

PROJECT ADMINISTRATION DATA SHEET

ORIGINAL

REVISION NO. \_\_\_\_\_

Project No. G-36-658

DATE: 8/20/81

Raymond Miller

Project Director: Richard Demillo, Kimberly King, & School/Lab ICS

Sponsor: National Science Foundation; Washington, D. C. 20550

Type Agreement: Grant No. MCS-8103608

Award Period: From 7/15/81 To 12/31/83 (Performance) \_\_\_\_\_ (Reports)

Sponsor Amount: \$86,986 Contracted through:

Cost Sharing: \$10,000 (G-36-345) GTRI/GIT

Title: Models of Computation and Algorithms

ADMINISTRATIVE DATA

OCA CONTACT Leamon R. Scott x4820

- 1) Sponsor Technical Contact: Ken K. Curtis, NSF Program Officer; Computer Science Section  
Division of Mathematical and Computer Sciences; Directorate for Mathematical &  
Physical Sciences; NSF; Washington, D. C. 20550 202-357-9747
- 2) Sponsor Admin./Contractual Contact: Myra Galinn, Grants Official; Section II MPS/STIA  
Branch; Division of Grants & Contracts; Directorate for Administration; NSF;  
Washington, D. C. 20550 Tel. 202-357-9671

Reports: See Deliverable Schedule Security Classification: \_\_\_\_\_

Defense Priority Rating: \_\_\_\_\_

RESTRICTIONS

See Attached NSF Supplemental Information Sheet for Additional Requirements

Travel: Foreign travel must have prior approval - Contact OCA in each case. Domestic  
travel requires sponsor approval where total will exceed greater of \$500 or  
125% of approved proposal budget category.

Equipment: Title vests with GIT

COMMENTS: \* Includes the usual six (6) month unfunded flexibility period.

COPIES TO:

- Administrative Coordinator
- Research Property Management
- Accounting Office
- Research Security Services
- Reports Coordinator (OCA)
- Legal Services (OCA)
- EES Research Public Relat
- Project File (OCA)
- Other:

SPONSORED PROJECT TERMINATION/CLOSEOUT SHEET

Date 6-15-87

Project No. G-36-658

School/~~XXX~~ ICS

Includes Subproject No.(s) N/A

Project Director(s) R.A. DeMillo

GTRC / ~~SKK~~

Sponsor National Science Foundation, Washington, D.C. 20550

Title Models of Computation and Algorithms

Effective Completion Date: 12/31/84 (Performance) 3/31/85 (Reports)

Grant/Contract Closeout Actions Remaining:

- None
- Final Invoice or Final Fiscal Report
- Closing Documents
- Final Report of Inventions
- Govt. Property Inventory & Related Certificate
- Classified Material Certificate
- Other \_\_\_\_\_

Continues Project No. \_\_\_\_\_

Continued by Project No. \_\_\_\_\_

COPIES TO:

- Project Director
- Research Administrative Network
- Research Property Management
- Accounting
- Procurement/GTRI Supply Services
- Research Security Services
- Reports Coordinator (OCA)

- Library
- GTRC
- ~~Research Communications~~
- Project File
- Other Duane H.
- Angela DuBose
- Russ Embry

