World Academy of Science, Engineering and Technology
International Journal of Computer and Information Engineering
Vol:16, No:04, 2022

Solving LWE by Pregressive Pumps and Its Optimization

Authors : Leizhang Wang, Baocang Wang

Abstract : General Sieve Kernel (G6K) is considered as currently the fastest algorithm for the shortest vector problem (SVP) and record holder of open SVP challenge. We study the lattice basis quality improvement effects of the Workout proposed in G6K, which is composed of a series of pumps to solve SVP. Firstly, we use a low-dimensional pump output basis to propose a predictor to predict the quality of high-dimensional Pumps output basis. Both theoretical analysis and experimental tests are performed to illustrate that it is more computationally expensive to solve the LWE problems by using a G6K default SVP solving strategy (Workout) than these lattice reduction algorithms (e.g. BKZ 2.0, Progressive BKZ, Pump, and Jump BKZ) with sieving as their SVP oracle. Secondly, the default Workout in G6K is optimized to achieve a stronger reduction and lower computational cost. Thirdly, we combine the optimized Workout and the Pump output basis quality predictor to further reduce the computational cost by optimizing LWE instances selection strategy. In fact, we can solve the TU LWE challenge (n = 65, q = 4225, = 0:005) 13.6 times faster than the G6K default Workout. Fourthly, we consider a combined two-stage (Preprocessing by BKZ- and a big Pump) LWE solving strategy. Both stages use dimension for free technology to give new theoretical security estimations of several LWE-based cryptographic schemes. The security estimations show that the securities of these schemes with the conservative Newhope's core-SVP model are somewhat overestimated. In addition, in the case of LAC scheme, LWE instances selection strategy can be optimized to further improve the LWE-solving efficiency even by 15% and 57%. Finally, some experiments are implemented to examine the effects of our strategies on the Normal Form LWE problems, and the results demonstrate that the combined strategy is four times faster than that of Newhope.

Keywords : LWE, G6K, pump estimator, LWE instances selection strategy, dimension for free
Conference Title : ICPQC 2022 : International Conference on Post-Quantum Cryptography
Conference Location : Istanbul, Türkiye
Conference Dates : April 21-22, 2022