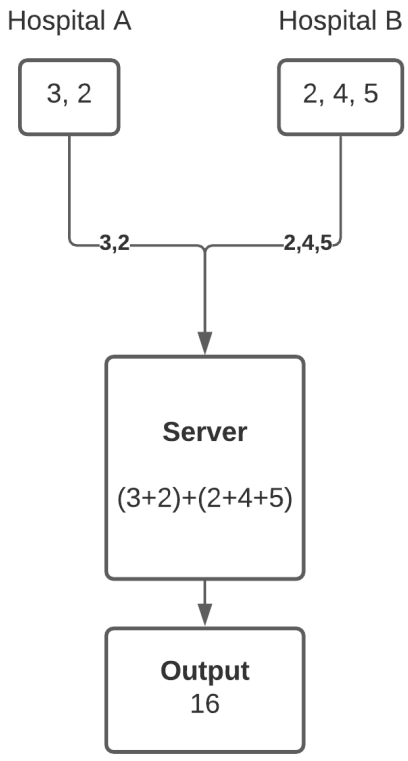
Federation and encryption

Imperial College London

A tale of two hospitals: k-anonymisation



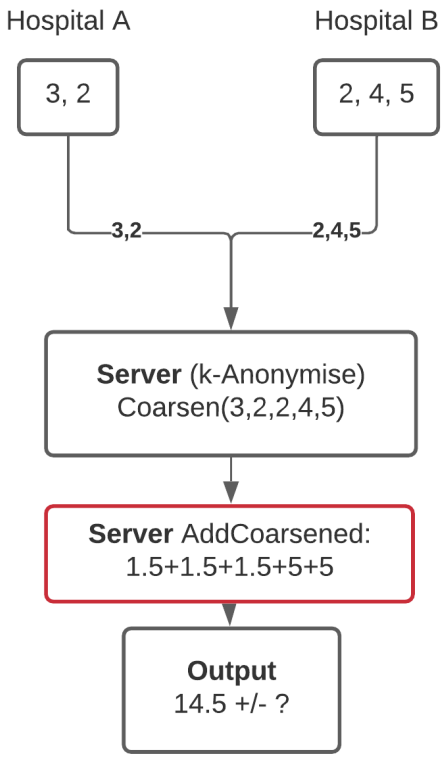


Figure 8: k-anonymisation requires the data to be transferred to a central location, but can then create a privacy-respecting version.