**PROPOSAL TO THE NATIONAL SCIENCE FOUNDATION**  
Cover Page

FOR CONSIDERATION BY NSF ORGANIZATIONAL UNIT (Indicate the most specific unit known, i.e. program, division, etc.)		IS THIS PROPOSAL BEING SUBMITTED TO ANOTHER FEDERAL AGENCY? Yes ___ No <u>X</u> ; IF YES, LIST ACRONYM(S):	
Theoretical Computer Science			
PROGRAM ANNOUNCEMENT/SOLICITATION NO.:	CLOSING DATE (IF ANY):		
NAME OF SUBMITTING ORGANIZATION TO WHICH AWARD SHOULD BE MADE (INCLUDE BRANCH/CAMPUS/OTHER COMPONENTS)			
Georgia Tech Research Institute			
ADDRESS OF ORGANIZATION (INCLUDE ZIP CODE)			
Atlanta, Georgia 30332			
TITLE OF PROPOSED PROJECT			
Research in Models of Computation and Algorithms			
REQUESTED AMOUNT	PROPOSED DURATION	DESIRED STARTING DATE	
\$99,825	12 months	January 1, 1983	
PI/PD DEPARTMENT	PI/PD ORGANIZATION	PI/PD PHONE NO.	
Information and Computer Science	Georgia Institute of Technology Atlanta, Georgia 30332	(404) 894-3180	
PI/PD NAME	SOCIAL SECURITY NO.*	DATE OF HIGHEST DEGREE ACHIEVED	MALE* FEMALE*
Richard A. DeMillo	469-48-0892	Ph.D. 1972	X
ADDITIONAL PI/PD			
Kimberly N. King	297-48-6607	Ph.D. 1980	X
ADDITIONAL PI/PD			
Raymond E. Miller	394-24-7522	Ph.D. 1957	X
ADDITIONAL PI/PD			
ADDITIONAL PI/PD			
FOR RENEWAL OR CONTINUING AWARD REQUEST, LIST PREVIOUS AWARD NO.:		IF SUBMITTING ORGANIZATION IS A SMALL BUSINESS CONCERN, CHECK HERE <input type="checkbox"/> (See CFR Title 13, Part 121 for Definitions)	
MCS-8103608		NA	
* Submission of SSN and other personal data is voluntary and will not affect the organization's eligibility for an award. However, they are an integral part of the NSF information system and assist in processing proposals. SSN solicited under NSF Act of 1950, as amended.			
CHECK APPROPRIATE BOX(ES) IF THIS PROPOSAL INCLUDES ANY OF THE ITEMS LISTED BELOW: NA			
<input type="checkbox"/> Animal Welfare	<input type="checkbox"/> Human Subjects	<input type="checkbox"/> National Environmental Policy Act	
<input type="checkbox"/> Endangered Species	<input type="checkbox"/> Marine Mammal Protection	<input type="checkbox"/> Research Involving Recombinant DNA Molecules	
<input type="checkbox"/> Historical Sites	<input type="checkbox"/> Pollution Control	<input type="checkbox"/> Proprietary and Privileged Information	
PRINCIPAL INVESTIGATOR/ PROJECT DIRECTOR	AUTHORIZED ORGANIZATIONAL REP.	OTHER ENDORSEMENT (optional)	
NAME	NAME	NAME	NAME
Richard A. DeMillo	G. D. Hutchison	Kimberly N. King	Raymond E. Miller
SIGNATURE	SIGNATURE	SIGNATURE	SIGNATURE
<i>[Signature]</i>			
TITLE	TITLE	TITLE	TITLE
Professor	Contracting Officer	Assistant Professor	Professor & Director
DATE	DATE	DATE	DATE
5-17-82	5-27-82	5-17-82	5-17-82



REQUEST FOR INCREMENTAL FUNDING FOR  
CONTINUING NSF GRANT No. MCS-81-03608

BRIEF SUMMARY OF SCIENTIFIC PROGRESS

Richard A. DeMillo, Co-Principal Investigator

Most of my work this year has concentrated on models of distributed and parallel computation. Of particular interest has been the exploration of distributed problems in which the underlying model of computation contains cryptographic transformations as explicit operations. The major results of this work have been reported in [1,2]. This grant has also supported a Ph.D. student, Michael J. Merritt, whose dissertation (expected completion: July, 1982) will deal with cryptographic protocols as distributed algorithms.

**Byzantine Generals:** The Byzantine Generals' Problem is a communications problem involving  $k$  processors,  $m$  of which may be faulty. Each processor  $P_i$  has a private value  $v_i$  to communicate. In synchronous rounds the processors send messages to obtain a vector of values  $V_i$  such that  $V_i = v_i$  if  $P_i$  is a non-faulty processor. It was previously known that no solution is possible if  $k < 2m+1$  provided that processors do not have the power to "sign" their messages. Signatures provide a sort of encryption capability and it was also known that with encryption available, there is a solution for any number of faulty processors. Upper and lower bounds on the number of communications rounds needed for a solution remained open for some time. In 1981, Mike Fischer, Nancy Lynch and Leslie Lamport proved that  $m+1$  rounds are necessary and sufficient in the absence of encryption.

