

高速可重构抽取移位单元研究与设计

常忠祥¹, 戴紫彬¹, 李 伟¹, 龚海宁²

(1 解放军信息工程大学, 河南 郑州 450001; 2 61587 部队, 上海 200000)

摘 要: 为了提升密码算法中抽取、移位等位操作的处理效率, 降低抽取和移位实现的硬件资源消耗, 构建了以 iButterfly 网络为基础的高速可重构抽取移位硬件架构, 提出架构所需的路由信息生成算法并进行高速硬件映射。最后对架构进行性能评估, 结果表明, 提出的抽取移位单元具有较高的处理效率和灵活性, 在 CMOS 65 nm 工艺下, 32 比特抽取移位工作频率可达到 2 GHz。

关键词: iButterfly 网络; 路由算法; 抽取移位; 抽取; 移位

中图分类号: TP302.2

文献标识码: A

文章编号: 1000-7180(2015)04-0021-04

Research and Design of High-speed Reconfigurable Extract-shift Unit

CHANG Zhong-xiang¹, DAI Zi-bin¹, LI Wei¹, GONG Hai-ning²

(1 PLA Information Engineering University, Zhengzhou 450001, China;

2 61587 Troops, Shanghai 200000, China)

Abstract: In order to enhance processing efficiency and reduce hardware resource consumption of the extraction replacement and shift replacement in cipher algorithm, a high-speed reconfigurable extraction-shift hardware architecture based on iButterfly is constructed in this paper. At the same time, the generating routing information of framework are put forward, then mapping high-speed hardware is realized. Finally, the results show that the proposed extraction-shift units have high efficiency and flexibility. The number of 32-bit extraction-shift replacement operating frequency is 2 GHz under the CMOS 65 nm.

Key words: iButterfly network; routing algorithm; extract-shift; extract; shift

1 引言

近年来, 密码算法应用场合越来越多, 对抽取操作的速度提出了更高的需求, 传统的移位、异或等基本逻辑操作完成抽取操作的方式已经满足不了高速的需求。针对以上问题, 近期出现了一系列可以加速抽取操作的指令, 有 BFLY^[1]、IBFLY^[2]、CROSS^[3]、OMFLIP^[3-4]、PPERM^[3]、SWPERM^[3,5]、SIEVE^[1,6] 和 GRP^[1,3] 等。

新指令的出现, 提升了抽取操作的实现效率, 其中 BFLY、IBFLY、CROSS、OMFLIP 和 GRP 以互连网络基础, PPERM、SWPERM、SIEVE 以数据选择器为基础, 只有 GRP 指令在实现抽取操作时只需要一条指令且不需要提前计算控制信息。但对密码

算法中的抽取操作来说, 其位宽以 64 bit、128 bit、256 bit 等^[1,7] 为主, 若采用位宽为 32 bit 的基本单元实现, 需要将数据按照位宽 32 bit 进行分组, 进行抽取操作, 然后将分组抽取后的数据进行组合(移位、或), 分组效率很大程度上影响大位宽数据抽取操作的效率。同时, 分组抽取后的数据进行组合所需的移位操作, 可以看作位置变换的一种特殊形式, 但是在实现移位时, 常常需要完全按照比特置换的实现方式来完成, 处理效率低下, 或者设计专门的移位单元, 资源消耗较大。

针对以上问题, 本文提出了抽取移位操作, 一次完成抽取和移位两种操作, 有效提升大位宽抽取操作的实现效率。构建了以 iButterfly (inverse butterfly) 网络为基础的抽取移位硬件架构, 并对整个架

构进行了硬件的高速映射,有效降低实现抽取、移位和抽取移位操作的硬件资源消耗和关键路径延迟。

2 抽取移位操作必要性分析

对 NESSIE 工程、ECRYPT 工程所征集到的 40 种序列密码算法进行了分析发现有近 30 余种算法用到了抽取、移位操作^[2,4,8-9]。以抽取操作为例进行了统计,如表 1 所示。

