Research and Design of Network Encryption Card Based on FPGA

Xiaosong Zhang [1], Linhong Guo [1], Yumin Liu [2]

[1]*Department of Computer Science and Technology, Tangshan College, Tangshan,China*

[2]*Department of Information Engeering, Tangshan College, Tangshan,China*

Email: zxs0224@163.com; glh800907@126.com; llyymm888@tom.com

Abstract: With the rapid development of Internet and the advancement of the global information process, the subsequent issues of network security are also increasing day by day. The solutions of hardware security based on the programmable logic device will not only provide parallel processing capabilities, but also have advantages of the designable fleribility, high reliability, good scalability, and so on. This paper makes the specific research and design on the network encryption card based on FPGA techniques. The hardware circuit and the software design of network encryption card are completed. The entire process of the data communication experiment is very successful. The experiment results show that the hardware circuit and software solution of the network encryption card are correct, and the encryption data transmission is very reliable without affecting the transmission speed.

Keywords: network encryption card; scream cipher; FPGA

基于 FPGA 的网络加密卡的研究与设计

张小松 [1]，郭琳虹 [1]，刘玉民 [2]

[1]唐山学院计算机科学与技术系，唐山，中国，063000

[2]唐山学院信息工程系，唐山，中国，063000

Email: zxs0224@163.com; glh800907@126.com; llyymm888@tom.com

摘　要：随着互联网的飞速发展和全球信息化进程的推进，随之而来的网络安全问题也日益加剧。基于可编程逻辑器件的硬件安全性解决方案不但可以提供并行处理的能力，而且具有设计灵活、可靠性高、扩展性好等一系列优点。本文即是针对基于 FPGA 的网络加密卡技术进行了具体的研究与设计，完成了网络加密卡的硬件电路和软件程序的设计，并成功地完成了数据通信实验的全过程，实验结果证明了网络加密卡硬件电路和软件设计方案的正确性，而且能够在不影响传输速度的前提下，实现加密数据的可靠传输。

关键字：网络加密卡；序列密码；FPGA

1 引言

计算机网络的飞速发展为社会、企业乃至个人都带来了前所未有的便利，它正在以惊人的速度改变着人们的生活方式和工作效率。然而，互联网络的开放性和匿名性等特征也不可避免地带来了信息安全的隐患，并且日趋严峻。随着各行各业对信息技术的依赖越来越强，大量在计算机网络中存储和传输的数据都需要进行加密保护，信息安全已经成为影响国计民生的一个焦点问题。因此，以密码学为理论基础的信息加密技术，作为确保信息安全的最重要的技术措施之一。

信息加密，就是按照某种确定的加密算法，对未经加密的明文信息进行处理，使其成为难以读懂的密文信息。而密文恢复原始信息的过程称为解密或脱密[1]。从实现加密的手段来看，目前的加密产品主要分为软件加密和硬件加密两种。软件加密即是指用纯软件的方法来实现加密算法，它可以作为安全软件包或通信软件包的一部分，多用于个人电脑上的文件加密。软件加密具有移植性好，改动方便的特性，但是其加密和解密的速度都比较慢；硬件加密则不同，它是为特定的加密算法设计专门的硬件电路来完成整个运算，其运行速度仅为软件加密的千分之一，而且具有更高的抗解密性，兼容性和稳定性。因此，出于速度、安全性等方面的考虑，目前硬件加密产品更加受到人们的青睐。

978-1-935068-42-6

近几年来，随着大规模集成电路的飞速发展，FPGA 芯片技术在设计、功能、性能和成本造价上都有了长足的进步，特别是片上系统技术的兴起使得解决上述的问题成为可能。由于对 FPGA 的开发是采用软件的设计思想对 FPGA 进行编程生成硬件逻辑，加密算法可以完全固化为硬件逻辑门电路，所以能够解决 CPU 串行工作时在速度上受限的问题，从而硬件加密的速度得以进一步地提高。国内利用 FPGA 技术实现加密算法的研究仍处于初级阶段，相关产品更是相当缺乏，因此，基于该项技术的网络加密卡和相关产品的研发具有重要意义。

