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

Progress Report: July 1, 1998—December 31, 1998

Tom Leighton, Michael Sipser,
Ron Rivest and Shafi Goldwasser

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 through December 1998:

We are happy to report that work has been initiated in several directions in the last few months. In particular, we have a project underway to implement secure scalable electronic voting. Kazuo Ohta (currently visiting LCS for a one year period) has had discussions with Ron Rivest on this project. Michael Sipser has obtained tight bounds on the complexity of several problems on a quantum computer. He has demonstrated that certain natural oracle problems do not admit any significant speed-up when using a quantum computer instead of a classical computer. In addition, Sipser has had several discussions with Kazuo Ohta on the preparation of a Japanese edition of a textbook in complexity theory. Shafi Goldwasser is continuing her work in cryptography, focusing on how to maintain security of cryptographic protocols when they are run in presence of active adversaries. Tom Leighton is on leave this term, and met with Dr. Kenji Koyama during his recent visit.

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 a couple of elections on the MIT campus. The software was written by Ben Adida, Mark Herschberg, and Randy Milbert. Brandon DuRette and Kevin McDonald are joining the project. There is a web site (http://theory.lcs.mit.edu/~cis/voting/voting.html) with more details.

Professor Rivest has had several discussions with Kazuo Ohta (now visiting our laboratory) and the EVOX team about extensions and improvements to the EVOX system. The most promising directions of research and implementation improvement seem to be:

* 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

We are optimistic that we can make substantial progress in these directions over the next year.