第34卷 第15期 计 算 机 工 程 2008年8月
Vol.34 No.15 Computer Engineering August 2008
·开发研究与设计技术· 文章编号：1000—3428(2008)15—0264—03 文献标识码：A 中图分类号：TP391

基于射频识别的防伪系统研究与开发

王俊宇，刘 丹，魏 鹏，闵 昊
(复旦大学专用集成电路与系统国家重点实验室，上海 200433)

摘 要：分析商品防伪技术的设计需求，提出一种基于射频识别(RFID)的防伪技术方案及防伪验证方法，设计一个基于RFID和GPRS网络的茶叶防伪系统，该系统通过唯一编码、数据加密等手段可以实现对商品的唯一身份识别，具有识别可靠性高、识别手段便捷等特点。讨论了基于RFID的商品防伪技术的局限性和可能的研究领域。

关键词：防伪；射频识别；数据加密

Research and Development of Anti-counterfeit System Based on RFID

WANG Jun-yu, LIU Dan, WEI Peng, MIN Hao
(State Key Laboratory of ASIC & System, Fudan University, Shanghai 200433)

【Abstract】 This paper analyzes the requirement of anti-counterfeit for item level product and proposes an anti-counterfeit solution based on Radio Frequency Identification(RFID). A prototype system, combined the RFID with GPRS, is designed, through which the tea can be authenticated efficiently and conveniently. The limits and possible research field of RFID anti-counterfeit technology are discussed.

【Key words】 anti-counterfeit; Radio Frequency Identification(RFID); data encryption

1 概述

现代社会，商品伪造正日益成为全球经济领域面临的严重问题。商品防伪系统设计需要解决如下问题：(1)身份认证的唯一性，保证商品的唯一性和不可抵赖性；(2)防伪系统的安全性，即防复制(防止将真品的认证信息拷贝到伪造商品上)；(3)系统的易用性、友好界面、高速度；(4)其他，如低成本、美观性、易回收等。

常用的防伪技术主要有纸基防伪、油墨基防伪、全息防伪、凹版印刷防伪、电话电码防伪等，主要通过在商品包装上附加物理特性或者通过电话密码查询来实现，存在容易被仿冒、重复使用包装、防伪验证方便性差等问题，防伪查询率较低，而且不能对物品跟踪和追溯。条码防伪技术可实现跟踪与追溯，但标签的防复制能力比较差[1]。

本文介绍的基于射频识别(Radio Frequency Identification, RFID)的商品防伪技术通过结合产品的唯一编码技术、RFID自动识别、数字加密技术和基于互联网的信息服务，不但可以通过编码对商品进行唯一识别，而且可以对其来源和供应渠道进行跟踪与追溯，安全可靠，是解决商品防伪问题的有效手段之一。

2 基于RFID的防伪系统架构及防伪验证方法

RFID是一种通过电磁感应或电磁发射的方式实现的无线识别技术，频率为30 kHz~30 GHz，识别距离从几厘米到几米。RFID系统包括电子标签、读写器和数据处理系统，标签信息通过读写器进入数据处理系统[2-4]。基于RFID的商品防伪系统框架如图1所示。该系统包括RFID系统、通信网络和防伪验证信息服务系统。其中，RFID系统可以在授权的情况下读取标签信息；通信网络可以是Internet, GSM或者其他无线网络；防伪验证服务系统包含产品历史文件和认证信息，包括产品属性、标签编码和读写器编码以及标签的读取时间等，防伪认证服务系统可由生产商或者第三方机构维护。

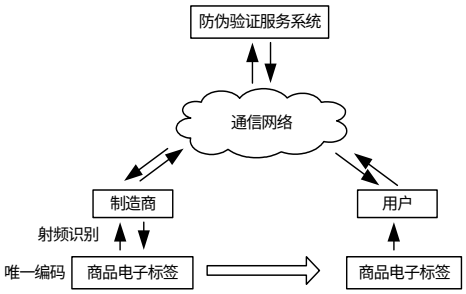

图1 基于RFID的商品防伪系统框架

标签存储两部分内容：产品的唯一标识和产品制造商的数字签名。产品标识识别单个物品；数字签名采用公共密钥体系，制造商用认证中心分配的私钥进行数字签名，签名信息包括产品的唯一编号的 *Hash* 函数值，以及产品信息，如生产日期、保质期、产品批次等。

上述防伪系统具有以下3个基本特征：

(1)通过产品编码对商品进行唯一标识。

产品代码至少包括生产商代码、产品类别代码和产品序列号、产品编码。在把标签贴到产品之前，将代码写入标签，并进行锁定，使得每一个产品获得唯一的、不可修改的编码，用于身份认证。

