文章编号:1671-4598(2014)08-2600-03　　中图分类号:TP202　　文献标识码:A

基于 AES 算法汽车门禁系统的设计与研究

谷聚辉，张学毅，周志伟，周美琴，邓　杰
（湖南工业大学 电气与信息工程学院，湖南 株洲　412007）

摘要：针对汽车采用传统机械方式打开车门操作复杂、安全系数低等问题，设计了汽车智能门禁控制系统；通过车载基站与智能钥匙的双频通信，实现了车门的开与关，根据钥匙的位置，还可实现发动机的一键启动；考虑到无线通信的随机性和可变性，为保证信号传输安全，系统采用 AES 算法加密技术，加入了动态循环扩展密钥，并对整个系统进行 MATLAB 建模仿真；实验研究结果表明，系统加密性能好，密码破解率仅为，当信噪比为 10 dB 时，系统误码率小于 10^{-4}，符合无线通信系统的性能指标要求。

关键词：车载基站；智能钥匙；AES 算法；扩展密钥；误码率

Design and Research of Car Access System Based on AES Algorithm

Gu Juhui, Zhang Xueyi, Zhou Zhiwei, Zhou Meiqin, Deng Jie
(School of Electrical and Information Engineering, Hunan University of Technology, Zhuzhou　412007, China)

Abstract: For automobile using the way of traditional mechanical to open door with the problem of complex operation and low safety, designed the car intelligent access control system. By car base station with smart key dual communications, opening and closing of the door, according to a key position, but also to achieve a key to start the engine. Considering the randomness and variability of wireless communication, in order to ensure security of signal transmission, systems used the AES encryption algorithm, adding a cyclic extension of dynamic keys, and the entire system for modeling and simulation of MATLAB. Experimental results show that the system encryption performance was good, password cracking was only, when the SNR is 10dB, the system bit error rate of less than 10^{-4}, meeting the performance requirements of wireless communication systems.

Keywords: car station; smart key; advanced encryption standard algorithm; extension keys; bit error rate

0　引言

随着汽车的普及和人们对汽车安全性与可操作性要求的提高，传统汽车门禁系统采用单向通信方式，并结合人工按键进行操作，但由于工作不稳定而且麻烦，显然不能满足人们的要求。因此，设计了免持式被动无钥匙门禁系统，该门禁系统采用双向双频无线通信和信息交互认证方式，车主无需按键就能打开车门。同时，在信息安全方面有了很大的提高，使用了信息密钥长度和分组长度独立可变，具有非线性滚动编码技术的加密算法。

在目前汽车门禁系统中，关于信息加密技术主要有两种，分别是 KEELOQ 加密技术和 AES 加密技术。KEELOQ 加密技术采用滚动编码技术，不仅需要硬件的参与，而且可扩展性差，容易产生误操作。而 AES 加密算法是采用非线性位移滚动编码技术，在加密数据中由于采用滚动编码技术，使加密数据灵活多变。本文结合 KEELOQ 和 AES 加密算法的优点，对 AES 算法进行了优化，在加密过程中动态改变扩展密钥使其参与每一轮的循环加密计算。通过对加密后的密文进行研究，得出该 AES 加密算法不仅能够灵活加密，而且极大地降低了信息的可破解性。

1　门禁系统

汽车门禁系统的主要组成模块是车载基站和智能钥匙。当钥匙进入基站射频信号感应范围时，基站中的低频（LF）发射模块便对信号进行编码调制，此时会产生一个电压通过模块中的 LC 串联谐振电路产生高频电流，该电流通过天线产生强磁场，当钥匙进入该磁场时，钥匙中的线圈便会产生感应电动势。此时，钥匙便对该感应电动势进行解调与解码，恢复原来的命令信号，若该命令信号的身份标识与设定一致，微控制器（MCU）便会产生一个加密信号，再通过该模块中的高频（UHF）发射模块向基站发射一个 433.92 MHz 的高频加密信号。基站中的 UHF 接收模块接收到此高频信号，并对其进行解码验证，若其密钥正确，则微控制器驱动相应的执行机构打开车门。此外，若基站检测到钥匙在主驾驶位置时，便可一键启动汽车引擎。

