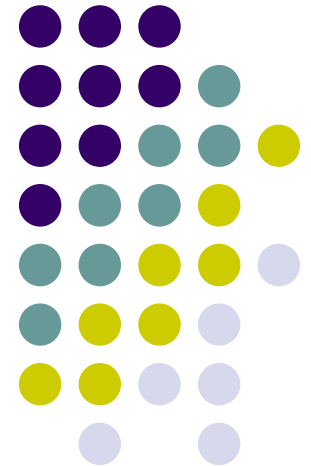
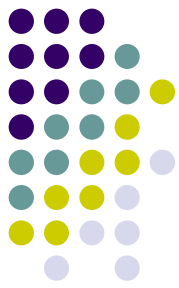


High Performance Computing over Finite Fields

21st Century COE Program, Chuo University
CREST, JST
Akira Nishida





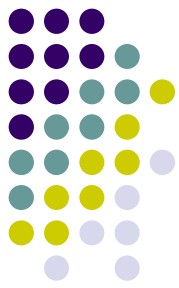
Motivation

- High Performance Computing for Cryptology
 - Long History in UK and US
 - First Supercomputer is “Bombe” for Enigma
 - First Cray-1 Customer is NSA
 - First Grid Application is Distributed.net
- In Japan...
 - Scientific Computing is a Major Research Area for Supercomputing
 - Calculation of π is a Major Application for (Super)computers
 - UD, United Devices is a Major Vendor for Distributed Computing
- Long Term Strategy is required

In This Research...



- Aim at
 - Record Breaking Performance for GNFS
 - Precise Estimation of Factorization Cost on State-of-the-art High Performance Computers



Related Work

- Robustness of Post Modern Cryptography Depends on...
 - Complexity of Factorization
 - (Generalized) Number Field Sieve (Lenstra and Lenstra, 1993)
 - Power of Computing Resource
 - TWIRL (Shamir and Tromer, 2003)
 - Precise Evaluation of Available Computing Resources (FLOPS)
 - www.top500.org (Dongarra and Strohmaier, -1995)



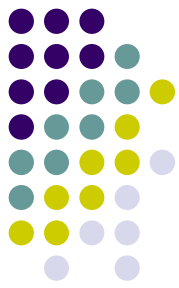
Prime Factorization

- In (G)NFS, we need...
 - Efficient Sieving
 - Efficient Solution of Sparse Linear System (on $GF(2)$)
 - Efficient Implementation of BIGNUM Library



Number Field Sieve

- Find $x, y \in \mathbb{Z}$ s.t. $x^2 \equiv y^2 \pmod{N}$
- Depends on the Size of the Composite Number N
 - $O(\exp(C(\ln N)^{1/3}(\ln \ln N)^{2/3}))$



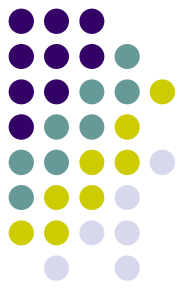
Factoring Records

- GNFS Historical Factoring Records

● Digits	Dates	Description	By
● 200	05/2005	RSA-200	Bonn Univ. et al.
● 193	11/2005	RSA-640	Bonn Univ. et al.
● 176	04/2005	cofactor of $11^{281}+1$	Rikkyo Univ. et al.
● 174	12/2003	RSA-576	Bonn Univ. et al.
● 164	12/2003	cofactor of $2^{1826}+1$	Rikkyo Univ. et al.
● 160	04/2003	RSA-160	Bonn Univ. et al.
● 158	01/2002	co-factor of $2^{953}+1$	Bonn Univ. et al.
● 155	08/1999	RSA-155	CWI et al.