(2)通过RFID技术进行商品自动识别。

防伪识别过程中通过读写器读取标签信息，并且可以通

基金项目：国家“863”计划基金资助项目(2006AA04A101)
作者简介：王俊宇(1973－)，男，副研究员、博士，主研方向：计算机体系结构，射频识别系统；刘 丹、魏 鹏，硕士研究生；闵 昊，教授、博士生导师
收稿日期：2007-09-07 **E-mail：**junyuwang@fudan.edu.cn

过 RFID 中间件过滤重复读取的标签，实现多标签识别，提高识别效率。供应链中的厂商的读写器在获得授权的情况下对标签进行读操作和灭活操作，读写器的授权信息保存在信息服务系统中。

(3)采用数字签名保证数据安全性和不可抵赖性。

为了加强信息的安全性，可在标签上保存制造商的数字签名，包括产品信息和产品编号，数字签名将在制造商处写入标签，并锁定。防伪验证时，可通过认证中心解密，提取产品信息的 *Hash* 函数值，与标签内保存的 *Hash* 函数值比较，判断产品是否为该制造商生产。

以 SHA-1 散列函数和 RSA 算法[5]为例，数字签名及认证过程如图 2 所示。在制造商处，首先用 *Hash* 函数 SHA-1 生成产品编码的数字摘要，然后采用 RSA 算法用制造商的私有密钥对数字摘要加密，生成数字签名。标签上同时保存数字签名和产品的编码。在防伪验证时，验证方使用 *Hash* 函数 SHA-1 生成产品 ID 号的数字摘要 1，同时利用 RSA 算法以制造商的公开密钥对数字签名进行解密操作，获得产品 ID 号的数字摘要 2，如果数字摘要 1 与数字摘要 2 相同，则签名有效。

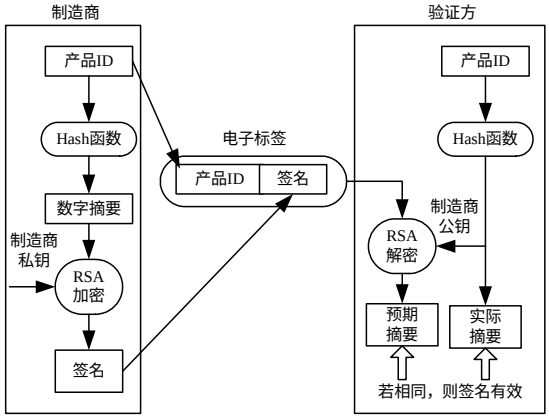

图 2　用散列函数和 RSA 算法进行的产品签名

3　基于 RFID 的茶叶防伪系统设计

3.1　防伪标签编码

设计的系统采用 96 bit 的 EPC 码[6]对研究对象——普洱茶进行编码，编码结构如表 1 所示，分成 4 个部分：标头，通用管理者代码，对象分类代码和序列号。其中，标头表示 EPC 码的版本和结构；通用管理者代码描述与 EPC 码相关的生产厂商信息，对每一个管理者来说“通用管理者代码”是唯一的；对象分类代码描述产品种类，在每一个通用管理者码之下是唯一的；序列号为每一个对象分类之内的单个产品的唯一编码。

表 1　EPC-96 编码结构

编码	标头	通用管理者代码	对象分类码	序列号
EPC-96	8	28	24	36

3.2　防伪标签选型

标签按照工作频率，分为低频(LF, 135 kHz 以下)、高频(HF, 13.56 MHz)、超高频(UHF, 900 MHz 左右)和微波(Microwave, 2.45 GHz, 5.8 GHz)等种类。本研究主要考虑 HF 和 UHF 标签，可供选择的 RFID 标准如表 2 所示，其中“下行”表示读写器至标签，“上行”表示标签至读写器。

考虑到茶叶防伪应用中不需要远距离识别，但对系统(包括标签、读写器和应用开发)成本比较敏感，因此，系统选择采用 ISO14443-A Ultra-light 标准的 RFID 系统，包括具有防复制功能的标签和包含 GPRS 模块的手持读写器。防伪标签采用易碎材料制成，当从商品包装上撕下标签时，标签及印刷天线将被破坏，从而使得标签丧失功能，以防止恶意的转移标签的攻击方法。

表 2　常见 HF 和 UHF 标签标准

通信协议	频率/MHz	存储容量	通信速度/ ($Kb{\cdot}s^{-1}$)	识别距离
ISO14443	13.56	64 Byte~ 1 KB	106	约 10 cm
ISO15693	13.56	2 Kb	下行：1.65 或 26.84 上行：6.62 或 26.50	约 80 cm
EPC Class0	902~928	64 bit	40 或 80	约 5 m
EPC Class1	902~928	96 bit	40 或 80	约 5 m
ISO18000-6A	860~930	1 KB	40	约 5 m
ISO18000-6B	860~930	1 KB	40	约 5 m
ISO18000-6C	860~960	128 bit～ 2 Kb	下行：40 或 80 或 160 上行：640	约 5 m

