# A Parallel $O\left(n 2^{7 n / 8}\right)$ Time-memory-processor Tradeoff for Knapsack-like Problems 

Li Ken-Li ${ }^{1,2}$, Li Ren-Fa ${ }^{1}$, Yang Lei ${ }^{1}$, Zhou Yan-Tao ${ }^{1}$<br>${ }^{1}$ School of Computer and Communication, Hunan University, Changsha, 410082, China<br>\{jt_lrf, jt-yl, jt_zyt\}@hnu.cn<br>${ }^{2}$ Department of Computer Science, University of Illinois at Urbana-Champaign, Champaign, 61801,USA<br>kenlili@uiuc.edu


#### Abstract

A general-purpose parallel three-list four-table algorithm that can solve a number of knapsack-like NP-complete problems is developed in this paper. Running on an EREW PRAM model, The proposed parallel algorithm can solve this kind of problems of size $n$ in $O\left(n 2^{9 n / 20}\right)$ time, with $O\left(2^{13 n / 40}\right)$ shared memory units and $O\left(2^{n / 10}\right)$ processors, and thus its time-space-processor tradeoff is $O\left(n 2^{7 n / 8}\right)$. The performance analysis and comparisons show that the proposed algorithms are both time and space efficient, and thus is an improved result over the past researches. Since it can break greater variables knapsackbased cryptosystems and watermark, the new algorithm has some cryptanalytic significance.


## 1 Introduction

Every NP-complete problem can be solved in $\mathrm{O}\left(2^{n}\right)$ time by exhaustive search, but this complexity becomes prohibitive when $n$ exceeds 70 or 80 . Assuming that $\mathrm{NP} \neq \mathrm{P}$, we cannot hope to find algorithms whose worst-case complexity is polynomial, but it is both theoretically interesting and practically important to determine whether substantially faster algorithms exist. In this paper we describe a parallel algorithm which can solve the knapsack problem. But owing to the work done by Schoreppel and Shamir [1], our proposed algorithm actually can solve a fair number of NP-complete problems including knapsack, partition, exact satisfiability, set covering, hitting set, disjoint domination in graphs, etc, which can be related by the composition operator [1]. Although the proposed algorithm is a versatile algorithm, to make this algorithm more easily be understood, we only take the knapsack problem as the representative to narrate this algorithm.
Given $n$ positive integers $W=\left(w_{1}, w_{2}, \ldots, w_{n}\right)$ and a positive integer $M$, the knapsack problem is the decision problem of a binary $n$-tuple $X=\left(x_{1}, x_{2}, \ldots, x_{n}\right)$ that solves the equation: $\sum_{i=1}^{n} w_{i} x_{i}=M$. This problem was proved to be NP-complete. Solving the knapsack problem can be seen as a way to study some large problems in number
theory and, because of its exponential complexity, some public-key cryptosystem are based on it [2-3]. Branch and Bound algorithms were proposed, but the worst case complexity is still $O\left(2^{n}\right)$ [4]. A major improvement in this area was made by Horowitz and Sahni [4], who drastically reduced the time needed to solve the knapsack problem by conceiving a clear algorithm in $O\left(n 2^{n / 2}\right)$ time and $O\left(2^{n / 2}\right)$ space. It is known as the two-list algorithm. Based on this algorithm, Schrowppel and Shamir [1] reduced the memory requirements with the two-list four-table algorithm which needs $O\left(2^{n / 4}\right)$ memory space to solve the problem in still $O\left(n 2^{n / 2}\right)$ time. Using unbalanced four tables, an adaptive algorithm is presented in [5], which can solve the knapsacklike problems according to the available computation source. Although the above algorithm is by far the most efficient algorithm to solve the knapsack problem in sequential, it can not solve any instances where the size $n$ is great.

