

# Comparison of Factorization Algorithms for Large Numbers

## *Project Specification*

Sashisu Bajracharya and Han Sang

Factoring a large integer into prime factors is one of the challenging tasks in cryptanalysis both in terms of computational complexity and the practical implementation. The widely used public key cryptosystem RSA mainly depends on this characteristic and recently there have been much focus on development and implementation of various factorization algorithms. Of these currently available algorithms, Number Field Sieve algorithm is known to be the most efficient with a large integer number (110 digits or more) and the project will research on two of the implementations proposed by Bernstein and the team of Shamir and Tromer. Our goal is to analyze each proposed implementation for its feasibility, and to develop high level hardware design to compare the difference of the two in terms of performance and cost.

1. Algorithms and implementations to be compared:
  - Bernstein's Factorization Circuit
  - Shamir and Tromer's Factorization Circuit
2. We are going to understand and analyze the two proposed circuits and build basic hardware implementation blocks. Furthermore, we are going to compare
  - a. Performance
    - Computational Complexity in number of operations
    - Complexity of subtasks
  - b. Cost
    - Computational Cells estimates for each subtask and for total circuit
    - Memory requirements for subtasks and for total circuit
  - c. Feasibility
    - Use of reconfigurable computer
    - Number of processors and FPGA estimates
  - d. Functionality
    - Scalability
3. Tentative list of questions:
  - a. How can the two conceptual implementations be realized in hardware?
  - b. What is the performance and cost of each implementation?
  - c. What are the subtasks of each algorithm and how can they be realized?
  - d. How feasible is the implementation of both algorithms to factor a reasonably large integer number?
4. Procedure for verifying the results of our investigation:

Report will be verified based on information from the papers published by the original authors, other related journal and conference papers on the factorization and the books in the field.
5. Tentative table of contents:
  - a. Introduction
  - b. Factorization Algorithms
    - Bernstein

- Shamir and Tromer
- c. High Level Design
  - Block Diagrams of the circuit
  - Design of basic components
  - Low level gate structure
- d. Comparison and analysis
  - Performance
  - Cost
  - Feasibility and Functionality
- e. Conclusion
- f. References

6. Tentative Time Schedule:

Sept 28-Oct3	Define the task
Oct 4	Final specification submission
Oct 5-15	Learn number theory principles and understand the algorithms
Oct 15	First progress report
Oct 15-29	Continue the study of algorithms and analyze implementation issues
Oct 29	Second Progress Report
Oct 29-Nov12	Comparison of the two algorithms and develop basic building blocks
Nov 12	Third progress report
Nov 12 – 22	Write draft report of findings and viewgraphs
Nov 22 – Dec2	Finish draft report and Viewgraphs
Dec 3	Final progress report with Draft
Dec 6	Project Report submission
Dec 9	Review reports
Dec 12	Oral presentation and revised report

7. Possible areas of change:

- Analysis criteria
- Final Report form

8. List of Literature:

RSA Security, *The new RSA factoring challenge*, web page, Jan. 2003,  
<http://www.rsasecurity.com/rsalabs/challenges/factoring/>

Factoring Large Numbers: Fun or Applied Science? <http://www.cwi.nl/publications/annual-reports/1999/AR/PDF/factoring.pdf>

A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone, "Handbook of Applied Cryptology," chapters 3.2.6-3.2.7, pp. 95-98.

D. J. Bernstein. *Circuits for integer factorization: a proposal*. <http://cr.yp.to/papers/nfscircuit.pdf>

Arjen K. Lenstra, Adi Shamir, Jim Tomlinson, Eran Tromer, *Analysis of Bernstein's Factorization Circuit* proc. Asiacrypt 2002, LNCS 2501, 1-26, Springer-Verlag, 2002 [\[ps.gz\]](#) [\[pdf\]](#) [\[html\]](#)  
<http://www.wisdom.weizmann.ac.il/~tromer/>

Adi Shamir, Eran Tromer, *On the cost of factoring RSA-1024*, RSA CryptoBytes, vol. 6 no. 2, 10-19, 2003 [\[ps.gz\]](#) [\[pdf\]](#) <http://www.wisdom.weizmann.ac.il/~tromer/>

