1116-VI-2133 **Bal K Khadka*** (bkhadka@fau.edu), 630 NW 13th St, Apt 27, Boca Raton, FL 33486, and **Spyros Magliveras**. *Drawbacks of LLL Lattice Basis Reduction Algorithm.*

In this paper we show how to circumvent some drawbacks and peculiarities of the LLL algorithm. To solve the *approximate shortest vector* in hard lattice problems, we have introduced some techniques such as: *lattice diffusion* and *sublattice fusion*, *hill climbing*, *simulated annealing* etc., each requiring a large number of parallel calls of the LLL algorithm, while attempting to solve the lattice basis reduction problem. The *lattice diffusion* and *sublattice fusion* algorithm is a technique based on the LLL algorithm. It relies on performing a large number of LLL reductions on permuted bases of a family of, not necessarily disjoint, sublattices and then fusing the reduced bases of the sublattices. In particular, we obtain best possible results for a number of competition instances in the problem.

Keywords: LLL, Lattice Basis Reduction, permutation matrix, Integer unimodular matrix. (Received September 22, 2015)