With the advent of the parallelism, much effort has been done in order to reduce the computation time of problems in all research areas [6-14], most of which are based on CREW (concurrent read exclusive write) PRAM (parallel random access machine) model. Karnin [6] proposed a parallel algorithm that parallelizes the generation routine of the two-list four-table algorithm. In his algorithm the knapsack problem could be solved with $O\left(2^{n / 6}\right)$ processors and $O\left(2^{n / 6}\right)$ memory cells in $O\left(2^{n / 2}\right)$ time. The algorithm proposed by Amirazizi and Helman [7] runs in $O\left(n 2^{\alpha{ }^{n}}\right)$ time, $0 \leq \alpha \leq 1 / 2$, by allowing $O\left(2^{(1-\alpha) n / 2}\right)$ processors to concurrently access a list of this same size. They also present a more feasible Time-Space-Processor (TSP) model for evaluation of performance of different algorithms for the solution of knapsack-like NP-complete problems [7]. Ferreira [8] proposed a parallel algorithm that solves the knapsack problem of size $n$ in time $T=O\left(n\left(2^{n / 2}\right)^{\varepsilon}\right), 0 \leq \varepsilon \leq 1$, when $P=O\left(\left(2^{n / 2}\right)^{1-\varepsilon}\right)$ processors $S=O\left(2^{n / 2}\right)$ memory units are available. Chang et al. [9] presented another parallel algorithm where the requirement of the sharing memory is $O\left(2^{n / 2}\right)$ by using $O\left(2^{n / 8}\right)$ processors to solve the knapsack problem still in $O\left(2^{n / 2}\right)$ time. Thereafter, based on Chang et al.'s parallel algorithm, Lou and Chang [10] successfully parallelize the second stage of the two-list algorithm. Regretfully, it is independently found in [11] and [12] that the analysis of the complexity of the Chang et al.'s algorithm was wrong. In addition to pointing out the wrong in literature [9], we also proposed a CREW-PRAM cost-optimal parallel algorithm [11], and thereafter, a cost-optimal algorithm without memory conflicts was further presented in [13]. It must be pointed out that the space complexity is very important when solving the knapsack-like problems [6,15]. However, because the memories required in both of these two costoptimal parallel algorithms are still $O\left(2^{n / 2}\right)$, it make the available memory cells a bottleneck when using these algorithms to break practical knapsack based cryptosystem.

Therefore, to further reduce the required memory units for the solution of this kind of NP-complete problems, based on Ferreira's CREW based parallel three-list algorithm [14], we proposed a new parallel three-list four-table algorithm. The main properties of the proposed algorithm are as follows:
(i) With this algorithm, we can solve knapsack-like problems in $O\left(n 2^{9 n / 20}\right)$ time, $O\left(2^{13 n / 40}\right)$ shared memory units when $O\left(2^{n / 10}\right)$ processors are available. It results in an $O\left(n 2^{7 n / 8}\right) T S P$ trade off, which is considerably better than those of all similar algorithms published so far.
(ii) It can be performed on an EREW (exclusive read exclusive write) PRAM machine model, and thus is a totally without memory conflicts algorithm. Furthermore, the algorithm is completely practical in the sense that it is easy to program and it can handle problems which are almost 1.5 times as big as those handled by previous algorithms.
The rest of this paper is organized as follows. Section 2 explains the parallel threelist algorithm, on which the proposed algorithm is based. The proposed parallel algorithm is described in Section 3. Then, in Section 4, the performance comparisons follow. Finally, some concluding remarks are given in Section 5.

## 2 The parallel three-list algorithm

In 1995, Ferreira presented a parallel three-list algorithm, which is based on a CREW PRAM model [14]. The number of processor, time complexity, and space requirements in it are $O\left(2^{\beta n}\right), O\left(n 2^{(1-\varepsilon / 2-\beta) n}\right), O\left(n 2^{\varepsilon n / 2}\right), 0<\varepsilon<1,0 \leq \beta \leq 1-\varepsilon / 2$, respectively. It is viewed as an important breakthrough in the research of knapsacklike problems for it can solve the knapsack-like problems in a way of both time and space effective [14]. Because our parallel algorithm is based on this algorithm, we introduce it. To make it easy be understood, let the number of processors be $O\left(2^{n / 10}\right)$.

