第34卷 第21期 计 算 机 工 程 2008年11月
Vol.34 No.21 Computer Engineering November 2008
·博士论文· 文章编号：1000—3428(2008)21—0035—03 文献标识码：A 中图分类号：TP391

基于FPGA的防伪阅读器

李 辉[1]，侯义斌[2]，黄樟钦[2]，何福贵[2]，陈 锐[2]
(1. 北京工业大学计算机学院，北京 100022；2. 北京工业大学软件学院，北京 100022)

摘 要：分析现有防伪技术的缺陷，结合射频识别和信息安全理论，提出符合国际标准的RFID防伪阅读器，讨论应用于防伪系统的防伪认证机制和加密算法，在此基础上实现基于现场可编程门阵列的防伪阅读器的原型系统。该原型系统集成了标签防伪的加密算法、阅读器身份防伪的认证算法以及IP核技术，有效实现了商品真伪的鉴别。

关键词：防伪阅读器；射频识别；IP核；现场可编程门阵列

Anti-forge Reader Based on FPGA

LI Hui[1], HOU Yi-bin[2], HUANG Zhang-qin[2], HE Fu-gui[2], CHEN Rui[2]
(1. College of Computer Science and Technology, Beijing University of Technology, Beijing 100022;
2. School of Software Engineering, Beijing University of Technology, Beijing 100022)

【Abstract】This paper analyzes the shortcoming of current anti-forge technique. Combining the information security with RFID technique theory, it presents the anti-forge RFID reader which conforms to international standard. The discussion about anti-forge mechanism and the encrypt algorithm are emphasized. The realization of anti-forge reader prototype system based on FPGA is introduced. The anti-forge algorithm and authentication of reader algorithm is realized. The IP core of anti-forge algorithm is realized in the hardware system. The effective distinguish and the protection for commodity is provided.

【Keywords】 anti-forge reader; Radio Frequency IDentification(RFID); IP core; FPGA

1 概述

射频识别(Radio Frequency Identification, RFID)技术是一项日渐成熟的自动识别技术。美国、欧洲及日本等发达国家将RFID技术应用于防伪领域，其主要目的是为了实现高效管理，采用标签中所带的唯一ID号，实现简单的防伪功 能[1-2]。然而现有的RFID阅读器功能单一，目前国际上还没有具有真正防伪功能的RFID阅读器。传统的防伪技术一般不具备唯一性和独占性且容易复制，因此，起不到真正的防伪作用。目前，国际上逐渐兴起了电子技术防伪潮流，射频标签引起了防伪界的广泛关注。

本文结合RFID技术和信息安全理论以及嵌入式理念，提出阅读器的防伪算法应用模型，给出基于FPGA的防伪阅读器的软硬件架构，为RFID技术与防伪技术的结合提供一个全新的参考。该防伪阅读器除具有RFID自身拥有的防伪功能外，还增加了一些新的防伪功能，如通过RFID防伪阅读器，实现对电子标签编码的二次加密，以解决单纯依靠电子标签防伪的缺陷。

2 基于RFID的防伪技术特点

本文提出的防伪技术具有如下特点：

(1)将数字签名技术应用于RFID标签生产过程中。为每件产品赋予一个唯一标识，此标识在生产、经销、验证等过程中唯一表示此件产品，终身不变。同时将标识生成为一个数字签名锁定并写入封装在商品包装中的RFID标签的存储区。

