IEEE Information Theory Society Newsletter

Vol. 54, No. 1, March 2004 Editor: Lance C. Pérez ISSN 1059-2362

It is my great pleasure and honor to serve as the President of the IEEE Information Theory Society.

Owing to the efforts of the former presidents and board members, the financial status of our society is out of trouble, with a "break-even" budget for the first time in several years following the IEEEs recent financial problems. However, the recent decrease in the number of society members could not be stopped. This is common to all IEEE societies, but the rate of decrease is rather high for our society. My primary goal as President is to improve this situation. For this purpose many measures can be taken. In the following I put forward two of them.

One measure is the extension of coverage of our society. We should carefully choose an area so that both our society and the area profit. One candidate area is cryptology, which is indeed included in the scope of our society, but is not very active. The most important paper for modern cryptography, "New directions in cryptography" by W. Diffie and M. Hellman, was published in the IEEE Transactions on Information Theory in 1976. Nevertheless, there are only a few researchers and engineers for cryptographic techniques in our society. Cryptography is the basis of information security technology, which is now widely recognized as one of the most important elements of information technology. The applications of cryptography are rapidly expanding and the number of researchers and engineers in this area is rapidly increasing.

In order to find close connections between Shannon Theory and cryptology, it is enough to consider Shannon's paper, "Communication theory of secrecy systems" published in the Bell System Technical Journal in 1949. If practical quantum computers were realizable, then almost all conventional public-key cryptosystems would collapse and cryptographic

IEEE
I T
S N

IEEE Informa ion Theor Socie Ne sle er

This time, with your indulgence, I will engage in a historical review of very narrow (and personal) scope. Having spent thirty three years at the University of Maryland's Electrical Engineering Department (now Electrical and Computer Engineering Department), and having witnessed and (hopefully) influenced the evolution of its attention to the field of Information Theory, I

GOLOMB'S PUZZLE COLUMN

AN INVERSE PROBLEM

Soloman W. Golomb

Suppose there is a set S of n distinct positive real numbers which you are asked to determine, given only the set T consisting of the $\binom{n}{k}$ sums of all the k-element subsets of S. (You are not told which sum corresponds to which subset.) For many values of n and k the reconstruction of the elements of S is unique. It is also possible to have two different solutions for S, given T, or even to have a continuum of values for the elements of S, given T, for certain pairs n and k. In the first four problems, find all possible sets S consistent with the given set T.

1. $n = 4, k = 2, T = \{24, 28, 30, 32, 34, 38\}$.

2. $n = 5, k = 2, T = \{21, 26, 28, 29, 31, 34, 36, 37, 42, 44\}$.

3. $n = 6, k = 2, T = \{32, 35, 37, 39, 41, 43, 44, 45, 48, 49, 51, 52, 54, 58, 62\}$.

4. $n = 6, k = 3, T = \{49, 54, 56, 57, 58, 60, 61, 65, 66, 67, 68, 69, 70, 74, 75, 77, 78, 79, 81, 86\}$.

The next four problems are more general.

5. Show that the problem of reconstructing S from T for given n and k is precisely equivalent (procedurally) to the corresponding problem for n and $k' = n - k$.

6. For $k = 2$ and each $n \geq 2$, how many solutions are there for S? (There are different answers for different values of n.)

7. How many solutions are there for S if $n = k > 1$?

8. For what pairs n and k are there exactly two reconstructions for S?

CALL FOR NOMINATIONS: IT SOCIETY DISTINGUISHED SERVICE AWARD

The IT Society Award honors individuals who have shown outstanding leadership in, and provided long-standing exceptional service to, the Information Theory Community.

Nominations:
Nominations for the Distinguished Service Award can be made by anyone and are made by sending a letter of nomination to the president of the IT Society by April 15. The individual or individuals making the nomination have the primary responsibility for justifying why the nominee should receive this award.

