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).
   A tale of a cave with a hidden door (Quisquater-Guillou-Berson 1989). Applications of protocols: signature schemes, group signature schemes, verifiable protocols including cash, voting, secret sharing. Recent industry development: DAA, U-Prove.
2. Definitions (30 minutes).
   Interactive proof systems. Proofs and arguments. Proofs of knowledge. Witness hiding and witness indistinguishable protocols. Zero knowledge and honest verifier zero knowledge.
3. Efficient interactive proof systems (20 minutes).
   Homomorphic commitment schemes. Protocols with 'algebraic' responses and with only a negligible soundness error (Chaum et al 1987, Schnorr 1989, Guillou-Quisquater 1988).
4. Protocols for Boolean OR and AND (10 minutes).
5. Committment schemes with groups of a hidden order (10 minutes).
6. Testing polynomial relations (70 minutes).
   'Verification polynomials' with witness replaced by Prover's response. Top coefficient of verification polynomial produced with responses of Chaum-Schnorr style. Alternative 'algebraic' responses. Testing polynomial identity, Schwartz-Zippel lemma. Protocols with multiple challenges.
   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).

[*] A proposal for 3rd International Conference on Security of Information and Networks (SIN 2010, Taganrog).

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

1. Argument of knowledge of a bounded error.
   An IACR preprint. Sibecrypt conference, 2009. Journal version (in Russian).
2. A signature scheme with approximate key matching.
   Information Security conference, Kiev 2007. ITaS conference, 2009, pages 396-400 (in Russian).
3. Proving polynomial identities.
   Information Security conference, Kiev 2008.
4. A protocol for K-multiple substring matching (with Vitaliy Sharapov).
   IACR preprint. ITaS conference, 2008, pages 459-466 (in Russian).
5. An argument for Hamiltonicity.
   IACR preprint. MaBIT conference, 2008. 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.
8. A blind signature scheme (submitted).