

Proceedings of the  
25th Symposium on Information Theory  
in the Benelux

June 2-4, 2004  
Kerkrade, The Netherlands

Edited by  
R. Pellikaan

Published by:  
Werkgemeenschap voor Informatie- en Communicatietheorie  
Eindhoven, The Netherlands, 2004

### Previous symposia

1.	1980	Zoetermeer, The Netherlands	Dept. of Electrical
2.	1981	Zoetermeer, The Netherlands	Engineering, Technical
3.	1982	Zoetermeer, The Netherlands	University, Delft
4.	1983	Haasrode, Belgium	ISBN 90-334-0690-X
5.	1984	Aalten, The Netherlands	ISBN 90-71048-01-2
6.	1985	Mierlo, The Netherlands	ISBN 90-71048-02-0
7.	1986	Noordwijkerhout, The Netherlands	ISBN 90-6275-272-1
8.	1987	Deventer, The Netherlands	ISBN 90-71048-03-9
9.	1988	Mierlo, The Netherlands	ISBN 90-71048-04-7
10.	1989	Houthalen, Belgium	ISBN 90-71048-05-5
11.	1990	Noordwijkerhout, The Netherlands	ISBN 90-71048-06-3
12.	1991	Veldhoven, The Netherlands	ISBN 90-71048-07-1
13.	1992	Enschede, The Netherlands	ISBN 90-71048-08-X
14.	1993	Veldhoven, The Netherlands	ISBN 90-71048-09-8
15.	1994	Louvain-la-Neuve, Belgium	ISBN 90-71048-10-1
16.	1995	Nieuwekerk a/d IJssel, The Netherlands	ISBN 90-71048-11-X
17.	1996	Enschede, The Netherlands	ISBN 90-365-0812-6
18.	1997	Veldhoven, The Netherlands	ISBN 90-71048-12-8
19.	1998	Veldhoven, The Netherlands	ISBN 90-71048-13-6
20.	1999	Haasrode, Belgium	ISBN 90-71048-14-4
21.	2000	Wassenaar, The Netherlands	ISBN 90-71048-15-2
22.	2001	Enschede, The Netherlands	ISBN 90-365-1598-X
23.	2002	Louvain-la-Neuve, Belgium	ISBN 90-71048-16-0
24.	2003	Veldhoven, The Netherlands	ISBN 90-71048-18-7

CIP-gegevens Koninklijke Bibliotheek, Den Haag (NL)

Proceedings

Proceedings of the 25-th Symposium on Information Theory in the Benelux/ ed.

R. Pellikaan, Eindhoven

Werkgemeenschap voor Informatie- en Communicatietheorie

ISBN:90-71048-20-9

The Twenty-fifth Symposium on Information Theory in the Benelux has been organized by

**Coding Theory and Cryptology Group**  
**Technical University of Eindhoven**  
**Eindhoven, The Netherlands**

on behalf of the Werkgemeenschap voor Informatie- en Communicatietheorie and the IEEE Benelux Information Theory Chapter.

**Program Committee:**

C.P.M.J. Baggen

A.A.C. Kalker

R. Pellikaan

H.C.A. van Tilborg

T.J. Tjalkens

L.M.G.M. Tolhuizen

B.M.M. de Weger

F.M.J. Willems

The organizing committee gratefully acknowledges the financial support of the Gauss foundation and the IEEE Benelux Information Theory Chapter.

# Preface

The Werkgemeenschap voor Informatie- en Communicatietheorie is organizing for the twenty-fifth time the annual Symposium on Information Theory.

This year the symposium is being held in Kerkrade, The Netherlands and has been organized by the Coding Theory and Cryptology Group of the Mathematics and Computer Science Faculty of the Technical University of Eindhoven.

We are very pleased that Prof. J.L. Massey has accepted our invitation to give an invited lecture for this special fifth lustrum of the symposium.

This book contains the 33 papers that have been accepted for presentation in oral sessions. We thank the programm committee consisting of Stan Baggen, Ton Kalker, Henk van Tilborg, Tjalling Tjalkens, Ludo Tolhuizen, Benne de Weger and Frans Willems for their reviews of the abstracts of submitted papers and the division in sessions.

The organizing committee gratefully acknowledges the IEEE Benelux Information Theory Chapter for their sponsorship and thanks the Gauss foundation for the financial support for the best Young Researcher Presentation Award.

Finally, I would like to express my thanks to Mrs. Anita Klooster for the assistance in the organization of this symposium.

