Jarní škola 2010: program

Středa

Hlaváč Martin - Fully homomorphic encryption

Keselý Michal - Samoopravné kódy

Kotil Jaroslav - Samoopravné kódy

Teplá Kateřina - Samoopravné kódy

Frisová Andrea - Quasigroups and their use in cryptography

Christov Adam - Quadratic quasigroups in public-key cryptography

Čtvrtek

Stankovianská Veronika - Feedback Shift Register Sequences

Kubečka David - Minimal Polynomials and Periods

Šlesinger Radek - Generátory pseudonáhodných čísel

Lechner Jiří - Generátory pseudonáhodných čísel

Kukučková Michaela & Jakub Bulín - Rational points on elliptic curves part I - introduction

Jabłoński Bartosz - What do we know about mode reducts of commutative monoids?

Pátek

Opršal Jakub - Rational points on elliptic curves part II – Points of orders 2 and 3

Kazda Alexandr - Elliptic curves, volume 4 - Points of finite order

Vlachý Jan - Elliptic curves - continued

Perůtka Lukáš - Mordell-Weil Theorem

Werl Milan - Diophantine Equation y^2 + 2 = x^3

Kuben Jaromír - Racionální body eliptických křivek

Hubáček Pavel - SAGE : Open-Source Mathematics Software

Sobota

Jirotka Tomáš - A Course in Logic and Complexity - Descriptive Complexity Theory

Paták Pavel - Finite model theory

Čarnoký Samuel - Logika a složitost

Pich Ján - Logika a složitost

Glivický Petr - Peano arithmetic - models and unprovability

Neděle

Veselý Petr - Boolean Functions in Cryptology - Introduction

Ferov Michal - Linear Cryptanalysis and Boolean Functions

Barboriková Jana - Differential Cryptanalysis and Boolean Functions

Skalický Jakub - Examples of Boolean Functions in Ciphers