(2)将公、私钥加密认证技术应用于经厂方授权的合法阅读器中并对产品的真伪进行检验。

(3)基于RFID技术的防伪系统渗透到了产品周期中的生产、经销、验证、消费等各个环节之中。

(4)生产者是产品防伪系统的中心，掌握防伪系统的关键环节。

本文提出的阅读器防伪算法遵循以下原则：

(1)真实产品通过合法经销渠道到达消费者手中。

(2)防伪系统的其他参与者不掌握系统的关键环节，不能破解密钥系统。

(3)任何人或组织无法仿造出防伪系统不能识别的产品。

(4)任何人或组织均无法使假冒产品通过防伪系统流通到消费者手中。

(5)经销商随时可以对产品进行验证。

(6)消费者也可以通过经销商随时对产品进行验证。

3 基于FRID技术的防伪系统架构

本文的防伪系统架构由图1所示的硬件(节点)组成，每个节点的角色和功能描述如下：

(1)嵌入式防伪阅读器：RFID防伪系统的重要设备。此设备由经销商从厂家购进，经销商通过终端计算机从防伪服务器下载防伪数据后，对产品的真伪进行验证。

(2)RFID防伪电子标签：即RFID射频电子标签码，由生产商设定标签并封装到产品中。

(3)防伪服务器：防伪服务器提供阅读器注册、认证、防伪数据下载和产品在线验证等功能。

作者简介：李 辉(1971－)，男，博士，主研方向：图像处理，人机交互技术；侯义斌，教授、博士生导师；黄樟钦，教授；何福贵，讲师；陈 锐，博士

收稿日期：2007-12-23 **E-mail：**hli@emails.bjut.edu.cn

(4)CA 认证中心计算机：防伪系统的 CA 认证中心。

(5)生产商终端：运行与生产商相关的防伪系统软件，包括密钥生成与管理子系统、生产子系统和销售子系统。

(6)经销商终端：在经销商端运行防伪阅读器的辅助程序，将防伪阅读器与之连接，并通过网络与防伪服务器连接，然后对防伪阅读器进行在线注册、下载防伪数据。

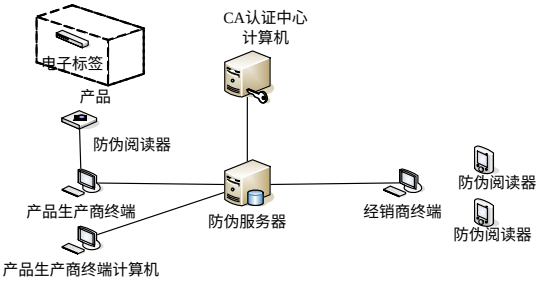

图 1　基于 RFID 技术的防伪系统架构

4　RFID 阅读器的算法及 IP 核实现

本文将SHA-1[3-4]算法应用于RFID标签的数字签名。SHA-1 是目前最常用的安全散列算法，它是由美国国家标准与技术学会(NIST)和美国国家安全局(NSA)设计的安全哈希算法，用于数字签名标准。SHA-1 同其他的哈希算法一样，将RFID的标签码运算后得到 160 bit输出，从中取出 128 bit 作为签名后的标签码，基本算法描述如下：

(1)填充消息。先填上一个 1，后跟一串 0，使得消息的长度为比 512 的倍数少 64 bit，最后还要加上一个 64 bit 表示消息长度。这 2 步使消息长度恰好是 512 的倍数，同时保证不同的消息在填充后仍然不同。

(2)变量初始化。要使 SHA_1 的输出为 160 bit，需要对 5 个 32 bit 变量初始化。即 A＝0x67452301, B＝0xefcdab89, C＝0x98badcfe, D＝0x10325476, E＝0xc3d2elf0。

(3)算法的主循环。以 512 bit 为一组，对消息的各块重复执行。将 5 个变量复制到不同的变量：A 复制到 a，B 复制到 b，C 复制到 c，D 复制到 d，E 复制到 e。主循环有 4 次，每次循环有 20 个操作，每个操作完成一个在 a, b, c, c, e 之中的非线性函数，然后做移位和加法。

SHA-1 的非线性函数集有以下 4 个，算法中使用了 4 个常数 K。

1) $f_t(X,Y,Z)=(X\wedge Y)\vee(\neg X\wedge Z)$

其中，t=0~19；K_t=0x5a827999。

2) $f_t(X,Y,Z)=X\oplus Y\oplus Z$

其中，t=20~39；K_t=0x6ed9eba1。

3) $f_t(X,Y,Z)=(X\wedge Y)\vee(X\wedge Z)\vee(Y\wedge Z)$

其中，t=40~59；K_t=0x8f1bbcdc。

4) $f_t(X,Y,Z)=X\oplus Y$

其中，t＝60~79；K_t=0xca62c1d6。

消息块从 16 个 32 bit字(M_0~M_{15})变换成 80 个 32 bit字(W_0~W_{79})，变换使用的算法为：W_t=M，对于t=0 到t=15，$W_t=W_{t-3}\oplus W_{t-8}\oplus W_{t-14}\oplus W_{t-16}<<<1$，对于 t=16~79，设t为操作号，从 1~80，W_t代表扩展后消息的第t个子块。

FOR　t=0 to 79

TEMP=(a<<<5)+f_t(b,c,d)+e+W_t+K_t

c=d

d=c

c=b<<<30

b=a

a=temp

(4)结果输出。将 a, b, c, d, e 和 A, B, C, D, E 分别相加，最后的输出为 A, B, C, D, E 的组合。由此产生 160 bit 的报文摘要。

根据 SHA-1 设计的 IP 核是根据原始标签加上密钥生成数字签名。该 IP 核是由 VHDL 编写逻辑与时序，用 Xilinx ISE 工具完成逻辑编译、化简、分割、综合、优化、布局、布线和仿真后验证的过程。IP 核的结构如图 2 所示。

