**Agnes Hui Chan**

College of Computer Science
Northeastern University
Boston, MA 02115

office: (617) 373-2390
Fax: (617) 373-5121
home: (781) 259-9691

Email: ahchan@ccs.neu.edu
URL: www.ccs.neu.edu/home/ahchan

## Research Interest

Cryptography and communication security; wireless networks; coding theory and combinatorial algorithms.

## Education

Ph.D. in Mathematics *August 1975*
Ohio State University, Columbus, Ohio
Thesis: "Reconstruction Problems of Graphs and Designs",
Advisor: D. K. Ray-Chaudhuri

MA in Mathematics *August 1972*
Ohio State University, Columbus, Ohio

AB magna cum laude in Mathematics *June 1970*
Smith College, Northampton, MA
Thesis: "Topological Characterization of the Arc and the Circle".

## Employment

Associate Dean and Director of Graduate Program *September 1994 – present*
College of Computer Science, Northeastern University

Visiting Research Scientist *August 1997 – July 1998*
Laboratory of Information and Decision Science, MIT

Professor *June 1993 – present*
College of Computer Science, Northeastern University

Visiting Scientist *Spring 1991*
Department of Information Sciences, Swiss Federal Institute of Technology

Associate Professor *June 1982 – May 1993*
College of Computer Science, Northeastern University

Member of Technical Staff *Summers 1978 – 1993*
MITRE Corporation, Bedford, MA

Assistant Professor *September 1977 – May 1982*
Department of Mathematics, Northeastern University

Visiting Scientist *summer 1977*
Department of Mathematics, MIT

Instructor *September 1975 – June 1977*
Department of Mathematics, Ithaca College

## **Ph. D. Students** (past and present)

J.Georges, Ph.D. in mathematics (1980), Professor of Mathematics, Trinity College
S. Ray-Chaudhuri, Ph.D. in Electrical Engineering (1995), Qualcomm
Y. Tsiounis, Ph.D. in Computer Science (1997), consultant
M. Zhang, Ph.D. in Computer Science (2000), Verizon Laboratory Inc.
S. Wong, Ph.D. in College of Computer Science (2002), Chinese University of Hong Kong
H. Ho-Fuente, Ph.D. candidate in College of Computer Science
Feng Zhu, Ph.D. student in College of Computer Science
Robbie Ye, Ph.D. student in College of Computer Science

## **Grants and Awards**

DARPA Grant *April 2000 – March 2003*
Principal Investigator, "Authentication and Key Revocation Protocols for Wireless Networks"

DARPA Grant (subcontract with Northwestern University) *July 2000 – June 2003*
Co-Principal Investigator, "Lightweight Cryptography"

GTE Laboratory Inc. University Research Grant *June 1997 – June 1999*
Principal Investigator, "Security Analysis and Countermeasures in Cellular Telecommunication"

NSF POWRE Grant *November 1997 – June 1999*
Principal Investigator, "On Reconfigurable Feedback Shift Registers"

GTE Laboratory Inc. University Research Grant *October 1995 – December 1996*
Principal Investigator, "On Electronic Cash"

CRA Distributed Mentor Program *summer 1994*
Principal Investigator, "On Pseudorandom Sequences"

NSA Cryptography Grant *June 1991 – May 1994*
Co-Principal Investigator, "A Study of Pseudorandom Sequences"

NSF CISE Institutional Infrastructure Grant *October 1990 – September 1995*
Co-Principal Investigator, "Research Instrumentation"

## **Recent Publications** (past 5 years)

F. Zhu, D.S. Wong, A.H. Chan and R. Ye, "*RSA-Based Password Authenticated Key Exchange for Imbalanced Wireless Networks*". Proceedings of International Conference on Information Security 2002, Sao Paulo, Brazil, September 2002

G. Noubir, F. Zhu and A.H. Chan, "*Key Management for Simultaneous Join/Leave in Secure Multicast*", Proceedings of ISIT'02, August 2002

D.S. Wong and A.H. Chan, "On the Insecurity of Authenticated Key Exchange Protocols for Wireless Communications", Proceedings of InfoSec 2002, Shanghai, China, July 2002

D.S. Wong and A.H. Chan, "*Efficient and Mutually Authenticated Key Exchange for Low Power Computing Devices*", Advances in Cryptology – Asiacrypt'01, LNCS, December 2001

