Secure MPC-Sortition: Consolidating Innovations in Democracy and Cryptography

Research question: How can MPC be used to make the sortition used in deliberative democracy fairer and more private?

Written by:
Wouter Maas w.maas@protonmail.com
Supervised by:
Zekeriya Erkin z.erkin@tudelft.nl

TU Delft Delft University of Technology
Cyber Security Group

1. Citizens' Assemblies

In a citizens' assembly a group of citizens is randomly selected through sortition such that they form an accurate representation of the society they are a part of. This group is then asked to draft recommendations for policy for a certain topic [1].

Especially in the case of deeply controversial topics citizens' assemblies have demonstrated to be an effective tool to resolve divisions in society [1].

Figure 1
The Irish Citizens' Assembly on Abortion

2. Multi-Party Computation

Multi-party computation (MPC) makes it possible to perform calculations on data from multiple sources without revealing it to the other processing parties or data contributors [2].

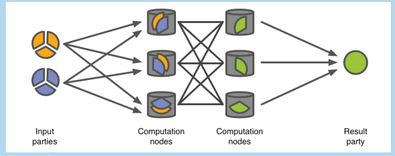

Figure 2
The computational steps in MPC

3. Methodology

The sortition and deliberative democracy community was surveyed to explore current issues in sortition. A literature study was then conducted to explore possible MPC designs which could solve these issues.

Given the fact that private data is necessary to perform sortition, can MPC be used to hide individuals' details whilst also guaranteeing fairer and more accurate sortition results for society as a whole?

4. Discussion

Different stakeholders in the sortition process had different needs. Some citizen assembly organisers questioned the necessity of the improvements, stating current anonymisation methods to be sufficient. Deliberative democracy activist organisations disagreed, stating that improved privacy was more important than being able to gain data insights.
Technical sortition experts (e.g., poling companies) indicated to be very interested in Design 2, seeing the benefit of combining different encrypted databases.

5. Results

See figure 3 and 4.

6. Conclusion

MPC can make sortition more private by encrypting sign-up information through secret shares, it can make it fairer by allowing the selection of a more accurate assembly.
Organisers indicated that current sign-up rates are only 5%, but the effect of privacy on this are yet unknown, future research could focus on the influence of privacy on this statistic. Additionally, future research could explore how MPC can be used for other use cases for polling companies.

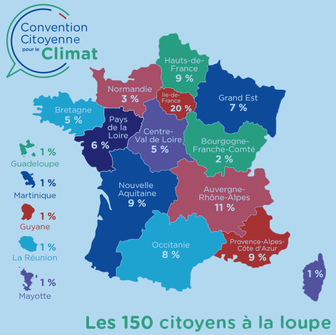

Figure 5
The French Convention on the Climate, an example of an diverse assembly selection, with representatives from the entire country.

8. Sources

Figure 1 https://img.rasset.ie/000db2a6-1600.jpg
Figure 2 https://sunfish-platform-documentation.readthedocs.io/en/latest/_images/smc-computation.png
Figure 5 https://www.resilience.org/stories/2020-01-17/convention-citoyenne-pour-le-climat-what-can-we-learn-from-the-french-citizens-assembly-on-climate-change/
[1] Marcin Gerwin. Citizens' Assemblies – Democracy that works, 2021. URL https:// www.citizensassemblies.org Accessed June 2021.
[2] Yehuda Lindell. Secure Multiparty Computation (MPC). IACR Cryptol. ePrint Arch., 2020:300, 2020.
Icons: https://www.flaticon.com/authors/monkik
[3] Riivo Talviste. Deploying secure multiparty computation for joint data analysis—a case study. Master's thesis, Institute of Computer Science, University of Tartu, 2011.

5. Results: Secure MPC-Sortition Designs

Design 1 uses MPC to encrypts sign-up information at the client side through secret shares [3], guaranteeing that participants' personal data is never decrypted during the sortition, making the process anonymous.

Design 2 uses Design 1, but also combines the participant sign-up sheet information with information available to governments (such as tax data), allowing for the selection of a more accurate depiction of society, making the result fairer.

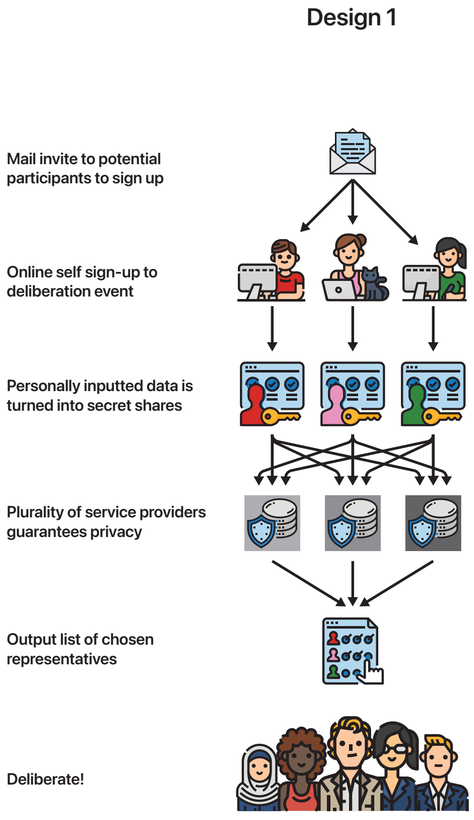

Figure 3

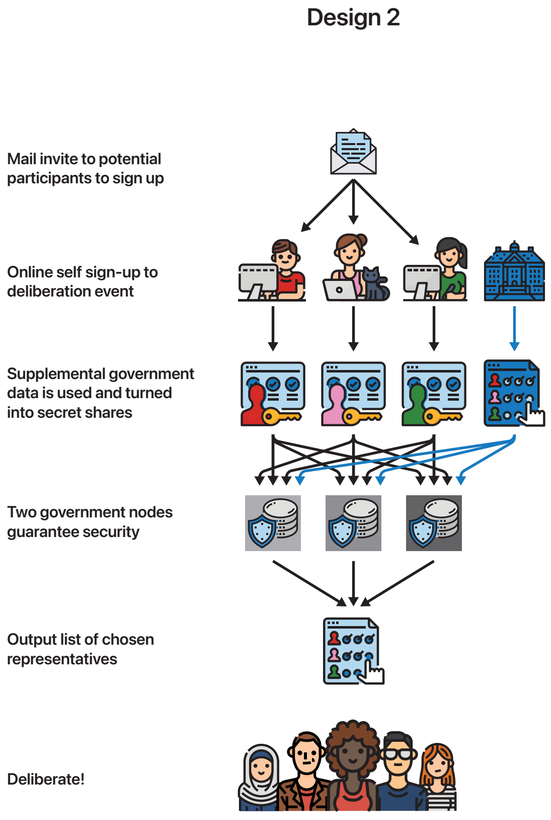

Figure 4