文章编号:1000 - 582X(2005)02 - 0074 - 03

基于混沌算法的软硬件相结合的加密方法*

杨　欣,李　强,黄席樾
(重庆大学 自动化学院,重庆　400030)

摘　要:加密是保护信息数据和加强知识产权保护的重要手段。以往人们多用软件方法进行加密,但是软件加密法存在运算量大,易于跟踪仿真攻击等缺点。硬件加密可减轻微处理器的负担,且具有物理保护,安全性较高。为了实现把硬件与软件结合起来共同加密,以达到优势互补的目的,可利用混沌算法的高随机性作为密钥流随机发生器的理论算法,用 VHDL(Very-High-speed Integrated Circuit Hardware Description Language)对 FPGA(Field Programmable Gate Array)进行设计,来实现混沌算法,开发出的应用软件对硬件进行控制,发送控制信号。实验证明,此法可提高加密算法的执行效率,增强加密系统的安全性。

关键词:加密;混沌序列;现场可编程门阵列;硬件描述语言
中图分类号:TP309.7　　**文献标识码**:A

当今是信息高速发展的时代,在竞争激烈的现代社会,信息就等同于机遇、利润和生存的力量。如何使自己的信息专利得到保护,越来越得到人们的关注。于是人们就把加密概念引入了信息领域里,形成一个新的科研领域——密码学。近年来,混沌现象引起人们的极大兴趣并得到深入研究,混沌现象具有的高随机性,使人们把它与密码学联系了起来,成为混沌理论应用的重要领域之一。在信息加密的初期,人们把目光都着眼于软件加密,研究各种算法,但是算法越严密,其计算量就越大,加重了微处理器的负担。随着 FPGA(Field Programmable Gate Array)器件的发展,使硬件加密技术得到完善,并广泛流行起来。硬件加密法解决了由于算法繁冗所引起的效率降低以及软件加密保密度不高等缺点,使硬件加密在加密市场占的份额日益增大。以下介绍一种用硬件方法实现混沌算法的加密方法,使软件与硬件相结合,相辅相成,扬长避短,以提高加密系统的安全可靠性。

1　密码体制准则及加密基本原理

20 世纪 40 年代,香农(Shannon)把信息论、密码学和数学结合起来,研究了"加密系统的数学结构",发表了关于加密技术的经典文章"Communication Theory of Secrecy System"(加密系统的通信理论)。该文首次从理论上提出了密码学的概念和原理,推动了加密技术的发展。

按照 C · F · Shannon 的提法,密码体制应该具备以下 5 个准则[1]:

1)破译密码需要极大的工作量;
2)密钥的长度很小;
3)加密和解密所进行的操作比较简单;
4)即使产生错误,错误的扩散也很小;
5)信息被加密后并不改变原信息的长度。

已知明文 P_i 与密钥 K_i 异或得到密文 C_i,而 C_i 在与密钥 K_i 异或就会恢复为明文 P_i,这种算法很简单,其表示如下:

加密　$C_i = P_i \oplus K_i$;
解密　$P_i = C_i \oplus K_i$;

从图 1 可以看出,这种方法有利于密钥的选取,只需选用一个密钥就可,加密密钥与解密密钥相同,便于密钥的管理,且不会改变明文的长度。

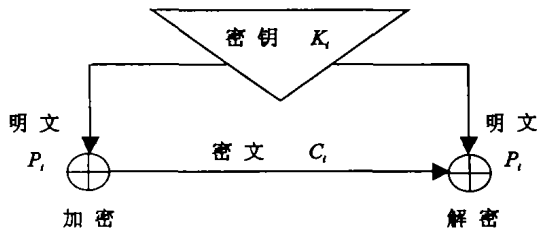

图 1　加密基本原理

* 收稿日期:2004 - 09 - 15
基金项目:重庆市科委攻关项目(2003035 - 02)
作者简介:杨欣(1977 -),女,甘肃兰州人,重庆大学硕士,主要研究方向:混沌加密,信息安全。

