Interactive proof systems
(3 hours tutorial)

Vadym Fedyukovych *

Abstract
This tutorial provides a survey of applications of interactive proof systems in cryptography and outlines recent development with challenge-response systems.

Outline of the Presentation
1. An Informal Introduction (10 minutes).
2. Definitions (30 minutes).
3. Efficient interactive proof systems (20 minutes).
4. Protocols for Boolean OR and AND (10 minutes).
5. Commitment schemes with groups of a hidden order (10 minutes).
6. Testing polynomial relations (70 minutes).
   Overview of protocols for a codeword of Goppa code and small error weight, small set difference, graph isomorphism and Hamiltonicity, multiple substring matching, boolean OR, exact threshold, blind signature scheme.
7. Questions and discussion (30 minutes).

Intended audience

This tutorial is intended to help students and researchers understand interactive proof systems. No special knowledge is required. Attendees are expected to understand basic logic and basic operations with polynomials. Basic knowledge of computationally hard problems (namely Discrete Logarithm and Factorisation) would be an advantage.

Short Biography of Presenter

Author’s recent academic interests include designing interactive proof systems for approximate matching, electronic signatures tolerating errors below a threshold, anonymous credentials systems. Author holds a Diploma in physics from Moscow Institute of Technology and in applied mathematics from a military academy.

Selected Publications

5. An argument for Hamiltonicity. [IACR preprint][CECC conference, 2009]
6. Committing with partial knowledge of group order. [CECC conference, 2010]
7. A strategy for any DAA Issuer and an additional verification by a Host. [IACR preprint][ITA conference, 2008]