2 网络加密方式

数据加密技术是所有网络上通信安全所依赖的基本技术。目前主要有三种方式：链路加密方式、节点对节点加密方式和端对端加密方式。数据保密变换使数据通信更安全，但不能保证在传输过程中绝对不会泄密，因为在传输过程中，还有泄密的隐患[2]。

采用链路加密方式，从起点到终点，要经过许多中间节点，到达每个节点时均要暴露明文，如果链路上的某一节点安全防护比较薄弱，那么即使是采取了加密措施，但整个链路的安全只相当于最薄弱的节点处的安全状况。

采用端端加密的方式，只是发送方加密报文，接收方解密报文，中间节点不必加、解密，也就不需要密码装置。此外，加密可采用软件实现也可以采用硬件实现，使用起来很方便。在端端加密方式下，每对用户之间都存在一条虚拟的保密信道，每对用户应共享密钥，所需的密钥总数等于用户对的数目。虽然用户需要保存的密钥数目比较大，但用户不会因为窃密者窃取部分密钥而导致整个保密信道失效，这种特性使得端端加密尤其适用于军事、外交等重要信息的发送[3]。

从身份认证的角度看，链路加密只能认证节点，而不是用户。使用节点 A 密钥的报文仅保证它来自节点 A，其实，报文可能来自 A 的任何用户，也可能来自另一个路过节点 A 的用户。因此链路加密不能提供用户身份鉴别。端端加密对用户是可见的，可以看到加密后的结果，起点、终点都很明确，可以进行用户认证。

综上可知，链路加密对用户来说比较容易，使用的密钥较少，而端端加密比较灵活，用户可见。对于安全性要求较高的用户，应采用端端加密的方式。

3 序列密码加密算法

序列密码加密算法是本文在加密网卡的设计中所采用的加密算法，它是一种将明文与密钥逐位异或转换成密文的密码算法[4]。其具体模型如图 1 所示。

在加密端，密钥序列跟明文序列异或运算产生密文序列，其加密过程为： $ci = mi \oplus Zi$ ；

在解密端，密文序列与完全相同的密钥序列异或恢复出明文序列，其解密过程为：$mi = ci \oplus Zi$ ；

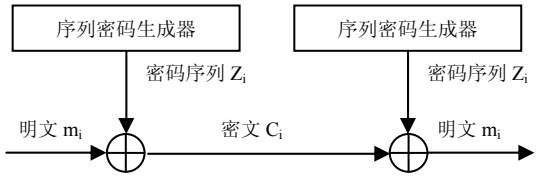

Figure 1. Sequence cryptograph
图 1. 序列密码体制

为了度量密钥序列的随机性，Golomb 提出了以下随机性公式[5]：

（1）设序列周期为 r，若 r 是奇数，则一个周期内 0 的个数比 1 的个数多一个或少一个；若 r 是偶数，则 0 和 1 的个数相等；

（2）在序列的一个周期内，长为 c 的游程占总游程总数的 1/2c (c=1,2,…)，1 的 c 游程个数和 0 的 c 游程个数相等；

（3）异自相关函数是一个常数。

4 基于 FPGA 的网络加密卡设计

4. 1 FPGA 选型

FPGA 是一种大规模可编程逻辑器件，它是可编程阵列逻辑、通用阵列逻辑、电可编程逻辑器件等可编程器件进一步发展的产物[6]。它不但拥有灵活的体系结构和逻辑单元，并且具有集成度高、适用范围宽、设计开发周期短、制造成本低、开发工具先进、标准产品无需测试、质量稳定以及可实时在线检验等特点，因此被广泛应用于产品的原型设计和产品的生产之中。

目前 FPGA 的品种很多，有 XILINX 的 XC 系列、TI 公司的 TPC 系列、ALTERA 公司的 FIEX 和 Cyclone 系列等。Altera CycloneTM FPGA 是目前市场上性价比最优且价格最低的 FPGA，本文设计的网络加密卡 FPGA 芯片采用的是 ALTERA 公司生产的 Cyclone 系列中的 EPIC6Q240C8，该款芯片具有较高的性价比。串行配置芯片采用的是 EPCS 1，对 EPCS1 编程后，程序烧入到 EPCS 1 的 EEPROM 中，上电后自动对 FPGA 进行配置。

