分组密码处理器的可重构分簇式架构

孟 涛 戴紫彬
(信息工程大学电子技术学院 郑州 450004)

摘 要：该文在研究分组密码算法处理特征的基础上，提出了可重构分簇式分组密码处理器架构。在指令的控制下，数据通路可动态地重构为 4 个 32bit 簇，2 个 64bit 簇和一个 128bit 簇，满足了分组密码算法数据处理所需的灵活性。基于分簇结构，提出了由指令显性地分隔电路结构的低功耗优化技术，采用此技术使得整体功耗降低了 36.1%。设计并实现了 5 级流水线以及运算单元内流水结构，处理 AES/DES/IDEA 算法的速度分别达到了 689.6Mbit/s, 400Mbit/s 和 416.7Mbit/s。

关键词：分组密码算法；分簇式架构；可重构计算；低功耗设计；流水线
中图分类号：TP303 **文献标识码**： A **文章编号**：1009-5896(2009)02-0453-04

Reconfigurable Clustered Architecture of Block Cipher Processor

Meng Tao Dai Zi-bin
(*Institute of Electronic Technology, Information Engineering University, Zhengzhou* 450004, *China*)

Abstract: This paper presents the reconfigurable clustered architecture of block cipher processor. Appointed by instructions, the data-path of this architecture can be dynamically configured to be three modes, which includes 4clusters, 2clusters and single cluster mode. In different mode, different operations can be done, which improves the flexibility of this processor. Basing on clustered architecture, Explicit-decomposition low-power-design method is presented, which can reduce the power by 36.1%. With 5stages pipeline and wave-pipeline, this processor can work in a high rate. And the performances of AES/DES/IDEA reach 689.6Mbit/s, 400Mbit/s, 416.7Mbit/s.

Key words: Block cipher; Clustered architecture; Reconfigurable computing; Low-power-design; Pipeline

1 引言

专用指令集处理器(Application Specific Instruction-Set Processor, ASIP)，针对特定的应用，对指令集和硬件架构进行优化设计，从而得到较高的性价比。分组密码算法的数据处理具有较强的特征，在研究这些特征的基础上，设计了基于 ASIP 的可重构分簇式分组密码处理器(Reconfigurable Clustered Block Cipher Processor, RCBCP)。

多发射和流水线技术提高指令级并行度(Instruction Level Parallelism, ILP)的同时，也给硬件架构带来了较大的负担，如：多端口寄存器堆的访问逻辑、旁路技术[1]的判断及前推逻辑等，这些逻辑会加大路径延迟，反过来影响系统指令级并行度的开发。采用分簇式架构，将整体架构分为可以相对独立执行的簇，减少簇与簇之间各种控制信息和数据的交互，从而可以减小整体电路的复杂度，减小路径延迟。例如：分为两个簇结构的处理器 Alpha21264[2]，仅用有限的前推逻辑，减小了关键路径延迟，提高了系统工作频率。

灵活性的需求，推动了可重构计算技术的快速发展，设计者们提出了各种可重构系统的方案，例如：基于粗粒度的静态可重构系统 RaPiD[3]，基于线性阵列结构部分动态可重构系统 PipeRench[4]。RCBCP 采用了粗粒度的动态可重构技术，在指令的控制下，其数据通路可动态重构为 4 个 32bit 簇(字宽簇)，2 个 64bit 簇和一个 128bit 簇(超字宽簇)。

2 可重构分簇式架构

寄存器堆是处理器的关键部件，基于分析寄存器堆容量、端口数、访问方式与访问速度、面积、功耗之间的关系，Tseng 等提出了支持任意读写的分 BANK 寄存器堆[5]，此结构保留了每个端口可以任意读写的功能，在一定程度上减小了路径延迟；而固定读写的 WSRS[6]的寄存器堆分隔方式，则牺牲了读写的灵活性，较大地减小了路径延迟。

RCBCP 采用了支持相对任意读、固定写的分块寄存器堆，总存储量为 32×32bit，被分为 4 个存储量为 8×32bit 的寄存器子块 RF-A, RF-B, RF-C 以及 RF-D。每个子块有 1 个写端口、2 个读端口的寄存器，每个子块支持任意读写操作，而对于整个寄存器堆，由 Inter Cluster Crass-bar (ICC) 完成相对任意读操作(如图 1 所示)。此结构在保持一定访问灵活性的前提下，有效减小了寄存器堆访问延迟，减小了前推逻辑的复杂度和路径延迟，降低了寄存器堆的功耗。基于此寄存器堆，对数据通路进行了可重构的分簇式设计，在指

