GEORGIA INSTITUTE OF TECHNOLOGY

OFFICE OF CONTRACT ADMINISTRATION

PROJECT ADMINISTRATION DATA SHEET

Project No. G-36-658

Raymond Miller

DATE: 8/20/81

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

Cost Sharing: $10,000 (G-36-345)

Contracted through: 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 Require

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 Security Services
Research Property Management EES Research Public Relat
Accounting Office Reports Coordinator (OCA)

Project File (OCA)
SPONSORED PROJECT TERMINATION/CLOSEOUT SHEET

GEORGIA INSTITUTE OF TECHNOLOGY

OFFICE OF CONTRACT ADMINISTRATION

Project No. G-36-658

Incorporates Subproject No.(s) N/A

School/ICS ICS

Date 6-15-87

Project Director(s) R.A. DeMillo

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

Title Models of Computation and Algorithms

Effective Completion Date: 12/31/84

(Performance) 3/31/85

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.

COPYES TO:

Research Director

Research Administrative Network

Research Property Management

Accounting

Procurement/GTRI Supply Services

Research Security Services

Reports Coordinator (OCA)

Library

GTRC

Project File

Other Duane H.

Angela DuBose

Russ Embry

FORM OCA 69.285
**PROPOSAL TO THE NATIONAL SCIENCE FOUNDATION**

**Cover Page**

**FOR CONSIDERATION BY NSF ORGANIZATIONAL UNIT**

Theoretical Computer Science

**IS THIS PROPOSAL BEING SUBMITTED TO ANOTHER FEDERAL AGENCY?**

Yes No X

**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**

$99,825

**PROPOSED DURATION**

12 months

**DESIRED STARTING DATE**

January 1, 1983

**PI/PD DEPARTMENT**

Information and Computer Science

**PI/PD NAME**

Richard A. DeMillo

Kimberly N. King

Raymond E. Miller

**PI/PD PHONE NO.**

(404) 894-3180

**PI/PD ORGANIZATION**

Georgia Institute of Technology

Atlanta, Georgia 30332

**ADDITIONAL PI/PD**

Kimberly N. King

Raymond E. Miller

**ADDITIONAL PI/PD**

Kimberly N. King

Raymond E. Miller

**FOR RENEWAL OR CONTINUING AWARD REQUEST, LIST PREVIOUS AWARD NO.:**

MCS-8103608

**IF SUBMITTING ORGANIZATION IS A SMALL BUSINESS CONCERN, CHECK HERE X (See CFR Title 13, Part 121 for Definitions):**

NA

**CHECK APPROPRIATE BOX(ES) IF THIS PROPOSAL INCLUDES ANY OF THE ITEMS LISTED BELOW:**

- Animal Welfare
- Human Subjects
- National Environmental Policy Act
- Endangered Species
- Marine Mammal Protection
- Research Involving Recombinant DNA Molecules
- Historical Sites
- Pollution Control
- Proprietary and Privileged Information

**PRINCIPAL INVESTIGATOR/PROJECT DIRECTOR**

Richard A. DeMillo

G. D. Hutchison

Kimberly N. King

Raymond E. Miller

**AUTHORIZED ORGANIZATIONAL REP.**

**OTHER ENDORSEMENT**

(optional)

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 \( V \) 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].


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

**PROPOSAL BUDGET**

**ORGANIZATION:** Georgia Institute of Technology  
School of Information and Computer Science

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

**PROPOSAL NO.**

**AWARD NO.**

**DURATION (MONTHS):** Proposed 12, Granted 12

### A. SENIOR PERSONNEL: PI/PD, Co-PI's, Faculty and Other Senior Associates

<table>
<thead>
<tr>
<th>Duration</th>
<th>NSF FUNDS</th>
<th>REQUESTED BY PROPOSER</th>
<th>FUNDS GRANTED BY NSF (IF DIFFERENT)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cal. Acd.</td>
<td>Person/Mos</td>
<td>$</td>
<td>$</td>
</tr>
<tr>
<td>1.</td>
<td>Richard A. DeMillo, Professor</td>
<td>1.2</td>
<td>6,334</td>
</tr>
<tr>
<td>2.</td>
<td>Kimberly N. King, Assistant Professor</td>
<td>2.0</td>
<td>6,764</td>
</tr>
<tr>
<td>3.</td>
<td>Raymond E. Miller, Professor</td>
<td>1.8</td>
<td>11,588</td>
</tr>
</tbody>
</table>

5. **OTHERS (LIST INDIVIDUALLY ON BUDGET EXPLANATION PAGE)**

5. ( ) TOTAL SENIOR PERSONNEL (1-5)

### B. OTHER PERSONNEL (SHOW NUMBERS IN BRACKETS)

1. ( ) POST DOCTORAL ASSOCIATES

2. ( ) OTHER PROFESSIONALS (TECHNICIAN, PROGRAMMER, ETC.)

3. ( ) GRADUATE STUDENTS (1/2 time)

4. ( ) UNDERGRADUATE STUDENTS

### C. FRINGE BENEFITS (IF CHARGED AS DIRECT COSTS) 22% of applicable salaries & wages

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

NONE

### E. TRAVEL

1. DOMESTIC (INCL. CANADA AND U.S. POSSESSIONS)

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

2. PUBLICATION COSTS/PAGE CHARGES

3. CONSULTANT SERVICES

4. COMPUTER (ADP) SERVICES

5. SUBCONTRACTS

6. OTHER Pro-rated cost of the ICS Comp. Lab ($7,000)

TOTAL OTHER DIRECT COSTS

### H. TOTAL DIRECT COSTS (A THROUGH G)

### I. INDIRECT COSTS (SPECIFY)

47.5% of H.

TOTAL INDIRECT COSTS

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

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

<table>
<thead>
<tr>
<th>Amount of this Request (J) OR (J - K)</th>
</tr>
</thead>
<tbody>
<tr>
<td>$99,825</td>
</tr>
</tbody>
</table>

### L. AMOUNT OF THIS REQUEST (J) OR (J - K)

**FOR NSF USE ONLY**

**INDIRECT COST RATE VERIFICATION**

**Date**

**DATE INST. REP. TYPED NAME & SIGNATURE**

**STIPENDS**

**FOR NSF USE ONLY**

**UPD TYPED NAME & SIGNATURE**
PART I—PROJECT IDENTIFICATION INFORMATION

1. Institution and Address
Georgia Institute of Technology
School of Information and Computer Science
Atlanta, Georgia 30332

2. NSF Program
Mathematics and Computer Science

3. NSF Award Number
MCS-8103608

4. Award Period
From 7/15/81 To 12/31/84

5. Cumulative Award Amount
$204,694

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)

<table>
<thead>
<tr>
<th>ITEM (Check appropriate blocks)</th>
<th>NONE</th>
<th>ATTACHED</th>
<th>PREVIOUSLY FURNISHED</th>
<th>TO BE FURNISHED SEPARATELY TO PROGRAM</th>
</tr>
</thead>
<tbody>
<tr>
<td>Abstracts of Theses</td>
<td></td>
<td></td>
<td></td>
<td>Check (✓)</td>
</tr>
<tr>
<td>Publication Citations</td>
<td></td>
<td></td>
<td></td>
<td>Approx. Date</td>
</tr>
<tr>
<td>Data on Scientific Collaborators</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Information on Inventions</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Technical Description of Project and Results</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Other (specify)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

3. Principal Investigator/Project Director Signature

Richard A. DeMillo
Kimberly N. King
Raymond E. Miller

4. Date
5/17/87
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 cryptoanalyses 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 $\mathbb{Z}_n$.

Publications


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 nonacceptibility 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


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


