Název práce: Interaktivní důkazy
Autor: Jana Kučerová
Katedra (ústav): Katedra algebry
Vedoucí bakalářské práce: Doc.RNDr. Jiří Tůma,DrSc.
e-mail vedoucího: tuma@karlin.mff.cuni.cz

Abstrakt: Předložená práce se věnuje kryptografickým protokolům pro interaktivní důkazy. Protože tyto protokoly jsou jedny ze složitějších, jsou v první části práce popsána některá jednodušší kryptografická schémata, která jsou později využita jako stavební prvky těchto protokolů. V této práci jsou interaktivní důkazy nejprve definovány jako výpočet spojené dvojice interaktivních Turingových strojů. Později je uvedena souvislost takto definovaného interaktivního důkazu s interaktivním důkazem znalosti dokazovatelova tajemství v identifikačních protokolech. Na příkladu několika identifikačních protokolů je ukázáno, jakým způsobem lze rozhodnout, zda se jedná o důkaz s nulovou znalostí nebo zda je daný protokol prokazatelně bezpečný.

Klíčová slova: kryptografický protokol, Turinguv stroj, prokazatelná bezpečnost, důkaz s nulovou znalostí

Title: Interactive proofs
Author: Jana Kučerová
Department: Department of Algebra
Supervisor: Doc.RNDr. Jiří Tůma,DrSc.
Supervisor's e-mail address: tuma@karlin.mff.cuni.cz

Abstract: The main topic of the present work is cryptographic protocols for interactive proofs. Because of complexity of these protocols, at first we describe some cryptographic elements, which we will use later as building blocs of interactive proof protocols. In this work, we define interactive proofs as a joint computation of a linked pair of two interactive Turing machines. Later, we explain the relation between this definition and an interactive proof of knowledge of a prover's secret in identification protocols. We present examples of several identification protocols and demonstrate how we can determine, if the given protocol is provably secure or if it is a zero-knowledge proof.

Keywords: cryptographic protocol, Turing machine, provable security, zero-knowledge proof