Research in Cryptography, Info security & Algorithm Development
9807 12&26

Proposal for 1999-2000 Funding

Shafi Goldwasser, Ronald L. Rivest, and Mike 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 protocols to protect intellectual property transmitted through the network; and on developing efficient algorithms on quantum computers.

Research Plan for July 1, 1999 through June 20, 2000.

1. Distributed cryptographic protocols

We plan to extend a threshold encryption scheme secure against chosen cyphertext attack, invented earlier 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 extensions planned involve 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.

2. Electronic voting

Continue our work on electronic voting protocols. 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, with solutions to such bottlenecks. We mention that the basis for 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.

3. Quantum Computation

We propose to continue our work on algorithms for quantum computers. In the past year we obtained results characterizing the quantum complexity of certain natural computational problems. Our results apply to relativized problems such as testing the parity (evenness or oddness) of the number of strings satisfying a given condition. We showed that significant quantum speedup is not possible for this problem, in contrast with Grover's celebrated result which shows that a square-root speedup is possible for the problem of testing the existence of a string satisfying a condition.

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.

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

4. 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 also 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.