

基于 USB Key 的水产品企业监管溯源系统设计与应用*

杨信廷¹ 吴滔^{1,2} 孙传恒^{1,3} 刘燕德² 周超¹

(1. 国家农业信息化工程技术研究中心, 北京 100097; 2. 华东交通大学机电工程学院, 南昌 330013;
3. 中国农业大学信息与电气工程学院, 北京 100083)

【摘要】 根据目前水产品监管溯源系统中水产品企业身份认证存在的问题,设计了一种基于 USB Key 的水产品企业监管溯源系统。首先,分析了几种身份认证技术的方法,重点阐述了其优缺点;然后,设计了 USB Key 硬件电路关键部分、软件系统以及基于 USB Key 认证的水产品企业的认证流程,解决了水产品信息传输的安全性问题;最后,描述了基于 USB Key 的水产品企业监管模式在江苏省水产品企业认证与监管追溯平台中的应用。研究结果表明,该监管溯源系统便捷安全,稳定可靠,能实现产地准出、市场准入、企业资质认证、政府实时监控的水产品企业监管溯源体系。

关键词: 水产品 USB Key 身份认证 监管溯源

中图分类号: S126; F307.4 文献标识码: A 文章编号: 1000-1298(2012)08-0128-06

Design and Application of Aquatic Enterprise Governance Traceability System Based on USB Key

Yang Xinting¹ Wu Tao^{1,2} Sun Chuanheng^{1,3} Liu Yande² Zhou Chao¹

(1. National Engineering Research Center for Information Technology in Agriculture, Beijing 100097, China
2. School of Mechatronics Engineering, East China Jiaotong University, Nanchang 330013, China
3. College of Information and Electrical Engineering, China Agricultural University, Beijing 100083, China)

Abstract

According to the aquatic trace identity in the existing regulatory system, a certification and traceability regulatory system based on USB Key was designed. Firstly, several authentication technologies were analyzed focusing on the advantages and disadvantages. Secondly, the key part of USB Key hardware circuit, software system and the certification process of USB Key aquatic products enterprises were designed to solve the security issues of aquatic information transmission. Finally, the aquatic product enterprise certification and traceability monitoring platform was applied in Jiangsu province. The results showed that the regulatory system was convenient, safety, stable and reliable. It can realize the origin of quasi-out, market access, business certification and real-time monitoring of aquatic enterprise governance traceability system.

Key words Aquatic product, USB Key, Identity authentication, Regulatory back

引言

水产品安全监管溯源关系到消费者身体健康和渔业长远发展等重大问题,随着国家对水产品安全

监管溯源的重视,水产品监管已经成为社会普遍关注的焦点和热点^[1~2]。水产品企业身份认证是实现水产品主体监管溯源的关键。近几年来,水产品企业逐渐显现出企业数目偏多、生产规模总体偏小、物

收稿日期: 2012-03-22 修回日期: 2012-04-25

* 国家高技术研究发展计划(863 计划)资助项目(2011AA100706、2012AA101905-02)

作者简介: 杨信廷,副研究员,博士,主要从事农产品质量安全溯源及农业信息化关键技术研究,E-mail: yangxt@ nercita. org. cn

通讯作者: 孙传恒,副研究员,主要从事农业信息化研究,E-mail: sunch@ nercita. org. cn

流供应链偏长、准入门槛偏低等特征。自 2005 年,水产品加工企业数量已达 8 758 个,年加工能力达 1 609 万 t,加工总产量 1 161.6 万 t^[3],因此合理监管多类别、大数目的水产品企业是困扰政府高效监管的主要问题^[4]。国内外学者对水产品物流链和监管中存在的问题进行了大量的研究,国外发达国家已经将企业主身份认证融入了监管的关键问题之一^[5-9]。国内的监管很大程度上依赖于周期性检查,出现安全问题层层上报,监管体系安全性能差,交易文件易伪造,难以实现产地准出、市场准入^[10]。

为提升水产品安全生产与质量监管水平,以水产品企业为研究对象,结合 USB Key 身份认证和分布式密钥管理技术,设计基于 USB Key 的水产品监管溯源系统,建立水产品产地准出认证、水产品市场准入认证、水产品省-县-企业三级认证的水产品企业分布式监管溯源体系^[11]。

