Title: Attacks based on hardware bugs
Author: Martina Válková
Department: Department of Algebra
Supervisor: Mgr. Štěpán Holub, Ph.D.
Supervisor's e-mail address: Stepan.Holub@mff.cuni.cz

Abstract: The study concerns hardware bugs producing computational errors and cryptanalytic attacks which utilize them. Particularly, the research is focused on attacks presented in the article by Biham E., Carmeli Y., Shamir A.: Bug Attacks [1] and their practical application in the case of schemes RSA and Pohlig-Hellman and various computational circumstances, which points out bigger vulnerability of schemes in the case of using the Right-to-Left modular exponentiation algorithm. The attacks have been tested against the software simulation of a faulty processor, which confirmed that they pose a real security threat in point of that situation. The mathematical part of this work concerns the problem of the finding any roots in $\mathbb{Z}_p$.

Keywords: hardware bug, attack, RSA, roots modulo p