基于嵌入式系统的密码机研究和实现①

A Cryptographic Device Based on Embedded System

叶展翔　(温州职业技术学院 计算机系 浙江 温州 325035)

王丽娜　(武汉大学 计算机学院 湖北 武汉 430072)

摘　要：密码机广泛地应用于信息的加密与解密。与单纯的软件技术和硬件技术相比，嵌入式技术为密码机提供了一种更高性价比的解决方案。本文在分析嵌入式密码机的结构的基础上，设计并实现了一种基于S3C2410的嵌入式密码机。该密码机通过网络接受客户的加密、解密请求，按客户要求对客户数据进行加密、解密处理，并回送处理结果。

关键词：密码机 ARM 以太网 加密 解密

1918年，德国发明家亚瑟·谢尔比乌斯(Arthur Scherbius) 发明了世界上第一台真正意义上密码机——ENIGMA，从而揭开密码技术发展的新的里程碑。今天，随着计算机技术的发展和Internet的普及，密码机在军事、通信、金融、商务等各个领域都得到广泛的应用。

在商用密码计算领域里，通常利用软件方法、或硬件方法来实现对数据的加密与解密，软件方法开发简单、灵活可变、易升级，但通常效率低，特别是可靠性不高；硬件方法具有运行速度快、可靠性高、使用简单等优点，但开发周期长、一次性投入大、缺乏灵活性；而嵌入式系统以MPU为核心，集软、硬件于一体，具有高集成、高可靠、功能强、成本低、可灵活定制等特点。作为可独立工作的SoC(System on Chip)，能很好地融合硬件实现方法和软件实现方法的优点，嵌入式技术为密码机提供了一种具有更高性价比的解决方案。

1　嵌入式密码机的结构

密码机是一种专用的高安全和高可靠的密码装置，主要为用户提供数据加密和通信保密功能。嵌入式密码机是一种基于嵌入式微处理器的SoC模块，图1给出了嵌入式密码机的基本结构[1]。

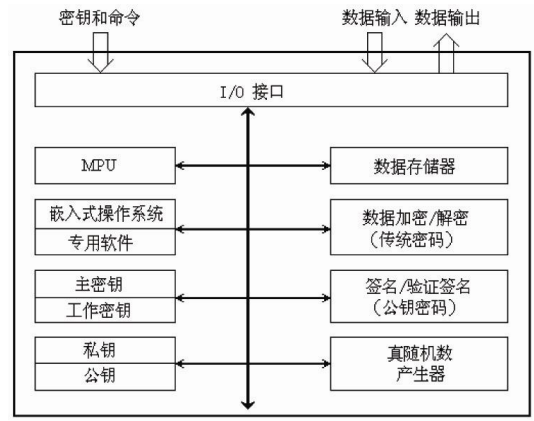

图1　密码机基本结构

(1) 嵌入式密码机本质上就是一种专用的嵌入式计算机系统，因此应具备嵌入式系统的基本资源：MPU、各类存储器（FLASH/SDRAM）、I/O接口、嵌入式操作系统等。