Imperial College London

A tale of two hospitals: randomisation

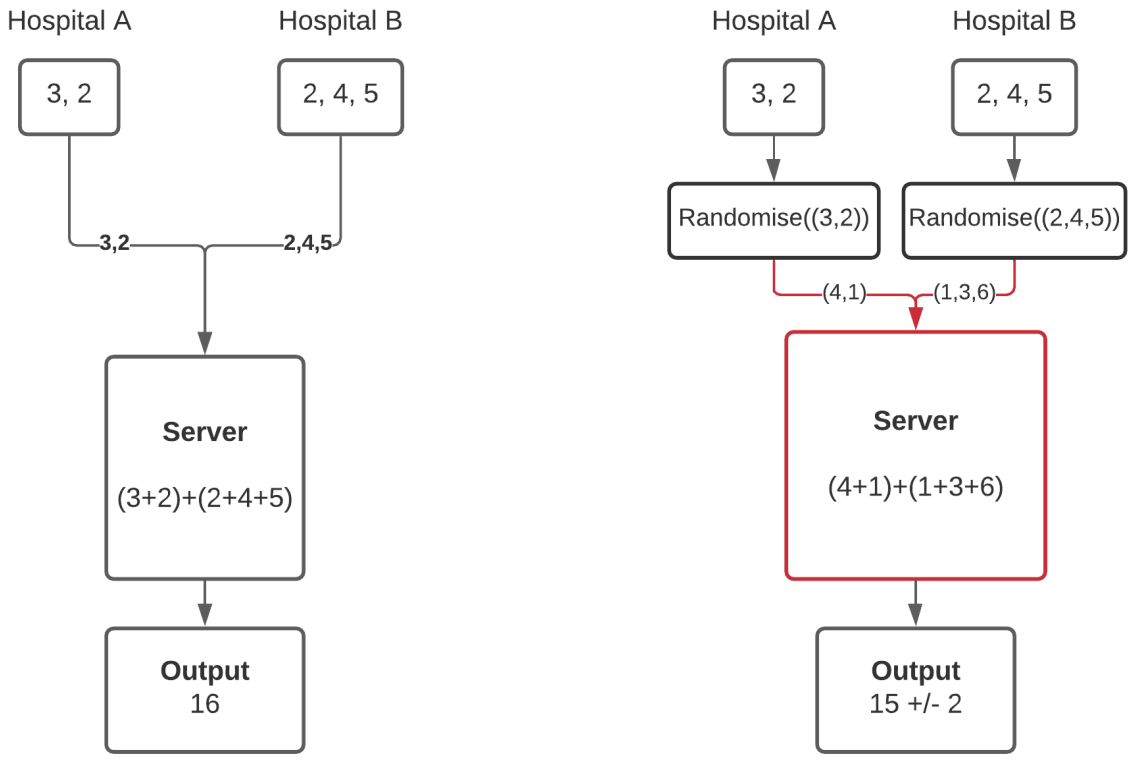


Figure 9: In randomised response, the data is perturbed before it leaves the hospital servers. The cost is additional uncertainty in the output.

Imperial College London

A tale of two hospitals: encryption

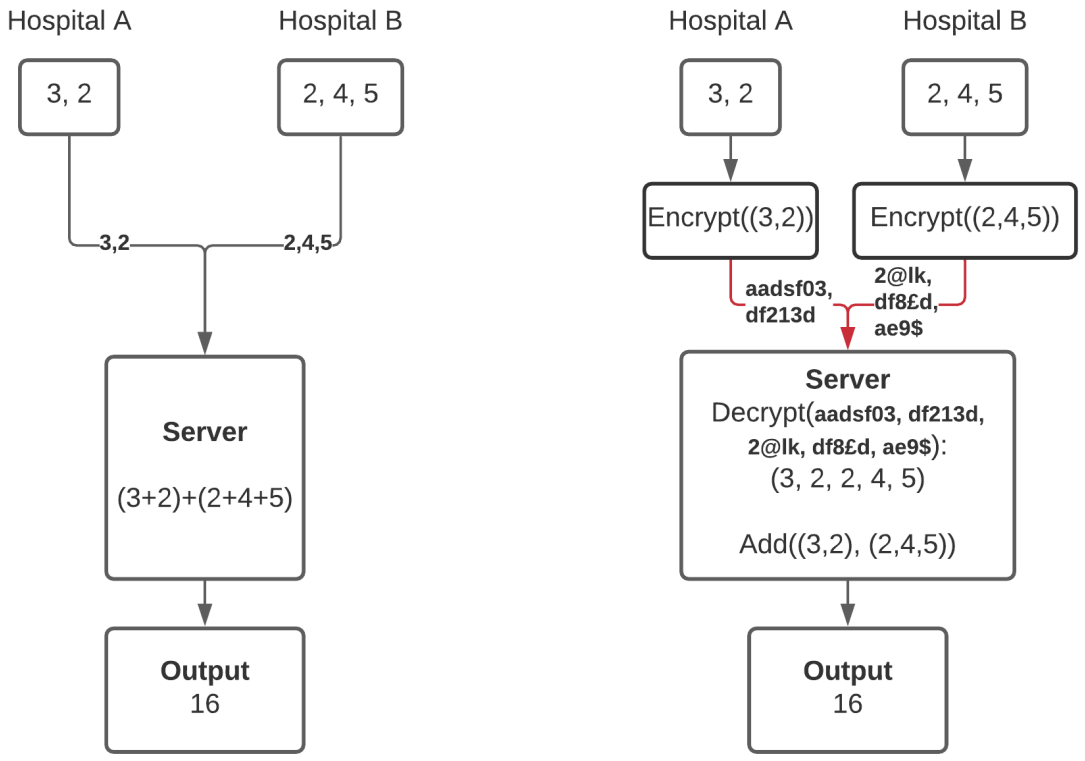


Figure 10: Encryption protects the data in transit, but still exposes it to privacy attacks or leakage while it is at rest.

