一类序列与分组混合密码可重构处理结构设计①

Design of Reconfigurable Processing Architecture for a Kind of Hybrid Encryption Based on Both Sequence and Block Ciphers

管子铭[1]　欧阳旦[2]　王志远[3]　张明清[1]

(1.解放军信息工程大学 电子技术学院 河南 郑州 450004; 2.空军电子技术研究所 北京 100195;
3.解放军信息工程大学 信息工程学院 河南 郑州 450002)

摘　要： 本文分析了一类序列密码和分组密码的混合加密体制，并为这类密码设计了一种可重构处理结构。实验表明，该结构最高可工作在100MHZ时钟下，占用资源少，可快速灵活的实现不同的混合密码。

关键词： 序列密码 分组密码 混合密码 可重构处理结构 线性反馈移位寄存器

人类早已步入了信息时代，信息在当今社会扮演着越来越重要的角色，“信息就是效益”，“信息就是财富”这样的观点早已被人们所广泛接受。因此，信息的安全性也越来越受到人们的重视，对信息进行加密成了一个行之有效的方法。

传统的加/解密算法实现主要有软件和硬件两种方法。软件实现是通过对密码算法进行编程，由通用微处理器运行程序来实现，软件实现方法的优点是通用性和灵活性好，缺点是运行速度慢。硬件实现是针对某种密码算法，为其设计专用密码芯片，这样可以实现该密码算法的高速运行，但通用性和可移植性差，即该专用芯片不能实现其它密码算法。可重构计算(Reconfigurable computing)技术可以弥补以上两种密码算法实现方法的缺点，这种计算方式是通过对结构可变的硬件进行指令配置，以适应不同算法的处理。这种计算方式既具有了软件的灵活性，又具备了专用密码芯片的高速性。

本文依据可重构计算思想，讨论了针对一类序列和分组的混合密码的可重构处理结构设计。

1　算法描述

现代密码学中，序列密码(sequence cipher)和分组密码(block cipher)是两类占有重要地位的密码[1]。序列密码又称为流密码，其主要思想是：加密时用一个随机密钥序列与明文序列进行异或得到密文序列，解密时用与加密时相同的随机密钥序列与密文序列进行异或即可恢复明文序列。序列密码的缺点是很难得到完全随机的密钥流。分组密码又称为块密码，其主要思想是：将明文序列按一定长度(例如 64bits)分组，然后对这些明文分组采用相同的密钥和算法进行加密，得到等长的密文分组；解密时用与加密相同的密钥对密文分组进行解密运算得到明文分组。分组密码的安全性主要依赖于密钥，而不依赖于对加密算法和解密算法的保密。分组密码的缺点是相同的明文分组用相同的密钥加密会得到相同的密文分组，这为选择明文攻击留下了漏洞。

为了最大限度地克服序列密码和分组密码各自的缺点，文献[2]提出了一类由序列密码和分组密码混合的密码。该类密码的总体结构如图 1 所示，其工作流程为：n 阶线性反馈移位寄存器(LFSR)通过给定的初始值和反馈函数 f(x)得到伪随机序列，将其按一定长度分组，作为分组密码的轮密钥输入，分组密码对明文加密后生成密文；解密时，需将加密过程中使用的每一组轮密钥反序使用，其它步骤与加密过程相同。其中 LFSR 由 GF(2p)上的 n 级移位寄存器和 P 个线性反馈函数组成，其中 P 可以取 1，2，4，8，16，32 等。

① 收稿时间:2008-09-05

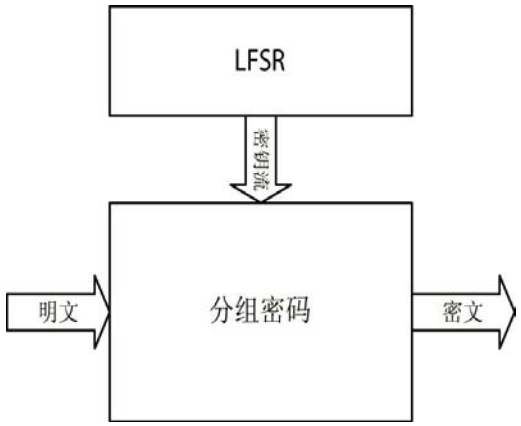

图 1　序列与分组混合密码算法结构

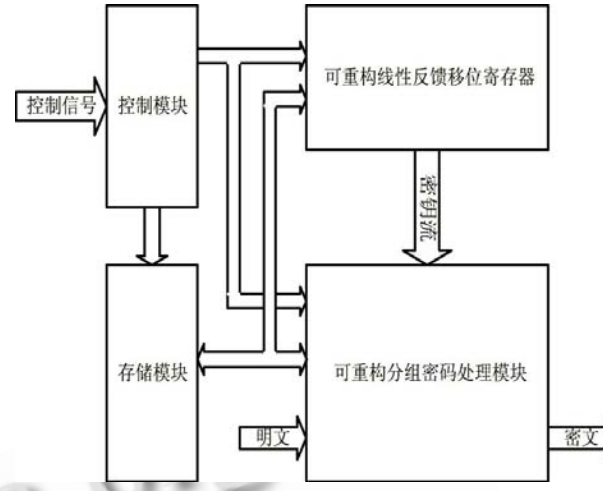

图 2　可重构密码处理结构整体架构

此类混合密码算法一定程度上弥补了序列密码和分组密码安全性的不足，这是因为此类密码算法每个分组加/解密的密钥是不同的，即对于相同的输入分组，加/解密后的输出分组不同。

