第33卷 第22期 计 算 机 工 程 2007年11月
Vol.33 No.22 Computer Engineering November 2007
·安全技术· 文章编号：1000—3428(2007)22—0178—03 文献标识码：A 中图分类号：TP309

一种基于BENES网络的可重构比特置换系统设计

向 楠，戴紫彬，徐劲松
(解放军信息工程大学电子技术学院，郑州 450004)

摘 要：采用ATM交换机中的BENES网络，提出了一种简洁正确的寻径算法，在可重构密码芯片上实现比特置换功能单元，能够完成$N!$种N到N的任意比特置换。该方法可以支持新的密码算法，加速分组密码，减少资源占用。

关键词：比特置换；BENES网络；可重构

Reconfigurable System for Bit Permutation Based on BENES Network

XIANG Nan, DAI Zi-bin, XU Jin-song
(Institute of Electronic Technology, PLA Information Engineering University, Zhengzhou 450004)

【Abstract】This paper proposes a new way of efficiently doing arbitrary N-bit permutations in reconfigurable cryptographic chip with very efficient hardware implementation. The new method is based on the BENES multistage interconnection network which is widely used in ATM switcher. An accurate and compact sorting routing algorithm is also described. This method can support new crypt algorithm, speed up execution, and reduce resource consumption.

【Key words】 bit permutation; BENES network; reconfigurable

1 概述

无论是密码学还是计算机体系结构方面，比特置换都是重要而有意义的。从密码学的角度来说，比特置换提供了字节操作所无法实现的混乱扩散等功能。置换作为扩散的首要手段，在密码算法中得到了广泛应用。从计算机体系结构的角度来说，随着多媒体和信息安全技术的发展，快速比特置换将成为面向字节的处理器的一个重要发展方向[1]。

本文主要介绍在可重构密码芯片中设计构造置换单元。根据重构元素的最大适应性原则，一个$N\times N$的置换单元应该实现N输入、N输出的所有的选择变换，即$N\times N$置换单元的N个输出中的任何一个能够选择N个输入中的任何一个。按照该原则设计的可重构比特置换单元所需要的可控编码的宽度和它所能实现的选择变换的个数可由下述定理描述：

定理 对于N比特置换，需要从$N!$的结果空间中挑选出一个作为结果，因此至少需要$\log_2(N!)$比特作为置换操作指定。可以证明：$N!=O(NN)$,$\log_2(N!)=O[N\log_2 N]$[2~3]。这意味着用于指定一个置换的比特数是$N\log_2 N$。设一个$N\times N$置换单元能够实现其输入到输出的所有选择变换，即其N个输出中的任何一个能够选择N个输入中的任何一个，则该置换单元需要$N\log_2 N$位可控编码，它能够实现的选择变换的个数为N^2，即N个N选1，见表1。

表1 一些常用分组密码算法涉及的比特置换

置换种类	输入位宽	输出位宽	置换种类	输入位宽	输出位宽
DES：P置换	32	32	LOKI97：P置换	64	64
DES：E置换	32	48	SERPENT：初始置换	128	128
DES：初始终结置换	64	64	SERPENT：终结置换	128	128
LOKI91：E置换	32	48	DES：子密钥扩展置换	64	56
LOKI91：P置换	32	32	DES：子密钥扩展置换	56	48

由于发现交换网络和密码学中的置换网络功能非常相似，本文借鉴通信交换网络及其路由算法方面的研究方法和成果，来进行密码学中比特置换单元的构造，在可重构密码芯片中实现任意的比特置换操作。

2 BENES网络结构

随着通信技术和计算机技术的迅速发展，特别是WWW和多媒体业务的爆炸式增长、Internet的数据流量急剧增加，对交换网络的研究也日益深入，出现了BENES、CLOS、BUTTERFLY、BANYAN等形式的交换网络[1]。许多互联网络被用于解决众多领域的交换排序问题。这些网络为了适应不同的应用需求，具有各自不同的性质。由于交换网络和密码学中的置换网络功能非常相似，笔者借鉴通信交换网络方面的研究方法和系统架构来实现密码学中的比特置换，期望找到一种合适密码算法中比特置换的网络。对于$N\times N$的任意比特置换，这种网络的硬件实现要比文献[4]中用N个N选1的交叉开关实现节省面积。

根据互联交换网络的阻塞特点，一般将其分为无阻塞型、广义无阻塞型、可重排无阻塞型[5]。绝对无阻塞型的互联网络是最为理想的实现方式，但是它对网络的级联级数以及相关的硬件设施要求很高，所以在比特置换系统的设计中，没有采用这种网络而是采用可重排无阻塞的BENES网络。

