Cryptography on the Grid

A. Suciu, R. Potolea

Technical University of Cluj-Napoca

Contents

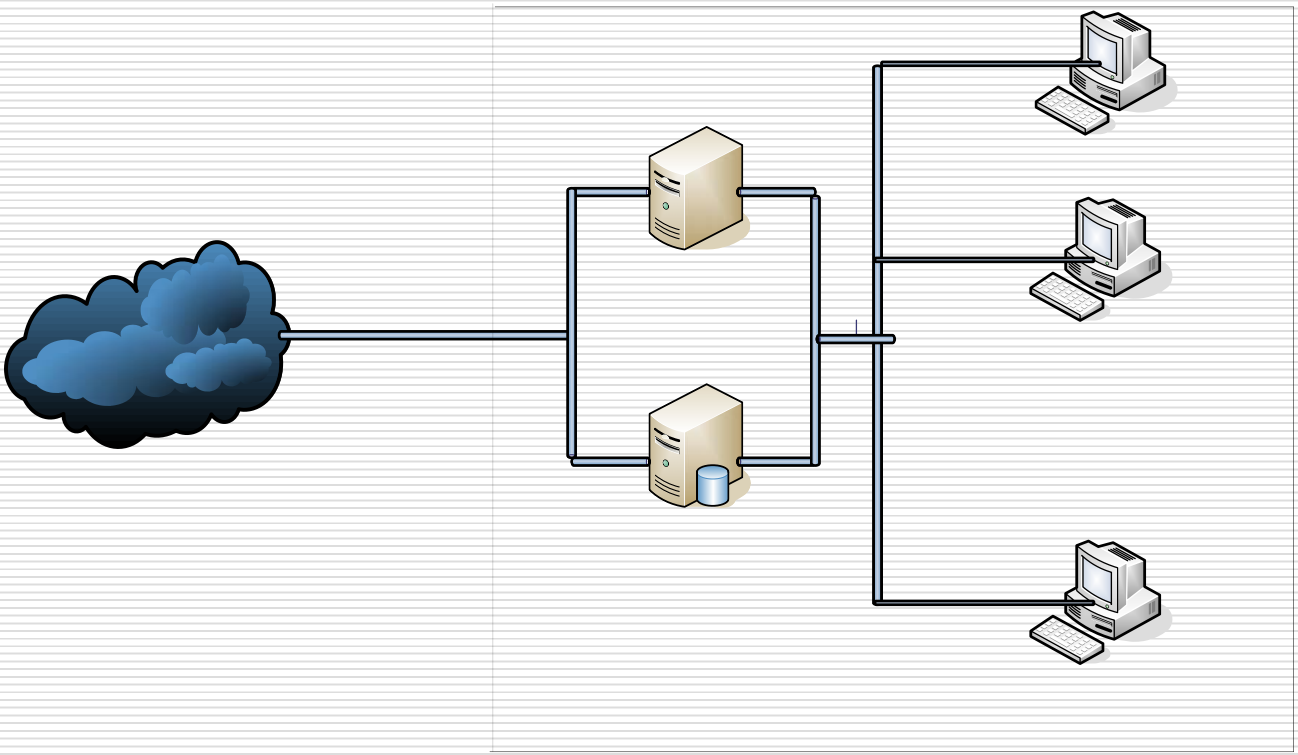
- Context
- Preliminary Work
- Goals
- Taxonomy for the Grid
- Cryptographic Algorithms
- Experimental Results
- Web Interface
- Conclusion

Context

- The GridMOSI Project (2005-2008)
- Virtual Organization using Grid Technology for High Performance Modeling, Simulation and Optimization
- Five Institutions (ICI, UPB, INCAS, UTCN, UVT)
- Lead by: Dr. Ing. Gabriel Neagu
- UTCN participation - Modeling and Optimization for Cryptology

Context (2)

- The UTCN grid node (simplified view)

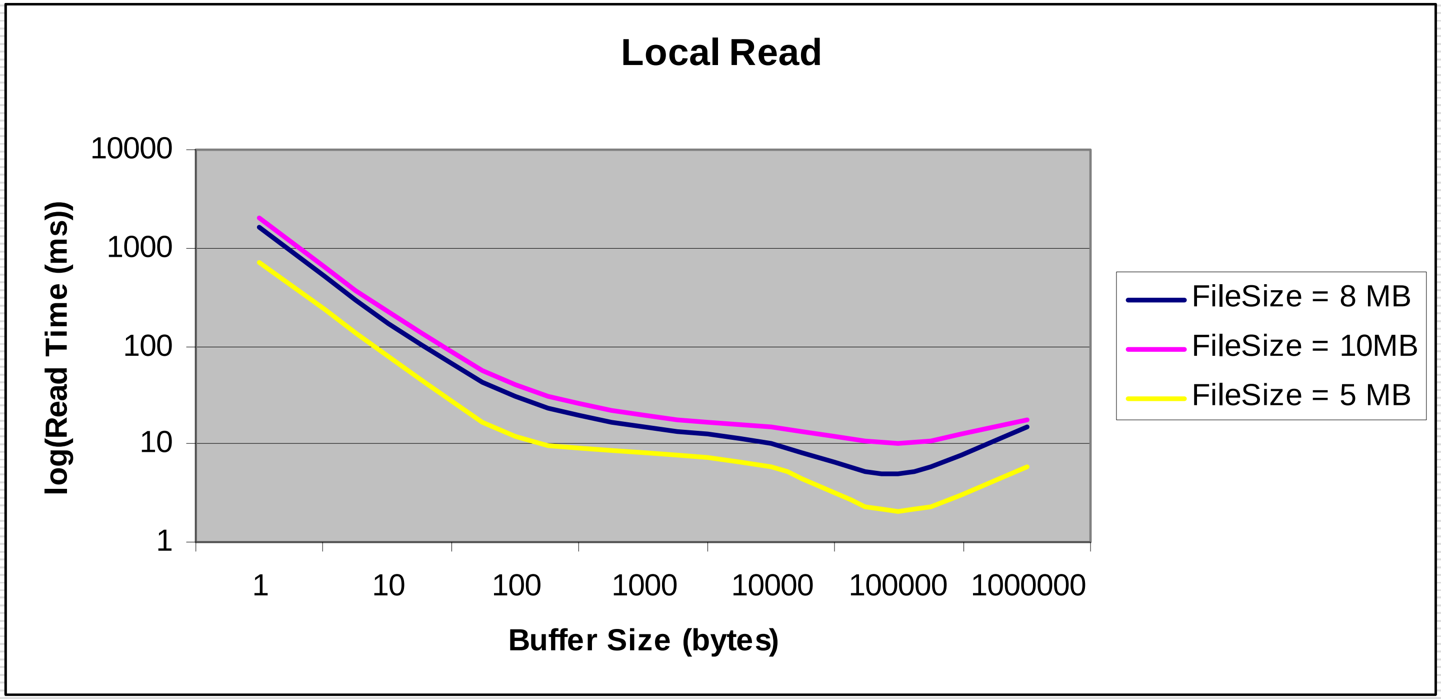


Context (3)

- □ The UTCN grid node:
- □ 22 processors – P4 class, 3GHz
- □ 1GB RAM / processor
- □ 160 GB HDD / processor
- □ OS – Scientific Linux 3.0.8
- □ Middleware - g-lite 3.0.2
- □ Experiments were performed on other nodes of the grid as well