表 1 密码算法中的抽取操作特征

算法种类	反馈函数		前馈函数	
	位宽/bit	抽取个数	位宽/bit	抽取个数
A5-1	19	4	64	3
	22	2		
	23	4		
ABC	128	96	128	64
DECIM	192	14	192	14
E0	25	4	128	4
	31	4		
	33	4		
	39	4		
Grain-80	160	14	160	12
Grain-128	256	20	256	17
LILI-II	128	66	127	12
	127	61		

从表 1 可以看出,密码算中的抽取操作存在以下特点。(1) 位宽大: 密码算法中的抽取操作位宽以 64 bit、128 bit、192 bit、256 bit 等为主;(2) 分布散: 需要选择出来参与后续运算的变量位置分布范围大;(3) 变量少: 需要选择出来参与后续运算的变量个数较少。

由密码算法中抽取操作的特点可知,将初始序列中的有效数据选择出来,需要将数据进行分组,将各分组中有效数据选择出来,存放在对应位置,最后拼接选择出来的有效数据,完成初始序列中所有有效数据的抽取,如图 1 所示。

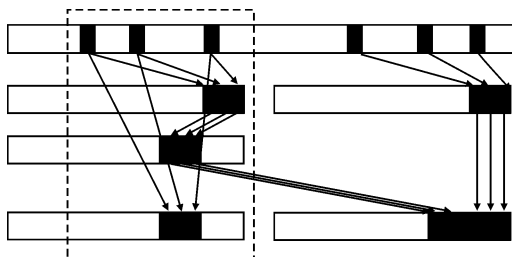


图 1 大位宽数据抽取置换

由图 1 可知,大位宽数据的抽取操作可以分解为抽取(图 2)、移位(图 3)、或三种操作的组合。

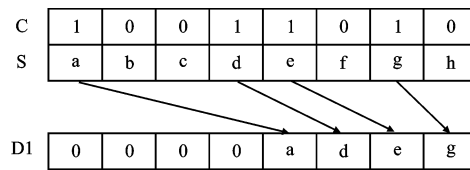


图 2 抽取

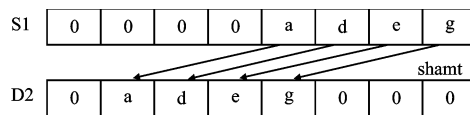


图 3 移位

若存在抽取移位操作(图 4),则可以一次完成抽取移位操作,有效降低数据选择定位的过程,提升大位宽抽取操作的实现效率。同时,可以通过配置抽取及移数的控制信息,分别支持抽取和移位操作。

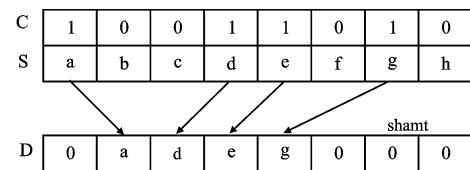


图 4 抽取移位

通过以上分析,抽取移位操作的实现具有较大的研究意义,由文献[4]可知,通过变换路由信息,iButterfly 网络可以支持抽取移位操作,因此,结合密码算中抽取操作的特点,本文构建了基于 iButterfly 网络的抽取移位操作的硬件架构。

如图 5 所示,架构包含路由信息生成电路、iButterfly 网络等,iButterfly 网络可以通过二选一的数据选择器实现,整个架构的处理效率取决于路由信息生成电路的速度,因此对路由信息的生成算法及其高速硬件映射进行了研究和设计。

