Seminars **Speaker: Salil Vadhan**

Robust Traceability from Trace Amounts

Institute of Statistical Science, Academia Sinica **Scribe: Chi-Ning Chou**

1 Overview and Model

This talk [DSS+15] is about the recent improvement of DP's (Differential Privacy) negative result. So far, all the lower bound result in DP is under worst-case setting. Namely, people constructed a bad instance so that a good DP mechanism will turn out to be a powerful pirate in the traitor-tracing framework. [BUV14, SU14]

Different from previous worst-case study, they started from defining a "well-separated" prior distribution on the parameter. For example, a d dimensional Bernoulli distribution. Then using this parameter we can have our **population data** while in the meantime we can only have access to the **case data**. The goal of the DP is to prevent individual privacy and here we consider a target y, which might be either drawn from the population or the case data.

After querying the case data m times in the DP mechanism, we put the output and target y into a tracing algorithm. Here, tracing algorithm is like a malicious data analyst who wants to use the query to reveal the personal information about y. As a result, our goal would be making the tracer get not additional information. Since here we want to derive a lower bound for the number of queries of DP mechanism, we would like to see how many number of queries will end up with a success tracing algorithm.

The central idea of their tracing algorithm utilize the so called *correlation attack*. They observed that when given a genomic data y which might be inside/outside the group $(x_1, \ldots, x_n)$. If $y \in (x_1, \ldots, x_n)$, then the correlation between y and the accurate summary statistics of $(x_1, \ldots, x_n)$ will be significantly larger than the correlation of y and the reference data z. On the other hand, if y is a fresh data that is independent to $(x_1, \ldots, x_n)$, then the correlation of y and the accurate summary statistics will be roughly the same as the correlation between y and z.

Here, let's formally define the model used in [DSS+15]. See Figure 1 for an overview.

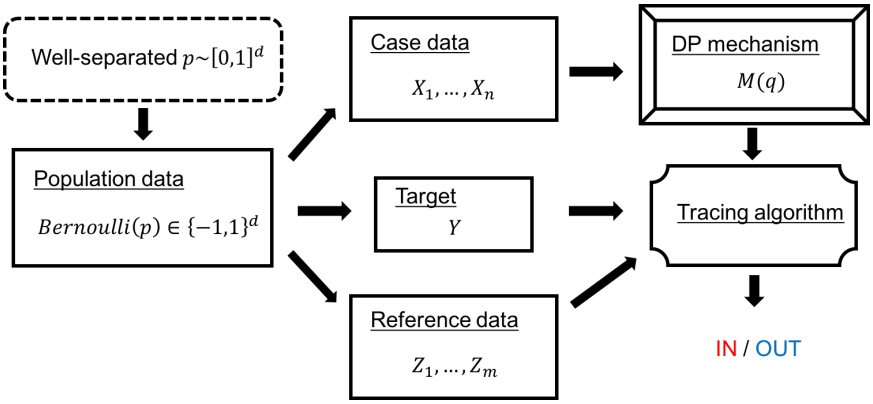

Figure 1: Framework of [DSS+15].

The data in our framework are drawn from the domain $\{-1,+1\}^d$ with population distribution $\mathcal{P}_p$, where $p \in [-1,1]^d$ specifies the mean of each column. Namely, for the j-th column, the probability of +1 is $(1+p_j)/2$ and the probability of -1 is $(1-p_j)/2$.

In this paper, the true p is unknown to the adversary. What we know is that p follows a *smooth and spread-out*[1] distribution $\rho : [-1,1] \to \mathbb{R}$.

2 Some thoughts

For me, there are several ideas in the talk that caught my eyes.

- Model the underlying distribution with a hidden parameter following certain well-separated conditions. Moreover, using reference data to quantify the amount of knowledge for analyst toward the population. I think this is the most difficult part of the average-case analysis in DP setting and this kind of data analysis framework. Since the database is given and people might have lots of prior knowledge/side information to it, it's impractical to assume the database is totally random/unknown. In this talk, they somehow used the concept of reference data to describe the prior knowledge. In some sense it is acceptable and have room for analysis.
- I haven't read through the details about well-separated prior distribution. But after a discussion with Wei-Kai, we thought that the goal of well-separated condition is to guarantee the amount of useful information in the database. Thus, we are thinking wether the condition can be modified into a information-theoretic setting such that maybe it will be more suitable for real-life application.

How to quantify prior knowledge/computational knowledge is still a quite open problem in TCS. This work showed us a simple way to do so. I will read the paper in the near future and write some of my feedback later.

References

[BUV14] Mark Bun, Jonathan Ullman, and Salil Vadhan. Fingerprinting codes and the price of approximate differential privacy. In *Proceedings of the 46th Annual ACM Symposium on Theory of Computing*, pages 1–10. ACM, 2014.

[DSS+15] Cynthia Dwork, Adam Smith, Thomas Steinke, Jonathan Ullman, and Salil Vadhan. Robust traceability from trace amounts. In *Foundations of Computer Science (FOCS), 2015 IEEE 56th Annual Symposium on*, pages 650–669. IEEE, 2015.

[SU14] Thomas Steinke and Jonathan Ullman. Interactive fingerprinting codes and the hardness of preventing false discovery. *arXiv preprint arXiv:1410.1228*, 2014.

[1] These two properties turn out to be the most important concept in this work, we will discuss them later.