置睡眠定时器的睡眠周期 T_{SLEEP} = 1 000 ms,允许中断。

2.8 程序设计

复位后由 IAR 提供的启动程序引导转入 C 语言主函数 main,主程序流程如图 4 所示。复位启动函数由 IAR 提供(也可自己编写),启动后转入 C 语言的 main( )函数;中断向量由 ioCC2530.h 定义;硬件配置 32 MHz 偏外石英晶体。

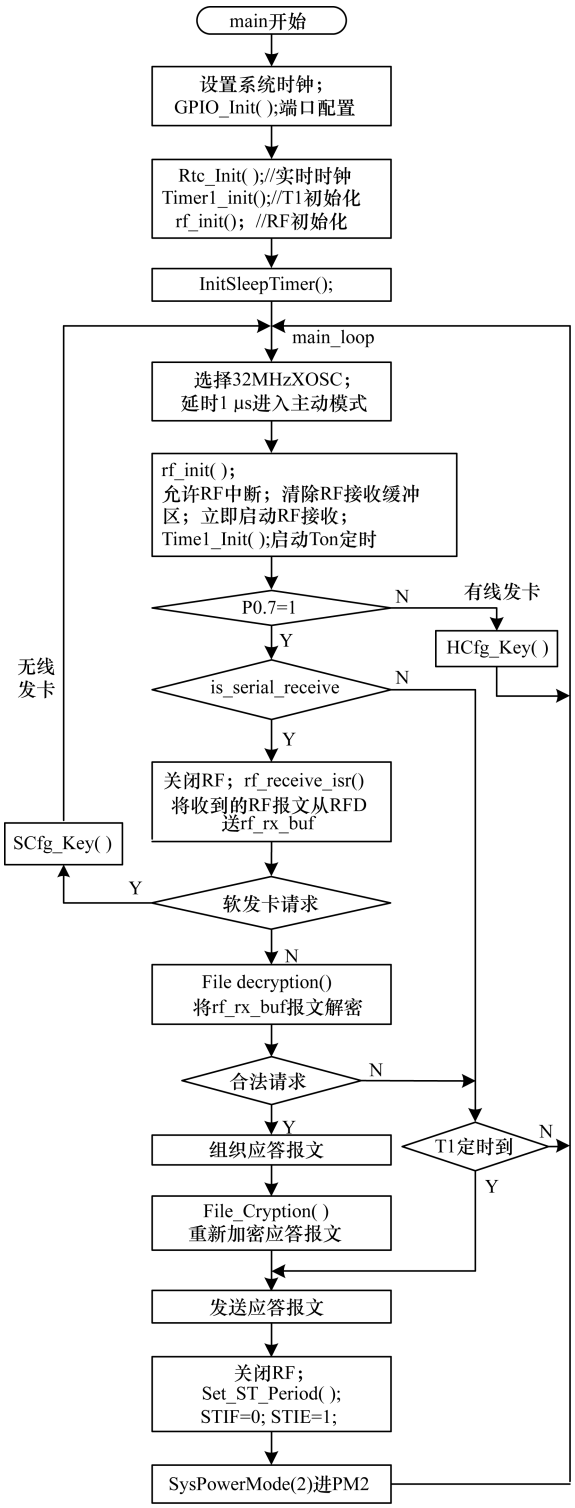


图 4 主程序流程

3 实验测试与分析

进行的功能和安全性测试有:锁与钥匙匹配性测试,距离测试,阻挡测试[14],门内外测试,多门锁测试[15]和按钮主动开锁测试等。门外钥匙与锁的距离测试和阻挡测试结果如表 5 所示。

表 5　门外钥匙与锁的距离测试和阻挡测试

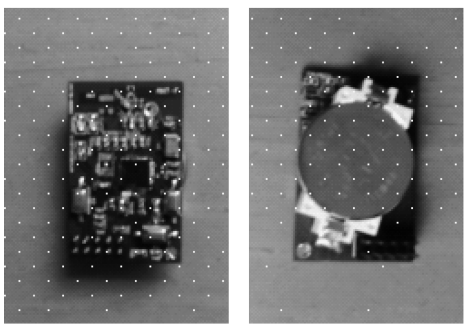
距离/m	能否开锁	阻挡物
0.3	能	口袋
0.8	能	食品袋
1.0	能	钱包
1.2	否	人
1.5	否	铁门