Our result resolves the lower bound problem in the model in which arbitrary encryption is available. In this model  $m+1$  rounds are required.

**Protocol Modelling:** As protocols become more complex, their correctness properties become more difficult to establish and there are no techniques available to prove the impossibility of solutions to certain protocol problems. Our progress in this area has been to isolate a general model of protocols and define a technique for establishing certain security properties. Security is defined with respect to a model of communication and inference. By using model-theoretic techniques, we can define a class of protocols with the following behavior. If an "enemy" tries to determine whether or not a set of properties  $S$  is true of the system, he is forced to test  $S$  against his own inferences and those messages he can derive from the set of messages he has received. Suppose there is a renaming of objects in the systems which causes (from the enemy's point of view) the protocol to behave in an entirely equivalent manner but which is undetectable to him. If in this renaming  $S$  is false, then the enemy cannot infer  $S$  from his current knowledge of the state of the system, i.e.,  $S$  is logically independent of his knowledge. This method of hidden automorphisms has been applied to the analysis of several protocols and has been extended to the case of randomness. These results are reported in more detail in [2].

1. R. DeMillo, N. Lynch and M. Merritt, "The Design and Analysis of Cryptographic Protocols," Crypto 81, Santa Barbara, August, 1981.
2. R. DeMillo, N. Lynch and M. Merritt, "Cryptographic Protocols," Proceedings of the 14th ACM Symposium of the Theory of Computing, San Francisco, May, 1982.

Kimberly N. King, Co-Principal Investigator

Together with doctoral student Eric Allender, I have been surveying current research in automation-based complexity and concrete complexity. We have identified several interesting problems which we hope to pursue in the near future. Under my direction, Allender has written a paper on multihead finite automata, which he is using to satisfy a departmental requirement. In addition to surveying known results about multihead finite automata, his paper gives improvements of several previously-known theorems and new proofs of others.

I have also begun to develop a research interest in algorithms for solving computer graphics problems. I intend to develop this interest further during the summer.

Raymond E. Miller, Co-Principal Investigator

Work continued on comparing models of parallel computation that had been started prior to the grant. A revision of a paper "Homomorphisms Between Models of Parallel Computation" by T. Kasai and R.E. Miller was completed. This revision includes new work relating the concepts of "reduction" and "contractions" of other researchers, to the computation system approach developed in this paper. A new area of study has also been initiated investigating formal models for specifying and verifying network protocols. There appear to be many similarities of modelling protocols with our previous studies in parallel computation and synchronization.

ESTIMATE OF UNOBLIGATED FUNDS AT THE END OF THE PERIOD FOR WHICH NSF CURRENTLY IS PROVIDING FUNDS

The School of Information and Computer Science request permission to carry forward approximately \$3,500 of non-personal services monies plus associated overhead costs of \$1,925. The total carry forward amount of \$5,425 represents less than 10% of the current funding increment.

SEE INSTRUCTIONS ON REVERSE BEFORE COMPLETING

Second Year Support (January 1, 1983 - December 31, 1983)

PROPOSAL BUDGET

FOR NSF USE ONLY

ORGANIZATION Georgia Institute of Technology  
School of Information and Computer Science

PROPOSAL NO.	DURATION (MONTHS)	
	Proposed	Granted

PRINCIPAL INVESTIGATOR/PROJECT DIRECTOR  
Richard A. DeMillo, Kimberly N. King, Raymond E. Miller

AWARD NO.		
-----------	--	--

A. SENIOR PERSONNEL: PI/PD, Co-PI's, Faculty and Other Senior Associates  
(List each separately with title; A.6. show number in brackets)

NSF FUNDED PERSON-MOS	FUNDS REQUESTED BY PROPOSER	FUNDS GRANTED BY NSF (IF DIFFERENT)