防伪标签的内存如图 3 所示，共计 64 Byte，其中黑框以外的存储器由芯片厂商定义，黑框以内的存储器由用户定义。序列号(Serial Number, SN)占 7 Byte，为标签芯片出厂时设定，用户不能修改；通过纵向冗余校验法(LRC)生成的块校验字符(BCC)占 2 Byte，只读，用于对 SN 校验；厂商使用的内部控制域(Internal)占 1 Byte；用户权限设置域(Lock)占 2 Byte，对用户数据区(Data0~Data47)的指定块进行锁定，一次性写入；OTP 域占 4 Byte，用户可操作，一次性写入；用户数据区(Data0~ Data47)占 48 Byte。

Byte Number	0	1	2	3	Page
Serial Number	SN0	SN1	SN2	BCC0	0
Serial Number	SN3	SN4	SN5	SN6	1
Internal/Lock	BCC1	Internal	Lock0	Lock1	2
OTP	OTP0	OTP1	OTP2	OTP3	3
Data read/write	Data0	Data1	Data2	Data3	4
Data read/write	Data4	Data5	Data6	Data7	5
Data read/write	Data8	Data9	Data10	Data11	6
Data read/write	Data12	Data13	Data14	Data15	7
Data read/write	Data16	Data17	Data18	Data19	8
Data read/write	Data20	Data21	Data22	Data23	9
Data read/write	Data24	Data25	Data26	Data27	10
Data read/write	Data28	Data29	Data30	Data31	11
Data read/write	Data32	Data33	Data34	Data35	12
Data read/write	Data36	Data37	Data38	Data39	13
Data read/write	Data40	Data41	Data42	Data43	14
Data read/write	Data44	Data45	Data46	Data47	15

图 3　ISO14443-A 标签内存

系统采用对称密钥 AES 算法进行数据加解密。96 bit 用户编码存入用户数据区的第 4 页～第 6 页。将序列号和校验码 72 bit(SN+BCC0+BCC1)进行 0 扩展后的 128 bit 作为明文，通过 AES 算法用 128 bit 密钥进行加密产生 128 bit 密文，存入用户数据区第 7 页～第 10 页。密钥为 EPC 厂商代码所对应密钥，不同厂商代码有着不同的密钥。

3.3　茶叶防伪系统架构及工作原理

基于 RFID 的茶叶防伪系统结构如图 4 所示。

(1)标签存储茶叶的序列号和数字签名信息，具有防复制功能。

(2)手持查询终端(内置 GPRS 模块的手持读写器)，可以与服务器进行无线远程通信。

(3)通信网络，即 GPRS 骨干网和 Internet 网。

(4)防伪验证服务器，存储茶叶信息数据库，有防伪校验和报警功能，主要功能有：1)对普洱茶真伪的校验，通过数字签名以及唯一编码来完成；2)提供对普洱茶信息的查询，包括产地、生产日期等。

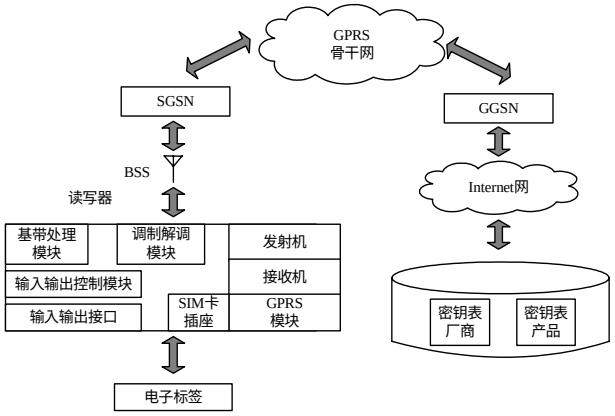

图 4　基于 RFID 的茶叶防伪系统框架

基于 RFID 的茶叶防伪系统的工作原理如下：

(1)数据传输

茶叶防伪系统的数据传输通道包括 RFID 空中接口、Internet 网和 GPRS 网络。其中，GPRS 网络是基于现有 GSM 网络实现的，主要包括 GSM 基站子系统(BSS)、GPRS 服务支持节点(SGSN)、GPRS 网关支持节点(GGSN)。

由读写器读取标签上的数据，产生分组数据单元(PDU)，发送给 GSM 基站子系统 BSS，处理后形成 LLC 帧，通过空中接口送到 GSM 网络中移动终端所处的 SGSN。GGSN 通过骨干网接收信息并最终传送给拥有固定 IP 地址的茶叶防伪认证系统。