2007-09-29 收到，2008-04-07 改回
公安部金盾工程(J1GAB23W013)资助课题

令控制下，可动态重构为字宽簇执行模式或超字宽簇执行模式。

2.1 字宽簇执行模式

当前密码算法流行的分组宽度已达 128bit，而流行的操作位宽是小于或等于 32bit 的，如：基于 SP 网络的 AES，其分组宽度为 128bit，处理时将 128bit 分组数据分为 16 个字节，分别进行 S 盒替代等操作；基于 Feistel 网络的 MARS 算法以 32bit 为操作位宽进行模乘等运算；而基于 LM 算法的 IDEA 算法，则以 16bit 为操作位宽进行运算。因此，为了完成这些小于字宽的操作，在指令的控制下，将宽度为 128bit 的数据通路，分为 4 个 32bit 簇，以完成操作位宽为 32bit 或小于 32bit 的各种运算。在字宽簇结构下，设 4 个簇结构分别为 Cluster1, Cluster2, Cluster3 和 Cluster4，如图 1 所示。

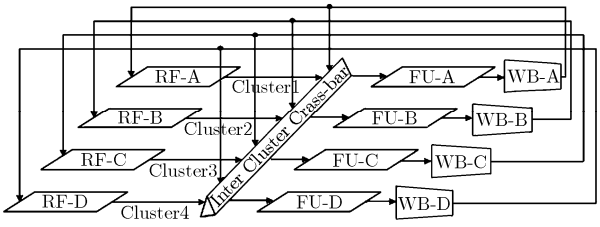

图 1 配置为字宽簇执行模式的数据通路

FU-X(X=A\B\C\D)为 4 个 32bit 功能单元组，每个 FU 内部包括了 6 种不同的运算单元；WB-X (X=A\B\C\D)代表 32bit 回写单元；Inter Cluster Crass-bar 为簇间数据交互与前推逻辑。在此结构下，每个簇中包括独自的寄存器子块(RF)、功能单元组(FU)、回写逻辑 (WB) 以及前推逻辑，数据在单个簇内完成相应的处理，簇与簇之间的数据交互由 ICC 完成，指令译码出回写逻辑的控制信号，控制 WB 选择相应 FU 的结果写回到相应 RF 中。如图 2 所示，给出了字宽簇结构中 Cluster1 的微结构。

ICC 内，首先完成前推数据和本寄存器子块输出的选择，然后完成其它 3 个簇操作数 ClusterX_op_a(X=2\3\4)和本簇操作数 Cluster1_op_a 的选择，以及 ClusterX_op_b (X=2\3\4)和 Cluster1 _op_b 的选择。相对任意读、固定

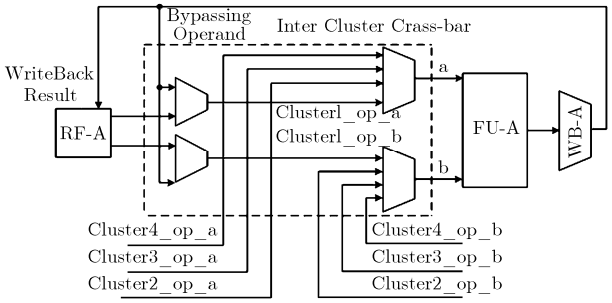

图 2 字宽簇结构中 Cluster1 的微结构

写的访问方式在有效减小访问延迟的同时，保持了在当前指令执行时，任意簇间数据交互的能力。FU 中包括了 SBOX 等 6 个 32bit 的可重构运算单元[7]，可完成 32bit 或小于 32bit 的相应密码运算。

2.2 超字宽簇执行模式

某些专用算法常包括有 128bit 位宽的操作，并且对于某些通用的密码算法，有些操作由 32bit 运算单元完成，其实现效率太低，如 AES 算法中的行移位，由 32bit 位宽的运算单元实现，要用到几十条运算指令，但如果采用 128bit 位宽的 bit 置换单元，则只需要一条指令。因此，设计了 128bit 位宽的运算单元，在执行此类运算时，则需要将数据通路配置为 128bit 的超字宽簇结构，在此工作模式下，128bit 簇设为 Cluster5，其结构如图 3 所示。

