This topic is tightly connected to the H2020 project PANORAMIX (http://cordis.europa.eu/project/rcn/194872_en.html). PANORAMIX aims to implements mix-nets for privacy-preserving applications like e-voting. A robust mix-net must use a zero-knowledge shuffle argument. Most existing zero-knowledge arguments are almost ideally parallelizable, and hence should be ideally suitable for implementing on GPUs. However, we are aware of no such implementation. The task of the student is, together with supervisor and European partners, to pick out one or two possible shuffle arguments and implement / optimize them on contemporary GPUs.