Název práce: Útoky založené na hardwarových chybách
Autor: Martina Válková
Katedra (ústav): Katedra algebry
Vedoucí bakalářské práce: Mgr. Štěpán Holub, Ph.D.
e-mail vedoucího: Stepan.Holub@mff.cuni.cz

Abstrakt: V předložené práci studujeme využití hardwarových výpočetních chyb pro realizaci kryptoanalytických útoků. Zaměřujeme se konkrétně na návrhy útoků prezentovaných v článku Biham E., Carmeli Y., Shamir A.: Bug Attacks [1] a zkoumáme jejich praktické použití vůči schématům RSA a Pohlig-Hellman, včetně možnosti rozšíření a adaptace útoků na různé výpočetní okolnosti, přičemž upozorňujeme na vyšší zranitelnost schémat při realizaci modulárního mocnění použitím algoritmu Right-to-Left. Přinášíme výsledky praktického testování útoků prováděných vůči softwarové simulaci bugového procesoru, které potvrzují skutečnou bezpečnostní hrozbu uvažované situace. Čistě matematická část práce je věnována výpočetnímu předpokladu jednoho z útoků, problematice hledání odmocnin v $\mathbb{Z}_p$.

Klíčová slova: hardwarová chyba, útok, RSA, odmocniny modulo p