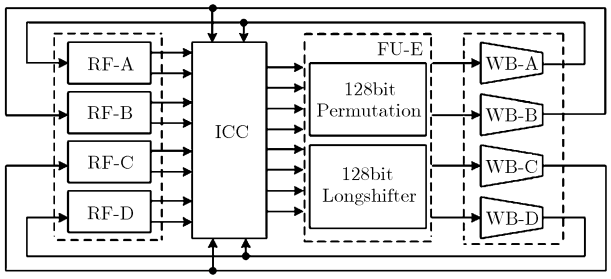

图 3 配置为超字宽簇结构的数据通路

此模式下，ICC，FU-E，4 个寄存器堆和 4 个回写逻辑共同构成了 Cluster5。所有源操作数经 ICC 后都参与了 FU-E 的运算，FU-E 中包括了 128bit 位宽的可重构 bit 置换运算单元[8]和 128bit 位宽的可重构移位运算单元[9]。

然而对于 IDEA 和 DES 等 64bit 分组宽度的算法，其处理过程中还要用到 64bit 位宽的操作，例如：DES 中要用到的 64bit 置换操作，IDEA 中要用到的 64bit 移位操作。因此，对 FU-E 中 128bit 位宽的运算单元进行了可重构设计，在指令控制下可重构为完成两路 64 bit 位宽的 bit 置换和移位运算单元。因此，当指令动态地将 128bit 运算单元重构为 64bit 运算单元的同时，数据通路被重构为两个 64bit 簇结构：Cluster6 和 Cluster7，此工作模式下每个簇可独立地完成 64bit 位宽的置换和移位操作。

3 基于分簇结构的低功耗设计

在 0.18μm 工艺以上，动态功耗占总功耗的 80%左右，研究者们提出了各种技术来减少动态功耗。基于统计分析，对有效工作电路和无效工作电路进行分隔的方法[10−12]，隐性地对译码电路、扩展的数据状态机和输入、输出电路等电路进行分组，减少了电路的无效翻转，有效地减小了动态功耗。基于分簇架构，RCBCP 采用了由指令显性地对译码电路、寄存器堆、功能单元以及回写单元进行分隔，从而减少电路无效翻转的低功耗设计技术。

将所有指令分为 4 个子集，包括 3 个运算指令子集以及 1 个控制指令子集。对应 4 个子集，将所有的译码电路分为 4 个部分，取出指令后，送到相应的部分进行译码，在本条指令执行译码的周期内，其它译码电路则为无效状态。因此，在每个指令译码部分的入口设计一个锁存器，当此部分有效执行时，打开锁存器，送入新的指令，否则，关闭锁存器，保持原值，使此部分译码电路不翻转。由 2.1 节~2.2 节知，数据通路可配置为 7 个簇结构，再加上控制指令执行所需的控制支路，共 8 条支路，当不同指令子集的指令执行时，8 个支路中只有特定的支路参与运算。因此，由指令显性地指定各个支路的是否处于有效工作状态，采用锁存器将无效支路的电路关闭。

当配置为字宽簇执行模式时，4 个指令槽的某个槽内会存在空操作，所以 Cluster1，Cluster2，Cluster3 和 Cluster4 内会存在无效翻转的电路，并且由于每个簇的 FU 内包括多个运算单元，而有效工作的只有一个运算单元，所以 FU 内也会存在无效翻转电路，因此对字宽簇执行模式下的电路结构进行了进一步的低功耗设计，其控制示意如图 4 所示。

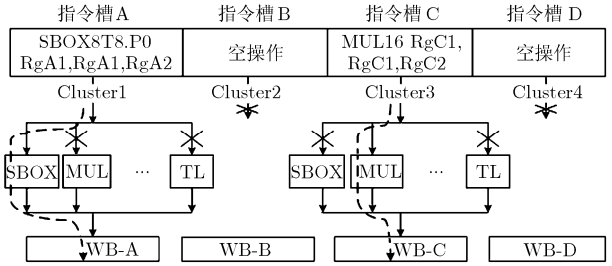

图 4 字宽簇执行模式下低的功耗控制

指令槽 B，D 中为空操作，所以将簇 B，D 的输入锁定在原值，使簇 B，D 中除寄存器堆和 ICC 之外的电路无翻转。指令槽 A 的指令指定要完成 S 盒运算，所以只打开 S 盒运算单元(SBOX)的输入，将功能单元组 FU-A 中的其它运算单元关闭，保持此运算支路内无翻转。同理，簇 C 中只有乘法单元(MUL)为有效工作单元，其它运算单元的输入锁定在原值。整个数据通路上只有两条虚线标识的支路处于有效工作状态，从而有效减小了电路翻转带来的动态功耗。

