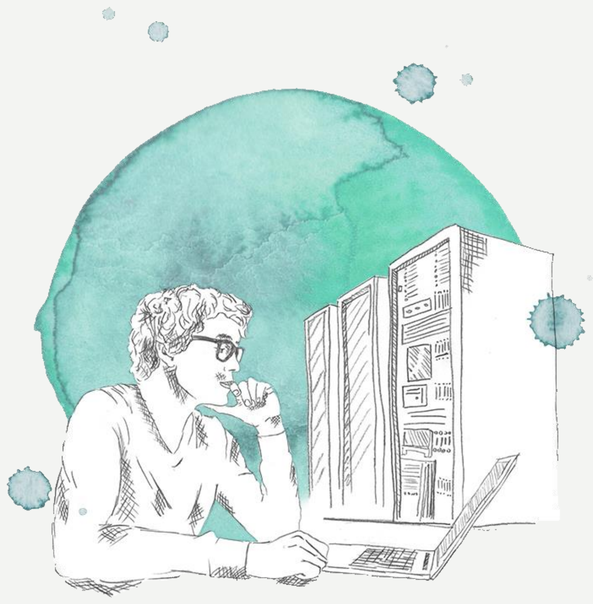
LMU LUDWIG-MAXIMILIANS-UNIVERSITÄT MÜNCHEN

UNIVERSITÄT HEIDELBERG | ZUKUNFT SEIT 1386
E-SCIENCE-TAGE

Secure Multiparty Computation in Clinical Research and Digital Health

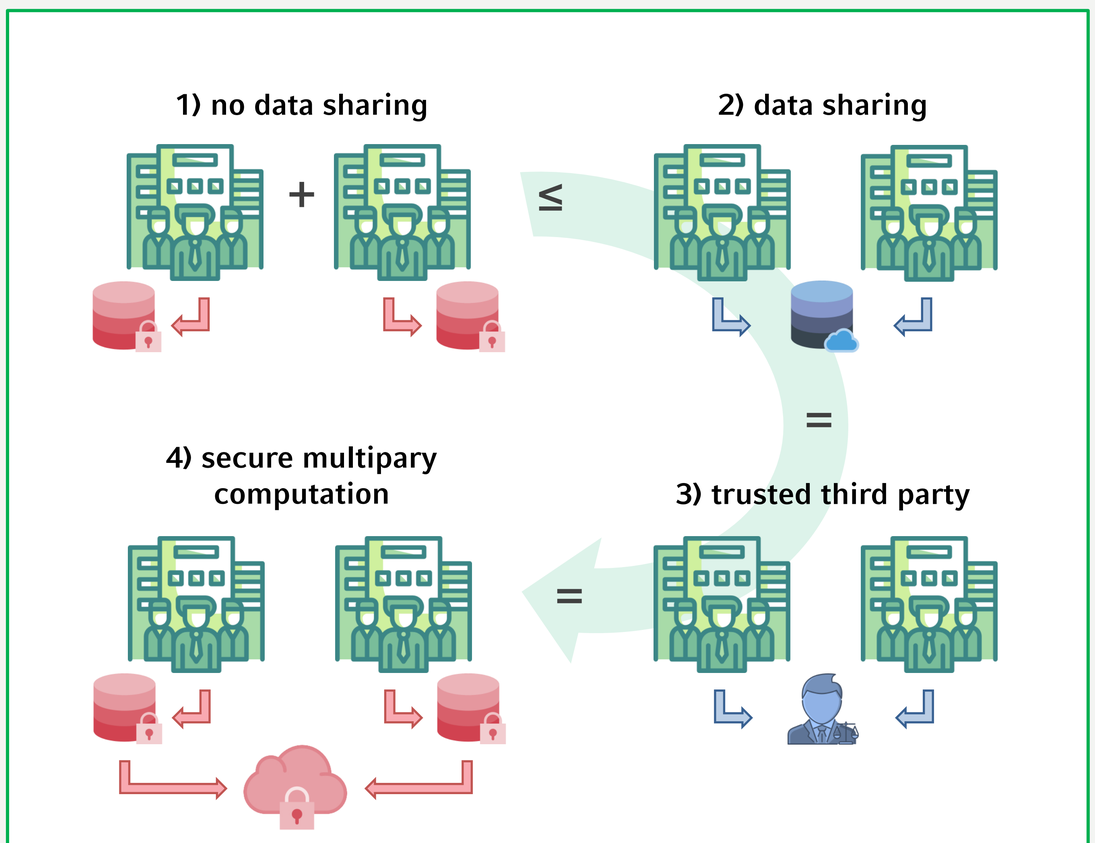
Hendrik Ballhausen*[1,4], Marcel von Maltitz*[2], Maximilian Niyazi[1,4], David Kaul[3,4], Claus Belka[1,4], Georg Carle[2]

