一种基于流处理框架的可重构分簇式分组密码处理结构模型

陈　韬*　　罗兴国　　李校南　　李　伟
(解放军信息工程大学　郑州　450001)

摘　要：可重构密码处理结构是一种面向信息安全处理的新型体系结构，但具有吞吐量和利用率不足的问题。该文提出一种基于流处理框架的阵列结构可重构分组密码处理模型(Stream based Reconfigurable Clustered block Cipher Processing Array, S-RCCPA)。针对分组密码算法特点，采用粗粒度可重构功能单元、基于 Crossbar 的分级互连网络、分布式密钥池存储结构以及静态与动态相结合的重构方式，支持密码处理路径的动态重组，以不同并行度的虚拟流水线执行密码任务。对典型分组密码算法的适配结果表明，在 0.18 μm CMOS 工艺下，依据所适配算法结构的不同，规模为 4×1 的 S-RCCPA 模型的典型分组密码处理性能可达其它架构的 5.28~47.84 倍。

关键词：分组密码；可重构；阵列结构；分级互连；流处理
中图分类号：TP309.7; TN492　　**文献标识码**：A　　**文章编号**：1009-5896(2014)12-3027-08
DOI: 10.3724/SP.J.1146.2014.00023

An Architecture of Stream Based Reconfigurable Clustered Block Cipher Processing Array

Chen Tao　　Luo Xing-guo　　Li Xiao-nan　　Li Wei
(*PLA Information Engineering University*, *Zhengzhou* 450001, *China*)

Abstract: Reconfigurable cipher processing architecture is a newly proposed architecture for security information processing, but it has the shortage of low throughput and low utilization. To solve the problem, this paper proposes the Stream based Reconfigurable Clustered block Cipher Processing Array (S-RCCPA) architecture based on the steam processor architecture. S-RCCPA incorporates coarse-grained reconfigurable function unit, hierarchy Crossbar interconnection network and distributed key storage, and it supports combined static-dynamic reconfiguration and variable virtual pipeline partition. Experiment results show that, for 0.18 μm technology, classical block ciphers can achieve 5.28~47.84 times speedup when mapped to 4×1 S-RCCPA.

Key words: Block cipher; Reconfigurable; Array architecture; Hierarchical interconnection; Stream processing

1　引言

随着人们对信息安全问题的日益关切，以及可重构计算技术在多领域的不断发展，为更好匹配不同应用的灵活性需求，传统的密码处理结构领域出现了一系列可重构结构，其中，基于 FPGA 的细粒度可重构分组密码处理系统[1]，具有丰富的逻辑资源和互连资源，能够以类似 ASIC 的处理性能实现任意一种或几种分组密码算法，具有较高的灵活性和处理性能，但其资源利用率低、配置信息量过大，且不能很好支持运行过程中的动态重构；面向分组密码设计的专用指令处理器[2−4]，如 RCBCP[2], SophSEC[3]等结构中，设计了面向分组密码的专用指令，重点开发分组密码处理的指令级并行性，具有较高的灵活性，但受体系结构的制约，处理器每个时钟周期只能实现一种密码操作，无法有效开发分组密码的流水特性，处理性能有待进一步提升；阵列结构分组密码粗粒度可重构处理[5−10]的典型代表 RCPA[9], RHCA[10]等结构，能够以较大的并行度和流水深度进行密码处理，通常针对分组密码优化设计了处理单元和互连结构，降低了系统的配置复杂度，但现有结构在特定的配置下只能完成一种运算，资源利用率相对较低。

针对上述问题，为解决现有密码可重构处理结构算法针对性差、性能相对不高，以及可重构结构资源利用率低等问题，本文针对分组密码的数据流处理特征[2,5−7,9]，借鉴流处理器模型的框架结构，提出了一种基于流处理架构的密码可重构分簇式处理阵列结构模型 S-RCCPA，分析了典型分组密码算法在 S-RCCPA 上的映射性能，完成了验证原型设计。该结构能够适应绝大部分应用对分组密码算法的密码处理需求，获得密码处理高效性与灵活性的统一。

2014-01-06 收到，2014-05-26 改回
国家 863 计划项目(2009AA012201)和国家自然科学基金(61302107)资助课题
*通信作者：陈韬　chentaoic@aliyun.com

2 可重构密码处理模型的研究与设计

2.1 可重构分组密码处理架构设计

可重构密码处理架构 S-RCCPA 的整体结构如图 1(a)所示，其核心是分组密码可重构分簇式处理阵列，其他组成部分包括完成输入、输出流控制的流控制器、完成 RCCPA 阵列控制的微内核控制器与主机接口、基于 NoC 的可扩展数据网络接口等。

可重构分簇式处理阵列作为 S-RCCPA 的核心模块，由可重构密码处理块(Reconfigurable Cipher processing Block, RCB)、可配置互连模块(Reconfiguration inter-Connection Module, RCM)、存储模块(Memory Access Module, MAM)和配置模块(Configuration Module, CM)等部分共同构成；结构类似二维阵列，在横向和纵向上组织 RCB，同一行上的各 RCB 可以并行执行，但同一行上的 RCB 之间除控制连接外，没有数据交互通路；在列方向上支持流水线操作，第 i 行的 RCB(j)通过 RCM(j)将运算结果传送到第 i+1 行的 RCB(j)中，最后一行 RCB(j)的运算输出可以反馈到第 1 行 RCB(j)的输入上。