1 身份认证技术

随着计算机技术的迅猛发展,用户信息安全成为全面实行管理信息化的重大问题,水产品企业身份认证对于水产品监管尤为重要。身份认证分为以下几类:按认证信息可分为静态认证和动态认证;按认证载体可分为硬件认证和软件认证。动态口令认证的密码随着时间和使用次数不断动态变化,较静态口令认证有更高的安全性。IC 卡通过存储的静态数据进行身份认证,USB Key 采用软硬件相结合、动态密码认证模式进行身份认证^[12]。表 1 为几种认证技术比较。

表 1 几种认证技术比较

Tab.1 Comparison of several authentication technologies

认证技术	使用便捷性	交易安全性	经济性	质量可靠性	PKI 体系
静态口令认证	便捷	低	便宜	好	不完善
动态口令认证	不便捷	中	便宜	好	不完善
IC 卡认证	便捷	低	中等	不好	不完善
USB Key 认证	便捷	高	中等	好	完善

1.1 静态口令认证方式

静态口令是身份认证方法中最简单也是最常用的,它是由静态用户名和静态密码组成,只要能够正确输入口令,就能合法登陆。静态口令存在如下不足:只能进行单向认证,且认证级别很低,存在口令容易泄露等很多安全问题;用户口令是静态的数据,验证时口令会在计算机内存中缓存,口令容易被计算机木马程序获取或修改,在网络传输时也容易被网络中的监听设备截获^[13]。因此,静态口令方式一

种是极不安全的身份认证方式。

1.2 动态口令认证方式

动态口令是一种根据专门算法生产的随机数字组合,密码生成芯片运行专门的加密算法,并在显示屏上显示。服务器确认,采用相同的算法计算来验证。由于每次密码都是有动态密码生成器随机生成,从而黑客无法窃取合法用户的身份。因而动态口令方式比静态口令方式安全性能高,但是也存在如下问题:客户端硬件与服务器端程序的时间或次数不能保持良好的同步,可能造成合法用户无法登陆;只能进行单向认证,系统可以认证用户,用户无法对系统认证;存在单点故障,一旦认证服务器出问题,整个系统就将崩溃;用户登陆要输入很长无规律的密码串,给用户使用带来不便。

1.3 IC 卡认证方式

IC 卡将微电子芯片嵌入到标准的卡基中,内置电子芯片储存用户身份信息,登陆需将 IC 卡靠近读卡器获取卡中信息,验证用户身份^[14]。由于 IC 卡使用的单一验证方式和每次读取的数据是静态数据,因此 IC 卡丢失或被窃,用户将不能进入系统;专用的读取器能读取 IC 卡中的数据,能对数据进行复制,伪造相同 IC 卡;木马程序通过内存扫描或网络监听技术很容易窃取到用户身份验证信息。因此,IC 卡认证方式还是存在着根本的安全隐患。

1.4 USB Key 认证方式

USB Key 身份认证采用软硬件相结合、随机密码的强双因子认证模式,集动态口令和硬件认证于一体。USB 支持热拔插,便于携带,数据传输快,内置微处理器实现加密算法和客户终端密码算法相互核算,高强度的加、解密机制,信息不易泄露,双向认证用户身份,传输过程信息完整,不易被恶意篡改。USB Key 具有双重验证机制,硬件和客户密码缺一不可,用户身份得到了有效保护^[15-16]。基于冲击-响应的认证模式,如图 1 所示,从根本上保证了用户身份无法被仿冒,基于 PKI 的数字证书认证模式有效保证用户的身份安全和数据传输安全^[17]。因此,USB Key 成为身份认证的最佳载体。