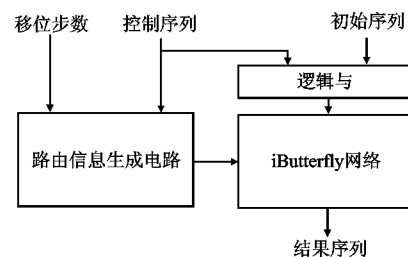


图 5 抽取移位硬件架构

3 路由算法提取

由 iButterfly 网络的互连函数和拓扑结构可知,若采用将路由信息直接配置的方式,则位宽为 n

的 iButterfly 网络需要 $(n \log_2 n)/2$ 比特路由信息,随着位宽的增大,路由信息的量及其需要的硬件资源是不可接受的,因此,需要研究通过外部控制信息生成所有路由信息的方法。

由抽取移位操作的特点可知,其抽取过程中需要专门的控制序列指示需要抽取的数据位置,移位过程中需要专门的移位值指示其移位的步数,因此,提出了由控制序列(C)和移位步数(shamt)共同生成抽取移位置换路由信息的方法。其中 Q 函数如图 6 所示,cnt 函数如图 7 所示。

抽取移位路由信息生成算法

Input: c, shamt
 output: cibly
 1. $\text{pc}[u] = \text{cnt}(c\{n;0\})$
 2. for $i = 1, 2, \dots, \log_2 n$
 3. $\{k = 2^i - 1,$
 4. $\{ \text{for } j = 1, 2, \dots, n/2^i - 1$
 5. $\{m = j * 2^i + k - 1$
 6. $\text{temp}[m] = Q(1^k, (\text{pc}[m] + \text{shamt}(\text{mod } 2^i)))$
 7. $\text{cibly} = \text{temp}[m] \parallel \text{cibly}\}$

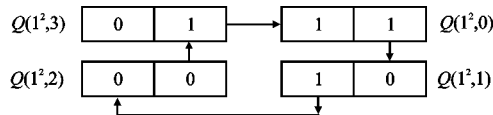


图 6 $Q(1^k, \text{shamt}(\text{mod } 2^i))$
 $(k=2, i=2, \text{shamt}=0, 1, 2, 3)$

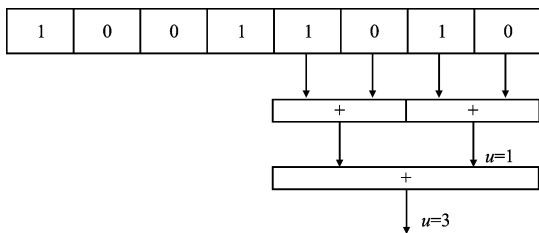


图 7 cnt

由抽取移位路由信息生成算法可知,算法中的 c 序列置为 0,可生成移位所需的路由信息;shamt 为 0,可生成抽取所需的路由信息。通过抽取移位路由信息生成算法和 iButterfly 网络实现抽取移数、抽取、移位功能,能够大幅节省硬件资源消耗。

将抽取移位路由信息生成算法生成的路由信息在 iButterfly 网络映射,如图 8 所示,将需要抽取的数据的控制位置为 1,其余置为 0,数据进入网络前,可以提前将控制序列与源数据序列进行逻辑与运算,完成无关数据的清零操作。

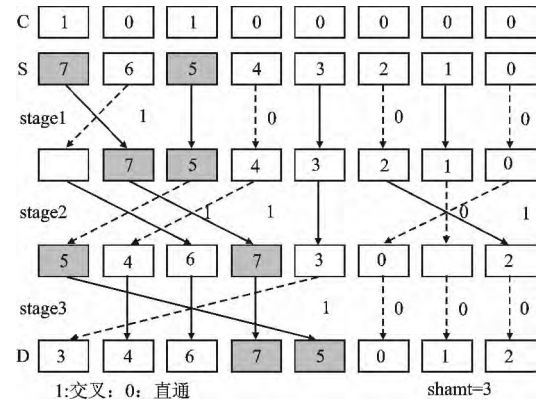


图 8 抽取移位 (8—8)

