平成１４年度　情報工学コース卒業研究報告要旨

高木 研究室	氏　　名	木村 和也
卒業研究題目	マイクロプロセッサにおける 完全シャフル回路を用いた パーミュテーションの高速化	

ワード内のパーミュテーション (ビット列の置換) は、ワード内のビットを指定された順に置換する操作であり、秘密鍵暗号の DES、Twofish、Serpent など、暗号化及び復号の処理の中で幅広く用いられている。現在のマイクロプロセッサには任意のパーミュテーションを効率よく実行できるような命令は実装されていないため、様々なパーミュテーションを高速に実行できる処理方法の開発が求められている。

高木研究室では、以前にマイクロプロセッサに専用回路を付加することにより、ワード内の任意のパーミュテーションを実行する方法を提案している。この方法では、パーミュテーションの対象ワードのビット数が n の場合、専用回路は $n\log_2 n - n + 2$ 個の２入力１出力のマルチプレクサで構成でき、パーミュテーションを実行するために必要な命令数は $((\log_2 n)^2 + \log_2 n)/2$ となる。

本研究では、その専用回路に改良を加えることによって、より少ないハードウェア量で、より高速にパーミュテーションを実行する方法を提案する。専用回路を用いてパーミュテーションを実行するために、高級言語向けのプリプロセッサを提案し、コンパイルの際に専用回路で用いる命令コード列を生成できるようにする。コンパイラは、ソーティングネットワークの一種であり、完全シャフルと隣り合う要素の比較交換の操作のみで構成できるバイトニックソートをシミュレートすることで、専用回路で用いる命令コード列を生成する。専用回路は、n 入力の完全シャフルを行う部分と $n/2$ 個のスイッチを行う部分から成り、配線と n 個の２入力１出力のマルチプレクサで構成される。提案方法を用いることによって、パーミュテーションを実行するために必要な命令数は $(\log_2 n)^2$ となる。特殊なパーミュテーションに対しては、完全シャフルの性質を用いることにより、命令数を削減することが可能である。また、専用回路を多段化することによっても、命令数を削減することができる。ワードのビット数を $n = 64$ とすると、以前提案された方法では、必要となるマルチプレクサの数が 322、命令数が 21 となるが、提案方法で専用回路を４段重ねた場合には、マルチプレクサの数は 256、命令数は 9 となり、以前のものよりも少ないハードウェア量と、約半分の命令数でパーミュテーションを実行することが可能となる。