Algorithm 1: The Three-list algorithm
Generation stage

1. Divide $W$ into three parts: $W_{1}=\left(w_{1}, w_{2}, \ldots, w_{9 n / 20}\right), W_{2}=\left(w_{9 n / 20+1}, w_{9 n / 20}+2, \ldots\right.$, $\left.w_{18 n / 20}\right), W_{3}=\left(w_{18 n / 20+1}, w_{18 n / 20+2}, \ldots, w_{n}\right)$.
2. Form all possible subset sums of $W_{1}, W_{2}$, then sorted them in an nondecreasing order and store them as $A=\left[A_{1}, A_{2}, \ldots, A_{\frac{9 n}{20}}\right]$ and $B=\left[B_{1}, B_{2}, \ldots, B_{\frac{9 n}{20}}\right]$, respectively.
3. Form all possible subset sums of $W_{3}$, and store them as $C=\left[C_{1}, C_{2}, \ldots, C_{2^{\frac{n}{10}}}\right]$.

## Search stage

1. For all $C_{i}$ in $C$ where $1 \leq i \leq 2^{n / 10}$
2. $C_{i}$ execute the binary search over $A+B$ :
3. If a solution is found: then stop, output the solution
4. If a solution cannot be found: then stop: output that there is no solution.

The time and space complexity of this algorithm are $O\left(n \times 2^{11 n / 20}\right)$ and $O\left(2^{9 n / 20}\right)$ [14].
Based on its serial algorithm, Ferreira's parallel algorithm is very direct. It runs on a CREW model. The subset sums in list $A$ and $B$ which hold $2^{9 n / 20}$ subset sums respectively are stored in the shared memory. And each processor $P_{i}(1 \leq i \leq P)$, which holds the subset sum $C_{i}$, execute a "virtual" binary search on the list $A+B$ to make sure whether $A[j]+B[l]=M-C_{i}$ is satisfied, $1 \leq j, l \leq 2^{9 n / 20}$. The parallel three-list algorithm consists of the following three main steps [14].
Algorithm 2: parallel three-list algorithm
for all $P_{i}$ where $1 \leq i \leq 2^{n / 10}$ do

1. Generation of the two lists $A, B$ and $C$
2. Sorting of the two lists
3. Binary search over $A+B$
end
The time and space needed in this algorithm are $O\left(n \times 2^{9 n / 20}\right)$ and $O\left(2^{9 n / 20}\right)$ [14].

## 3 The proposed parallel algorithm

Although Ferreira's above algorithm is considered as a main breakthrough for the researches on the knapsack problem, it still have an obvious shortcoming, i.e. the TSP tradeoff is $O\left(n \times 2^{n}\right)$, which is greater than that of the recent parallel algorithms in $[11,14]$ by a factor $n$. To overcome this shortcoming, we redesign the two main stages of the parallel three-list algorithm. In list generation stage, we introduce four tables to produce two ordered list $A$ and $B$ dynamically. Doing so we can reduce the space complexity from $O\left(2^{9 n / 20}\right)$ to $O\left(2^{13 n / 40}\right)$. While in list search stage, we replace the matrix search way in [14] with the two-list like search algorithm, which is more simply and can reduce the time needed by a factor $O(n)$ in search stage.

In our proposed algorithm, each of the two lists stored in shared memory have a size of $O\left(2^{9 n / 20}\right)$, whose elements will be dynamically generated one by one, by using only $O\left(2^{13 n / 40}\right)$ shared memory units. Now consider the two stages of the algorithm.

### 3.1 The generation stage

Using the selection technique [14], Ferreira's parallel search algorithm is subtle. For it reduced the time needed otherwise for direct enumerating on the virtual list $A+B$ from $O\left(2^{9 n / 10}\right)$ to $O\left(n \times 2^{9 n / 20}\right)$. However, it is a little complicated for it concerns the search of "virtual" matrix [14]. Now we use the simply two-list like search to fulfill the list search stage.

Suppose the two ordered list $A$ and $B$ exist before the following algorithm 3 executes. We can use the following two-list like search algorithm to make sure that for any $C[k], 1 \leq k \leq 2^{n / 10}$ whether exist $A[i]$ and $B[j], 1 \leq i, j \leq 2^{9 n / 20}$, such that the formula $A[i]+B[j]+C[k]=M$ can be satisfied.

