基于Microchip公司的被动门禁系统分析与设计

程和生[1],丁 路[1],王丹丹[2]
(1.合肥工业大学 计算机与信息学院,安徽 合肥 230009;
2. 安庆师范学院 计算机与信息学院,安徽 安庆 246011)

摘 要:被动无钥门禁(PKE)作为新一代的遥控加密技术,是在传统的遥控车门开关(RKE)的基础上发展而来,正在逐步发展壮大且将会成为主流。文中剖析Microchip公司基于PIC16F639的PKE解决方案,结合作者设计体会,分析整个设计参考,展现整个设计理念,充分利用硬件与软件优势以及独特的用户身份的识别和自动开锁车门。Microchip公司的PKE方案的显著特点是采用KEELOQ加密技术,以及应答器中采用集成模拟前置终端,很大程度上降低了成本。基于该PKE设计参考研发的产品将有很好的应用前景。

关键词:被动门禁系统;滚码KEELOQ;设计参考
中图分类号:TP27 **文献标识码**:A **文章编号**:1673-629X(2011)04-0171-04

Analysis of Microchip Passive Keyless Entry System Reference Design

CHENG He-sheng[1], DING Lu[1], WANG Dan-dan[2]
(1. School of Computer & Information, Hefei University of Technology, Hefei 230009, China;
2. Dept. of Computers, Anqing Teachers College, Anqing 246011, China)

Abstract: As a new generation technology of remote control and encryption, Passive Keyless Entry (PKE) is growing gradually and becoming a mainstream of market. This article deeply analyzes the Microchip PKE solution which based on PIC16F639. According to the author's experience of PKE system development, the whole design concept of Microchip's reference design is presented and discussed, from the aspects of both hardware and software. Attractive features of Microchip PKE solution include KEELOQ encryption algorithm and the integrated analog front end, which gives high security and low cost. Products based on this PKE reference design have prospective applications.

Key words: passive keyless entry; KEELOQ; reference design

0 引 言

根据Strategy Analytics汽车电子服务发布的最新研究报告,被动系统(Passive Systems)将挑战遥控门禁系统(Remote Key Entry-RKE),到2016年大概有8.67亿美元市场规模[1]。目前汽车电子钥匙使用比较普遍且种类繁多,不仅在奔驰、宝马等豪华车型上广泛使用,中档车和国产车也相继采用,例如华晨、奇瑞等[2]。国际知名芯片公司,如Freescale、Atmel、Microchip、TI等,依托各自芯片硬件的特点提供了各自的门禁系统设计参考方案。国内车厂基本上使用国外公司的设计方案[3]。

Microchip公司的方案实现成本比较低,安全性能比较高,应用前景较好。但是Microchip设计参考方案,其中的文档资料介绍比较笼统,给参考设计者带来困扰和不便。文中根据使用Microchip设计参考和设计制作PKE过程的经验,对相关问题和技术细节作了比较详细的分析和讨论。文中采用了KEELOQ加密技术,是一种先进的RFID技术,具有数据存储大、非接触、识别距离远和保密性好等优点,应用广泛[4]。

1 系统构成和工作原理概述

PKE系统的组成是由低频(LF)发射器模块、特高频(UHF)解码器模块和应答器三部分组成,如图1所示。车载基站是由LF发射器和UHF解码器模块组成,应答器是钥匙部分。低频发射器发射125kHz低频未加密报文用来激活应答器,唤醒应答器的MCU数字部分。应答器主要由模拟前置终端(AFE)和数字部分组成,数字部分一般处于休眠状态,等待125kHz的LF信号的唤醒。解码器功能主要解密应答器发送433MHz的加密报文,且检验报文内容的正确性及通

收稿日期:2010-10-24;**修回日期**:2011-01-28
基金项目:安徽省自然科学研究项目(KJ2007A124ZC)
作者简介:程和生(1985-),男,安徽怀宁人,硕士研究生,研究方向为汽车电子、嵌入式系统。

