Author/s:
Farokhi, F

Title:
Development and Analysis of Deterministic Privacy-Preserving Policies Using Non-Stochastic Information Theory

Date:
2019-10

Citation:
Farokhi, F. (2019). Development and Analysis of Deterministic Privacy-Preserving Policies Using Non- Stochastic Information Theory. IEEE Transactions on Information Forensics and Security, 14 (10), pp.2567-2576. https://doi.org/10.1109/TIFS.2019.2903660.

Persistent Link:
https://hdl.handle.net/11343/285056

Development and Analysis of Deterministic Privacy-Preserving Policies Using Non-Stochastic Information Theory

Farhad Farokhi

***Abstract*—A deterministic privacy metric using non-stochastic information theory is developed. Particularly, maximin information is used to construct a measure of information leakage, which is inversely proportional to the measure of privacy. Anyone can submit a query to a trusted agent with access to a non-stochastic uncertain private dataset. Optimal deterministic privacy-preserving policies for responding to the submitted query are computed by maximizing the measure of privacy subject to a constraint on the worst-case quality of the response (i.e., the worst-case difference between the response by the agent and the output of the query computed on the private dataset). The optimal privacy-preserving policy is proved to be a piecewise constant function in the form of a quantization operator applied on the output of the submitted query. The measure of privacy is also used to analyze k-anonymity (a popular deterministic mechanism for privacy-preserving release of datasets using suppression and generalization techniques), proving that it is in fact not privacy-preserving.**

***Index Terms*—Non-stochastic Information Theory, Maximin Information, Privacy, Piecewise Constant Function, Quantization.**

I. Introduction

Advances in communication and computation engineering have enabled the use of big data analysis for answering societal challenges. These advances have motivated incorporation of new tools for collection and analysis of datasets, and reporting data-driven insights. The erosion of privacy caused by the adoption of such tools has resulted in adoption of new rules by governments, such as the General Data Protection Regulation (GDPR) in the European Union, for protecting citizens, customers, and their data.

Anonymization is most often used as a method of choice by governments or companies alike for releasing private datasets[1] to the broader public for analysis. Although popularly adopted, anonymization has been proved to be insufficient for privacy preservation [1]–[3]. Therefore, systematic methods for privacy preservation in a provable manner should be developed.

Differential privacy and its variants, such as local differential privacy and probabilistic differential privacy, form a category of methodologies with provable privacy guarantees [4]–[10]. These methods, in summary, rely on the use of randomized policies, such as additive noise, to ensure that the statistics of the reported outputs do not change noticeably by variations in an individual entry of the dataset. This property ensures that an adversary cannot reverse-engineer differentially-private outputs to accurately estimate an individual private entry of the dataset, even in the presense of side information. Various studies have been devoted to finding "optimal" noise distribution in differential privacy [11]–[13]; however, off-the-shelf mechanisms, such as the additive Laplace and Gaussian noise with scales proportional to the sensitivity of the submitted query with respect to the individual entries of the dataset, are often used to ensure differential privacy [5]. Note that the use of randomized policies for privacy protection in itself is not particularly new [14] but, prior to differential privacy, provable guarantees were often missing.

Another methodology for privacy protection is the use of information theoretic metrics dating back to the pioneering work on secrecy in [15]. In the secrecy problem, a sender wishes to devise an encoding scheme to create a secure channel for communicating with a receiver while hiding her data from an eavesdropper (similar to the setup of encryption). The privacy problem with the emphasis on masking or equivocating of information from the intended primary receiver (rather than an eavesdropper) or a secondary receiver with as much information as the primary receiver have been studied in [16]–[19]. Information-theoretic guarantees have been also provided on the amount of leaked private information when utilizing differential privacy [20], [21]. Furthermore, entropy, mutual information, Kulback-Leiber divergence, and Fisher information have been repeatedly used as measure of privacy in [22]–[29].

A common thread or assumption among all these methodologies is that they utilize randomization for safeguarding privacy. In fact, the definition of differential privacy assumes the use of randomized functions and information theoretic tools used so far have been based on randomized random variables. However, many popular[2] heuristic-based privacy-preserving methods, such as k-anonymity [30], [31] and ℓ-diversity [32], are deterministic (i.e., deterministic mappings, such as suppression and generalization, applied to non-stochastic datasets).

Randomized, or stochastic, privacy-preserving policies have been shown to cause problems, such as un-truthfulness [33], which can be undesirable in practice [34]. This is perhaps one of the reasons behind low popularity of randomized privacy-

The work of F. Farokhi was partially supported by the McKenzie Fellowship at the University of Melbourne and the VESKI Victoria Fellowship by the Victorian State Government. He also would like to thank the office of the Deputy Vice-Chancellor (Research) at the University of Melbourne for funding his current fellowship position at the university.

F. Farokhi is with the CSIRO's Data61 and Department of Electrical and Electronic Engineering at the University of Melbourne. e-mail: farhad.farokhi@{unimelb.edu.au,data61.csiro.au}

[1]See https://data.gov.au for an example of government initiave. Many other examples can be found in https://www.kaggle.com.

[2]Popularity of these methods is somehwat evident from the sheer number of available toolboxes for implementation https://arx.deidentifier.org/overview/related-software/

preserving policies, such as differential privacy, within the financial or health sectors [33]. For instance, randomized privacy-preserving policies in financial auditing have been criticized for complicating fraud detection [35], [36]. Also, generation of unreasonable and unrealistic outputs by randomness can cause undesirable financial outcomes (e.g., misleading investors or market operators by reporting noisy outputs that point to lack of liquidity in a bank). Randomized privacy-preserving policies, in general, have also encountered difficulties in medical, health, or social sciences [37], [38]. Finally, undesirable properties of differentially-private additive noise, especially the Laplace noise, might make it less appealing. For instace, optimal variable estimation in the presence of privacy-preserving Laplace noise is computationally expensive [39] and probability of returning impossible reports (e.g., negative median income) could be relatively high due to slow-decaying nature of Laplace noise [40].

In addition to the aforementioned difficulties or negative consequences associated with randomized policies, the popularity of non-stochastic methods might also be caused by the simplicity of implementing deterministic policies, in the sense of not requiring a working knowledge of random variables and their generation by laymen. Deterministic privacy-preserving policies and non-stochastic measures of information leakage, if designed correctly, can also provide concrete guarantees regarding the amount of the information that can be inferred about each instance of the private dataset, rather than stochastic measures of privacy that only provide guarantees in average (i.e., in a statistical sense).

So far, deterministic privacy-preserving policies are generated in an *ad hoc* manner and are often vulnerable to attacks (e.g., k-anonimity has been proved to be vulnerable to attacks, such as homogeneity attack [32]). This is because there is no good measure of privacy that works for deterministic policies on deterministic datasets. Therefore, one cannot prove (in some sense) privacy guarantees of the methods (even if weak or limited in scope or practice). The popularity of non-stochastic privacy-preserving policies justifies requiring a metric for their analysis and comparison (irrespective of their inherent philosophical weaknesses in comparison to stochastic policies).

Motivated by this observation, in this paper, a deterministic privacy metric based on non-stochastic information theory is developed. Traditional information theory, starting with Shannon's seminal work in [41], usually assumes that data (source) and communication channels are stochastic in nature. This has been proved to be extremely powerful in modelling and analysing communication systems; see, e.g., [42] and references therein. However, the notion of information within the traditional information theory literature, such as mutual information, is not useful for analysing non-stochastic uncertain variables (an analogue of random variables but without a probability measure) and deterministic privacy-preserving policies. This is because such definitions require a probability density function to exist for variables, which is not the case in the absence of additive privacy-preserving noise (with a known probability density function) or stochasticity assumptions on the private dataset.

There is a parallel less-studied (within tertiary colleges) theory of non-stochastic information theory [43]–[47], which has been recently used within engineering [48]–[50]. Non-stochastic information theory relies on uncertain variables and extension of analogues of probabilistic ideas, such as independence. Non-stochastic information theory is not equivalent to treating input variables with known, bounded ranges as uniformly distributed random variables because such an approach is still probabilistic, and the output random variables may exhibit non-uniform distributions despite the uniform inputs. In contrast, in the uncertain variable model, only the support sets are considered, and no distributions are derived at any stage. Measures of information in non-stochastic information theory deal with counting/measuring the worst-case size of uncertainty sets with favourable fundamental properties, such as post-processing inequality.

