一种改进的分组密码可重构处理结构设计①

褚有睿[1]　欧阳旦[2]　王志远[2]

(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 100089)

摘　要： 应用于密码运算的粗粒度可重构处理结构,以其高性能和较好的灵活性而受到广泛研究。在密码可重构处理结构中,结构合理的配置电路对于提高整个电路的配置速度，加速密码运算非常重要,因此在已有的一种分组密码可重构处理结构的基础上对其配置电路进行改进。从而可以大大提高结构规整的分组密码算法的配置速度。

关键词： 分组密码；可重构；处理结构；配置电路

Design of An Improved Block Cipher Reconfigurable Architecture

CHU You-Rui, OU YANG Dan, WANG Zhi-Yuan (1.Information Engineering University of PLA, Zhengzhou 450004, China；2.The electronic technology graduate school of Air Force, Beijing 100089, China)

Abstract: Coarse-Grained Reconfigurable Architecture aimed at cryptographic processing has been widely studied because of its good performance and flexibility. In a cipher reconfigurable processing architecture, a configuration circuit that has heigh efficiency can greatly reduce the configuration time and accelerate the accounting. In this paper, we improve the configuration circuit of a block cipher reconfigurable processing architecture and speed up the configuration of the block ciphers that have regular structure.

Keywords: block cipher; reconfigurable; processing architecture; configuration circuit

1　概述

采用可重构计算技术来设计密码处理系统既可以满足密码处理对性能和灵活性的需求，又可以有效提高密码处理系统的安全性，在军事及政府部门有着广泛的应用前景。近年来可重构计算领域研究成果主要有 PipeRench，Morphosys，RapiD，COBRA，国防科技大学的 RHCA，及北京科技大学的 RELOG—DIGG。

论文[1-3]提出了一种新的分组密码可重构处理结构 RCPA(Reconfigurable Cipher processing Architecture)。该结构的设计结合了分组密码的一般结构和可重构处理结构设计方法,具有广泛的适应性和代表性。因此本文以该结构为基础对其配置电路进行了改进,提出一种改进的分组密码可重构处理结构。

2　RCPA分组密码可重构处理结构简介

RCPA 结构如图 1 所示，该结构包括可重构密码处理单元模块 RCU(Reconfigurable Cipher processing Unit)、互连模块 ICM(Inter-Connection Module)、存储模块 MAM(Memory Access Module)以及配置控制模块 CCM(Configuration Control Module)，其设计特点是粗粒度、类 VLIW/EPIC 计算结构、动态与静态配置相结合，交换网络设计采用 Crossbar 和线性阵列混合型互连网络。

RCPA 中各模块功能如下：配置控制模块 CCM 主要控制完成内部各个模块的配置操作，内部各模块之间的数据传递以及与外部的数据交互；互连模块 ICM 主要完成 RCU 之间的数据交互操作以及存储模块与

① 收稿时间:2009-11-18;收到修改稿时间:2010-01-18

RCU 之间的互连；存储模块 MAM 用来对加解密算法中的密钥、常数以及运算中的临时数据进行存储；可重构密码处理单元 RCU 负责数据的运算处理。其中每个 RCU 包括基本逻辑运算单元，比特置换单元，S 盒代替单元等六种分组密码常用的运算单元。

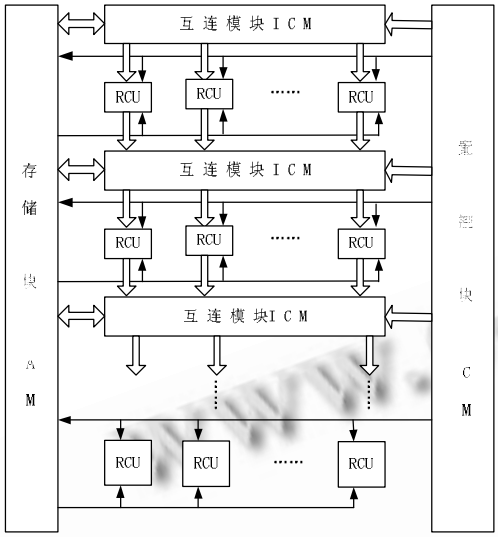

图 1　可重构密码处理结构 RCPA 架构图

在此结构中，外部输入数据在 CCM 控制下进入到存储模块 MAM，然后再将其读出输入到互连模块 ICM 以及可重构密码处理单元 RCU 中进行运算。各级 RCU 的输入来自 ICM 和 MAM，输出则写入 MAM 或直接进入下一级 ICM。