4　流水线设计及实现

本文设计了 4 种深度的流水线方案：3 级流水线方案 A；4 级流水线方案 B；6 级流水线方案 C，包括 2 级运算单元流水线；8 级流水线方案 D，包括 3 级运算单元流水线。使用 Verilog 硬件描述语言实现了各方案，用 modelsim SE 5.5e 进行了功能仿真，结果正确。使用 Synopsys 公司 Design Complier for Solaris 工具，采用 0.18μm CMOS 工艺库和 RAM 硬核对 RTL 代码进行逻辑综合，最终得各方案的最高工作频率分别为 168MHz，180MHz，312.5MHz 和 370MHz。针对每个方案，适配了 3 种算法 AES，DES，IDEA，其处理性能如表 1 所示。

如表 1 所示，方案 C，D 的处理性能明显高于方案 A，B。由于运算单元的关键路径较长，方案 C，D 中运算单元内部分别设计了 2 级和 3 级流水线。由于 AES，DES 算法中用到了大量被分为 3 级流水线的运算，所以方案 C 处理 AES, DES 的性能高于方案 D；而 IDEA 算法中用到的 3 级运算相对较少，所以方案 D 的处理性能有小幅度的提升。在权衡各方案实现复杂度，以及所需面积、功耗与所得性能增益的关系后，选择了方案 C。

表 1 4 种流水线方案处理 AES，DES，IDEA 算法的性能比较

	3 级流水线	4 级流水线	6 级流水线	8 级流水线
AES	416	447	689.6	642.7
DES	304	326.7	400	377
IDEA	297	319.3	416.7	438

方案 C 的流水段分别为：地址生成(Address Generation, AG)、分支及流水线仲裁(Branch and Pipeline arbitration, BP)、操作数分配(Operand Distribution, OD)、执行(EXecution, EX)和回写(Write Back, WB)，运算单元内部设计了两级流水线 EX1 和 EX2。AG 经过处理 BP 级反馈的地址信息，生成指令存储器的读地址；BP 主要完成分支及流水线的仲裁，以及计数器访问等操作；OD 主要完成操作数的读取及分配；EX1, EX2 共同完成运算操作，WB 将运算结果回写到寄存器。由于分组密码算法处理过程中存在高强度的数据相关，以及高成功率的分支规律性，因此 RCBCP 采用旁路技术和硬件分支预测选中的方法，高效、简单地解决了数据和控制冲突所带来的性能损失。

5　功耗及性能分析

使用 Magma 公司 BlasterCreat/Fusion/Rail 工具，采用 0.18μm CMOS 工艺库，对未加入低功耗设计和加入低功耗设计的 RCBCP 分别进行了分析、综合，最后给出了功耗报告，如表 2 所示。Leakage 为漏电功耗，Internal 为电路的内部功耗，Scap 为动态功耗。由于采用了低功耗设计，动态功耗降低了 37.9%，内部功耗降低了 37.8%，但由于控制逻辑增加，导致电路面积的的增加，使得漏电功耗增加了 12%，但在 0.18μm 工艺下，动态功耗所占比例较大，而漏电功耗所占比例较小，所以总的功耗降低了 36.1%，从而达到了设计的目标。

经算法适配，RCBCP 可处理 SP 网络、Feistel 网络及

表 2 RCBCP 与采用低功耗设计 RCBCP 的功耗比较(mw)

	Leakage	Internal	Scap	Tatal
未采用低功耗设计的 RCBCP	5.8	14	140.3	160.1
采用低功耗设计的 RCBCP	6.5	8.7	87.1	102.3

LM 网络的 AES、DES、IDEA、SHA、Safer+和 twofish 等 30 多种算法，将 AES，DES，IDEA 3 种不同结构、不同分组宽度、不同操作位宽的算法的实现性能，与其它几种专用密码处理器的实现性能进行了比较，比较结果如表 3 所示。

表 3 AES, DES 及 IDEA 算法的实现性能比较(Mbps)

算法	COBRA	Crypto-Maniac	Crypto-nite	RELOG_DIGG	RCBCP
AES	229	511	731	--	689.6
DES	--	204	128	76.2	400
IDEA	--	400	569	76.2	416.7

