DOI:10.13657/j.cnki.gxkxyxb.2013.01.009

广西科学院学报
Journal of Guangxi Academy of Sciences
2013,29(1):28～30
Vol. 29,No. 1 February 2013

射频识别系统加入 AES 算法的数据加密通信设计

RFID System based on the Data Encryption Communication with Advanced Encryption Standard Algorithm

曹林峰[1],蒋 泰[2],高雪晨[1]
CAO Lin-feng[1],JIANG Tai[2],GAO Xue-chen[1]

(1.桂林电子科技大学电子工程与自动化学院,广西桂林 541004;2.广西瀚特信息产业股份有限公司,广西桂林 541004)
(1. Institute of Electronic Engineering and Automation,Guilin University of Electronic Technology,Guillin, Guangxi,541004,China;2. Guangxi Hunter Information Industry Co. ,Ltd. Guilin,Guangxi,541004,China)

摘要:将高级加密标准(Aadvanced Encryption Standard,AES)算法加入射频识别系统(RFID)系统,对 RFID 数据进行加密通信设计,提高 RFID 系统的数据安全性,有效地防止恶意入侵。

关键词:射频识别系统 数据安全 AES 算法
中图法分类号:TP391.45 **文献标识码**:A **文章编号**:1002-7378(2013)01-0028-03

Abstract:AES Advanced Encryption Standard algorithm was applied to the RFID system to optimize its data encrypted communication,which can effectively prevent malicious intrusion and improve data security of the system.

Key words:RFID,data security,AES encryption

射频识别(Radio Frequency Identification,RFID)是一种无线通信技术,它通过无线电讯号识别特定目标并读写相关数据。由于其具有识别过程中无须人工干预、能同时识别多个高速运动的目标等方面的优势,广泛应用于制造、军事、消费、物流、贸易、公共信息服务等各个领域[1]。随着物联网的不断发展,其核心技术 RFID 的应用范围越来越广,但是随之而来的数据安全问题也越来越突出,尤其是在 RFID 系统的数据通信安全方面越来越严重。在物流管理等系统中,虽然外界入侵可能会干扰到系统的工作,但是不会产生很大的个人利益,所以采用简单的电子标签即可。而对于涉及金融资产的 RFID 相关系统中,由于对任何人都是开放的,所以潜在的入侵是无法界定的,如果非法入侵成功,则有可能对整个系统的安全构成威胁。因此针对不同的应用领域,对 RFID 系统的数据通信要求不同,尤其是对涉及金融资产的 RFID 系统,保证数据通信安全是非常有必要的[2]。

RFID 系统的数据通信安全最重要的就是确定读写器能够准确识别到合法的电子标签,同时电子标签也能正确识别到合法的读写器,保证彼此能够进行相互身份认证,这样就可以防止恶意入侵[3]。我们把高级加密标准(Aadvanced Encryption Standard,AES)算法与 RFID 通信系统结合在一起,对 RFID 数据进行加密通信,从而保障 RFID 数据通信的安全。

1 RFID 系统加入 AES 算法的加密通信基本原理

在 RFID 系统中加入 AES 算法可以增强系统的数据通信安全,防止恶意入侵。结合 AES 算法,

收稿日期:2012-10-18
修回日期:2013-01-06
作者简介:曹林峰(1986-),男,硕士研究生,主要从事物联网与应用研究。

本设计中的 RFID 系统采用导出密钥的相互鉴别方法来进行读写器与电子标签之间的身份认证。其中 KM 表示主控密钥,主控密钥是读写器、电子标签生产过程中固定分配的,KX 表示私有密钥,可以通过 AES 算法计算出来。AES 算法中所用到的密钥实质就是在加密过程或者解密过程中系统输入的参数。RFID 系统加密通信基本原理如图 1 所示。