图 1 中每个 RCU 的内部以及互联模块 ICM 中都设置有独立的专用配置寄存器，该寄存器中的内容决定着 RCU 的功能及 ICM 的互连形式。在执行算法前，CCM 需要对 RCU 和 ICM 进行静态重构，将配置信息注入到各个 RCU 以及互联模块 ICM 内的专用寄存器中。当需要执行某个配置时， CCM 动态的产生相应的配置地址信号选择所需的配置文件即可。如果专用配置寄存器不能够容纳一个应用中的所有配置字，就必须中断算法的执行，再去从 CCM 中去取配置字。

3　改进的RCPA结构设计

3.1 RCPA 配置效率分析

由于分组密码算法具有并行性、规则性及若干轮叠代的特性,因此将结构规整的分组密码算法映射到 RCPA 上时会出现大量专用寄存器冗余的现象，致使算法占用资源较多,同时频繁读取配置字，功耗较大。

以 DES 算法[4]配置过程中的 S 盒查表信息为例[5]：在十六轮完全展开的 DES 结构中，每轮都要进行 8 个 6*4 的查表操作,虽然每轮并行的 8 个 S 盒内容不同，但各轮之间的 S 盒内容完全相同，也就是说同一列的 S 盒完全相同。在配置中却需要对相同的 S 盒重复配置 16 次，这造成了多次读取 CCM，同时算法占用面积较大。再以互连网络为例：DES 算法 16 轮迭代中的 P 盒置换完全相同，但在配置时也必须对其进行重复配置，这耗费了 ICM 中大量的配置寄存器，造成资源的浪费。

3.2 基于新型配置电路的改进 RCPA 结构设计

基于以上分析本文提出了一种可用于 RCPA 的新型配置寄存器设置结构—混合型寄存器设置，即在专用寄存器的基础上增加通用寄存器来达到高效快速配置的目的。采用混合型配置寄存器设置的分组密码可重构处理结构如图 2 所示[6]。

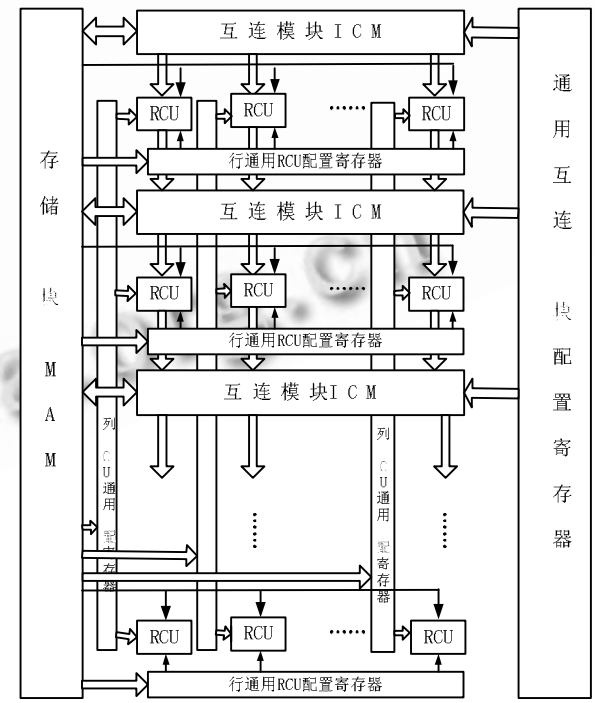

图 2　改进的 RCPA 结构

本文在图 1 的基础上为每行 RCU 增加了一个行通用 RCU 配置寄存器 RGPRCUCR(Row General Purpose RCU Configuration Register),为每列的 RCU 增加一个列通用 RCU 配置寄存器 CGPRCUCR