知基站相应的操作。

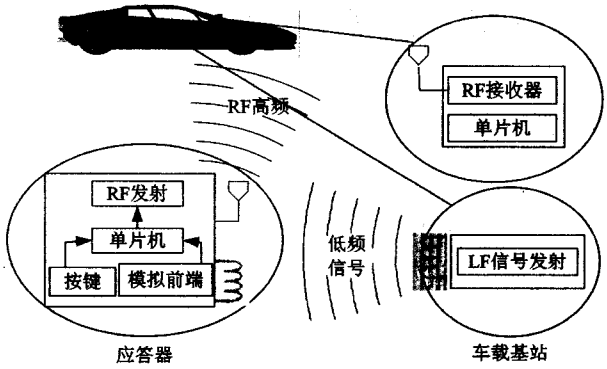


图 1 PKE 基本工作框图

PKE 工作的基本通信流程为,当应答器处于 LF 发射器发射的 125kHz 信号的有效范围内,应答器中的 MCU 的数字部分就被激活,激活之后,应答器发送 433MHz 的 UHF 加密报文,接着车载基站部分的解码器接收到 UHF 报文,进行解密、检验和数据确认。如果数据有效,基站则根据报文中的功能码指令,进行相应的操作。

2 PKE 硬件设计

2.1 车载基站

车载基站主要由 LF 发射模块、UHF 解码器接收模块等组成。基站中引入的 LF 信号是实现被动门禁的核心,通过一个触发信号(比如按键按下)激活 PIC 单片机,激活的单片机发送 LF 信号来唤醒应答器。

通过单片机 PIC16F636 的一个引脚发射 PWM 信号,如图 2 所示。经过 TC4422 电流驱动器。电流驱动器 U1 放大 PIC 微控制器输出的 125kHz 方波脉冲信号。U1 的方波输出通过 L1、C2、C3 和 C4 组成的 LC 串联振谐电路。L1 是用于 LF 信号的空芯电感。LC 串联振谐电路被调谐到 PWM 信号的频率时,天线辐射最强,LC 电路阻抗最小,使得过 L1 电流最大,来产生很强的磁场。可以通过 L1 两端的线圈电压来调谐 LC 电路。解码器部分,是由 GW-R5C1 接收模块、微控制器 PIC16F636 等组成,结构比较简洁。GW-R5C1 实时处于监听和接收 PWM 数据信号,当接收到的数据格式符合预定义格式,产生中断,PIC 微控制器读取接收模块数据。本设计使用的接收模块采用的是 GW-R5C1,应答器中发射模块 TX-1G,两者配套使用,可以实现 300 M 的通信,效果比较明显。

2.2 应答器

应答器是由 PIC16F639 微控制器,三个正交接收天线,振荡器与电感、电容做成的高频发射器,若干按钮等组成。PIC16F639 是由微控制器 PIC16F636 和模拟前置终端(AFE)集成,此器件可用于低频检测和双向智能通信应用。图 3 是 PIC16F639 应用电路图。

采用三个彼此正交天线 LX,LY 和 LZ,三个天线分别指向 x 轴、y 轴和 z 轴的三个方向,因此应答器可随时接收来自任意方向的信号,从而降低由天线的方向性而造成信号丢失的可能性[5]。三个天线和 PIC16F639 器件连接具有高的模拟输入灵敏度(高达 1mVpp)。各个天线的引脚的输入信号的检测是相互独立的,并加权相加。通过配置寄存器进行编程,每个输入可以单独的使能或禁止[6]。针对实际需求,可以通过配置寄存器 3、4 和 5[7]来选择开启或关闭某些天线,来减少能耗。

引入模拟前置终端(AFE)实现免持操作,由于应答器需要不停地检测是否有输入信号,就会产生很大的功耗,因此,为了减少工作的电流,当 AFE 搜索到有效 LF 输入信号时,通过输出使能滤波器唤醒 PIC16F639 的数字部分,这样就有效地减少功耗。

AFE 部分共享微控制器的三个 I/O 引脚:RC1,RC2,RC3,这些引脚在内部分别连接到 AFE,CS,SCLK/ALERT 还有以及 LFDATA/CCLK/RSSI/SDIO 焊盘上链接在一起,LFDATA/CCLK/RRSI/SDIO 和 ALERT 为 AFE 的输出[4]。SDIO、SCLK 和 CS 用于编程

