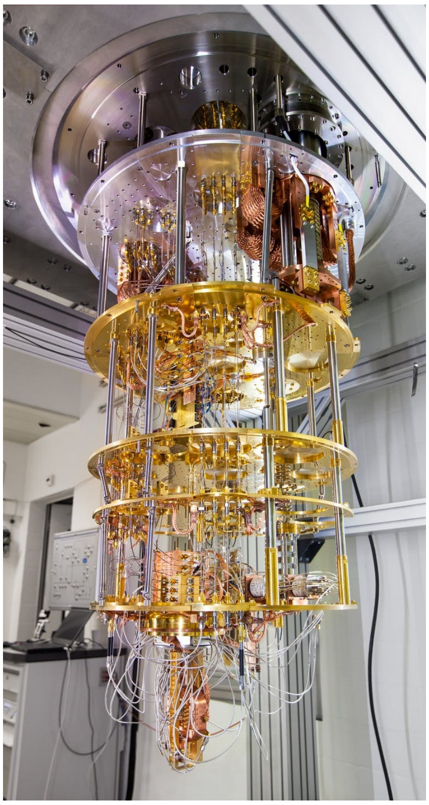
Problem 5. «A promise and money»

A group of young cryptographers are interested in quantum computings and really want to buy a quantum computer. A millionaire gave them a certain amount of money (say, n cryptographers; X_i for each of them, $i = 1, \ldots, n$). He also made them promise that they would not tell anyone, including each other, how much money everyone of them had received.

- Could you help the cryptographers to invent an algorithm how to find out (without breaking the promise) whether the total amount of money they have, $\sum_{i=1}^{n} X_i$, is enough to buy a quantum computer?
- What do you think whether there are such algorithms protecting the secrets of honest participants from dishonest ones?
- What weaknesses does your algorithm have (if someone breaks the promise)? Does it always protect the secret of the honest participants from the dishonest ones?



IBM's 50 qubit quantum computing system