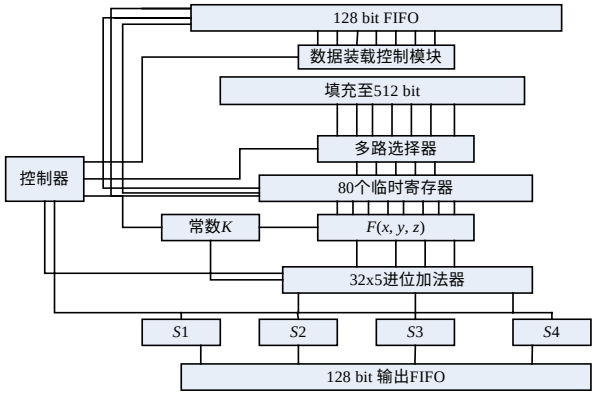

图 2　加密模块 IP 核结构

5　软硬件协同设计

5.1　RFID 阅读器的硬件结构

RFID 防伪阅读器是以 FPGA 为核心进行逻辑控制和数据处理交换的系统结构。防伪算法、用户接口以及 CPU 模块均由 FPGA 实现。该系统所有的控制和数据处理都通过 FPGA 内部可编程逻辑电路实现，由它完成与射频模块的通信，通过射频前端与标签的空中接口读取标签信息来获取标签 ID，通过 FPGA 内部的可编程逻辑单元中防伪 IP 核进行密文运算处理，与存储在 FLASH 中的密码比较，进行真伪判别。同时，FPGA 还实现与用户的人机交互接口。系统结构见图 3。本文采用 2.4 GHz 射频模块，符合 ISO14443 标准电子标签，标签中的 ID 为 128 bit，硬件开发板型号为 Xilinx Spartan-3 LC1500。

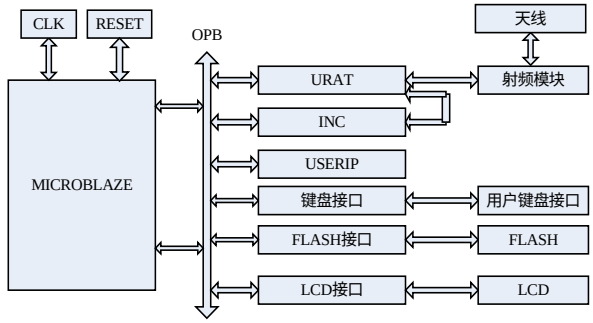

图 3　RFID 防伪阅读器的硬件结构

5.2　RFID 阅读器软件结构

程序的执行从键盘触发开始，通过向射频模块发出读标签命令，射频模块返回标签的信息，触发串口中断服务程序执行，将读出的信息放入 FIFO 队列，由防伪 IP 核进行解密运算并与存储在 FLASH 中的密码数据比较，将比较结果送 LCD 显示。RFID 防伪阅读器的软件结构如图 4 所示。

本文中的软件开发集成环境是 Xilinx Platform Studio 7 以及 Xilinx ISE 7。软件程序执行流程见图 5。

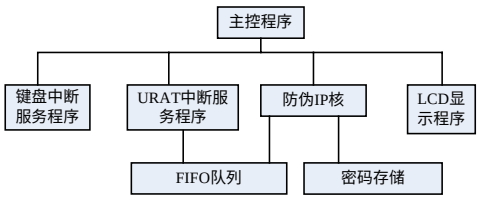

图 4　RFID 防伪阅读器的软件结构

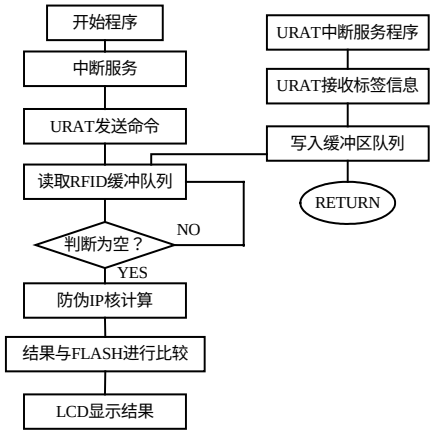

图 5　软件程序执行流程

6　系统实现及结果评价

FPGA 开发板的 URAT 接口与射频模块连接的实验如图 6 所示。

通过射频模块可以读取电子标签信息，在 Xilinx EDK 的 main()函数中发送命令：02 0B 03，液晶模块显示加密的标签信息码如下：

02 00 E8 00 00 08 00 00 00 00 00 00 01 34 DD F5 C8 27 03

图 6　FPGA 开发板与射频模块连接

7　结束语

本文的 RFID 防伪阅读器采用硬件 IP 核实现数字签名加密技术，加强了系统的安全性。系统的接收数据直接通过硬件电路计算获得结果，提高了系统的运算速度，实现了对商品电子标签的快速防伪验证。

参考文献

[1] Weinstein R. RFID: A Technical Overview and Its Application to the Enterprise[J]. IT Professional, 2005, 7(3): 27-33.

