9807-12&26
Research in Cryptography and Information Security, and Algorithm Development

Progress Report
January 1 — June 30, 1999

Shafi Goldwasser, Ronald L. Rivest and Michael Sipser

Project Overview

This project encompasses a broad range of topics in the security, complexity, and algorithms areas of mutual interest to researchers in LCS and NTT. Particular focus is on:

- developing electronic voting protocols;
- developing routing protocols and algorithms for high speed networks;
- developing protocols to protect intellectual property that is transmitted through the network;
- developing very fast error-correction coding and decoding algorithms; and
- developing efficient algorithms on quantum computers.

Progress Report

A. Verifiable Pseudo-Random Functions

Professor Goldwasser has been actively researching connections between verifiable pseudo-random functions (VRF) and digital signatures.

A verifiable pseudo random function f is a function such that even though an adversary cannot distinguish between f(x) and a random string for x's of its choice, he can nonetheless be convinced non-interactively that for a given x,y, y=f(x).

We show that VRF exist if and only if deterministic digital signature schemes exist which are secure against chosen message attack. We also show using the concept of VRF that there exists concepts in learning theory which are harder to generate than the are to learn. A previous weaker result in this vein was show by Naor who used a digital signature scheme by Bellare and Goldwasser for this purpose.

B. Electronic Voting

Here is more detail on the LCS electronic voting project. The basis this project is the paper, "A Practical Secret Voting Scheme for Large Scale Elections," by Atsushi Fujioka, Tatsuaki Okamoto, and Kazuo Ohta of NTT Laboratories, published in the proceedings of the 1992 AUSCRYPT conference.

Our software, called EVOX, is written in Java, and has been used with some success in several elections on the MIT campus. The software was written by Ben Adida, Mark Herschberg, and Randy Milbert, and Brandon DuRette. There is a web site with more details: http://theory.lcs.mit.edu/~cis/voting/voting.html

Professor Rivest has worked with Kazuo Ohta of NTT (now visiting our laboratory) and the EVOX team about extensions and improvements to the EVOX system. We have begun exploration of the following:

- using multiple voting registrars (administrators) and threshold signatures, to make it harder for an administrator to cheat (by voting for non-present voters)

- improving the signing time of the administrators, by using batch signature techniques (such as that proposed by Amos Fiat), or by using delegation techniques.

- improving the graphical interface, and more cleanly separating the computation portions of the code from the user interface portions of the code.

- further analysis to identify computational bottlenecks to scalability, and solutions to such bottlenecks,

- further analysis of ease of use, especially for voters, but also for system administrators

The EVOX system was successfully demonstrated at the MIT Laboratory for Computer Science 35th Birthday Celebration held in April, 1999. Approximately 1500 guests were able to see the system running, to vote in a sample election, and to ask questions of the student developers.

C. Quantum Computation

In the area of quantum computation, we have obtained the following two results:

1. A quantum algorithm for insertion into an ordered list. We consider the problem of inserting one item into a list of N-1 ordered items. We previously showed that no quantum algorithm could solve this problem in fewer than log N/(2 log log N) queries, for N large. Here we give a quantum algorithm that performs the insertion in fewer queries than is classically possible. Our result is that the insertion problem can be solved in 0.53 log_2 N quantum queries for large N (where log_2 N is the classical lower bound). One implication of this result is that N items can be sorted in 0.53 N log_2 N queries, better than possible classically.

Paper: Invariant Quantum Algorithms for Insertion into an Ordered List Authors: Edward Farhi, Jeffrey Goldstone, Sam Gutmann, Michael Sipser Appears in quant-ph/9901059 .

2. A quantum algorithm for distinguishing functions. Suppose an oracle is known to hold one of a given set of D binary functions (from {0,1}^N to {0,1}). To successfully identify which function the oracle holds with a classical algorithm, at least log_2 D queries are required. In this paper we derive a upper bound on the number of functions that can be distinguished with k queries on a quantum computer.

Paper: How many functions can be distinguished with k quantum queries? Authors: Edward Farhi, Jeffrey Goldstone, Sam Gutmann, Michael Sipser Appears in quant-ph/9901012 .

Plans for the Next Six Months

A. Cryptographic Protocols and Encryption Methods

The first part of this proposal is to study cryptographic protocols and encryption methods suitable for a distributed environment.

In particular, we plan to extend a threshold encryption scheme secure against chosen cyphertext attack, invented eailer this year by Goldwasser and Canetti (appeared in Eurocrypt 99). The security of this scheme is based on the difficulty of the Decisional Diffie-Hellman problem (DDH). The extentions planned invlove finding efficient and secure threshold pseudo-random functions which are non-interactive. Currently, all known pseudo-random functions implementations are interactive when used in a distributed setting. Such pseudo-random functions will prove useful in other applications beside encryption as well. We hope to host a visit by a post-doc — Omer Reingold — who has done quite a bit of work in this area of research of constructing secure pseudo random functions based on the DDH problem.

B. Electronic Voting

Current research avenues are directed toward scaling such protocols up to nation-sized elections. In particular, we plan to explore using multiple voting registrars (administrators) and threshold signatures, to make it harder for an administrator to cheat (by voting for non-present voters), and analysis to identify computational bottlenecks to scalability, and solutions to such bottlenecks.

C. Quantum Computation

We propose to continue our work on algorithms for quantum computers.

For the coming year, we plan to look at nonrelativizing techniques that may apply to quantum computers. Such techniques offer the only hope of improving upon Grover's result, because Grover's result has been shown to be optimal if relativizability is allowed.

We are currently attempting to look at nonrelativizing techniques that may apply to quantum computers. Such techniques offer the only hope of improving upon Grover's result, because Grover's result has been shown to be optimal if relativizability is allowed. We have some ideas for algorithms that may be able to improve upon Grover's result, but we have not been able to analyze them yet.

In addition we will host Professor Tetsuro Nishino (at the request of Kazuo Ohta) during September 1999, for collaboration on quantum computation.

D. Probabilistic Property Testing

We are continuing our investigation of the power of various models of computation and associated complexity classes. Our student Sofya Raskhodnikova will contribute to this project through her work on "probabilistic property checking", a natural extension of the classical problem of property testing where we exclude "borderline cases" from consideration. Algorithms which test objects for a property may have an easier time and hence may be more efficient if they are only required to operate on inputs which exhibit the property in an "extreme" way. Such probabilistic property checking algorithms are not required to give a correct answer if the input can be modified in a minor way to alter the presence or absence of the property.

This approach has been applied by Goldwasser, Goldreich and Ron to efficiently test NP-hard graph properties such as k-coloring, bisection, and various versions of the clique and cut problems examining only a constant amount of information about the graph. It has alos been applied by Sudan and students in LCS to achieve super efficient error detection and correction in error correcting codes. This work is in continuation.