Imperial College London

A tale of two hospitals: encryption

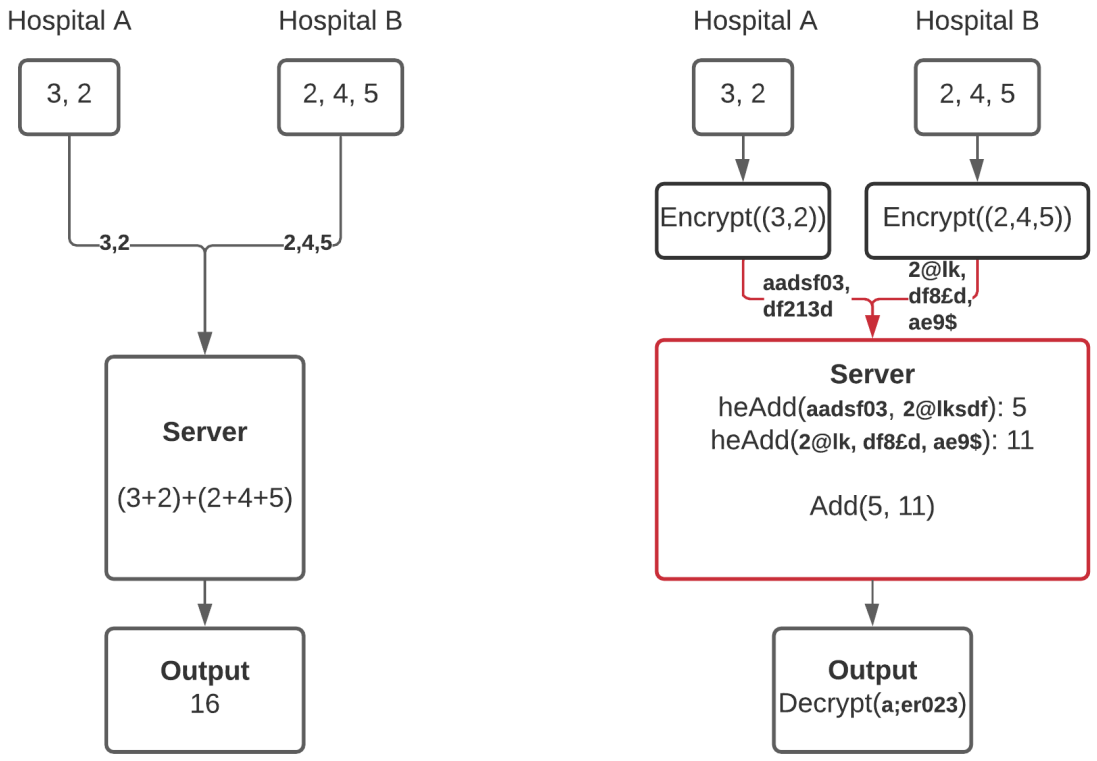


Figure 11: Homomorphic encryption is a state-of-the-art technique that protects the data at all times, but is computationally more expensive.