[2] Flores J L M. A Performance of RFID Tags in Near and Far Field[C]//Proc. of ICPWC'05. New Delhi, India: [s. n.], 2005.

[3] Geilen M C W. Formal Techniques for Verification of Complex Real-time Systems[D]. Eindhoven, Netherlands: Eindhoven University of Technology, 2002.

[4] Vogt H. Multiple Object Identification with Passive RFID Tags[C]// Proceedings of the IEEE International Conference on Systems, Man and Cybernetics. Yasmine Hammamet, Tunisia: [s. n.], 2002.

（上接第 27 页）

5　效率分析

本文方案最大的特色在于利用椭圆曲线离散对数问题构建整个方案，因此，方案中涉及的主要运算是椭圆曲线上倍点运算。而原有的无证书加密方案大都建立在基于身份密码学基础上，不可避免地要使用双线性对计算和椭圆曲线点求幂运算。相比较而言，双线性计算必须建立在所谓的“弱”椭圆曲线群上，这将一定程度上局限椭圆曲线的选择。此外椭圆曲线上的对运算所耗费的计算时间远大于椭圆曲线上的倍点运算，表 1 给出了在 Pentium 3.4 GHz，内存 1 GB，基域 q 为 302 bit 且使用 SSE2 指令集的测试环境下，点运算与 Tate 对计算所用时间对比。

可以看出，倍点运算的计算时间开销远小于对计算的计算时间开销，一次 Tate 对计算时间开销大约是一次倍点运算的 7 倍。若将 n 倍点运算优化为 2 倍点运算和点加运算，还可以进一步提高执行效率。

表 1　椭圆曲线中点运算与对运算时间比较　　s

2 倍点运算	点加运算	n 倍点运算	求幂计算	Tate 对计算
5.6×10^{-6}	7.8×10^{-6}	2.24×10^{-3}	2.77×10^{-3}	19.98×10^{-3}

另外本方案采用了 KEM-DEM 混合加密结构，公钥部分计算只涉及产生会话密钥和会话密钥封装，而实际的明文加密计算则有对称加密完成。对称加密函数具有更快的加密速度，以 AES 加密方案为例，其基本的运算如乘法和求逆运算都可以通过查表方式实施，效率非常高。对称加密算法对明文没有严格的限制，这样通过 KEM-DEM 结构可以以较低的代价加密任意长度的消息。

6　结束语

本文提出的基于椭圆曲线离散对数的混合加密方案，保持了无证书加密方案在公钥分发和管理上的优势，避免了原无证书方案中普遍采用的双线性对计算。改用基于椭圆曲线离散对数的签名方案，有效地保证了公钥的真实性。方案采用了 KEM-DEM 混合加密结构，可以用更少的公钥加密开销加密任意长度消息。

参考文献

[1] Al-Riyami S S, Paterson K G. Certificateless Public Key Cryptography[C]//Proc. of ASI-ACRYPT'03. [S. l.]: Springer-Verlage, 2003.

[2] Huang Xinyi, Susilo W, Mu Yi, et al. On the Security of Certificateless Signature Schemes[C]//Proceedings of CANS'05. [S. l.]: Springer- Verlag, 2005.

[3] Li X, Chen K, Sun L. Certificateless Signature and Proxy Signature Schemes from Bilinear Pairings[J]. Lithuanian Mathematical Journal, 2005, 45(1): 76-83.

[4] Libert B, Quisquater J J. On Constructing Certificateless Cryptosystems from Identity Based Encryption[C]//Proc. of PKC'06. [S. l.]: Springer-Verlag, 2006.

[5] Yum D H, Lee P J. Generic Construction of Certificateless Encryption[C]//Proc. of ICCSA'04. [S. l.]: Springer-Verlag, 2004.

[6] Shoup V. Using Hash Functions as a Hedge Against Chosen Ciphertext Attack[C]//Proc. of Eurocrypt'00. [S. l.]: Springer-Verlag, 2000.

[7] Miller V. Use of Elliptic Curves in Cryptography[C]//Proc. of Crypto'85. [S. l.]: Springer-Verlag, 1985.