## Algorithm 3: parallel two-list like search algorithm

The subset sums in list $A$ and $B$ are sorted in increasing and decreasing order
for all processors $P_{k}$ where $1 \leq k \leq 2^{n / 10}$ do

1. $i=1, j=1$.
2. If $A[i]+B[j]=M-C[k]$, then stop: a solution is found, and write the result into the shared memory.
3. If $A[i]+B[j]<M-C[k]$, then $i=i+1$; else $j=j+1$.
4. If $i>2^{9 n / 20}$ or $j>2^{9 n / 20}$ then stop: there is no solution.

## 5. Goto Step 2.

End
Lemma 1. Let all elements in list $A$ and $B$ are given, the time needed to perform the algorithm 3 is at most $2 \times 2^{9 n / 20}$.
Proof. The condition that the loop ends shows that once the variables $i$ or $j$ is greater than $2^{9 n / 20}$, the algorithm terminates. While for each computation step, the value of one of the above two variables must increase by 1 . So it is obvious that the maximum of the needed time to perform the algorithm 3 is $2 \times 2^{9 n / 20}$.

Compared with the Ferreira's search algorithm [14], the search time needed here is reduced by a factor $O(n)$. But the space requirements do not increase.

### 3.2 The search stage

We discuss how to produce all elements of lists $A$ and $B$ stored in the shared memory. Note that in list search algorithm 3, each processor accesses the elements of the sorted lists $A$ and $B$ sequentially, and thus there is no need to store all the possible subset sums of $A$ and $B$ simultaneously in the shared memory-what we need is the ability to generate them quickly (on-line, upon request) in sorted order. So if we generate the two ordered lists dynamically, the needed space will reduced greatly. To implement this key idea, we explore the thoughts in [1] where four tables are used to dynamically produce the two sorted lists. Use four tables $T_{1}, T_{2}$, and $T_{3}, T_{4}$ to produce the two sorted lists $A$ and $B$, where $T_{1}$ includes all possible subset sums of knapsack entries $\left(w_{1}, w_{2}, \ldots, w_{9 n / 40}\right), \ldots, T_{4}$ includes all sums of $\left(w_{27 n / 40+1}, w_{27 n / 40+2}, \ldots, w_{36 n / 40}\right)$. let $e$ $=2^{9 n / 40}$, and mark $T_{i}=\left(t_{i 1}, t_{i 2}, \ldots, t_{i e}\right), i=1,2,3,4$. We first sort all sums in $T_{1}$ in an increasing order. Then use a priority queue $Q_{1}$ which has a length of $O\left(2^{9 n / 40}\right)$. At start, $Q_{1}$ stores all pairs of first $\left(T_{1}\right)$ and all elements $t_{2 i}$. It can be updated by two operations deletion and insertion, which enables arbitrary insertions and deletions to be done in logarithmic time of the length of the queue, and makes the pair with the smallest $t_{1 i}+$ $t_{2 j}$ sum accessible in constant time. Through the efficient heap implementations of priority queues [1], the following algorithm is designed to dynamically produce all sums of $T_{1}+T_{2}$ in an increasing order. For the processes to generate list $A$ and $B$ are similar, we focus on the procedures on the process to generate list $A$.

## Algorithm 4: algorithm for generating all sums of $\boldsymbol{T}_{\mathbf{1}}+\boldsymbol{T}_{\mathbf{2}}$ dynamically

Tables $T_{1}=\left(t_{11}, t_{12}, \ldots, t_{1 e}\right), T_{2}=\left(t_{21}, t_{22}, \ldots, t_{2 e}\right)$ are given
(1) sort $T_{1}$ into increasing order;
(2) insert into $Q_{1}$ all the pairs (first $\left(T_{1}\right), t_{2 i}$ ) for all $t_{2 i} \in T_{2}$;
(3) Repeat until $Q_{1}$ becomes empty.
$\left(t_{1}, t_{2}\right) \leftarrow$ pair with smallest $t_{1}+t_{2}$ sum in $Q_{1}$;
$S_{1} \leftarrow\left(t_{1}+t_{2}\right)$
if $S_{1}$ is needed and used for the objectivity of computation;
delete ( $t_{1}, t_{2}$ ) from $Q_{1}$;
if the successor $t_{1}{ }^{1}$ of $t_{1}$ in $T_{1}$ is defined, insert $\left(t_{1}{ }^{1}, t_{2}\right)$ into $Q_{1}$;

Lemma 2. One element in $T_{1}+T_{2}$ can be produced in $O(9 n / 40)$ time; while all $2^{9 n / 20}$ elements can be dynamically generated in $O\left(n 2^{9 n / 20}\right)$ time with $O\left(2^{9 n / 40}\right)$ shared memory units.

