1. **Summary.** The paper presents two important theoretical results for two party protocol in the differential privacy setting. The results show that solving differentially private computation in two party protocol is considerably more harder than in the server-client interaction. In fact in the two party protocol there is the need of a two-sided privacy that induces a greater loss of accuracy. The first result proposed by the authors shows that in any protocol for computing Hamming distance between two $n$-bits vectors that satisfies differential privacy we incur in an additive error of $\tilde{\Omega}(\sqrt{n})$, while in a server-client side scenario the error is only constant. The second result shows that there exists a two-way relationship between differential privacy and communication complexity.

2. **Positive Points.**

   - Although the analysis through the paper has been done considering the Hamming distance as the only computational function in the protocol, the results proposed by authors can be extended to a series of other functions (e.g. inner product of binary vectors).
   - The connection between differential privacy and communication complexity presented in this paper holds in general. This result is very interesting and somehow natural since the information cost measures the amount of information shared between the party and differential privacy tends to limit this information.

3. **Discussion.**

   - The first important thing from this paper is that the two-sided privacy is more harder to guarantee with respect to the server-client setting. This is an aspect that sometime is underestimated, but we can see that from this paper even for basic functions like Hamming distance the difference in the error in these settings are considerable.
• The second import aspect is that the two-way connection between differential privacy and communication complexity allows us to develop strong theoretical results for several function for the former using the results developed in the past years in the latter.