In Favour of Posting

香港中文大學
The Chinese University of Hong Kong

Institute of Theoretical Computer Science and Communications

ITCSC Seminar

Cryptographic Elections - Challenges and Opportunities

By

Prof. Alon Rosen
School of Computer Science, The Herzliya Interdisciplinary Center, Israel

July 28, 2010 (Wednesday)

2:30 pm – 3:30 pm

Rm. 121, Ho Sin Hang Engineering Building, CUHK

Abstract:

Advances in computer technology have created the illusion that electronic means would bring us closer to achieving improved voting systems. However, if not designed properly, electronic elections carry more risk than reward. The core of the problem is that computers cannot be trusted, both because of malicious software, and because code verification is effectively infeasible. Needless to say that this reduces the trust in the result of the election, and may have disastrous consequences.

In this talk I will survey the saga of electronic elections in the United States, and use it to motivate the concept of "software independence" (Rivest and Wack '06). I will then describe how modern cryptographic techniques can be harnessed in order to implement election mechanisms that enable both public verifiability and ballot secrecy. This is a combination that is not known to be achievable by other means.

Biography:

Dr. Alon Rosen is a faculty member in the School of Computer Science at the Herzliya Interdisciplinary Center. Before that he spent two years as a postdoc. in the Cryptography Group of MIT's Computer Science and AI Lab, and two years as a postdoc. in the Center for Research on Computation and Society at Harvard's department of Electrical Engineering and Computer Science. He received his Ph.D. at the Weizmann Institute of Science, under the supervision of Oded Goldreich and Moni Naor. His research interest are Cryptography and Computational Complexity.

***** ALL ARE WELCOME *****

Hosted by: Prof. Andrej Bogdanov Tel: 31634261
Enquiries : Institute of Theoretical Computer Science and Communications Tel: 2696 1257