BENES网是一种可重排网，能实现输入端到输出端的所有置换，作为非阻塞开关网络在通信领域得到广泛的应用。这种网络的特点是可以通过具体的寻径路由算法，根据全通道排序的要求，实时改变各级节点开关的状态(直通或交叉)，

作者简介：向 楠(1982－)，女，硕士研究生，主研方向：信息安全；戴紫彬，教授；徐劲松，讲师

收稿日期：2006-11-30 **E-mail：**thincat2001@126.com

从而有效避免路径冲突。由于它能实现输入到输出的所有置换，因此利用它来实现需要能实现输入端到输出端所有置换的可重构比特置换单元。

BENES 网的结构在文献[6]中有详细的描述，这里就不再赘述。8 输入的 BENES 网结构见图 1。这种网络具有以下一些很好的特性，可以用于解决可重构密码芯片中任意比特置换的问题。

(1)BENES 网络由两个背靠背的 BANYAN 网络连接而成。该网络可以通过开关状态的改变实现 $N\times N$ 的任意交换。因此可以利用它来构造能完成任意比特置换的可重构比特置换单元。应用于比特置换操作时，这种网络的特点就表现为可以通过寻径算法，产生各个开关的控制信息，实时改变各级节点开关的状态(直通或交叉)，实现 $N!$ 种置换中要求的任何一种。

(2)BENES 网络可以被拆分成不同的级，因此可以逐级利用和控制这个网络。

(3)规模为N的BENES网是由 $2\log_2 N-1$ 级 2×2 的开关构成，开关总数是$N\log_2 N-N/2$。每个开关由两个 2 选 1 的数据选择器构成。与文献[4]中用N个N选 1 的数据选择器来实现的方法相比，能有效地节省面积。

(4)BENES 网的每一个 2×2 开关，2 个输入和 2 个输出定义为互斥对。这些互斥对可以由一个比特配置。即每一级的 $N/2$ 个开关可以由 $N/2$ 个比特来配置，决定其状态(交叉或直通)，进而决定数据在网络中的路径。利用网络寻径算法，给定一个置换即可得出每个开关的状态。通过改变这些开关的状态可以实现不同的置换。

(5)BENES 网络是一种递归结构。可以用较小的 BENES 网构成较大的 BENES 网。

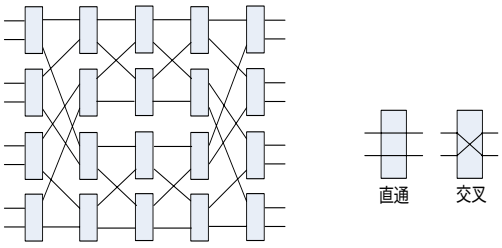

图 1　8×8 的 BENES 网络及其开关状态

3　BENES 网络的寻径算法

由于 BENES 网络是一种可重排的网络，如何控制网络中各个开关的状态(直通或交叉)，进而决定各个待置换的比特如何在网络中选路，而不至于发生阻塞，就需要有一种正确简洁的寻径算法。

本文借鉴一种光互联网络排序算法，改进之后用于比特置换网络寻径。这种算法本来是利用二分法构造二分图依次确定内外各级开关的连接状态，可以在BENES、OMEGA等网络中实现$N\times N$信号全排列无阻塞的输出和排序[7]。将这种算法中利用二分法构造二分图的步骤加以改进，使原有算法更简洁和有效，因而更适合编程实现。

算法描述如下：

利用该算法确定每级开关的状态。对于 2×2 节点开关，定义同一节点开关中，2 输入互斥，2 输出互斥，而任意属于不同开关的输入或输出不互斥；根据实际的输入和输出互斥对，得到一个二分图，确定两互斥对点集 X 和 Y。X 中的元素开关连线接上，Y 中的元素开关连线接下。这样确定出最左最右两级开关的状态。根据这 2 列开关状态把待置换的比特通过级间连线送往左边第 2 级和右边第 2 级。由此得到新的互斥对，由互斥对确定新的 X、Y 集合，进而确定两列开关的状态。循环这个过程，直到所有的开关状态都确定完毕。

描述如下：

(1) 输入待置换的比特序列 $1,2,3,\cdots,N\text{-}1,N$；输出 $\prod(1),\prod(2),\prod(3),\cdots,\prod(N\text{-}1),\prod(N)$。定义$\prod$为置换变换关系。