(Column General Purpose RCU Configuration Register)。以行通用 RCU 配置寄存器为例，当每行中各个 RCU 中的配置数据完全相同时，在对该行的 RCU 进行配置时，从配置控制模块 CCM 中读取的配置数据就不用在每个 RCU 中重复加载，而只需加载在此行的 RGPRCUCR 即可。该行通用 RCU 配置寄存器结构和 RCU 内部的专用寄存器结构完全相同，唯一的区别在于本行的所有 RCU 可同时对该行通用 RCU 配置寄存器进行读取操作。

同时为所有的 ICM 增加了一个通用互连模块配置寄存器 GPICMCR(General Purpose ICM Configuration Register)用来存储通用互连模块的配置信息。该模块和所有的互连模块相联，即所有 ICM 都可对其进行读取。在对整个可重构处理结构进行配置时，选取 CCM 中不同的 ICM 配置信息中使用频率最高的四种直接加载到该模块中，在每个 ICM 中的专用寄存器中只加载与这四种配置文件不同的配置信息。

在互连模块的实现上，文采用了文献[7]提出的基于 BENES 交换网络实现比特置换的设计方法。该设计共需 2Nlog2N-N 个 2 选 1 数据选择器，是目前已知的最有效的设计方式。互连模块整体电路结构如图 3 所示，主要由比特置换网络和静态配置寄存器堆组成。

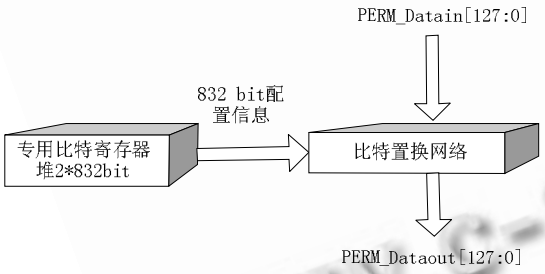

图 3　比特置换单元内部结构图

在该设计中专用配置寄存器堆对配置信息进行存储，并完成对比特置换网络的配置。该电路能实现 128bit 位宽的任意置换，用户可根据需要对该项网络进行配置，实现所需要的置换。每个置换网络的实现需要 832 比特的配置信息，根据对常用分组密码算法使用频率的分析，本设计为每个专用配置寄存器设置了 2 组 832 比特的寄存器堆，为通用互连模块配置寄存器设置了 4 组 832 比特的配置寄存器堆，因此每个 ICM 最多拥有 6 组配置信息。由于每 832bit 配置信息可以实现对 4 个 32*32 置换，或是 2 个 64*64 置换，或是 1 个 128*128 置换，这保证了每个 ICM 最多可实现 24 个 32*32 置换，或是 12 个 64*64 置换，或是 6 个 128*128 置换。该设计极大的扩展了 ICM 置换的范围，同时保证了在其功能扩展的情况下占用面积没有显著的增加。

3.3 改进的 RCPA 上典型算法配置分析

下面以典型的 Feistel 结构密码算法 DES 为例在改进的分组密码可重构处理结构上进行配置，本文的设计中采用了 128bit 全流水结构[8]。由于 DES 算法是 64bit 的明/密文，所以该结构可以同时并行处理两个分组。128bit 明/密文先进入第一级 ICM 互连模块，进行了 2 个分组的 64bit 初始置换，然后将第一级 RCU 旁路；将置换后的数据输入至第二级 ICM 互连模块用来完成 32bit 到 48bit 的 E 盒扩展，然后第二级 RCU 将完成与密钥的异或及 S 盒代替运算；最后第三级 ICM 执行 P 盒置换，第三级 RCU 完成异或运算。这样第二三两级 ICM 和 RCU 完成了 DES 算法中完整的一轮运算。接下来第四级 ICM 和第四级 RCU 分别对应完成和第二级 ICM 和第二级 RCU 相同的功能，第五级 ICM 和 RCU 分别对应完成和第三级 ICM 和 RCU 相同的功能，即第四五两级 ICM 和 RCU 完成 DES 算法的第二轮运算。如此循环反复直到第 32 级和第 33 级完成最后一轮运算。在 DES 算法 16 轮运算之后再利用第 34 级 ICM 完成最后的末置换，便完整的运行了 DES 算法。分析可知从第 2 级到第 32 级中所有的偶数级中的 ICM 都完成相同的功能—E 盒扩展，RCU 完成相同的运算—异或和 S 盒代替；所有奇数级中的 ICM 都完成相同的运算—P 盒置换，RCU 完成相同的运算—异或。