Proof. According to the theory of heap [1], one time of deletion and insertion on the heap can be performed with logarithmic time of the size of the heap. Since the heap constructed in algorithm 4 has a size of $2^{9 n / 40}$ and the combinations of $T_{1}+T_{2}$ have $2^{9 n / 20}$ elements. It validates the results of lemma 2.

To make the search algorithm perform successfully, we must prepare two queues (heaps) for each processor. As a result, in parallel case, the shared memory must have more memory units than that needed in sequential case.

Combine the above discussions into a whole; we get the final parallel three-list four-table algorithm and an overall conclusion on the solution of knapsack-like NPcomplete problems.

## Algorithm 5: An EREW based parallel three-list four-table algorithm

for all processors $P_{k}$ where $1 \leq k \leq 2^{n / 10}$ do

1. generate list $C$ and four tables $T_{1}, T_{2}$ and $T_{3}, T_{4}$ and sort $T_{1}$ and $T_{3}$ in parallel.
2. construct one $\min$ heaps for queue $Q_{1}$, and one $\max$ heaps for queue $Q_{2}$.
3. perform algorithm 4.
4. perform two-list like search algorithm (algorithm 3).
end
Theorem 1. $n$-variable knapsack-like problems can be solved on EREW model in $O\left(n 2^{9 n / 20}\right)$ time when $O\left(2^{n / 10}\right)$ processors and $O\left(2^{13 n / 40}\right)$ memory units are available.

Proof. Producing list $C$ and tables $T_{2}$ and $T_{4}$ can be finished in $n$ and $2 n \times 2^{5 n / 40}$ time, while tables $T_{1}$ and $T_{3}$ can be sorted in $4 \times 2^{5 n / 40}$ time [13]. Each processor will take $2 \times 2^{9 n / 40}$ time to construct two heaps. Following the lemmas 1 and 2 , the total needed time is: $n+2 n \times 2^{5 n / 40}+4 \times 2^{5 n / 40}+2 \times 2^{9 n / 20} \times\left(\frac{9 n}{40}\right)=O\left(\frac{9 n}{40} \times 2^{9 n / 20}\right)$.

The linear factor has little impact on the time complexity and thus is usually omitted [6-9,14]. So the time complexity of the proposed parallel algorithm is $O\left(2^{9 n / 20}\right)$. As for the space complexity, since there are $2^{n / 10}$ processors, and each of them need $2 \times 2^{9 n / 40}$ for the construction of heaps, the total space requirements is $O\left(2^{13 n / 40}\right)$. To avoid memory conflicts, at first, we copy the knapsack vector $W$ and scalar $M$ for each processor, which doesn't affect the overall complexity of the proposed algorithm. Thereafter, each processor access and update its own heaps, so it is obvious that all processors have no memory conflicts, and it can be performed on EREW PRAM machine model.

## 4 Performance comparisons

For the importance of the space complexity [6,15], we adopt the time-space-processor tradeoff (TSP tradeoff) [10], as the criterion of evaluation of relevant algorithms.
the TSP tradeoff of Karnin's parallel algorithm is $O\left(2^{5 n / 6}\right)$ [6]. The number of processor, time complexity, and the TSP tradeoff of Ferreira's parallel three-list search
algorithm in [14] are $O\left(2^{\beta n}\right), O\left(n 2^{(1-\varepsilon / 2-\beta) n}\right), 0 \leq \beta \leq 1-\varepsilon / 2$, and $O\left(n 2^{n}\right)$, respec-
tively. The parallel algorithm [7] runs in $O\left(n 2^{\alpha n}\right)$ time, $0 \leq \alpha \leq 1 / 2$, by allowing $O\left(2^{(1-\alpha) n / 2}\right)$ processors to concurrently access a list of this same size, hence the TSP tradeoff of this algorithm is also $O\left(n 2^{n}\right)$. Ferreira's parallel one-list algorithm [8] bears $O\left(n 2^{n}\right)$ TSP tradeoff. The performance of Chang et al.'s parallel algorithm [9] is $T=O\left(2^{n / 2}\right), P=O\left(2^{n / 8}\right)$, and $S=O\left(2^{n / 2}\right)$, thus results in a TSP tradeoff of $O\left(2^{9 n / 8}\right)$. The parallel algorithm Lou and Chang presented had a same performance as Chang et al.'s algorithm. In addition, both of the algorithms in [11] and [13] have a TSP tradeoff of $O\left(2^{n}\right)$. From our parallel three-list four-table algorithm, one can get a TSP tradeoff of $O\left(9 n / 40 \times 2^{n / 10} \times 2^{13 n / 40} \times 2^{9 n / 20}\right)=O\left(n 2^{7 n / 8}\right)$.