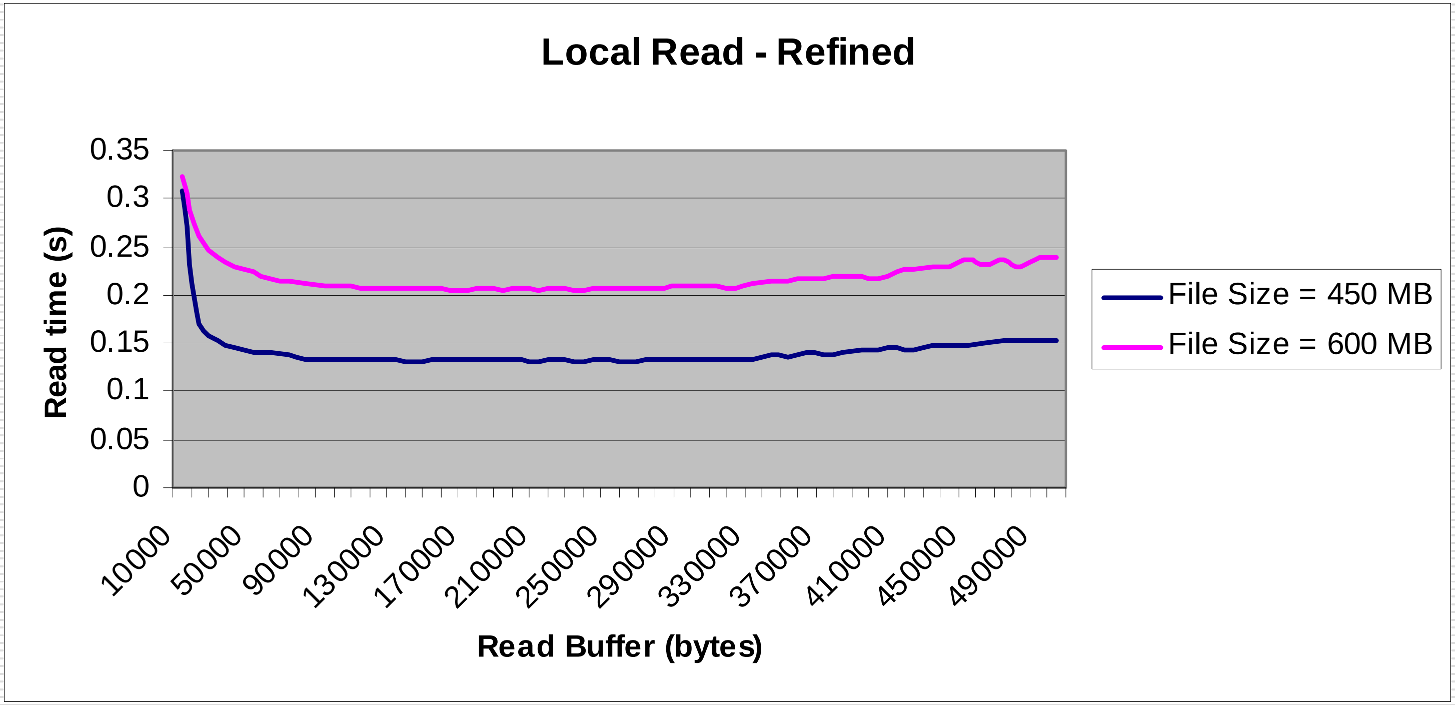
Preliminary Work

- Finding the Optimal Read Buffer Size for Grid Applications



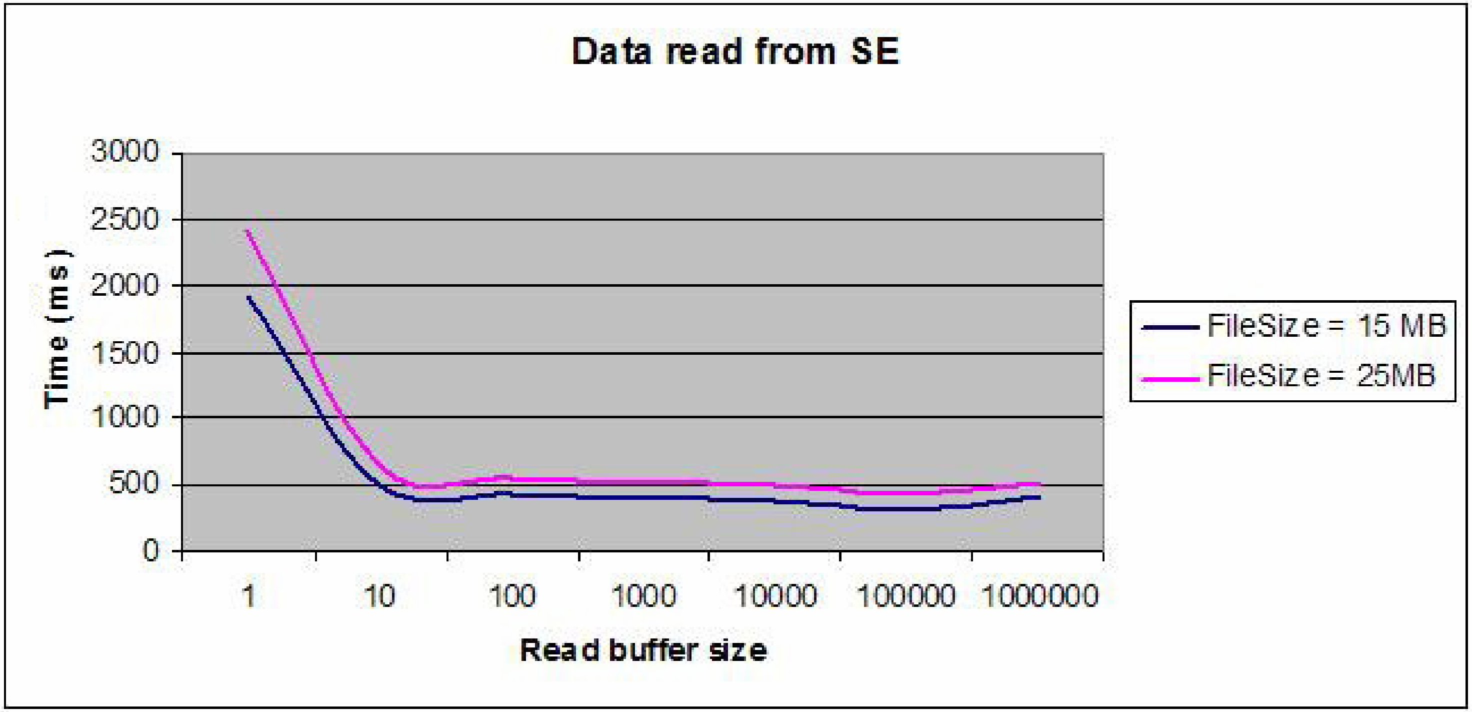
Preliminary Work (2)

- Finding the Optimal Read Buffer Size for Grid Applications - [130,000; 290,000]



Preliminary Work (3)

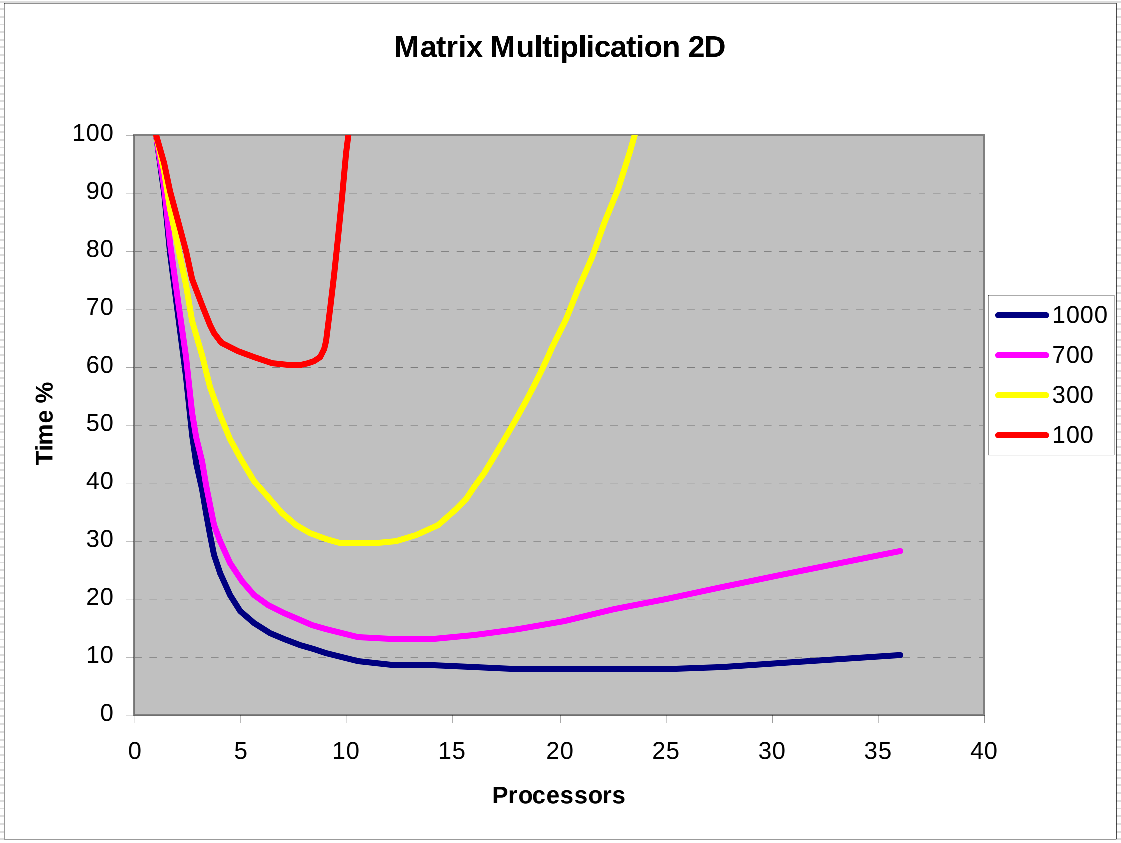
- □ Finding the Optimal Read Buffer Size for Grid Applications - [150,000; 300,000]



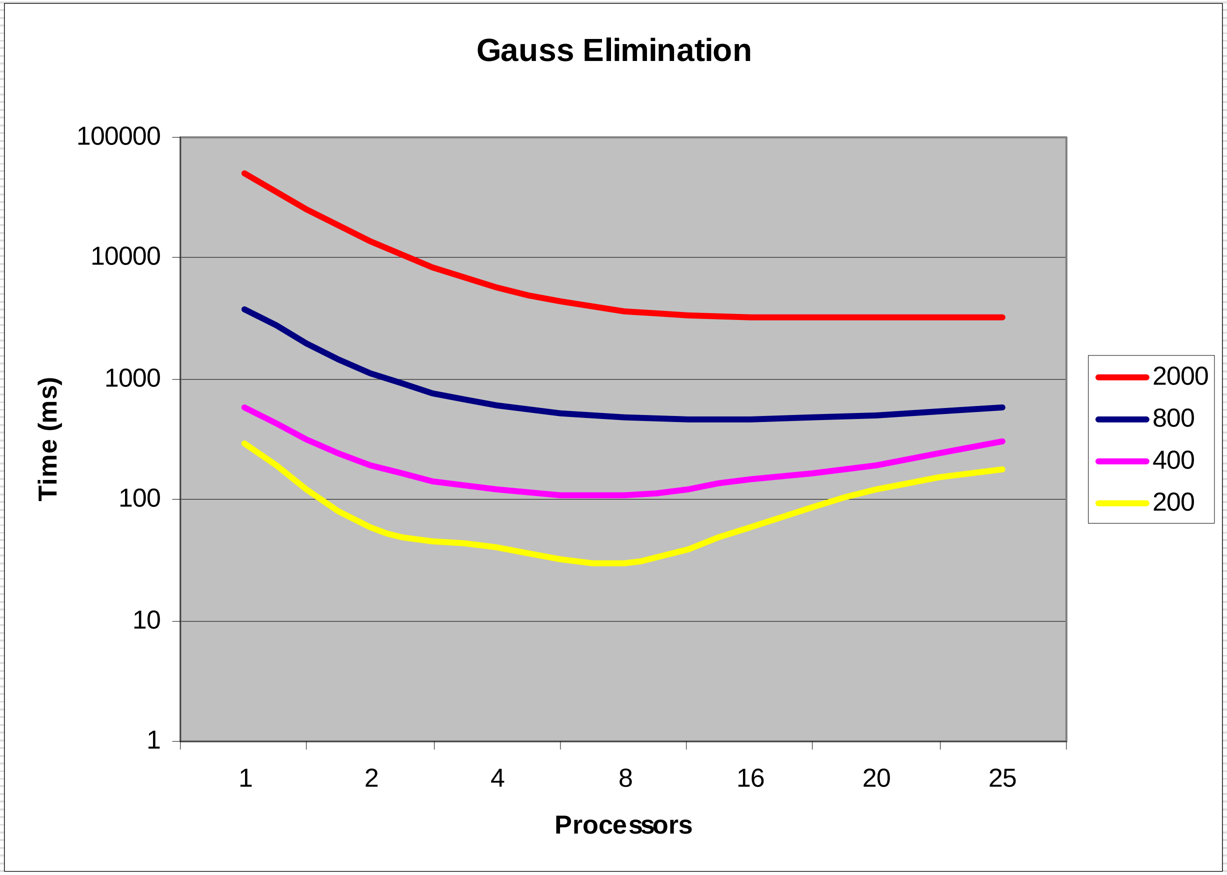
Preliminary Work (4)

- Finding the optimal number of worknodes for a given size of a problem:
  - Matrix Multiplication
  - Gauss Elimination
  - Minimum Spanning Tree
  - Shortest Path
  - Transitive Closure
  - Graph Isomorphism
  - Sorting Algorithms

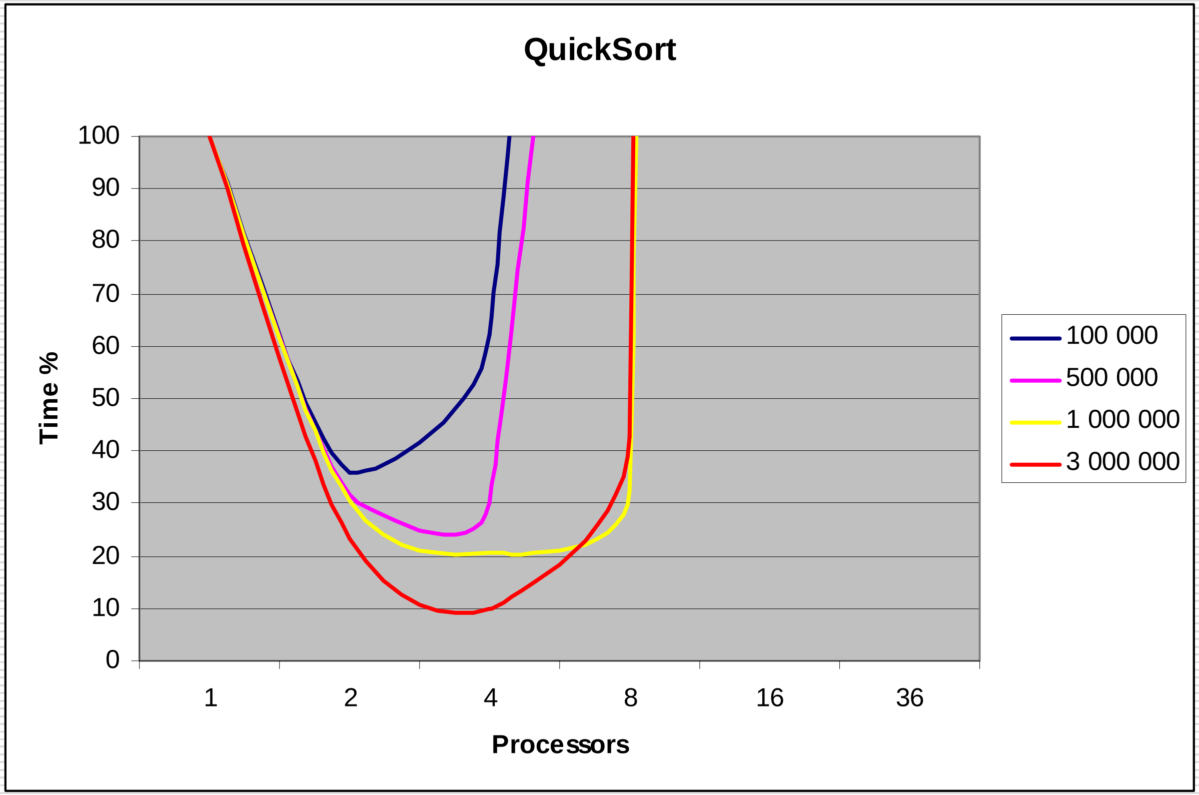
Preliminary Work (5)



