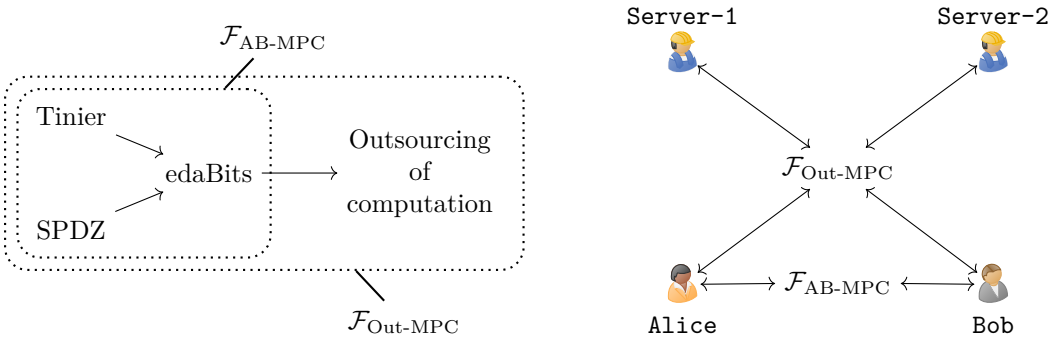
Outsourcing MPC Precomputation for Location Privacy [1]

Ivan Oleynikov[1] Elena Pagnin[2] Andrei Sabelfeld[1]

[1]Chalmers University of Technology
[2]Lund University

May 12, 2022



Proximity testing is at the core of several Location-Based Services (LBS) offered by, e.g., Uber, Facebook, and BlaBlaCar, as it determines closeness to a target. Unfortunately, modern LBS demand not only that clients disclose their locations in plain, but also to trust that the services will not abuse this information. These requirements are unfounded as there are ways to perform proximity testing without revealing one's location.

We propose Polar, a protocol that implements privacy-preserving proximity testing for LBS. The selling features of Polar are actively security (it tolerates misbehaving parties) and extremely good client-side performance. The clients in Polar run a fully fledged MPC protocol to perform the proximity testing functionality. Normally, this would bring huge computation and communication overhead since MPC protocols require a lot of resources for the initial precomputation phase. We overcome this by introducing two servers which aid clients in precomputation, essentially trading some security for big client performance boost. The servers never get to handle client input data since the precomputation doesn't use it. The clients are the only parties working with their data when they run the extremely fast online phase of the MPC protocol.

In this talk we will have a high-level overview of the protocol and see how it's built using the existing MPC protocols, and also discuss the two-server model that the protocol uses.

References

[1] Ivan Oleynikov, Andrei Sabelfeld, and Elena Pagnin. Outsourcing MPC Precomputation for Location Privacy. In *EuroS&P Location Privacy Workshop*, 2022. `https://www.cse.chalmers.se/research/group/security/polar/`.

*{ivanol,andrei}@chalmers.se, elena.pagnin@eit.lth.se