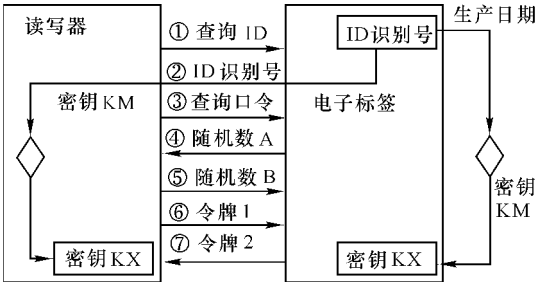

图 1 RFID 系统加密通信基本原理

图 1 中 RFID 系统加密通信的具体步骤如下:(1)当电子标签进入读写器的读写范围后,读写器通过天线发射的射频信号将标签激活,然后根据读写器的查询 ID 指令,电子标签将自己的 ID 识别号发送给读写器[4];(2)读写器接收到电子标签的 ID 识别号后,利用自身的主控密钥 KM 和接收到的标签 ID 识别号,通过 AES 加密算法计算出私有密钥 KX;(3)接着读写器再向标签发送一个查询数据的指令,电子标签即刻发送一个随机数 A,读写器接收到随机数 A 后,也立即发送一个随机数 B 给电子标签;(4)然后读写器利用计算出的私有密钥 KX 和 AES 算法以及随机数字 A、B 两个参数计算出令牌 1 发送给电子标签;(5)电子标签接收到令牌 1 后,利用自己的私有密钥 KX 和 AES 解密算法,计算出随机数 A,如果得出的随机数 A 与电子标签之前发送的随机数 A 一样,则电子标签可以确定读写器是合法的;(6)同样,电子标签在接收到读写器发送的随机数 B 后,也利用自己的私有密钥 KX 和 AES 算法以及随机数字 B 计算出令牌 2 发送给读写器;(7)读写器接收到令牌 2 后,利用自己的私有密钥 KX 和 AES 解密算法,计算出随机数 B,如果得出的随机数 B 与读写器之前发送的随机数 B 一样,则读写器可以确定电子标签也是合法的。

采用导出密钥的鉴别方法来进行读写器与电子标签之间的身份认证具有很多优势:首先,每次不用传输密钥,只是传输带有密码的随机数字;其次,总是两个随机数同时加密,排除了为了计算密钥用随机数 A 执行逆变换获取令牌 1 的可能性;同时,通过严格使用来自两个独立源(标签、读写器)的随机数,使回放攻击而记录鉴别序列的方法失败。

2 RFID 系统加入 AES 算法的加密通信设计

2.1 RFID 系统的整体硬件架构

本设计的 RFID 系统的整体硬件架构如图 2 所示,上述的 AES 算法只是一个抽象的描述,具体的加密算法可以在单片机 STC89C52 上实现。该 RFID 系统以 STC89C52 单片机为整个系统的控制中心,分别与 PC 机、AES 加解密模块、读卡器 MF RC500 相连接,起到整个系统的核心作用,PC 机通过 RS232 向单片机发送控制指令,指导单片机完成读写、加解密等系列动作[5]。

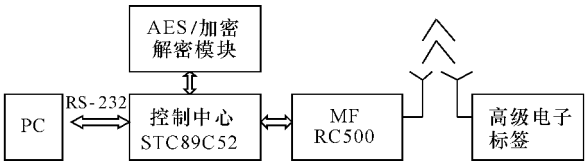

图 2 RFID 系统的整体硬件架构

2.2 AES 算法的实现与优化

AES 算法在不同的平台上实现还要进行相应的优化工作。本设计采用 8 位单片机 STC89C52 作为 AES 算法实现平台,其中,数据块长度、电子标签 ID 和密钥长度都为 128 位。随机数 A 和 B 均是 64 位。由于 RFID 系统中电子标签成本的限制,遂采用 8 位单片机进行试验平台。具体过程如下:(1)ExpansionKey(扩展密钥)在电子标签中是固定不变的,在出厂时就设置好,并且固定存储在存储器中,加密时再用查表法进行读取具体的数据;(2)SubBytes(字节替换)可以采用一个容纳 256 个元素的查表来实现;(3)ShiftRows(行偏移)可以用一个含 256 元素的查表来实现;(4)MixColumns(列混合)可以使用 N 次线性转换实现;(5)由于 AddRoundKey(密钥加层运算)、SubBytes、ShiftRows 都是针对字节的运算,为了减少系统开销,可以把三者结合在一起,每一次对一个状态字节只执行一次运算[6]。