2　混沌 Logistic 映射

2.1　密钥流选取及混沌 Logistic 映射

由于选取的加密密钥与解密密钥相同，所以这个加密方法的重点就在于怎样设计一个合理的密钥流发生器。而作为密钥流的最好选择是一组随机序列，随机度越高，加密特性越好，安全度越高。随机序列不仅要求统计学上的随机，而且要求它是不可预测的，即给定完整的算法知识或硬件随机序列生成器和已有的比特流，下一随机位从计算上必须是难以预测的。而现在比较流行的伪随机序列发生器产生的序列的周期都是有限的，其随机性及不可预测性都不高，所以人们希望有其他更好的随机序列发生器。20 世纪 80 年代以来，混沌现象及其伪随机性的深入研究，使混沌理论应用于加密领域。

混沌的一个最基本的特征就是对初始条件的敏感性。任意 2 个有细小差别的初始值 x_0 和 x'_0，在经过多轮迭代后，得到的 2 个迭代序列 $\{x_0, x_1, \cdots, x_n\}$ 和 $\{x'_0, x'_1, \cdots, x'_n\}$ 会发生背离，使输出的结果完全不相关[2]。利用这一特性，可以产生许多非相关、高随机性的混沌序列，完全可以选取混沌序列作为密钥流。

在这里，选取混沌 Logistic 映射。离散时间动态系统 Logistic 映射定义如下[3]：

$$x_{n+1} = \mu x_n (1 - x_n)$$

$$0 < x_n < 1 \qquad 0 < \mu < 4$$

其中 x_n 为状态，μ 为参数，当以初始值 x_0 为初始状态进行迭代，再通过调节参数 μ，就可以得到一个理想的混沌序列。Schuster 导出当 $\mu_\infty < \mu < 4$，$\mu_\infty = 3.569\,945\,6$ 时，Logistic 映射处于混沌状态，其周期 $N \to \infty$。图 2 所示是当 $\mu = 3.0 < \mu_\infty$，$x_0 = 0.625$ 时的混沌序列，序列在迭带一定次数后，会发生收敛现象，出现周期性。图 3所示是 $\mu = 4$，$x_0 = 0.625$ 时迭代产生的混沌序列，所产生的混沌序列具有很好的随机性，近似于现实世界的白噪声随机序列。

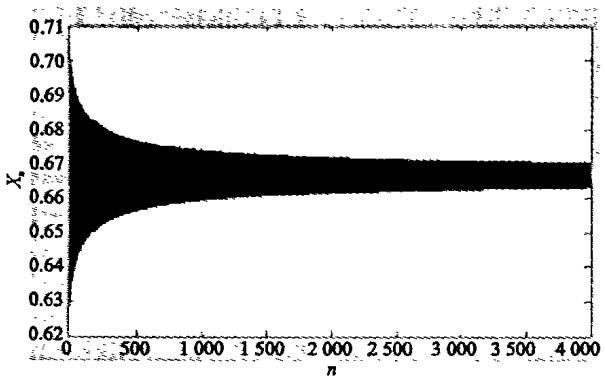

图 2　$\mu = 3.0, x_0 = 0.625$ 时的随机序列

但是，直接用此法产生的随机序列有一个缺陷，就是在初始值相近的情况下，要经过多轮迭代，序列才出现背离，产生不相关的 2 个随机序列。这样，攻击者可以通过选取 2 个相近的初始值，截取开始片段，就能解出相应的参数和初始值，这样就降低了整个加密系统的安全度。所以，在使用混沌序列时，要截取掉前面的一部分序列，具体截取多少，视选取的参数和初始值而定。

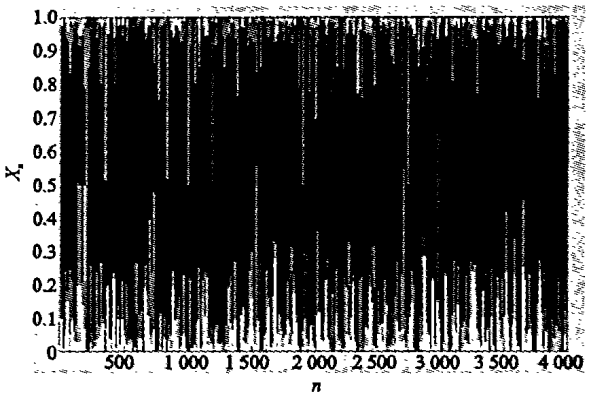

图 3　$\mu = 4.0, x_0 = 0.625$ 时的随机序列

2.2　混沌 Logistic 映射的性能分析

1）抗攻击能力

根据以上的分析，当 $\mu > \mu_\infty = 3.569\,945\,6$ 时，Logistic 映射处于混沌状态，其周期 $N \to \infty$，若攻击者用穷举法进行蛮力攻击，则需要 2^N 次操作，不管是从现实世界还是从成本利润的角度看都是很难成功的。