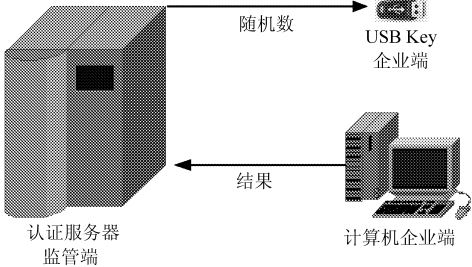


图 1 基于冲击-响应的认证模式

Fig. 1 Authentication of based on impact-response model

2 USB Key 软硬件实现

2.1 USB Key 硬件组成

一般 USB Key 的硬件构成包括 7 个组成部分：

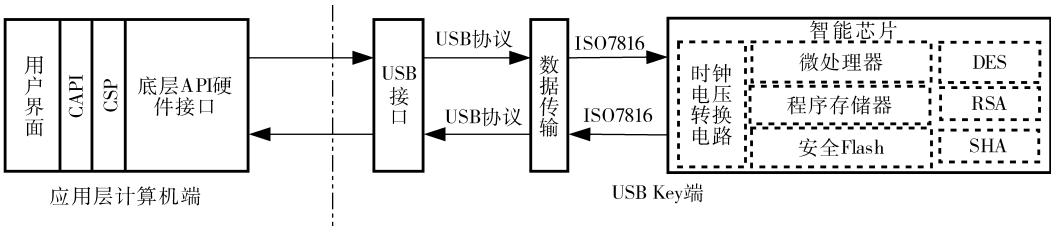


图 2 客户端系统结构图
Fig. 2 Structure of client system

微处理器是 USB Key 的核心,完成基本指令执行、存储控制和逻辑控制等。USB Key 多采用 8 位或 16 位的微处理器。本设计选用了 8 位 USB 微控制器 MC9S08JS16,它使用了增强型 HCS08 内核,内置全速 USB 2.0(12 Mb/s)控制器,集成了 3.3 V 调

节器和收发器,48 MHz 处理器频率,高达 16 Kb 的片上在线可编程 Flsah 和 256 B 的 USB RAM。USB 模块的 2 个时钟分别是 27 MHz 和 48 MHz^[19]。USB Key 企业身份认证系统 MC9S08JS16 芯片原理图,如图 3 所示。

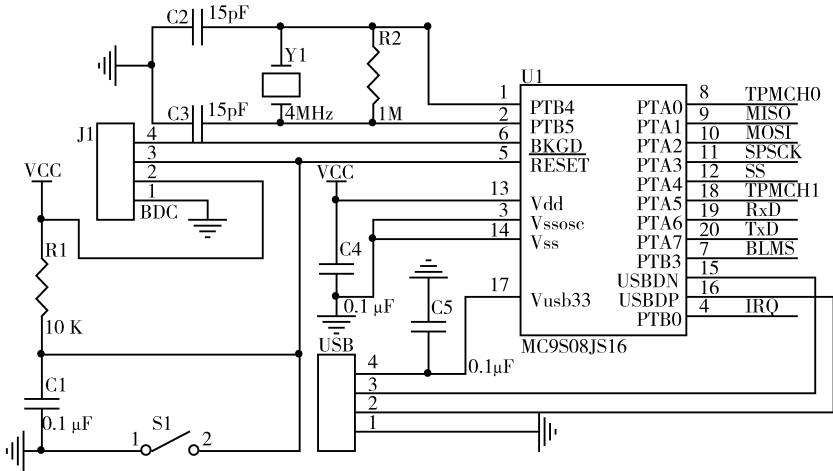


图 3 USB Key 硬件原理图
Fig. 3 Principle diagram of USB Key

2.2 USB 设备初始化

初始化是在 USB 插入计算机时完成,USB 模块复位,USB 传输和稳压器控制存储器的 RESET 位置 1,重置 USB 模块和所有寄存器为默认值,成功对 USB RAM 和缓冲区描述寄存器初始化。复位完成后,对初始化端点 0 的缓冲区描述寄存器设置 EPAD 寄存器,设置 USB RAM 为端点寄存器的存储空间,为了成功接收 DATA0 数据包,状态与控制寄存器设置为 DTS = 1, OWN = 1, DATA0/1 = 0^[20]。EPCTL0 置 0X0D,配置 USB 模块(使能电阻上拉,稳压器与 PHY)。使能 USB 模块和 USB 中断,设备实现连接状态,USB 模块初始化流程图,如图 4 所示。

2.3 USB 收发数据过程

USB 模块传送或接收数据时,首先会根据端点号、数据方向、偶或奇缓冲计算缓冲区描述表 BDT

地址,然后读取缓冲区描述寄存器 BD。一旦缓冲区描述寄存器 BD 已经被读取且 OWN = 1 时,串行接口引擎将会把数据包传送到缓冲区或接收来自缓冲区的包数据,地址为 BD 中的 EPADR 字段指向的地址。当 USB Key 处理结束,USB 模块会更新 BDT 并且置 OWN = 0。