优化的 AES 算法如图 3 所示。

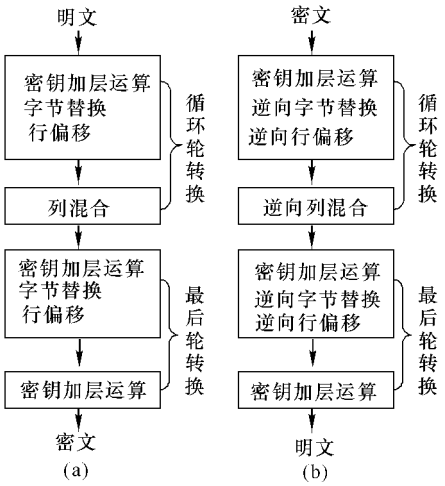

图 3 优化的 AES 算法加密/解密过程

(a)加密,(b)解密。

3 实验与仿真

AES 算法可以在 STC89C52 单片机上进行实验。本设计中采用 11.0592MHz 的晶振,其中加密程序占用 986 个字的程序存储单元,6524 个指令周期,这在普通的单片机上一般都可以实现的。同时 AES 的解密程序占用 896 个字的程序存储单元,5623 个指令周期,其中加密、解密速度都可以达到 45kb/s。根据以上实验步骤和优化方法可以得出如下实验结果:

主控密钥:0213ac1d2057c25c35fed0b021e01f0c (128bit)

加密明文:0120221d001ddd1200dde11dff10d110

密　　文:6522189d1cf451dc24f1c424f1cc12d1

解密密文:6522189d1cf451dc24f1c424f1cc12d1

明　　文:0120221d001ddd1200dde11dff10d110

实验结果表明,基于 AES 高级密码算法的 RFID 通信系统,可以实现读写器与电子标签之间的安全通信,有效防止非法入侵,同时采用 AES 算法在使用很少的计算能力下,依然能够提供非常高的安全性,并且在算法层面上保证了不可破译性[7]。RFID 系统安全性的提高,进一步促进了物联网的快速发展,拓展了 RFID 系统的应用范围,尤其是在涉及金融、军队等数据安全要求严格的领域。

参考文献:

[1] 黄友森,米志强. 射频识别(RFID)技术与应用[M]. 北京:电子工业出版社,2011.
[2] 姚磊,单玉峰. 射频识别(RFID)原理与应用[M]. 北京:电子工业出版社,2008.
[3] 刘岩. RFID 通信测试技术及应用[M]. 北京:人民邮电出版社,2010.
[4] 黄玉兰. 物联网射频识别(RFID)核心技术详解[M]. 北京:人民邮电出版社,2010.
[5] 关强. RFID 系统测试与应用实务[M]. 北京:电子工业出版社,2010.
[6] 谷大武, 徐胜波. 高级加密标准 AES 算法[M]. 北京:清华大学出版社, 2010.
[7] 石秀民,魏洪兴. 嵌入式系统原理与应用[M]. 北京:北京航空航天大学出版社,2007.

(责任编辑:邓大玉)

(上接第 27 页)

将提高企业计划层对生产制造车间的管理效率。

3 结束语

本文针对当前 ERP 与 MES 集成模式中存在的不足,根据消息传递集成模式的原理,提出运用 BizTalk Server 中间服务器解决 ERP 与 MES 间数据传输问题的集成模型,并结合柳州某汽车配件企业信息化集成项目的实际情况,对该模型进行实例应用。实例结果表明,该方法很大程度上屏蔽了数据库中数据的异构性,应用在 ERP 与 MES 集成方面可行有效。

参考文献:

[1] 高远飙,刘仁金. ERP 与 MES 集成技术及其应用研究[J]. 计算机应用与软件,2009,26(9):69-74.
[2] 马万太,楼佩煌. 基于 XML/OPC 的 ERP/MES/底层控制集成系统研究[J]. 机械科学与技术,2005,24(3):346-349.
[3] WANG Y. SCM/ERP/MES/PCS integration for process enterprise[C]. Beijing: The 29th Chinese Control Conference,2010:5329-5332.
[4] 王成桥,乔非. ERP 与 MES 集成模式方法与研究[J]. 工业工程,2006(2):68-72.
[5] 余腊生,王鲁鹏. 面向消息的实时中间件的研究与实现[J]. 计算机工程,2004,30(11):16-18.
[6] 赖成. 基于 BizTalk Server 的格卫企业服务总线设计[D]. 上海:复旦大学,2011:5-14.
[7] 何忠,张申生. XML 映射器的实现[J]. 计算机工程与应用,2004(4):137-139.
[8] KENT W, CARL D. Microsoft BizTalk 2010: line of business systems integration[M]. Birmingham: Packt Publishing,2011. 237-315.

(责任编辑:邓大玉)