S-RCCPA 核心架构采用层次化方式组织其处理单元，以降低互连网络和处理单元的设计复杂性，如图 1(b)所示，每个 RCB 包含 4 个可重构密码处理簇(Reconfigurable Cipher processing Cluster, RCC)；每个 RCC 包含针对分组密码设计的 9 个 32 bit 可重构密码处理单元(Reconfigurable Cipher processing Unit, RCU)，各 RCU 在 RCC 中的组织形式如图 1(c)所示，其中 32 bit 的 RCU 共 7 种：S 盒替代、移位、GF(2^n)上的矩阵乘法、算术乘法、算术模加/减、三输入逻辑运算、二输入逻辑等单元，另外针对分组密码运算中出现的 128 bit 移位和置换操作，专门设置了两个 128 bit 位宽的比特置换和基于比特置换的长移位单元；4 个 RCC 组成的 RCB 可以完成 128 bit 的密码操作，S-RCCPA 架构中同一行的多个 RCB 可以并行处理多个密码分组；对于 128 bit 的置换和移位单元，将其输入、输出分成 4 组 32 bit 信号接入到相邻 4 个 RCC(同一 RCB 所包含的 4 个 RCC)对应的互连网络上，使两个单元在逻辑上为同一 RCB 的 4 个 RCC 所共有。

S-RCCPA 架构采用静态与动态相结合的配置方式，配置模块 CM 用于完成 S-RCCPA 架构的静态配置与动态控制。S-RCCPA 架构中 RCU 的功能配置采用静态重构的方式完成，如：S 盒替代、比特置换、有限域乘法等单元的功能配置，均采用静态重构在 S-RCCPA 架构执行密码处理任务前完成。动态重构采用基于多重上下文的配置机制实现，主要完成 S-RCCPA 架构中互连网络、RCU 功能选择以及数据输入输出的控制。灵活的配置方式使 S-RCCPA 架构能够实时组织密码处理路径、以虚拟流水线的方式完成密码处理任务。

2.2 分级互连结构研究与设计

S-RCCPA 架构中的 RCB 可以满足一个或多个分组的处理需求，RCB 中的每个 RCC 可以满足大多数分组密码中单个子块的处理需求，因此 S-RCCPA 架构中只有同一列的相邻两个 RCB 之间，可以通过 RCM 进行数据交互，不同列的 RCB 之间不存在数据交互通路。结合分组密码子块间数据交互少、子块内密码操作前后连接关系复杂多变的特点，设计了基于 Crossbar 的分级可配置互连结构。

S-RCCPA 架构中 RCM 的连线位宽为 32 bit，本文以同一列上相邻两个 RCB 的连接关系说明 RCM 的结构，第 i 行 RCB(j)中的 4 个 RCC 与第(i+1)行 RCB(j)的 4 个 RCC 之间，采用基于 Crossbar 的分级互连结构进行数据交互，其中第 i 行 RCB(j)中 RCC(k)(k=1,2,3,4)的各 RCU 输出与第(i+1)行 RCB(j)中 RCC(k)的各 RCU 输入之间采用 Level-1 的全 Crossbar 互连，与 RCC(s)(s=1,2,3,4 且 $s \neq k$)的各 RCU 输入之间采用 Level-2 的部分 Crossbar 互连。S-RCCPA 架构中 Level-1 的全 Crossbar 互连结构如图 2 所示，用于实现同一列中第 i 行 RCC(k)与第 i+1 行 RCC(k)中各个 RCU 间的全连接，同时还将上级其它 RCC 的运算结果、本级数据存储器的数据接入到互连网络上，以实现上述数据到本级 RCU 的连接。

第 i+1 行 RCB(j)的 RCC(k)中各 RCU 的数据来源分为 3 类：第 i 行 RCB(j)的 RCC(k)内各 RCU 的运算结果，由于每个 RCC 中包含 9 种类型的 RCU，该类型的输入共有 9 个；第 i 行 RCB(j)的 RCC(s)通过 Level-2 输入的运算结果，该类型的输入共有 6 个；输入数据，主要指从第 i+1 行数据存储器中读取的数据。为方便 RCC 的处理结果输出到数据存储器、子密钥存储器或输出缓冲器中，Level-1 互连结构专门设计了数据输出端口，其数据来源与各 RCU 的数据来源相同，众多的数据来源保证了运算结果输出的灵活性。尤其是在子密钥生成过程中，上述输出结构可以实现外部输入的密码常数、上级 RCC 的运算结果、上级其它 RCC 的处理结果，灵活写入到当前 RCC 所对应的子密钥存储器中，提高了子密钥数据的使用灵活性。Level-1 的全 Crossbar 互连结构，适应了分组密码子块内密码操作前后连接关系复杂多变的特性，满足了密码处理灵活性的需求。

