SODA
Scalable Oblivious Data Analytics

The practical implications of MPC when Introduced to People

Mads Schaarup Andersen – 12 August 2019

MPC (multi-party computation) is a technology which has applicability to a wide range of problems, and that has a lot of potential uses within the security and privacy domain as it lets participating parties get insights from their own and other parties' data without ever having to share or receive any sensitive data. However, MPC technology has been around for many years without getting used in more than a few, mainly research oriented, projects like Boston Universities gender wage gap study[1] or the Danish beet secret auction system[2]. This begs the question: *"why isn't MPC being wider applied?"*

In an ongoing study looking at the possibilities of creating MPC systems, we are examining this question by exploring how MPC can be explained and how it can be applied in the health domain in the context of the Danish and the UK health systems. The user studies are divided in two parts. The first is about explaining the technology to patients in a health system context, so that they would be able to give an informed consent to their data being used in an MPC system. This is done with early and late stage dementia as well as diabetics and pregnant diabetics. The second part is concerned with explaining and exploring the use of MPC by stakeholders in the health sector. The studies were conducted in Denmark and the UK. As mentioned above, this is an ongoing study, and due to space limitations, we focus on explaining MPC and trust.

One of the main things that has emerged from the user studies is that MPC is very difficult to explain to non-MPC experts. MPC is a complex technology and it is therefore interesting to try to explore to which degree patients and stakeholders need to understand the technology to be able to use it.

From the patients' perspective, the preliminary results indicate that they are not all that interested in understanding the details of the technology. Within the dementia group talking about MPC is made difficult by the fact that they are, to a large degree, non-digital natives. This means that they have a hard time relating to the concept of data, which makes it really hard to give consent to their data being used even without the MPC technology. So, with this group giving consent should probably focus more on understanding what happens in basic data sharing. The work with diabetics indicates that it is more important to know what it means for them in the end. For example, they seemed to care more about knowing whether they are anonymous towards certain parties that understanding the inner workings of the technologies. To a large degree, the patients seemed to have a bigger need to be able to delegate trust to a trusted party such as the EU. One participant even said that if the EU guaranteed that

[1] https://www.bu.edu/macs/2015/04/27/big-news/
[2] https://partisia.com/mpc-goes-live/

it was secure (or anonymous), then he trusted it. Whether EU would be the trusted party for all patients is probably questionable, but all participants indicated that they needed someone to guarantee the properties of the MPC system.

The question of trust is very interesting in an MPC context as the technology is often sold by technologists as *eliminating the need for a trusted 3rd party*. As mentioned above, the patients actually expressed the need of trusting a 3rd party with guaranteeing the security and privacy of the MPC system. The need for some form of trusted 3rd party also emerged during a workshop with stakeholders in the UK health sector – in that case to help make the participating parties agree on what the MPC system should be able to do. This kind of trusted third party was thought up even though the participants had previously been told that the technology eliminated the need for the trusted third party. However, the participants felt that it was unrealistic that the parties would be able to agree on what such a system should be able to do without having some mediating party. This is a very interesting result as it points out how the perspective on trust differs from cryptology experts to others. Where cryptology experts often see trust in the technology and the mathematical proof, non-experts seem to find trust in people and organizations. Overall, it seems that the issue of eliminating the trusted 3rd party does not seem to be an issue in our studies. This might be explained by the fact that there is a large trust in the public health systems in both Denmark and the UK[3]. Participants often questioned why one would not trust the system? This indicates that the need to eliminate the trusted 3rd party might not be relevant in a lot of cases in the health sector in Denmark and the UK. This points towards that the cases in which MPC makes sense really need to be thought through.

We did, however, identify a number of situations where MPC was seen as beneficial. This was for example: getting access to data which was not allowed to be shared for legal reasons (e.g., gaining insights into which patients were less likely to show up for treatment[4]), benchmarking oneself against other diabetics, having to move less data around, etc. Since it does have its merit in the health sector, it is important to explain MPC to the decision makers and technicians in the health sector (and other sectors where MPC might find use). We are therefore currently user testing a video in which we explain MPC which will form the basis of a one-page document which will give decision makers the information they need to make a decision of whether MPC is a technology to consider. As mentioned above, this is ongoing work and apart from the preliminary results discussion here, we are also looking into the main challenges of and solutions to setting up MPC collaborations, what the general challenges are in data sharing, and how and where MPC could practically be applied in the Danish health sector.

[3] This part of the study was conducted before the DeepMind scandal (https://www.independent.co.uk/life-style/gadgets-and-tech/news/google-nhs-health-app-deepmind-artificial-intelligence-ai-privacy-streams-app-a8633316.html)

[4] Whether the suggested use of getting access to otherwise inaccessible data in this way is ethical is another question our of scope of this work.

The project SODA has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 731583.