使用 3 把锁(L_A,L_B,L_C)、三把钥匙(K_1,K_2,K_3)进行多对多的测试,其中 K_1 只匹配 L_A,K_2 与 L_A 和 L_B 匹配,K_3 与 L_A,L_B 和 L_C 匹配。实验结果如表 6 所示。其中,Y 表示开锁成功;N 表示开锁失败。

表 6　锁与钥匙匹配性测试

按键	把手开锁			钥匙按键开锁		
	L_A	L_B	L_C	L_A	L_B	L_C
K_1	Y	N	N	Y	N	N
K_2	Y	Y	N	Y	Y	N
K_3	Y	Y	Y	Y	Y	Y

测试结果表明:1)钥匙能够对授权锁开门,未授权锁不能开门。2)当钥匙与门锁距离在 0 m ~ 1 m 时,能够开门,距离大于 1 m 时,不能开门。3)钥匙在门内与锁的距离小于 1 m 时,外部把手开门发送主动认证信息时,钥匙收不到请求报文,不能开门。4)钥匙放在口袋中,能够开门。钥匙前面有人阻挡时,不能开门。5)在小于 1 m 处,使用按键 K_2 和 K_3,能够主动开门。6)一把钥匙能够给授权的多个门锁开门。在功耗测试上,钥匙处于睡眠 PM2 模式时,测得电流不到 2 μA,通过 RF 发送或接收报文时,测得电流为 20 多 mA。使用 CR2477 给钥匙供电,从钥匙出厂至此已工作一年时间。智能钥匙实物照片如图 5 所示。



(a) 反面　　(b) 正面

图 5　智能钥匙实物照片

4　结束语

本文以 CC2530 为核心,用 RSSI 值进行距离有效性识别,利用锁 ID 与地址选择匹配密码词典,并用动态密码索引字在匹配密码词典中选择密码,确保了智能钥匙与智能锁具在多对多配对时的安全性,通过定时休眠与唤醒机制实现了低功耗。经理论分析和初步实验验证,该机制可满足智能家居锁具的安全性与使用方便性的要求。

参考文献

[1] 杨官贵,刘陆元. 自动感知的智能锁[J]. 中国安防,2014(19):64-66.

[2] 周晓凌,张力平. 智能门锁打造安全的智能家居[N]. 人民邮电,2015-01-16.

[3] 何文才,杨　伟,刘培鹤. 基于 SIM900A 模块的远程门禁控制系统的设计与实现[J]. 网络安全技术与应用,2014(12):12-13.

[4] 钟召辉. 基于 ZigBee 的无线智能锁设计[D]. 杭州:杭州电子科技大学,2013.

[5] 钟召辉,程知群. 基于 ZigBee 网络的智能锁系统研究[J]. 电测与仪表,2012,49(9):91-96.

[6] 瞿小玲. 基于 RFID 的低功耗智能门禁系统的设计与研究[D]. 成都:成都理工大学,2012.

[7] 倪　龙,和军平,林廖军. 交互式无线汽车智能钥匙系统设计[J]. 计算机测量与控制,2010(5):1136-1138,1157.

[8] 毛雅佼,孙达志. 一种新的 RFID 标签所有权转移协议[J]. 计算机工程,2015,41(3):147-150,166.

[9] 贾　宁. 基于 RFID 的智能购物管理系统设计与实现[J]. 计算机工程,2015,41(9):25-30,38.

[10] 黄　凯,金孝飞,修思文,等. 高效可配的对称密钥算法硬件架构设计[J]. 计算机工程,2015,41(9):85-91.

[11] 李志坚,肖熠琳. 一种基于二进制码调制的射频识别防碰撞算法[J]. 计算机工程,2015,41(2):308-312.

[12] 闫文耀,王志晓,李军怀,等. 基于多模智能网关的智能家居系统设计[J]. 计算机工程,2015,41(9):31-38.

[13] 张亚飞. 基于可信执行环境的智能密码钥匙设计与实现[D]. 西安:西安电子科技大学,2014.

[14] 王　鑫,周孝华,李冬阳,等. 基于 ZigBee 无线通讯技术的智能门锁设计[J]. 计算机光盘软件与应用,2015(3):304-305.

[15] 白　燕,楼燚航. 基于 ZigBee 的智能家居设计[J]. 电子制作,2014(12):60-61.

编辑　顾逸斐