In this paper, non-stochastic measures of information, such as maximin information, from the non-stochastic information theory literature are used to develop a measure of privacy. Anyone can submit a query to a trusted agent with access to a non-stochastic uncertain private dataset. An optimization problem is posed to maximize the measure of privacy subject to a constraint on the worst-case quality of the response (i.e., the worst-case difference between the response by the agent and the output of the query computed on the private dataset). The solution to the optimization problem captures the optimal deterministic privacy-preserving policies for responding to submitted queries. The optimal privacy-preserving policy is in fact proved to be a quantization operator applied on the output of the submitted query computed based on the private dataset. The developed measure of privacy is utilized to analyze the privacy credentials of k-anonymity, proving that it is not privacy-preserving, which was previously observed using adversarial attacks in [32].

The rest of the paper is organized as follows. Section II provides a summary of non-stochastic information theory. The problem formulation is presented in Section III. In Section IV, a piecewise constant function, in the form of a quantization operator, is proved to be an optimal privacy-preserving policy. The privacy of k-anonymity is analyzed using the proposed non-stochastic privacy metrics in Section V. Finally, Section VI concludes the paper and presents future directions for work.

II. Non-stochastic Information Theory

In this section, an overview of non-stochastic information theory is presented. First, uncertain variables, which are analogues of random variables but without a probability measure, are introduced. Then, various measures of information, i.e., non-stochastic information based on Rényi differential 0-entropy, non-stochastic information leakage, and maximin information are presented.

A. Uncertain Variables

Consider sample space Ω. Each element $\omega \in \Omega$ is referred to as a sample. The sample space is the source of uncertainty. Any mapping $X : \Omega \to \mathbb{X}$ defines an uncertain variable. A

realization of such a variable is $X(\omega)$. However, for the ease of presentation, $X(\omega)$ is replaced by X when the dependence of the uncertain variable to the sample is evident from the context. Up to this point, the difference between uncertain variables and random variables is the absence of a measure on the space Ω. Throughout this paper, it is assumed that all uncertain variables are real-valued, i.e., $\mathbb{X} \subseteq \mathbb{R}^{n_x}$ for some $n_x \in \mathbb{N}$. Marginal range of X is defined as

$$[\![X]\!] := \{X(\omega) : \omega \in \Omega\} \subseteq \mathbb{X}.$$

Joint range of two uncertain variables $X : \Omega \to \mathbb{X}$ and $Y : \Omega \to \mathbb{Y}$ is

$$[\![X, Y]\!] := \{(X(\omega), Y(\omega)) : \omega \in \Omega\} \subseteq \mathbb{X} \times \mathbb{Y}.$$

Finally, conditional range of X (conditioned on the observation of another uncertain variable $Y(\omega) = y$) is given by

$$[\![X|y]\!] := \{X(\omega) : \exists \omega \in \Omega \text{ such that } Y(\omega) = y\} \subseteq [\![X]\!].$$

The family of all conditional ranges is denoted by

$$[\![X|Y]\!] := \{[\![X|y]\!] : y \in [\![Y]\!]\} \subseteq 2^{[\![X]\!]}.$$

This should not be mistaken with the union of all such conditional ranges given by $\bigcup_{y\in[\![Y]\!]}[\![X|y]\!] = [\![X]\!]$. In fact, regarding the union, it can be proved that $\bigcup_{y\in[\![Y]\!]}[\![X|y]\!]\times\{y\} = [\![X, Y]\!]$.

Definition II.1 (Unrelatedness)**.** *Uncertain variables X_i, $i = 1, \dots, n$, are unrelated if $[\![X_1, \dots, X_n]\!] = [\![X_1]\!] \times \cdots \times [\![X_n]\!]$. Further, they are conditionally unrelated (conditional on Y) if $[\![X_1, \dots, X_n|y]\!] = [\![X_1|y]\!] \times \cdots \times [\![X_n|y]\!]$ for all $y \in [\![Y]\!]$.*

For two uncertain variables, this definition is equivalent to stating that X_1 and X_2 are unrelated if $[\![X_1|x_2]\!] = [\![X_1]\!], \forall x_2 \in [\![X_2]\!]$, and *vice versa*. Again, for two uncertain variables, this definition is equivalent as saying that X_1 and X_2 are conditionally unrelated (conditional on Y) if $[\![X_1|x_2, y]\!] = [\![X_1|y]\!]$, $\forall (x_2, y) \in [\![X_2, Y]\!]$, Finally, for uncertain variables X and Y_i, $i = 1, \dots, n$, it can be seen that $[\![X|y_1, \dots, y_n]\!] \subseteq \bigcap_{i=1}^{n}[\![X|y_i]\!]$, where the equality is achieved, i.e., $[\![X|y_1, \dots, y_n]\!] = \bigcap_{i=1}^{n}[\![X|y_i]\!]$, if Y_i, $i = 1, \dots, n$, are unrelated conditional on X.

B. Non-stochastic Entropy and Information

The non-stochastic entropy of uncertain variable X can be defined as

$$h_0(X) := \log(\mu([\![X]\!])) \in \overline{\mathbb{R}}, \tag{1}$$

where μ is the Lebesgue measure, $\overline{\mathbb{R}}$ is the extended real line $\mathbb{R} \cup \{\pm\infty\}$, and the logarithm can be taken in any basis. In line with the differential entropy for random variables, the logarithm is in the natural basis throughout the rest of the paper. The non-stochastic entropy in (1) is sometimes referred to as Rényi differential 0-entropy [46].

Remark II.1 (ε-entropy)**.** *This notion of Rényi differential 0-entropy is intimately related to the ε-entropy [44] defined as $h_\epsilon(X) := \log(N_\varepsilon([\![X]\!]))$, where $N_\epsilon(\cdot)$ is the smallest number of sets of diameter 2ε such that their union covers $[\![X]\!]$, referred to as the minimal ε-covering. The inequality $\varepsilon^{n_x} N_\varepsilon([\![X]\!]) \leq \mu([\![X]\!]) \leq (2\varepsilon)^{n_x} N_\varepsilon([\![X]\!])$ implies that $0 \leq h(X) - [h_\varepsilon(X) + n_x \log(\varepsilon)] \leq n_x \log(2)$. These two notions of entropy are similar.*

Similarly, the non-stochastic relative (or conditional) entropy of uncertain variable X conditioned on uncertain variable Y can be defined as

$$h_0(X|Y) := \operatorname*{ess\,sup}_{y\in[\![Y]\!]} \log(\mu([\![X|y]\!])), \tag{2}$$

where, for any real-valued function $f : \mathcal{X} \to \mathbb{R}$ for some $\mathcal{X} \subseteq \mathbb{R}^m$, the essential supremum is defined as

$$\operatorname*{ess\,sup}_{x\in\mathcal{X}} f(x) := \inf\{b \in \mathbb{R} : \mu(\{x \in \mathcal{X} : f(x) > b\}) = 0\}.$$

Based on the definition of entropy, the non-stochastic information between two uncertain variables X and Y can also be defined as

$$\begin{aligned} I_0(X;Y) :=& h_0(X) - h_0(X|Y) \\ =& \operatorname*{ess\,inf}_{y\in[\![Y]\!]} \log\left(\frac{\mu([\![X]\!])}{\mu([\![X|y]\!])}\right). \end{aligned} \tag{3}$$

Note that Kolmogorov had defined 'combinatorial' conditional entropy using $\log(\mu([\![X|y]\!]))$ and the measure of information gain was defined as $\mu([\![X]\!])/\mu([\![X|y]\!])$ in [44]. These quantities are only defined for an observed value of uncertain variable $Y = y$; however, the definition in (3) relies on the worst-case ratio.

Now, a non-stochastic version of Fano's inequality can be established. Let the uncertain variable $\hat{X}(y)$ denote an estimate of an uncertain variable X based on uncertain variable Y for measurement $Y = y$. In this paper, only unbiased estimators, defined below, are considered.