整个汽车门禁系统的工作原理如图 1 所示。

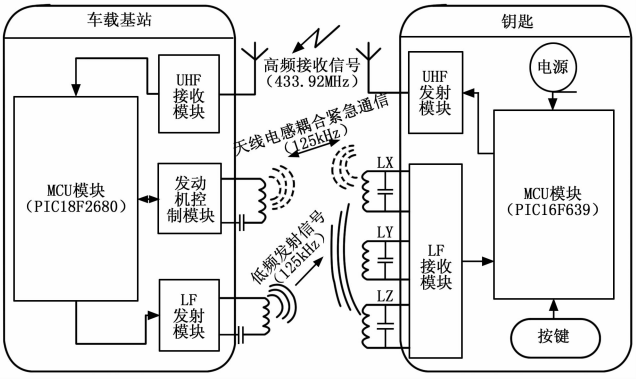

图 1　汽车门禁系统的工作原理

收稿日期:2014-01-13；　**修回日期**:2014-03-10。
基金项目:湖南省科技厅科技计划项目(2013FJ3099)。
作者简介:谷聚辉(1988-),男,河南洛阳人,硕士研究生,主要从事电工理论与新技术方向的研究。

1.1　车载基站

车载基站由 LF 发射模块、UHF 接收模块、MCU 及发动机防盗控制模块组成，微控制器采用 PIC18F2680 芯片。LF 发射模块采用 LC 串联谐振回路，所产生的信号经过编码调制后，因频率低还不能直接发送，需通过倍频方式来提高信号的频率，以达到系统所要求的信号发射频率，即发射一个频率为 125 kHz 低频命令信号。基站模块中的发射天线采用具有矩形结构的绕线天线，这种结构的天线设计，很大程度上能够使基站很好地感应到钥匙信号并被触发。UHF 接收模块用于接收来自钥匙端发射的高频加密信号，这里基站对高频信号的接收采用时分放大器序列混合接收机。该接收机对相应频段的信号有很强的捕捉能力，而且对信号的强弱有很好的取舍能力，对于一些低频或不在该频段的信号，接收机就会予以忽略，其不仅减小了基站的工作负担，而且提高了基站的工作效率。

车载基站控制流程如图 2 所示。

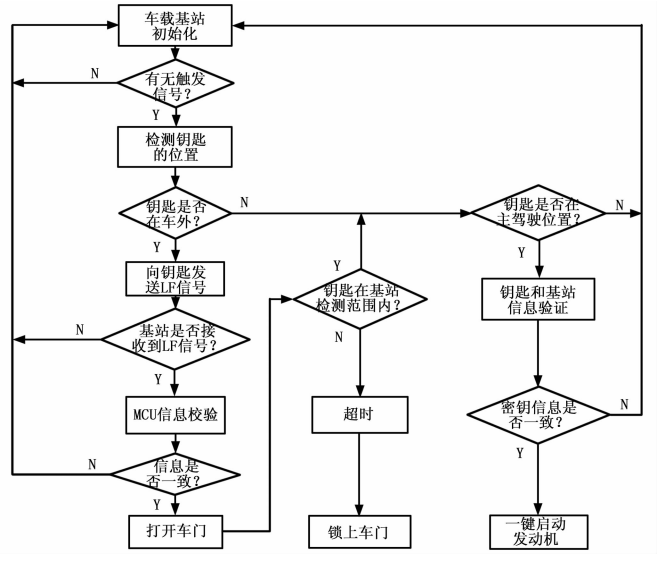

图 2　车载基站控制流程

这里的触发信号可以是汽车门把手上的微动开关信号、基站射频信号范围内的感应信号、智能钥匙按键信号等。车门打开后会出现以下两种情况：1）若车主进入车内，系统会继续检测钥匙的位置，一旦检测到钥匙在主驾驶位置时，通过钥匙和基站再一次双向身份认证，确定无误后按下钥匙上的启动按钮便可发动引擎，这样可以很好地防止当车主不在主驾驶位置时，汽车出现误启动的安全隐患；2）车门打开后，若车主携带钥匙又离开了汽车，一旦基站在相应区域检测不到钥匙触发信号时，车门便会自动锁住。当钥匙中电池电量将要耗尽时，发动机控制模块中的 LC 模块与钥匙端的 LC 模块通过电感耦合，使钥匙获得能量并通过身份认证，也可启动发动机。

