A NEW ALGORITHM FOR THE VARIANTS OF APPROXIMATE GREATEST COMMON DIVISOR PROBLEM

Changmin Lee [1]

1) *The Research Institute of Basic Sciences, Seoul National University, Seoul 08826, KOREA*

Corresponding Author : Changmin Lee, cocomi11@snu.ac.kr

ABSTRACT

The AGCD-CRT problem, which is a variant of approximate greatest common divisor problem, has been served as a useful tool for constructing several cryptographic schemes such as a candidate of multilinear map. The AGCD-CRT problem is to find a prime factor of $N = \prod_{i=1}^{n} p_i$ when an integer N and AGCD-CRT samples which are congruent to a ρ-bit integer modulo each η-bit prime p_i are given.

In this paper, we propose a novel algorithm to solve the AGCD-CRT problem by employing lattice reduction algorithms and quadratic form under the Gaussian Heuristics assumption. Our algorithm takes $2^{\tilde{O}(\frac{n}{\eta-3\rho})}$ time complexity. Additionally, we revisit the previous lattice attack for solving AGCD-CRT and show that it takes $2^{O(n)}$ time complexity. From the result, we conclude that our algorithm is better than the previous attack.