表 3 中 COBRA [13]是一款专用可重构分组密码处理器。RELOG_DIGG[14]是北京科技大学研制的可重组密码逻辑。Crypto-Maniac[15]采用了一种具有 4 路并行的 VLIW 处理器结构。Crypto-nite[16]采用一种两路并行的 RISC 结构，每一路 RISC 处理器能够处理 64bit 位宽数据。由上算法适配结果以及上表的性能分析可得，RCBCP 可灵活地适配多种算法，并且对于不同结构、不同分组宽度、不同操作位宽的算法均有较高的处理性能。

6 结束语

基于对分组密码、杂凑函数等算法的研究，设计并实现了采用可重构分簇架构的密码处理器，其数据通路动态地重构为 4 个 32bit 簇，2 个 64bit 簇和一个 128bit 簇，满足了分组密码算法数据处理所需的灵活性；基于分簇的架构，提出了由指令显性地分隔电路结构，以降低动态功耗的设计技术；采用 5 级流水线以及运算单元内部流水的结构，提高了系统工作频率，有效提高了 ILP，与其它的密码处理器相比，在灵活性和性能上都具有较大的优势。但此架构中由于采用了结构较复杂的可重构运算单元，其关键路径较大，在一定程度上限制了系统性能，因此，需要采用更合适的硬件实现算法，减小运算单元的关键路径延迟。

参 考 文 献

[1] Abnous A and Bagherzadeh N. Pipelining and bypassing in a VLIW Processor [J]. *IEEE Trans. on Parallel and Distributed Systems*, 1994, 5(6): 658–664.

[2] Kessler R E. The alpha 21264 microprocessor [J]. *IEEE Micro*, 1999, 19(2): 24–36.

[3] Ebeling C, Cronquist D C, and Franklin P. RAPID-Reconfigurable Pipelined Datapath[C]. The 6th International Workshop on Field Programmable Logic and Applications, Darmstadt, Germany, Sep. 23-25, 1996: 126–135.

[4] Goldstein S C, Schmit H, and Budiu M, *et al.*. PipeRench: A reconfigurable architecture and compiler [J]. *Computer*, 2000, 33(4): 70–77.

[5] Tseng J H and Asanovic K. A speculative control scheme for an energy-efficient banked register file [J]. *IEEE Trans. on Computers*, 2005, 54(6): 741–751.

[6] Seznec A, Toullec E, and Rochecouste O. Register write specialization register read specialization: A path to complexity-effective wide-issue superscalar processors [C]. The 35th Annual IEEE/ACM International Symposium on Microarchitecture, Istanbul, Turkey, Nov. 18-22, 2002: 383–394.

[7] 杨晓辉. 面向分组密码处理的可重构设计技术研究[D]. [硕士论文], 解放军信息工程大学, 2007.

[8] 向楠. 比特置换网络及其在密码处理器中的应用研究[D]. [硕士论文], 解放军信息工程大学, 2007.

[9] Yu Xue-rong. Design and implementation of reconfigurable shift unit using FPGAs [C]. The 1st International Symposium on Pervasive Computing and Applications Proceedings. Urumchi, Xingjiang, China, August. 3-5, 2006: 543–545.

[10] Lee Ming Hung, Hwang TingTing, and Huang Shi-yu. Decomposition of extended finite state machine for low power design [C]. The Design, Automation and Test in Europe Conference and Exhibition, Messe Munich, Mar.3-7, 2003: 1152–1153.

[11] Kuo Wu-An, Hwang TingTing, and Wu A C-H. Decomposition of instruction decoder for low power design [C]. The Design, Automation and Test in Europe Conference and Exhibition, CNIT La Defese, Pairs, France, Feb.16-20, 2004, Vol.1: 664–665.

[12] Hu Chi-Wei and Hwang TingTing. Output-pattern directed decomposition for low power design [C]. The Design, Automation and Test in Europe Conference and Exhibition, CNIT La Defese, Pairs, France, Feb.16-20, 2004, vol.5: 137–140.

[13] Elbirt A J. Reconfigurable computing for symmetric-key algorithms [D]. [Doctor thesis], Massachusetts: Electrical and Computer Engineering Department University of Massachusetts Lowell, 2002.

[14] 曲英杰. 可重组密码逻辑的设计原理[D]. [博士论文], 北京科技大学, 2002.

[15] Wu Lisa, Weaver C, and Austin T. CryptoManiac: A fast flexible architecture for secure communication [C]. The 28th Annual International Symposium on Computer Architecture, Goteborg, Sweden, Jun.30–July4, 2001: l10–119.

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

孟 涛： 男，1982年生，硕士生，研究方向为信息安全、体系结构.

戴紫彬： 男，1966年生，硕士生导师，主要研究方向为信息安全、体系结构.