Information-theoretic metrics for Local Differential Privacy protocols

Milan Lopuhaä-Zwakenberg  
Dept. of Mathematics and Computer Science  
Eindhoven University of Technology  
Eindhoven, the Netherlands  
m.a.lopuhaa@tue.nl

Boris Škorić  
Dept. of Mathematics and Computer Science  
Eindhoven University of Technology  
Eindhoven, the Netherlands  
b.skoric@tue.nl

Ninghui Li  
Dept. of Computer Sciences  
Purdue University  
West Lafayette, United States  
ninghui@purdue.edu

I. INTRODUCTION

The aim of our research is to use information theory to study local privacy protocols, i.e. a setting where users do not trust the data aggregator with their private data, and they obfuscate their private data by applying a privacy protocol $Q$. The de facto metric for the privacy of $Q$ in this setting is local differential privacy (LDP) [1], which has several drawbacks: it is too strict for many applications, it can only be applied to probabilistic $Q$, and it does not give a clear answer as to what extent private data is vulnerable to the aggregator. Current utility metrics are focused on the accuracy of frequency estimations of the state of the art metrics addressed in the introduction. On the side of privacy, $\text{Priv}_Q$ is less strict than LDP since it measures ‘average’ rather than ‘worst case’ privacy. Furthermore, it can also be applied in a more general setting than LDP. Finally, $\text{Priv}_Q$ can be viewed as the part of $i$’s private data that is hidden from the aggregator, which gives the metric a clear meaning. Regarding utility, the metric $\text{Uti}_{i_1,\Delta}$ does not depend on estimators, and as such does not have to deal with negative frequency estimations. Instead, this metric is closely related to $P$’s posterior distribution that can be computed by the aggregator.

II. DEFINITION OF NEW METRICS

We introduce the following information-theoretic metrics for utility and privacy of $Q$: Let $X_1, \ldots, X_n$ be the users’ private data, each drawn independently from an unknown probability distribution $P$ on a finite set $\mathcal{A}$. We regard $P$ as a continuous random variable on the simplex $\mathcal{P}_\mathcal{A}$ of probability distributions on $\mathcal{A}$. Its distribution $\Delta$ reflects the aggregator’s prior knowledge. Its value is unknown to the aggregator, and the aggregator’s goal is to learn $P$. Let $Y_i = Q(X_i)$ be $i$’s output; this is sent to the aggregator. This setup is illustrated in Fig. 1.

![Probabilistic model of a local privacy protocol](image)

**Definition.** Let $i \in \{1, \ldots, n\}$ (the choice does not matter). Then we define

\[
\text{Uti}_{i,\Delta}(Q) = \frac{I(Y_1, \ldots, Y_n; P)}{I(X_1, \ldots, X_n; P)},
\]

\[
\text{Priv}_\Delta(Q) = \frac{H(X_i|Y_i, P)}{H(X_i|P)}.
\]

III. NEW METRICS ADDRESS CURRENT METRICS’ SHORTCOMINGS

These information-theoretic metrics address the shortcomings of the state of the art metrics addressed in the introduction. On the side of privacy, $\text{Priv}_\Delta$ is less strict than LDP since it measures ‘average’ rather than ‘worst case’ privacy. Furthermore, it can also be applied in a more general setting than LDP. Finally, $\text{Priv}_\Delta(Q)$ can be viewed as the part of $i$’s private data that is hidden from the aggregator, which gives the metric a clear meaning. Regarding utility, the metric $\text{Uti}_{i_1,\Delta}$ does not depend on estimators, and as such does not have to deal with negative frequency estimations. Instead, this metric is closely related to $P$’s posterior distribution that can be computed by the aggregator.

IV. LEARNING $P$

We can quantify the aggregator’s knowledge about $P$ when the number of users is large:

**Theorem.** There exists an explicitly computable constant $c(Q)$ such that, as $n \to \infty$,

\[
I(Y_1, \ldots, Y_n; P) \approx H(P_{\frac{1}{2}\log n + c(Q)}),
\]

where $P_{d}$ is the $d$-digit discretisation of $P$.

This theorem shows that the aggregator can learn $P$ up to approximately $\frac{1}{2}\log n + c(Q)$ digits; hence the constant $c(Q)$ is an important characteristic of $Q$’s asymptotic utility.

REFERENCES