Ruud Pellikaan, editor

Eindhoven, May 2004

# Table of Contents

## Channel coding & decoding

- *Chase-like bounded-distance decoding with  $O(d^{2/3})$  trials,*  
J.H. Weber\*, M.P.C. Fossorier, pp. 1-8.
- *Turbo-like soft-decision decoding of Reed-Solomon codes,*  
G. Van Meerbergen\*, M. Moonen, H. De Man, pp. 9-16.
- *To significantly reduce the computational load of UMTS turbo decoding,*  
A.P. Hekstra\*, J. Dielissen, pp. 17-24.
- *On the selection of guided scrambling sequences that provide  
guaranteed maximum run-length constraints,*  
A.J. van Wijngaarden\*, K.A. Schouhamer Immink, pp. 25-29.
- *Guaranteed scrambling*  
A.P. Hekstra, L. Tolhuizen\*, pp. 31-38.
- *On the size of a type of RLL codes,*  
K.A. Schouhamer Immink\*, C. Kui, pp. 39-46

## Invited lecture

- *The footsteps of Shannon,*  
J.L. Massey, pp. 47.

## Signal detection

- *A simple adaptive interference cancelation method for power line  
reduction in electrocardiography,*  
S.M.M. Martens\*, J.W.M. Bergmans, S.G. Oei, pp. 49-56.
- *Fundamental limits of non-linear receivers in optical fibre systems,*  
A. Martinez\*, F.M.J. Willems, pp. 57-64.
- *Improved correlation receiver for frame synchronization,*  
A. Nowbakht\*, J.W.M. Bergmans, S. Van Beneden, W.M.J. Coene,  
M. Ciacci, A.H.J. Immink, J. Riani, pp. 65-72.

## Source coding & data compression

- *Occurrence of patterns in random fields*,  
J.-R. Chazottes, F. Redig, E. Verbitskiy\*, pp. 73-80.
- *A comparative complexity study of fixed-to-variable length and variable-to-fixed length source codes*,  
T. Tjalkens\*, pp. 81-88.

## Cryptography & Cryptanalysis

- *Covering radius of the  $(N - 3)$ -rd order Reed-Muller code in the set of resilient functions*,  
Y. Borissov, A. Braeken, S. Nikova\*, pp. 89-96.
- *On the security of certain DPA countermeasures*,  
M. Ciet, F. Sica\*, J.-J. Quisquater, pp. 97-103.
- *Information theoretic measures applied to power and electromagnetic traces measured from an FPGA performing an elliptic curve point multiplication*,  
E. Dewitte\*, B. De Moor, B. Preneel, pp. 105-112.
- *On cheating immune secret sharing*,  
A. Braeken\*, S. Nikova, V. Nikov, pp. 113-120.

## Shannon theory

- *Optimal strategies for hierarchical guessing problem*,  
A.R. Ghazaryan\*, E.C. van der Meulen, pp. 121-128.
- *Code constructions for multiple-access channels with side information at the encoders*,  
P. Vanroose\*, pp. 129-136.

## **Biometrics**

- *Two-stage face recognition incorporating individual-class discrimination criteria,*  
F. Zuo\*, P.H.N. de With, pp. 137-144.
- *Figures of merit for biometric verification and a means for dimension reduction,*  
R. Veldhuis\*, A. Bazen, pp. 145-152.

## **Security**

- *Wireless security design overview,*  
N. Aboudagga, D. Giry\*, J.-J. Quisquater, pp. 153-160.
- *Secrecy in mobile code,*  
K. Cartrysse\*, J.C.A. van der Lubbe, pp. 161-168.
- *Security aspects of DRM systems,*  
H.L. Jonker\*, S. Mauw, J.H.S. Verschuren, A.T.S.C. Schoonen, pp. 169-176.
- *Cryptographic approach to patient records privacy protection in emergency situations,*  
K. Kapis\*, J.C.A. van der Lubbe, K. Cartrysse, pp. 177-184.
- *Security analysis of physical uncloneable functions,*  
P. Tuyls\*, B. Skoric, T. Akkermans, W. Ophey, S. Stallinga, pp. 185-192.

## **Video compression & signal processing**

- *On the computing analysis of arbitrary shape video coding in MPEG-4,*  
M. Pastrnak\*, P.H.N. de With, pp. 193-200.
- *Estimating physical camera parameters for 3DAV video coding,*  
D. Farin\*, P.H.N. de With, pp. 201-208.
- *Lossless and fine-granularity scalable near-lossless color image compression,*  
R.J. van der Vleuten\*, S. Egner, pp. 209-216.
- *Perceptual quality impact of geometric distortion in images,*  
I. Setyawan\*, R.L. Lagendijk, pp. 217-224.