1. Richard A. DeMillo, Professor	1.2			\$ 6,334	\$
2. Kimberely N. King, Assistant Professor			2.0	6,764	
3. Raymond E. Miller, Professor	1.8			11,588	
4.					
5. ( ) OTHERS (LIST INDIVIDUALLY ON BUDGET EXPLANATION PAGE)					
6. ( 3 ) TOTAL SENIOR PERSONNEL (1-5)	3.0		2.0	24,686	

B. OTHER PERSONNEL (SHOW NUMBERS IN BRACKETS)

1. ( ) POST DOCTORAL ASSOCIATES					
2. ( ) OTHER PROFESSIONALS (TECHNICIAN, PROGRAMMER, ETC.)					
3. ( 2 ) GRADUATE STUDENTS (1/2 time)				22,800	
4. ( ) UNDERGRADUATE STUDENTS					
5. ( 1 ) SECRETARIAL CLERICAL (1/3 time)				4,829	
6. ( ) OTHER					
TOTAL SALARIES AND WAGES (A+B)				52,315	
C. FRINGE BENEFITS (IF CHARGED AS DIRECT COSTS) 22% of applicable salaries & wages				6,493	
TOTAL SALARIES, WAGES AND FRINGE BENEFITS (A+B+C)				58,808	

D. PERMANENT EQUIPMENT (LIST ITEM AND DOLLAR AMOUNT FOR EACH ITEM EXCEEDING \$1,000; ITEMS OVER \$10,000 REQUIRE CERTIFICATION)

NONE

TOTAL PERMANENT EQUIPMENT

E. TRAVEL 1. DOMESTIC (INCL. CANADA AND U.S. POSSESSIONS)				3,000	
2. FOREIGN					

F. PARTICIPANT SUPPORT COSTS

- 1. STIPENDS \$ \_\_\_\_\_
- 2. TRAVEL \_\_\_\_\_
- 3. SUBSISTENCE \_\_\_\_\_
- 4. OTHER \_\_\_\_\_

TOTAL PARTICIPANT COSTS

G. OTHER DIRECT COSTS

1. MATERIALS AND SUPPLIES				1,500	
2. PUBLICATION COSTS/PAGE CHARGES				1,500	
3. CONSULTANT SERVICES					
4. COMPUTER (ADPE) SERVICES					
5. SUBCONTRACTS					
6. OTHER Pro-rated cost of the ICS Comp. Lab (\$7,000)				2,870	
TOTAL OTHER DIRECT COSTS				5,870	

H. TOTAL DIRECT COSTS (A THROUGH G)

67,678

I. INDIRECT COSTS (SPECIFY)

47.5% of H.

TOTAL INDIRECT COSTS

32,147

J. TOTAL DIRECT AND INDIRECT COSTS (H + I)

99,825

K. RESIDUAL FUNDS (IF FOR FURTHER SUPPORT OF CURRENT PROJECTS GPM 252 AND 253)

(NA)

L. AMOUNT OF THIS REQUEST (J) OR (J MINUS K)

\$ 99,825

PI/PD TYPED NAME & SIGNATURE\*

DATE

FOR NSF USE ONLY

INST. REP. TYPED NAME & SIGNATURE\*

DATE

INDIRECT COST RATE VERIFICATION		
Date Checked	Date of Rate Sheet	Initials - DGC

Program



NATIONAL SCIENCE FOUNDATION  
Washington, D.C. 20550

**FINAL PROJECT REPORT**  
NSF FORM 98A

*PLEASE READ INSTRUCTIONS ON REVERSE BEFORE COMPLETING*

**PART I—PROJECT IDENTIFICATION INFORMATION**


1. Institution and Address Georgia Institute of Technology School of Information and Computer Atlanta, Georgia 30332 Science	2. NSF Program <b>Mathematics and Computer Science</b>	3. NSF Award Number <b>MCS-8103608</b>
4. Project Title  <b>Models of Computation and Algorithms</b>	4. Award Period From <b>7/15/81</b> To <b>12/31/84</b>	5. Cumulative Award Amount <b>\$204,694</b>

**PART II—SUMMARY OF COMPLETED PROJECT (FOR PUBLIC USE)**

This grant supported work by Professors R. A. DeMillo, K. N. King, and R. E. Miller as well as several PhD students working with the three professors.