如果 TOKDNE(包完成)中断置位,那么 STAT 寄存器将被更新。当微控制器处理 TOKDNE 中断时,它将读取状态寄存器。从而把要处理的端点的所有信息传递给 CPU。这样微控制器可以分配一个新的缓冲区描述寄存器 BD,其他的 USB 数据可以被发送或接收,而且它可以处理先前的缓冲区描述寄存器 BD^[21]。

2.4 USB Key 身份认证流程

资质合格的企业通过上级监管部分颁发的 USB

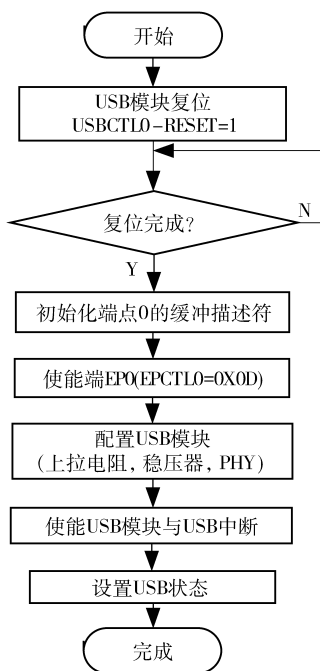


图 4 USB 模块初始化流程图

Fig. 4 Flow chart of USB module initialization

Key 可以进行企业身份认证,图 5 为水产品企业 USB Key 身份认证流程图。

其中 USB Key 内置密钥为 S_2 , 认证密钥为 S_1 , 认证密钥的加密密钥为 S_3 , 认证密钥的解密密钥为 K , 将 K 存储于 USB Key 内。

企业登陆企业资质认证系统时,首先要在 PC 机上插入 USB Key,自动获取用户证书,键入 PIN 码。正确后才能继续进行操作,输入错误,则返回上层,重新输入 PIN 码,输入错误口令超过 3 次后,用户密码将被锁住,向管理机构申请方能重新使用。

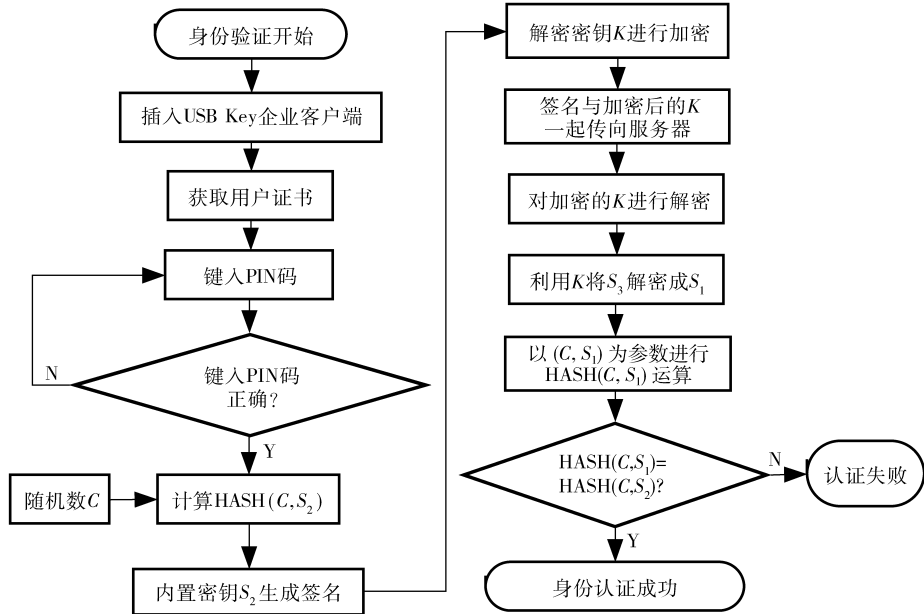


图 5 USB Key 身份认证流程图

Fig. 5 Flow chart of USB Key identity authentication

企业资质认证系统接收到认证申请时,认证服务器将产生随机数 C ,并将其传给客户端的 USB Key。USB Key 以 (C, S_2) 为参数,进行 $\text{HASH}(C, S_2)$ 运算,将运算结果与认证密钥的解密密钥 K 一起传送给认证服务器^[22]。

