Secure multi-party computation (MPC) enables a set of parties to jointly run a protocol that computes some function f on their private inputs, while preserving a number of security properties. Two of the most important properties are privacy and correctness. A specific variant of multiparty computation is the set intersection problem, which is a fundamental problem in secure MPC and has been a hot-topic in the past years.

Private set intersection is a secure way of computing the intersection of sets of two or multiple parties. Namely, in a two-party case, two parties hold two private data sets X_1 and X_2, and the protocol outputs the intersection of the two sets $X_1 \cap X_2$ and no extra information about the inputs of the parties. In the multi-party case, the secure intersection will be computed among the private data sets of n parties each of which holds X_i's, that is, $X_1 \cap \cdots \cap X_n$. On top of this, threshold private set intersection becomes an object of interest recently. Basically, they compute the threshold intersection which outputs the result if the cardinality of intersection is over some threshold in the two-party case. While in the multi-party case, if an element appears in the different private data set above a number of times (threshold), it is outputted in the intersection. However, until recently, threshold two-party and multiparty PSI have not been well-studied yet.

Hence, we are looking for a master student who is going to design new secure private set intersection protocols and make their software implementation for his master thesis. Students who like cryptographic protocols and applied cryptography courses come to talk to Asli Bay (a.bay@cs.ru.nl) about details of the project.