1.2　智能钥匙

智能钥匙主要由 MCU、LF 接收模块、UHF 发射模块和按键组成。MCU 采用 PIC16F639 芯片，该芯片含有模拟前端（AFE）和数字微控制器结构。正常情况下，芯片处于休眠状态，当模拟前端接收到来自基站发射的 125 kHz 低频命令信号时，微控制器才会被唤醒。通过这种方式唤醒 MCU，不仅降低了电子元件因持续工作而老化，也延长了电池的使用寿命。此外，微控制器含有 3 个用于外接天线的引脚分别是 LCX、LCY、LCZ。其低频接收天线采用 3 组两两正交的 LC 并联谐振线圈，通过分析天线产生的感应电动势，可以得出感应电动势只与天线的位置有关。因而这种天线设计方式使钥匙在汽车基站周围空间的任意方向，天线面向基站的几率都接近 100%。当车主从不同方向接近汽车时，都能使钥匙和基站进行正常通信。

智能钥匙控制流程如图 3 所示。

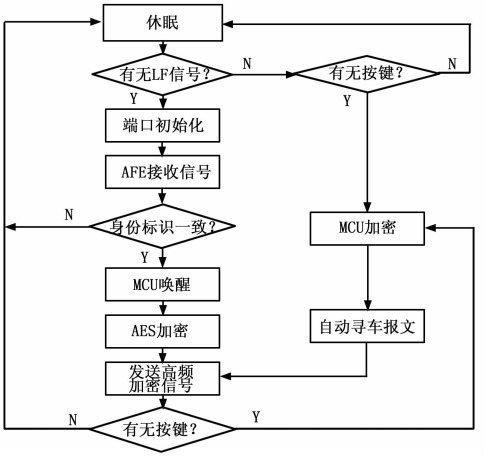

图 3　智能钥匙控制流程

2　AES 算法

信息安全是汽车门禁系统设计的关键，因为无线信道环境易变，导致信息在传输过程中容易被他人窃取，因此，很有必要对系统信息进行加密研究。AES 加密算法采用非对称滚动编码技术，在此基础上对 AES 加密算法进行了优化，利用动态循环扩展密钥参与每一轮的计算，并在加密数据中加入同步计数器来产生滚动编码，通过改变每次数值来产生一个新的编码，继而使每次生成的密文不同。它还具有独立灵活改变数据长度，减少了信息码中固定码的位数，优化对功能码的检错能力，使加密方式更加灵活。

AES 加密算法中密钥长度为 128 位，分别是由数据排列序号（8 位）、序列号（32 位）、计数器（32 位）、数据位（24 位）及保留位（32 位）组成。在信号加密过程中，所用的密钥一个用来加密，另一个用来解密。明文与密钥采用多轮加密解密方式，而且每轮需要多个密钥参与异或运算，优化后的算法所采用的扩展密钥很好地满足了这一加密要求。该算法明文采用 4×4 的矩阵结构，矩阵中的每一个元素代表一个字节，每一列代表一个字，总共 4 个字（128 位）。

AES 算法加密流程如图 4 所示。

假设 AES 加密算法变换轮数为 N_r，变换过程分为前（N_r—1）轮和第 N_r 轮。

1）前（N_r—1）轮：

首先，将明文信息（Plain Text）和密钥进行分组，使两者的分组数和每组字数保持一致；将每一组明文与密钥进行异或运算（AddRoundKey），得到一个新的矩阵（分组结构）；其次将新的矩阵进行字节代替变换（SubBytes），具体就是求其中每一个元素乘法的逆，再通过查 S－Box 得出；将上一步得到的矩阵，对其每一行进行循环移动一定的字节数，这里要求第 i 行向左循环移动 i 个字节，以此类推；然后，对分组结

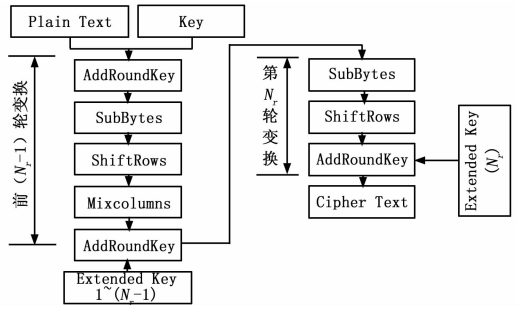

图 4　改进型 AES 算法加密流程图

构的每一列进行列混合变换（MixColumn），形式如 $\boldsymbol{Y}=\boldsymbol{AX}$，这里 $\boldsymbol{Y}$、$\boldsymbol{X}$ 分别是列矩阵，$\boldsymbol{X}$ 是原分组结构的列矩阵，Y 是新变换后的矩阵，其运算规则遵循异或运算和模乘运算。上述过程变换需要循环（N_r—1）次，则需要（N_r—1）个扩展密钥（Extended Key）参与异或运算。