为防止黑客进攻,本系统还将认证密钥进行加密存储,即将 S_1 变成 S_3 ,认证服务器收到运算结果和解密密钥 K 后,利用 K 对 S_3 进行解密,将其变成 S_1 ,以 (C, S_1) 为参数进行 $\text{HASH}(C, S_1)$ 运算。当 $\text{HASH}(C, S_2)$ 等于 $\text{HASH}(C, S_1)$,也就说明 $S_2 = S_1$ 得到认证,企业资质认证成功,即该企业提供的水产品是安全的,市场准许进入。

3 水产品监管溯源体系应用实现

3.1 水产品监管体系构架

一般水产品供应链模式为:养殖场→水产品企业→水产品批发商→水产品零售商→消费者。水产品企业是生产者与消费者之间的纽带,水产品企业身份的合法性对水产品质量安全控制起着关键作用^[23-24]。USB Key 使水产品在物流链的各个环节的信息准确性得以保障,图 6 为水产品监管溯源体系。横向由监管追溯系统、生产管理系统、交易管理系统、追溯信息查询系统组成;纵向由监管主体、责任主体、信息传递、实物流转组成。

监管主体包括国家监管平台和省监管平台,负责签发 USB Key 省级公钥以及一些规则的制定,同时向消费者发布水产品信息及接受消费者投诉与信息反馈。责任主体即水产品企业要为养殖和收购的水产品承担责任。批发商要通过企业的 USB Key

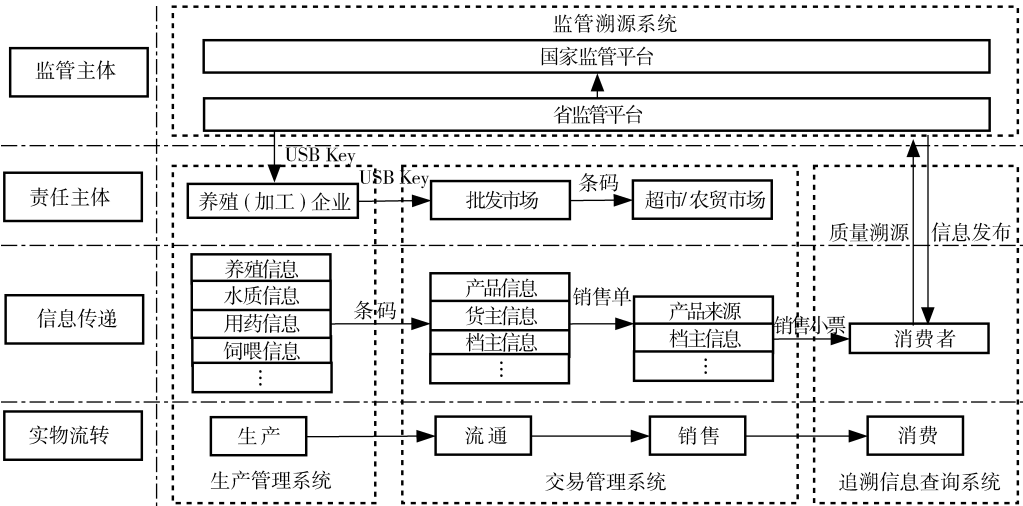


图 6 水产品监管体系框架图

Fig.6 Supervision system of aquatic products

验证企业的合法身份,方能合法进货,同时农贸市场要根据企业打印的有效条码,才能使水产品合法流入市场。水产实物和信息的传递伴随着 USB Key 验证,二维条码打印,销售小票记录确保水产品实物与信息安全流动,图 7 为打印的水产品质量安全追溯标签,其中明文记录了产品名称、批次号、交易日期与数量、水产品企业名称及追溯号,暗文记录着带鱼的各项养殖指标。一旦发生安全事故,可准确定位事故源。



