Implementing the dual approaches for solving LWE

Baptiste Maillard

The observed performance of two dual lattice attacks should encourage us to develop these attacks further.

Lattice-based cryptography relying on the LWE problem is becoming more and more essential in post-quantum cryptography. Recently, Guo and Johansson as well as MATZOV have both proposed an improved dual lattice attack against several NIST lattice candidates. The results achieved by these two attacks in this work lead us to believe that the development of dual lattice attacks should be pursued.

This work is part of post-quantum cryptography, a branch of cryptography aiming at guaranteeing the security of information against the hypothetical advent of quantum computers, whose theoretical power would make it possible to solve computational problems (like the factoring and discrete log problems) on which many of today's security systems are based.

This work adopts a practical approach to the two different procedures that enables the testing and validation of the theoretical constructs presented in these two papers. Through practical implementation, this thesis evaluates the efficacy of these procedures within real-world scenarios. This shift from essentially theoretical analyses to concrete application lends substantial importance to both papers, affirming the significance of their findings.

One of the aims of this work was to obtain statistics on the performance of the two dual attacks by carrying out experiments and then comparing them with the theory found in the papers from which the attacks studied were taken. The experiments consisted in observing the number of short vectors required for the attack to be successful. The experiments were carried out for each dual lattice attack, and the impact of changing a parameter on the results was also observed. The first thing to notice is that, in each case, both attacks were successful, i.e., the part of the secret key we wanted to guess was determined. In addition, the effect of the parameter change on the result was correctly identified. One of the conclusions of this work is that the results obtained from the experiments are close to the theoretical results presented in formula form in the papers from which the attacks studied were taken. This work also contains comments and explanations of the results. This work also highlights the similarities and differences between the two attacks.

In conclusion, this work serves as a solid foundation for future research, particularly for delving deeper into statistical assessments of dual lattice attacks' performance. This work can and should provide encouragement for further development and improvements in dual lattice attack strategies.