基于 FPGA 的 DES 算法的并行加密技术

肖新帅 刘洪鹏
(聊城大学物理科学与信息工程学院 山东 聊城 252059)

【摘 要】本文利用 FPGA 的高集成度,硬件加密速度快的特点,提出了利用多个 DES 加密器对图像、表格、传真、文字或网络数据进行并行加密,但这些加密信息必须是二进制编码。

【关键词】FPGA;DES 算法;并行加密;二进制编码

Parallel Encryption Technology of DES Based on FPGA

XIAO Xin-shuai LIU Hong-peng
(School of Physics Science and Information Engineering, Liaocheng University, Liaocheng Shandong, 252059 China)

【Abstract】With characteristics of the high integration rate of FPGA and the high-speed encryption of hardware, the article proposes using many DES encryptions to the image, the form, the facsimile, the words and the network datas to carry on the parallel encryption, however, the encryption information must be binary-coded.

【Key words】FPGA; DES algorithm; Parallel encryption; Binary encoding

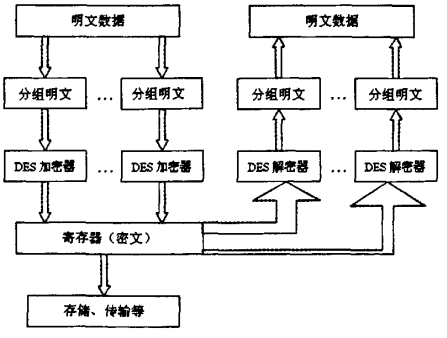
0 引言

计算机和通信技术的飞速发展,使得多媒体在人们的生活占有很大比重。信息更容易被剪切、复制、携带,在方便人们工作生活的同时,这也为信息的安全保密带来了许多不定因素。因此,加密技术对这些信息存储、传输将带来很好的保护作用,使得只有特定人看到特定的信息。当前,最直接的加密技术就是将多媒体信息(图像、音频等)当作普通的二进制数据,利用 RSA 和 DES 来进行加密。由于多媒体信息数据量一般都很庞大,这种加密方法速度较慢,效率也低。本文提出了一种改进的 DES 算法的加密技术,利用 FPGA 的高速度、高集成度[1],用其来实现多个 DES 硬件加密器[2]。加密时,将庞大的数据量分成多个固定长度的明文信息,然后将这些明文信息利用多个 DES 硬件加密器同时进行加密。大大提高了加密速度和效率。

1 基本原理

1.1 主系统结构图

该加密系统主要由明文分组模块、DES 加密模块、DES 解密模块、寄存器模块组成。如图所示:



1.2 各部分功能介绍

明文分组模块:用来存储被分成 64bit 的二进制数据一组的明文;

DES 加密模块:该模块是基于 FPGA 的硬件加密模块。用来将 64bit 的分组明文进行加密,其输出的密文也是 64bit;

DES 解密模块:将 DES 加密模块输出的 64bit 密文进行解密。其密钥与加密模块中的密钥相同,只不过其解密的子密钥使用顺序与加密时正好相反;

寄存器模块:在其内部的指定位置存储相应的密文。

2 具体加密/解密步骤

加密过程:

步骤 1:首先确定二进制明文数据的大小,其大小可能不是 64 的整数倍。这时要对原明文数据进行预处理,使其大小为 64 的整数倍,其方法是在原始明文尾部填充 0。然后对明文数据进行分组,让每一组都是 64bit。本文采用的是 635 位的原始明文数据。

步骤 2:将待加密的 64bit 的各个分组明文输入到相应的 DES 加密器中。首先分组明文进行初始置换 IP,然后将置换后的 64bit 明文数据分为左右两个部分各 32bit:L0 和 R0,接下来进行 16 圈迭代,在每一圈中,右半部分在 48bit 圈子密钥 k 的作用下进行 f 变换,得到 32bit 数据与左半部分异或,产生的 32bit 数据作为下一圈迭代的右半部分,原右半部分直接成为下一圈迭代的左半部分,但第 16 圈不进行左右对换。R16,L16 为第 16 圈迭代后输出的左半部分和右半部分,最后对(R16,L16)进行末置换 IP-1(初始置换 IP 的逆置换),所得结果 IP-1(R16,L16)即为密文。关于算法的详细介绍可参阅文献[3]

步骤 3:输出的密文,每一个 DES 加密器输出对应着寄存器的相应位置,将密文序存储到指定的位置。

解密过程的步骤同加密过程,在这里不再赘述,只不过解密的圈子密钥与加密时的使用顺序正好相反。

3 结论与展望

传统的 DES 加密算法只是对明文进行串行加密,这样当数据量很大时,将极大地影响加密速度,降低了工作效率。本文提出的并行加密是对串行加密的改进,在实验中,采用了 10 个 DES 加密器,这样比串行加密工作效率提高了 10 倍。另外,本文的 DES 加密器是基于 FPGA 的,它是一种硬件加密器,与单纯利用软件加密相比,这也很好地提高了加密速度。

随着微电子技术的发展,电子器件的集成度[1]将会越来越高,完全可以将多个 DES 加密器集成在一块板子。在实际应用中,可以增加 DES 加解密器的个数来进一步提高加密速度。

【参考文献】

[1]潘松,黄继业.EDA 技术实用教程.第二版[M].科学出版社.

[2]王简瑜,张鲁国.基于 FPGA 实现 DES 算法的性能分析[J].微计算机信息,2007,23(8):217-218.

[3]祝跃飞,王磊.密码学与通信安全基础[M].武汉:华中科技大学出版社,2008,11:90-92.

作者简介:肖新帅(1985—),男,聊城大学硕士研究生,研究方向为智能信息处理。

刘洪鹏(1986—),男,聊城大学硕士研究生,研究方向为智能信息处理。

[责任编辑:王静]