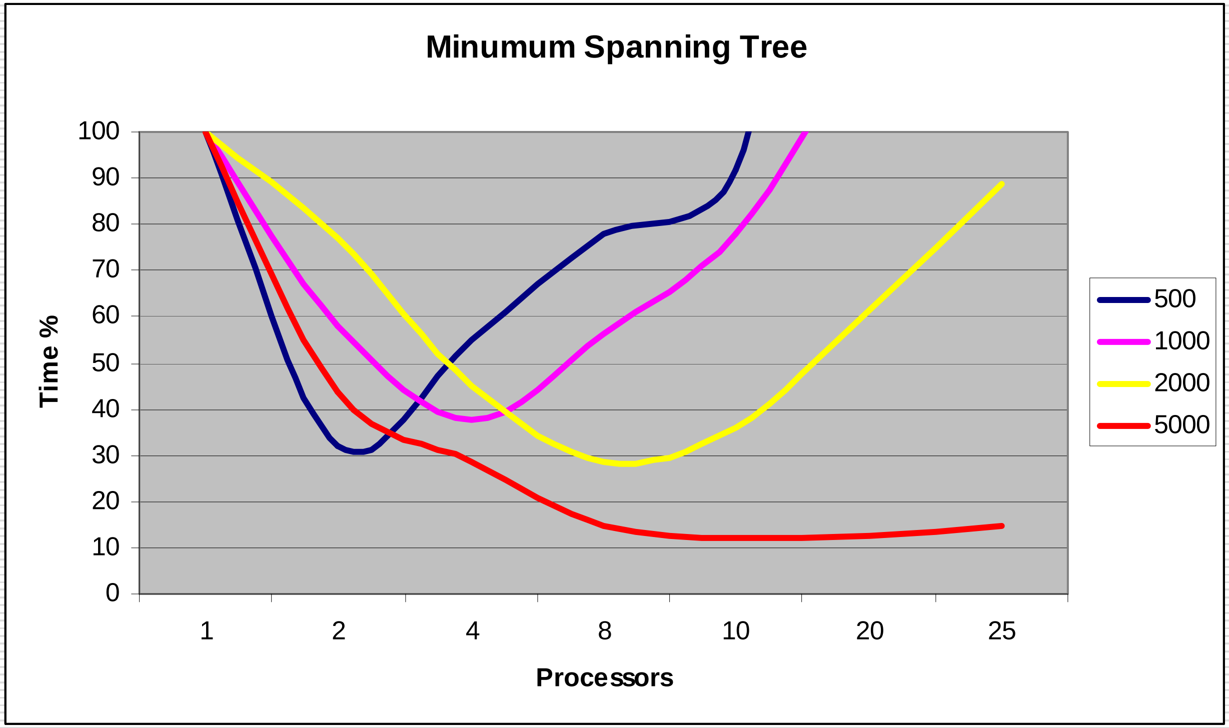
Preliminary Work (6)



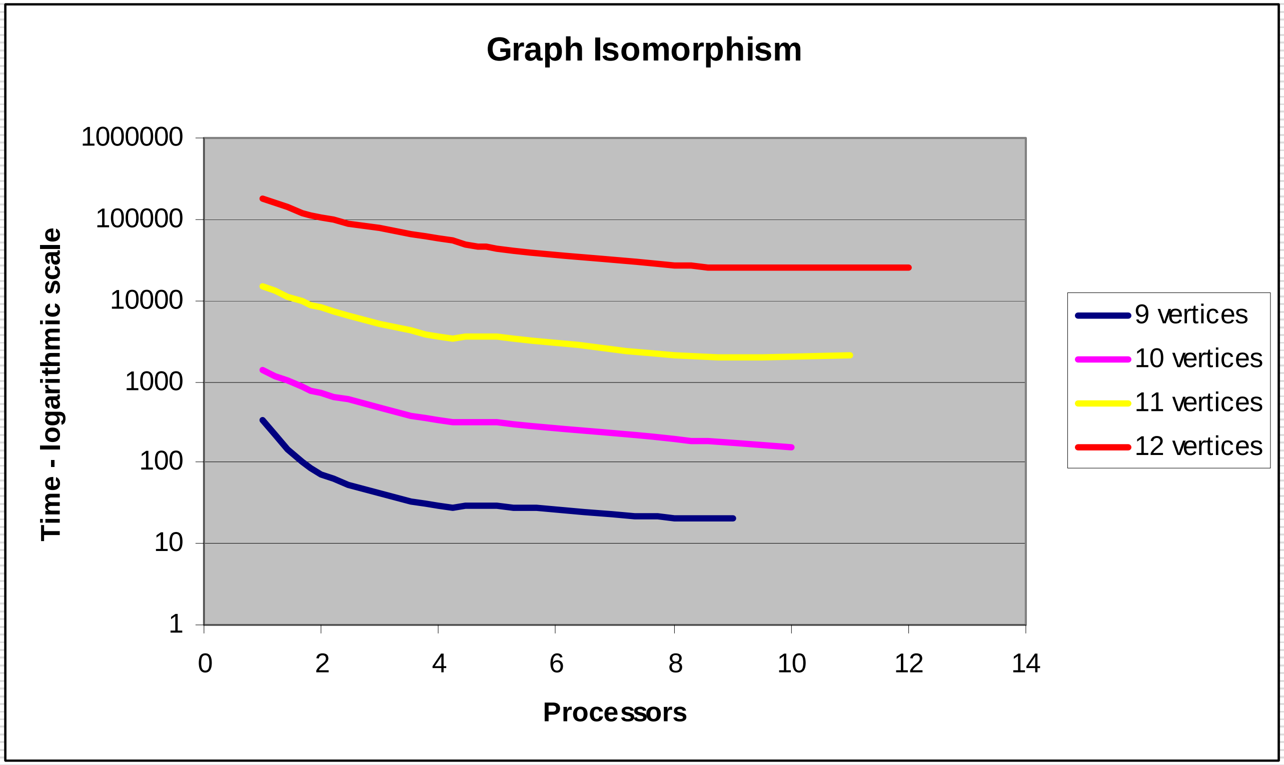
Preliminary Work (7)



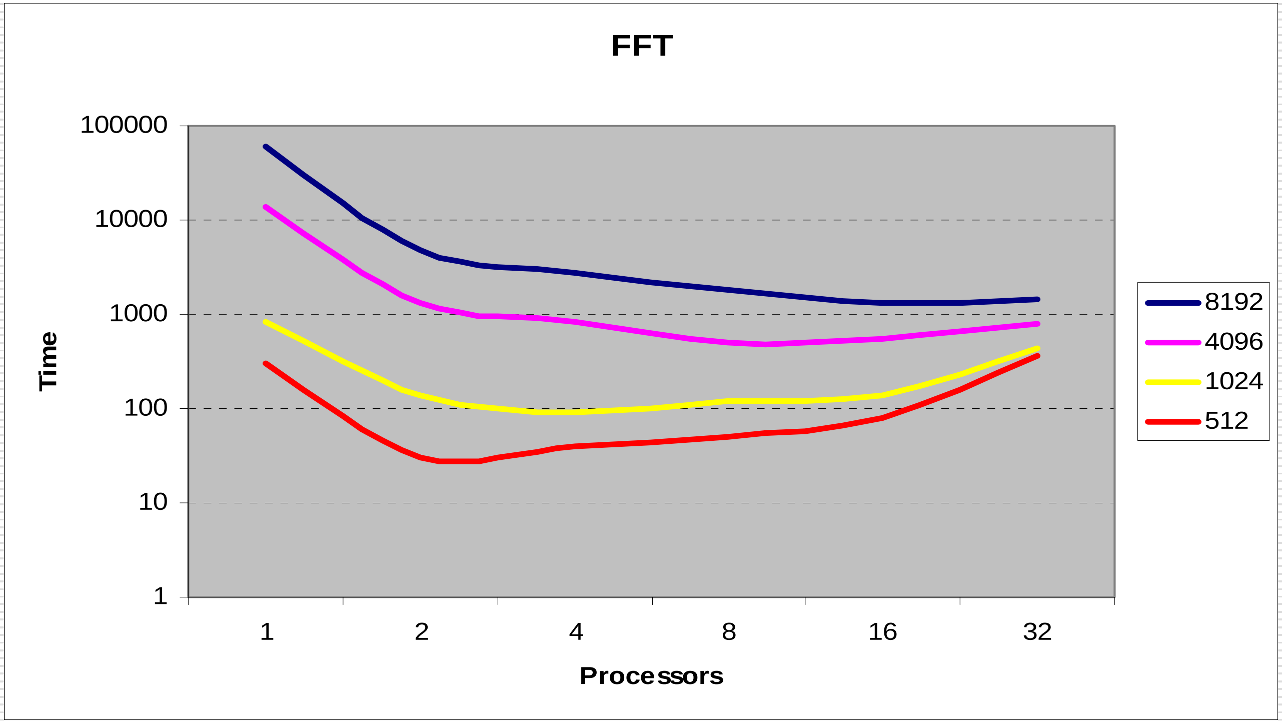
Preliminary Work (8)



Preliminary Work (9)



Preliminary Work (10)



Papers (2006)

- I. Gligan, R. Potolea and A. Suciu. *Grid Computing: A New Approach to Solving Large Scale Problems*. ACAM, ISSN 1221–437X, Vol. 15 (2006) no. 1, pp. 159–170.
- A. Mascasan, R. Potolea and A. Suciu. *Optimal Buffer Size for Grid Applications*. ACAM, ISSN 1221–437X, Vol. 15 (2006) no. 1, pp. 203–210.
- I. Leonte, A. Suciu and E. Cebuc. *Optimizing Cryptographic Algorithms by Parallel Grid-based Execution*. ACAM, ISSN 1221–437X, Vol. 15 (2006) no. 1, pp. 185–192.