Arjen K. Lenstra, Eran Tromer, Adi Shamir, Wil Kortsmit, Bruce Dodson, James Hughes, Paul Leyland, *Factoring estimates for a 1024-bit RSA modulus*, proc. Asiacrypt 2003, Springer-Verlag, to appear. [\[ps.gz\]](#) [\[pdf\]](#) <http://www.wisdom.weizmann.ac.il/~tromer/>

Adi Shamir, Eran Tromer, *Factoring Large Numbers with the TWIRL Device*, proc. Crypto 2003, LNCS 2729, 1-26, Springer-Verlag, 2003 [\[ps.gz\]](#) [\[pdf\]](#) (revised 2003-06-28) [\[details\]](#)  
<http://www.wisdom.weizmann.ac.il/~tromer/>

Adi Shamir, *Factoring large numbers with the TWINKLE device (extended abstract)*, proc. CHES'99, LNCS 1717 2-12, Springer-Verlag, 1999

Arjen K. Lenstra, Adi Shamir, *Analysis and optimization of the TWINKLE factoring device*, proc. Eurocrypt 2002, LNCS 1807 35-52, Springer-Verlag, 2000

Willi Geiselmann, Rainer Steinwandt, *A dedicated sieving hardware*, proc. PKC 2003, LNCS 2567 254-266, Springer-Verlag, 2002

Willi Geiselmann, Rainer Steinwandt, *Hardware to solve sparse systems of linear equations over GF(2)*, proc. CHES 2003, LNCS, Springer-Verlag.

Hea Joung Kim and William H. Mangione-Smith, *Factoring Large Numbers with Programmable Hardware* (Presentation) UCLA Electrical Engineering Dept. [kimmer,billms@icsl.ucla.edu](mailto:kimmer,billms@icsl.ucla.edu)  
[http://klabs.org/richcontent/MAPLDCon99/Presentations/D5A\\_Kim\\_S.PDF](http://klabs.org/richcontent/MAPLDCon99/Presentations/D5A_Kim_S.PDF)

A.K. Lenstra, H.W. Lenstra, Jr., (eds.), *The development of the number field sieve*, Lecture Notes in Math. 1554, Springer-Verlag 1993

D. Coppersmith, *Modifications to the number field sieve*, Journal of Cryptology 6 (1993) 169-180

S. Cavallar, B. Dodson, A.K. Lenstra, W. Lioen, P.L. Montgomery, B. Murphy, H.J.J. te Riele, et al., *Factorization of a 512-bit RSA modulus*, Proceedings Eurocrypt 2000, LNCS 1807, Springer-Verlag 2000, 1-17

D. Coppersmith, *Solving homogeneous linear equations over GF(2) via block Wiedemann algorithm*, Math. Comp. bf 62 (1994) 333-350

A.K. Lenstra, H.W. Lenstra, Jr., *Algorithms in number theory*, chapter 12 in *Handbook of theoretical computer science, Volume A, algorithms and complexity* (J. van Leeuwen, ed.), Elsevier, Amsterdam (1990)

P.L. Montgomery, *A block Lanczos algorithm for finding dependencies over GF(2)*, Proceedings Eurocrypt'95, LNCS 925, Springer-Verlag 1995, 106-120

C.P. Schnorr, A. Shamir, *An Optimal Sorting Algorithm for Mesh Connected Computers*, Proceedings 16th ACM Symposium on Theory of Computing, 255-263, 1986

D. Wiedemann, *Solving sparse linear equations over finite fields*, IEEE Transactions on Information Theory, **IT-32** (1986), 54-62

C. D. Thompson and H. T. Kung, "*Sorting on a mesh-connected parallel computer*", Communications of the ACM 20, 1977, pp 263-271.

E. Kaltofen, A. Lobo , *Distributed Matrix-Free Solution of Large Sparse Linear Systems over Finite Fields* Algorithmica 24 (1999), 331-348. MR 2000b:65093

Manfred Schimpler, *Fast sorting on the instruction systolic array*, Report 8709, Christian Albrecht University Kiel, 1987.

<http://www.crypto-world.com/FactorPapers.html>

<http://www.crypto-world.com/FactorCode.html>

<http://www.nfsnet.org/>

<http://citeseer.nj.nec.com/398050.html>

<http://www.crypto-world.com/FactorLinks.html>