(2) 嵌入式密码机是专用于密码处理的设备，因此传统密码和公钥密码是必须的，传统密码主要用于数据加密、解密，公钥密码主要用于数字签名和验证签名。

(3) 嵌入式密码机还必须提供密码处理的配套功能：密钥生成、密钥的保存、随机数产生、Hash处理等。

① 收稿时间:2008-08-29

2　软件系统设计

2.1 系统分析与模块划分

本嵌入式密码机设计的主要功能是通过网络为客户提供数据加密和解密功能，工作流程如图 2 所示。

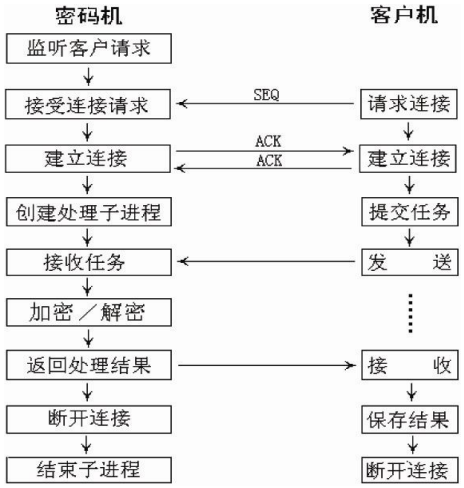

图 2　嵌入式密码机工作流程

根据密码机处理流程，嵌入式密码机软件系统分为密码机端代码(Server)和客户机端代码(Client)两部分，从功能上可划分为 3 个模块：

(1) 网络通信模块：负责实现密码机与客户机之间的网络通信。

(2) 加密/解密模块：负责对用户提交的数据进行加密或解密处理。

(3) 通信安全模块：负责确保密码机和客户机之间的通信安全。

2.2 网络通信模块

采用 SOCK_STREAM 类型建立 S/C 通信模型[2]，嵌入式密码机为 Server，客户端为 Client，提供面向连接的数据传输服务。

客户向密码机提交连接请求，通过三次握手建立 TCP 连接，然后双方接收或发送数据，通信完成后，关闭 Socket 拆除连接，如图 3 所示。

针对嵌入式密码机的应用需求，为了提高其工作效率，对 Server/Client 通信模型进行改进：

① Server 端改进：支持响应多客户并发请求；

② Client 端改进：支持发送数据与接收数据并行；

③ 收发数据改进：采用标准 I/O，提供数据输入/输出缓冲；

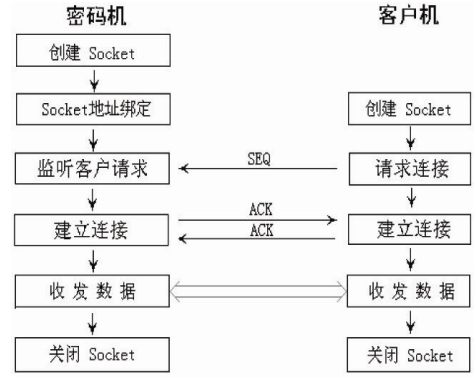

图 3　Server/Client 通信模型

2.3 加密/解密模块

密码机的核心功能是加密/解密数据，本密码机可提供多种传统密码算法供用户选择,如 3DES、AES 等，对客户提交的数据按客户要求进行加密或解密处理。

短块是分组密码的关键问题，文件的最后一个分组难免存在短块，采用密文挪用技术解决短块问题，即保证数据安全，同时又不引起文件大小的扩展，如图 4 所示。

加密处理：M_{n-1}➔a+b(被挪用)，M_n+b(挪用)➔Cn ；

解密处理：C_n➔M_n+b(被挪用)，a+b(挪用)➔M_{n-1} ；

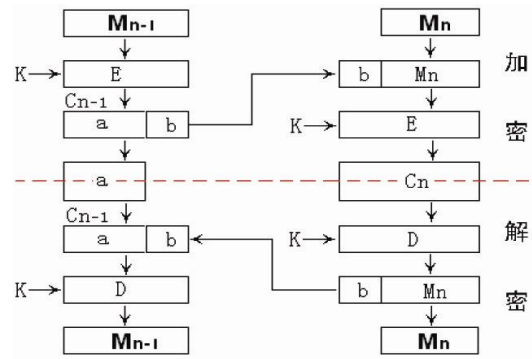

图 4　数据加密解密

2.4 通信安全模块

密码机选择以太网为输入、输出方式，首先必须确保通过网络传输的信息安全。在本密码机设计中，基于公钥密码 RSA 算法、传统密码 DES 算法和 Hash 函数 SHA1 算法，实现通信保密、数据保真和身份认证等多种安全机制，从而确保在开放的网络中确保通信安全。

(1) 通信保密

Client→Server 保密：Client 对发送的数据采用 RSA 公钥加密，Server 对接收的数据采用 RSA 私钥解密；只有密码机(Server)持有私钥，所以 Client→Server 是保密的。