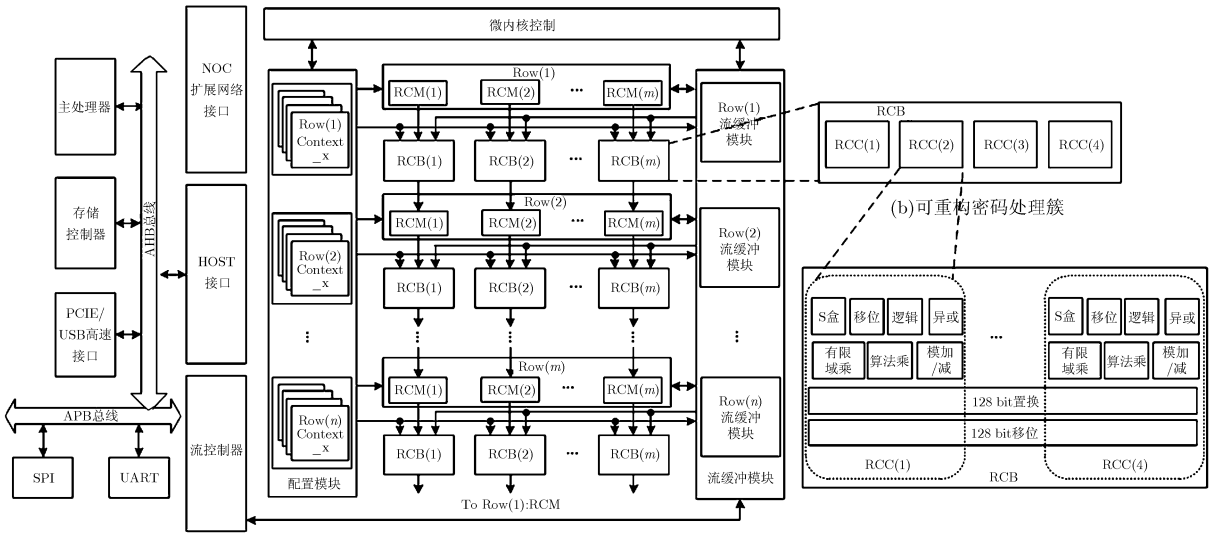

图 1　S-RCCPA 整体结构

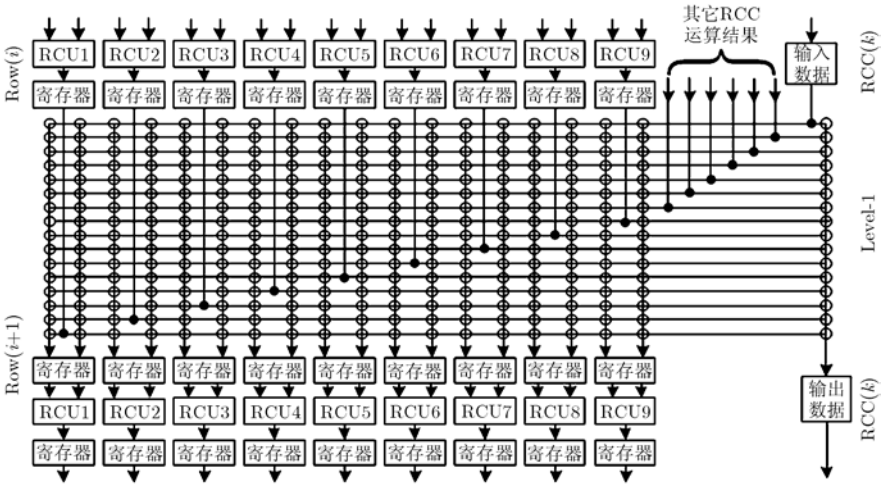

图 2　Level-1 的互连结构

为实现分组密码子块间的数据交互需求，同时结合子块间数据交互较少的特性，在 S-RCCPA 架构中设置了 Level-2 的部分 Crossbar 互连结构。在第 i 行 RCB(j)的 RCC(k)中设置了 6 个输入端口，6 个输出端口，每个端口的位宽为 32 bit，分别用于接收第 $i-1$ 行 RCB(j)中 RCC(s)的运算结果，或将当前 RCC(k)的两路运算结果输出到第 i+1 行 RCB(j)的 RCC(s)中。

每个RCC均采用图3所示的结构将结果输出到下级其它 RCC 中，为保证下一行 RCC 运行时的时序匹配，接入到下级其它 RCC 中的输出数据不再进行寄存。Level-2 部分 Crossbar 互连结构，适应了分组密码子块间数据交互较少的特性，为子块间进行数据通信提供了一定的交互带宽，使每列的 RCB 能够通过子块间的数据交互，灵活组织成 1 个 128 bit, 2 个 64 bit 或 4 个 32 bit 的流水线。

2.3　分离-分布式存储结构设计

为方便临时数据和子密钥数据的灵活存取，针对 S-RCCPA 架构特点，设计了分布式的存储结构，其整体结构如图 4 所示。S-RCCPA 架构为每个 RCB 设置了 4 个数据存储器和 4 个密钥存储器，分别对应 RCB 模块中的 4 个 RCC，每个数据存储器和子密钥存储器均包含 1 个读端口和 1 个写端口。如图 4(a)所示，第 i 行 RCB(j)中的各 RCC 可以通过 Level-1 总线中为各 RCC 设置的输入数据端口，直接读取对应数据存储器的内容。通过 Level-2 的总线可实现 RCC 对其它数据存储器的间接读取。4 个密钥存储器 KDM-A(Key Data Memory A), KDM-B, KDM-C 以及 KDM-D，分别将密钥输出端口接入到 RCC(1), RCC(2), RCC(3), RCC(4)中各 RCU 的密

