The Blömer-May’s weak key revisited

ABSTRACT

Blömer-May's attack is a notable cryptanalysis towards RSA cryptosystem, which can be viewed as an extension of the Wiener's attack such that focused on its generalized for of key equation. Note that the said attack can lead a polynomial time factorisation of modulus N via continued fraction method. Later, the attack was reformulated to satisfies xy<N/(4(p+q)). In this paper, we propose an improved bound of Blömer-May's generalized key exponents that satisfies xy<(3(p+q)N)/(2((p-q)N^(1/4+(p+q)^2))). We show that our result is marginally better than the previous study.

Keyword: RSA cryptosystem; Cryptanalysis; Weak key; Generalized key equation; Continued fraction