Názov práce: Důkazy bezpečnosti digitálních podpisů

Autor: Anna Godušová

Katedra (ústav): Katedra algebry

Vedúci bakalárskej práce: Mgr. Štěpán Holub Ph.D.

Abstrakt: Predložená práca sa zaoberá podpisovacími schémami, ktoré sa používajú na digitálne podpisovanie dokumentov. Presnejšie sa zaoberá obecnými podpisovacími schémami založenými na permutácii s padajúcimi dvierkami. Na úvod dokážeme bezpečnosť obecnej schémy, ďalej kvantifikujeme túto bezpečnosť a dokážeme bezpečnosť podpisovacej schémy na základe bezpečnosti permutácie s padajúcimi dvierkami. Na záver predstavíme upravenú schému s pravdepodobnostným hašovaním pre lepšie odhady v bezpečnosti.

Kľúčové slová: digitálny podpis, podpisovacia schéma, kvantifikovaná bezpečnosť, PSS