[1] Department of Radiooncology, University Hospital, LMU Munich
[2] Chair of Network Architecture and Services, Department of Informatics, TU Munich
[3] Department of Radiation Oncology, Charité – University Medicine, Berlin
[4] DKTK, Deutsches Konsortium für Translationale Krebsforschung, German Cancer Research Center



SECURE MULTIPARTY COMPUTATION

In a perfect word, freely sharing data allows optimal decisions based on the entirety of the available information. Often, a trusted third party can yield the same results, catalyzing the exchange of information even between participants who do not trust each other. Sometimes, even that is not an option, as e.g. legislation rules out data exchange in the first place, most commonly for reasons of privacy or security. The idea is then to simulate the third party by an encrypted protocol which does not rely on sharing actual data in the clear.



In general terms, secure multiparty computation allows a number of parties to jointly compute a function, without revealing their private inputs to each other.

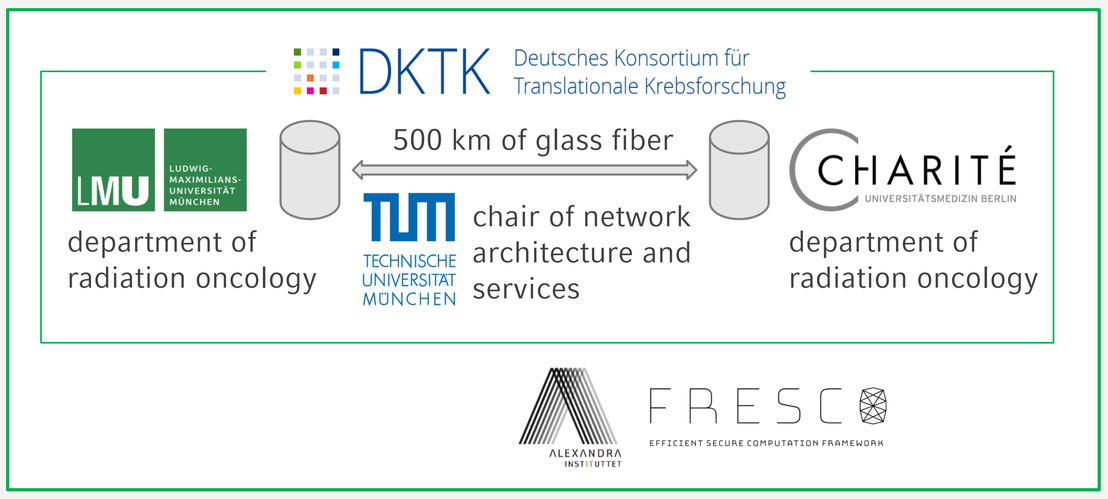
We consider secure multiparty computation for use cases in clinical research and digital health, where privacy concerns are especially demanding.

SUGGESTED READING

Ronald Cramer, Ivan Bjerre Damgård, Jesper Buus Nielsen: “Secure Multiparty Computation and Secret Sharing”, Cambridge University Press, 2015

SURVIVAL OF GLIOBLASTOMA PATIENTS

As a proof of principle, we have implemented a secure multiparty version of the log-rank test and conducted a real-life computation with glioblastoma patient data from the radiation oncology departments of LMU and Charité, both within the data umbrella of the German Cancer Research Center DTKT. We were able to achieve the same level of sensitivity and specificity in the search for confounding factors of survival as we would achive by sharing, i.e. pooling, the data in a central repository.



FUTURE APPLICATIONS IN DIGITAL HEALTH

As health data will increasingly resides on consumers’ mobile devices and as concerns for privacy increase, MPC might help to link distributed health data in a secure, transparent way, including revokable consent.

- consumers retain full ownership (and actual agency) over their data
- data does not leave consumers’ devices
- full transparency on how data is used
- consent can be revoked at any time
- no attack vectors against central databases
- no external attackers can spy on network traffic
- participants do not need to know or trust each other