Assumption II.1 (Unbiased Estimator)**.** *An estimator $\hat{X} : [\![Y]\!] \to [\![X]\!]$ is unbiased if $\hat{X}(y) \in [\![X|y]\!]$.*

This essentially means that the estimate is consistent with the received measurement, i.e., $X, \hat{X}(y) \in [\![X|y]\!]$. A measure of the quality of the estimate can be defined as

$$d_{\max}(X, \hat{X}(Y)) := \operatorname*{ess\,sup}_{y\in[\![Y]\!]} \operatorname*{ess\,sup}_{x\in[\![X|y]\!]} \|x - \hat{X}(y)\|_2. \tag{4}$$

This measure captures the largest worst-case distance between uncertain variable X and its estimate. Before stating the following theorem, a notation needs to be defined. Let $\Gamma : z \mapsto \int_0^\infty x^{z-1} \exp(-x)\mathrm{d}x$ be the Gamma function (extension of factorial to real numbers).

Theorem II.1. *Consider X and $Y = f(X)$ are uncertain variables for some function $f : [\![X]\!] \to [\![Y]\!]$. Assume that $[\![X|y]\!]$ is a Borel set for all $y \in [\![Y]\!]$. Then,*

$$\frac{\Gamma(n_x/2 + 1)^{1/n_x}}{\sqrt{\pi}} \exp\left(\frac{h_0(X|Y)}{n_x}\right) \leq d_{\max}(X, \hat{X}(Y)).$$

Proof. Note that

$$\begin{aligned} &\operatorname*{ess\,sup}_{y\in[\![Y]\!]} \operatorname*{ess\,sup}_{x\in[\![X|y]\!]} \|x - \hat{X}(y)\|_2 \\ &\qquad \geq \operatorname*{ess\,sup}_{y\in[\![Y]\!]} \inf_{\hat{X}} \operatorname*{ess\,sup}_{x\in[\![X|y]\!]} \|x - \hat{X}(y)\|_2 \\ &\qquad \geq \operatorname*{ess\,sup}_{y'\in[\![Y]\!]} \frac{1}{2} \operatorname{diam}([\![X|y']\!]), \end{aligned}$$

where the last inequality follows from the fact that $\operatorname{ess\,sup}_{x\in[\![X|y']\!]}\|x-\hat{X}(y')\|_2$ is the radius of a ball that encompasses $[\![X|y']\!]$ and is centred at $\hat{X}(y')\in[\![X|y']\!]$ (see Assumption II.1) and the smallest such radius is always larger than or equal to half of the diameter. Therefore,

$$\operatorname*{ess\,sup}_{x\in[\![X]\!]}\ \operatorname*{ess\,sup}_{y:x\in[\![X|y]\!]}\|x-\hat{X}(y)\|_2\geq\frac{1}{2}\operatorname*{ess\,sup}_{y\in[\![Y]\!]}\mathfrak{H}^{n_x}([\![X|y]\!])^{1/n_x},$$

where $\mathfrak{H}^{n_x}(\cdot)$ denotes the outer Hausdorff measure, and the last step follows from the relationship between Hausdorff and Lebesgue measures [51, p 28-30] for Borel sets, i.e., $\mathfrak{H}^{n_x}([\![X|y]\!])=2^{n_x}\Gamma(n_x/2+1)\mu([\![X|y]\!])/\pi^{n_x/2}$. This completes the proof. □

Example II.1. *The notions of non-stochastic information and relative entropy are not useful for measuring privacy leakage. This is because it considers the size of the largest $\mu([\![X|y]\!])$, while privacy wants to ensure that all $\mu([\![X|y]\!])$ are large. To see this, consider the following example:*

$$f(X):=\begin{cases}X, & 0\leq X<1/2,\\ 1, & \textit{otherwise},\end{cases}$$

where X is an uncertain variable with $[\![X]\!]=[0,1]$. It is easy to show that $h_0(X|f(X))=\log(1/2)$; note that $h_0(X)=0$. Construct an estimator of the form

$$\hat{X}(Y):=\begin{cases}Y, & 0\leq Y<1/2,\\ 3/4, & \textit{otherwise},\end{cases}$$

Note that $d_{\max}(X,\hat{X}(f(X)))=1/4$ attaining the lower bound in Theorem II.1 (as $\Gamma(3/2)=\sqrt{\pi}/2$), proving that $\hat{X}(\cdot)$ is optimal in the sense of minimizing $d_{\max}(X,\hat{X}(f(X)))$. The function $f(\cdot)$ is clearly not privacy-preserving as $f(X)=X$ for many inputs! In fact, $\inf_{y\in[\![Y]\!]}\mu([\![X|y]\!])=0$.

Therefore, a notion of *relative disarray* can be defined:

$$d_0(X|Y):=\inf_{y\in[\![Y]\!]}\log(\mu([\![X|y]\!])).\tag{5}$$

Following this, *non-stochastic information leakage* can be defined as

$$L_0(X;Y):=h_0(X)-d_0(X|Y).\tag{6}$$

Another useful measure of the quality of an estimator is

$$d_{\min}(X,\hat{X}(Y)):=\operatorname*{ess\,inf}_{y\in[\![Y]\!]}\operatorname*{ess\,sup}_{x\in[\![X|y]\!]}\|x-\hat{X}(y)\|_2.\tag{7}$$

This measure captures the smallest worst-case distance between uncertain variable X and its estimate. If $d_{\min}(X,\hat{X}(Y))$ is small, it means that there exist some values for uncertain variable X for which the privacy is not preserved in the sense that an adversary can reconstruct X for those values accurately based on Y.

Theorem II.2. *Consider X and $Y=f(X)$ are uncertain variables for some function $f:[\![X]\!]\to[\![Y]\!]$. Assume that $[\![X|y]\!]$ is a Borel set for all $y\in[\![Y]\!]$. Then,*

$$\frac{\Gamma(n_x/2+1)^{1/n_x}}{\sqrt{\pi}}\exp\left(\frac{d_0(X|Y)}{n_x}\right)\leq d_{\min}(X,\hat{X}(Y)).$$

Proof. The proof follows the same line of reasoning as in the proof of Theorem II.1. Note that,

$$\begin{aligned}&\operatorname*{ess\,inf}_{y\in[\![Y]\!]}\operatorname*{ess\,sup}_{x\in[\![X|y]\!]}\|x-\hat{X}(y)\|_2\\ &\qquad\geq\operatorname*{ess\,inf}_{y\in[\![Y]\!]}\operatorname*{ess\,inf}_{\hat{X}}\operatorname*{ess\,sup}_{x\in[\![X|y]\!]}\|x-\hat{X}(y)\|_2\\ &\qquad\geq\operatorname*{ess\,inf}_{y\in[\![Y]\!]}\frac{1}{2}\operatorname{diam}([\![X|y]\!]).\end{aligned}$$

This completes the proof. □

Example II.1 (Cont'd)**.** *In this example, $d_0(X|f(X))=-\infty$ (by the convention that $\log(0)=\lim_{t\searrow 0}\log(t)=-\infty$) and $L_0(X;f(X))=+\infty$. Hence, non-stochastic information leakage $L_0(X;f(X))$ can accurately capture the fact that $f(X)$ is not privacy preserving. In addition, it can be seen that $d_{\min}(X,\hat{X}(Y))=0$, which proves that again $\hat{X}(Y)$ is optimal in the sense of the cost function $d_{\min}(X,\hat{X}(Y))$ (as the lower bound in Theorem II.2 is achieved).*

In general, the non-stochastic information $I_0(\cdot;\cdot)$ and non-stochastic information leakage $L_0(\cdot;\cdot)$ are not symmetrical, that is, $I_0(X;Y)\neq I_0(Y;X)$ and $L_0(X;Y)\neq L_0(Y;X)$ in general (contrary to mutual information in the information theory literature). Many measures of information have been introduced in the past for stochastic variables that are asymmetric and have been proved to be useful in practice [52]–[55]. However, symmetry enables proving useful relaxations; see Proposition III.1 in the next section. A non-stochastic information transmission was proposed in [56], defined as

$$T_0(X;Y):=h_0(X)+h_0(Y)-h_0(X,Y).\tag{8}$$

This new measure of information is symmetric, that is, $T_0(X;Y)=T_0(Y;X)$. Although being symmetric in general, utilization of this measure is not possible (because $[\![Y]\!]$ can be a discrete set $\mu([\![Y]\!])=0$ and thus $h_0(X,Y)=0$ in all such cases). Another symmetric measure of information is the maximin information. In order to define this measure of information, the notion of taxicab connectivity must be defined, borrowed from the pioneering works in [46], [48] on non-stochastic information theory.