(2)输入互斥对：$O_1=\{1，2\}$，$O_2=\{3,4\},\cdots,O_{N/2}=\{N\text{-}1,N\}$；

(3) 输出互斥对：$P_1=\{\prod(1),\prod(2)\},P_2=\{\prod(3),\prod(4)\},\cdots,P_{N/2}=\{\prod(N\text{-}1),\prod(N)\}$；

(4)构造 X、Y，每组均包含 $N/2$ 个元素，满足条件

$$|X\cap P_i|=|X\cap O_i|=1 \quad (1)$$

$$|Y\cap P_i|=|Y\cap O_i|=1 \quad (2)$$

其中，$1\le i\le N/2$。

具体操作如下：

任选一个P_i，在P_i中选择一个元素a作为X中的一个元素，令$a\in O_j$，找出符合条件的O_j；设b为除去a之外的另一个元素，令$b\in P_k$，则b不能被选为X的元素，而只能选择P_k中的另一个元素作为X的元素。依次对每个$P_i(1\le i\le N/2)$作筛选，如此循环，可得X。则不在X中的元素就组成了Y。

(5)X、Y 用来确定位置左右对称的两级开关的状态(交叉或直通)。对于左边的一级 2×2 开关，X 中的元素对应接开关两输出端中上面的一个输出，Y 中的元素对应接开关两输出端中下面的一个输出；对于右边的一级开关，X 中的元素对应接开关两输入端中上面的一个输入，Y 中的元素对应接开关两输入端中下面的一个输入。由此左右两列开关状态得到确定。

(6)根据步骤(5)确定的两列开关，把待置换的比特通过开关经过级间连线送到中间两级开关的输入和输出。由此得到新的互斥对。重复步骤(4)和步骤(5)。直到所有开关的状态都被确定。

8×8 置换在 BENES 网络上的举例见图 2。

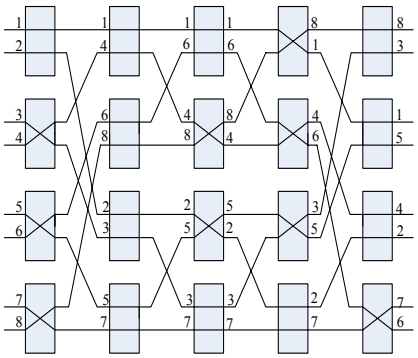

图 2　8×8 置换在 BENES 网络上的举例

用 8×8 的 BENES 网络实现 8×8 的置换。输入信号序列 1，2，3，4，5，6，7，8；输出 8，3，1，5，4，2，7，6。

(1)$\prod(1)=8$，$\prod(2)=3$，$\prod(3)=1$，$\prod(4)=5$，$\prod(5)=4$，$\prod(6)=2$，$\prod(7)=7$，$\prod(8)=6$；

(2)输入互斥对：

$O1=\{\underline{1}，2\}$，$O2=\{3，\underline{4}\}$，$O_3=\{5，\underline{6}\}$，$O_4=\{7，\underline{8}\}$；

(3)输出互斥对：

$P_1=\{\underline{8}，3\}$，$P_2=\{\underline{1}，5\}$，$P_3=\{\underline{4}，2\}$，$P_4=\{7，\underline{6}\}$；

(4)构造 X、Y，每组均包含 4 个元素，满足条件

$$|X\cap P_i|=|X\cap O_i|=1 \quad (3)$$

$|Y\cap P_i|=|Y\cap O_i|=1$ (4)

其中，$1\le i\le 4$。

$X=\{1，4，6，8\}$，$Y=\{2，3，5，7\}$；

(5)得到网络中最左和最右两级开关状态；

(6)得到新的互斥对；重复步骤(4)和步骤(5)，得到中间两级开关状态；最后得到最中间一级开关状态。

该算法用VC实现，用来提取用于进行比特置换的BENES网各个开关的控制信息。结果为 $2\log_2 N$-1 列，$N/2$ 行的矩阵，0 表示对应位置的开关状态为直通，1 表示对应位置开关状态为交叉，见表 2。

表 2　控制信息矩阵

0	0	0	1	0
1	0	1	1	0
1	0	1	1	0
1	0	0	0	1

4　网络的硬件实现和性能分析

本文基于 Altera 的 FPGA 器件实现了 128×128 比特置换电路。电路由 13×64 的开关矩阵组成，每个开关由两个数据选择器构成，由控制信息 con 控制其数据的选通，每个开关对应 1bit 控制信息，整个置换电路共 832bit 控制信息。当其为 1 时，数据交叉通过开关，当其为 0 时，数据直接通过开关。如图 3 所示，128bit 待置换的数据 Datain[0…127]在 con[0…831]的控制下，经过置换电路运算后得到 128bit 置换结果 Dataout[0…127]。