- Curve Fitting and Extrapolation (Brent, 2000)

- $D^{1/3}=(Y-1928.6)/13.24$ (assuming Moore's Law)
- 200 digits in 2006



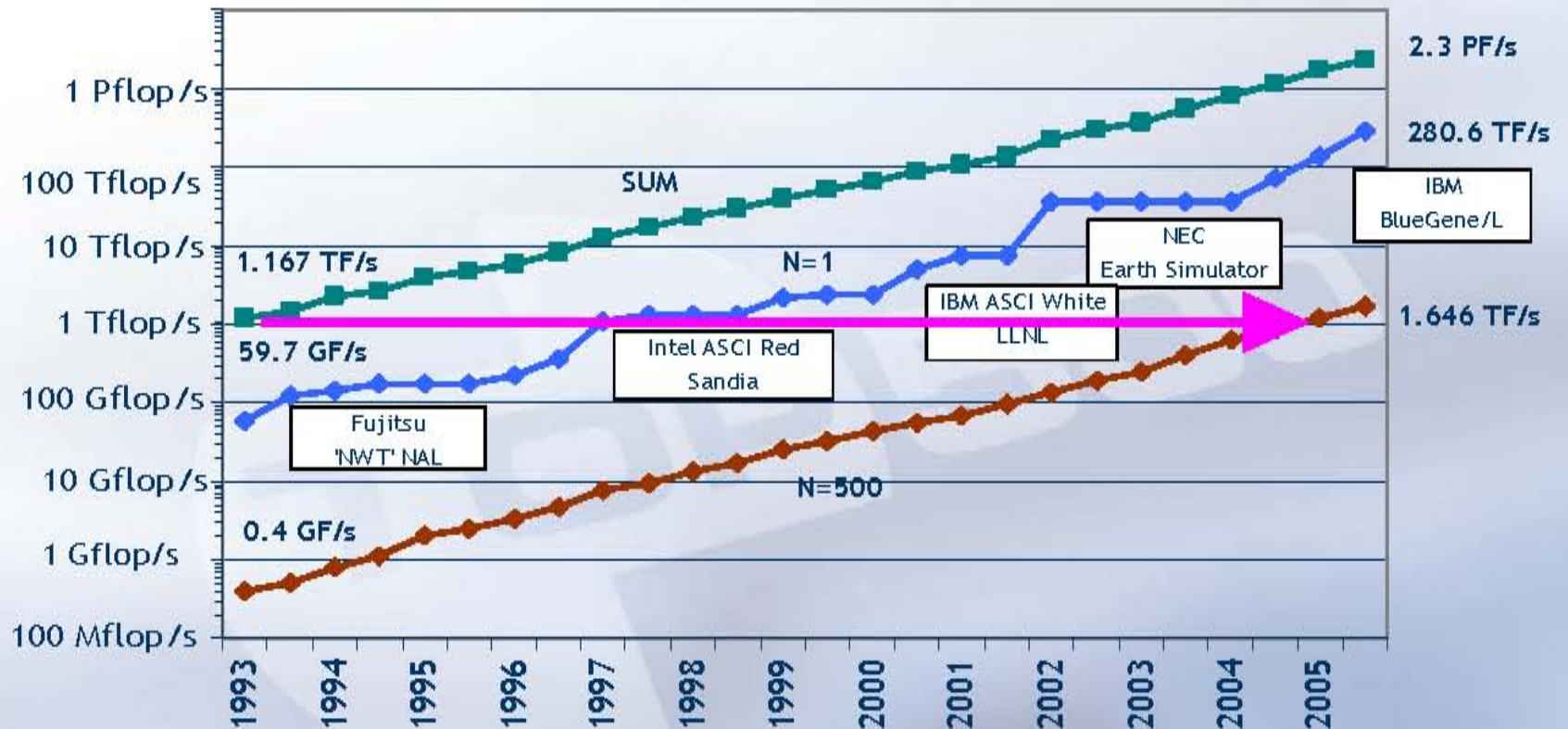
Computer Time

- For RSA-155 (1999)
 - 8000MIPS-Years
 - Sieving Step
 - 8000MIPS-Years
 - Matrix Step
 - 224CPU-Hours on Cray C916
 \doteq 6MIPS-Years
- For RSA-200 (2005)
 - 70000MIPS-Years
 - Sieving Step
 - 55 Years on Single 2.2GHz Opteron CPU
 \doteq 50000MIPS-Years
 - Matrix Step
 - About 3 Months on 80 2.2GHz Opterons
 \doteq 20000MIPS-Years



TOP500

- Listing of the 500 Most Powerful Computers in the World
 - Yardstick: Rmax from LINPACK
 - $Ax=b$, Dense Problem
 - Updated Twice a Year:
 - ISC'xy in Germany, June xy
 - SC'xy in USA, November xy
- All Data Available from www.top500.org



TOP500 Data Analysis



- Annual performance growth about a factor of 1.82
- Two factors contribute almost equally to the annual total performance growth
 - Processor number grows per year on the average by a factor of 1.30
 - Processor performance grows by 1.40 compared to 1.58 of Moore's Law

Strohmaier, Dongarra, Meuer, and Simon, *Parallel Computing* 25, 1999, pp 1517-1544.

