This thesis focuses on proof of reduction from approximate SBP to SIS. The proof was already accomplished by Miklós Ajtai in 1996 in his groundbreaking work, however his proof lacks level of detail. The reduction is worst-case to average-case and no reduction of this type was known prior to the Ajtai's one. That is the reason why we found appropriate to return to the proof and provide it in more detailed form. Furthermore, the complexity of basic lattice problems is summarized. Based on these complexities and proven reduction, it is possible to define collision-resistant hash functions. This work is also briefly focused on such functions.