4 路由算法高速硬件实现

为了保证抽取移位硬件架构的高速实现,对抽取移位路由信息算法的进行高速设计。分析抽取移位路由信息生成算法,可以发现,算法主要包含 cnt 函数和 Q 函数两部分,分别对 cnt 函数和 Q 函数进行高速设计。

cnt 函数为连加运算,且每一位相加的结果都要输出,因此,为了降低 pc 函数中连加电路的延迟,借鉴了超前进位加法器的思想,设计了基于树形加法器的高速连加电路。如图 9 所示。

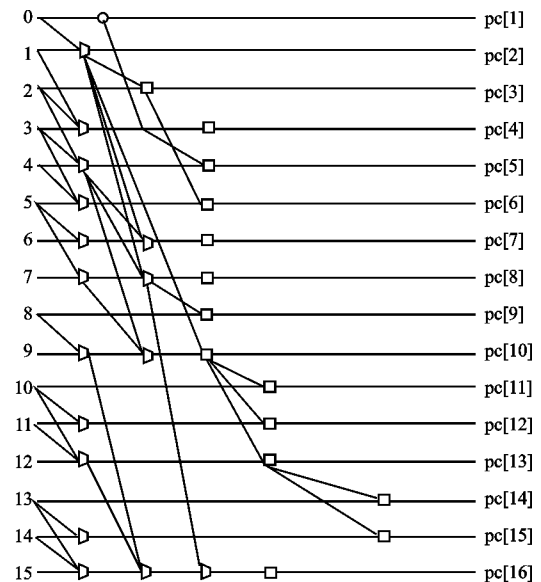


图 9 树形连加电路 (16 bit)

图 9 中梯形符号代表一个全加器,正方形则代表一个进位加和电路,对于不同的级数进位加和电路略有所不同,这是因为只有在 iButterfly 第一级的连加和需要全部输出用于下一阶段的计算,而其他的则只需要低几位的输出即可。因此,在图 6 中的

16 位树形连加电路最后一级的进位加和电路中,对不要参与后续运算的输出比特屏蔽即可。

Q 函数从 cnt 函数中获取要移位的数值,因第 i 级的路由信息分为 $n/2^i$ 组,各组信息独立,且每组信息以 2^i 为周期循环。因此,对应 cnt 函数, i 为 4 时, Q 函数计算可化简为图 10,第一层包含一个非门,第二层包含与非门的延迟,第三层包含异或门的延迟。

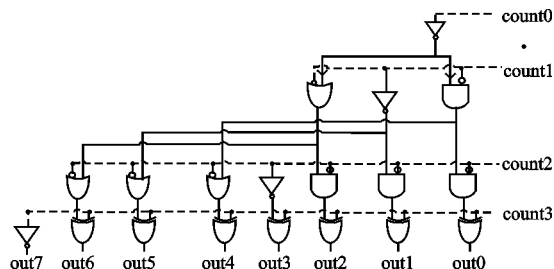


图 10 Q 函数化简

5 性能评估

为了分析本文提出的可重构抽取移位单元,在 CMOS 65 nm 下以 32 比特为例进行了综合,并对密码算法中的大位宽数据进行适配。分别从关键路径、资源占用、数据分组等方面进行了分析。性能分析如图 11 所示。

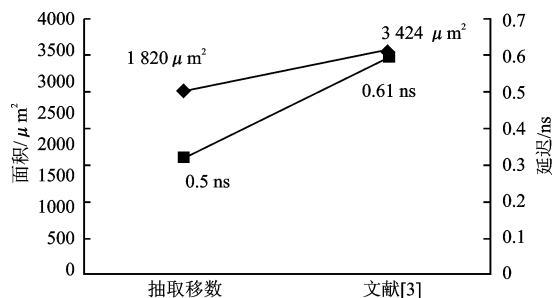


图 11 性能分析 (32-bit)