Server→Client 保密：Server 对发送的数据进行 DES 加密，Client 对接收的数据进行 DES 解密；DES 密钥是由 Client 提交给 Server，由于 Client→Server 是保密的，所以只有 Client 自己与 Server 知道密钥，所以 Server→Client 是保密的。

(2) 数据保真

发送端 Hash 发送的报文，生成发送报文摘要；接收端 Hash 接收的报文，生成接收报文摘要；接收端比较发送报文摘要与接收报文摘要，验证数据的真实性。

(3) 身份认证

Server 对 Client 认证：只有授权用户拥有 RSA 公钥，Server 通过验证 RSA 公钥，实现对 Client 身份的合法性进行认证。

Client 对 Server 认证：只有 Server 采用 RSA 私钥进行数字签名，Client 利用 RSA 公钥验证数字签名，实现对 Server 的身份认证[3]。

3　硬件系统设计

嵌入式密码机系统基于 ARM9 硬件平台实现其加密、解密功能，硬件平台如图 5 所示。

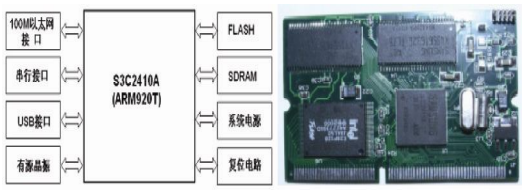

图 5　嵌入式密码机硬件系统

微处理器选择 Samsung 公司的 ARM920T 核的 S3C2410[4]，SDRAM 采用采用 2 片 Samsung 公司的 K4S561632E-TL75(32M)，FLASH 采用 Intel 公司的 E28F128(16M)，10M/100M 自适应以太网接口负责数据的输入输出，串行接口提供控制终端接入，硬件系统还包括系统电源、有源晶振、复位电路等外围辅助电路。

4　设计实现与测试

整体设计完成后，在嵌入式开发板上进行了具体的测试，本实验硬件系统采用北京博创兴业科技有限公司的 UP-NETARM2410-S 开发平台，核心硬件为：S3C2410X、64MB SDRAM 与 64MB NAND FLASH，系统测试模型[5]如图 6 所示。

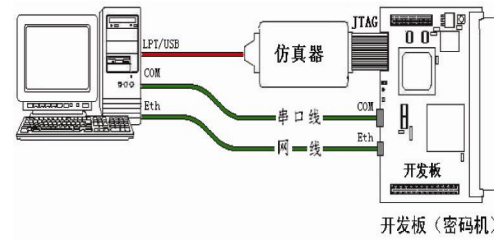

图 6　系统测试模型

软件系统包括嵌入式操作系统与密码机软件系统，嵌入式操作系统采用基于 Linux 2.0 Kernel 的 μClinux，密码机软件系统中的传统密码系统采用 DES 算法，公钥密码系统采用 RSA 算法，Hash 函数采用 SHA-1。

经测试，本密码机加密、解密速率达到 542Kbps，测试结果证明系统完全满足各种加密、解密操作。

5　结束语

本嵌入式密码机以嵌入式微处理器为核心，通过固化相应软件，组成一个 SoC 固件。与基于软件加密/解密相比，嵌入式密码机作为一个独立的设备能有效地隔断外界的影响，具有更好的安全性；与基于硬件的加密/解密卡相比，嵌入式密码机具有明显的成本优势与灵活性，能轻而易举地实现多种加密/解密算法。

本文的嵌入式密码机设计是嵌入式技术在信息安全领域内应用的一种尝试，为信息安全设备探索一种更灵活、更高效和高性价比的解决方案。

参考文献

1 张焕国.密码学引论.武汉:武汉大学出版社,2004:222－223.

2 Warren WG. 实战 Linux Socket 编程. 西安:西安电子科技大学, 2002:119－150.

3 张花,崔慧娟,唐昆.一种 RSA 算法之数字签名系统的快速实现方案.计算机工程, 2006,32(3):156－160.

4 s3c2410 Datasheet. Samsung Electronics Co, Ltd.

5 李驹光. ARM 应用系统开发详解.北京:清华大学出版社, 2004:218－243.