Preliminary program for WCC'2005: Updated March 2

		Time incl. questions
Sunday afternoon	Registration	
Monday 7:30-	Registration	
Monday 8:45-9:00: Welcome		
Monday 9:00-10:00 Invited talk: Open problems related to algebraic attacks on stream ciphers	**Anne Canteaut**	01:00
Monday 10:00-11:50	**Coding Theory 1**	
Second Generalized Hamming Weights for Extremal Self-Dual Codes	Keisuke Shiromoto	0:30
(Break)		
Error and Erasure Correction of Interleaved Reed--Solomon Codes	Georg Schmidt, Vladimir R. Sidorenko, Martin Bossert	0:30
A Welch--Berlekamp like algorithm for decoding Gabidulin codes	Pierre Loidreau	0:30
On codes correcting symmetric rank errors	Nina I. Pilipchuk , Ernst M. Gabidulin	0:20
Monday 12:10-13:40	**Lunch**	
Monday 13:40-17:00	**Cryptography 1**	
Interpolation of the discrete logarithm in a finite field of characteristic two by Boolean functions	Nina Brandstaetter, Tanja Lange, Arne Winterhof	0:30
On Degrees of Polynomial Interpolations Related to Elliptic Curve Cryptography	Takakazu Satoh	0:30
Interpolation of Functions Related to the Integer Factoring Problem	Clemens Adelmann, Arne Winterhof	0:30
(Break)		
Finding good differential patterns for attacks on SHA-1	Krystian Matusiewicz, Josef Pieprzyk	0:30
Shorter keys for code based cryptography	Philippe Gaborit	0:30
Dimension of the linearization equations of the Matsumoto-Imai cryptosystems	A. Diene, J. Ding, J. E. Gower, T. J. Hodges, Z. Yin	0:30
Tuesday 9:00-10:00 Invited talk: Pseudocodewords, polytopes and low complexity coding techniques	**Ralf Koetter**	01:00
Tuesday 10:00-12:40	**Sequences**	
Constructions of Complementary Sequences for Power-Controlled OFDM Transmission	Kai-Uwe Schmidt, Adolf Finger	0:30
A Novel Method for Constructing Almost Perfect Polyphase Sequences	Xiangyong Zeng, Lei Hu, Qingchong Liu	0:30
(Break)		
Linear Filtering of Nonlinear Shift Register Sequences	Berndt M. Gammel, Rainer Göttfert	0:20
Realization of Decimation-Hadamard Transform for Binary Generalized GMW Sequences	Nam Yul Yu, Guang Gong	0:20
Reconstruction of Kronecker Sequences	Quanlong Wang, Qingchong Liu, Lei Hu	0:20
Frequency/Time Hopping Sequences with Large Linear Complexities	Yun-Pyo Hong, Hong-Yeop Song	0:20
Tuesday 12:40-14:10	**Lunch**	
Tuesday 14:10-17:20	**Coding Theory 2**	
New results on 2-weight projective cyclic codes	Jacques Wolfmann	0:30