资源占用方面来说,本设计相对于文献[3]中抽取和移数统一硬件单元,具有较大优势,本设计只有一种路由信息生成算法,而文献[3]中需要两种路由信息生成算法,需要对移数和抽取的结果进行选择。虽然采用了高速连加电路,增加了局部硬件资源,但在资源占用方面仍然提升 47%。电路延迟方面来说,本设计明显优于文献[3],其主要原因在于,本文采用了高速连加电路和简化 Q 函数,同时不需要对移数和抽取结果选择,关键路径提升 17%。

对密码算法中的大位宽数据进行分组操作,设基本处理位宽为 32 bit,其支持 64 bit、128 bit、160 bit、256 bit 数据分为多组 32 比特数据所需的运算

次数。

从图 12 可知,由于本设计支持抽取移位操作,在实现大位宽数据分组时具有较大优势,随着位宽的增大,本设计的优势越来越明显,不仅支持已有的抽取和移位操作,还支持抽取移位操作。

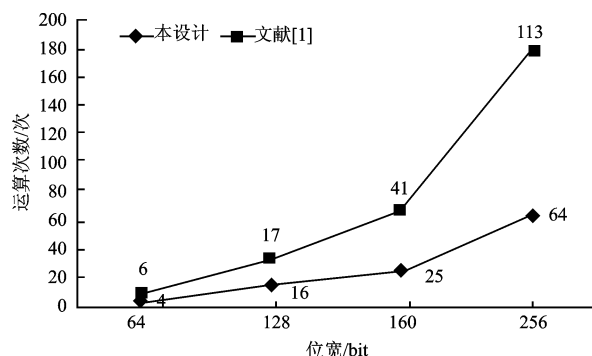


图 12 数据分组

6 结束语

本文构建了抽取移位硬件架构,提出了支持该架构的路由信息生成算法,并对架构进行了高速硬件映射。对架构的处理性能和灵活性进行评估,结果表明,本文设计的抽取移位硬件单元在处理性能、资源占用均具有较大的优势,同时为抽取移位指令的设计提供了硬件基础。

参考文献:

- [1] 徐建博,戴紫彬. 面向序列密码抽取与插入单元可重构设计研究[J]. 电子技术应用, 2011, 37(7): 65-67.
- [2] Lee R B, Shi Z, Yang Z. Efficient permutation instructions for fast software cryptography[J]. IEEE Micro, 2001, 21(6): 56-69.
- [3] Yedidya Hilewitz, Zhijie Jerry Shi, Ruby B Lee. A new basis for shifters in general-purpose processors for existing and advanced bit manipulations[J]. IEEE Transactions on computers, 2009, 58(8): 1035-1048.
- [4] Hilewitz Yedidya, Advance bit manipulation instructions: architecture, implementation and applications [D]. New Jersey: Princeton University, 2008.
- [5] John P McGregor, Ruby B Lee. Architectural techniques for accelerating subword permutations with repetitions[J]. IEEE Transactions on Very Large Scale Integration Systems, 2003, 11(3): 325-335.
- [6] Xiao Yang, Ruby B Lee. Fast subword permutation instructions using omega and flip network stages[C]// Proceedings of the International Conference on Computer Design, USA: Austin, Texax, 2000: 15-22.

(下转第 30 页)

在传送数据包时,随着失效率的增大,基于双缓冲和 XYX 的检错重传机制与端到端随机路由算法的平均发送微片数目也随之增大.当失效率小于 2% 时,基于双缓冲和 XYX 路由的检错重传机制转发的平均微片数目比端到端随机路由算法小约 30%,当失效率大于 2% 时,基于双缓冲和 XYX 路由的检错重传机制中转发的总微片数的平均值约等于端到端随机路由算法.

5 结束语

本文设计了一种基于双缓冲和 XYX 路由的容错机制.该机制通过采用双缓冲机制和 XYX 路由策略来循环交替发送数据包,从而减少等待延时和冗余包发送数目,在保证容错性能的同时,达到了延时和功耗优化的目的.通过使用 SystemC 设计的路由器模型构建的 4×4 的 2D-Mesh 网络平台,进行了多组仿真实验,实验结果表明,基于双缓冲和 XYX 路由的检错重传机制具有接近 100% 的容错性能,而且在失效率小于 2% 时,数据的传输延时和功耗开销相对端到端随机路由算法分别降低约 50% 和 20%,从而保证了高可靠高效率的数据传输.