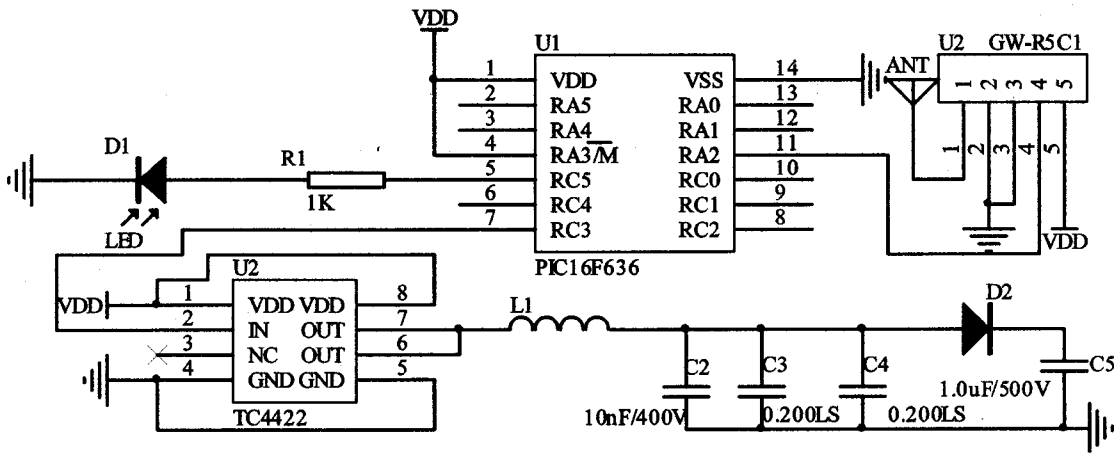


图 2 基站低频发射与 UHF 接收模块图

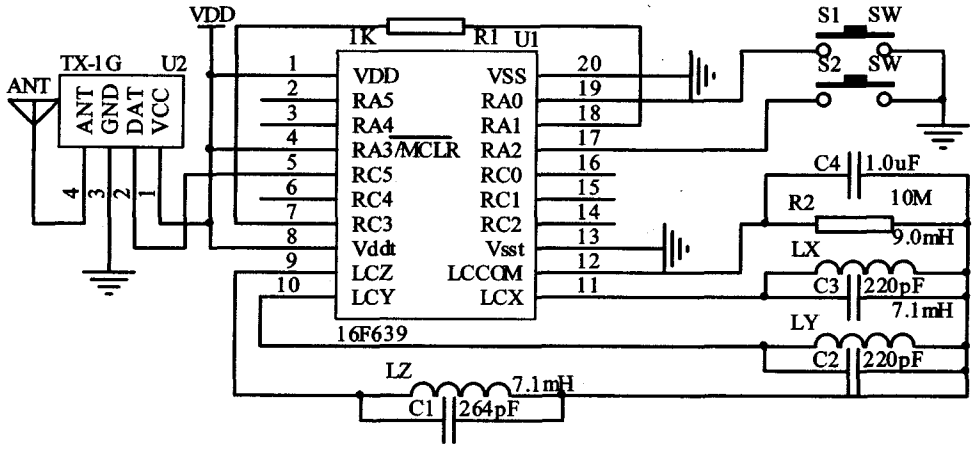


图 3　PIC16F639 应用电路

或读取 AFE 配置寄存器。在 LFDATA 引脚有 AFE 输出,ALERT 引脚有 AFE 输出或按下 PORTA 上的开关按钮时,在其中一种事件发生的话,钥匙的数字 MCU 就会被激活。

AFE 集成在 PIC16F639,这样可以减少设计的成本,是 Microchip 设计参考方案的一个优势。AFE 的使用主要通过 SDIO、SCLK 和 CS 引脚,SPI 方式进行编程配置参数。总共有 8 个配置寄存器。其中 6 个用于配置器件的操作,1 个用作列奇偶校验位,还有 1 个用于指示器件的工作状态,每个寄存器都含有 9 个位,其中包含一个行奇偶校验位,除状态(STATUS)寄存器是只读的外,所有寄存器都可通过 SPI 命令读写[7]。

3　报文格式

报文格式有两种,一种是 125kHz 的报文格式,另一种是 433MHz 的 UHF 报文格式。

3.1　低频报文格式与算法

LF 信号主要唤醒应答器,LF 数据包协议格式是先发射 125kHz 唤醒起始位,再激励代码和 UHF 响应间隙。125kHz 唤醒起始位主要是由自动增益控制器(AGC)稳定时间和唤醒滤波器序列组成,AGC 稳定需要 4ms,而唤醒滤波器序列是通过 AFE 配置寄存器 0[7]控制,本设计选择 2ms 高电平和 2ms 低电平。具体的 LF 激励报文,通过 PIC16F636 内部含有 CCP 模块来发送 PWM 信号[8],也可以通过引脚输出 PWM 信号的方式,如下:

(1)导通 4ms 以使应答器 MCU 中的模拟前置终端(AFE)的 AGC 稳定;

(2)PWM 关闭 500μs;

