I M B M **istanbul matematiksel bilimler merkezi**
**istanbul center for mathematical sciences**

# Mathematical Aspects of Curve Based Cryptography

29-30 May 2014

The workshop includes constructive and algorithmic topics from finite fields, algebraic curves, coding theory and cryptography.

**Speakers :**

Murat Cenk (Middle East Technical University) *New efficient multiplication algorithms for binary extension fields and applications to curvebased cryptography*

Cem Güneri (Sabancı University) *TBA*

Stefan Hellbusch (Carl von Ossietzky University of Oldenburg) *Riemann-Roch on graphs*

Florian Hess (Carl von Ossietzky University of Oldenburg) *Zeta functions of curves over finite fields*

Jan Steffen Müller (Carl von Ossietzky University of Oldenburg) *Canonical heights on Jacobian surfaces*

Chrisitan Neurohr (Carl von Ossietzky University of Oldenburg) *Construction of minimal relative quadratric extensions*

Ferruh Özbudak (Middle East Technical University) *Non-extendable $\mathbb{F}_q$-quadratic perfect nonlinear maps*

Buket Özkaya (Sabancı University) *Multidimensional Quasi-Cyclic and Convolutional Codes*

Seher Tutdere (Gebze Institute of Technology) *Recursive Quadratic Towers of Function Fields over $\mathbb{F}_2$*

Emrah Sercan Yılmaz (Middle East Technical University) *Jouxs Algorithm for Discrete Logarithms in Small Characteristic)*

**Place :** IMBM Seminar Room, Boğaziçi University South Campus

The workshop is supported by a BMBF (Federal Ministry of Education and Research, Germany)-TÜBİTAK project on mathematical aspects of curve-based cryptography (No: 112T011)