An Efficient and Practical Privacy-Preserving Kidney Exchange Problem Protocol

Timm Birka∗, Tobias Kussel, Helen Möllering, Thomas Schneider
Technical University of Darmstadt

33rd Crypto Day, 17 September 2021

Humans are able to live a normal life with at least one functioning kidney [9]. However, when both kidneys of a person are malfunctioning, this person typically requires a donation of a functioning kidney to survive. One option is to find a living person that is willing to donate one of their kidneys. Unfortunately, finding a willing, living donor does not guarantee compatibility with the patient. Hence, the living donor exchange system was introduced in 1991 [6], which allows patients with incompatible living donors, in the following referenced as pairs, to exchange their donors such that ideally each patient can receive a compatible kidney. In our scenario, several pairs exchange their donors in a cyclic fashion, so that each donating pair receives a compatible kidney. These cycles are called exchange cycles [2].

As a first step for finding possible exchange cycles, we have to evaluate the patients and donors medical data to determine compatibility between pairs. This requires the analysis of sensitive medical health data, which makes it crucial that no information are leaked. Afterwards, we have to identify possible exchange cycles. This problem is known as the kidney exchange problem (KEP) [2] and can be described as finding cycles in a directed graph where each vertex represents a pair and a directed edge describes the compatibility between two pairs. There are already approaches for solving the KEP [4, 11], but these fail to address data privacy. Breuer et al. [3] design a privacy-preserving KEP protocol which, however, does not scale well for larger quantities of pairs.

In our work, we design and implement an efficient, privacy-preserving, and robust protocol for solving the KEP in the semi-honest security model. In contrast to Breuer et al. [3], who only include HLA cross matching [7] and ABO compatibility [13], we consider additional medical factors, i.e., HLA match [8], age [12], sex [14], and size of the kidneys [10], which also have a significant impact on the outcome of transplantation. By considering these factors, we increase the chances of a patient not rejecting the new kidney and living a healthy life [1]. Furthermore, to significantly enhance efficiency, we use the secure mixed protocol two-party computation framework ABY [5] in contrast to Breuer et al. [3] who heavily rely on expensive Homomorphic Encryption. In addition, our protocol allows the computation of the compatibility graph independently of the length of the exchange cycles and enables medical experts to modify the algorithmic importance of the different medical factors making our protocol more flexible.

∗Corresponding author: timm.birka@stud.tu-darmstadt.de
References