Goals

- determine the degree of suitability of cryptographic algorithms for grid execution
- finding ways of parallelization of the algorithms on a grid architecture
- finding suitable execution (working) modes for the grid infrastructure
- improve performance
- provide a “library” of algorithms for grid applications

Taxonomy (0)

- Practical observation on what happens on the grid:
- Programs consume files and produce other files
- It would be nice to be able to:
  - Apply same program on several files
  - Apply several programs on the same file
  - Apply several programs on several files

Taxonomy

- Flynn’s taxonomy :
- SISD
- SIMD
- MISD
- MIMD

- Our taxonomy :
- SPSD
- SPMD
- MPSD
- MPMD

Taxonomy (2)

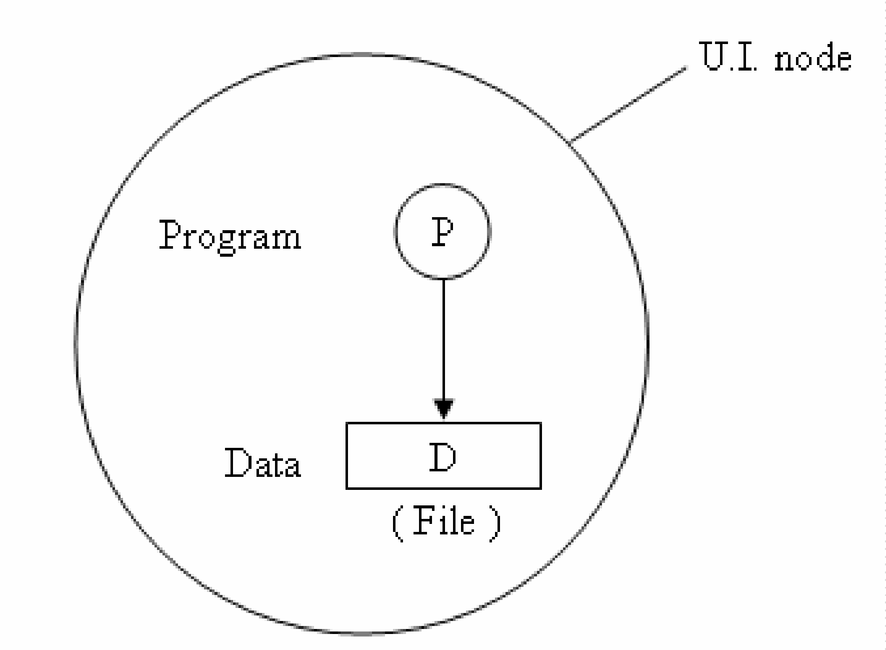
- Adapting our taxonomy for the Grid
- Program = Executable
- Data = File / Files
- Problems:
  - Programs have additional parameters
  - Find a unitary approach for all 4 categories – batch scripts, easy to use
  - Exploit parallelism where available

Taxonomy (3)

- SPSD/L [Local execution]
- SPSD/G [Grid execution]
- SPMD/G [Grid]
- SPMD/G/DP [Grid, data parallel]
- MPSD/G [Grid]
- MPSD/G/DP [Grid, data parallel]
- MPMD/G [Grid]
- MPMD/G/DP [Grid, data parallel]

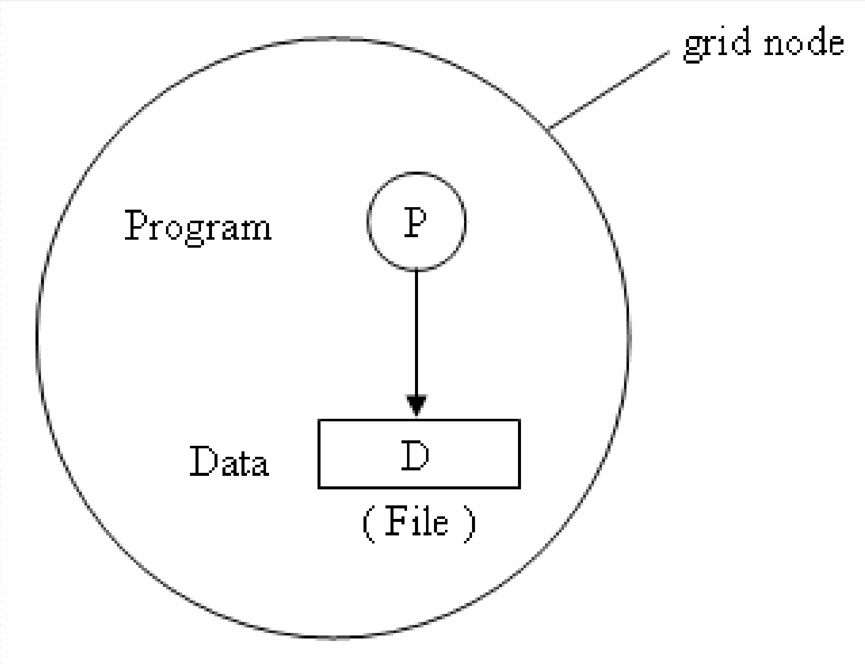
Taxonomy (4)

- SPSD-L (Single Program Single Data - Local)



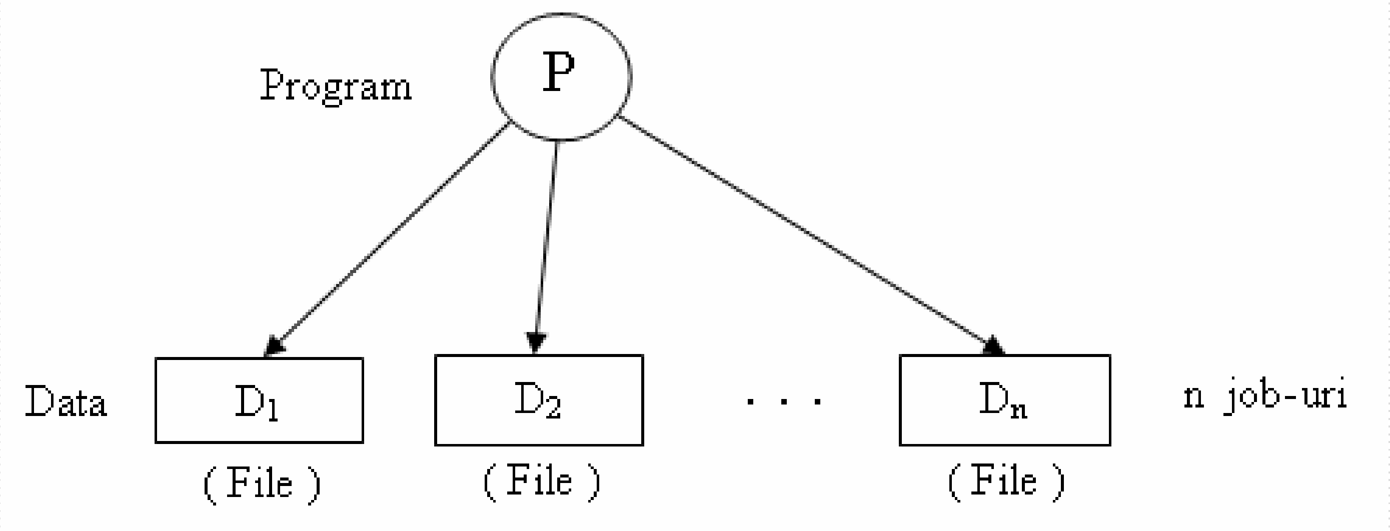
Taxonomy (5)

- SPSD-G (Single Program Single Data - Grid)



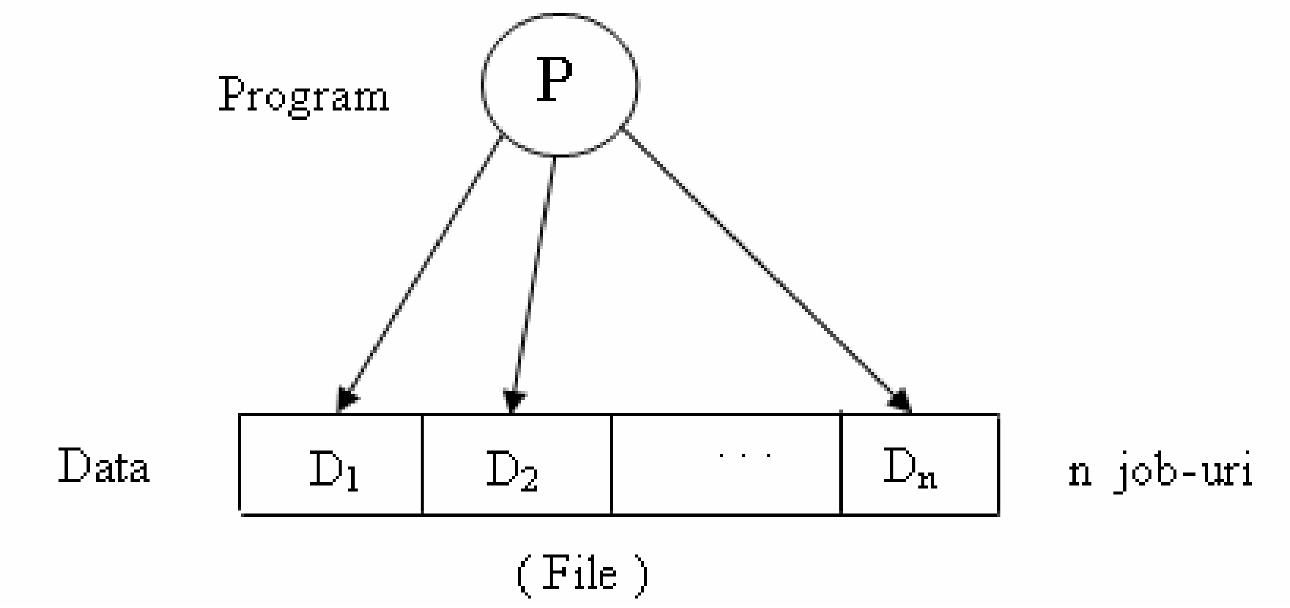
Taxonomy (6)

- SPMD-G (Single Program Multiple Data - Grid)



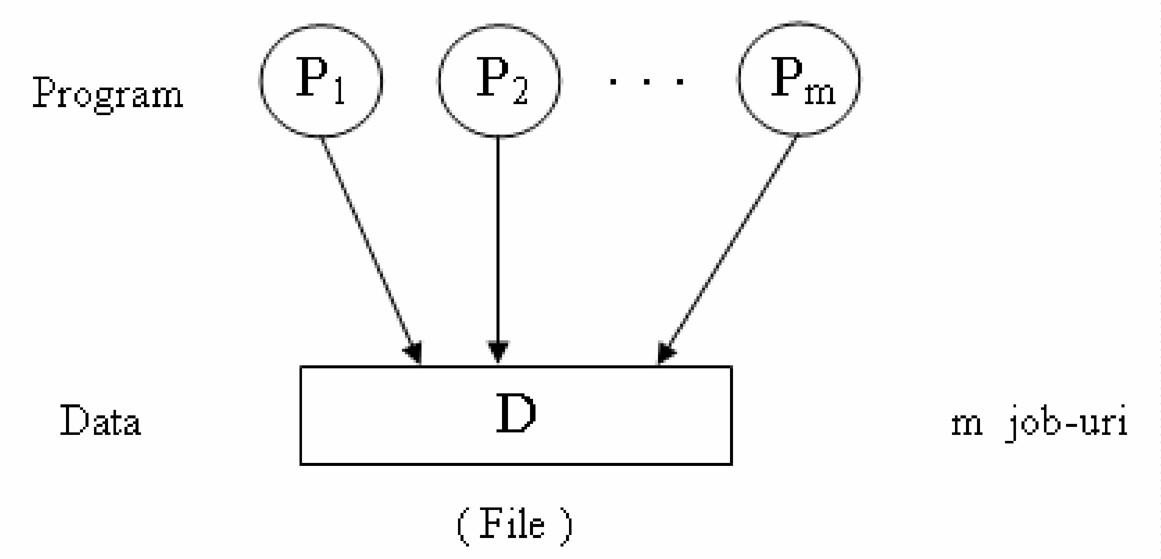
Taxonomy (7)