How to nominate:
Letters of nomination should

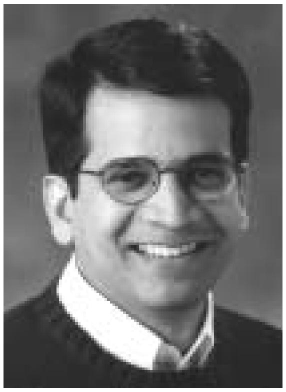
- Identify the nominee's areas of leadership and exceptional service, detailing the activities for which the nominee is believed to deserve this award;
- Include the nominee's current vita;
- Include two letters of endorsement.

Current officers and members of the IT Society Board of Governors are ineligible.

The prize shall be an ISIT or ITW participation fee waiver, a specially engraved plaque and a certificate, and shall be presented at the ISIT meeting held during the summer following selection of the winner or at an appropriate IEEE IT Society activity selected by the recipient.

Nomination Deadline:
April 15, 2004
Please send your letter of nomination by e-mail to
imai@iis.u-tokyo.ac.jp

G C : NSF P D



V V.V

Greetings! In early October 2003, I took on the Program Director position for communications research at the U.S. National Science Foundation. I decided recently to begin writing this column to document my experiences, keep members of the community informed as to happenings at NSF that might affect their research and funding, and to engage members in dialogue about issues that affect us all. I also am hopeful that raising awareness of what this position entails might encourage others to take up the torch after me.

I expect that this column will mostly be of interest to the US research community, but I would also appreciate any comments/feedback from our international readership.

First, I'd like to offer some background on how I came to take on this position. When Julia Abrahams announced her intention to resign as Program Director of communications research at NSF during ISIT 2003, I approached her hoping to get some information about what the position entails. After talking with her, I expressed some interest in the position, and a few weeks later the Division Director, Kamal Abdali, invited me to NSF and began to recruit me for the position.

After discussing the prospect with others in the community, I initially declined the position. Some of my reasons were that I felt that the absence from the University of Illinois might be unfair to my graduate students, and would interrupt my research efforts. I was also concerned about the potential negative effects to my own efforts to find research funding. In addition, several senior members of the community expressed that the position may be inappropriate for someone in my stage of career, reasoning that it is perhaps too administrative in function.

Dr. Abdali persisted in recruiting me, however, and I reconsidered my misgivings. As I thought, I became increasingly convinced that it is vital that the person who takes on the position be someone with the interests of the community at heart. During the interview process, I also learned about the CISE (Computer and Information Science and Engineering) directorate reorganization. I felt that it was particularly important in this time of flux, to have someone with a strong understanding of the IT research community to represent our interests at NSF.

Now, five months into my assignment, I remain convinced that I have made the right decision. However, I am concerned about the future of the position. I believe that any negative perceptions associated with the Program Director position are undeserved and misplaced – and perhaps dangerously so.

I have just finished a term as Associate Editor with the IT Transactions, a job that is typically given the nod as an important community service, despite the heavy administrative burden of the position. While editorial positions are of course very important, I cannot help but believe that the contributions of an NSF program director are just as important, if not more so. Consider that while the Editor-in-Chief of the IT Transactions helps to maintain the infrastructure for the academic review process – certainly an important function – a Program Director at NSF actually can work to affect the amount and direction of future government funding, as well as setting the agenda for future research in an area!

I have found, meanwhile, that the administrative burden associated with this position is not much greater than that of doing an associate editorship job well, and leaves ample time for keeping up-to-date on research and working towards defining the research frontier for communications. Furthermore, NSF traditionally allows rotators from universities to spend up to one day a week to maintain their research programs at their home institution, and I have found this time to be adequate for advising my students at the University of Illinois. I have been making week-long trips to Illinois roughly once a month since I joined NSF. There are some restrictions on my applying for federal research funding while I am at at NSF; however, I believe that these will be more than compensated for by my increased understanding of the funding process, and exposure to new research areas.

