



# IEEE NEWSLETTER

## KITCHENER - WATERLOO SECTION



March 1997

### MEETING

Mark these dates on your calendar:

**Tuesday, March 4th:** Professor Gordon Agnew on Applications of Public Key Cryptography, University of Waterloo, Davis Centre, Room 1302, 5:30 p.m. (see page 2).

**Wednesday, March 19th:** Student Papers Night, University of Waterloo, Davis Centre, Rooms 1301 and 1302, 7:00 p.m. (see page 2).

**Monday, April 21st:** Linda Weaver on Telemedicine, University of Waterloo, Davis Centre, Room 1302, 7:00 p.m. (see pages 2-3).

### Feature Articles

|  |        |                    |        |
|--|--------|--------------------|--------|
| Looking for a Job?   | page 3 | News from Academia | page 4 |
| IEEE to Network the World with New Slogan                                    | page 3 | News from Industry | page 4 |
| Conferences in Canada  | page 3 | ICR Short Courses  | page 4 |
| Stanley Lipshitz Described the Quantization Quandary and Demonstrated Dither | page 4 | A Happy Thought    | page 5 |



**Section Officers**

Chair: David Wang, (519)885-1211 ext. 3968  
 Vice Chair: Wai-Cheung Tang, (519)622-2300 ext. 255  
 Secretary: Rosalind Hood-Morris, (519)748-2462 email: rhoodm@hookup.net  
 Treasurer: John Mowbray, (519)884-1710 ext. 5371, 5569

**Chapter Chairs**

Computers: Slawo Wesolkowski, (519)884-1710 ext. 5130  
 Antennas and Prop., Microwave Theory and Tech.:\* Raafat Mansour, (519)622-2300 ext. 246  
 Circuits and Systems, Electron Devices:\* Arokia Nathan, (519)885-1211 ext. 4803  
 Signal Processing Amir Khandani, (519)885-1211 ext. 5324

\*Combined Chapter

**Committee Chairs**

Publicity: Shesha Jayaram, (519)885-1211 ext. 5337  
 Education: Rosalind Hood-Morris (519)748-2462 email: rhoodm@hookup.net  
 Program: Shesha Jayaram, (519)885-1211 ext. 5337  
 Membership and Transfers: Arvind Vyas (519)884-1710 ext. 245  
 Publications (News Letter): Tom East, (519)746-7809  
 Awards: Amir Khandani, (519)885-1211 ext. 5324  
 Nominations: R.H. MacPhie (519)885-1211 ext. 2842

**Student Activities Chairs**

Conestoga College: Jake Huschilt (519)748-5220 ext. 299  
 Univ. of Waterloo: e-mail ieesb@electrical.watstar.uwaterloo.ca (519)885-1211 ext. 6955 FAX: (519)746-3077  
 Stream A: Richard Hornsey, (519)885-1211 ext. 5336  
 Spring 1997  
 Stream B: Stephen Bagshaw, sabagsha@novice.uwaterloo.ca  
 Winter 1997 George H. Freeman, (519)885-1211 ext. 2876  
 Address IEEE K-W Section c/o Elect. & Comp. Eng. DC2597 University of Waterloo Waterloo, Ont., N2L 3G1 E-Mail: KWIEEE@sunee.uwaterloo.ca

**PROFESSOR AGNEW ON APPLICATIONS OF KEY TECHNOLOGY**

Date: Tuesday, March 4, 1997  
 Time: 5:30 p.m.  
 Place: University of Waterloo Davis Centre Room 1302  
 Subject: Applications of Public Key Cryptography  
 Speaker: Gordon B. Agnew received his B.A.Sc. and Ph.D. in Electrical engineering from the University of Waterloo in 1978 and 1982 respectively. He joined the faculty at Waterloo in 1982 and is currently an Associate Professor. He has been involved in the development of public key based cryptographic systems for many years. Dr. Agnew is also co-founder of CERTICOM Corp., a spin-off company from the University of Waterloo. CERTICOM is a world leader in Elliptic Curve based Public key technology and employs over 60 people.  
 Subject: Prof. Agnew's talk will examine the introduction and evolution of Public Key Cryptographic systems including RSA, Discrete Exponentiation and Elliptic Curves. He will review implementations and requirements of the various systems. In addition, he will examine applications such as wireless communications, internet commerce, Secure Electronic Transactions (SET) and other initiatives.