2）第 N_r 轮：

将前（N_r—1）轮变换结果进行字节代替变换和行位移变换后得到一个新的分组，将新分组再与扩展密钥进行异或运算，最终便可得到一个密文，该密文就是经过 AES 算法加密后的密文，即钥匙端向基站发射的高频加密信号。

假设密钥为：0101010202020303030000A0A0A0B0B0B，共 128 位，序列号为：1A2B3C4D，计数器为：0A0B0C0D，数据位为：010203，保留位为：00000000。由密文的组成原理可知，前八位的数据排列序号决定了密文中序列号（00）、计数器（01）、数据位（10）、保留位（11）的排列顺序。当数据排列序号为 00011011 时，通过 AES 算法加密运算后，得到的密文结果为 5E26351B6A8FB3862C35D56CE5203C3D，当数据排列序号为 01001011 时，得到的密文结果为：3C6D56F500BB546C223B9CD6A335E6CC。

从上述得出的密文结果中，可以看出仅仅改变数据排列序号中的两位，所生成的密文完全不同，如果改变算法密钥中的任意一个组成部分，也可得到不同的密文。这就说明只要数据排列序号发生变动，得到的密文就会发生很大的改变。因此，只要动态改变每次发送的数据排列序号，那么每次得到密文也就不同，显然每一次发送的高频加密信号都不一致，这也使信号在传输过程中密钥不容易被他人窃取，同样，也符合门禁系统对汽车安全性的要求。

3　系统仿真分析

由于无线通信信道存在随机性，信号的传输容易受到噪声和电磁干扰的影响，可能会产生信息丢失或乱码，导致系统不能正常工作。因此，本节对整个无线通信系统进行建模仿真，并在信道中加入噪声和干扰，使仿真信道更好地接近真实物理信道。系统发射的低频信号和高频信号均采用曼彻斯特编码，它是一个同步时钟编码技术，通过频率是数据信号 2 倍的时钟信号与数据信号进行异或运算得到。由于发送信息的每一位都发生了跳变，也很好的解决了低频和高频信号传输不同步的问题。对于信号调制采用幅度键控调制（ASK），则 ASK 信号产生的表达式为

$$S_{ASK}(t) = S_d(t) \cdot A\cos_{\omega_0} t \tag{1}$$

其中：$S_d(t)$ 为数字基带信号，$A\cos_{\omega_0} t$ 为调制的载波信号，数字基带信号可写

$$S_d(t) = \Sigma_n a_n g(t-nT) \tag{2}$$

式中，T 为码元宽度；$g(t)$ 是宽度为 T，高度为 1 的矩形脉冲；a_n 为二进制码元，且 $a_n = \begin{cases} 1 & p \\ 0 & 1-p \end{cases}$，其中 p 为二进制码元 0 或 1 发生的概率。设系统采样时间为 0.01 s，将低频数据位发射速率设定为 3.9 kbit/s，高频数据比特率为 2 kbit/s，ASK 信号带宽为 $B = 2f_t$，式中，$f_t = \frac{1}{T}$ 为码元速率，由此可计算出信号的带宽。短距离无线通信系统的通信信道相当于一个小尺度衰落模型，信号传输是通过散射来实现的。运用概率统计学可知，无线低通信道的冲击响应为一个零均值复高斯随机过程，其幅度服从瑞利分布，其瑞利衰减概率密度函数为

$$p(r) = \frac{r}{\sigma^2}\exp(-\frac{r}{2\sigma^2}), r \geqslant 0 \tag{3}$$

在信号发射过程中，信号产生的衰减会影响接收信号幅度，由于信号幅度参数 r 服从瑞利分布。这里将无线通信信道建模为瑞利衰减信道，设多普勒频移为 50 Hz，离散路径延迟时间为（1e—6）s，路径数为 N（N>0），对所建模型进行仿真，得出信号传输误码率如图 5 所示。