Definition II.2 (Taxicab Connectivity)**.**

- *$(x,y),(x',y')\in[\![X,Y]\!]$ are taxicab[3] connected if there exists a sequence of points $\{(x_i,y_i)\}_{i=1}^n\subseteq[\![X,Y]\!]$ such that $(x_1,y_1)=(x,y)$, $(x_n,y_n)=(x',y')$, and either $x_i=x_{i-1}$ or $y_i=y_{i-1}$ for all $i\in\{2,\dots,n\}$;*
- *$\mathcal{A}\subseteq[\![X,Y]\!]$ is taxicab connected if all points in $[\![X,Y]\!]$ are taxicab connected;*
- *$\mathcal{A},\mathcal{B}\subseteq[\![X,Y]\!]$ are taxicab isolated if there do not exist points $(x,y)\in\mathcal{A}$ and $(x',y')\in\mathcal{B}$ such that (x,y) and (x',y') are taxicab connected;*
- *A taxicab partition of $[\![X,Y]\!]$ is a set of sets $\mathfrak{F}(X,Y):=\{\mathcal{A}_i\}_{i=1}^n$ such that $[\![X,Y]\!]\subseteq\bigcup_{i=1}^n\mathcal{A}_i$, any $\mathcal{A}_i,\mathcal{A}_j$ are taxicab isolated if $j\neq i$, and $\mathcal{A}_i$ is taxicab connected for all i.*

[3]The term refers to taxis/cabs in New York in which they connect two intersections by a sequence of horizontal or vertical moves.

There exists a unique taxicab partition for any $[\![X,Y]\!]$ [46]. Maximin information can be defined as

$$I_\star(X;Y) := \log(|\mathfrak{F}(X,Y)|), \tag{9}$$

where $\mathfrak{F}(X,Y)$ denotes the unique taxicab partition of $[\![X|Y]\!]$. It has been proved that $|\mathfrak{F}(X,Y)| = |\mathfrak{F}(Y,X)|$ and thus $I_\star(X;Y) = I_\star(Y;X)$ resulting in a symmetric notion of information [46].

Example II.1 (Cont'd)**.** *In this example, $I_\star(X;f(X)) = +\infty$. This instantly shows that $f(X)$ is not privacy preserving.*

III. Problem Formulation

In what follows, it is assumed that a private dataset X is available to a secure trusted agent. Anyone may submit a query of the form $f(\cdot)$, i.e., it can request that the trusted agent compute and provide the response $f(X)$.

Definition III.1 (Measure of Privacy)**.** *Let $\tilde{f}(\cdot)$ be a reporting function and define uncertain variable Y based on uncertain variable X such that $Y = \tilde{f}(X)$. Then, the measure of privacy for the reporting function $\tilde{f}$ is*

$$\mathcal{P}_1(\tilde{f}) := \frac{1}{L_0(X;Y)}, \tag{10a}$$

$$\mathcal{P}_2(\tilde{f}) := \frac{1}{I_\star(X;Y)}. \tag{10b}$$

The inverse relationship between the measures of privacy and information in (10) is because information leakage reduces the privacy guarantee. A useful and intuitive property for the aforementioned measures of privacy can be proved to illustrate that after releasing an output it is not possible to gain more information from the data by additional manipulations.

Theorem III.1 (Post Processing)**.** *$\mathcal{P}_i(g\circ f) \geq \mathcal{P}_i(f)$ for both $i = 1, 2$.*

Proof. Let uncertain variable Y and Z be defined as $Y(\omega) := f(X(\omega))$ and $Z(\omega) := g(Y(\omega))$ for all $\omega \in \Omega$. The data processing inequality in [46] implies that $I_\star(X;Z) \leq I_\star(X;Y)$. Therefore, $\mathcal{P}_2$ can be only increased by post processing. For the other measure of privacy note that

$$\begin{aligned} d_0(Z|X) &= \operatorname*{ess\,inf}_{z\in[\![Z]\!]} \mu([\![X|z]\!]) \\ &= \operatorname*{ess\,inf}_{z\in[\![Z]\!]} \mu\Big(\bigcup_{y'\in[\![Y|z]\!]} [\![X|y']\!]\Big) \\ &\geq \operatorname*{ess\,inf}_{z\in[\![Z]\!]} \operatorname*{ess\,inf}_{y\in[\![Y|z]\!]} \mu([\![X|y]\!]) \\ &= \operatorname*{ess\,inf}_{y\in[\![Y]\!]} \mu([\![X|y]\!]) \\ &\geq d_0(X|Y). \end{aligned}$$

Hence, $\mathcal{P}_1$ can also be only increased by post processing. This concludes the proof. □

The best policy for preserving privacy, maximizing the measure of privacy, is to ensure that X and $f(X)$ are unrelated (making $\mathcal{P}_i(f) = 0$). This is, of course, without any value as all the information regarding X would be lost and the utility of the report (in every possible sense) is zero. Therefore, there is a need for balancing utility and privacy.

Definition III.2 (Measure of Quality)**.** *The measure of quality for the reporting function $\tilde{f}$ for the query f is*

$$\mathfrak{Q}(\tilde{f}) := \frac{1}{\operatorname*{ess\,sup}_{x\in[\![X]\!]} \|f(x) - \tilde{f}(x)\|_2}. \tag{11}$$

With these definition ready, the optimal privacy-preserving policy $\tilde{f}$ can be computed by solving the optimization problem in

$$\mathbf{P}_\gamma : \max_{\tilde{f}\in\mathcal{F}} \quad \mathcal{P}_i(\tilde{f}), \tag{12a}$$

$$\text{s.t.} \quad \mathfrak{Q}(\tilde{f}) \geq \gamma, \tag{12b}$$

where $\mathcal{F}$ denotes the set of functions over which the privacy measure is optimized, i.e., the set of functions of interest for implementing as potential privacy-preserving policies.

Proposition III.1. *Assume that $[\![Y]\!] \subseteq \mathbb{R}$. For any $\tilde{f} = g\circ f$,*

$$I_\star(X; g(f(X))) \leq I_\star(f(X); g(f(X))), \tag{13a}$$

$$\mathfrak{Q}(\tilde{f}) = 1/\operatorname*{ess\,sup}_{y\in[\![Y]\!]} \|y - g(y)\|_2. \tag{13b}$$

Proof. Let uncertain variable Y and Z be defined as $Y(\omega) := f(X(\omega))$ and $Z(\omega) := g(Y(\omega))$ for all $\omega \in \Omega$. The data processing inequality [46] shows that $I_\star(X;Z) \leq \min(I_\star(X;Y), I_\star(Z;Y))$. This concludes the proof for (13a). The proof for (13b) follows from the definition. □

Proposition III.1 states that, when restricting the search for privacy-preserving policies over the set of policies $\mathcal{F} := \{\tilde{f} | \exists g \in \mathcal{G} : \tilde{f} = g\circ f\}$ for some set $\mathcal{G}$, the privacy metric can be relaxed to $I_\star(f(X); g(f(X)))$. Thus, the optimization problem in (12) with privacy measure (10b) can be *relaxed* to:

$$\mathbf{P}'_\gamma : \min_{g\in\mathcal{G}} \quad I_\star(Y; g(Y)), \tag{14a}$$

$$\text{s.t.} \quad \operatorname*{ess\,sup}_{y\in[\![Y]\!]} \|y - g(y)\|_2 \leq 1/\gamma, \tag{14b}$$

In the relaxed problem, f does not directly play a role in the privacy metric and, therefore, the optimal privacy-preserving policy becomes independent of f. Note that such a relaxation is not possible for the privacy measure (10a) because this measure of information is not symmetric and thus the data processing inequality does not hold for it in both directions.