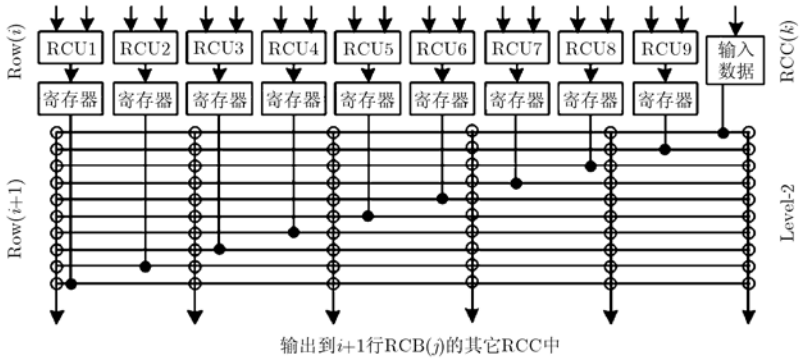

图 3 Level-2 的互连结构

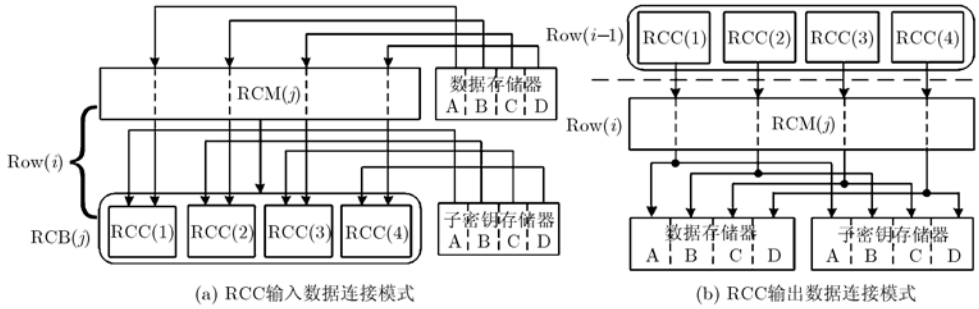

图 4 分离-分布式存储器结构

钥输入端口上，实现了 RCC 从对应子密钥存储器中读取子密钥数据。

如图 4(b)所示，通过 Level-1 总线为各 RCC 设置的输出端口，可以将第 $i-1$ 行 RCB(j)中各 RCC 的运算结果，写入到第 i 行 RCB(j)对应的 4 个数据存储器或子密钥存储器中。通过 Level-2 总线，RCC 可以将运算结果写入到下一行 RCB(j)的其它数据存储器或子密钥存储器中。通过将同一列各数据存储器、子密钥存储器的数据输出端口连接到一个 n 选 1 的选择器上，将选择器的输出接入到各 RCC 的输入端口或子密钥输入端口上，可使得数据存储器与子密钥存储器的读操作更加灵活。

3 S-RCCPA 模型处理模式研究

分组密码具有深度流水特性，非常适合流水执行，可以使用单向流水结构加速密码处理。S-RCCPA 架构具有灵活的互连结构、丰富的密码运算资源，可以充分开发分组密码的流水特性。

3.1 S-RCCPA 模型可变位宽流水处理模式

通过配置 RCM 可以使同一列的 RCB 组成密码处理流水线，加速分组密码任务的处理。分组密码存在分组间以及分组内两个方面的并行性，S-RCCPA 架构可以充分开发分组密码两个方面的并行性，S-RCCPA 架构中的 RCB 可以并行处理同一分组间的多个子块，同一行上的多个 RCB 可以并行处理多个密码分组。

对于分组长度为 128 bit，需要 4 个 RCC 同时参与运算的分组密码算法，如：AES, Twofish, SMS4 等算法，规模为 $n\times1$ 的 S-RCCPA 架构可以将同一列上的 RCB 组织成 1 个 128 bit 的流水线，完成密码分组的处理如图 5 所示，4 个 RCC 中的 RCU 在横向上可以完成 1 个 128 bit 的密码操作，最后一行 RCB 的处理结果可以反馈到第 1 行的 RCB 中。由于每列相邻两个 RCB 之间采用基于 Crossbar 的分级互连结构，提供了较大的互连带宽，虽然只包含 n 行的互连结构和 n 行的处理单元，但是可以提供远大于 $2n$ 级的流水线深度。只要 RCB 的同一 RCC 中用于密码处理的 RCU 不存在冲突、RCM 满足带宽需求，同一时刻可以有多个 RCU 进行密码运算。理想情况下，当分组密码轮函数的 k 步操作均使用不同的 RCU 时，每个 RCC 中 k 个不同类型的 RCU 可以同时工作，结构的资源利用率和流水深度得到有效提高。

对于分组长度为 64 bit，需要 2 个 RCC 同时参与运算的分组密码算法，如：DES, Skipiack, SAFER, LOKI91 等算法，规模为 $n\times1$ 的 S-RCCPA 架构可以将同一列 RCB 中的 RCC 组成 2 个 64 bit 的流水线并行处理；类似地，对于只需要 1 个 RCC 参与运算的分组密码算法，如 GOST 算法，规模为 $n\times1$