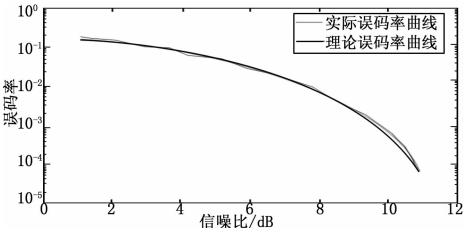

图 5　系统信号传输误码率曲线

图 5 中，横坐标是系统的信噪比（SNR），纵坐标是信号误码率（BER）。评价一个通信系统的好坏，信噪比和误码率作为一个重要的衡量指标。从该图可以得出，当系统信噪比在 0～4 dB 之间误码率比较高，随着信噪比的增大，当信噪比在 10 dB 时误码率符合通信系统对信号传输误码率的要求。这里，对信噪比为 10 dB 的整个通信系统进行分析，可验证门禁系统信号发射速率的最优值，在低频信号发射频率为 125 kHz，高频信号发射频率为 433.92 MHz 的条件下，系统无线通信信号此时的失真最小，也更好地保持了发送信号和接收信号的一致。因此，选择合理的信号发射模型和信道模型，对整个系统的仿真和数据分析起到了至关重要的作用。

4　结束语

传统的汽车门禁系统功能单一，而且工作不稳定，新型免持式无钥匙门禁系统的出现，不仅融入了更为人性化的设计元素，而且也极大地方便了人们的生活。基于 AES 算法汽车门禁系统通过双向无线通信方式，进行车门的开关及发动机的一键启动，符合人们对智能汽车的要求。对 AES 加密算法进行研究，得出基站和钥匙的每一次通信所使用的密钥都不相同，不仅提高了信息的安全性，而且有效地保护了用户的财产安全。本设计还采用了低功耗器件，并对电路的设计进行了优化，延长了钥匙中电池的使用寿命，即使当钥匙电量几乎耗尽时，车门和发动机照样也可以打开和启动。由于其成本低，使用方便，安全可靠，未来在普通汽车上的应用前景将更加广阔。

（下转第 2605 页）

相的顺序依次写入 FIFO，PC 机先从 FIFO 中读取所有的数据，然后按照顺序将数据分成 A 相、B 相、C 相三段显示。

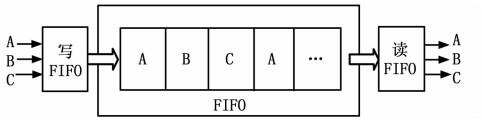

图 5　FIFO 数据流示意图

4　实验验证

选择 FPGA 仿真信号作为三相输入，通过在 PC 机上实时控制参数变化、调节 PI 参数，并观测锁相环的输出来实现锁相环性能的实时监测。

PC 机上的锁相环性能测试界面如图 6 所示，设置 FPGA 程序流水线的重复周期为 10 kHz，则 FPGA 模拟通道采样率为 10 kHz，设置 KI 参数为 4 000，KP 参数为 10。设置如下仿真信号的参数进行实验：

设置 A、B、C 三相的幅度为 3 V，频率为 50 Hz，观测锁相环输出；

设置 A 相幅值为 4 V，其他参数不变，观测锁相环输出。

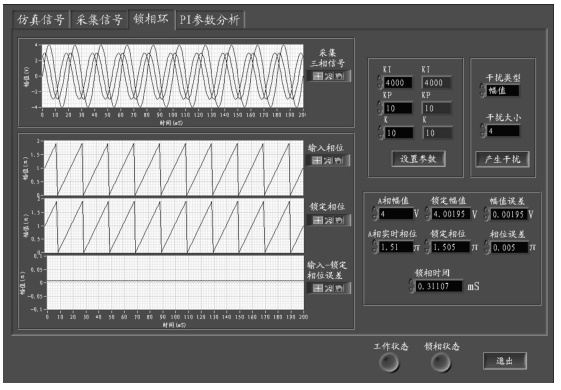

图 6　锁相环性能测试界面

记录实验结果如表 1 所示。当锁相环输出稳定时，相位误差约为 0.03 rad。

经分析，锁相程序的运行周期为 10 kHz，由公式（2）可知，T 为 0.1 ms，f 为 50 Hz，则可知 $\Delta\theta$ 约为 0.031 4 rad，如果相位误差不考虑 $\Delta\theta$ 的影响，可得出锁相输出与输入信号相位基本一致。从实验结果中可知，当 A 相电压的幅值突变时，锁相环在 0.31 ms 后跟踪到输入相位，FPGA 程序的运行周期为 0.1 ms，锁相环经过 3 个周期的运算后跟踪到相位，如果不考虑信号采样的一个周期，则实际上锁相环经过 2 个周期的运算就能跟踪到相位。

