

## Invited Talks (List Decoding Session; Organizer: Madhu Sudan)

- **List decoding and pseudorandom constructions**  
Venkatesan Guruswami
- **Iterative list decoding of LDPC codes**  
Tom Høholdt
- **Optimizing multivariate interpolation**  
Ralf Koetter
- **Efficient list decoding of explicit codes with optimal redundancy**  
Atri Rudra

## Invited Talks (General)

- **TBD**  
Manindra Agrawal
- **Error correction for network coding channels**  
Ralf Koetter
- **New attacks on the filter generator**  
Tor Helleseth
- **TBD**  
Tanja Lange
- **Spectra of boolean functions, subspaces of matrices, and going up versus going down**  
Gary McGuire
- **Algebraic structure theory of tail-biting trellises**  
Priti Shankar
- **Nice codes from nice curves**  
Henning Stichtenoth

## Contributed Talks

- **The tangent FFT**  
Daniel Bernstein
- **On quasi-cyclic codes over integer residue rings**  
Maheshanand Bhaintwal
- **Extended norm–trace codes with optimized correction capability**  
Maria Bras-Amoros and Michael O’Sullivan
- **Determining the nonlinearity of a new family of APN functions**  
Eimear Byrne

- **Links between discriminating and identifying codes in the binary Hamming space**  
Gerard Cohen, Irene Charon, Olivier Hudry, and Antoine Lobstein
- **Novel algebraic structure for cyclic codes**  
Bac Dang
- **On the computation of non-uniform input for list decoding on Bezerra-Garcia Tower**  
Prem Das
- **A Path To Hadamard Matrices**  
Peter Embury and Asha Rao
- **Generalized Sudan's list decoding for order domain codes**  
Olav Geil and Ryutaroh Matsumoto
- **Normalized minimum determinant calculation for multi-block and asymmetric space-time codes**  
Camilla Hollanti and Francis Lu
- **On generalized Hamming weights and the covering radius**  
Heeralal Janwa and Arbind Lal
- **Joint source-cryptographic-channel coding based on linear block codes**  
Haruhiko Kaneko and Eiji Fujiwara
- **The "Art of Trellis Decoding" is NP-hard**  
Navin Kashyap
- **Generalized rotation symmetric and dihedral symmetric boolean functions - 9 variable boolean functions with nonlinearity 242**  
Selcuk Kavut and Melek Yucel
- **Linear complexity and autocorrelation of prime cube sequences**  
Young-Joon Kim, Seok-Yong Jin, and Hong-Yeop Song
- **Lattices for distributed source coding: jointly gaussian sources and reconstruction of a linear function**  
Dinesh Krithivasan and Sandeep Pradhan
- **Dense MIMO matrix lattices - a meeting point for class field theory and invariant theory**  
Jyrki Lahtonen and Roope Vehkalahti
- **A note on a class of quadratic permutations over  $\mathbb{F}_{2^n}$**   
Yann Laigle-Chapuy
- **Fault-tolerant finite field computation in the public key cryptosystems**  
Silvana Medos

- **On the structure of inversive pseudorandom number generators**  
Harald Niederreiter and Arne Winterhof
- **An improvement of Tardos's collusion-secure fingerprinting codes with very short lengths**  
Koji Nuida, Satoshi Fujitsu, Manabu Hagiwara, Takashi Kitagawa, Hajime Watanabe, Kazuto Ogawa, and Hideki Imai
- **Space-time codes from crossed product algebras of degree 4**  
Frederique Oggier and Gregory Berhuy
- **Key independent bias in the permutation after RC4 key scheduling**  
Goutam Paul, Subhamoy Maitra, and Rohit Srivastava
- **Distribution of trace values and two-weight, self-orthogonal codes over  $GF(p, 2)$**   
Nimalsiri Pinnawala, Asha Rao, and T. Aaron Gulliver
- **Subcodes of Reed-Solomon codes suitable for soft decoding**  
Safitha J Raj
- **Quaternary Plotkin constructions and quaternary Reed-Muller codes**  
Josep Rifà, Jaume Pujol, and Faina Solov'eva
- **Construction of rotation symmetric boolean functions on odd number of variables with maximum algebraic immunity**  
Sumanta Sarkar
- **Constructions of orthonormal lattices and quaternion division algebras for totally real number fields**  
B.A. Sethuraman and Frederique Oggier
- **On the key-privacy issue of McEliece public-key encryption**  
Shigenori Yamakawa, Yang Cui, Kazukuni Kobara, Manabu Hagiwara, and Hideki Imai
- **Homomorphic encryptions of non-cyclic abelian groups**  
Akihiro Yamamura
- **Correctable errors of weight half the minimum distance plus one for the first-order Reed-Muller codes**  
Kenji Yasunaga and Toru Fujiwara
- **Secure cross-realm client-to-client password-based key exchange against undetectable on-line dictionary attacks**  
Kazuki Yoneyama, Haruki Ota, and Kazuo Ohta
- **Codes with low peak-to-average power ratio for multi-code CDMA**  
Jianqin Zhou