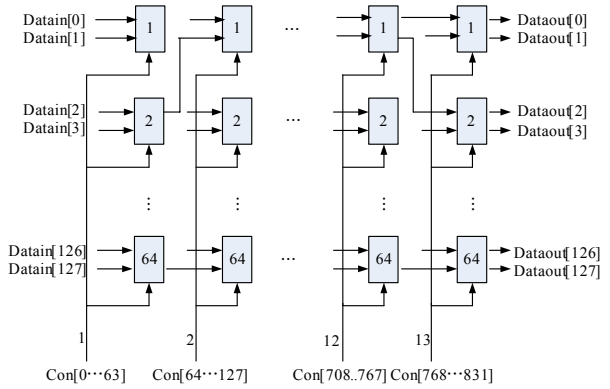

图 3　128×128 的置换单元电路结构

下面将本文中N比特任意置换的实现方法和文献[4]中的实现方法进行比较。对于$N\times N$的置换，本文以 $2\log_2 N$-1 级 BENES网络来实现，而文献[4]用N个N选 1 的数据选择器来实现。以 128×128 的置换为例，本文需要 13 级 2×2 的开关，文献[4]中需要 128 个 128 选 1 的数据选择器，见表 3。

表 3　128×128 的置换单元硬件性能参数

ALUTs	pins	tpd	device
1 600	1 088	19.294	EP2S180F1508C3

一个N选 1 的多路选择器的功能可以由$\log_2 N$级共N-1 个 2 选 1 的选择器实现。那么一个 128 选 1 的多路选择器就相当于 7 级 127 个 2 选 1 数据选择器。而 128 个 128 选 1 的数据选择器就相当于 128×127=16256 个 2 选 1 数据选择器。这样的电路结构，延迟和资源占用都是相当大的。而本文提出的置换单元的电路要相对简单得多。每个开关相当于两个 2 选 1 的数据选择器，一共是 13 开关，2×64×13=1 664 个 2 选 1 的选择器，见表 4。

表 4　以不同方法实现 128×128 置换资源占用情况比较

实现方法	资源占用	相当于 2 选 1 数选器的数量
本文方法	13 级 2×2 开关	1 664
文献[4]	128 个 128 选 1	16 256

5　结束语

本文基于 ATM 交换机中的 BENES 网，提出了一种简洁正确的寻径算法，构造出能够实现任意置换的可重构比特置换单元。该单元不仅能实现现有分组密码算法中的所有置换表，而且任意置换还能支持新的密码算法。完成同种功能，资源占用仅是文献[4]中所用方法的 10.2%。不仅能有效完成任意置换，而且大幅度节省了面积。

参考文献

1 Shi Z J. Bit Permutation Instructiong: Architecture, Implementation, and Cryptographic Properties[D]. U.S.A: Princeton University, 2004-06.

2 Abramowitz M, Stegun I A. Handbook of Mathematical Functions[Z]. Washington, D.C., US: Dept. of Commerce and National Bureau of Standards, 1970.

3 Cormen T H, Leiserson C E, Rivest R L, Introduction to Algorithms [M]. Cambridge, Mass: MIT Press, 1994.

4 曲英杰. 可重组密码逻辑的设计原理[D]. 北京: 北京科技大学, 2003.

5 金惠文. 现代交换原理[M]. 北京: 电子工业出版社, 2000-03.

6 Zhong Jiling. Upper Bound Analysis and Routing in Optical BENES Networks[D]. Department of Computer Science, Georgia State University, 2005-11-10.

7 杨俊波. 光互联网络中排序算法研究[J]. 光电工程, 2004, 31(增刊).

(上接第 150 页)

参考文献

1 Rosenberg J. SIP: Session Initiation Protocol[S]. RFC 3261, 2002.

2 雷为民, 张　伟. SIPNAT 问题阐述及其解决方案[J]. 通信世界, 2005, 6(4): 38-39.

3 Koski P, Ylinen J, Loula P. The SIP-based System Used in Connection with a Firewall[C]//Proc. of AICT-ICIW '06. 2006.

4 Arango M. Media Gateway Control Protocol (MGCP)[S]. RFC 2705, 1999.

5 Rosenberg J. An Extension to the Session Initiation Protocol (SIP) for Symmetric Response Routing[S]. RFC 3581, 2003.

6 张　波, 胡瑞敏, 边学工. 一种实现 SIP 穿越 NAT 的新方案[J]. 计算机工程, 2005, 31(2): 119-121.