Let’s say that I have a private dataset of my employee’s ages. I allow someone to use my private data to perform a computation without releasing the data itself (either encrypting it with the enclave’s public key or using MPC.

The person who uses my (private) data could simply add 1 to every age value, receive the computed result, and then subtract 1, thus resulting in the original dataset.

How are these attacks mitigated? Does anyone know papers/books that explore these types of attacks?