IV. Privacy-Preserving Policies

Before stating the results of the paper, the set of piecewise constant functions should be defined. Over the real line $\mathbb{R}$, a mapping $g : [\underline{y}, \overline{y}] \to [\underline{y}, \overline{y}]$ is a piecewise constant function if there exist $\underline{y} = a_1 \leq a_2 \leq \cdots \leq a_{q+1} = \overline{y}$ and $b_1 \leq b_2 \leq \cdots \leq b_q$ for some arbitrary number $q \in \mathbb{N}$ such that $g(y) = b_i$ for all $y \in [a_i, a_{i+1})$ except for $i = q$ in which case $g(y) = b_q$ for all $y \in [a_q, a_{q+1}]$. The ordered sets $(a_i)_{i=1}^{q+1}$ and $(b_i)_{i=1}^{q}$ are referred to as the parameters of the piecewise constant function. Let $\mathcal{Q}([\underline{y}, \overline{y}])$ denote the set of all piecewise constant functions. For more general domains $\mathcal{X}$, a function

$g : \mathcal{X} \to \mathbb{R}$ is a piecewise constant function if there exist sets $\{\mathcal{X}_i\}_{i=1}^q$ such that $\mathcal{X} \subseteq \bigcup_{i=1}^q \mathcal{X}_i$, $\mathcal{X}_i \cap \mathcal{X}_j = \emptyset$ if $i \neq j$, and $g(x) = b_i$ if $b_i \in \mathcal{X}_i$. The ordered sets $(\mathcal{X}_i)_{i=1}^q$ and $(b_i)_{i=1}^q$ are referred to as the parameters of the piecewise constant function. Let $\mathcal{Q}(\mathcal{X})$ denote the set of all piecewise constant functions. When $\mathcal{X}$ is obvious from the context, $\mathcal{Q}$ is used instead of $\mathcal{Q}(\mathcal{X})$. The set of piecewise constant functions is dense in L^p for all $p \in [1, +\infty)$ [57]. In the next theorem, it is shown that searching over the set of piecewise constant functions is enough for finding the solution of (12).

Theorem IV.1 (Solution Class)**.** *The solution of* (12) *for the privacy metric in* (10b) *over the set of piecewise differentiable functions is a piecewise constant function.*

Proof. Let $x \in [\![X]\!]$ be any point such that $\nabla \tilde{f}(x) \neq 0$. Then there exists a direction d such that $d^\top \nabla \tilde{f}(x) \neq 0$. Assume that $d^\top \nabla \tilde{f}(x) > 0$; the proof for the other case is identical and is thus omitted. By piecewise continuity of the derivatives, it can be deduced that there exists a small enough neighbourhood around x of the form $\|\tilde{x} - x\| \leq \epsilon \|d\|$ inside which $d^\top \nabla \tilde{f}(\tilde{x}) > 0$. Therefore, for all $w \in (-\epsilon, \epsilon)$, $\tilde{f}(x + wd)$ is increasing and takes a unique value for any $w \in (-\epsilon, \epsilon)$. It must be established that no two distinct points in $\{(x + wd, \tilde{f}(x + wd))|w \in (-\epsilon, \epsilon)\}$ are taxicab connected. This is done by contrapositive. Assume that this not the case. Therefore, there exists $(x, y), (x', y') \in \{(x + wd, \tilde{f}(x + wd))|w \in (-\epsilon, \epsilon)\} \subseteq [\![X, Y]\!]$ that are taxicab connected. This implies that there exists a sequence of points $\{(x_i, y_i)\}_{i=1}^n \subseteq [\![X, Y]\!]$ such that $(x, y) \neq (x', y')$, $(x_1, y_1) = (x, y)$, $(x_n, y_n) = (x', y')$, and either $x_i = x_{i-1}$ or $y_i = y_{i-1}$ for all $i \in \{2, \ldots, n\}$. Because f is a function (i.e., $y_i = \tilde{f}(x_i) = \tilde{f}(x_{i-1}) = y_{i-1}$ if $x_i = x_{i-1}$), all transitions such that $x_i = x_{i-1}$ can be eliminated (as it would also implies that $y_i = y_{i-1}$). Therefore, a subsequence of points $\{(\bar{x}_i, \bar{y}_i)\}_{i=1}^{\bar{n}} \subseteq \{(x_i, y_i)\}_{i=1}^n \subseteq [\![X, Y]\!]$ can be constructed so that $(\bar{x}_1, \bar{y}_1) = (x, y)$, $(\bar{x}_{\bar{n}}, \bar{y}_{\bar{n}}) = (x', y')$, and $\bar{y}_i = \bar{y}_{i-1}$ for all $i \in \{2, \ldots, \bar{n}\}$. This implies that $y' = \bar{y}_{\bar{n}} = \bar{y}_{\bar{n}-1} = \cdots = \bar{y}_2 = \bar{y}_1 = y$. This is in contradiction with the assumption that $(x, y) \neq (x', y')$ because it must be that $y \neq y'$; note that if $x_1 \neq x_2$ in $\{(x + wd, \tilde{f}(x + wd))|w \in (-\epsilon, \epsilon)\}$, it must also hold that $y_1 \neq y_2$. Noting that no two distinct points in $\{(x + wd, \tilde{f}(x + wd))|w \in (-\epsilon, \epsilon)\}$ are taxicab connected, there needs to be, at least, as many taxicab partitions as in the number of points in $\{(x + wd, \tilde{f}(x + wd))|w \in (-\epsilon, \epsilon)\}$. This implies that $|\mathfrak{F}(X, Y)| = \infty$. The other category of functions is all functions for which $\nabla \tilde{f}(x) = 0$ (where defined) for all x. The only functions that satisfy this condition are piecewise constant functions. For piecewise constants $|\mathfrak{F}(X, Y)| = q < \infty$ with q denoting the number of disjoint sets $\{\mathcal{X}_i\}_{i=1}^q$. □

This fundamental result restricts the set of optimal privacy-preserving policies greatly and thus reduces the complexity of finding one.

Definition IV.1 (Uniform Quantizer)**.** *A uniform quantizer is a scalar piecewise constant function with parameters* $(a_i)_{i=1}^{q+1}$ *and* $(b_i)_{i=1}^q$ *such that* $a_{i+1} - a_i = a_{j+1} - a_j$ *and* $b_j = (a_j + a_{j+1})/2$ *for all* $1 \leq i, j \leq q$*. A uniform quantizer can be equivalently represented by the range* $[a_1, a_{q+1}]$ *and the number of bins* q*.*

As the first step, the relaxed problem in (14) is solved for scalar cases in the next theorem.

Theorem IV.2 (Relaxed Policy)**.** *Assume that* $[\![Y]\!] = [\underline{y}, \overline{y}] \subseteq \mathbb{R}$*. The solution of* (14) *over* $\mathcal{F} = \mathcal{Q} \circ \{f\}$ *is a uniform quantizer, equi-dividing* $[\![Y]\!]$ *into* $\lceil \gamma(\overline{y} - \underline{y})/2 \rceil$ *bins.*

Proof. Note that, for any $\tilde{f} \in \mathcal{F}$,

$$\begin{aligned}\frac{1}{\mathfrak{Q}(\tilde{f})} &= \operatorname*{ess\,sup}_{x \in [\![X]\!]} |f(x) - g(f(x))| \\ &= \operatorname*{ess\,sup}_{y \in [\![Y]\!]} |y - g(y)| \\ &= \max_{1 \leq i \leq q} \max(|b_i - a_i|, |b_i - a_{i+1}|),\end{aligned}$$

where g is any function in $\mathcal{Q}$. Furthermore, $I_\star(Y; g(Y)) = q$. The problem (14) can be rewritten as

$$\begin{aligned}\min_{(a_i)_{i=1}^{q+1}, (b_i)_{i=1}^q} \quad & q, \\ \text{s.t.} \quad & \max_{1 \leq i \leq q} \max(|b_i - a_i|, |b_i - a_{i+1}|) \leq \frac{1}{\gamma}, \\ & a_{q+1} = \overline{y}, \quad a_1 = \underline{y}.\end{aligned}$$

By selecting $b_i = (a_i + a_{i+1})/2$, $\max(|b_i - a_i|, |b_i - a_{i+1}|)$ can be made as small as possible. Thus, this problem can be rewritten as

$$\min_{(a_i)_{i=1}^{q+1}, (b_i)_{i=1}^q} \quad q, \tag{15a}$$

$$\text{s.t.} \quad \max_{1 \leq i \leq q} \frac{1}{2}|a_{i+1} - a_i| \leq \frac{1}{\gamma}, \tag{15b}$$

$$\sum_{i=1}^q |a_{i+1} - a_i| = \overline{y} - \underline{y}. \tag{15c}$$

It is easy to show that $q < \gamma(\overline{y} - \underline{y})/2$, the problem is not feasible. This is because

$$\begin{aligned}\sum_{i=1}^q |a_{i+1} - a_i| &\leq q \max_{1 \leq i \leq q} |a_{i+1} - a_i| \\ &\leq q2/\gamma \\ &< \overline{y} - \underline{y}.\end{aligned}$$

Therefore, a lower bound on the solution of (15) is then the smallest integer that is larger than $\gamma(\overline{y} - \underline{y})/2$, i.e., $\lceil \gamma(\overline{y} - \underline{y})/2 \rceil$. The uniform quantizer in the statement of theorem achieves the lower bound. □

Now, the general problem in (12) can be considered for scalar queries over the set of piecewise continuous functions.