2）性复杂度

在序列密码理沦中，线性复杂度是序列密码体制的一个重要指标，无论在密码系统的设计还是在分析中，线性复杂度都是进行系统性能评估的重要指标之一。混沌 Logistic 映射的线性复杂度为[4]：

$$C_L(X_n) \approx N/2$$

其中 N 为序列的周期，当 $N \to \infty$ 时，序列的线性复杂度 $C_L \to \infty$。

3）平均非线性复杂度

由于序列加密体制的非线性化趋势，线性复杂度已不再是序列加密体制优劣判别的唯一标志，这是因为在非线性序列中，线性复杂度高的体制未必一定安全，还可找到其他非线性的攻击方法，因此非线性复杂度的指标在密码学中的作用也很重要，而系统的平均非线性复杂度更有代表意义。混沌 Logistic 映射的平均线性复杂度为[5]：

$$E(C_N(X_n)) = O(\log N)$$

其中 $O(\log N)$ 为 $\log N$ 的同阶无穷大量。

3　硬件实现

由于选取混沌序列作为密钥流，而混沌方法产生的混度序列是通过迭代产生的，这种迭代过程的计算量很大，在加密过程中也有许多对位串的复杂操作，这些都要占用微处理器来进行运算，大大降低了其工作效率，这样是得不偿失的。如果用设计的硬件来实现这些计算和操作，将大大减轻微处理器的负担，提高运

行速度。并且硬件由于有物理物质支托,使攻击者无法用调试工具和打开物理外壳的方法进行修改和窥探加密数据,从而提高了安全性。再者,加密硬件易于安装,可以减少工作量,提高效率。所以,用硬件方法实现加密算法不失为一种明智的选择。

用户现场可编程门阵列 FPGA 是一种新兴的高密度的可编程逻辑器件。它具有门阵列的高密度集成性和 PLD 的现场可编程的灵活性,成为目前可编程逻辑器件的新星,得到越来越多用户的认可。选取 ACTEL 公司的 FPGA 器件,是因为其 A1010、A1020 有很好的保密性,主要是因为其制作工艺是采用难以摄像的 NT fuse技术,且码点内容在 FPGA 本身片内,所以用物理剖解法很困难,且码点内容不易拷贝[6]。在硬件设计中,采用硬件描述语言 VHDL(VHSIC Hardware Description Language)设计硬件电路。因为 VHDL 具有功能强大的语言结构,可用简洁明确的代码描述来进行复杂控制逻辑的设计。

其硬件实现如图 4 所示。微处理器读取密钥(初始值),启动密钥流和计数器开始动作,当计数器计数到应截取的密钥流个数时,微处理器发送信号启动加密转换。

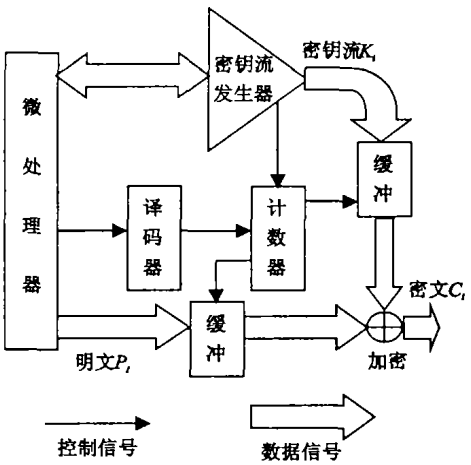

图 4 硬件电路结构示意图

4 软件实现

根据混沌算法对初始值敏感这一特性,可以选取初始值作为加密密钥和解密密钥,以触发密钥流发生器动作。软件就是用来实现密钥的读取,计数值的读取,并使微处理器实时地发送各种动作信号,以启动和结束加密过程。图 5 是软件程序简略实现流图。图 6 是此方法的加密效果 。

5 结 语

加密与解密是一对矛盾共同体,相互制约,相互促进。一种新的加密方法出现,紧随其后就会有相应的解密手段产生,解密手段的产生又促使加密方法不断改进。用硬件与软件相结合所实现的加密系统,具有较高的安全度, 使攻击者在相当一段时期内难以破解。但是用混沌算法,对精度要求较高,在精度低的情况下,容易陷入周期循环。所以,要进一步提高加密系统的安全度,就要提高硬件的精度,以满足加密系统的需求。