4.2 网络加密卡的硬件电路设计

本文研究的网络加密卡的主体设计思想是将主机接口电路中加入 FPGA 芯片，并在 FPGA 芯片中加入加密模块，对接收和发送帧中的数据部分进行加/解密。此方法的特点是不会对 IP 路由等信息造成破坏，而且适用于现有的网络设备。加密卡电路框图如图 2 所示。

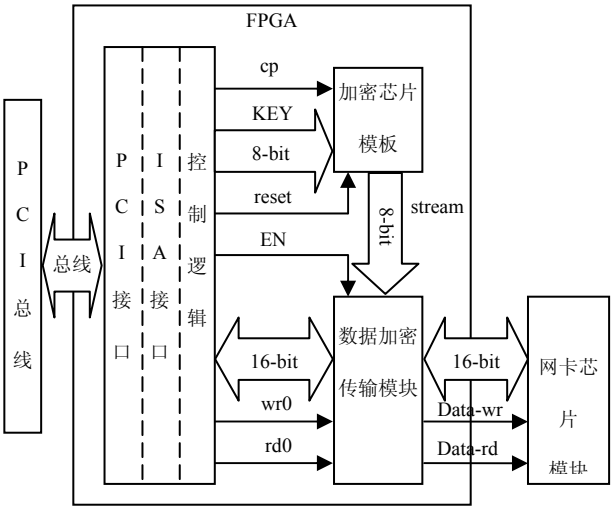

Figure2. Block diagram of the network data encryption card

图 2. 网络数据加密卡电路框图

加密卡 FPGA 模块中主要包括 PCI 接口、ISA 接口、控制逻辑、加密芯片模块和数据加/解密模块。PCI 接口主要负责产生与计算机 PCI 接口进行总线读写的交易时序。从计算机传来的 PCI 时序由 ISA 接接口负责转换为可对 RTL8019AS 进行读写的时序。该模块由一个延时模块和一个锁存模块构成。控制逻辑主要是处理来自 ISA 接口的数据，控制加密芯片的初始化和复位，控制数据加/解密模块。数据加/解密模块通过明文（密文）与密码序列进行二元加进行数据的加密（解密），由控制模块传来的使能信号决定是否对数据进行加（解）密。

4.3 网络加密卡的软件设计

4.3.1 驱动程序设计

开发驱动程序采用的是 Jungo 公司出版的 windriver 设备驱动程序开发组件，它可以方便 Windows 程序员快速开发出 PCI/ISA 设备的 Windows 驱动程序。利用 WinDriver 开发设备驱动程序，不需要熟悉操作系统的内核，整个驱动程序中的所有函数都是工作在用户态下的，通过与 WinDriver 的*.Vxd 或者*.Sys 文件交互来达到驱动硬件的目的。并可大大减少研制加密卡的时间。

4.3.2 网卡发送进程

网卡的发送进程主要是指 TCP 文件的传输。文件传输可选择加密或非加密方式。无论是何种传输，TCP 首先进行“三次”握手建立连接，随后发送进程以二进制只读方式打开文件，判断此次传输是加密传输还是非加密传输，具体的发送流程如图 3 所示。

其中，如果是非加密传输，数据经发送程序打包后发送。非加密传输的代码如下：

```
for(ii=4;ii<length+4;ii++)
write(reg10,txdnet.bytes.bytebuf[ii]);  //数据传输
write(reg00，0x3e);    //启动发送命令;
```

如果是加密传输，在发送第一帧之前，发送进程会调用下面的函数对密码芯片进行复位并设定初始密钥。

```
void_fasteall TForm_main::setpassword () {
write(reg11,0xff);  //芯片复位
write(reg12，password);  //发送密钥 }
```

