Název práce: Kryptografie založená na kvadratických tělesech

Autor: Milan Straka

Katedra (ústav): Katedra algebry

Vedoucí diplomové práce: RNDr. David Stanovský, Ph.D.

E-mail vedoucího: *David.Stanovsky@mff.cuni.cz*

Abstrakt: Imaginární kvadratická tělesa byla navržena pro použití v asymetrické kryptografii Buchmannem a Williamsem již v roce 1988 a od té doby vznikly i další kryptografické protokoly. I když tyto protokoly nejsou tak efektivní jako podobná schémata s eliptickými křivkami, mohou konkurovat schématům založeným na RSA, a navíc je jejich bezpečnost považována za nezávislou na bezpečnosti běžných kryptosystémů jako RSA, DSA a ECC.

Tato práce shrnuje dosavadní výsledky v oboru kvadratické kryptografie. Jednak popisuje algebraickou teorii nutnou pro zavedení třídové grupy imaginárních kvadratických těles a dále studuje algoritmy operací v třídové grupě, jak asymptoticky, tak prakticky efektivní. Také rozebírá vhodná kryptografická schémata a útoky na ně.

Součástí této práce je knihovna, která popsané protokoly efektivně implementuje.

Klíčová slova: třídová grupa imaginárního kvadratického tělesa, diskrétní logaritmus, asymetrická kryptografie, šifrovací a podpisové schéma

Title: Qudratic field based cryptography

Author: Milan Straka

Department: Department of Algebra

Supervisor: RNDr. David Stanovský, Ph.D.

Supervisor's e-mail address: *David.Stanovsky@mff.cuni.cz*

Abstract: Imaginary quadratic fields were first suggested as a setting for public-key cryptography by Buchmann and Williams already in 1988 and more cryptographic schemes followed. Although the resulting protocols are currently not as efficient as those based on elliptic curves, they are comparable to schemes based on RSA and, moreover, their security is believed to be independent of other widely-used protocols including RSA, DSA and elliptic curve cryptography.

This work gathers present results in the field of quadratic cryptography. It recapitulates the algebraic theory needed to work with the class group of imaginary quadratic fields. Then it investigates algorithms of class group operations, both asymptotically and practically effective. It also analyses feasible cryptographic schemes and attacks upon them.

A library implementing described cryptographic schemes is a part of this work.

Keywords: class group of imaginary quadratic field, discrete logarithm, public-key cryptography, encryption and signature scheme