Lattice-Based Cryptography

Katharina Boudgoust

February 25, 2021

Let us assume there are two people who want to exchange messages safely, such that a third person cannot extract any information on their content. To imagine the situation better, let us call the three Frances, Barbara and Shafi.[1] In order to choose a good solution, Frances and Barbara read up on *cryptography.* They think that this sounds nice and further look into the topic. They learn that if they use a *provable secure* encryption scheme, the fact that their messages stay unintelligible for Shafi is guaranteed by the difficulty of some mathematical problem. In other words, any information leaked on their exchanged messages could be used to solve a mathematical problem that is believed to be intractable. And as there were many mathematicians who have already tried for a long time to solve this mathematical problem, this seems quite improbable. However, Frances reads about a threat that some of the problems used in cryptography may be solved much faster than what people thought before. More precisely, if we were in the possession of super computers that use quantum instead of classical mechanics, some mathematical problems would become easy to solve and with them many of the current cryptographic schemes insecure. After reading this, Frances feels uncomfortable, this super computer sounds really dangerous. Barbara reassures her, it is quite difficult to build quantum computer and currently, no such one powerful enough to solve a cryptographic challenge exists. However, it is important to start thinking about alternatives which are not threatened by those super computers as soon as possible. This field of research is called *post-quantum cryptography*, and *lattice-based cryptography*, where my research focuses on, is a subfield of it. Its cryptographic protocols are based on the intractability of problems on Euclidean lattices. Those problems have been studied quite some time and, so far, nobody knows how a quantum computer could solve them in a faster way than a classical computer. That means, even if Shafi possessed a powerful quantum computer, she would need as much time as with a less powerful normal computer to solve the mathematical problem on lattices. That reassures Frances and Barbara! I am part of the researchers who are studying such quantum resistant alternatives in order to prepare us for the future. Therefore, I investigate the theoretical and practical security of schemes that are based on the hardness of lattice problems. In particular, I study schemes that are based on slightly modified versions of them.

[1] An attentive reader may have recognized that those are the three women that have been awarded the Turing Award, Frances Allen, Barbara Liskov and Shafi Goldwasser.