2　可重构处理结构设计

2.1 总体结构

通过对序列与分组混合密码算法的分析可以看出，线性反馈移位寄存器和分组密码处理部分为可重构的部件，所以此类密码的可重构处理结构(RPA：Reconfigurable Processing Architecture)由控制模块，存储模块，可重构线性反馈移位寄存器和可重构分组密码处理模块四部分组成[3]，如图 2 所示。控制模块接收主处理器送来的控制指令和配置指令，对配置指令进行译码后将配置数据存入存储模块，并根据控制指令控制可重构处理模块的运行；存储模块用来对加解密算法中的密钥、常数以及运算数据进行存储；可重构处理模块在控制模块的控制下，从存储模块读取相应的配置数据进行配置，完成相应的加/解密运算。

RPA 工作时，控制模块控制输入数据进入存储模块中，然后读出数据输入到可重构线性反馈移位寄存器和可重构分组密码处理模块中进行运算。在运算加/解密算法前，控制模块根据配置指令对可重构部分进行重构；算法执行时，控制模块根据算法的要求对可重构部分注入部分配置信息进行动态重构，可构成完整的算法硬件电路。

该结构设计采用粗粒度系统，线性阵列结构互连网络和基于多配置文件的动态可重构处理结构[4]，可根据需求进行配置，便可得到不同形式的可重构密码处理结构。粗粒度的处理结构更能匹配分组密码算法的处理，采用粗粒度的单元将避免大量布线及较低的布线效率等问题，减小配置存储容量，减轻结构的配置压力；线性阵列结构主要针对流水线应用，在此结构中，相邻可重构处理单元被连接为一个或多个线性阵列，线性阵列结构中的每个功能处理单元都可以作为流水线的一级；在多配置文件系统中，重构的过程可以和运算执行同时或交叉进行，即同时有多个配置文件驻留在可重构处理单元内，这使得可以通过切换配置文件的方法很方便地实现不同的功能，而不必从外部重新装载配置文件，这种配置策略能够很大程度上减少新系统重构的时间，增强了可重构系统的性能。

2.2 线性反馈移位寄存器设计

线性反馈移位寄存器(LFSR)是序列密码的重要组成部分，用于产生伪随机密钥流。本文设计的 LFSR 结构如图 3 所示。其主要由 64 个基本可重构单元 RE(Reconfigurable Element)，一个互连网络，一个整体反馈值寄存器 WFVR 组成。

工作时，先根据控制模块发送的 8 比特外部配置数据信号对各 RE 和互连网络进行配置，配置后即构成指定域和指定长度的 LFSR。所有 RE 的内部结构相同，重构粒度均为 8 比特，通过配置每个 RE 构成指定的寄存器并产生部分反馈值。整体反馈值寄存器 WFVR 寄存各 RE 输出的部分反馈值按位异或后的值，WFVR 的值将反馈给指定的 LFSR 的最后一级。互连网络根据配置数据信号中的 LFSR 域值等各种信息，将各 RE

及 WFVR 进行连接，生成需要的结构。

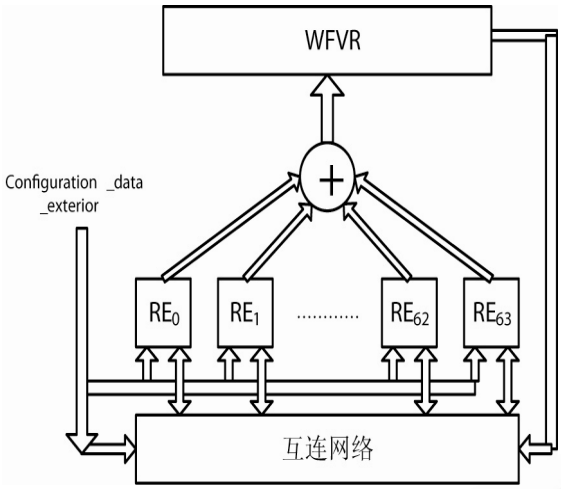

图 3　可重构线性反馈移位寄存器

该可重构 LFSR 最高可工作在 GF(232)域上，此时其反馈值是 32 比特宽，而每个 RE 均可能与此反馈值有关，即每个 RE 需要产生 32 比特的部分反馈值。所有 RE 的部分反馈值按位异或后即得到整体反馈值。

