On-Chip High-Speed Solver of Inverse Problems Based on Quantum-Computing Principle

Minoru Fujishima* and Masahiro Shimura**

* School of Frontier Sciences, The University of Tokyo
** Broadband System LSI Division, Toshiba Corp.
1. Introduction
   - Importance of inverse problems to a one-way function
   - Advantage of quantum computing for inverse problems
   - Our approach to the inverse problems

2. Dual-Instruction-Multiple-Data Architecture
   - Evolution from quantum operation
   - Processor architecture

3. Implementation
Contents

1. Introduction
   - Importance of inverse problems to a one-way function
   - Advantage of quantum computing for inverse problems
   - Our approach to the inverse problems

2. Dual-Instruction-Multiple-Data Architecture
   - Evolution from quantum operation
   - Processor architecture

3. Implementation
Inverse problems to a one-way function in the world

- Database retrieval
- Route Search Problem
- Constraint Satisfaction Problem

Power consumption becomes restricted

To obtain maximum value

The concept of a Chip multi-processor (CMP) is a solution
Quantum computing procedure is a candidate of dedicated architectures for inverse problems.
Advantage of Quantum Computing for Inverse Problems

Advantage of quantum computing

Simultaneous calculation of massive data

Quantum bit (qubit)

000, 001, 010, 011
100, 101, 110, 111

Parallel operation

Classical bit

3bit

000

f(x)

Advantage of quantum computing is to process massive data with parallel operation.

f(000) f(001) f(010) f(011)
f(100) f(101) f(110) f(111)
Utilization of Quantum Computing Procedure

Quantum computing procedure for inverse problems

Quantum Processing Element (QPE)

Produce Processing Element

Controlled SIMD Operation

Search

Data Memory

NOT instruction

\[ f(x) \]

\[ \text{index QPE} \]

\[ \begin{array}{c}
\text{000} \\
\text{001} \\
\vdots \\
\text{111}
\end{array} \]

Example of factorization

\[ \text{3551} = ? \quad \text{?} \quad 3551 \mod x \quad 3551 \mod x = 0 \]

\[ 53 \]

Fast & correct

Answer
CMP architecture can operate with the same procedure as quantum computing.
Contents

1. Introduction
   - Inverse problems to a one-way function
   - Advantage of quantum computing
   - Approach to the inverse problems

2. Dual-Instruction-Multiple-Data Architecture
   - Evolution from quantum operation
   - Processor architecture

3. Implementation
Features of Quantum Computing Procedure

Quantum Processing Element (QPE)

Local Memory

Available Instruction only

“NOT”, “NOP” Disadvantage

Fundamental operation

NOT NOT NOT NOT

QPE QPE QPE QPE

(NOP: No Operation)
Conditional SIMD Architecture Based on Quantum Computing

PE

index

ALU

flag

Local Memory

Fundamental Instruction set

ADD, SUB, OR, XOR, AND, MOV, SFT, NOP,

SIMD Operation
ADD ADD ADD
PE PE PE

Controlled SIMD Operation

index?
ADD NOP NOP
PE PE PE

Memory data?
ADD NOP ADD
PE PE PE

They cover general instruction sets.

Instruction code
opcode
operand
condition

PE of idle state
Inefficient !!

PEs without executing operations are unutilized.
Dual Instruction Multiple Data (DIMD) Architecture

Instruction code

<table>
<thead>
<tr>
<th>opcode1</th>
<th>opcode2</th>
</tr>
</thead>
<tbody>
<tr>
<td>operand</td>
<td>condition</td>
</tr>
</tbody>
</table>

**Dual Instruction**

PE

Local Memory

ALU

Index

Selector

Operand

Condition

Flags, which is compared to conditional code, determines one of two opcodes.

SIMD Operation

ADD ADD ADD

PE PE PE

Controlled SIMD Operation

index? Memory data?

ADD NOP NOP

ADD PE PE

DIMD Operation

index? Memory data?

ADD OR OR

ADD PE PE

Operation efficiency is improved!!
Architecture of a Processing Element

**Dual Instruction**

- **opcode1**
- **opcode2**

**Selector**

**Input:**
- **reg1**
- **reg2**
- **index**

**Output:**
- **Local Memory**
  - **Index**
  - **direct addressing**
  - **indirect addressing**

**ALU**

- **Z, C, S, V, T, E**
- **Flag**

**Condition**

**Comparator**

**External Data**

**Operand**

**To neighbor PE**

**For high-speed search**

**Local Memory**

(16bit - 128 address)
Binary Connection between PEs for Search Answer

- In quantum computing procedure
  - Only one answer
  - Observation
  - Search algorithm
  - etc.

- In DIMD architecture
  - Only one answer has to be found in solving inverse problems
  - The number of wire connections should be as small as possible.

Binary connection
**Internal Construction in the Processor**

PEs occupy most processor area, while a controller verifies a candidate of answers picked up from PEs.

- Verification of a candidate of answer
- Control instruction

Independent instructions are issued simultaneously.
1. Introduction
   - Inverse problems to a one-way function
   - Advantage of quantum computing
   - Approach to the inverse problems

2. Dual-Instruction-Multiple-Data Architecture
   - Evolution from quantum operation
   - Processor architecture

3. Implementation
### Performance of DIMD processor

<table>
<thead>
<tr>
<th>Feature</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of gates</td>
<td>1.2M gates</td>
</tr>
<tr>
<td>Number of PE</td>
<td>192</td>
</tr>
<tr>
<td>Clock frequency</td>
<td>40MHz</td>
</tr>
<tr>
<td>Data bit width</td>
<td>16bit</td>
</tr>
<tr>
<td>Local Memory in PE</td>
<td>2048bit</td>
</tr>
</tbody>
</table>

### Cell Processor

<table>
<thead>
<tr>
<th>Feature</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of gates</td>
<td>234M gates</td>
</tr>
<tr>
<td>Number of PE</td>
<td>8 (only SPE)</td>
</tr>
<tr>
<td>Data bit width</td>
<td>128bit</td>
</tr>
</tbody>
</table>

If current process technology is used and data bit width is 128bit, about 4000~5000 PEs will be available!!
64-bit Factorization Algorithm and Result

Non-restoring division algorithm

\[ P = \begin{cases} 
3n+4 & (n=1,3,5,\ldots) \\
3n+5 & (n=0,2,4,\ldots) 
\end{cases} \]

64bit factorization time (longest)

<table>
<thead>
<tr>
<th>Processor</th>
<th>Clock Frequency</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>DIMD processor [40MHz]</td>
<td></td>
<td>34s</td>
</tr>
<tr>
<td>Intel Pentium4 (non SSE) [3.4GHz]</td>
<td></td>
<td>52s</td>
</tr>
</tbody>
</table>

DIMD processor reduces calculation time by 35% compared with general purpose processor with 3.4GHz clock frequency.
Conclusion

* New processor based on quantum computing procedure is proposed to realize a CMP dedicated to inverse problems to the one-way function.

* 64bit integer is factorized using DIMD processor, which reduces the calculation time by 35% compared with a general purpose processor with 3.4GHz clock frequency.

* DIMD processor solves the inverse problems, such as factorization, consuming the limited power at higher speed than a general purpose processor.
Thank you for your attention!