**STUDENT PAPERS NIGHT WEDNESDAY MARCH 19TH**

Presented by: K-W Section; Student Branch B, University of Waterloo; and Student Branch, Conestoga College.  
 Time: 7:00 p.m. Wednesday, March 19, 1997  
 Place: University of Waterloo Davis Centre rooms 1301 and 1302

You are cordially invited to the annual Student Papers Night. Students from Conestoga College and the University of Waterloo will deliver oral presentations of their technical papers. The best paper from the College is awarded the Ken McKenzie Award and the best paper from the University receives the George Dufault Award: the awards include cash prizes.  
 Refreshments will be provided.

**LINDA WEAVER ON TELEMEDICINE**

Date: Monday, April 21, 1997  
 Time: 7:00 p.m.  
 Place: University of Waterloo Davis Centre Room 1302  
 Subject: Reach Out and Diagnose Someone  
 Speaker: Linda Weaver, P.Eng., MBA is the Chief Technical Officer and Chair of the Board of TecKnowledge Healthcare Systems Inc. She sees the development of telemedicine as inevitable, given the huge size of Canada - the largest nation on earth. Her primary responsibility (and love) is the matching of clinical requirements to available and affordable technologies. She will describe the business and technology of telemedicine, and will give us some insight into future applications of communications technologies in medicine. Linda is also the 1996-97 President of IEEE Canada with the responsibility of managing IEEE activities in Canada and representing the Canadian members at the International Board of Directors.

The Kitchener-Waterloo Section of the Institute of Electrical and Electronics Engineers serves all members whose mailing address is in Bruce, Grey, Perth, Waterloo or Wellington Counties.

**Subject:** The latest buzz in the medical field is telemedicine, remote diagnosis using cameras and computers. The company that has the leading edge in the field is TecKnowledge Healthcare Systems Inc., which sells computer-based systems to help doctors see, diagnose and treat patients who may be hundreds of kilometers away. The basis of the system is digital cameras that enable doctors or radiologists to view everything from an X-ray to a live patient on a computer screen. TecKnowledge has installed a dozen sites in three provinces in less than two years and is looking at expanding it's installed base 10-fold in the next year. The company is also beginning installation of systems internationally - in the U.S., the Caribbean, and the United Arab Emirates.

**LOOKING FOR A JOB?**

Starting with our next issue, this newsletter will contain a "Jobs Wanted" column. If you are a full member of the IEEE we will post your advertisement at no charge (sorry, student members not eligible). Send this information: Name, Phone number, e-mail address, and a resume of 25-50 words by e-mail to: Tom East 102432.2337@compuserve.com

**IEEE TO NETWORK THE WORLD WITH NEW SLOGAN**

The IEEE Board of Directors has approved a new slogan - "IEEE: Networking the World".

No doubt we will read more about it in The Institute.

**CONFERENCES IN CANADA**

**1997**

- May 12-15 Int'l Conference on 3D Digital Imaging and Modeling. Ottawa. Marc Rioux 613-993-7902, e-mail: rioux@iit.nrc.ca
- May 12-16 Particle Accelerator Conference. Vancouver. E. Driessen. 604-222-7352, e-mail: pac97@triumf.ca
- May 19-23 Graphics Interface'97. Kelowna BC. V. Klassen 716-422-5760, e-mail: klassen@wrc.xerox.com or M Mantei 416-978-5512, e-mail: mantei@dgp.utoronto.ca http://www.dgp.utoronto.ca/gi97
- May 19-21 IEEE Instrumentation & Measurement Technology Conference IMTC 97. Ottawa. R. Myers 310-287-1463, e-mail: bob.myers@ieee.org
- May 25-28 1997 Canadian Conference on Electrical and Computer Engineering. St. John's, Nfld. Paper deadline: Feb. 21/97. D. Collett 709-737-1372, e-mail: t.d.collett@ieee.org
- May 26-28 CORS'97 Canadian Operational Research Society Annual Conference. Ottawa. D. Meister 613-520-2600 (x 2397), e-mail: cors97@business.carleton.ca
- May 27-30 Joint Int'l Conference on Open Distributed Processing and Distributed Platforms. Toronto. John Botsford 416-488-2096, e-mail: icodp97@sce.carleton.ca

