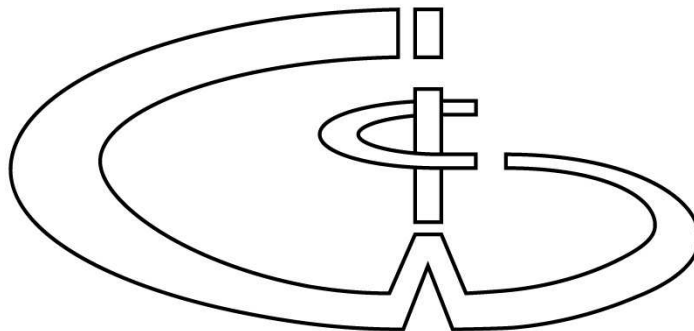


Program of the
24-th Symposium on Information Theory in the Benelux
De Koningshof, Veldhoven, The Netherlands
May 22 & 23, 2003

Organized by Philips Research Laboratories Eindhoven for the
Werkgemeenschap voor Informatie- en Communicatie theorie (WIC)



Co-sponsored by the IEEE Benelux Information Theory Chapter

Prize for the best presentation of a young researcher donated by the Gauss foundation.

Thursday, May 22

9.15 **Registration**

10.00 **Opening**

10.05 - 11.25 **Channel Coding and Decoding**

On understanding the performance of the IEEE 802.11a WLAN physical layer for the Gaussian channel,

Wim J. van Houtum, Philips Research Laboratories, Eindhoven

Set Decoding of Convolutional Codes with Application to GSM/GPRS,

Andries P. Hekstra, Philips Research Laboratories, Eindhoven

On the Use of the Cut-Off Rate for Determining Optimal Input Quantization of a Viterbi Decoder on Fading Channels,

Stan Baggen, Sebastian Egner, and Bertrand Vandewiele, Philips Research Laboratories, Eindhoven.

Static and Dynamic Chase-Like Bounded Distance Decoding,

Jos H. Weber, Delft University of Technology.

11.25 - 11.45 **Coffee and tea break**

11.45 - 12.45 **Invited Presentation**

Analyzing DNA microarrays to unravel gene function,

Marcel Reinders, Delft University of Technology.

12.45 - 13.45 **Lunch**

13.45 - 14.45 **Cryptanalysis**

Side-channel entropy for modular exponentiation algorithms,

Lejla Batina and Cees Jansen, SafeNet BV, Vught, and Katholieke Universiteit Leuven.

Extending the Boneh-Durfee-de Weger's attack to RSA-like Cryptosystems,

Fabien Laguillaumie and Damien Vergnaud, France Télécom R&D, Caen, and Université de Caen.

Key-Dependent Approximations in Cryptanalysis – An Application of Multiple \mathbb{Z}_4 and Non-Linear Approximations,

F.X. Standaert, G. Rouvroy, G. Piret, J.J. Quisquater, and J.D. Legat, Université Catholique de Louvain.

14.45 - 15.05 **Coffee and tea break**

15.05 - 16.25 Source coding

Huffman codes revisited,

R. Stasiński and G. Ulacha, Poznań University of Technology and Szczecin University of Technology

Improved Elastic Storage of Digital Still Images,

René J. van der Vleuten, Philips Research Laboratories, Eindhoven.

Optimal Partitioning of Video Sequences for MPEG-4 Sprite Encoding,

Dirk Farin, Peter H.N. de With, and Wolfgang Effelsberg, University of Mannheim, Logica CMG, and Eindhoven University of Technology.

A SW-based Complexity Scalable MPEG Encoder for Mobile Consumer Equipment,

S. Mietens, P.H.N. de With, and C. Hentschel, Eindhoven University of Technology, Logica CMG, and Philips Research Laboratories, Eindhoven.

16.25-16.45 Coffee and tea break

16.45 - 17.25 Data-embedding and Signal Separation

Capacity of reversible information embedding for small distortions,

Deran Maas, Ton Kalker and Frans Willems, Technical University Eindhoven, and Philips Research Laboratories Eindhoven.

Blind source separation of speech and background music for improved speech recognition, P. Vanroose, Katholieke Universiteit Leuven.

17.40 - 19.00 General Assembly of the WIC

19.00 Symposium Dinner

Friday, May 23

9.00 - 10.20 Biometrics

Biometric verification: A result and an exotic example,

Raymond Veldhuis, Asker Bazen, and Maarten Boersma, Twente University.

Verification using partially known biometrics,

Jasper Goseling, Stan Baggen and Ton Akkermans, Twente University, and Philips Research Laboratories, Eindhoven.

Reliable (robust) biometric authentication with privacy protection,

E. Verbitskiy, P. Tuyls, D. Denteneer, and J.-P. Linnartz, Philips Research Laboratories, Eindhoven.

Experimenting with Face Detection and Recognition for Home Surveillance: a Status Report,

F. Zuo and P.H.N. de With, Eindhoven University of Technology and Logica CMG.

10.20 - 10.40 **Coffee and tea break**

10.40 - 12.00 **Transmission and Recording Channels**

Equalization and Target Response Optimisation for High-Density Two-Dimensional Optical Storage,

J. Riani, J.W.M. Bergmans, S.J.L. van Beneden, W.M.J. Coene, and A.H.J. Immink, Eindhoven University of Technology and Philips Research Laboratories Eindhoven

Index Assignment Schemes for M-description Coding,

Jean Cardinal, Université Libre de Bruxelles.

An efficient algorithm for computing the entropy of output sequences for bitshift channels, Stan Baggen and Vladimir B. Balakirsky, Philips Research Laboratories, Eindhoven, and EIDMA.

Higher order asymptotics of mutual information for nonlinear channels with non-Gaussian noise,

V.V. Prelov and E.C. van der Meulen, IPPI, Moscow, and Katholieke Universiteit Leuven.

12.00 - 13.00 **Lunch**

13.00 - 14.20 **Cryptography**

A structure of block ciphers achieving some resistance against fault attacks,

Mathieu Ciet, Gilles Piret and Jean-Jacques Quisquater, Université Catholique de Louvain

Tensor Transform of Functions over finite fields,

Alexander Kholosha, Eindhoven University of Technology.

Efficient Designated Verifier Signature Schemes,

Shahrokh Saeednia, Steve Kremer, and Olivier Markowitch, Université Libre de Bruxelles.

Authenticated and efficient key management for ad-hoc networks,

Stefaan Seys and Bart Preneel, Katholieke Universiteit Leuven.

14.20 - 14.40 **Coffee break**

14.40 - 16.00 **Wireless Communication**

Algebraic Techniques for Signal Separation, L. de Lathauwer, B. de Moor, J. Vandewalle, and A. de Baynast, ETIS, Cergy-Pontoise, and Katholieke Universiteit Leuven.

Power allocation and optimal Tx/Rx structures for MIMO systems,

R. Cendrillon, O. Rousseaux, M. Moonen, Etienne van den Bogaert, and Jan Verlinden, Katholieke Universiteit Leuven, and Alcatel Bell Antwerpen.

A Power-Efficient Compound Modulation Scheme for Addressing Multiple Users in the Downlink,

Gerard J.M. Janssen, Delft University of Technology.

Novel Sampling Method for increased spectral efficiency in wireless communication systems,

J. Levendovsky, L. Kovács, A. Olah, D. Varga, and E.C. van der Meulen, Budapest University of Technology and Economics, and Katholieke Universiteit Leuven.