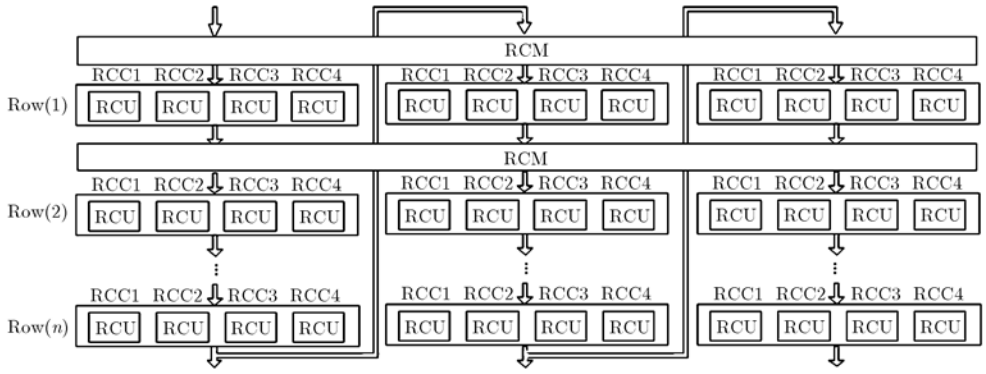

图 5　S-RCCPA 架构 128 bit 位宽的流水处理结构

的 S-RCCPA 架构可以将同一列 RCB 中的 RCC 组成 4 个 32 bit 位宽的密码处理流水线，用于处理相同或不同的密码算法；对于规模为 $n \times m$ 的 S-RCCPA 架构，其流水线的组织形式更加灵活，可以同时组织成若干条 128 bit 位宽，64 bit 位宽以及 32 bit 位宽的流水线，同样即使组织成相同位宽的流水线，流水线完成的密码任务也可以不同。这种灵活的流水线处理结构，使 S-RCCPA 架构能够同时完成多个相同或不同分组密码的处理。

3.2 S-RCCPA 虚拟流水处理模式

若 S-RCCPA 架构规模不能支持以流水方式实现一个轮函数或分组密码时，需要将复杂轮函数或密码算法分多次映射到 S-RCCPA 架构上，从而影响 S-RCCPA 架构的处理性能[11]。为减小或隐藏多次映射带来的配置时间消耗，本文采用动态配置信息自动切换的方式，在有限的硬件资源上实现多级流水，通过将配置消耗隐藏于执行过程中，以充分发挥流水线性能。

为简化动态配置的复杂度，针对每个 RCB 及其对应的 RCM, MAM 设计了动态配置信息存储器，如图 6 所示。系统工作时在微内核控制器的作用下，配置模块 CM 为每个 RCB 选择正确的配置上下文，并进行动态配置信息的译码、缓存，将译码生成的控制信息输入到 S-RCCPA 架构每个处理单元和互连单元的控制端上。每个上下文的有效时间为一个时钟周期，CM 将上下文信息依次从配置信息存储器中读取、译码、激活，实现了处理单元执行密码运算的同时，完成动态配置信息的自动切换。

动态配置信息的自动切换实现了 S-RCCPA 架构计算过程的流水化，通过自动切换不同的配置上下文，实现了 S-RCCPA 架构处理资源的流水线分级和管理，进而实现了分组密码处理任务在 S-RCCPA 架构中的流水化计算，通过在有限的处理资源上“虚拟”出无限硬件资源，有效支持了复杂

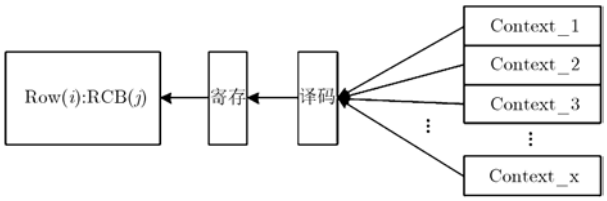

图 6　S-RCCPA 架构配置信息的自动切换

分组密码处理任务，提高了硬件资源的利用率。图 7 描述了 S-RCCPA 架构以 4 级流水线执行多级密码处理任务的操作情况。通过配置信息的自动切换，可以使 S-RCCPA 架构以 4 级流水线虚拟执行具有多级流水的密码处理任务，提高了 S-RCCPA 架构的适应性和单元利用率。

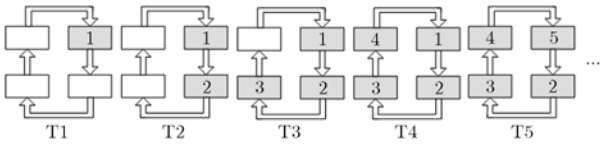

图 7　S-RCCPA 架构 4 级虚拟流水处理结构

4　实现验证与性能分析

本文在 Stratix III 系列型 EP3SL340H1152C3 的 FPGA 上实现了 1×1 规模的 S-RCCPA 架构，实现性能如表 1 所示。

表 1　基于 FPGA 的验证原型实现性能

工作频率	资源占用		
(MHz)	逻辑资源(ALUT)	存储资源(bit)	DSP
57.48	31978	417548	16

为准确评估 S-RCCPA 架构的 ASIC 实现性能，使用 Synopsys 公司的 Design Complier 工具，采用 SMIC 0.18 μm CMOS 工艺标准单元库进行了逻辑综合，综合结果如表 2 所示。

表 2 基于 ASIC 的验证原型实现性能

约束 (ns)	面积 (μm^2)	等效门数 (万门)	Slack	工作频率 (MHz)
4.1	13381704	133.82	0.01	243.9

对以 AES, DES, IDEA, SHA, MD5 为代表的 40 多种公开密码算法[12]的适配结果表明，S-RCCPA 架构可以高效处理构造分组密码的 SP 网络、Feistel 网络及 LM 网络模型。典型的 AES 算法虚拟流水适配流程如图 8 所示。