D.S. Wong, H. Ho-Fuentes and A.H. Chan, "*The Performance Measurement of Cryptographic Primitives on Palm Devices*", Proceedings of the 17th Annual Computer Security Applications Conference, December 2001

D.S. Wong and A.H. Chan, "*Mutual Authentication and Key Exchange for Low Power Wireless Communications*", Proceedings of IEEE MILCOM 2001, Washington D.C. October 2001

M.Zhang and A.H. Chan, "*Maximum Correlation Analysis of Nonlinear S-boxes in Stream Ciphers*", Advances in Cryptology - Crypto'00, LNCS 1880, August 2000

M.Zhang, A.H. Chan and C. Carroll, "*Analysis of IS-95 CDMA Voice Privacy*", Workshop on Selected Areas in Cryptography 2000, Waterloo, Canada, August 2000

M.Zhang, A.H. Chan and C. Carroll, "*The Software-Oriented Stream Cipher SSC2*", Proceedings of Fast Software Encryption Conference, LNCS 1978, April 2000

M.Zhang, A.H. Chan, C. Carroll and Y. Tsiounis, "*A Software-Oriented Stream Cipher for Cellular and Personal Communications Service*", Proceedings of 37th Annual Allerton Conference on Communication, Control, and Computing, September 1999, Champagne-Urbana, Illinois.

A.H. Chan, M. Medard and J. Yueh, "*On the Complexity of Reconfigurable Feedback Shift Register Sequences*", Proceedings of ISIT'98, August 1998

M. Medard, A.H. Chan, J.D. Moores, K.A. Hall, K.A. Rauschenbach, S. Parikh, "*Ultrafast Cryptography Using Optical Logic in Reconfigurable Feedback Shift Registers*", Proceedings of SPIE, August 1997.

A.H. Chan and M. Medard, "*On Reconfigurable Feedback Shift Registers*", Proceedings of ISIT'97, June 1997.

A.H. Chan and V.W.S. Chan, "*Reliable Message Delivery via Unreliable Network*", Proceedings of ISIT'97, June 1997.

A.H. Chan, Y. Frankel and Y. Tsiounis, "*On Divisible E-Cash*", Advances in Cryptology – EUROCRYPT'98

## Patents

"Software-Based Stream Cipher, SSC2", A.H. Chan and M. Zhang 1999

"Reconfigurable Feedback Shift Registers", A.H. Chan, M. Medard, K Hall, J. Moore, S. Parihk, K. Rauschenbach 1997

"Divisible Electronic Cash", A.H. Chan, Y. Frankel and Y. Tsiounis 1997

## Selected Invited Talks

"Authentication and Key Exchange Protocols for Wireless Imbalanced Networks", PARC, June 2002

"Security for Wireless Ad Hoc Networks", Draper Lab Workshop on Communications and Network Technology for Distributed Robotics, May 2002

"Secure Communication in Wireless Networks", colloquium talk at University of Maryland, April 2002

"Authentication and Data Security over Wireless Networks", Air Force Rome Research Lab, Rome, New York, June, 2001

"Sequences for Ultrafast Communication Network", NATO Workshop on Sequences, Difference Sets and Correlations, August 1998

"Ultrafast Generation of Pseudorandom Sequences", Institute of Mathematics Applications, Minnesota, August 1998

"On Electronic Commerce", chair of Panel Discussion, IEEE Conference on Application in Local Area Network, November 1997

"Cryptography and Coding", NSF Workshop, April 1997

"On Pseudorandom Sequences", Crypto Workshop, University of Arizona, March 1997

"On Electronic Commerce", IEEE Communication Society, Boston Chapter, February 1997

"On Pseudorandom Sequences", one day long seminar given at Crypto-Mathematics Institute, NSA, Baltimore, MD, June 1994

## Selected Professional Activities

| | |
|---|---|
| Program Chair, International Conference on Information Security, 2002, Brazil | *Sept 2002* |
| Local Arrangement Committee, IEEE ISIT'98, Cambridge, MA | *Aug 1998* |
| Editorial Board, Journal of Cryptogia | *1998–2001* |
| Board of Directors, IEEE Information Theory Society | *1995 – 1997* |
| Member, International Association of Cryptologic Research | |
| Member, IEEE Information Theory Society | |
| Member, ACM Society | |