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 compatibilitiy [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

[1] Valarie B. Ashby, Alan B. Leichtman, Michael A. Rees, Peter X-K Song, Mathieu Bray, Wen Wang & John D. Kalbfleisch (2017). A Kidney Graft Survival Calculator That Accounts for Mismatches in Age, Sex, HLA, and Body Size. *Clinical Journal of the American Society of Nephrology* 1148–1160. URL `https://doi.org/10.2215/CJN.09330916`.

[2] Péter Biró, Joris van de Klundert, David Manlove, William Pettersson, Tommy Andersson, Lisa Bunapp, Pavel Chromy, Pablo Delgado, Piotr Dworczak, Bernadette Haase, Aline Hemke, Rachel Johnson, Xenia Klimentova, Dirk Kuypers, Alessandro Nanni Costa, Bart Smeulders, Frits Spieksma, María O. Valentín & Ana Viana (2021). Modelling and Optimisation in European Kidney Exchange Programmes. *European Journal of Operational Research* **291**(2), 447–456.

[3] Malte Breuer, Ulrike Meyer, Susanne Wetzel & Anja Mühlfeld (2020). A Privacy-Preserving Protocol for The Kidney Exchange Problem. *WPES* .

[4] Margarida Carvalho, Xenia Klimentova, Kristiaan Glorie, Ana Viana & Miguel Constantino (2020). Robust Models for The Kidney Exchange Problem. *Informs Journal on Computing* URL `https://doi.org/10.1287/ijoc.2020.0986`.

[5] Daniel Demmler, Thomas Schneider & Michael Zohner (2015). ABY - A Framework for Efficient Mixed-Protocol Secure Two-Party Computation. *Network and Distributed System Security Symposium(NDSS)* .

[6] Blake Ellison (2014). A Systematic Review of Kidney Paired Donation: Applying Lessons From Historic and Contemporary Case Studies to Improve The US Model. *Wharton Research Scholars* **107**.

[7] Eurotransplant (2018). Histocompatibility Testing. *Eurotransplant Manual ver. 4.5* URL `https://www.eurotransplant.org/wp-content/uploads/2020/01/H10-Histocompatibility.pdf`.

[8] Bernd Döhler Gerhard Opelz (2012). Association of HLA Mismatch with Death with a Functioning Graft after Kidney Transplantation: A Collaborative Transplant Study Report. *American Journal of Transplantation* .

[9] Hassan N. Ibrahim, Robert Foley, LiPing Tan, Tyson Rogers, Robert F. Bailey, Hongfei Guo, Cynthia R. Gross & Arthur J. Matas (2009). Long-Term Consequences of Kidney Donation. *The New England Journal of Medicine* URL `https://dx.doi.org/10.1056/NEJMoa0804883`.

[10] Amanda J. Miller, Bryce A. Kiberd, Ian P. Alwayn, Ayo Odutayo & Karthik K. Tennankore (2017). Donor-Recipient Weight and Sex Mismatch and The Risk of Graft Loss in Renal Transplantation. *Clinical Journal of the American Society of Nephrology* .

[11] Radu-Stefan Mincu, Péter Biró, Márton Gyetvai, Alexandru Popa & Utkarsh Verma (2020). IP Solutions for International Kidney Exchange Programmes. *Central European Journal of Operations Research* **29**, 403–423. URL https://doi.org/10.1007/s10100-020-00706-5.

[12] Johannes Waiser, Matthias Schreiber, Klemens Budde, Lutz Fritsche, Torsten Böhler, Ingeborg Hauser & Hans-H. Neumayer (2000). Age-matching in Renal Transplantation. *Nephrology Dialysis Transplantation* .

[13] Annelies E. de Weerd & Michiel G.H. Betjes (2018). ABO-Incompatible Kidney Transplant Outcomes: A Meta-Analysis. *Clinical Journal of the American Society of Nephrology* .

[14] Jing-Yi Zhoua, Jun Chenga, Hong-Feng Huanga, Yi Shenb, Yan Jianga & Jiang-Hua Chena (2013). The Effect of Donor-Recipient Sex Mismatch on Short- and Long-term Graft Survival in Kidney Transplantation: A Systematic Review and Meta-Analysis. *Clinical Transplantation* .