Now, let me describe some of the particulars of my work. When I joined NSF in early October, I found thirty-five Career proposals waiting to be processed. I quickly set up my first panel to assess these proposals, and was pleased at the prompt and mostly positive responses I received. The panel ran smoothly, and I even found time to have a discussion with the panel about what they perceived as the future directions of research in communications. I am still in the process of making awards on these proposals. Due to congressional continuing resolutions, the budget outlook was somewhat unclear until recently, and thus I have had to hold off on making decisions on some of the proposals.

I know many of you have concerns about the reorganization of the CISE Directorate. As a brief introduction to the reorganization, CISE is grouping closely related programs into clusters. Clusters will support traditional disciplinary research, while providing a better setting to review and support research that is interdisciplinary or that can influence related areas. The old Communications Program is now part of the Formal and Mathematical Foundations (FMF) cluster within the Division of Computing and Communication Foundations (CCF) of CISE. For more information about the reorganization, see the CISE website at http://cise.nsf.gov. John Cozzens, the program director for the former Signal Processing Systems program, and I worked together on rewriting our program descriptions so as to fit them into the reorganization structure.

By the time you read this, I will be handling proposals submitted to the ITR solicitation, with a February 24 deadline, and the FMF Cluster, with a March 4 deadline. I expect that March and April will be very busy as I organize panels and make decisions about these awards.

On a slightly different note, a few weeks ago, I was sent to Program Directors' "boot camp". I had already made a few blunders, and asked why this training wasn't offered earlier. I was informed that we were allowed time to err so that we would see the need for instruction. The strategy worked - I found much of the training to be directly relevant to my everyday needs. I have to admit, though, that on the bus ride to the conference grounds, I wasn't exactly looking forward to the long training sessions, wondering whether I should keep a supply of toothpicks in my pocket to prop my eyes open. I'm happy to say that the instruction was made very enjoyable. I commend the organizers, who primarily used instructive case studies and entertaining group activities to involve all of us personally. I was also very happy that, though I almost won the geek award, I was overthrown in the final round by George Strawn, the Chief Information Officer at NSF, because I had never worn a pocket protector.

In conclusion, I want to emphasize that I really cannot do my job well without help from you - ask not what NSF can do for you but what you can do for NSF. I would like to hear from you - please send suggestions for changes in the funding process, feedback on the reorganization, and your ideas on the future of communications research, including future applications areas. It is also very important that you keep me informed about success stories surrounding your NSF-funded research, so that we can keep the folks on The Hill aware that we are doing important work.

Also, if you happen to be in the DC area, I also encourage you stop by NSF, and if possible to meet with the Division Director of CCF, Kamal Abdali and the Assistant Director of CISE, Peter Freeman. I would also encourage you to be open to participation in advisory boards and external committees at NSF.

My intention is to spend only one year at NSF and return to the University of Illinois on August 15, 2004. I am trying my best to maintain a detailed set of notes to help my successor. I am hoping that this column would also help to maintain some continuity from one program director to the next. If you have any interest in taking over the position in 2004-05, please let me know.

That is all I have to report for now. Stay in touch. My email address is vveerava@nsf.gov.

N B

Raymond Yeung

Mathematics of Information and Coding,
by Te Sun Han and Kingo Kobayashi. American Mathematical Society, 2002, 286 pp., $99, ISBN 0-8218-0534-7.
Con en s:
What is Information Theory? Basics of Information Theory; Sources and Coding; Arithmetic Codes; Universal Coding of Integers; Universal Coding of Texts; Universal Coding of Compound Sources; Data Analysis and MDL Principle.

Wireless Communications and Networking,
by Jon W. Mark and Weihua Zhuang. Prentice Hall, 2003, 356 pp., $98, ISBN 0-13-040905-7.
Con en s:
Overview of Wireless Communications and Networking; Characterization of the Wireless Channel; Bandpass Transmission Techniques for Mobile Radio; Receiver Techniques for Fading Dispersive Channels; Fundamentals of Cellular Communications; Multiple Access Techniques; Mobility Management in Wireless Networks; Wireless/Wireline Interworking.