图 7 水产品质量安全追溯标签

Fig.7 Labels of aquatic products quality safety back

3.2 水产品监管体系实现

本文开发的基于 USB Key 的水产品企业监管溯源系统为企业用户提供了一套有效的生产流程,为政府监管人员提供了一个便捷的监管途径。该系统已经成功应用于江苏省水产品安全养殖管理体系中。研制的 USB Key 设备如图 8 所示,当 USB Key 插入计算机时,系统将自动弹出企业用户 USB Key 登陆界面(图 8)。

当身份认证成功,系统将进入江苏省水产品安全养殖管理系统的登陆主界面,如图 9a 所示。在系统中能添加企业产品的产地、生产日期、生产者、质量检查结果等信息,如图 9b 所示。成体销售记录



图 8 企业用户 USB Key 登陆界面

Fig.8 USB Key landing interface of enterprise users

与条码打印为水产品安全消费提供了追溯平台,如图 9c 所示。水产品企业权限分配,如图 9d 所示。

4 结束语

水产品企业监管是水产品质量安全与追溯的关键因素之一,本文以 USB Key 为基础,构建了以企业身份认证为对象的水产品监管体系,系统能实现监管部门管理系统以管理模式登陆,被授权的企业用户通过 USB Key 访问控制终端并进行网上资质认证。二维条码作为水产品溯源信息的载体,实现水产品源头可追溯,流程可跟踪,信息可查询,产品可召回,弥补了市场对水产品企业资质分辨模糊,溯源条码防伪性差、易于仿制等不足。在选择核心芯片和认证加密方式的基础上设计了 USB Key 的软硬件,结合嵌入式和 .NET 技术开发了江苏省水产品企业监管溯源系统,实现了水产品企业生产标准化流程作业和政府机构有效便捷监管的新途径,优化加密算法将会使得监管系统安全性能得到进一步提高。但是在实际使用过程中,有时会出现 PC 机无法识别硬件或系统崩溃的情况,重新启动后,可以正常使用,但是这种情况发生的频率不高,下一步的

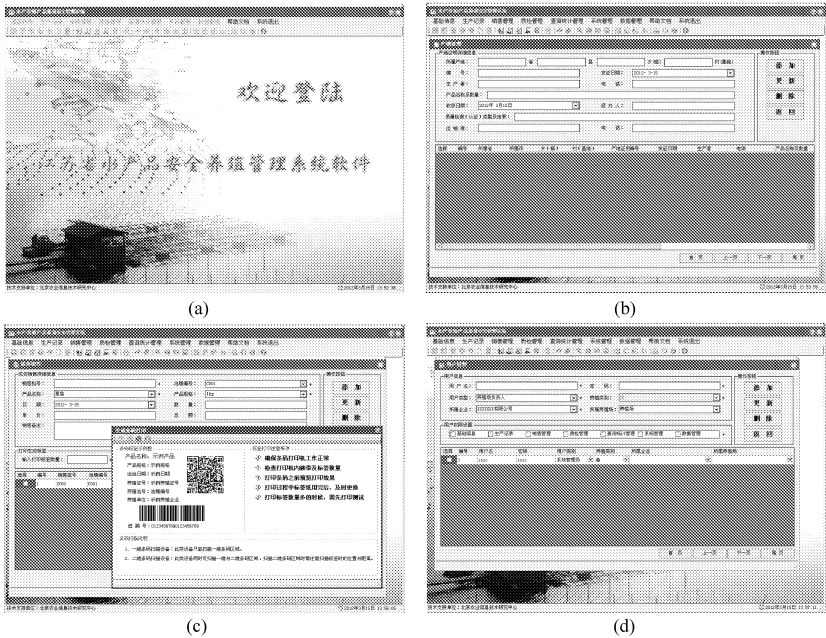


图 9 江苏省水产品企业监管溯源系统

Fig.9 Authentication and aquatic products back regulatory platform of Jiangsu province enterprise
(a) 登陆成功主界面 (b) 水产品产地证明 (c) 水产品销售及条码打印 (d) 监管权限分配

工作将是扩大系统的应用范围及提高系统稳定兼容性,该监管系统为水产品质量安全控制提供了理论

依据,同时该系统 USB Key 身份认证的方法也为其他领域监管提供了实践参考。

参 考 文 献

1 孙建富, 鹿丽. 我国水产品质量安全问题探析[J]. 大连海事大学学报: 社会科学版, 2008, 7(3): 124 ~ 127.