Theorem IV.3 (Optimal Policy)**.** *Assume that* $[\![Y]\!] \subseteq \mathbb{R}$*. The solution of* (12) *for privacy measures in* (10a) *over* $\mathcal{F} = \mathcal{Q}([\![X]\!])$ *is given by*

$$b_i^* \in \arg\min_{b_i} \max_{x \in \mathcal{X}_i^*} |f(x) - b_i|, \tag{16a}$$

$$\{\mathcal{X}_i^*\}_{i=1}^{q^*} \in \operatorname*{arg\,max}_{\{\mathcal{X}_i\}_{i=1}^q : [\![X]\!] \subseteq \bigcup_{i=1}^q \mathcal{X}_i} \min_{1 \leq i \leq q} \mu(\mathcal{X}_i), \tag{16b}$$

$$\text{s.t.} \quad \max_{1 \leq i \leq q} \operatorname{rad}(f(\mathcal{X}_i)) \leq \frac{1}{\gamma}. \tag{16c}$$

For privacy measures in (10b) *over* $\mathcal{F} = \mathcal{Q}([\![X]\!])$ *is given by*

$$b_i^* \in \arg\min_{b_i} \max_{x \in \mathcal{X}_i^*} |f(x) - b_i|, \tag{17a}$$

$$\{\mathcal{X}_i^*\}_{i=1}^{q^*} \in \arg\max_{\{\mathcal{X}_i\}_{i=1}^{q}: [\![X]\!] \subseteq \bigcup_{i=1}^{q} \mathcal{X}_i} q, \tag{17b}$$

$$\text{s.t.} \quad \max_{1 \le i \le q} \operatorname{rad}(f(\mathcal{X}_i)) \le \frac{1}{\gamma}. \tag{17c}$$

Proof. Note that, for any $\tilde{f} \in \mathcal{F} = \mathcal{Q}([\![X]\!])$, there exists $\{\mathcal{X}_i, b_i\}_{i=1}^q$ such that $[\![X]\!] \subseteq \bigcup_{i=1}^q \mathcal{X}_i$, $\mathcal{X}_i \cap \mathcal{X}_j = \emptyset$ if $i \neq j$, and $\tilde{f}(x) = b_i$ if $b_i \in \mathcal{X}_i$. Hence,

$$\begin{aligned}\frac{1}{\mathfrak{Q}(f)} &= \operatorname*{ess\,sup}_{x \in [\![X]\!]} |f(x) - \tilde{f}(x)| \\ &= \max_{1 \le i \le q} \sup_{x \in \mathcal{X}_i} |f(x) - b_i|.\end{aligned}$$

Let us consider the privacy measure in (10a). It can be shown that

$$\begin{aligned} d_0(X|\tilde{f}(X)) &= \operatorname*{ess\,inf}_{x \in [\![X]\!]} \log(\mu([\![X|\tilde{f}(x)]\!])) \\ &= \operatorname*{ess\,inf}_{1 \le i \le q} \log(\mu([\![X|\tilde{f}(x) = b_i]\!])) \\ &= \min_{1 \le i \le q} \log(\mu(\mathcal{X}_i)).\end{aligned}$$

The problem (12) can be rewritten as

$$\begin{aligned} \max_{\{\mathcal{X}_i, b_i\}_{i=1}^q} & \min_{1 \le i \le q} \log(\mu(\mathcal{X}_i)), \\ \text{s.t.} \quad & \max_{1 \le i \le q} \sup_{x \in \mathcal{X}_i} |f(x) - b_i| \le \frac{1}{\gamma}, \\ & [\![X]\!] \subseteq \bigcup_{i=1}^{q} \mathcal{X}_i. \end{aligned}$$

This problem can be rewritten again as

$$\begin{aligned} \max_{\{\mathcal{X}_i\}_{i=1}^{q}: [\![X]\!] \subseteq \bigcup_{i=1}^{q} \mathcal{X}_i} & \min_{1 \le i \le q} \mu(\mathcal{X}_i), \\ \text{s.t.} \quad & \max_{1 \le i \le q} \min_{b_i} \sup_{x \in \mathcal{X}_i} |f(x) - b_i| \le \frac{1}{\gamma}. \end{aligned}$$

Noting that $\operatorname{rad}(f(\mathcal{X}_i)) = \min_{b_i} \sup_{y \in f(\mathcal{X}_i)} |y - b_i|$ concludes the proof for the first part. Now, let us consider the privacy measure in (10b). It can be seen that $I_\star(X; \tilde{f}(X)) = q$. This is because $(\mathcal{X}_i \times \{b_i\})_{i=1}^q$ forms a taxicab partition for $[\![X, f(X)]\!]$. Hence, the problem (12) can be rewritten as

$$\min_{\{\mathcal{X}_i\}_{i=1}^{q}: [\![X]\!] \subseteq \bigcup_{i=1}^{q} \mathcal{X}_i} \quad q, \tag{18}$$

$$\text{s.t.} \quad \max_{1 \le i \le q} \min_{b_i} \sup_{x \in \mathcal{X}_i} |f(x) - b_i| \le \frac{1}{\gamma}. \tag{19}$$

This concludes the proof. □

For the case where $[\![X]\!] \subseteq \mathbb{R}$, the results of Theorems IV.3 and IV.2 are equal [58]. Therefore, there is no loss of generality in designing the quantizer after computing $f(x)$ rather than designing a general $\tilde{f}(x)$. In the next corollary, this property is proved for general queries under mild assumptions.

Corollary IV.1. *Let f be a function that $f^{-1}(y) := \{x | f(x) = y\}$ is a connected set for all $y \in [\![Y]\!]$. Then, the optimal policy in Theorem IV.3 for the privacy metric* (10b) *is equal to the the optimal policy in Theorem IV.2.*

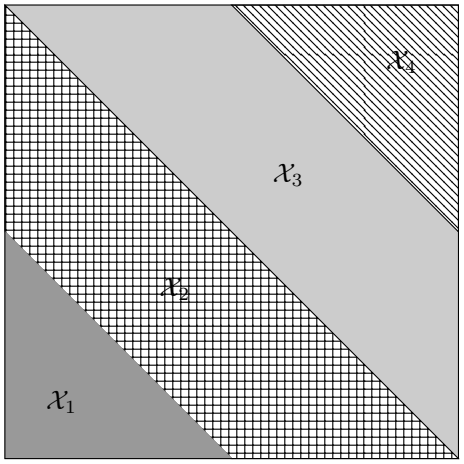

Fig. 1. The regions $\{\mathcal{X}_i\}_{i=1}^4$ for the optimal privacy-preserving policy in Theorem IV.3 for $[\![X]\!] = [-2, 2]^2$, $\gamma = 2$, and linear query $f(x) = \mathbb{1}^\top x/2$. For the optimal policy, $b_1 = -1.5$, $b_2 = -0.5$, $b_3 = 0.5$, and $b_4 = 1.5$.