For further information see the final report.

**PART III—TECHNICAL INFORMATION (FOR PROGRAM MANAGEMENT USES)**

ITEM (Check appropriate blocks)	NONE	ATTACHED	PREVIOUSLY FURNISHED	TO BE FURNISHED SEPARATELY TO PROGRAM	
				Check (✓)	Approx. Date
Abstracts of Theses					
Publication Citations					
Data on Scientific Collaborators					
Information on Inventions					
Technical Description of Project and Results					
Other (specify)					
1. Principal Investigator/Project Director Name (Typed) Richard A. DeMillo Kimberly N. King Raymond E. Miller	3. Principal Investigator/Project Director Signature  			4. Date  <b>5/19/87</b>	

FINAL REPORT  
NSF MCS-8103608

This grant supported work by Professors R. A. DeMillo, K. N. King, and R. E. Miller as well as several PhD students working with the three professors. This final report provides a summary of work done by each professor.

A. R. DeMillo's work on this grant concentrated mainly on defining and applying models of distributed and parallel computation to problems arising in multi-level computer security and cryptography. One major product of this work was a book-length research monograph published by The American Mathematical Society.

This work falls into broad categories. The first is the modeling of cryptographic protocols. This work, conducted jointly with PhD student M. Merritt, led to a new model of security - the hidden automorphism model - and to a new lower bound on the complexity of a variant of the Byzantine Agreement problem. Hidden automorphisms were used subsequently to prove the security of a number of important cryptographic protocols. The second area is the use of secure protocols to define operating system priorities to guarantee multi-level secure functions in distributed environments. The third area consisted of a number of cryptanalyses of major public key systems that had been proposed by 1983. Included among these was a simplified and generalized version of the "chosen signature" attack on public key systems that are defined by automorphisms on  $Z_n$ .

Publications

G. Davida, R. DeMillo, and R. J. Lipton, "Achieving Security Computers through Distributed Computing, Proc. 3rd International Conference on Distributed Computing, 1981.

R. A. DeMillo, N. A. Lynch, and M. J. Merritt, "Cryptographic Protocols", Proc. 14th ACM Symposium on the Theory of Computing, May 1982, pp. 383-400.

R. A. DeMillo, and M. J. Merritt, "Chosen Signature Cryptanalysis of Public Key Cryptosystems", Technical Memorandum, Georgia Institute of Technology, October 1982.

R. A. DeMillo and M. J. Merritt, "Protocols for Data Security", IEEE Computer, Vol. 16, No. 2 (February 1983), pp. 39-54.

M. J. Merritt, "Cryptographic Protocols", PhD Thesis, Georgia Institute of Technology, Atlanta, Georgia, GIT-ICS-83/06, February 1983.

R. A. DeMillo, et.al. Applied Cryptology, Cryptographic Protocols, and Computer Security, American Mathematical Society (PSAM 19), 1984.

B. The research with K. N. King covered several different areas. One study conducted with the support of this grant explored the question of how a complex function must be to compute for its inverse to be difficult. We have been able to show that, if a function is easy enough to compute, then



its inverse is easy to compute, in the sense that it can be computed in polynomial time. In fact, we were able to prove the stronger result that the inverses of such functions can be computed extremely quickly on a parallel computer that has a feasible number of processors. In order to make that notion precise, we defined a new complexity class, PUNC, that models the notion of "feasible parallelism" more naturally than classes that have been studied previously. We discovered several equivalent characterizations of PUNC and explored relationships between PUNC and other complexity classes.

Other work focused on systolic tree automata (STA's). In this model, which was inspired by VLSI circuits, a number of processors are connected to form a tree. An input string is fed to the processors at one level of the tree. Information is then processed in parallel, bottom-up toward the root, one level at a time. Results include a characterization of k-ary STA acceptable languages over a one-letter alphabet, a nonacceptability lemma for 2-ary STA's, and proofs of decidability of superstability for k-ary STA's and emptiness for arbitrary STA's.