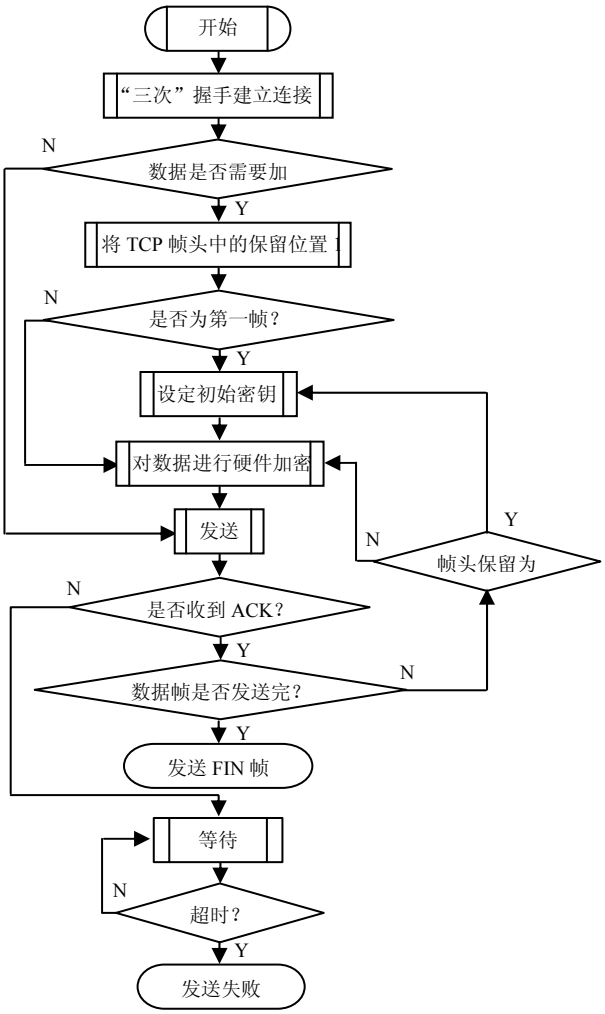

Figure 3.Flow chart of sending

图 3. 发送流程图

978-1-935068-42-6 © 2010 SciRes.

密钥设定后，发送程序进行 TCP 打包，打包中会将 TCP 数据报中的保留位置 1 作为标记供接收方识别，然后发送，加密传输的代码如下：

```
for(ii=60;ii<length+4;ii++) {
write(regl3，0xff);  //向密码芯片发送脉冲信号
write(reg14，txdnet.bytes.bytebuf[ii]);  //对传输数据进行加密 }
write(reg00，0x3e);  // 启动发送命令
```

在等待 ACK 应答帧时，TCP 程序启动一个定时器，在规定时间内如果没有收到应答帧，则取消发送任务，同时在接收窗口显示发送失败，收到接收方 ACK 确认后，发送下一帧，直至文件完全发送完毕。发送完毕时向接受方发送 FIN 结束帧。

4.3.3 网卡接收进程

网卡的接收进程与发送进程类似，三次握手建立连接后，接收进程会启动一个定时器，如果在规定时间内没有收到数据，则结束接收，同时打印错误报告；如果收到数据，接收进程会读取数据报头部信息，判断 TCP 的保留位是否为 1（1 代表数据已经加密，0 代表数据没有加密），如果收到的是加密文件，发送程序会首先对密码子芯片进行设定，然后进行解密接收，并发送 ACK 应答。在收到 FIN 结束数据报后，发送 FINACK 确认并结束接收。

4.4 数据通信实验

数据通信实验的平台为两台安装了基于 FPGA 的网络加密卡的计算机和一台锐捷 S3526 以太网交换机。

实验中，传输一个大小为 9.572KB 的文本文件，以加密和非加密两种方式发送。实验结果是：正常传输和加密传输（接收方和发送方输入密钥一致），数据无任何变化。如果加密传输时接收方和发送方输入的密钥不一致，则接收时无法正常解密，会接收到乱码。

