A Novel Partial Key Exposure Attack on CRT-RSA Cryptosystem

Amir Hamzah Abdul Ghafar
Universiti Putra Malaysia

Abstract

Partial key exposure attack on a cryptosystem is becoming a more common cryptanalysis method since it has been shown that machine learning applications can aid it. However, a traditional approach to conduct this attack by manipulating the algebraic structure of the targeted cryptosystem is still producing some fascinating results. In this talk, we discuss a novel attack of partial key exposure on the CRT-RSA cryptosystem. The attack differs from previous methods due to its flexible properties to adjust the probability of a successful attack based on the computational power of an adversary. The method relies on a special function called Dickman's function that is generally used to estimate the proportion of smooth numbers up to a given bound. We also discuss the possibility to extend this attack to other variants of RSA.