此时在配置时从 CCM 中读取两组配置数据到 RGPICMCR 中，扩展置换配置数据和 P 盒置换配置数据分别有不同的寄存地址，分别为 RAddress1，RAddress2。算法在执行时 CCM 为所有的偶数行 ICM 选择 RAddress1，为所有的奇数行 ICM 选择 RAddress2，则所有的偶数行 ICM 执行扩展置换，所有的奇数行 ICM 执行 P 盒置换。

在 DES 算法中，由于并行执行的 8 个 6*4S 盒不相同，因此不能使用行通用 RCU 配置寄存器 RGPRCUCR 对其进行配置。但 DES 算法的各轮之间的运算步骤完全相同，因此我们可以对列通用 RCU 配

置寄存器 CGPRCUCR 进行配置。假设异或后 S 盒运算和异或运算的配置数据地址为 CAddress1,CAddress2。则在执行算法时，所有偶数行 RCU 选择 CAddress1，即执行异或后 S 盒；所有奇数行 RCU 选择 CAddress2，即执行异或运算，至此 DES 算法配置完成。

在对 RCU 进行配置时，具体是采用行通用配置寄存器还是列通用配置寄存器取决于具体的算法：若每行 RCU 功能相同，但各行之间的 RCU 功能不同，则可对行通用配置寄存器进行配置；若每列 RCU 功能相同，但各列之间 RCU 功能不同，则需对列通用配置寄存器进行配置。如在 Serpent 算法中，就只能对 RGPRCUCR 进行配置，因为该算法第 1 轮到第 8 轮使用不同的 S 盒。在 AES 算法中，每行，每列 RCU 功能完全相同，因此既可对 RGPRCUCR 进行配置，也可对 CGPRCUCR 配置。

以上针对 DES 算法的全流水结构映射做了一些分析和讨论。非全流水的情况一般是由于面积受限才采用的，在此情况下增加通用配置寄存器会显著的增加算法所占用的资源，同时对性能的提高也不是很明显。因此在算法只展开很少的轮数时建议不采用增加通用配置寄存器的设计。

4 结论

本文在分析研究一种分组密码可重构处理结构 RCPA 结构设计和配置原理的基础上对其进行改进，提出了改进的 RCPA 结构。该结构可快速高效的完成多种常用分组密码算法的配置，并有效减小配置电路面积，降低配置功耗，具有较强的实用价值。

参考文献

1 杨晓辉，面向分组密码处理的可重构设计技术研究[硕士学位论文]. 郑州:解放军信息工程大学, 2007.

2 于学荣,并行分组密码处理结构研究及指令系统设计[硕士学位论文].郑州:解放军信息工程大学, 2007.

3 向楠,比特置换网络及其在密码处理器中的应用研究[硕士学位论文].郑州:解放军信息工程大学, 2007.

4 施奈尔,吴世忠等译.应用密码学:协议、算法与 C 源程序.北京:机械工业出版社, 2001.189－194.

5 冯登国，裴定一.密码学导引.北京:科学出版社, 2001. 107－110.

6 Kim Y, Park I, Choi K, Paek Y. Power-Conscious Configuration Cache Structure and Code Mapping for Coarse-Grained Reconfigurable Architecture. 4ISL PED506,Tegernsee,6German. 2006.24－29

7 向楠,戴紫彬,徐劲松.一种基于BENES网络的可重构比特置换系统设计.计算机工程, 2007,22:178－180.

8 Lambrechts A, Raghavan P, Jayapala M, “Energy-Aware Interconnect-Exploration of coarsegrained2 reconfigurable5processors. 8in5Processing of Workshop on Application Specific Processors, 2005.