- SPMD-G-DP (Single Program Multiple Data - Grid - Data Parallel)



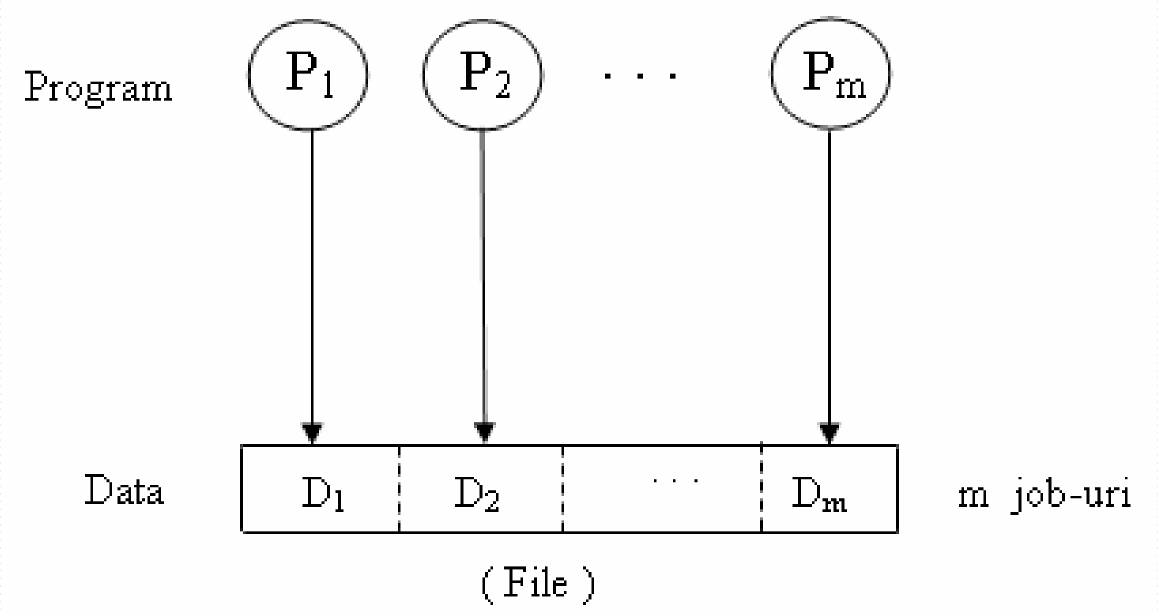
Taxonomy (8)

- MPSD-G (Multiple Program Single Data - Grid)



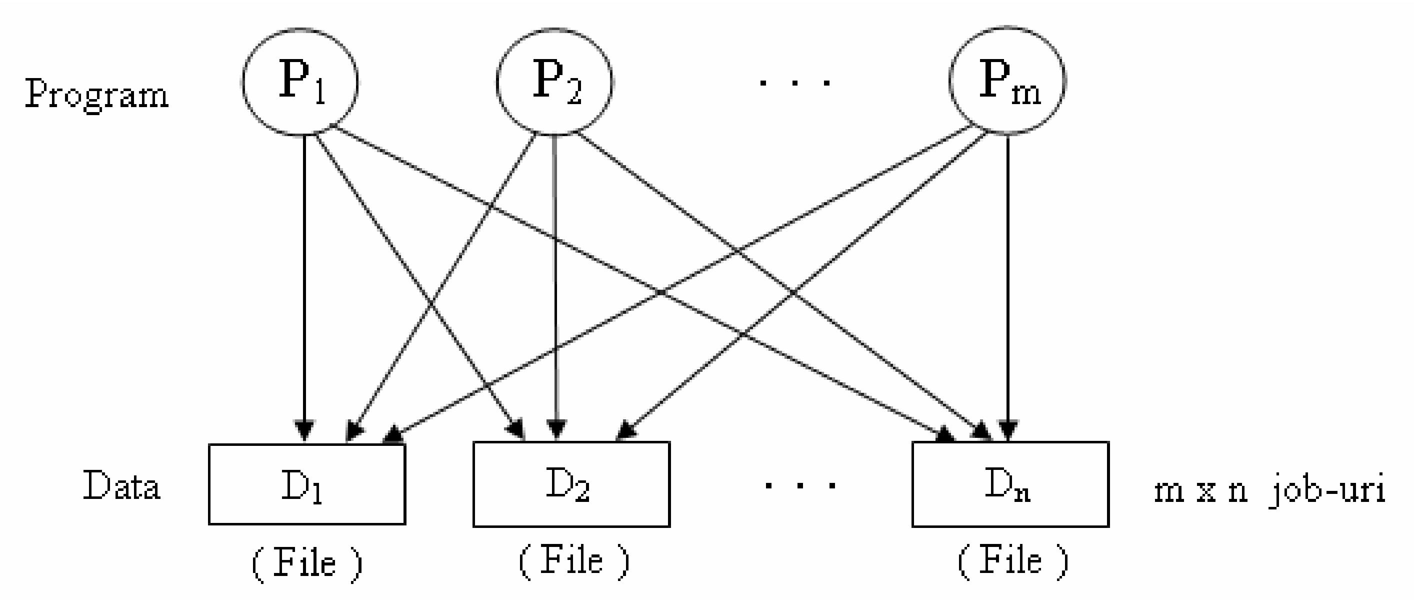
Taxonomy (9)

- MPSD-G-DP (Multiple Program Single Data - Grid - Data Parallel)



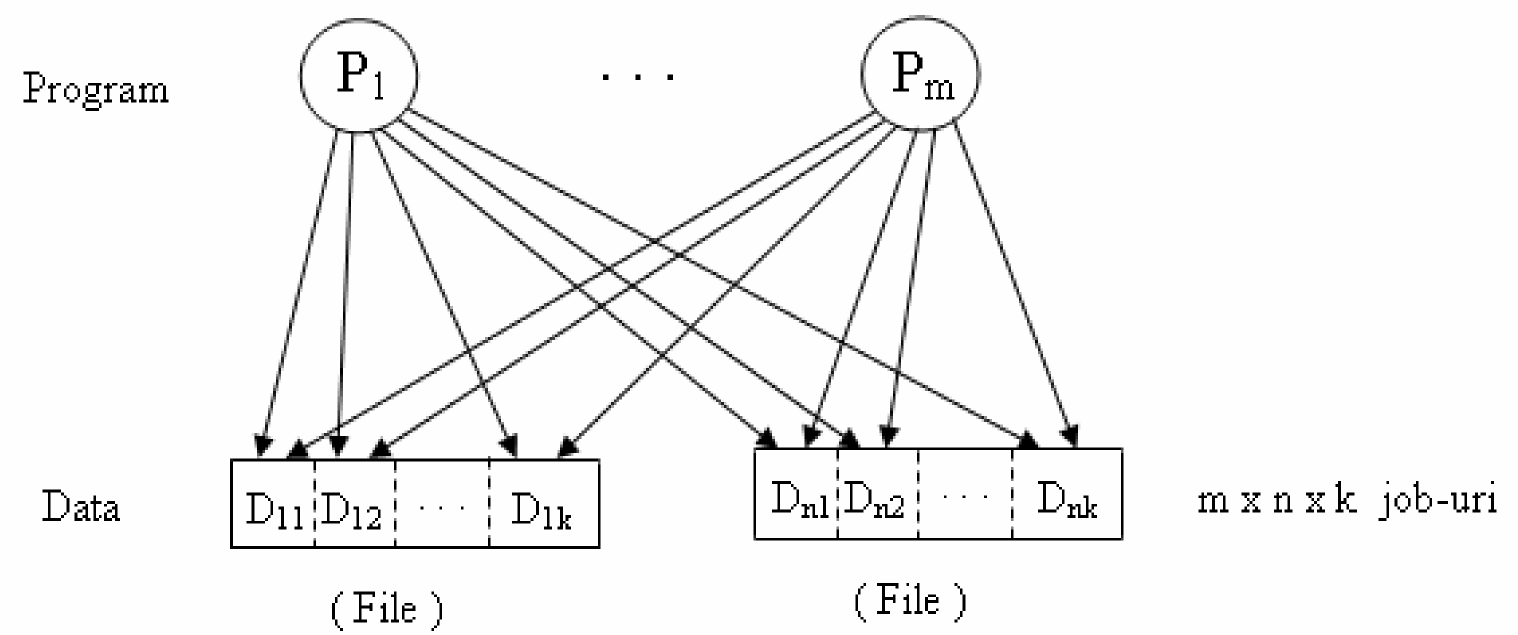
Taxonomy (10)

- MPMD-G (Multiple Program Multiple Data - Grid)



Taxonomy (11)

- MPMD-G-DP (Multiple Program Multiple Data-Grid-Data Parallel)

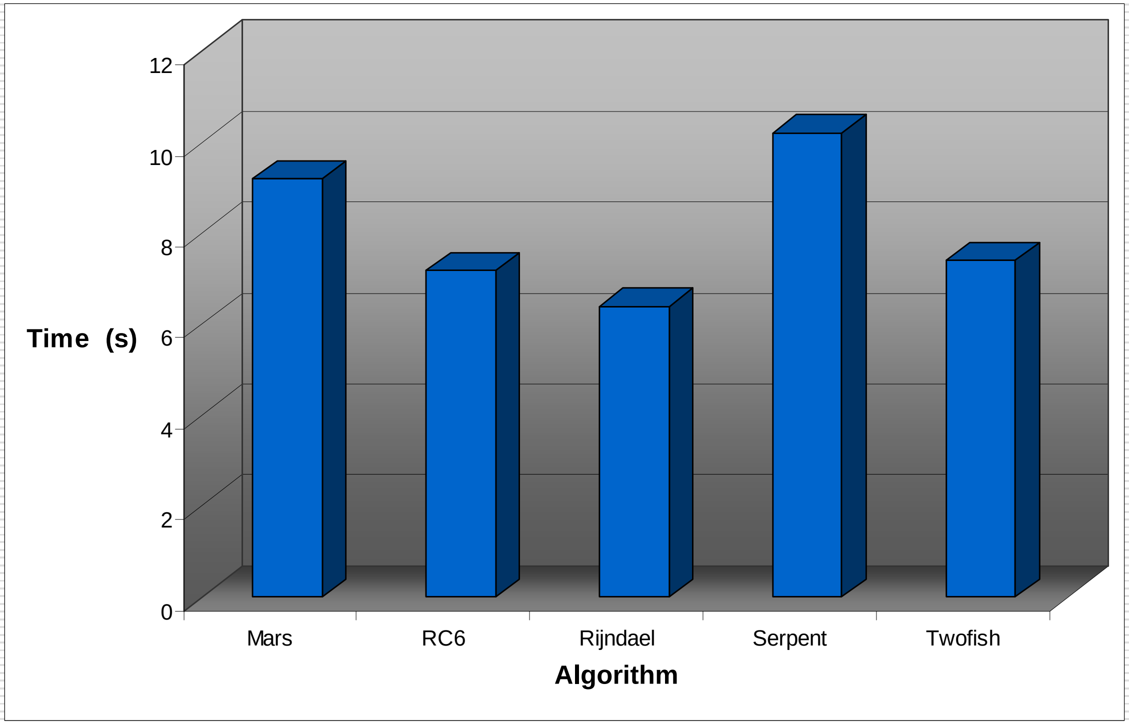


Cryptographic & Cryptanalitic Algorithms

- Block ciphers (all AES finalists)
- Stream ciphers (RC4)
- Public key ciphers (RSA)
- Hash functions (SHA-1, SHA-2)
- Random number generators (NIST, Diehard)
- Random number tests (NIST, Diehard)