Imperial College London

A tale of two hospitals: federation

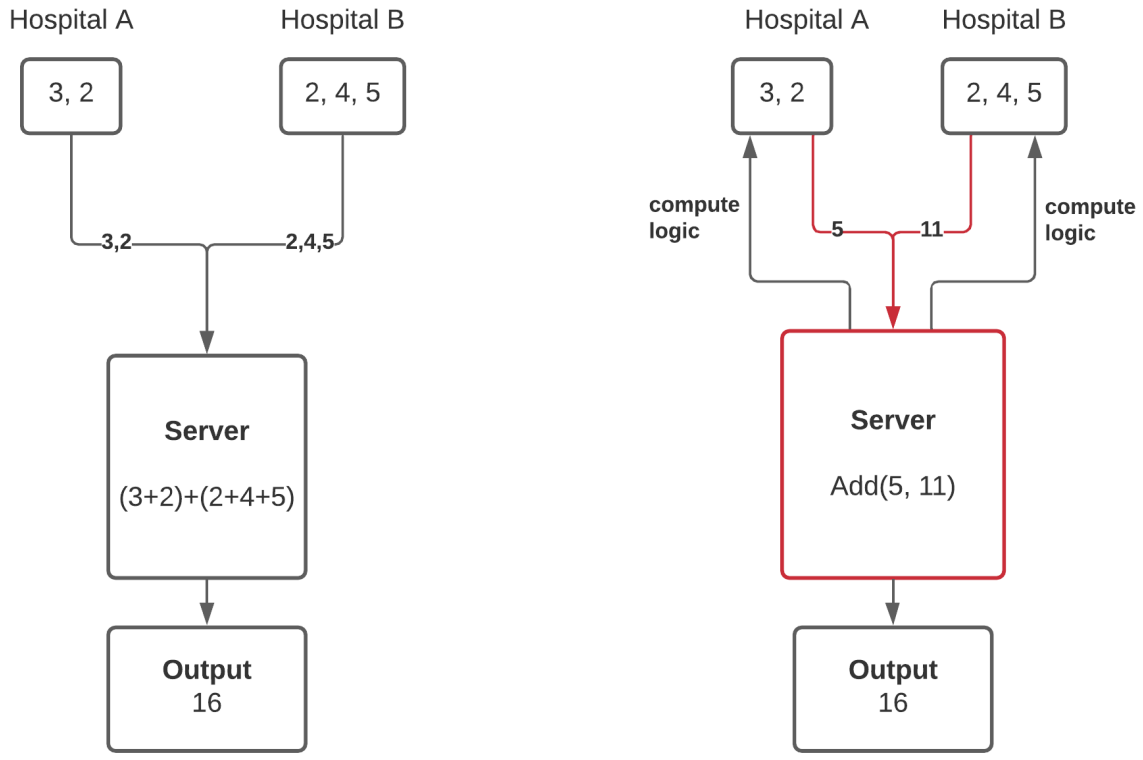


Figure 12: Federation performs partial computations on each hospital, protecting individual patient privacy, and yields accurate results.

Imperial College London

Privacy: summary

From a foundational perspective:

- Privacy is one fundamental right among many
- Informed consent rarely does away with privacy altogether
- Privacy lies at the very core of data ethics and FIPs
- Always assume that leaking private data will be harmful
- Using data and making data public is worth some risk

Privacy: summary

From a technical perspective:

- Anonymisation is hard to achieve and hard to check
- k-Anonymisation is easier on both counts, but imperfect
- Randomisation is an alternative way to protect privacy
- Try to make the tradeoff between privacy and accuracy explicit
- Federated learning and encryption offer alternative ways out

Privacy: summary

Overall:

- Protecting privacy is a cornerstone value in data ethics and regulation (e.g., FIPs, GDPR, HIPAA)
- There are many technical solutions, each with a different cost in terms of accuracy, computational requirements and infrastructure
- At its core, privacy is a contract of trust between the data scientist and the user/patient/consumer/...

Hippocrates might have called it a *sacred* contract of trust.

Imperial College London

Bibliography I

Basu, Subhajit (2012). "Privacy protection: a tale of two cultures". In: *Masaryk University Journal of Law and Technology* 6.1, pp. 1–34.

Bronfenbrenner, Urie (1979). *The ecology of human development: Experiments by nature and design*. Harvard university press.

Council of Europe (1981). *Convention for the protection of individuals with regard to automatic processing of personal data*. Council of Europe.

Crisp, Roger and Trevor J Saunders (1999). "Aristotle: Ethics and politics". In: *Routledge history of philosophy* 2, pp. 109–146.

Erlingsson, Úlfar, Vasyl Pihur, and Aleksandra Korolova (2014). "Rappor: Randomized aggregatable privacy-preserving ordinal response". In: *Proceedings of the 2014 ACM SIGSAC conference on computer and communications security*, pp. 1054–1067.

Etzioni, A. (2007). "Are New Technologies the Enemy of Privacy?" In: DOI: 10.1007/s12130-007-9012-x.

Lensvelt-Mulders, Gerty JLM et al. (2005). "Meta-analysis of randomized response research: Thirty-five years of validation". In: *Sociological Methods & Research* 33.3, pp. 319–348.

Imperial College London

Bibliography II

Narayanan, Arvind and Vitaly Shmatikov (2008). "Robust de-anonymization of large sparse datasets". In: *2008 IEEE Symposium on Security and Privacy (sp 2008)*. IEEE, pp. 111–125.

OECD (1980). *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data - OECD*. URL: http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm (visited on 03/14/2021).

— (2013). *The OECD Privacy Framework*. Tech. rep. URL: https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf.

Ohm, Paul (2009). "Broken promises of privacy: Responding to the surprising failure of anonymization". In: *UCLA l. Rev.* 57, p. 1701.

UN General Assembly (1948). "Universal declaration of human rights". In: *UN General Assembly* 302.2, pp. 14–25.

US Privacy Protection Study Commission (1977). *Personal Privacy in an Information Society: The Report of the Privacy Protection Study Commission*. Vol. 2. US Privacy Protection Study Commission.

Westin, Alan F (1968). "Privacy and freedom". In: *Washington and Lee Law Review* 25.1, p. 166.