Department of Computer Science, University of Helsinki

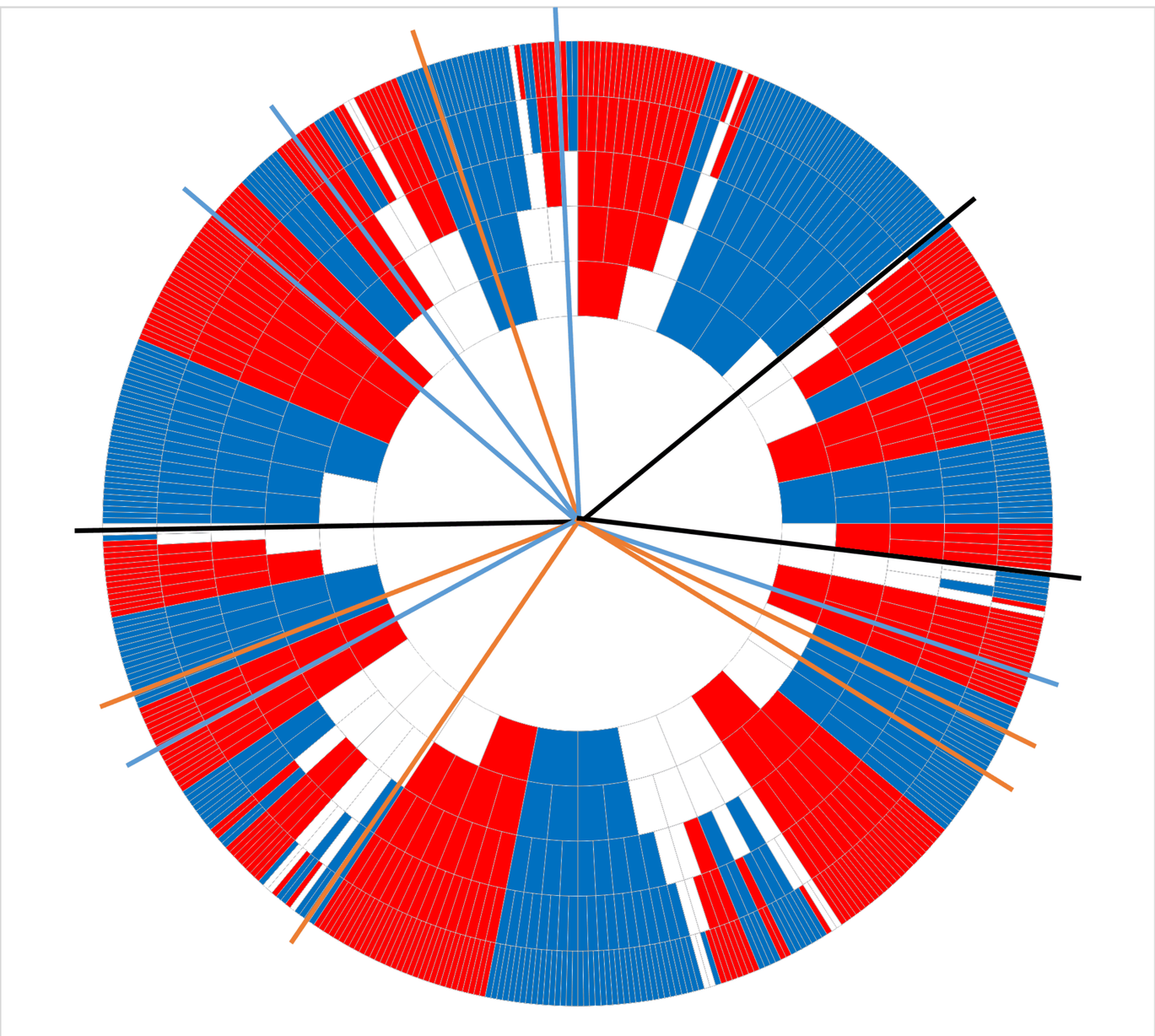
Tommi Meskanen, Jarkko Kuusijärvi, Sara Ramezanian and Valtteri Niemi
(tommi.meskanen@helsinki.fi)

Privacy-friendly Finding of Common Friends in P2P Networking

We studied the problem of two users finding out (how many) common friends they have without revealing all their friends.

Our solution is based on gradually revealing and discarding hash values that do not belong to common friends.

It is faster than earlier solutions for Private Set Intersection but it leaks some information.



Meskanen, Kuusijärvi, Ramezanian, Niemi, "Privacy-friendly Discovery of Common Friends". In 2022 31st Conference of Open Innovations Association (FRUCT), IEEE.

Subroutine for discarding prefixes

(There are 2048 different hash value prefixes of length k bits left.)

Step 1: Initiator chooses 512 of these that are not prefixes of the hash values of their friends and tells Responder to discard all hash values that have these prefixes.

Step 2: Responder chooses another 512 of these that are not prefixes of the hash values of their friends and tells Initiator to discard all hash values starting with these prefixes.

(There are 2048 different hash value prefixes of length k+1 bits left.)

Algorithm for finding common friends

Initiator:=Alice; Responder:=Bob

For k=11 to 30

Run one round of Subroutine for discarding prefixes with length k.

Switch roles of Initiator and Responder.

Alice checks whom of her friends do not have discarded prefixes.

Bob checks whom of his friends do not have discarded prefixes.

This project has received funding from the European Union's Horizon 2020 Research and Innovation Programme under Grant Agreement N° 825585

@heliosEUproject
@HeliosEUProject
social-media@helios-project.eu
helios-social.eu/blog/