(3)在导通 2ms 后,再关闭 2ms 以使钥匙的 AFE 的输出滤波器,此处导通的方式可以软件配置,OEH(配置寄存器 0<8,7>[7])输出使能滤波器的高电平时间选择位,OEL(配置寄存器 0<6,5>[7])输出使能滤波器低电平时间选择位 6;

(4)PWM 关闭 50ms,保护时间。

为了设计方便,LF 信号触发方式采用了按键的方式,按下按键,就发送低频唤醒报文。

3.2　UHF 报文格式与算法

UHF 信号主要发送指令来操作和控制基站,PWM 调制方式的 UHF 报文格式,先序言序列,再头序列、数据位,最后时隙。UHF 报文由序言序列、头序列、数据位和时隙组成,序言序列是通知接收器准备开始接收报文,头序列是实现接收解码器与发射信号同步,头序列结束后,接收报文的数据部分,一般接收一个完整的报文之后插入保护时间间隔,可以确保发射的信号功率在法定的范围内。数据部分是由固定码和滚动码组成,固定码又是由序号、功能码和校验码组成,滚动码是由同步计数值、识别码(序号的低 10 位)、功能码经过加密生成的数据。解密 UHF 信号,可以通过检验识别码与序号的低 10 位,固定码中的功能码与滚动码中的功能码,以及同步计数值的有效性,具体的过程如下:

(1)通过 TMR0 中断采样单片机引脚数据,获取完整的数据报文;

(2)检验固定码中的序号与解码器保存序号是否一致,相同就转到(3),否则丢弃此报文,跳到(1);

(3)解密接收的报文,获得功能码、识别码和同步计数器值等;

(4)检验 10bit 的识别码与序号的低 10 位是否相同,是的话,转到下一步,否则丢弃此报文,跳到(1);

(5)检验固定码中功能码与滚动码中功能码是否相同,相同转到下一步,否则丢弃此报文,跳到(1);

(6)判断 FLAG 是否为 0,是的话,转到下一步,否则,就跳到(9);

(7)判断同步计数器值增加是否小于 16,是的话,转(10),当增加值大于 16 小于 32k 时,就暂时保存接收的同步计数器值 temp,并转到下一步,其他的情况,

就丢弃此报文;

(8)赋 FLAG=1,标记接收是第二个报文;

(9)判断同步计数器值与第一次接收同步计数值 temp,增加值是否小于 16,是的话,转到下一步,否则丢弃此报文,并认为上一次的报文无效,跳到(1);

(10)保存报文同步计数值,根据功能码,进行响应的操作,并跳到(1)。

4 安全性分析

安全性问题是 PKE 设计的核心,安全的加密技术可以确保用户的财产安全。KEELOQ 技术作为一种安全实用的加密解密技术,具有以下特点:

(1)KEELOQ 具有安全实用性,同一指令,经过 KEELOQ 加密,得到码字都不相同。

(2)通过特定方式学习获得密钥。

(3)这种技术能防止发送码被截获后再转发带来的危害。

正是这些特点使得 KEELOQ 技术越来越受重视,越来越广泛使用[9]。

4.1 编码密码生成

PKE 的基站可以通过简单编码、标准编码和安全编码的模式,获取不同的编码密码,编码密码主要参数是制造商代码、序号和同步计数值。制造商代码是每个制造商所特有的 64 位代码,序号是每款芯片分配的 28 位代码,同步计数值是应答器和基站之间的同步值,可采用 16 位或 18 位。

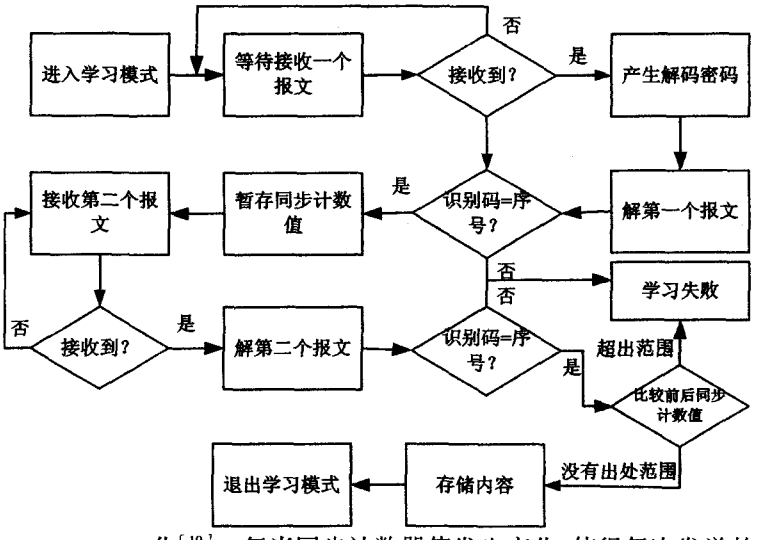
简单编码模式中,编码代码直接采用制造商代码,优点是简单易懂和解码程序容易实现,缺点是制造商代码泄露了,编码密码就丢失了,安全性比较差。标准编码模式,编码密码是由制造商代码和序号生成,由于序号的唯一性,生成的编码密码也是唯一的,优点就是编码密码得到安全的保护,编程实现复杂。安全模式下,编码密码是由制造商代码、序号和用户码生成,用户可以自行安排使用代码,这样编码密码安全性得到了进一步的提高。文中就以标准模式下为例,程序流程图如图 4 所示。