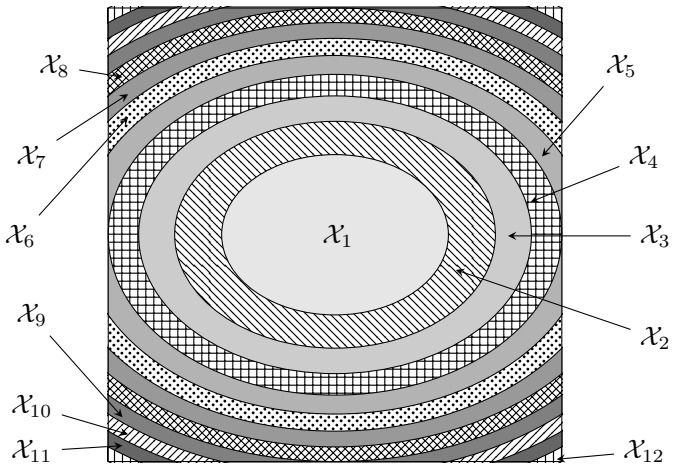

Fig. 2. The regions $\{\mathcal{X}_i\}_{i=1}^{12}$ for the optimal privacy-preserving policy in Theorem IV.3 for $[\![X]\!] = [-2, 2]^2$, $\gamma = 2$, and nonlinear query $f(x) = x^\top \operatorname{diag}(1, 2)x$. For the optimal policy, $b_i = i - 0.5$ for all $1 \le i \le 12$.

Proof. The solution of (12) for the privacy measure in (10b) is given by (18). Define $\mathcal{Y}_i' = \{y | \exists x \in \mathcal{X}_i : y = f(x)\}$. The inequality constraint in (18) is equivalent to saying that that $\max_{1 \le i \le q} \min_{b_i} \sup_{y \in \mathcal{Y}_i'} |y - b_i| \le 1/\gamma$. Let $\mathcal{Y}_i$ be defined such that $\mathcal{Y}_1 = \mathcal{Y}_1'$ and $\mathcal{Y}_i = \mathcal{Y}_i' \backslash (\mathcal{Y}_1 \cup \cdots \cup \mathcal{Y}_{i-1})$ for all $i > 1$. Clearly, $\mathcal{Y}_i \subseteq \mathcal{Y}_i'$ and thus $\max_{1 \le i \le q} \min_{b_i} \sup_{y \in \mathcal{Y}_i} |y - b_i| \le 1/\gamma$. If $\mathcal{Y}_i$ is connected, it should take one of the following forms $[a_i, a_{i+1}]$, $[a_i, a_{i+1})$, $(a_i, a_{i+1}]$, or (a_i, a_{i+1}). Therefore, by selecting $b_i = (a_i + a_{i+1})/2$ minimizes $\sup_{y \in \mathcal{Y}_i} |y - b_i|$. This implies that (18) can be rewritten as the optimization problem in the statement of Theorem IV.2. □

Example IV.1. *Consider a simple example in which reporting the average of two real numbers in $[-2, 2]$ is of interest. Therefore, the query is $f(x) = \mathbb{1}^\top x/2$. First, consider the relaxed problem in* (14)*. Assume that $\gamma = 2$. The optimal policy in this case is to quantize y with a uniform quantizer*

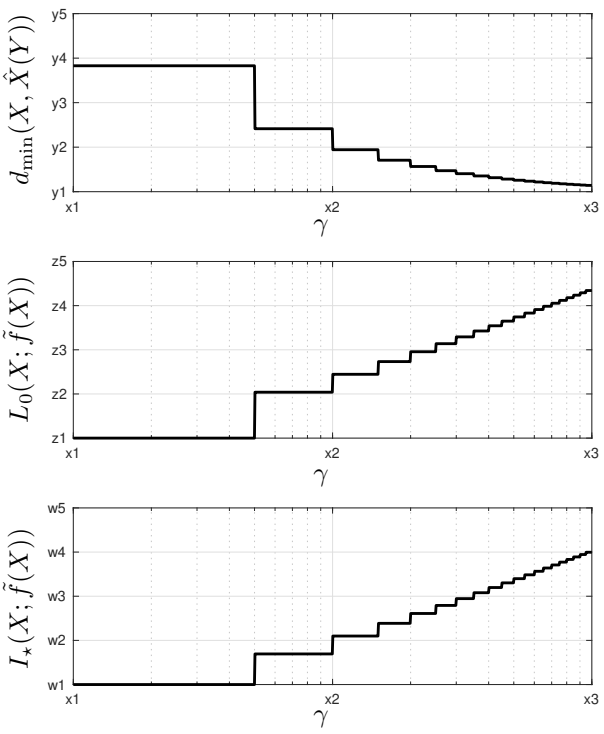

Fig. 3. The effect of parameter γ on the trade-off between utility γ and privacy, captured using the amount of private information leaked $L_0(X;\tilde{f}(X))$ and $I_\star(X;\tilde{f}(X))$ as well as the adversary's estimation error $d_{\min}(X,\hat{X}(Y))$.

over $[-2,2]$ *with* 4 *bins, denoted by* $g(\cdot)$*. Thus,*

$$\tilde{f}(x)=g(f(x))=\begin{cases}-1.5, & -2\le f(x)<-1,\\ -0.5, & -1\le f(x)<0,\\ 0.5, & 0\le f(x)<1,\\ 1.5, & 1\le f(x)\le 2.\end{cases}$$

This function can be rewritten as

$$\tilde{f}(x)=\begin{cases}-1.5, & -4\le x_1+x_2<-2,\\ -0.5, & -2\le x_1+x_2<0,\\ 0.5, & 0\le x_1+x_2<2,\\ 1.5, & 2\le x_1+x_2\le 4,\end{cases}\tag{20}$$

where x_i *denotes the* i*-th entry of* x*. Now, Theorem IV.3 can be used to find the optimal privacy-preserving policy for the case with privacy metric in* (10b)*. Figure 1 illustrates the regions* $\{\mathcal{X}_i\}_{i=1}^4$ *for the optimal privacy-preserving policy in Theorem IV.3 for* $[\![X]\!]=[-2,2]^2$*,* $\gamma=2$*, and linear query* $f(x)=\mathbb{1}^\top x/2$*. For the optimal policy in Figure 1,* $b_1=-1.5$*,* $b_2=-0.5$*,* $b_3=0.5$*, and* $b_4=1.5$*. It is interesting to note that the optimal policy in Figure 1 is in fact equal to* (20)*. Therefore, the relaxation in* (14) *is without loss of generality in this example. This is because* f *meets the condition of Corollary IV.1.*

The parameter γ *determines the trade-off between privacy and utility: by increasing* γ*, a larger bound on the quality is required and privacy guarantee must be weakened. To demonstrate this, consider the example discussed above with a general* $\gamma>0$*. The optimal policy in this case is to quantize* y *with a uniform quantizer over* $[-2,2]$ *with* $\lceil 2\gamma\rceil$ *bins. Figure 3 illustrates the amount of private information leaked* $L_0(X;\tilde{f}(X))$ *and* $I_\star(X;\tilde{f}(X))$*, and the adversary's estimation error* $d_{\min}(X,\hat{X}(Y))$*. Evidently, as the quality improves (*γ *increases), the privacy guarantee weakens (the amount of leaked information increases and the adversary's estimation error decreases).*

Now, focus on a non-linear query of the form $f(x)=x_1^2+2x_2^2$*. In this case,* $[\![Y]\!]=[0,12]$*. Therefore, the optimal policy of the relaxed problem in* (14) *for* $\gamma=2$ *is a uniform quantizer over* $[0,12]$ *with* 12 *bins. Again, use* g *denote this quantizer. It can be seen that*

$$\tilde{f}(x)=i+0.5,\ i\le x_1^2+2x_2^2<i+1,\ \forall i\in\{0,\dots,11\},\tag{21}$$

Again, Theorem IV.3 can be used to find the optimal privacy-preserving policy in this case. Figure 2 illustrates the regions $\{\mathcal{X}_i\}_{i=1}^{12}$ *for the optimal privacy-preserving policy in Theorem IV.3 for* $[\![X]\!]=[-2,2]^2$*,* $\gamma=2$*, and non-linear query* $f(x)=x^\top\mathrm{diag}(1,2)x$*. For the optimal policy,* $b_i=i-0.5$ *for all* $1\le i\le 12$*. Similarly, the optimal policy in Figure 2 is equal to* (21) *and thus, the relaxation in* (14) *is again without loss of generality as* f *meets the condition of Corollary IV.1.*