(2)防伪校验

验证方通过带 GPRS 模块的手持终端(读写器)读取标签的芯片序列号 SN(72 b，含 BCC 校验码)，EPC 码(96 b，每盒茶叶具有唯一编码)，SN 密文(128 b)。密文是通过 AES 对零扩展后的 SN 进行加密产生的，密钥长度为 128 b。上述信息通过网络传输到后台防伪认证服务器。后台服务器保存所有商品信息和厂家密钥。服务器若接收到标签发来的信息，则按照 EPC 厂家代码在数据库中寻找匹配密钥，若无匹配记录则发送“无厂家记录，谨防假冒”。若找到匹配密钥，则对密文进行 AES 解密。解密得到的数据与接收到的 SN 进行对比，若不相同则发送“标签未通过验证，谨防假冒”。若 AES 验证通过，则按照厂商代码寻找茶叶信息，无匹配记录则发送“无商品记录，谨防假冒”，若找到匹配记录，则根据指令发送相关茶叶信息。

(3)信息查询

如果标签通过防伪验证，则可以用 EPC 为索引查找后台信息系统中的产品信息。为了简便起见，将防伪认证服务系统和后台信息系统设计成一个集中的系统。通过设置手持终端，可在其上显示“未读到正确标签”、“正在发送数据”、“数据发送成功”等信息。如果验证通过，显示出产品信息菜单“1.基本信息 2.生产信息 3.质量信息 4.其他信息”。

4　基于 RFID 的防伪系统分析与讨论

本文设计的 RFID 茶叶防伪系统与基于物理属性的商品防伪技术和中心数码防伪技术相比，具有通用性强、验证效率高、验证方法可靠等优点，并且可以实现对商品的跟踪与追溯；与条码的防伪技术相比，其防复制能力强，而且由于采用电磁波进行信息传输，RFID 技术易于与其他无线通信技术结合，成本较低。各种防伪技术的比较如表 3 所示。

表 3　商品防伪技术比较分析

防伪技术	标签防复制能力	标签防转移能力	验证设备	标签成本	防伪验证成本	防伪验证可靠性	防伪验证效率	跟踪与追溯功能
基于物理属性的防伪技术	强	有	专用	高	高	高	低	无
中心数码防伪技术	弱	无	通用	低	低	低	低	无
条码防伪技术	弱	有	扫描器	低	低	高	高	有
RFID 防伪技术	强	有	阅读器	低	高	高	高	有

基于 RFID 的防伪系统可以避免传统防伪技术的识别速率低等缺陷，但也面临一些问题：(1)RFID 技术因为采用电磁感应或电磁反射进行识别，所以对金属和水比较敏感，对此类商品的识别效果较差；(2)需要成本较高的标准读写器，目前短距离无线通信(NFC)手机的兴起有望解决上述问题；(3)基于 RFID 的防伪系统对通信网络的速度、安全性和可靠性有较高的要求。

5　结束语

本文介绍了基于 RFID 的商品防伪系统的基本原理和防伪认证方法，比较了该技术与传统商品防伪技术的特点，设计了一个可用于茶叶防伪的系统。该系统包括高频标签、手持读写器、GPRS 网络和 Internet 网络，产品编码采用 96 b EPC 码。验证系统通过 AES 算法和芯片唯一序列号进行防伪校验，实现了茶叶身份识别。此外，该系统还可在网上即时更新防伪信息，使防伪系统更加可靠，较好地解决了现有防伪技术存在的技术缺陷和查询率低的问题。

参考文献

[1] Lei P, Claret-Tournier F, Chatwin C, et al. A Secure Mobile Track and Trace System for Anti-counterfeiting[C]//Proceedings of IEEE International Conference on E-Technology, E-Commerce and E-Service. Hong Kong, China: [s. n.], 2005-04.

[2] Ollivier M M. RFID——A New Solution Technology for Security Problems[C]//Proceedings of European Convention on Security and Detection. Brighton, United Kingdom: [s. n.], 1995.

[3] Tuttle J R. Traditional and Emerging Technologies and Applications in the Radio Frequency Identification(RFID) Industry[C]//Proc. of IEEE Radio Frequency Integrated Circuits Symposium. Denver, CO, USA: [s. n.], 1997.

[4] Su M, Hwang Y J, Lee D H, et al. Efficient Authentication for Low Cost RFID Systems[C]//Proc. of International Conference on Computational Science and Its Applications. [S. l.]: Springer-Verlag, 2005.

[5] Denning D E. Digital Signatures with RSA and Other Public-key Cryptosystems[J]. Communication of the ACM, 1984, 27(4): 388-392.

[6] Brock D L. The Electronic Product Code (EPC)——A Naming Scheme for Physical Objects[Z]. (2000-10-05). http://www.autoidlabs.org/ whitepapers/MIT-AUTOID-WH-002.pdf.