在标准模式下,编码密码是由制造商代码、序号和同步计数值生成。基站生成获得编码密码分两步:第一步,基站接收第一个 UHF 报文,可以获得序号、同步计数值和识别码,此时可以通过制造商代码和序号生成编码密码了。第二步,接收第二个报文,再用刚生成的编码密码,解密滚动码部分,解密后检验识别码是否与序号的低 10 位相同,同步计数值是否自动加一,相符的话,就保存编码密码、同步计数值和序号,退出标准模式。此过程完成了基站获取编码密码。

图 4 标准学习流程图

4.2 KEELOQ 加密算法

KEELOQ 加密技术,此技术是非线性加密技术,KEELOQ 加密技术的特点,当参与加密的数据其中有一位发生变化,使得加密生成的报文将近一半发生变化[10]。每当同步计数器值发生变化,使得每次发送的编码报文都是唯一的,且不重复,所以很难跟踪、截取和破译。这样有效克服了固定编码的缺点,具有很好的保密性[11]。下面给出加密算法的伪代码[12]:



#define BIT(X,N) ((X>>N)&0x01) 取数据 X 的第 N 位

(1)输入 32 位数据 x,NLF = 0x3A5C742E,64 位 key,i= 0;

(2)BIT(X,1)与 BIT(X,16)相异或得到 Y1, BIT(KEY,i&63)赋给 Y2

取 G= BIT(X,1) * 1+BIT(X,9) * 2+BIT(X,20) * 4+ BIT(X,26) * 8+ BIT(X,31) * 16, Y3 = BIT(NLF,G);

(3)Y1,Y2,Y3 相异或得到 y;

(4)Y 左移 31 位得到 Z1,X 右移 1 位得到 Z2,X= Z1 与 Z2 异或,i++;

(5)如果 i < 528,转到(2),否则,返回 x。

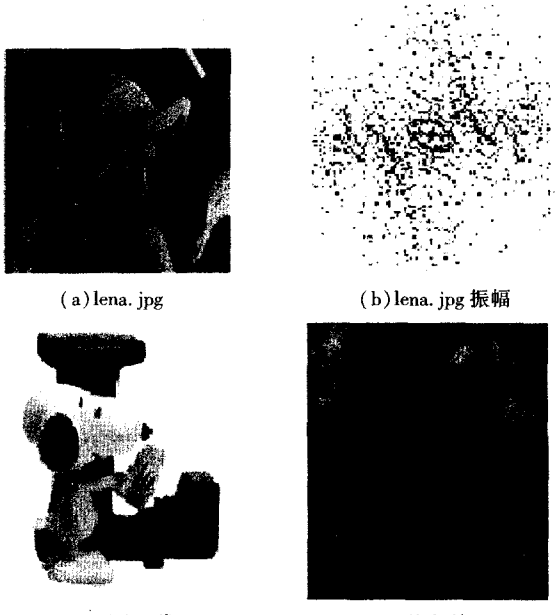
5 结束语

采用 KEELOQ 算法,每次传输的代码重复的概率非常小,PKE 系统可以自动地识别用户,增强了用户的安全。但是,缺点是制造商代码是核心密码,只要知道制造商代码就可以做成匹配的钥匙;受硬件设计限制,没有核心技术,受制于人。解决的方法,用户可以随机地选择数据参与编码密码的生成,这样就不担心制造

(下转第 178 页)

图形图像知识,实现了灰度图像的隐藏,隐藏的信息量也明显降低。

文中最重要的是实现了提取出的傅里叶相位图像与一幅新图像的傅里叶振幅图像结合,原始隐藏图像被恢复,验证了图像相位的主导性,且运用这种特性可有效地实现信息的隐藏与恢复。将数字水印技术与图像傅里叶的相位特性结合,在信息隐藏与恢复方面有明显的应用前景。



(a) lena. jpg (b) lena. jpg 振幅

(c) 原始图像 (d) 恢复结果

图 5 由相位信息与振幅信息恢复原始图

参考文献:

[1] GE Xiu-hui, TIAN Hao. Research on information hiding theoretic model[J]. Electronic Measurement and Instruments, 2007(2): 227-232.