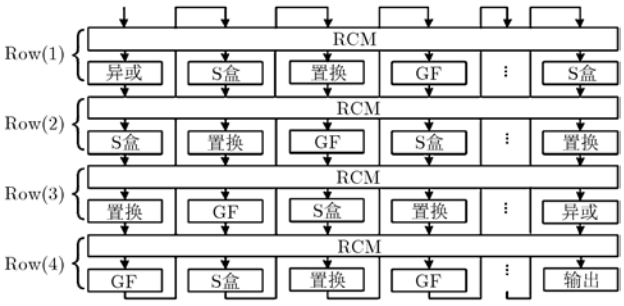

图 8 AES 在 4×1 的 S-RCCPA 架构上的映射

AES-128 算法由 3 部分组成：初始轮密钥加、中间轮变换、末尾轮变换。其中，中间轮变换包括：字节代替、行移位、列混合和密钥加 4 个步骤，共需要循环迭代 9 次；末尾轮变换包含：字节代替、行移位和密钥加 3 个处理步骤。由于 S-RCCPA 架构中每个 RCB 在横向上可以完成 128 bit 的密码操作，因此每行中 m 个 RCB 可以并行处理 m 个 AES-128 算法。AES 算法映射时，轮运算中 4 个 32 bit 的字节代替操作可使用 4 个 S 盒替代单元实现，128 bit 行移位通过 128 bit 的置换单元实现，4 个 32 bit 的列混合和密钥加操作使用 4 个 RCC 中带后异或的 GF(2^n)上矩阵乘法单元实现，S-RCCPA 架构以虚拟流水方式处理 AES 算法时，每个 RCC 中可以有 3 个 RCU 同时工作，由于 RCU 和 RCM 均包含一级寄存器，因此可以形成深度为 24 的虚拟流水线，即 4×1 的 S-RCCPA 架构上能够以流水方式处理 24 个 AES 密码分组。

DES 算法在规模为 4×1 的 S-RCCPA 架构上的映射如图 9 所示。S-RCCPA 架构通过将 DES 算法处理过程流水化，依次映射到 S-RCCPA 架构各行的 RCB 上，考虑到 DES 算法的轮变换虽然只对右半部分 32 bit 数据进行操作，但每轮变换中有多个 48 bit 的运算，共需要 2 个 RCC 并行处理，1 个 RCB 可以在横向上同时处理 2 个 DES 分组，因此，4×1 的 S-RCCPA 架构可以组成两条 64 bit 位宽的流水线，分别以虚拟流水线的方式完成 DES 算法的处理。

为了能够在每条流水线中处理更多的 DES 分组，将初始置换后的数据暂停了一级(通过将数据与“0”异或实现处理暂停)，同时不再将异或操作合并在置换单元中。在流水线 1 中 DES 算法的 64-64 的初始 IP 置换、末尾 IP 逆置换以及轮运算中 32-48 的 E 盒扩展等操作使用 RCC(1), RCC(2)中的比特置换单元完成，轮运算中 48 bit 的密钥加操作使用 RCC(1), RCC(2)的二输入逻辑完成，查找表、P 盒置换、异或等操作分别使用 RCC(1)中的 S 盒查找表、置换以及二输入逻辑完成。S-RCCPA 架构的 RCC 中可以有 2 个 RCU 同时工作，由于 RCU 和 RCM 均包含一级寄存器，因此每条虚拟流水线的深度为 16，即 4×1 的 S-RCCPA 架构中每条流水线能够流水处理 16 个 DES 密码分组，2 条流水线可以同时处理 32 个分组。

基于待处理数据、子密钥分量均已准备好，且不考虑系统配置、数据输入/输出、密钥扩展等时间消耗的这一常用假定，在 1×1 规模配置下，将典型的 AES, DES, IDEA 这 3 种不同结构、不同分组宽度、不同操作位宽的算法在 S-RCCPA 架构上进行