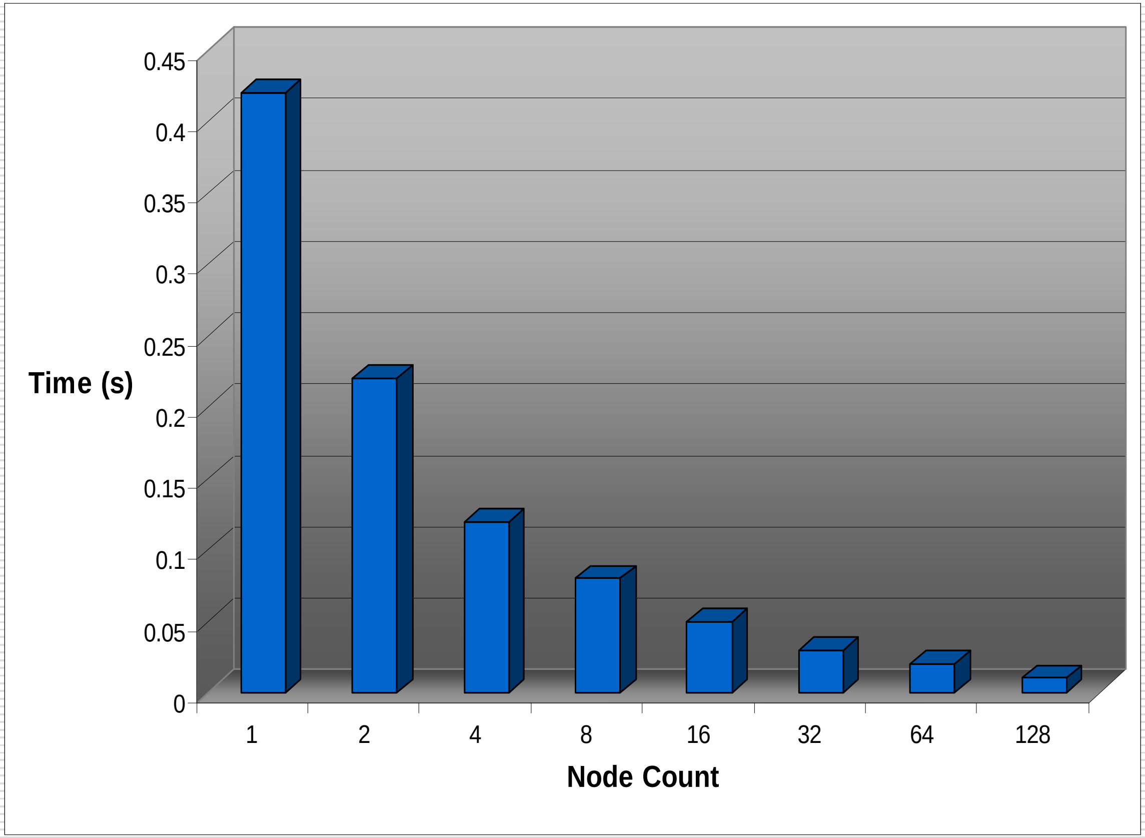
Experimental Results

- Block ciphers:
  - Mars
  - RC6
  - Rijndael
  - Serpent
  - Twofish



Experimental Results (2)

- □ Block ciphers:
- □ Rijndael - in data parallel, grid based execution mode

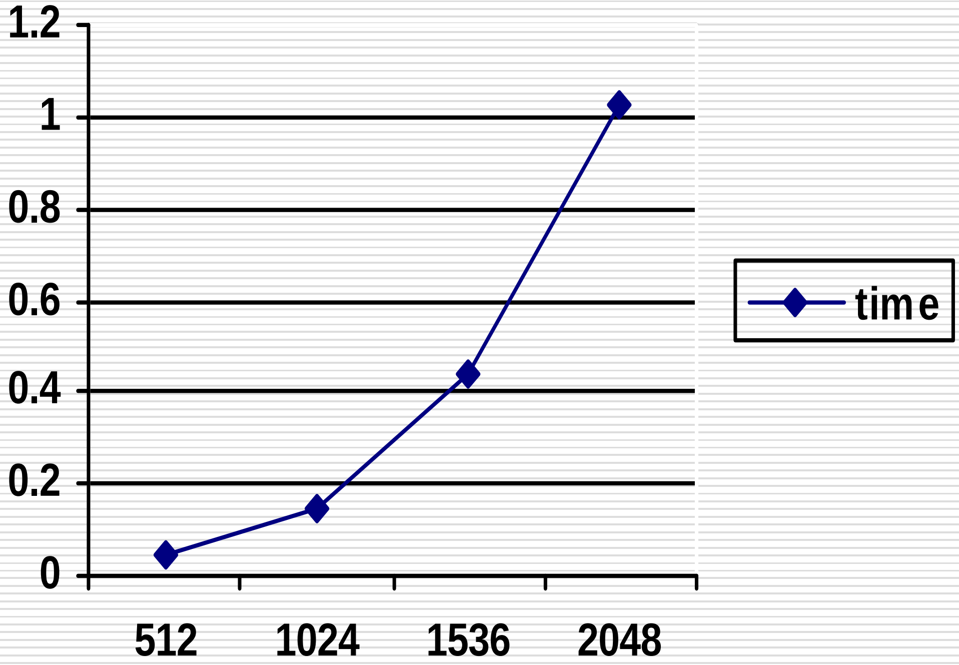


Experimental Results (3)

- Stream ciphers:
  - RC4
- **Not suitable** for data parallel, grid based execution
- Inherently sequential
- Each byte depends on all previous bytes
- Can be used, but not in data parallel modes

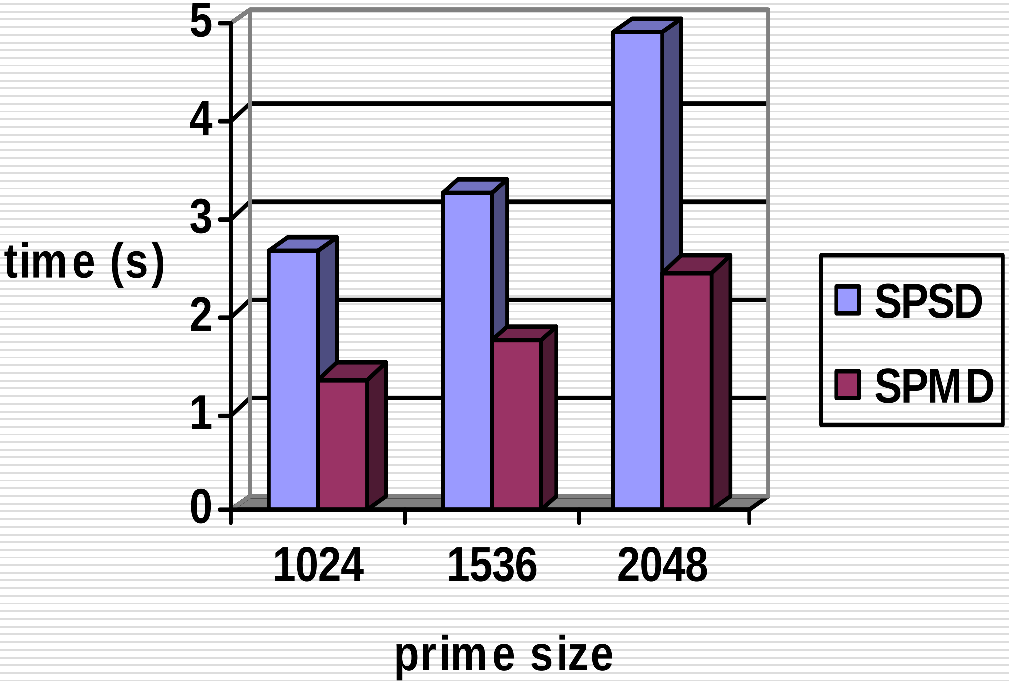
Experimental Results (4)

- Public key ciphers:
  - RSA
- Most time consuming operation is key-pair generation



Experimental Results (5)

- Public key ciphers:
  - RSA
- Fortunately key-pair generation can be parallelized



Experimental Results (6)

- Hash functions:
  - SHA-1
  - SHA-2
- **Not suitable** for data parallel, grid based execution
- Inherently sequential
- Can be used, but not in data parallel modes

Experimental Results (7)

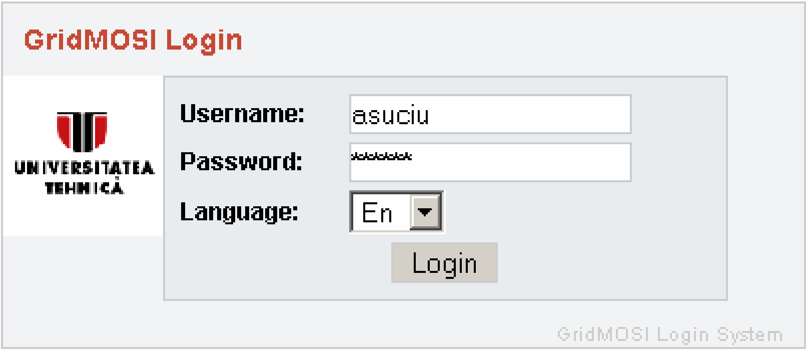
- Random number generators:
  - Linear-Congruential
  - Blum-Blum-Shub
  - Micali-Schnorr
  - Modular-Exponentiation
  - Quadratic-Congruential-1,2
  - Cubic-Congruential
  - XOR
  - Mersenne Twister
- **Extremely suitable** for data parallel, grid based execution

Experimental Results (9)

- Random number testing:
  - NIST tests (16)
  - Diehard tests (15)
- Some tests are very time consuming (ex: Fourier spectral test)
- **Extremely suitable** for data parallel, grid based execution

Web interface

- Authentication



GridMOSI Login

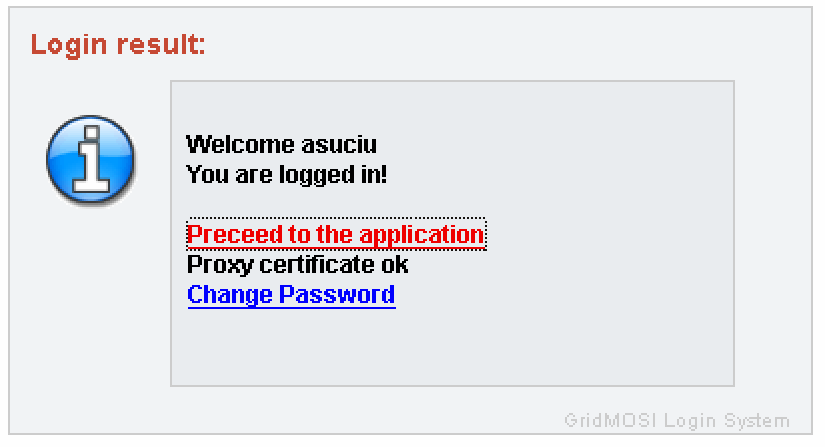
Username: asuciu

Password: ******

Language: En

Web interface

- Validation



Login result:

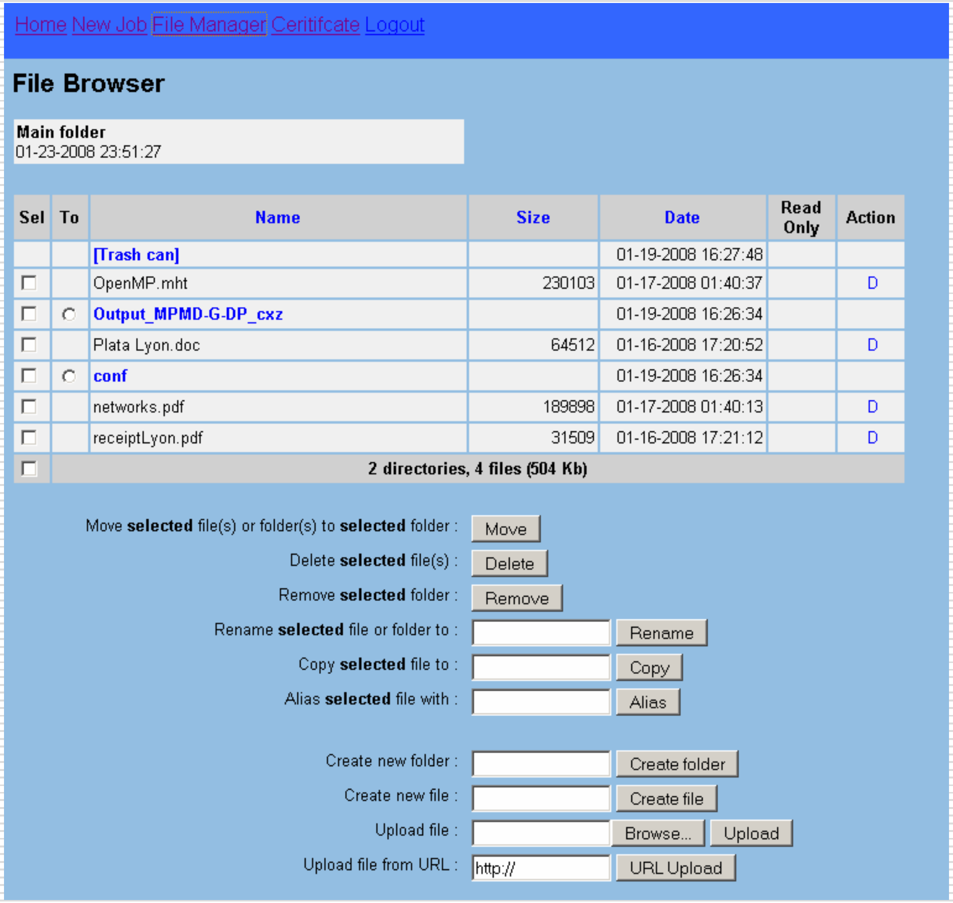
Welcome asuciu
You are logged in!

Preceed to the application
Proxy certificate ok
Change Password

GridMOSI Login System

Web interface

File transfer



File Browser

Main folder
01-23-2008 23:51:27

Sel	To	Name	Size	Date	Read Only	Action
		[Trash can]		01-19-2008 16:27:48		
□		OpenMP.mht	230103	01-17-2008 01:40:37		D
□	○	**Output_MPMD-G-DP_cxz**		01-19-2008 16:26:34		
□		Plata Lyon.doc	64512	01-16-2008 17:20:52		D
□	○	**conf**		01-19-2008 16:26:34		
□		networks.pdf	189898	01-17-2008 01:40:13		D
□		receiptLyon.pdf	31509	01-16-2008 17:21:12		D
□	**2 directories, 4 files (504 Kb)**					

Move **selected** file(s) or folder(s) to **selected** folder : Move

Delete **selected** file(s) : Delete

Remove **selected** folder : Remove

Rename **selected** file or folder to : Rename

Copy **selected** file to : Copy

Alias **selected** file with : Alias

Create new folder : Create folder

Create new file : Create file

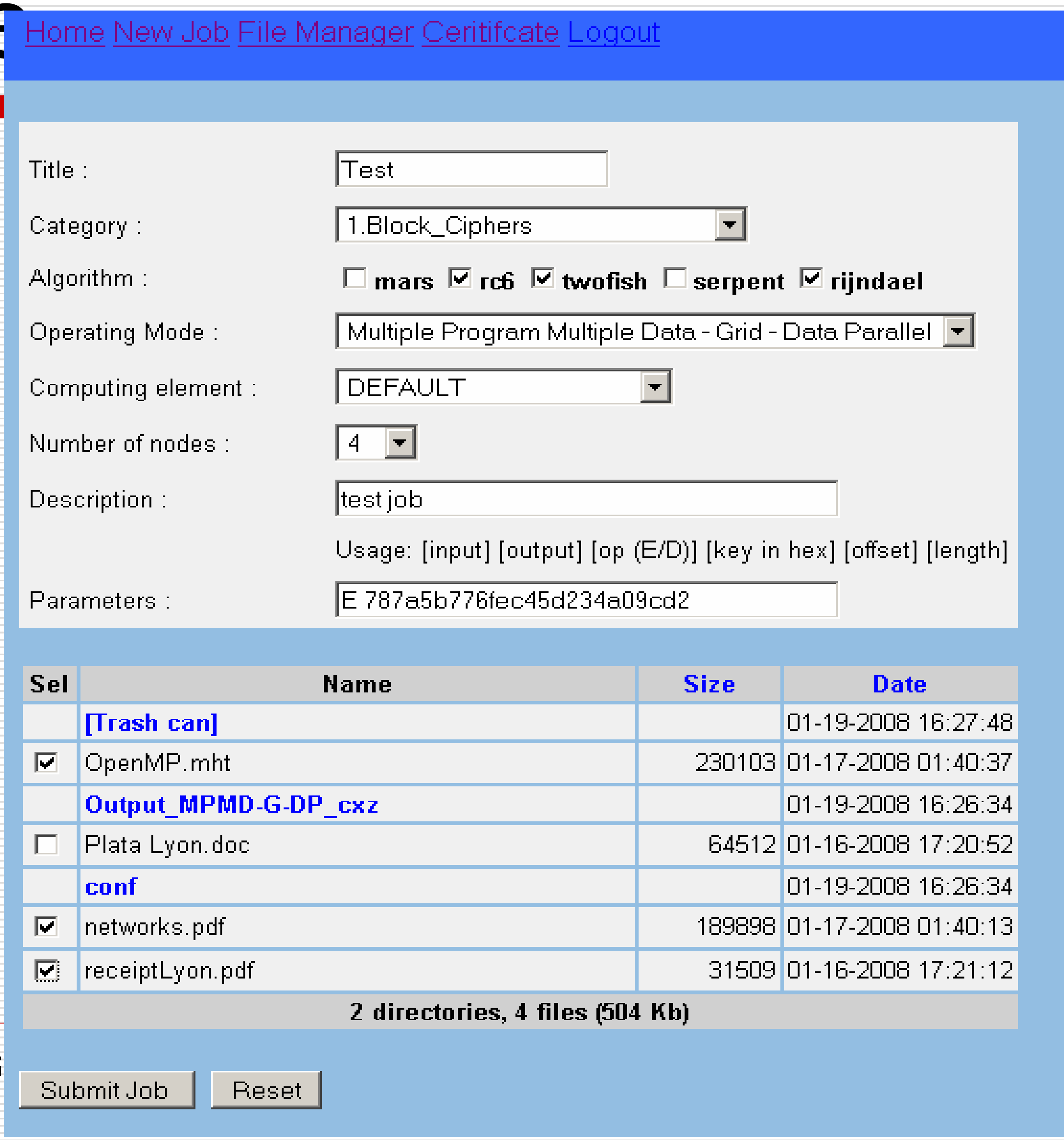
Upload file : Browse... Upload

Upload file from URL : http:// URL Upload

Web interface

- □ Encrypting

MPMD-G-DP



Title : Test

Category : 1.Block_Ciphers

Algorithm : □ mars ☑ rc6 ☑ twofish □ serpent ☑ rijndael

Operating Mode : Multiple Program Multiple Data - Grid - Data Parallel

Computing element : DEFAULT

Number of nodes : 4

Description : test job

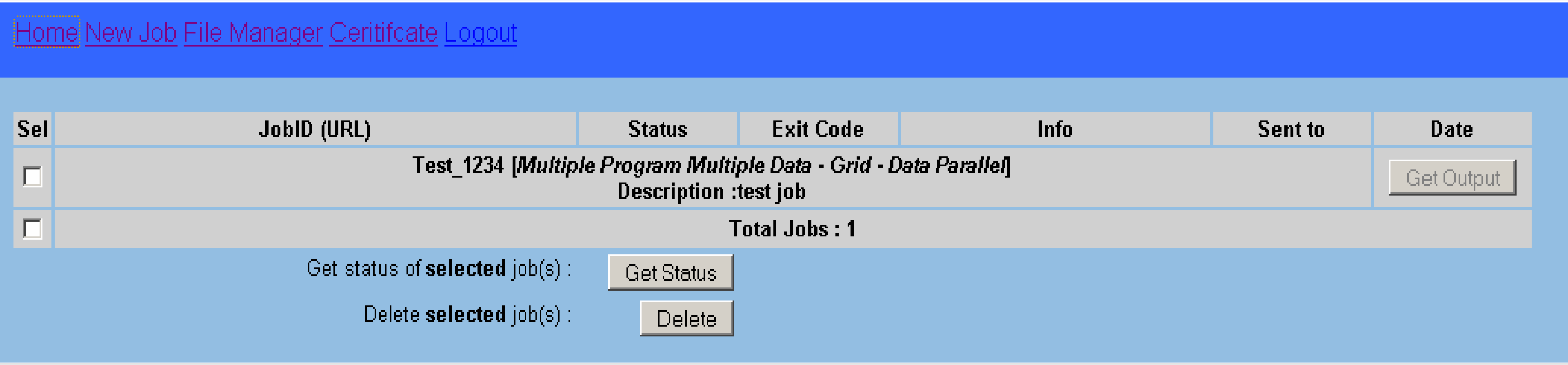
Usage: [input] [output] [op (E/D)] [key in hex] [offset] [length]

Parameters : E 787a5b776fec45d234a09cd2

Sel	Name	Size	Date
	[Trash can]		01-19-2008 16:27:48
☑	OpenMP.mht	230103	01-17-2008 01:40:37
	Output_MPMD-G-DP_cxz		01-19-2008 16:26:34
□	Plata Lyon.doc	64512	01-16-2008 17:20:52
	conf		01-19-2008 16:26:34
☑	networks.pdf	189898	01-17-2008 01:40:13
☑	receiptLyon.pdf	31509	01-16-2008 17:21:12
2 directories, 4 files (504 Kb)			