Among all algorithms that have been published, the TSP tradeoff of Karnin’s algorithm [6] is the lowest, which is $O\left(n 2^{5 n / 6}\right)$. However, it has an obvious defect that it can't reduce the execution time even in parallel. In spite of our proposed algorithm is not cost optimal, it go further on the overall time and memory performance than Ferreira's parallel three-list algorithm did. Moreover, our algorithm is totally without memory conflicts when different processors access the shared memory.
For the purpose of clarity, the comparisons of the main parallel algorithms published by far for solving the knapsack-like problems are depicted in Table 1. It is obvious that our parallel algorithm outtakes undoubtedly other parallel algorithms in the overall performance.

Table 1. Comparisons of the parallel algorithms for solving the knapsack-like problems

| Algorithm | Model | Processor | Time | Memory | TSP tradeoff |
| :--- | :--- | :--- | :--- | :--- | :--- |
| $1^{[6]}$ | CREW | $O\left(2^{n / 6}\right)$ | $O\left(2^{n / 2}\right)$ | $O\left(2^{n / 6}\right)$ | $O\left(2^{5 n / 6}\right)$ |
| $2^{[7]}$ | $C R E W$ | $O\left(2^{(1-\alpha) n / 2}\right)$ | $O\left(2^{\alpha n}\right)$ | $O\left(2^{(1-\alpha) n / 2}\right)$ | $O\left(2^{n}\right)$ |
| $3^{[14]}$ | $C R E W$ | $O\left(2^{\beta n}\right)$ | $O\left(2^{(1-\varepsilon / 2-\beta) n}\right)$ | $O\left(2^{\varepsilon n / 2}\right)$ | $O\left(2^{n}\right)$ |
| $4^{[8]}$ | $C R E W$ | $O\left(2^{(1-\varepsilon) n / 2}\right)$ | $O\left(2^{\text {gn/2 }}\right)$ | $O\left(2^{n / 2}\right)$ | $O\left(2^{n}\right)$ |
| $5^{[9]}$ | $C R E W$ | $O\left(2^{n / 8}\right)$ | $O\left(2^{n / 2}\right)$ | $O\left(2^{n / 2}\right)$ | $O\left(2^{9 n / 8}\right)$ |
| $6^{[10]}$ | $C R E W$ | $O\left(2^{n / 8}\right)$ | $O\left(2^{n / 2}\right)$ | $O\left(2^{n / 2}\right)$ | $O\left(2^{9 n / 8}\right)$ |
| $7^{[11]}$ | $C R E W$ | $O\left(\left(2^{n / 4}\right)^{1-\varepsilon}\right)$ | $O\left(2^{n / 4}\left(2^{n / 4}\right)^{\varepsilon}\right)$ | $O\left(2^{n / 2}\right)$ | $O\left(2^{n}\right)$ |
| $8^{[13]}$ | EREW | $O\left(\left(2^{n / 4}\right)^{1-\varepsilon}\right)$ | $O\left(2^{n / 4}\left(2^{n / 4}\right)^{\varepsilon}\right)$ | $O\left(2^{n / 2}\right)$ | $O\left(2^{n}\right)$ |
| Ours | EREW | $O\left(2^{n / 10}\right)$ | $O\left(2^{9 n / 20}\right)$ | $O\left(2^{n / 4}\right)$ | $O\left(2^{7 n / 8}\right)$ |

Notation: $0 \leq \varepsilon \leq 1,0 \leq \alpha \leq 1 / 2,0 \leq \beta \leq 1-\varepsilon$. The linear factor $n$ in algorithms numbered by $1-6$ and ours has been ignored for its little impact on the overall performance [6-9,14].