## Transmission channels

- *Simple Doppler compensation for DVB-T*,  
S.A. Husen\*, S. Baggen, M. Stassen, H.Y. Tsang, pp. 225-232.
- *Designing optimal link scaling for routing with incomplete information in packet switched networks*,  
J. Levendovszky, A. Molnár\*, P. Boros, E.C. van der Meulen, pp. 233-239.
- *CNN based multiuser detection and equalization in wireless communication systems*,  
J. Levendovszky\*, A. Oláh, D. Varga, E.C. van der Meulen, pp. 241-248.

## Recording channels

- *Equalizer based tilt estimation for two-dimensional optical storage*,  
M. Ciacci\*, J. Riani, J.W.M. Bergmans, A.H.J. Immink, pp. 249-256.
- *Minimum loop-delay adaption and timing recovery for two-dimensional and optical storage*,  
S. Van Beneden\*, J.W.M. Bergmans, J. Rianni, M. Ciacci, A. Nowbakht, A.H.J. Immink, pp. 257-264.

Paper presented by \*

<i>Author</i>	<i>page</i>	<i>Author</i>	<i>page</i>
<i>N. Aboudagga</i>	153	<i>A. Molnar</i>	233
<i>T. Akkermans</i>	185	<i>M. Moonen</i>	9
<i>S. Baggen</i>	225	<i>B. De Moor</i>	105
<i>A. Bazen</i>	145	<i>V. Nikov</i>	113
<i>S. Van Beneden</i>	65, 257	<i>S. Nikova</i>	89, 113
<i>J.W.M. Bergmans</i>	49, 65, 249, 257	<i>A. Nowbakht</i>	65, 257
<i>Y. Borissou</i>	89	<i>S.G. Oei</i>	49
<i>P. Boros</i>	233	<i>A. Olah</i>	241
<i>A. Braeken</i>	89, 113	<i>W. Ophey</i>	185
<i>K. Cartrysse</i>	161, 177	<i>M. Pastrnak</i>	193
<i>J. – R. Chazottes</i>	73	<i>B. Preneel</i>	105
<i>M. Ciacci</i>	65, 249, 257	<i>J. – J. Quisquater</i>	97, 153
<i>M. Ciet</i>	97	<i>F. Redig</i>	73
<i>W. Coene</i>	65	<i>J. Riani</i>	65, 249, 257
<i>D. Giry</i>	153	<i>A.T.S.C. Schoonen</i>	169
<i>E. Dewitte</i>	105	<i>K.A. Schouhamer Immink</i>	25, 39
<i>J. Dielissen</i>	17	<i>I. Setyawan</i>	217
<i>S. Egner</i>	209	<i>F. Sica</i>	97
<i>D. Farin</i>	201	<i>B. Skoric</i>	185
<i>M.P.C. Fossorier</i>	1	<i>M. Stassen</i>	225
<i>A.R. Ghazaryan</i>	121	<i>S. Stallinga</i>	185
<i>A. Hekstra</i>	17, 31	<i>T. Tjalkens</i>	81
<i>S.A. Husen</i>	225	<i>L. Tolhuizen</i>	31
<i>A.H.J. Immink</i>	65, 249, 257	<i>H.Y. Tsang</i>	225
<i>H.L. Jonker</i>	169	<i>P. Tuyls</i>	185
<i>K. Kapis</i>	177	<i>P. Vanroose</i>	129
<i>C. Kui</i>	39	<i>D. Varga</i>	241
<i>R. L. Lagendijk</i>	217	<i>R. Veldhuis</i>	145
<i>J.C.A. van der Lubbe</i>	161, 177	<i>E. Verbitskiy</i>	73
<i>J. Levendovszky</i>	233, 241	<i>J.H.S. Verschuren</i>	169
<i>H. De Man</i>	9	<i>R.J. van der Vleuten</i>	209
<i>S.M.M. Martens</i>	49	<i>J.H. Weber</i>	1
<i>A. Martinez</i>	57	<i>A.J. van Wijngaarden</i>	25
<i>J.L. Massey</i>	47	<i>F.M.J. Willems</i>	57
<i>S. Mauw</i>	169	<i>P.H.N. de With</i>	137, 193, 201
<i>G. Van Meerbergen</i>	9	<i>F. Zuo</i>	137
<i>E.C. van der Meulen</i>	121, 233, 241		