表 1　实验结果

输入信号	锁相误差 /rad	锁相时间 /ms
$\mu_a=\mu_b=\mu_c=3$ V，$f=50$ Hz	0.031 42	——
$\mu_a=4$ V，$\mu_b=\mu_c=3$ V，$f=50$ Hz	0.031 56	0.31

由此可见，该锁相环具有锁相实时和锁相误差小的特点，并可直接在 PC 机上进行性能监测。

5　结束语

本文介绍了基于 LabVIEW FPGA 的三相锁相环实现的新方法，该方法利用 LabVIEW 图形化语言编程控制 FPGA 的逻辑配置，与传统设计方法相比，简单灵活，可靠性高，实用性强，设计的三相锁相环具有良好的人机交互界面。经过实验分析，锁相环具有较高的实时性和较小的锁相误差，在电力设备的锁相控制中具有较高的应用价值。

参考文献：

[1] Hu J B，He Y K，Nian H. Enhanced control of DFIG used back－to－back PWM voltage－source converter under unbalanced grid voltage conditions [J]. Journal of Zhejiang University Science A，2007，8 (8)：1330－1339.

[2] 龚锦霞，解　大，张延迟. 三相数字锁相环的原理及性能 [J]. 电工技术学报，2009，24 (10)：94－99.

[3] National Instruments，NI sbRIO－961x/963x/964x and NI sbRIO－9612XT/9642XT User Guide [Z]. 2010.

[4] 田桂珍，王生铁，林百娟，等. 电压不平衡条件下改进型锁相环的设计与实现 [J]. 电力电子技术，2010，44 (4)：85－86.

[5] 王颢雄，马伟明，肖　飞，等. 双 dq 变换软件锁相环的数学模型研究 [J]. 电工技术学报，2011，26 (7)：237－241.

[6] 胡仁喜，高海宾. LabVIEW2010 中文版虚拟仪器从入门到精通 [M]. 北京：机械工业出版社，2012.

[7] 刘　涛，张盛兵，黄小平. 微处理器中异步 FIFO 的一种优化方法 [J]. 计算机测量与控制，2009，17 (1)：148－149.

[8] National Instruments，LabVIEW FPGA Design for Code Modules [Z]. 2010.

(上接第 2602 页)

参考文献：

[1] Hammad I，Kamal El－sankary. High－speed AES encryptor with effcient merging techniques [J]. IEEE Embedded Systems Letters，2010，2 (3)：67－71.

[2] 昂志敏，孙述鹏，韦　康，等. 汽车智能无钥匙门控系统的设计与应用 [J]. 电子技术应用，2007，(8)：48－51.

[3] Becker J. Passive keyless entry and drive system [J]. Auto Technology，2002，(2)：56－58.

[4] 杨　毅，刘志强. 基于对称分组加密算法的汽车门禁控制系统 [J]. 仪表技术，2011，(10)：56－57.

[5] Lee Y，Nolan J. Low frequency bidirectional communication transponder for security and automotive applications [J]. Circuit Theory and Design，2005，(2)：185－188.

[6] 程和生. 被动门禁系统的设计及关键技术的研究 [D]. 合肥工业大学，2011，3.

[7] Microchip. PIC12F635/PIC16F636/639 Data Sheet：8/14－Pin Flash－Based，8－Bit CMOS Microcontrollers with nano Watt Technology [Z]. 2005.

[8] 王　超，郑　宾，吴柯锐. 汽车被动无钥门禁系统（PKE）研究 [J]. 电脑知识与术，2009，19 (5)：5304－5305.

[9] 杨　彪. 125 kHz 射频识别收发器解调模块的研究与设计 [D]. 武汉：华中科技大学，2008，5.