## 5 Conclusions

A new parallel three-list four-table algorithm for solving the knapsack-like problems is presented. Through dynamically producing the elements of the two lists which is to be searched in our two-list like search algorithm, we dramatically reduce the space requirements from $O\left(2^{9 n / 20}\right)$ in three-list algorithm in [14] to $O\left(2^{13 n / 40}\right)$. Moreover, the
memory conflicts in [14] are also avoided by leave different memory address segment for different processors, permitting the algorithm being able to perform on an EREW machine model. Performance comparisons shows our proposed algorithm greatly outweighs the parallel algorithms presented by far, and thus it is an improved result over the past researches. To our knowledge it is the first time that the knapsack-like problems can be solved without memory conflicts with less than $O\left(2^{n / 2}\right)$ running time when the hardware is also much smaller than $O\left(2^{n / 2}\right)$. Since it can solve problems that are almost 1.5 times as big as those handled by previous algorithms, it has some importance in research of cryptosystem.

## References

1. Schroeppel, R., Shamir, A. A $T=O\left(2^{\mathrm{n} / 2}\right), S=\mathrm{O}\left(2^{\mathrm{n} / 4}\right)$ algorithm for certain NP-complete problems. SIAM J. Comput, 1981,10(3):456-464.
2. Chor, B., Rivest, R.L. A knapsack-type public key cryptosystem based on arithmetic in finite fields. IEEE Trans. Inform. Theory, 1988,34(5):901-909.
3. Zhang, B., Wu, H.J., Feng, D.G, Bao, F. Cyptanalysis of a knapsack based two-lock cryptosystem. ACNS 2004, Lecture Notes in Computer Science, Vol. 3089. Springer-Verlag, Berlin Heidelberg New York (2004) 303-309.
4. Horowitz, E., Sahni, S. Computing partitions with applications to the knapsack problem. J. ACM, 1974,21(2): 277-292.
5. Li, K.L, Li,Q.H., Dai, G.M. An adaptive algorithm for the knapsack problem. Journal of Computer Development and Research, 2004,12(7): 1024-1029.
6. Karnin, E.D. A parallel algorithm for the knapsack problem. IEEE Trans, Comput, 1984, 33(5): 404-408.
7. Amirazizi, H.R., Hellman, M.E. Time-Memory-Processor trade-offs, IEEE Transactions on Information Theory, 1988,34(3):505-512.
8. Ferreira, A.G. A parallel time/hardware tradeoff $T \cdot H=\mathrm{O}\left(2^{\mathrm{n} / 2}\right)$ for the knapsack problem. IEEE Trans. Comput, 1991,40(2):221-225.
9. Chang, H.K.-C., Chen, J.J.-R., Shyu, S.-J. A parallel algorithm for the knapsack problem using a generation and searching technique. Parallel Computing, 1994,20(2):233-243.
10.Lou, D.C., Chang, C.C. A parallel two-list algorithm for the knapsack problem. Parallel Computing, 1997,22(14): 1985-1996.
11.Li, K.L, Li Q.H., Jiang, S.Y. An optimal parallel algorithm for the knapsack problem. Journal of Software, 2003,14(5): 891-896. (in Chinese)
12.Aanches, C.A., Soma, N.Y., Yanasse, H.H. Comments on parallel algorithms for the knapsack problem. Parallel Computing, 2002,28(10): 1501-1505.
13.Li, K.L., Li, Q.H., Li, R.F. Optimal parallel algorithm for the knapsack problem without memory conflicts. Journal of Computer Science and Technology. 2004,19(6): 760-768
14.Ferreira, A.G, Work and memory efficient parallel algorithms for the knapsack problem. International Journal of High Speed Computing, 1995,7(4): 595-606.
15.Woeginger G.J. Space and time complexity of exact algorithms: some open problems. In: R. Downey etc. Proceeding of IWPEC 2004, Lecture Notes in Computer Science, Vol. 3162. Springer-Verlag, Berlin Heidelberg New York (2004) 281-290.