Convex Analysis and Optimization,
by Dimitri P. Bertsekas, with Angelia Nedic and Asuman E. Ozdaglar. Athena Scientific, 2003, 560 pp., $79, ISBN 1-886529-45-0.
Con en s:
Basic Convexity Concepts; Convexity and Optimization; Polyhedral Convexity; Subgradients and Constrained Optimization; Lagrange Multipliers; Lagrangian Duality; Conjugate Duality; Dual Computational Methods.

Information Theory, Inference, and Learning Algorithms,
by David MacKay. Cambridge University Press, 2003, 640 pp., $50, ISBN 0521642981.
Con en s:
Data Compression; Noisy-Channel Coding; Further Topics in Information Theory; Probabilities and Inference; Neural Networks; Sparse Graph Codes.

Components of Variance,
by David R. Cox and P. J. Solomon. CRC Press, 2003, 184 pp., $69.95, ISBN 1-58488-354-5.
Con en s:
KeyModels and Concepts; One-Way Balanced Case; More General Balanced Arrangements; Unbalanced Situations; Non-Normal Problems; Model Extensions and Criticism; Appendix: Fitting Separate Logistics Regressions to the ANZICS Data.

Fundamentals of Error Correcting Codes,
by W. Cary Huffman and Vera Pless. Cambridge University Press, 2003, 664 pp., $80, ISBN 0-521-78280-5.
Con en s:
Basic Concepts of Linear Codes; Bounds on Size of Codes; Finite Fields; Cyclic Codes; BCH and Reed-Soloman Codes; Duadic Codes; Weight Distributions; Designs; Self-Dual Codes; Some Favourite Self-Dual Codes; Covering Radius and Cosets; Codes over Z4; Codes from Algebraic Geometry; Convolutional Codes; Soft Decision and Iterative Decoding.

Introduction to Space-Time Wireless Communications,
by Arogyaswami Paulraj, Rohit Nabar, and Dhananjay Gore. Cambridge University Press, 2003, 308 pp., £45, ISBN 0-521-82615-2.
Con en s:
Introduction; Space-Time Propagation; Space-Time Channel and Signal Models; Capacity of Space-Time Channels; Spatial

Diversity; Space-Time Coding without Channel Knowledge at the Transmitter; Space-Time Receivers; Exploiting Channel Knowledge at the Receiver; Space-Time OFDM and Spread Spectrum Modulation; MIMO-Multiuser; Space-Time Co-Channel Interference Mitigation; Performance Limits and Trade-offs in MIMO Channels.

Multidimensional Discrete Unitary Transforms: Representation, Partitioning, and Algorithms,

by Artyom M. Grigoryan and Sos S. Agaian. Marcel Dekker, 2003, 544 pp., $185, ISBN 1-8247-4596-5.

Con en s:

Basic Concepts and Notations; Tensor Representation of Multidimensional Signals; Discrete Transform Tensor Representations; Discrete Transform Paired Representations; Multipaired Unitary Transforms; Analysis and Effective Computing Procedures; Fast 1-D Transforms; Fast 2-D Transforms; Paired Algorithms; Applications of Paired Transformations; Fourier Transform, Geometrical Interpretation, and Convolution; Image Enhancement by Paired Transforms; Image Reconstruction from Projections by Paired Transforms.

Cryptography: Theory and Practice, Second Edition,

by Douglas R. Stinson. Chapman & Hall/CRC, 2002, 360 pp., $79.95 ISBN 1-5848-8206-9.

Con en s:

Classical Cryptography; Shannon's Theory; Block Ciphers and the Advanced Encryption Standard; Cryptographical Hash Functions; The RSA Cryptosystem and Factoring Integers; Public-Key Cryptography Based on the Discrete Logarithm Problem; Signature Schemes.