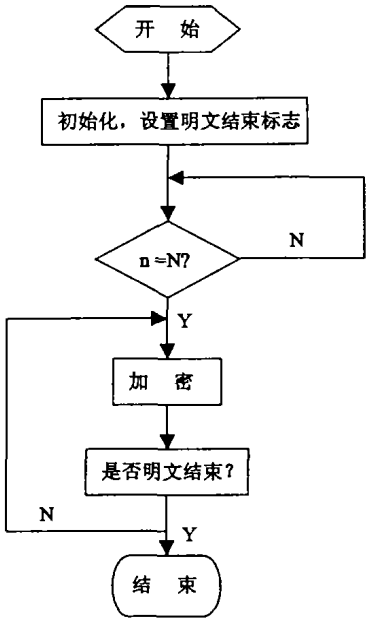

图 5 软件实现流图

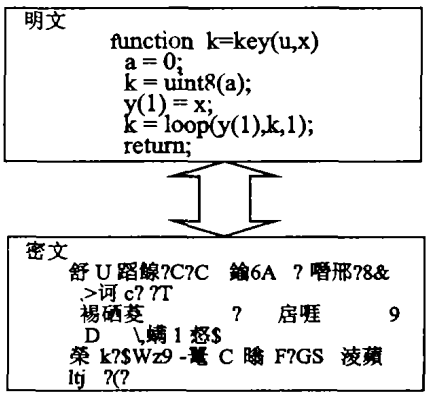

图 6 明文加密

参考文献:

[1] 雷方桂. 件加密解密技术及应用[M]. 长沙:中南工业大学出版社,1995.

[2] GOCE JAKIMOSKI, LJUPCO KOCAREV. Chaos and Cryptography: Block Encryption CiphersBased on Chaotic Maps [J]. Circuits and Systems—I:Fundamental Theory and Applications,2001,(2):163 - 169.

[3] 赵嘉莉,罗四维,温津伟. 基于神经网络的混沌加密算法[J]. 计算机研究与发展,2001,(12):1 475 - 1 479.

[4] 杨义先. 编码密码学[M]. 北京:人民邮电出版社,1992.

[5] 沈世镒. 组合密码学[M]. 杭州:浙江科学技术出版社,1992.

[6] 李华. 硬件加密解密技术综述[J]. 广东自动化与信息工程,1996,(3):42 - 48.

(下转第 96 页)

Predictions for the Strengths of Symmetry Composite Laminates Under Matrix Cracking

WANG Fang, ZHANG Jun-qian, DING Jun

(College of Resource & Environment Science, Chongqing Unversity, Chongqing 400030, China)

Abstract: The model is constructed based on *Equivalent Constraint Model* proposed by Zhang to establish a predictive method for the remaining strength of symmetry laminates under matrix damage. Because matrix cracking leads to re-distribution of stress of the laminates, the stress or strain of the primary load-bearing lamina (i. e. 0° lamina) will be greatly deteriorated, while 0° lamina controls the final fracture of the laminates. If 0° lamina grows a crack, the laminates are ruptured. The authors calculate the results for different materials and different lamina arrangement of laminates. It shows that the correlation between the experimental results and the theoretical predictions is quite reasonable.

Key words: symmetry laminates; ECM; primary load-bearing lamina; Hoffman rule; utmost strength

(编辑 张小强)

(上接第 76 页)

Cryptography of Combining Hardware and Software Based On Chaotic Algorithm

YANG Xin, LI Qiang, HUANG Xi-yue

(College of Automation, Chongqing University, Chongqing 400030, China)

Abstract: Encryption is vital for protection of data and intelligence property, which is often used to encrypt products by software. However, software encryption has some shortcoming such as mass operations and easy being simulated. Hardware encryption has high security because this method can relieve burden of MPU and has physical protection layer. We can use high randomicity of chaotic algorithm as generator for cipherkey in order to combining software and hardware to realize respective value. Through VHSIC hardwaredescription language to design FPGA, cryptography can use hardware to realize chaotic algorithm and software to manage hardware by sending control signal. The experiment has proved that this method can enhance operating efficiency of algorithm and strengthen security of cryptography.

Key words: encryption; chaotic sequence; FPGA; VHDL

(编辑 张 苹)