2.3 分组密码处理结构设计

目前分组密码所采用的整体结构可分为 Feistel 网络结构(例如 DES，CAST—256、DEAL、DFC、E2 等)、SP(Substitution-Permutation)网络结构(例如 AES,Safer+、Serpent 等)及其他密码结构(例如 Frog 和 HPC)。加解密相似是 Feistel 型密码的一个实现优点，但它在密码的扩散似乎有些慢，例如需要两轮才能改变输入的每一个比特。SP 结构每轮改变整个数据分组，Feistel 密码每轮只改变输入分组的一半。SP 的网络结构非常清晰，S 一般被称为混淆层，主要起混淆作用。P 一般被称为扩散层，主要起扩散作用。在明确 S 和 P 的某些密码指标后，设计者能估计 SP 型密码抵抗差分密码分析和线性密码分析的能力。SP 网络和 Feistel 网络相比，可以得到更快速的扩散。其实，SP 密码是 Feistel 密码的推广，也就是说 Feistel 密码是一类特殊的 SP 结构，因此在此类混合密码中的分组密码部分采用 SP 网络结构。

可重构分组密码处理模块由可重构处理单元(RPU：Reconfigurable Processing Unit)和互连网络组成，RPU 在控制模块的控制下完成各种加/解密运算[5,6]。其中 RPU 包括：基本逻辑运算电路、移位运算电路、S-盒替代电路、P 置换运算电路、模加 / 减法运算电路、模乘法运算电路等。

在可重构分组密码处理模块中，互连网络接收配置数据对各 RPU 和互连网络进行重构，生成相应的处理结构，同时将线性反馈移位寄存器生成的密钥流进行分组，作为分组密码部分的轮密钥输入，并且每一分组使用不同的密钥加密。根据分组密码运算的特点，可重构处理单元 RPU 处理的数据位宽设为 32 比特适合大多数分组密码算法的要求，每一轮由 4 个 RPU 组成，相应的 RPU 中各可重构运算电路的处理位宽也是 32 比特，可支持多种位宽的处理操作。RPU 内部的可重构处理电路的连接方式可分为并行连接、串行连接和串并混合连接。

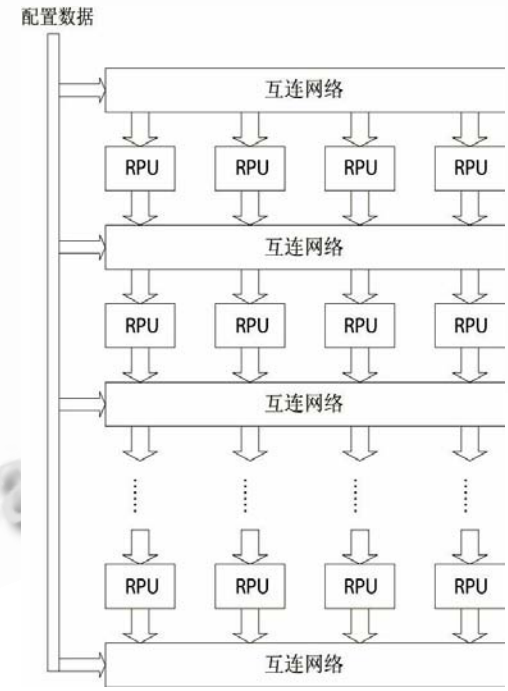

图 4　可重构分组密码处理模块

3　性能分析

以分组密码采用分组和密钥长度均为 128bits 的 Rijndael 算法为例，选取 LFSR 的部分输出作为分组密码的密钥输入，加/解密一个分组需要 29 个时钟周期，线性反馈移位寄存器产生伪随机序列需要一个时

(下转第 69 页)

(上接第 48 页)

钟周期，按照主频为 100MHZ 的情况估算，可重构处理结构的处理速度为 426.7Mbit/s，与 CPU 为 Pentium4 2.40GHz 的通用处理器相比性能提高了 3.2~43.6 倍，与专用密码芯片相比性能提高了 1.7~2.3 倍。结果表明，该结构所需的资源较少，能够快速灵活的实现各种序列和分组混生密码，有效地提高了加/解密的处理速度。

4 小结

本文在分析了通用微处理器和专用密码芯片的优缺点的基础上，利用可重构计算技术针对一类序列与分组混合密码算法设计了一种可重构密码处理结构，该结构能够为此类密码算法提供与之相匹配的硬件结构，从而可以灵活、快速地实现多种此类密码算法，有效的解决了资源受限的问题。另外，利用可重构技术设计密码处理结构，只在密码算法运行时才配置为相应电路结构，不运行时芯片中不含具体算法的电路结构，提高了安全性。可重构密码处理结构可作为信息安全系统的重要部分而被广泛的应用，随着可重构计算技术的不断发展，它将在更广的领域发挥重要的作用。

参考文献

1 陈鲁生,沈世镒.现代密码学.北京:科学出版社,2003.

2 杜奕智,琚耀,吴伟.序列密码和分组密码的混合加密体制研究.合肥工业大学学报, 2005,(6).

3 曲英杰.可重构密码协处理器的组成与结构.计算机工程与应用, 2003,(23).

4 杨博涵.针对多媒体图像处理的可重构处理元设计.西安:西北工业大学, 2005.

5 Yukio MITSUYAMAt. A Dynamically Reconfigurable Hardware-Based Cipher Chip. IEEE, 2001:11－12.

6 Seth Copen Goldstein. PipeRench: A Reconfigurable Architecture and Compiler.IEEE Computer,2000:70－77.