Specifications of a quantum computer for factoring

Noboru Kunihiro
The University of Electro-Communications, Japan

Asiacrypt2004 rump session, Jeju island, Korea
7th, Dec. 2004

Factoring by Quantum: in Theory

In 1994, Peter Shor proposed a good factoring algorithm.
This algorithm succeeds in factoring in polynomial time.

In Theory:
If the large-scale quantum computers are realized,
RSA, ElGamal and ECC will be totally broken.

But, in practice?

Factoring by Quantum : Now and Future

Current Technology

In 2001, Chuang et.al. implemented the Shor's factoring algorithm by using NMR with 7 qubits to factorize 15.

Target of Near Future:

factoring 128bit composite within 30seconds.

Final Target of Future:

factoring 1024 bit composite within practical time.

Candidates of Algorithms

	# of qubits	# of gates
based on R-ADD	$3n+2$	$270\ n^3$
based on Q-ADD	$2n+3$	$97n^4$

of qubits and gates for 576 and 1024 bits

	576bit integer		1024bit integer	
	qubit	# of gates	qubit	# of gates
R-ADD	1730	5.14*10^10	3074	2.90*10^11
Q-ADD (with Approx.)	1155	3.34*10^11	2051	2.14*10^11

Candidates of Devices

We need at least 10^10 operations.

	maximal available time	gate operation time	max of gate operation
Nuclear Spin	10^{-2} - 10^{8} sec	10^{-3}-10^{5} sec	10^{-5}-10^{14}
Electron Spin	10^{-3} sec	10^{-7} sec	10^{4}
Ion trap	10^{-1} sec	10^{-14} sec	10^{13}
Quantum dot	10^{-6} sec	10^{-9} sec	10^{3}
Optical cavity	10^{-5} sec	10^{-14} sec	10^{9}
Microwave cavity	10^{0} sec	10^{-4} sec	10^{4}

(QIC by Nielsen and Chuang,)

Running Time for 576 bit composite

gate operation time	1msec 10^{-3} sec.	10 μ sec 10^{-4} sec.	1 μ sec 10^{-6} sec.
R-ADD	1.63Years	6days	14Hours
Q-ADD with approximation	11Yeasr	1.3 Month	3.9days

To factorize within 1 month,
the gate operation time should be
less than 50 μ sec, 7.8 μ sec.

Candidates of Devices (again)

less than 50 μ sec, 7.8 μ sec

	maximal available time	gate operation time	max of gate operation
Nuclear Spin	10^{-2} - 10^{8} sec	10^{-3} - 10^{5} sec	10^{-5} - 10^{14}
Electron Spin	10^{-3} sec	10^{-7} sec	10^{4}
Ion trap	10^{-1} sec	10^{-14} sec	10^{13}
Quantum dot	10^{-6} sec	10^{-9} sec	10^{3}
Optical cavity	10^{-5} sec	10^{-14} sec	10^{9}
Microwave cavity	10^{0} sec	10^{-4} sec	10^{4}

But, less scalability

Conclusion:

- Factoring seems difficult if we follow the current technology and the extension of the current technology.
- BUT, I never claim that factoring is impossible.
- We need some kinds of big breakthrough !!!

What kinds of breakthrough?

1. new devices?
2. new algorithm?
3. development of parallel computation?

•NMR: 7qubits and very slow operation
•2qubits

•more than 1730 qubits and faster than 50 μ sec
•more than 1115 qubits and faster than 7.8 μ sec