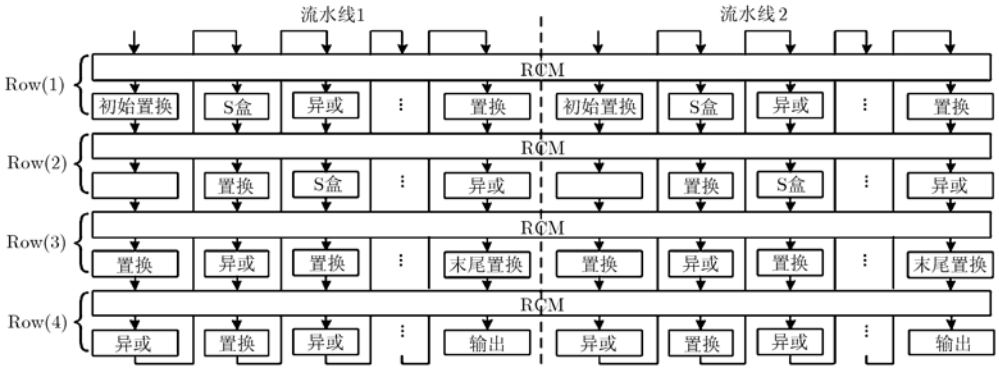

图 9 DES 在 4×1 的 S-RCCPA 架构上的映射

映射实现，与其它几种专用密码处理结构的实现性能进行了比较分析，结果如图 10 所示。其中，RCBCP[2] 是一款可重构分组密码处理器；SophSEC[3]是复旦大学设计的可扩展的密码处理结构；RCPA[9]，RHCA[10]是阵列结构可重构密码处理系统的代表；PipeRench[11]是基于线性阵列结构部分动态可重构系统；Crypto-Maniac[13]采用了一种具有 4 路并行的 VLIW 处理器结构；COBRA[14]是一款专用可重构分组密码处理器；RELOG_DIGG[15]是北京科技大学研制的可重组密码逻辑；Cryptonite[16]采用一种两路并行的 RISC 结构，每一路 RISC 处理器能够处理 64 bit 位宽数据。

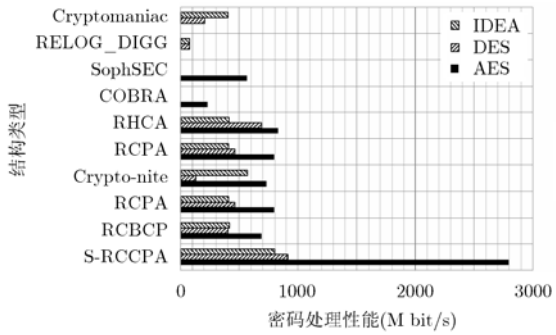

图 10　不同架构上的典型算法实现性能对比

从不同架构上典型算法的性能横向对比图可以看出：由于 AES 算法采用 SP 模型设计，规模为 1×1 的 S-RCCPA 架构能够以深度为 6 的虚拟流水线处理 AES 算法，AES 的密码处理性能可达其它架构的 3.3~12.2 倍；DES 算法采用 Feistel 模型设计，迭代轮数较多，且轮运算中连续使用置换操作，因此 S-RCCPA 架构处理 DES 算法的性能较 AES 低，在 1×1 规模下可以配置成 2 条深度为 4 的虚拟流水线执行，相较其他结构，DES 的处理性能提升约为 1.32~11.96 倍；IDEA 算法采用 LM 模型设计，轮运算中广泛使用异或、模 2^{16} 加和模 $2^{16}+1$ 乘等运算，迭代轮数较少，规模为 1×1 的 S-RCCPA 架构能够组成一条 128 bit 位宽、深度为 6 的虚拟流水线，可以同时处理 12 个 IDEA 分组，性能是其它处理架构的 2.8~21 倍。

若使用 n×1 规模的多簇结构实现 S-RCCPA 架构，基于流处理的框架模型可以高效地将多组明文在流控制器的控制下，流入 S-RCCPA 阵列结构，通过集约的配置文件管理，在不增加 1×1 规模 S-RCCPA 结构配置信息的情况下，AES，DES，IDEA 这 3 类密码算法的实现性能可线性提高到 1×1 规模 S-RCCPA 结构性能的 n 倍，具体如表 3 所示，表中 M 表示 S-RCCPA 架构可同时处理的分组数，N 表示分组长度，CP 表示系统处理 M 个分组所需要的时钟周期数。

表 3　n×1 规模 S-RCCPA 架构的 ASIC 原型性能

密码算法	架构规模	M	N(bit)	CP	性能 (Mbit/s)
AES-128	4×1	24	128	85	8814.8
	2×1	12	128	73	5131.9
	1×1	6	128	67	2795.7
DES	4×1	32	64	181	2759.7
	2×1	16	64	139	1796.7
	1×1	8	64	137	911.5
IDEA	4×1	48	64	135	5550.1
	2×1	28	64	125	3496.6
	1×1	12	64	117	1600.9

在典型的 4×1 规模配置的情况下，S-RCCPA 架构的 ASIC 实现的等效门数为 414.97 万门，较 1×1 规模配置的面积增加约 2.13 倍，具有良好的资源效率和可扩展性。

5　结束语

本文在流处理框架模型下，基于分级的全互连结构构造了一种粗粒度可重构的分组密码处理阵列结构模型，可动态改变粗粒度可重构分组密码处理单元的互连关系，通过分布式的存储结构、静态与动态配置方式的配合，能够以虚拟流水的方式开发可重构阵列的横向与纵向两个方向的并行性，相较于其它结构，在同样的资源情况下大幅提升了分组密码处理性能。对于 AES, DES, IDEA 等经典分组密码算法的适配结果表明，即使规模设定为 1×1, S-RCCPA 架构的处理性能也可达其它典型架构的 1.32~21 倍，具有密码算法结构适应性好，密码处理性能和单元利用率高，结构可扩展能力强的特点。论文存在的主要不足在于控制的复杂度较高，虚拟流水线的加入使得同时参与运算的数据量极大增长，在带来单元利用率增加的同时，使得结构控制的复杂度也相应增加；下一步，拟考虑将分簇式多核密码处理结构与本模型进行有机融合，进一步在密码处理的资源效率、控制效率、配置效率与互连结构效率上寻求应用上的综合平衡。

参 考 文 献

[1]　李可长. 基于 FPGA 可重构快速密码芯片设计[J]. 计算机测量与控制, 2011, 19(7): 1665–1667.
Li Ke-chang. Design of fast reconfigurable cipher chip based on FPGA[J]. *Computer Measurement & Control*, 2011, 19(7): 1665–1667.