Reasoning about Uncertainty,

by Joseph Y. Halpern. MIT Press, 2003, 456 pp., $55, ISBN 0-262-08320-5.

Turing (A Novel about Computation),

by Christos H. Papadimitriou, MIT Press, 2003, 284 pp., $24.95, ISBN 0-262-16218-0.

The Mathematical Theory of Information,

by Jan Kahre. Kluwer, 2002, 520 pp., $145. ISBN 1-4020-7064-0.

Third Generation Wireless Systems, Volume 1: Post-Shannon Signal Architectures,

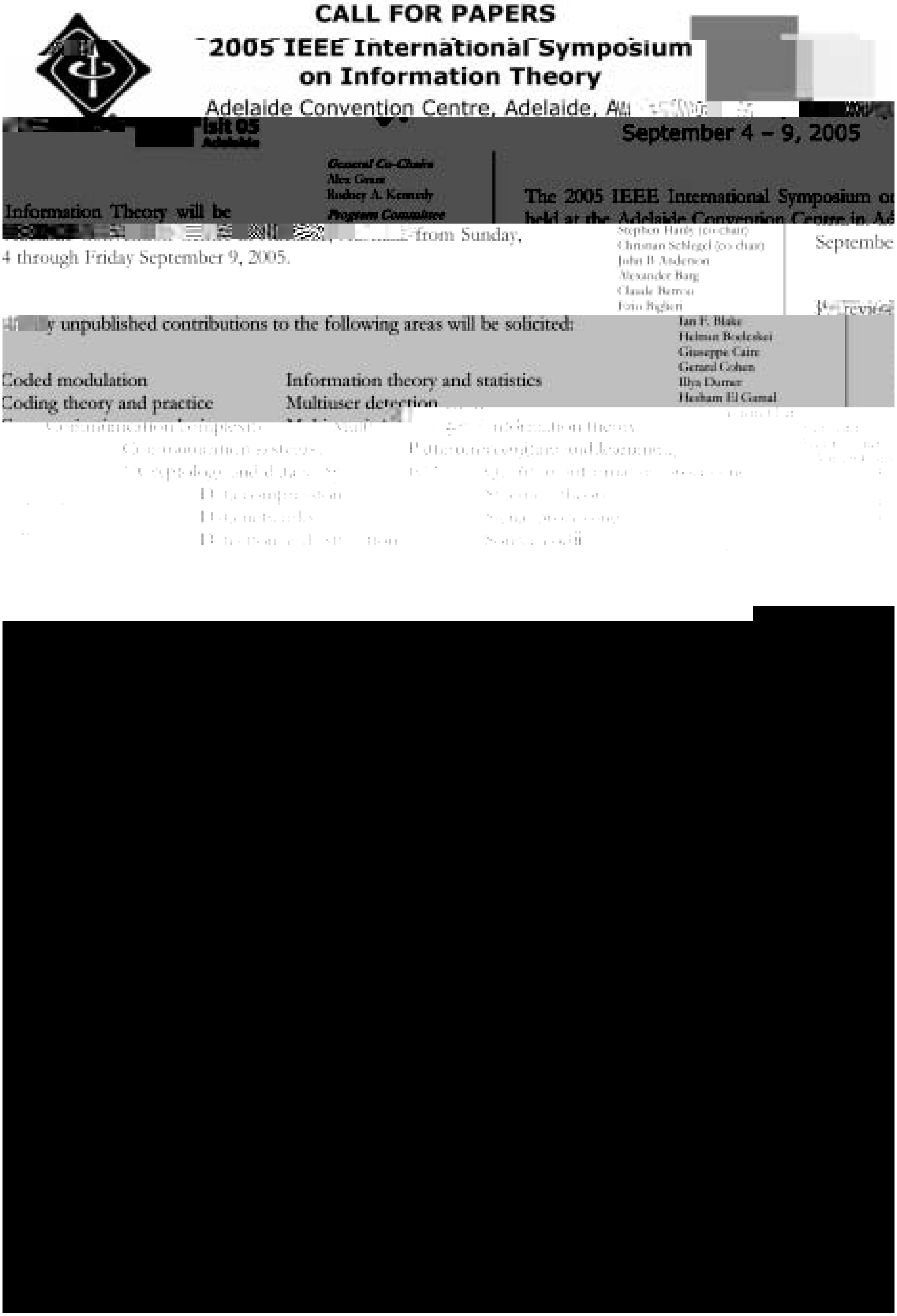
by George W. Calhoun. Artech House, 2003, 514 pp., £59, ISBN 1-58053-043-5.

