SPA on NTRU software implementation

T. Rabas, R. Lorencz, J. Bucek
Czech Technical University, Prague, Czech republic

Abstract

Assuming the existence of quantum computers, currently, standardized public-key cryptosystems are broken. NTRU is a promising candidate for standardization as a post-quantum public-key cryptosystem based on lattices. As its security evaluation process continues, researchers shift their attention also to side-channel attacks like power analysis or others. Several implementations claim to be power analysis resistant, especially resistant against simple and single-trace power analysis. An Soojung, et al. describe in the article "Single trace side channel analysis on NTRU implementation." an attack by power analysis and suggest protected implementation that should be resistant against all currently known power analysis attacks. We describe in our article a new simple power analysis attack that exploits a systematic weakness in the suggested implementation. We theoretically explain the attack and show its simulation on a computer. We discuss possible countermeasures and show that even the promising ones would not help to protect against the attack in a substantial manner.