[2] JIAN Zhao, Koch E. A Generic Digital Watermarking Model [J]. Computer & Graphics, 1998, 22(4): 397-403.

[3] 刘晓柯,苏显渝. 基于图像部分加入的数字全息水印技术[J]. 光子学报,2008,37(4):740-744.

[4] 钮心忻. 信息隐藏与数字水印[M]. 北京:北京邮电大学出版社,2004.

[5] 韩东初,刘缅方. 基于文本的信息隐藏技术研究[J]. 计算机安全,2008(8):60-63.

[6] 李丽娟,熊淑华. 基于文本的信息隐藏技术研究[J]. 现代电子技术,2006,29(5):67-69.

[7] 孙依薇,杨武剑. 信息隐藏在数字签名中的研究[J]. 电子科技大学学报,2009,38(11):49-52.

[8] 于帅珍,冯丽平. 数字水印的关键技术[J]. 计算机技术与发展,2010,20(2):148-151.

[9] 张 勇,赵东宁,李德毅. 数字水印技术及发展[J]. 解放军理工大学学报(自然科学版),2003,4(3):1-5.

[10] 袁占亭,张秋余,刘洪国,等. 一种改进的 LSB 数字图像隐藏算法[J]. 计算机应用研究,2009,26(1):372-374.

[11] Hayers M H. The reconstruction of a multidimensional sequencefrom the phase or magnitude of the FFT[J]. IEEE Transactions on ASSP, 1992, (4): 140-154.

[12] Hsiao Wen-Hsin, Hons B E, Sci B. Aspects of Fourier imaging[D]. New Zealand: University of Canterbury Christchurch, 2008.

(上接第 174 页)

商代码丢失了,加密技术也可以通过改进加密的算法,或是用户自选择其他的编码密码。

参考文献:

[1] Strategy Analytics[EB/OL]. 2010-09-21. https://www.strategyanalytics.com/default.aspx?mod=ReportAbstractViewer&a0=4936.

[2] 世界电子元器件. 无钥匙门禁系统完全解决方案[J]. 世界电子元器件,2009(7):1-2.

[3] MICROCHIP. Using the PIC16F639 MCU for Smart Wireless Application. pdf[EB/OL]. 2005. http://www.microchip.com/stellent/idcplg?IdcService=SS_GET_PAGE&nodeId=1824&appnote=en021451.

[4] 王浩远,梁昌勇,俞家文,等. 基于 RFID 技术的汽车总装 MES 系统研究[J]. 计算机发展与技术,2010,20(9):222-226.

[5] Low-Frequency Magnetic Transmitter Design[EB/OL]. 2010-09-21. http://ww1.microchip.com/downloads/en/AppNotes/00232B.pdf.

[6] 刘正琼. 智能 PKE 系统设计[J]. 仪器仪表学报,2007,28(4):319-322.

[7] MICROCHIP. Passive Keyless Entry (PKE) Reference Design User's Manual[EB/OL]. 2010-09. http://www.microchip.com/stellent/idcplg?IdcService=SS_GET_PAGE&nodeId=1406&dDocName=en024488&part=APGRD001.

[8] 李学海. PIC 单片机原理[M]. 北京:北京航空航天大学出版社,2004.

[9] MICROCHIP. PIC16F639Datasheet[EB/OL]. 2010-09. http://www.microchip.com/wwwproducts/Devices.aspx?dDocName=en022266.

[10] 袁 刚. PKE 系统中滚码技术的软件实现[J]. 合肥工业大学学报,2009,32(12):1859-1862.

[11] 董 辉,卢建刚. 一种基于 KEELOQ 的改进加密算法及其在单片机中的实现技术[J]. 电子技术应用,2004(9):14-17.

[12] HCS365datasheet[EB/OL]. 2010-09-21. http://www.microchip.com/wwwproducts/Devices.aspx?dDocName=en010765.