Other studies include improved lower bounds for the cycle detection problem and an analysis of the number of cycles possible in directed graphs with no short cycles (digraphs with large girth).

#### Publications

E. W. Allender, "Invertible Functions", Technical Report GIT-ICS-85/20, School of Information and Computer Science, Georgia Institute of Technology, September 1985.

E. W. Allender, "P-Uniformity, Parallelism, and Precomputation", Technical Report GIT-ICS-85/11, School of Information and Computer Science, Georgia Institute of Technology, April 1985.

E. W. Allender, "Invertible Functions", PhD Thesis, School of Information and Computer Science, Georgia Institute of Technology, 1985.

A. F. Foufa, "Some Results on Systolic Tree Automata as Acceptors", M. S. Thesis, School of Information and Computer Science, Georgia Institute of Technology, 1985.

E. W. Allender and M. Klawe, "Improved Lower Bounds for the Cycle Detection Problem", Theoretical Computer Science, 36, (1985), pp. 231-237.

K. N. King, "Alternating Multihead Finite Automata", submitted to Theoretical Computer Science.

E. W. Allender, "Solutions for Problems P90 and P91", EATCS Bulletin #26, (June 1985), pp. 243-244.

E. W. Allender, "On the Number of Cycles Possible in Digraphs with Large Girth", Discrete Applied Mathematics, 10, (1985), pp. 211-225.

E. W. Allender and M. Klawe, "Improved Lower Bounds for the Cycle Detection Problem", IBM Research Report RJ 4078 (45456), October 1983.

K. N. King, "Alternating Multihead Finite Automata", Technical Report GIT-ICS-83/26, School of Information and Computer Science, Georgia Institute of Technology, September 1983.

E. W. Allender, "On the Complexity of Acceptance Problems for Multihead Automata", Technical Report GIT-ICS-83/22, School of Information and Computer Science, Georgia Institute of Technology, September 1983.

E. W. Allender, "On the Number of Cycles Possible in Digraphs with Large Girth", Technical Report GIT-ICS-83/10, School of Information and Computer Science, Georgia Institute of Technology, June 1983.

E. W. Allender, "An Improved Lower Bound for the Cycle Detection Problem", Technical Report GIT-ICS-83/04, School of Information and Computer Science, Georgia Institute of Technology, February 1983.

C. The work of R. E. Miller supported by this grant involved two area of work; models of parallel computation and modeling communication protocols. In the first area relationships between various models of parallel computation were studied in a formal manner. To do this a new computation system formulation was devised that enabled one to represent other models of parallelism such as vector addition systems, vector replacement systems, Petri nets and generalized Petri nets. Isomorphisms and homomorphisms were shown within this model that demonstrated what properties of these models were carried over from one model to the next. This work appeared as reference [1] below.

Within the communication protocol area a finite state communicating machine model was used for representing protocols. Working with a PhD student, T. Y. Choi, a structured partition decomposition technique was discovered that provides a substantial simplification for the analysis and synthesis of protocols. This work was published in references [2-5] below.

#### Publications

T. Kasai and R. E. Miller, "Homomorphisms between Models of Parallel Computation", JCSS, Vol. 25, No. 3, December 1982, pp. 285-331.

T. Y. Choi, "A Structured Approach to the Analysis and Design of Finite State Protocols", PhD Thesis, Georgia Institute of Technology, August 1983.

T. Y. Choi and R. E. Miller, "Network Protocol: A Structured Approach", Proceedings of the ACM 1983 Annual Conference, October 1983, pp. 155-162.

T. Y. Choi and R. E. Miller, "A Decomposition Method for the Analysis and Design of Finite State Protocols", IEEE Proceedings of the Eighth Data Communications Symposium", October 1983, pp. 167-176.

T. Y. Choi and R. E. Miller, "Protocol Analysis and Synthesis by Structured Partitions", Computer Networks and ISDN Systems, Vol. 11, No. 5, May 1986, pp. 367-381.