On the weights of irreducible cyclic codes	Yves Aubry, Philippe Langevin	0:30
Sperner's theorem and unidirectional codes	Bella Bose, Torleiv Kløve	0:30
(Break)		
Geometric conditions for the extendability of ternary linear codes	Tatsuya Maruta, Kei Okamoto	0:30
Negacyclic Duadic Codes	Thomas Blackford	0:30
On semisimple algebra codes	Edgar Martinez-Moro	0:20
Wednesday 9:00-13:00	**Cryptography 2 and unrelated topics**	
Rate-Diversity Optimal Space-Time Code Constructions Based on the Generalized Binary Rank Criterion	A. Roger Hammons Jr.	0:20
New Constructions of Codes for DNA Computing	Olgica Milenkovic, Navin Kashyap	0:20
Reduction of conjugacy problem in braid groups, using theirs double Garside's structure	Samuel Maffre	0:20
Multi-Dimensional Hash Chains and Application to Micropayment Schemes	Quan Son Nguyen	0:20
(Break)		
A Chosen Ciphertext Attack on a Public Key Cryptosystem Based on Lyndon Words	Ludovic Perret	0:20
On the Affine Parts of HFE-Cryptosystems and Systems with Branches	Patrick Felke	0:20
RSA-Based Secret Handshakes	Damien Vergnaud	0:20
(Break)		
ID-Based Series-Parallel Multisignature Schemes for Multi-messages from Bilinear Maps	Lihua Wang, Eiji Okamoto, Ying Miao, Takeshi Okamoto, Hiroshi Doi	0:20
A new public-key cryptosystem based on the problem of reconstruction of p -polynomials	Cédric Faure, Pierre Loidreau	0:20
On Wagner-Magyarik cryptosystem	Françoise Levy-dit-Vehel, Ludovic Perret	0:20
Wednesday 13:00-14:30	**Lunch**	
Wednesday afternoon	**Excursion**	
Wednesday evening 19:00: Reception	**Schøttstuene**	
Thursday 9:00-10:00 Invited talk: Homomorphic Encryption for Secure Watermark Detection	**Ton Kalker**	01:00
Thursday 10:00-12:20	**Discrete Mathematics 1**	
Differentially Affine Maps	Gohar M. Kyureghyan	0:30
(Break)		
New Constructions of Almost Bent and Almost Perfect Nonlinear Polynomials	Lilya Budaghyan, Claude Carlet, Alexander Pott	0:30
On the Non-Existence of Crooked Functions on Finite Fields	Eimear Byrne, Gary McGuire	0:20

Classes of Plateaued Rotation Symmetric Boolean Functions under Transformation of Walsh Spectra	Alexander Maximov	0:20
Group Actions based Perfect Nonlinearity	Laurent Poinsot, Sami Harari	0:20
Thursday 12:20-13:50	**Lunch**	
Thursday 13:50-17:10	**Cryptography 3**	
The Asymptotic Behavior of 2-Adic Complexity	Andrew Klapper	0:30
A New Key Assignment Scheme for Access Control in a Complete Tree Hierarchy	Alfredo De Santis, Anna Lisa Ferrara, Barbara Masucci	0:30
Threshold Secret Sharing Schemes for XOR-based Visual Cryptography	P. Tuyls, H.D.L. Hollmann, J.H. van Lint, L. Tolhuizen	0:30
(Break)		
On a Relation Between Verifiable Secret Sharing Schemes and a Class of Error-Correcting Codes	Ventzislav Nikov, Svetla Nikova	0:30
Extending Gibson's attacks on the GPT cryptosystem	Raphael Overbeck	0:20
Information-Theoretically Secure Anonymous Group Authentication with an Arbiter	Kazuyuki Kinose, Takenobu Seito, Junji Shikata, Tsutomu Matsumoto	0:20
k-Resilient ID-Based Key Distribution Schemes from Pairing --- Three Party Case	Takeshi Okamoto, Raylin Tso, Tsuyoshi Takagi, Eiji Okamoto	0:20
Thursday 19:00	**Dinner**	
Friday 9:00-10:00: Invited talk: : Space-Time Codes Achieving the Diversity-Multiplexing Gain Tradeoff	**P. Vijay Kumar**	01:00
Friday 10:00-11:50	**Coding theory 3**	
3-Designs from Z_4-Goethals-like Codes and Variants of Cyclotomic Polynomials	Jyrki Lahtonen, Kalle Ranto, Roope Vehkalahti	0:30
(Break)		
Quaternary Convolutional Codes From Block Codes Over Galois Rings	Patrick Solé, Virgilio Sison	0:30
Improved Bounds On Weil Sums Over Galois Rings and Homogeneous Weights	San Ling, Ferruh Özbudak	0:30
Friday 11:50-13:20	**Lunch**	
Friday 13:20-16:00	**Discrete Mathematics 2**	
Bent Functions with 2^r Niho Exponents	Gregor Leander	0:30
Monomial Bent Functions	Gregor Leander	0:30
Spectral Interpretations of the Interlace polynomial	Constanza Riera, Matthew G. Parker	0:30
(Break)		
Inverses of Multivariate Polynomial Matrices using Discrete Convolution	Ruben Lobo, Donald Bitzer, Mladen Vouk	0:20
On reconstruction of functions on the hypercube	Anastasia Vasil'eva	0:30