Abstract:
A major goal of computational complexity theory is to classify computational problems into tractable and intractable ones. The most adopted definition of tractability is polynomial time solvability.

Problems are shown to be intractable based on assumptions such as "P is not equal to NP" or "integer factorization requires super-polynomial time".

The goal of fine-grained complexity theory is to determine more precise complexities of computational problems using more quantitative but plausible hardness assumptions. Recently we have seen lots of exciting algorithmic and hardness results in this rapidly developing field. I will present a personal survey on fine-grained complexity focusing on topics related to cryptography such as the shortest and closest vector problems, systems of multivariate polynomial equations and fine-grained average-case hardness.