Performance Issues



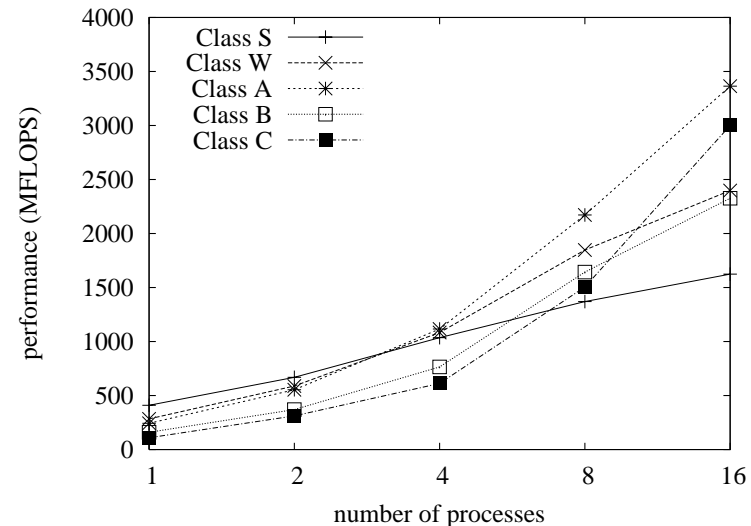
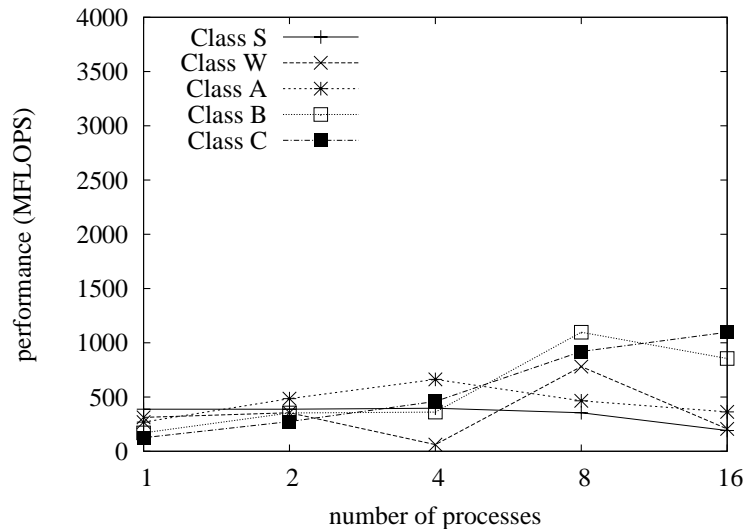
- Interconnects



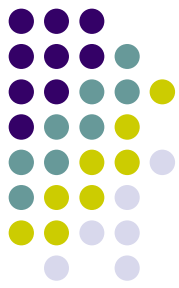


Performance Issues

- NAS Parallel Benchmark CG Kernel
 - Sparse Linear Solver (Conjugate Gradient Method)
 - GbE (Left) and PCI Express + InfiniBand (4GB/s Bidirection BW, Right)



Strategies



- Focus on the Performance Improvement
- Reconsider
 - The Linear Solver
 - Solve Normal Equations
 - In general, CG is much faster than Lanczos
 - Reported to work (Bell Laboratories, 1980's)
 - Stabilization Required ($u^T u$ can vanish for $u \neq 0$ over a Finite Field)
 - No Additional Cost
 - The Platform
 - Use Supercomputer Centers
 - Free or Very Low Cost
 - The Interconnect
 - Use Higher Bandwidth Interconnects
 - Need Replacement

Status



- Development of a Scalable Parallel Linear Solver over Finite Fields
 - We have a General Purpose CG Solver with 99.997% Parallel Efficiency (on Blue Gene)
 - Developing Earth Simulator Version
 - We need Joint Researchers!