- May 28-30 ISMVL'97 - IEEE Int'l Symp on Multiple-Valued Logic. Antigonish, Nova Scotia. Gerhard Dueck 902-867-2376, e-mail: gdueck@stfx.ca URL: http://juliet.stfx.ca/~gdueck/ismvl97/
- Jun 3-6 IEEE International Conference on Multimedia Computing and Systems. Ottawa. Nicolas D. Georganas 613-562-5800 (x 6225), e-mail: georgana@mcrclab.uottawa.ca URL: http://www.mcrclab.uottawa.ca/ICMCS97.html
- Jun 3-5 Canadian Wireless 1997. Montreal. 613-233-4888.
- Jun 8-12 ENM-97 First IEEE Enterprise Networking Mini-Conference. Quebec. Bhumip Khasnabish e-mail: bhumip@gte.com
- Jun 8-12 ICC'97 - IEEE International Conference on Communications. Montreal. Roland Oliver 514-870-3060, e-mail: oliverr@stentor.ca or Celia Desmond 905-615-6507, e-mail: desmondCL@stentor.ca
- Jun 8-12 1st IEEE Enterprise Networking Mini-Conference (ENM-97) in Conjunction with ICC'97. Montreal. Vijay Bhagavath e-mail: bhagavath@bell-labs.com
- Jun 9-12 1997 IEEE Digital Cross-Connect Systems Workshop VII. Whistler, BC. James H. Simester 908-949-7336, e-mail: sims@bostare.ho.att.com
- Jun 10 A Wireless Mini Conference. Quebec. Vino Vinodrai 416-789-5039
- Jun 16-19 DCS-97 Digital Cross Connect Systems Workshop. Whistler, BC. Richard Hamley 613-763-4591, e-mail: hamleyrd@stentor.ca
- Jun 22-24 MPPOI Fourth Intl Conf on Massively Parallel Processing Using Optical Interconnections. Montreal. E Schenfeld 609-951-2742, e-mail: mppoi@research.nj.nec.com
- Jul 13-18 IEEE AP-S International Symposium and URSI North American Radio Science Meeting. Montreal. D. Ruest 613-993-9228, e-mail: ursiaps97@nrc.ca or doris.ruest@nrc.ca; or P. Bhartia 902-426-3100 (x 133), e-mail: bhartia@drea.dnd.ca
- Jul 21-23 1997 IEEE Signal Processing Workshop on Higher Order Statistics. Banff, Alberta. Keh-Shin Lii 909-787-3836, e-mail: ksl@ucrstat.ucr.edu
- Jul 24-25 DMS'97 Pacific Workshop on Dist. Multimedia Systems. Vancouver. Taieb Znati 412-624-8490, e-mail: znati@cs.pitt.edu
- Aug 24-28 World Power Beaming Conference. Montreal.
- Aug 25-29 1997 10th International Symposium on High Voltage Engineering. Montreal. Farouk A.M.Rizk 514-652-8210
- Sep 15-17 1997 IEEE Petroleum & Chemical Industry Technical Conference (PCIC 97). Banff, Alberta. R.W.Gallant 403-237-3511

- Sep 16-18 1997 International Display Research Conference. Toronto. Ralph Nadell 212-620-3341, e-mail: madell@newyork.palises.org
- Sep 21-26 ISS'97 World Telecommunications Congress (International Switching Symposium). Toronto. Irving Elbert 416-588-3522 http://www.ISS97.org/ e-mail: info@ISS97.org/
- Oct 5-8 1997 IEEE Ultrasonics Symposium. Toronto. Stuart Foster 416-480-5716, e-mail: stuart@srcl.sunnybrook.utoronto.ca
- Oct 6-9 OCEANS'97. Halifax. IEEE Ocean Engineering Society and the Marine Technology Society. Ms. Michael Ellis 908-562-5362, e-mail: m.ellis@ieee.org

#### 1998

- May 4-7 1998 IEEE/IAS Industrial and Commercial Power Systems Technical Power Conference (I&CPS). Edmonton. M.Bince 403-468-6673
- May 18-21 1998 IEEE Vehicular Technology Conference (VTC). Ottawa. Tara Hennessy 613-990-4711, e-mail: hennessytara@ic.gc.ca
- Sep 15-18 1998 IEEE International Professional Communication Conference (IPCC 98). Quebec. Cheryl Reimold 914-725-1024, e-mail: c.reimold@ieee.org

#### 1999

- Jul 18-22 1999 IEEE Power Engineering Society Summer Meeting. Edmonton. D Fraser 403-448-3554

### STANLEY LIPSHITZ DESCRIBED THE QUANTIZATION QUANDARY AND DEMONSTRATED DITHER

by George Freeman

Would you ever think to ADD about 30 dB of random noise to your high-quality music signal in order for it to sound about 20 dB LESS noisy after quantization? It seems counter to engineering intuition. Yet, in this talk we learned why this might be so and heard demonstrations to illustrate the point.

The problem is simple. The noise in quantizing one music sample depends on that sample's value, so the music signal and the quantization noise are probabilistically dependent. For a signal whose frequency spectrum is not too complex (we heard a piano piece), this correlation of signal with noise can be heard as either outright distortion of the tonal character of the music or as modulation of the power level in an otherwise "white"-sounding background noise.