2 Ampatzidis Y G, Vougioukasa S G. Field experiments for evaluating the incorporation of RFID and barcode registration and digital weighing technologies in manual fruit harvesting[J]. Computers and Electronics in Agriculture, 2009, 66(2): 166 ~ 172.

3 邵征翌. 中国水产品质量安全管理战略研究[D]. 青岛: 中国海洋大学, 2007.

4 Regattieri A, Gamberia M, Manzinia R. Traceability of food products: general framework and experimental evidence[J]. Journal of Food Engineering, 2007, 81(2): 347 ~ 356.

5 Li L, Liu Q, Jiang X. USB Key-based dual-factor dynamic authentication scheme[C] // Proceedings of the 2010 International Conference on Computational Intelligence and Security Washington, DC, USA, 2010.

6 Schwagele F. Traceability from European perspective[J]. Meat Science, 2005, 71(1): 164 ~ 173.

7 Smith G C, Tatum J D, Belk K E. Traceability from a US perspective[J]. Meat Science, 2005, 71(1): 174 ~ 193.

8 Opara L U. Traceability in agriculture and food supply chain; a review of basic concepts, technological implications, and future prospects[J]. Food, Agriculture & Environment, 2003, 1(1): 101 ~ 106.

9 Yang F Y, Wu T D, Chiu S H. A secure control protocol for USB mass storage devices[J]. IEEE Transactions on Consumer Electronics, 2010, 56(4): 2 339 ~ 2 343.

10 陈长喜, 张宏福, 飞颀经纬. 肉鸡产业技术体系生产监测与产品质量可追溯平台设计[J]. 农业机械学报, 2010, 41(8): 100 ~ 106.

Chen Changxi, Zhang Hongfu, Feixie Jingwei. Traceability platform design of production monitoring and products quality for broilers industry technology system[J]. Transactions of the Chinese Society for Agricultural Machinery, 2010, 41(8): 100 ~ 106. (in Chinese)

11 刘东红, 周建伟, 莫凌飞. 物联网技术在食品及农产品中应用的研究进展[J]. 农业机械学报, 2012, 43(1): 146 ~ 152.

Liu Donghong, Zhou Jianwei, Mo Lingfei. Applications of internet of things in food and agri-food areas[J]. Transactions of the Chinese Society for Agricultural Machinery, 2012, 43(1): 146 ~ 152. (in Chinese)

12 吴永英, 邓路, 肖道举. 一种基于 USB Key 的双因子身份认证与密钥交换协议[J]. 计算机工程与科学, 2007, 29(5): 56 ~ 59.

