Optimal Communication Unbalanced Private Set Union

Alexis GALAN

February 20, 2024

Abstract

We consider a protocol allowing a whislteblower to report an alert to a supranational institution. The supranational institution is expected to have much more computational ressources than the whistleblower, who might only use a phone to communicate. The security expected in such a protocol is the following: The institution should not learn which data it already owned, because it could leak some clue on the identity of the whistleblower and compromise its anonymity. Also, the whistleblower should not learn anything from the data owned by the institution, so in particular, it should not learn which data the institution already had.
Such a protocol is an unbalanced private set union protocol (UPSU), where a receiver inputs a large data set and a sender inputs a small data set. The protocol should output to the receiver the union of the two sets, without learning anything on the intersection of the sets, while the sender should not learn anything.
Our main goals in the conception of an UPSU are to achieve asymptotically a communication volume linear in the size of the small set, and a computation cost for the sender independant of the size of the receiver's set. Using an efficient multipoint polynomial evaluation algorithm together with a linearly homomorphic encryption scheme (LHE) and an efficient polynomial remainder algorithm together with a fully homomorphic encryption scheme (FHE), we have reached those goals. To our knowledge, ours is the first protocol that has a communication volume independant of the size of the receiver's set.

Keywords— UPSU, LHE, FHE, multipoint evaluation, polynomial remainder, communication volume.