Speech Processing,

by Li Deng and Douglas O'Shaughnesy. Marcel Dekker, 2003, 752 pp., $175, ISBN 1-8247-4040-8.

Nonlinear Signal and Image Processing,

by Kenneth Barner and Gonzalo R. Arce. CRC Press, 2003, 392 pp., $99.95, ISBN 0-8493-1427-5.



CALL FOR PAPERS

2005 IEEE International Symposium on Information Theory

Adelaide Convention Centre, Adelaide, Au

isit 05
Adelaide

September 4 – 9, 2005

General Co-Chairs
Alex Grant
Rodney A. Kennedy

Program Committee
Stephen Hanly (co-chair)
Christian Schlegel (co-chair)
John B Anderson
Alexander Barg
Claude Berrou
Ezio Biglieri
Ian F. Blake
Helmut Bolcskei
Giuseppe Caire
Gerard Cohen
Ilya Dumer
Hesham El Gamal

The 2005 IEEE International Symposium on Information Theory will be held at the Adelaide Convention Centre in Ad from Sunday, September 4 through Friday September 9, 2005.

y unpublished contributions to the following areas will be solicited:

Coded modulation
Coding theory and practice
Communication complexity
Communication systems
Cryptology and data security
Data compression
Data networks
Detection and estimation

Information theory and statistics
Multiuser detection
Multi information theory
Pattern recognition and learning
Quantum information processing
Shannon theory
Signal processing
Source coding

Septembe

Peer review

London

istration

DATE	CONFERENCE	LOCATION	CONTACT/INFORMATION	DUE DATE
June 27 - July 2, 2004	**2004 IEEE International Symposium on Information Theory (ISIT)**	Chicago Downtown Marriot Chicago, Illinois, USA	chair@isit2004.org http://www.isit2004.org	Dec. 1, 2003
June 20-24, 2004	**2004 International Conference on Communications (ICC)**	Paris, France	http://www.icc2004.org	Sept. 1, 2003
July 19-24, 2004	**2004 Stochastic Networks Conference**	Centre de Recherches Mathematiques Universite de Montreal Montreal, Canada	http://www.stanford.edu/group/stochnetconf/	
September 15-16, 2004	**InOWo '04 - 9th International OFDM Workshop**	Dresden, Germany	http://ofdm.tu-harburg.de Prof. Herman Rohling, TU Hamburg-Harburg, Eissendorfer Str. 40, D-21073 Hamburg, Germany, ofdm@tu-harburg.de	April 30, 2004
October 6-8, 2004	**2004 Asia-Europe Workshop on Information Theory (AEW4)**	Viareggio, Italy	http://www.exp-math.uni-essen.de/~vinck/aew4/aew4.html	May 1, 2004
October 10-12, 2004	**2004 International Symposium on Information Theory and its Applications (ISITA 2004)**	Parma, Italy	isita2004@sita.gr.jp http://www.sita.gr.jp/ISITA2004/new.htm	March 26, 2004
November 29- December 3 2004	**GLOBECOM 2004** ItalyMar.on Hoteew4/aohling, 2004 IEEE I nternational	Hyatt Regency Dallas at	http://www.globecom2004.org	March 1, 2004

IEEE Information Theory Society Newsletter
445 H e Lane, P. O. B 1331
Pi ca q a , NJ 08855-1331 USA