Web interface

- List of submitted jobs



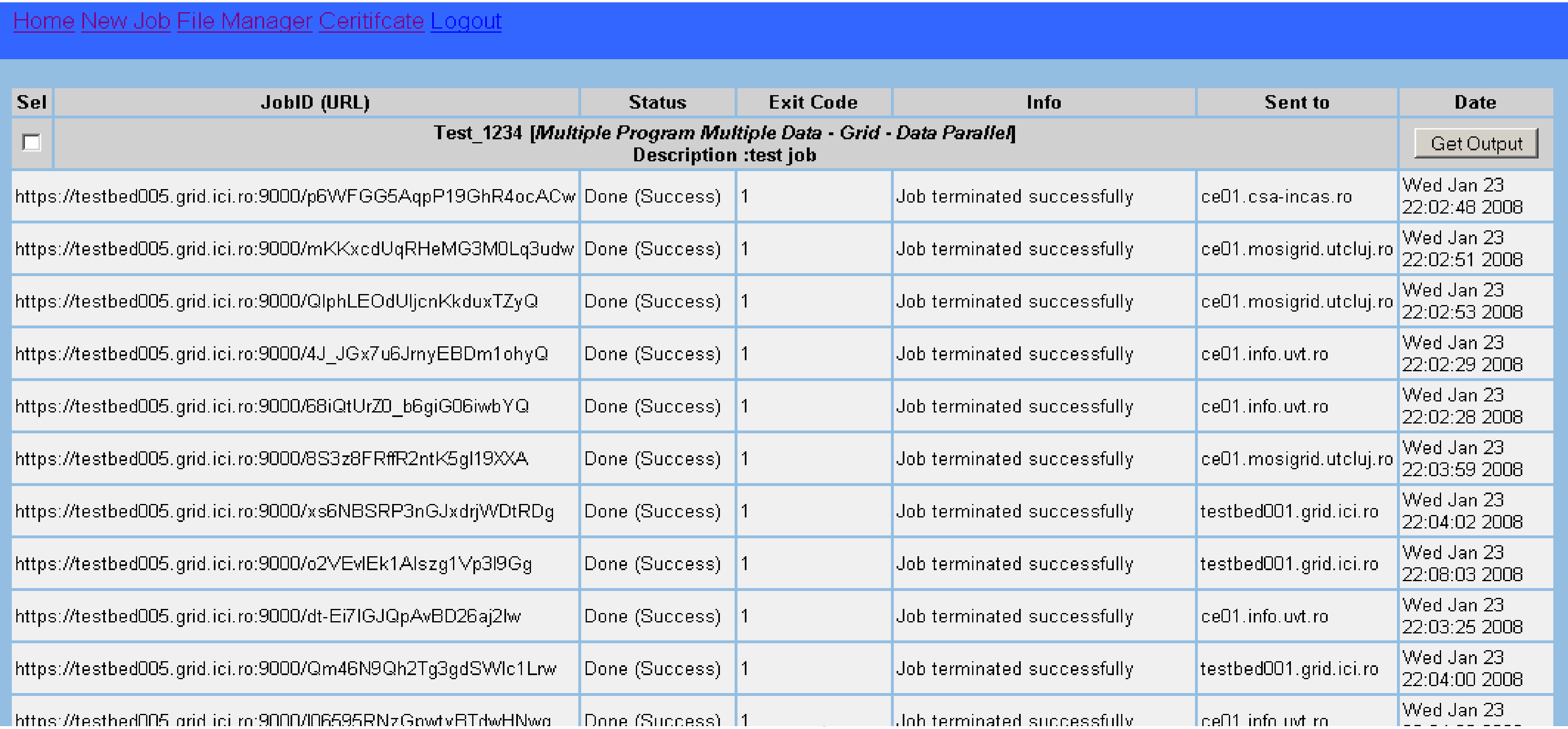
Sel	JobID (URL)	Status	Exit Code	Info	Sent to	Date
☐	Test_1234 [*Multiple Program Multiple Data - Grid - Data Parallel*] Description :test job					Get Output
☐	Total Jobs : 1					

Get status of **selected** job(s) : Get Status

Delete **selected** job(s) : Delete

Web interface

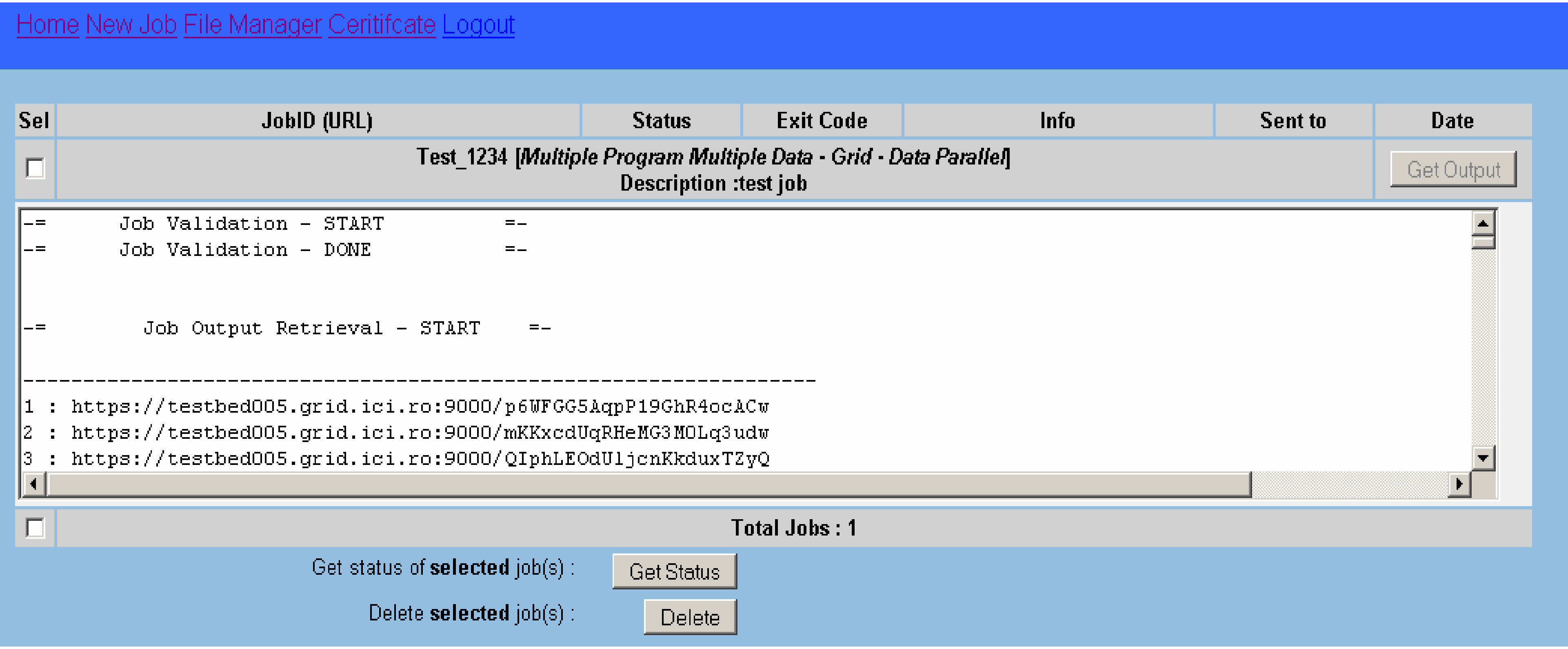
- Get status



Sel	JobID (URL)	Status	Exit Code	Info	Sent to	Date
□	**Test_1234 [*Multiple Program Multiple Data - Grid - Data Parallel*]** **Description :test job**					Get Output
	https://testbed005.grid.ici.ro:9000/p6WFGG5AqpP19GhR4ocACw	Done (Success)	1	Job terminated successfully	ce01.csa-incas.ro	Wed Jan 23 22:02:48 2008
	https://testbed005.grid.ici.ro:9000/mKKxcdUqRHeMG3M0Lq3udw	Done (Success)	1	Job terminated successfully	ce01.mosigrid.utcluj.ro	Wed Jan 23 22:02:51 2008
	https://testbed005.grid.ici.ro:9000/QIphLEOdUljcnKkduxTZyQ	Done (Success)	1	Job terminated successfully	ce01.mosigrid.utcluj.ro	Wed Jan 23 22:02:53 2008
	https://testbed005.grid.ici.ro:9000/4J_JGx7u6JrnyEBDm1ohyQ	Done (Success)	1	Job terminated successfully	ce01.info.uvt.ro	Wed Jan 23 22:02:29 2008
	https://testbed005.grid.ici.ro:9000/68iQtUrZ0_b6giG06iwbYQ	Done (Success)	1	Job terminated successfully	ce01.info.uvt.ro	Wed Jan 23 22:02:28 2008
	https://testbed005.grid.ici.ro:9000/8S3z8FRffR2ntK5gl19XXA	Done (Success)	1	Job terminated successfully	ce01.mosigrid.utcluj.ro	Wed Jan 23 22:03:59 2008
	https://testbed005.grid.ici.ro:9000/xs6NBSRP3nGJxdrjWDtRDg	Done (Success)	1	Job terminated successfully	testbed001.grid.ici.ro	Wed Jan 23 22:04:02 2008
	https://testbed005.grid.ici.ro:9000/o2VEvlEk1Alszg1Vp3l9Gg	Done (Success)	1	Job terminated successfully	testbed001.grid.ici.ro	Wed Jan 23 22:08:03 2008
	https://testbed005.grid.ici.ro:9000/dt-Ei7IGJQpAvBD26aj2lw	Done (Success)	1	Job terminated successfully	ce01.info.uvt.ro	Wed Jan 23 22:03:25 2008
	https://testbed005.grid.ici.ro:9000/Qm46N9Qh2Tg3gdSWlc1Lrw	Done (Success)	1	Job terminated successfully	testbed001.grid.ici.ro	Wed Jan 23 22:04:00 2008
	https://testbed005.grid.ici.ro:9000/l06595RNzGpwtvBTdwHNwg	Done (Success)	1	Job terminated successfully	ce01.info.uvt.ro	Wed Jan 23

Web interface

- □ Get output



Sel	JobID (URL)	Status	Exit Code	Info	Sent to	Date
□	Test_1234 [*Multiple Program Multiple Data - Grid - Data Parallel*] **Description :test job**					Get Output

```
-=      Job Validation - START          =-
-=      Job Validation - DONE           =-


-=        Job Output Retrieval - START    =-


------------------------------------------------------------------
1 : https://testbed005.grid.ici.ro:9000/p6WFGG5AqpP19GhR4ocACw
2 : https://testbed005.grid.ici.ro:9000/mKKxcdUqRHeMG3MOLq3udw
3 : https://testbed005.grid.ici.ro:9000/QIphLEOdUljcnKkduxTZyQ
```

□ **Total Jobs : 1**

Get status of **selected** job(s) : Get Status

Delete **selected** job(s) : Delete

Papers (2007)

- A. Suciu, R Potolea, *“Towards a GridMOSI Library”*, 6th RoEduNet International Conference, 23-24 Nov. 2007, Craiova, Romania, ISBN 987-973-746-581-8, pp. 74-79.
- R. Potolea, A. Suciu, A. Măşcăşan, *"Benchmarking the Gridmosi Library"*, eChallenges 2007, 24-27 Oct. 2007, The Hague, Netherlands, ISBN 978-1-58603-801-4, pp. 138-145.

Papers (2007)

- R. Potolea, A. Suciu, *"Finding the Optimal Read Buffer Size for Grid Applications"*, 9th International Symposium on Symbolic and Numeric Algorithms for Scientific Computing Timisoara, Romania September 26-29, 2007, Workshop on Grid Computing Applications Development, pp. 51-54.
- A. Suciu, R. Potolea, *"Cryptographic and Cryptanalytic Algorithms for Grid Applications"*, 2007 IEEE International Conference on Intelligent Computer Communication and processing, 6-7 September 2007, Cluj-Napoca, Romania, Workshop on Grid Computing (WGC).

Conclusion

- Several categories of cryptographic algorithms were analyzed, implemented and tested for grid-based execution
- A taxonomy for grid-based execution was developed – 8 execution modes
- Experimental results show substantial performance improvements (especially in data parallel modes)
- A “library” of algorithms was developed and is available for grid applications

Questions

- Thank you for your attention
- Questions, please?