经测试，非加密文件的传输速度为 45.260kbps，加密传输的速度为 43.836kbps。因此，加密以后对数据传输速度的影响很小，和正常文件的传输速度基本持平。

最终的数侧通信实验验证了基于 FPGA 技术的网络加密卡硬件电路逻辑和软件程序设计的正确性，成功地实现了加密数据的可靠传输。

5 结束语

当前国内外所研制的加密卡不是基于 DSP（Digital Signal Processing）,就是利用专用芯片方式。这两种方式都存在其固有的弊端。DSP 方式和专用芯片方式虽然可以达到较高的速度，但是它的致命弱点就是算法不能及时更新，DSP 的算法描述非常复杂，而专用芯片一旦要更换算法就得重新设计加密芯片，这必然会增加开发的成本，延长开发周期。此外，生产专用加密芯片的成本非常高，而且由于受到国内生产工艺的限制，使得所生产出的专用芯片在某些方面的性能会受到影响，不能达到理想的要求。

基于 FPGA 技术的网络加密卡的研究和设计正是弥补了基于 DSP 方式和专用芯片方式的加密卡的诸多不足，从技术和经济上都具有很好的可行性。

本文针对基于 FPGA 的网络加密卡技术进行了具体的研究与设计，完成了网络加密卡的硬件电路和软件程序的设计。硬件设计上，在分析了网卡芯片功能与结构的基础上，成功地完成了 PCI 接口与 ISA 接口之间的通讯，设计了控制逻辑模块和数据加/解密模块，将各模块有机地结合在一起，有效地解决了控制模块、密码芯片和数据加/解密模块之间的协作问题。软件设计上，不但完整地实现了网卡传输数据的功能，而且为用户提供了加密和非加密两种可选的数据传输方式。通过数据通信实验，验证了网络加密卡的整体设计方案的正确性，具有较好的人机交互界面，不但成功地完成了加密数据的可靠传输，而且硬件设计部分数据加/解密模块的引入并没有过多地影响文件的正常传输速度。

基于 FPGA 技术的网络加密卡的研究尚处于初步阶段，比如对其它加密算法的研究与实现以及利用中断方式对数据传输速度的进一步提高等，都有待于更加深入的研究。

References (参考文献)

[1] Liu Yi. Intemet security mechanism [J]. Bohai University journal, 2004,25 (4) :384-386
刘艺．Intemet 上的安全机制[J]．渤海大学学报，2004，25(4)：384-386．

[2] Ji Bu-mei. Communication Leaks and Confidential [J]. Modern communications, 2004, 11:35-37.
季卜枚．通信泄密与保密[J]．现代通信，2004, 11：35-37.

[3] Ding Qun. Research of Encryption Methods of DES and RSA and Development of Seqence Cipher [J]. Natural Science journal of Heilongjiang University, 2002, 21 (2): 71-74.
丁群．DES 和 RSA 加密方法以及序列密码的发展研究[J]．黑龙江大学自然科学学报，2002, 21 (2) ： 71-74.

[4] Alfred J., Menezes, Paul C., Van Oorschot, Scott A. Vanstone. Handbood of Applied Cryptography [M]. Hu Lei, Wang Peng translation. Beijing: Electronic Industry Press ,2005:152-159.
Alfred J.， Menezes, Paul C.， Van Oorschot, Scott A. Vanstone． Handbood of Applied Cryptography[M]．胡磊，王鹏译．北京：电子工业出版社，2005：152-159.

[5] Lu Kai-cheng. Computer cryptography - Data security in computer networks [M]. Beijing: Tsinghua University Press, 1998 :185-205.
卢开澄．计算机密码学—计算机网络中的数据保密与安全[M]．北京：清华大学出版社，1998 ：185-205．

[6] Xu Wei-ye, Jiang Bing, Yu Xiang-Bin. Comparison of Development and Application of CPLD / FPGA [J]. Modern electronic technology ,2007,2:4-7.
徐伟业，江冰，虞湘宾．CPLD/FPGA 的发展与应用之比较[J]．现代电子技术，2007，2：4-7

978-1-935068-42-6