参考文献:

- [1] Simn Ogg, Bashir Al-Hashimi, Alex Yakovlev. Asynchronous transient resilient links for NoC [C]// the 6th IEEE/ACM/IFIP international conference on Hardware/Software codesign and system synthesis. USA: New York, 2008: 1-6.
- [2] Muhammad Ali, Michael Welzl, Sven Hessler. A fault tolerant mechanism for handling permanent and transient failures in a network on chip [C]// the 4th international information technology conference. USA: Los Vegas, 2007: 1027-1032.
- [3] Dumitras T, Kemer S, Marculescu R. Towards on-chip fault-tolerant communication [C]// Proc. ASP-DAC. Kitakyushu, Japan: IEEE, 2003: 225-232.
- [4] Muralli S, Theocharides T, Vijaykrishnan N, et al. Analysis of error recovery schemes for networks on chips [J]. IEEE Design & Test of Computers, 2005, 22(5): 434-442.
- [5] Paul Bogdan, Tudor Dumitras, Radu Marculescu. Stochastic communication: a new paradigm for fault-tolerant networks networks-on-chip [C]// VLSI Design 2007. Bangalore, 2007: 1-17.
- [6] Muhammad Ali, Michael Welzl, Sven Hessler. An efficient fault tolerant mechanism to deal with permanent and transient failures in a network on chip [J]. High Performance System Architecture, 2007, 1(2): 113-123.
- [7] 张磊,李华伟,李晓维. 用于片上网络的容错通信算法 [J]. 计算机辅助设计与图形学学报, 2007, 4(4): 904-912.
- [8] Ahmad Patooghy, Seyed Ghassem Miremadi. XYX: a power & performance efficient fault-tolerant routing algorithm for network on chip [C]// Proceedings of the 2009 17th international Conference on Parallel, Distributed and Network-based Processing. Germany: Weimar, 2009: 245-251.
- [9] Karp R. Randomized rumor spreading [C]// Proc. of the 41th Annual Symposium on Foundations of Computer Science. San Diego, USA: IEEE Press, 2000: 565-574.
- [10] 罗莎莎. 片上网络瞬时故障容忍算法研究 [D]. 长沙: 湖南大学, 2009.

作者简介:

周 芳 女, (1979-), 硕士, 讲师. 研究方向为数字系统设计与计算机应用、专用集成电路设计. E-mail: zfnuaa@nuaa.edu.cn.

吴 宁 女, (1956-), 教授, 博士生导师. 研究方向为数字系统理论与技术、电子系统集成与专用集成电路设计.

(上接第 24 页)

- [7] 蔡宇东, 沈海斌, 严晓浪. AES 算法的高速实现 [J]. 微电子学与计算机, 2004, 21(1): 83-85.
- [8] Chen Jun Hong, Shieh Ming Der, Lin Wen Ching. A high performance unified-field reconfigurable cryptography processor [J]. IEEE Transaction on VLSI, 2010, 18(8): 1145-1158.
- [9] Chang Peichann, Huan Weihsuig. A block mining and recombination enhanced genetic algorithm for the permutation flow shop scheduling problem [J]. Int. J.

Production Economics, 2013, 141(1): 45-55.

作者简介:

常忠祥 男, (1985-), 博士研究生. 研究方向为专用集成电路设计. E-mail: changzhongxiang0@126.com.

戴紫彬 男, (1966-), 教授, 博士生导师. 研究方向为密码微系统设计.

李 伟 男, (1983-), 讲师. 研究方向为密码微系统设计.

龚海宁 男, (1980-), 工程师. 研究方向为软件工程.