- [J]. Transactions of the Chinese Society of Agricultural Engineering, 2011, 27(8):99~105. (in Chinese)
- 8 侯方安. 中国农业机械化经营模式研究[M]. 北京:中国农业出版社,2010.
 - 9 顾基发,汪浣尘,唐锡晋,等. 综合集成方法体系与系统学研究[M]. 北京:科学出版社,2007.
 - 10 石浩然,王维锐,吴参,等. 知识集成环境下产品设计过程动态组织方法[J]. 农业机械学报,2011, 42(11): 183~188.
Shi Haoran, Wangweirui, Wu Can, et al. Dynamic reconstructing of the product design process in knowledge integrated environment [J]. Transactions of the Chinese Society for Agricultural Machinery, 2011, 42(11): 183~188. (in Chinese)
 - 11 钱学森. 创建系统学[M]. 太原:山西科学技术出版社,2001.
 - 12 万麟瑞,李绪荣. 系统集成方法学研究[J]. 计算机学报,1999,22(10):1 025~1 030.
Wan Linrui, Li Xurong. Researches on system integration methodology[J]. Chinese Journal of Computers, 1999, 22(10): 1 025~1 030. (in Chinese)
 - 13 殷瑞钰. 钢铁制造流程的解析和集成[J]. 金属学报,2000,36(10):1 077~1 084.
Yin Ruiyu. Analysis and inergration of steel manufacturing process [J]. Acta Metallurgica Sinica, 2000, 36(10): 1 077~1 084. (in Chinese)
 - 14 舒光复. 综合集成系统重构及宏观经济研究中的应用[J]. 系统工程学报,2001,16(5):349~352.
Shu Guangfu. Meta-synthetic system reconstruction and applications in macro-economic researches[J]. Journal of Systems Engineering, 2001, 16(5): 349~352. (in Chinese)
 - 15 程先东. 中国高速铁路系统集成方法与工程实践[J]. 中国铁路,2010(12):38~40.
 - 16 冯炳元. 农业机械学科的发展动向[J]. 农业机械学报,2003,34(1):127~129.
Feng Bingyuan. Development of the discipline of agricultural machinery [J]. Transactions of the Chinese Society for Agricultural Machinery, 2003, 34(1):127~129. (in Chinese)
 - 17 蒋亦元. 农机科技创新中的农机与农艺相结合问题[J]. 农业机械学报,2007,38(3):179~181.
Jiang Yiyuan. Combination of agricultural machinery and agronomy in their scientific and technological innovations [J]. Transactions of the Chinese Society for Agricultural Machinery, 2007, 38(3):179~181. (in Chinese)
 - 18 夏连明,王相友,耿瑞阳,等. 丸粒化玉米种子精密排种器[J]. 农业机械学报,2011,42(6): 53~57.
Xia Lianming, Wang Xiangyou, Geng Ruiyang, et al. Precision seed-metering device for pelleted corn seeds [J]. Transactions of the Chinese Society for Agricultural Machinery, 2011, 42(6): 53~57. (in Chinese)
 - 19 张杨. 工程中的组织集成问题研究[J]. 科技情报开发与经济,2007,17(33):169~170.
Zhang Yang. Research on the organizational integration in engineering[J]. Sci-Tech Information Development & Economy, 2007, 17(33): 169~170. (in Chinese)
 - 20 洪巍,陈星光. 集成管理与管理集成辨析[J]. 管理观察,2010(28): 24~25.
 - 21 钱学森. 论系统工程[M]. 修订本. 长沙:湖南科学技术出版社,1988:33.

(上接第 133 页)

- 13 张引兵,刘楠楠,张力. 身份认证技术综述[J]. 电脑知识与技术,2011, 7(9):2 014~2 016.
- 14 冯志兴,李建华,王轶俊. 金融 IC 卡认证体系及其安全性分析[J]. 信息安全与通信保密,2009(3):58~61.
- 15 段钢. 加密与解密[M]. 2 版. 北京:电子工业出版社,2003.
- 16 李顺东,王道顺. 现代密码学:理论、方法与研究前沿[M]. 北京:科学出版社,2009.
- 17 周广辉. USB Key 用户认证平台的研究和实现[J]. 信息安全与通信保密,2009(9):113~118.
- 18 杨帆. USB Key 体系研究与技术实现[D]. 武汉:武汉大学,2004.
- 19 Liu D. USB device development with the MC9S08JM60[R]. Asia & Pacific Operation Microcontroller Division, 2008.
- 20 赵明辉,张红雨,李亮. 基于 MC9S08JS16 和 AES 的 USB Key 设计[J]. 电子设计工程,2010(10):119~122.
- 21 李顺,肖龙远. 基于 Linux 的身份认证系统设计与实现[J]. 微处理机,2010(3): 97~100.
- 22 黄兴燕,詹林. 基于 USB-Key 的数字图书馆身份认证技术[J]. 电脑知识与技术,2009,5(34):9 777~9 778,9 784.
- 23 杨信廷,孙传恒,钱建平. 基于流程编码的水产养殖产品质量追溯系统的构建与实现[J]. 农业工程学报,2008, 24(2):159~164.
Yang Xinting, Sun Chuanheng, Qian Jianping. Based on the process of coding aquaculture products quality tracking system to the construction and implementation[J]. Transactions of the CSAE,2008,24(2):159~164. (in Chinese)
- 24 杨信廷,钱建平,范蓓蕾. 农产品物流过程追溯中的智能配送系统[J]. 农业机械学报,2011,42(5): 125~130.
Yang Xinting, Qian Jianping, Fan Beilei. Agricultural logistics process back on the wisdom of the distribution system[J]. Transactions of the Chinese Society for Agricultural Machinery, 2011,42(5): 125~130. (in Chinese)