# Table of Contents

## Session 1: Channel coding and decoding

- On understanding the performance of the IEEE 802.11a WLAN physical layer for the Gaussian channel  
  Wim J. van Houtum  
  1

- Set Decoding of Convolutional Codes with Application to GSM/GPRS  
  Andries P. Hekstra  
  9

- 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  
  17

- Static and Dynamic Chase-Like Bounded Distance Decoding  
  Jos H. Weber  
  27

## Session 2: Invited lecture

- Analyzing DNA microarrays to unravel gene function  
  Marcel Reinders  
  35

## Session 3: Cryptanalysis

- Side-channel entropy for modular exponentiation algorithms  
  Lejla Batina and Cees Jansen  
  37

- Extending the Boneh-Durfee-de Weger's attack to RSA-like Cryptosystems  
  Fabien Laguillaumie and Damien Vergnaud  
  45

- Key-Dependent Approximations in Cryptanalysis – An Application of Multiple $\mathbb{Z}_4$ and Non-Linear Approximations  
  FX Standaert, G Rouvroy, G Piret, JJ Quisquater, and JD Legat  
  53

## Session 4: Source coding

- Huffman codes revisited  
  R. Stasiński and G. Ulacha  
  63

- Improved Elastic Storage of Digital Still Images  
  René J. van der Vleuten  
  71

- Optimal Partitioning of Video Sequences for MPEG-4 Sprite Encoding  
  Dirk Farin, Peter H.N. de With, and Wolfgang Effelsberg  
  79

- A SW-based Complexity Scalable MPEG Encoder for Mobile Consumer Equipment  
  S. Mietens, P.H.N. de With, and C. Hentschel  
  87
Session 5: Data-embedding and Signal Separation

- Capacity of reversible information embedding for small distorsions
  Deran Maas, Ton Kalker, and Frans Willems 95

- Blind source separation of speech and background music for improved speech recognition
  P. Vanroose 103

Session 6: Biometrics

- Biometric verification: A result and an exotic example
  Raymond Veldhuis, Asker Bazen, and Maarten Boersma 109

- Verification using partially known biometrics
  Jasper Goseling, Stan Baggen, and Ton Akkermans 117

- Reliable (robust) biometric authentication with privacy protection
  E. Verbitskiy, P. Tuyls, D. Denteneer, and J.P. Linnartz 125

- Experimenting with Face Detection and Recognition for Home Surveillance: a Status Report
  F. Zuo and P.H.N. de With 133

Session 7: Transmission and Recording Channels

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

- Index Assignment Schemes for M-description Coding
  Jean Cardinal 149

- An efficient algorithm for computing the entropy of output sequences for bitshift channels
  Stan Baggen and Vladimir B. Balakirsky 157

- Higher order asymptotics of mutual information for nonlinear channels with non-Gaussian noise
  V.V. Prelov and E.C. van der Meulen 165
Session 8: Cryptography

• A structure of block ciphers achieving some resistance against fault attacks
  Mathieu Ciet, Gilles Piret, and Jean-Jacques Quisquater 171

• Tensor Transform of Functions over finite fields
  Alexander Kholosha 179

• Efficient Designated Verifier Signature Schemes
  Shahrokh Saeednia, Steve Kremer, and Olivier Markowitch 187

• Authenticated and efficient key management for ad-hoc networks
  Stefaan Seys and Bart Preneel 195

Session 9: Wireless Communication

• An algebraic technique for blind MIMO deconvolution of constant modulus
  L. de Lathauwer, J. Vandewalle, and B. de Moor 203

• New algebraic techniques for the separation of DS-CDMA signals
  L. de Lathauwer, A. de Baynast, J. Vandewalle, and B. de Moor 211

• Power allocation and optimal Tx/Rx structures for MIMO systems
  R. Cendrillion, O. Rousseaux, M. Moonen, Etienne van den Bogaert, and Jan Verlinden 219

• A Power-Efficient Compound Modulation Scheme for Addressing Multiple Users in the Downlink
  Gerard J.M. Janssen 227

• 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 235