Adding random noise to the signal, a process called dithering, can make arbitrary statistical moments of the noise (mean noise value, mean noise power, etc.) constant, that is, not dependent on the input signal. This mimics the situation in analog signal processing where the dominant noise components are usually thermal and totally unrelated to the input signal. Dither, with a uniform probability density over one quantizer level, can make the mean noise value as signal independent so most distortion is eliminated. A little more dither, with a triangular probability density over two quantizer levels, can further make the mean noise power as signal

independent and eliminate the noise-modulation effects. Controlling these first two moments is enough to satisfy the human ear in the case of music.

Having made the quantization noise somewhat larger but considerably less signal dependent, it is possible to shape the noise spectrum (for example, to the inverse of the spectral sensitivity of the ear) in order to hide the louder noise level in places where it actually sounds much quieter. Thus, the approximately 20 dB improvement by adding about 30 dB of noise.

Dither is now found in places where signal-dependent quantization noise is problematic, such as converting 20-bit master recordings to the 16-bit compact disc format, input digitizing for spectral analyzers, or some crucial rounding/truncation steps in numerical algorithms. For those of us attending the talk, Professor Lipshitz has expanded our intuitive understanding to include a situation, the quantization quandary, where a little added noise can make a significant improvement.

#### NEWS FROM ACADEMIA

The University of Waterloo is running a course on entrepreneurship, technology and information for mathematics students. It will include guest lecturers involved in the business community. It is given by Prof. Mark Arnason 519-888-4571 ext. 2041.

The Xerox Teaching Internships Program enters its second year. It has placed 10 UW coop education students in high schools to work transferring information technology skills to high school students and teachers. Xerox is contributing \$250,000 over 5 years to the program as part of Campaign Waterloo.

#### NEWS FROM INDUSTRY

Sybase Inc. has signed agreements for the use of its SQL Anywhere mobile database to be used by Cisco Systems for internetworking, and by Landmark Graphics Corp. for its software applications for the oil exploration and production industry. Their Waterloo operation, formerly WATCOM, is very active on Phillip Street.

Vivtek Vision Corporation has extended its agreement with MiTek Industries Inc. to exclusively distribute the Vivtek TrussLine systems in North America and Australia. TrussLine is used in the prefabricated construction industry for placing nail plates on roof trusses. Other Vivtek systems are used in the aircraft industry and by leather manufacturers.

#### INSTITUTE FOR COMPUTER RESEARCH SHORT COURSES, March to May 1997

##### Wireless and Mobile Computing

March 19-20, 1997  
(two days - \$500+GST)

Thomas Kunz, Dr.Eng.  
Assistant Professor, Computer Science  
Member, ICR Computer Communications Networks Group

##### Hypermedia, Multimedia, Metamedia, and the Web

April 8-9, 1997  
(two days - \$600+GST)

Michael McCool, Ph.D.  
Assistant Professor, Computer Science  
Member, ICR Computer Graphics Lab

**Using the C++ Standard Template Library**

May 5, 1997

(one day - \$250+GST)

Darrell Raymond, Ph.D.

Adjunct Assistant Professor, Computer Science

**A VHDL-Based Introduction to Digital and Analogue**

**Hardware Description Languages**

May 28-29, 1997

(two days - \$500 + GST)

Farhad Mavaddat, Ph.D.

Associate Professor, Computer Science

Member, ICR Software Engineering Group and Very Large

Scale Integration

Research Group

**REGISTRATION**

Everyone is welcome to attend the ICR Short Courses. You should register early as space is limited. Employees of companies that are ICR Corporate Partners/Corporate Associates may attend free-of-charge. ICR faculty members and graduate students supervised by ICR faculty members may attend free-of-charge, subject to availability of space.

**Location/Schedule:**

All short courses are held in the Davis Centre, Room 1304, University of Waterloo. Each course begins at 9:30 a.m. and ends at 4:30 p.m.

**To Register:**

Mail/Fax/Phone: Institute for Computer Research, University of Waterloo, Waterloo, ON N2L 3G1, attn: Jean Webster. Ph: 519-888-4530, Fax: 519-885-1208, email: jrwebste@icr.uwaterloo.ca. Or, visit ICR's Website to register: <http://icr.uwaterloo.ca/ICR/>.

**HAPPY THOUGHT**

Jill: Why do you always make such a point of attending the funerals of your colleagues and friends?

Jack: Because if I don't go to theirs, they won't come to mine.