[2]　孟涛, 戴紫彬. 分组密码处理器的可重构分簇式架构[J]. 电子

与信息学报, 2009, 31(2): 453–456.
Meng Tao and Dai Zi-bin. Reconfigurable clustered architecture of block cipher processor[J]. *Journal of Electronics & Information Technology*, 2009, 31(2): 453–456.

[3] Huang Wei, Han Jun, and Wang Shuai. A low-complexity heterogeneous multi-core platform for security SoC[C]. IEEE Asian Solid-State Circuits Conference, Beijing, 2010: 1–4.

[4] 宋奂寰, 王树宗, 邵利兵. 基于可重构计算技术的 ASIP 设计与实现[J]. 舰船科学技术, 2012, 34(5): 78–82.
Song Huan-huan, Wang Shu-zong, and Shao Li-bing. Design and realize for ASIP based on reconfigurable computing[J]. *Ship Science and Technology*, 2012, 34(5): 78–82.

[5] 何乃味. 基于模块划分的可重构分组密码芯片设计[J]. 计算机工程与设计, 2012, 33(12): 4536–4540.
He Nai-wei. Design of block cipher algorithm chip based on module division[J]. *Computer Engineering and Design*, 2012, 33(12): 4536–4540.

[6] 何乃味. 分组密码算法的可重构设计模型与结构分析[J]. 河池学院学报, 2012, 32(5): 98–103.
He Nai-wei. Reconstructure design model and structure analysis for block cipher algorithm[J]. *Journal of Hechi University*, 2012, 32(5): 98–103.

[7] 朱敏, 刘雷波, 尹首一. 面向对称密码领域的可重构阵列设计[J]. 微电子学, 2012, 42(6): 815–818.
Zhu Min, Liu Lei-bo, and Yin Shou-yi. Design of reconfigurable architecture for symmetric cipher domain[J]. *Microelectronics*, 2012, 42(6): 815–818.

[8] 李可长. 粒度可配置的密码算法重构单元设计[J]. 计算机测量与控制, 2012, 20(3): 830–835.
Li Ke-chang. Design of reconstructure cells for cryptographic algorithm with configurable granularity[J]. *Computer Measurement & Control*, 2012, 20(3): 830–835.

[9] 杨晓辉, 戴紫彬, 张永福. 可重构分组密码处理结构模型研究与设计[J]. 计算机研究与发展, 2009, 46(6): 962–967.
Yang Xiao-hui, Dai Zi-bin, and Zhang Yong-fu. Research and design of reconfigurable computing targeted at block cipher processing[J]. *Journal of Computer Research and Development*, 2009, 46(6): 962–967.

[10] 姜晶菲. 可重构密码处理结构的研究与设计[D]. [博士论文], 国防科学技术大学, 2004.
Jiang Jing-fei. The research and design of reconfigurable cipher processing architecture[D]. [Ph.D. dissertation], National University of Defense Technology, 2004.

[11] Goldstein S C, Schmit H, and Moe M. PipeRench: a coprocessor for streaming multimedia acceleration[J]. *ACM Sigarch Computer Architecture News*, 1999, 27(2): 28–39.

[12] 戴紫彬. 面向分组密码处理的协处理器体系结构研究与设计实现[D]. [博士论文], 解放军信息工程大学, 2007.
Dai Zi-bin. The research and implementation of the coprocessor architecture for block cipher[D]. [Ph.D. dissertation], PLA Information Engineering University, 2007.

[13] Wu L, Weaver C, and Austin T. Cryptomaniac: a fast flexible architecture for secure communication[C]. The 28th Annual International Symposium on Computer Architecture, G6teborg, Sweden, 2001: 110–119.

[14] Elbirt A J and Paar C. Instruction-level distributed processing for symmetric-key cryptography[J]. *IEEE Transactions on Parallel and Distributed System*, 2005, 16(5): 468–480.

[15] 曲英杰. 可重组密码逻辑的研究与设计[D]. [博士论文], 北京科技大学, 2002.
Qu Ying-jie. The research and design of reconfigurable cryptographic logic[D]. [Ph.D. dissertation], University of Science and Technology Beijing, 2002.

[16] Buchty R. Cryptonite: a programmable crypto processor architecture for high-bandwidth applications[D]. [Ph.D. dissertation], Institut fur Informatik der Technischen Universitat Munchen, 2002.

陈 韬： 男，1979 年生，讲师，研究方向为通信与信息安全专用集成电路设计、专用指令集处理器体系结构设计技术、多属性决策方法.

罗兴国： 男，1951 年生，教授，研究方向为数字通信、移动通信与高效能计算机体系结构.

李校南： 男，1986 年生，工程师，研究方向为信息安全专用集成电路设计.

李 伟： 男，1983 年生，讲师，研究方向为信息安全专用集成电路设计.

一种基于流处理框架的可重构分簇式分组密码处理结构模型

作者： 陈韬， 罗兴国， 李校南， 李伟， Chen Tao， Luo Xing-guo， Li Xiao-nan， Li Wei
作者单位： 解放军信息工程大学 郑州 450001
刊名： 电子与信息学报 ISTIC EI PKU
英文刊名： Journal of Electronics & Information Technology
年，卷(期)： 2014(12)