Example IV.2. *Consider a practical example in which the private dataset contains the height of* n_x *individuals in the range of* $[100,250]$ *centimetres. The submitted query is to compute the average height of the individuals in the dataset, i.e.,* $f(x)=\mathbb{1}^\top x/n_x$*. Following the results of the paper, the optimal privacy-preserving policy is to quantize* $f(x)$ *using a uniform quantizer over* $[100,250]$ *with* $\lceil 75\gamma\rceil$ *bins. In this case,* $d_{\min}(X,\hat{X}(\tilde{f}(X)))=150\sqrt{2}/\lceil 75\gamma\rceil$*, which is independent of* n_x*. This is because the worst-case in terms of preserving privacy occurs in a society with* n_x-2 *individuals whose heights are equal to* 250 *and two individuals whose heights are within* $(250-150/\lceil 75\gamma\rceil,250]$*. To be able to guarantee an error of at least* 10 *centimetres for the adversary,* γ *must be selected to be larger than* $22/75\approx 0.2933$*.*

V. Relationship to Other Notions of Privacy

In this section, the privacy credentials of k-anonymity is analyzed using the measures of privacy in (10). Consider a dataset $x\in\mathbb{X}\subseteq\mathbb{R}^{n\times m}$ with n rows (entries or individuals) and m columns (attributes). The following argument can easily be extended to other sets and is thus without loss of generality.

Definition V.1 (k-anonymity [30], [31], [59])**.** *A release of data is said to have the* k*-anonymity property if the information for each individual contained in the release cannot be distinguished from at least* $k-1$ *individuals whose information also appear in the release.*

Proposition V.1. *There exists a reporting function* $\tilde{f}(X)$ *admitting* k*-anonymity property for which the following holds:*

- $d_0(X|f(X))=0$ *(and thus* $L_0(X;f(X))=h_0(X)$*);*
- $I_\star(X;f(X))=\infty$*.*

Proof. Consider the case where x is a dataset that has k identical individuals. Let the first k rows denote the identical individuals. This is without the loss of generality as otherwise the rows can be swapped. Let $f : \mathbb{R}^{n\times m} \to \mathbb{R}^{n\times m}$ be any k-anonymous reporting function. Assume that the i-th row of $f(x)$ is report corresponding to the i-th row of x. This is again without the loss of generality as otherwise the output rows can be swapped. Construct $\tilde{f}$ such that

$$\tilde{f}(x) = \begin{bmatrix} x_1 \\ \vdots \\ x_k \\ \begin{bmatrix} 0_{(n-k)\times n} & I_{n-k} \end{bmatrix} f(x) \end{bmatrix}.$$

By construction $\tilde{f}$ is also a k-anonymous reporting function. However,

$$[\![X|\tilde{f}(x)]\!] = [\![X|f(x)]\!] \cap \left\{ \begin{bmatrix} w \\ z \end{bmatrix} \in \mathbb{X} \,\middle|\, w = \begin{bmatrix} x_1 \\ \vdots \\ x_k \end{bmatrix} \right\},$$

which shows that $\mu([\![X|\tilde{f}(x)]\!]) = 0$. Thus, $d_0(X|\tilde{f}(X)) = 0$. Finally, noting that $[\![X|\tilde{f}(x)]\!]$ must be included in the taxicab partitions for all choices of $x_1 = \cdots = x_k$, $|\mathfrak{F}(X, \tilde{f}(X))| = +\infty$. This shows that $I_\star(X; \tilde{f}(X)) = +\infty$. □

Proposition V.1 shows that k-anonymity is not private. This is because of the homogeneity attack [32], i.e., attacks that leverage the cases in which all the values for a sensitive value within a set of k records are identical. In such cases, even though the data has been k-anonymized, the sensitive value for the set of k records may be exactly predicted. Such cases are explored to prove Proposition V.1.

VI. Conclusions and Future Work

A deterministic privacy metric using non-stochastic information theory was presented. It was assumed that anyone can submit a query to a trusted server with access to a non-stochastic uncertain private data. Optimal privacy-preserving policy was proved to be a quantized version of the output of the submitted query. Finally, it was proved that k-anonymity is not privacy-preserving using the proposed privacy metric. Future work can focus on analysing non-scalar queries as well as demonstrating the performance of the method on publicly available datasets.

VII. Acknowledgement

The author is thankful to G. Nair at the University of Melbourne for discussions and comments.

References

[1] A. Narayanan and V. Shmatikov, "Robust de-anonymization of large sparse datasets," in *Security and Privacy, 2008. SP 2008. IEEE Symposium on*, pp. 111–125, IEEE, 2008.

[2] J. Su, A. Shukla, S. Goel, and A. Narayanan, "De-anonymizing web browsing data with social networks," in *Proceedings of the 26th International Conference on World Wide Web*, pp. 1261–1269, 2017.

[3] Y.-A. De Montjoye, C. A. Hidalgo, M. Verleysen, and V. D. Blondel, "Unique in the crowd: The privacy bounds of human mobility," *Scientific reports*, vol. 3, p. 1376, 2013.

[4] C. Dwork, "Differential privacy: A survey of results," in *Theory and Applications of Models of Computation: 5th International Conference, TAMC 2008, Xi'an, China, April 25-29, 2008. Proceedings* (M. Agrawal, D. Du, Z. Duan, and A. Li, eds.), pp. 1–19, Berlin, Heidelberg: Springer Berlin Heidelberg, 2008.

[5] C. Dwork and A. Roth, "The algorithmic foundations of differential privacy," *Foundations and Trends in Theoretical Computer Science*, vol. 9, no. 3–4, pp. 211–407, 2014.

[6] J. C. Duchi, M. I. Jordan, and M. J. Wainwright, "Local privacy and statistical minimax rates," in *Foundations of Computer Science (FOCS), 2013 IEEE 54th Annual Symposium on*, pp. 429–438, IEEE, 2013.

[7] P. Kairouz, S. Oh, and P. Viswanath, "Extremal mechanisms for local differential privacy," in *Advances in Neural Information Processing Systems*, pp. 2879–2887, 2014.

[8] A. Machanavajjhala, D. Kifer, J. Abowd, J. Gehrke, and L. Vilhuber, "Privacy: Theory meets practice on the map," in *Proceedings of the 2008 IEEE 24th International Conference on Data Engineering*, pp. 277–286, IEEE Computer Society, 2008.

[9] R. Hall, A. Rinaldo, and L. Wasserman, "Random differential privacy," *Journal of Privacy and Confidentiality*, vol. 4, no. 2, pp. 43–59, 2012.

[10] A. Padakandla, P. Kumar, and W. Szpankowski, "Preserving privacy and fidelity via Ehrhart theory," in *2018 IEEE International Symposium on Information Theory (ISIT)*, pp. 696–700, IEEE, 2018.

[11] J. Soria-Comas and J. Domingo-Ferrer, "Optimal data-independent noise for differential privacy," *Information Sciences*, vol. 250, pp. 200–214, 2013.

[12] Q. Geng and P. Viswanath, "The optimal mechanism in differential privacy," in *Proceedings of the IEEE International Symposium on Information Theory (ISIT)*, pp. 2371–2375, 2014.

[13] Q. Geng and P. Viswanath, "The optimal noise-adding mechanism in differential privacy," *IEEE Transactions on Information Theory*, vol. 62, no. 2, pp. 925–951, 2016.

[14] S. L. Warner, "Randomized response: A survey technique for eliminating evasive answer bias," *Journal of the American Statistical Association*, vol. 60, no. 309, pp. 63–69, 1965.

[15] A. D. Wyner, "The wire-tap channel," *Bell System Technical Journal*, vol. 54, no. 8, pp. 1355–1387, 1975.

[16] L. Sankar, S. R. Rajagopalan, and H. V. Poor, "Utility-privacy tradeoffs in databases: An information-theoretic approach," *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 6, pp. 838–852, 2013.

[17] T. Courtade, "Information masking and amplification: The source coding setting," in *Proceedings of the IEEE International Symposium on Information Theory Proceedings (ISIT)*, pp. 189–193, 2012.

[18] H. Yamamoto, "A source coding problem for sources with additional outputs to keep secret from the receiver or wiretappers," *IEEE Transactions on Information Theory*, vol. 29, no. 6, pp. 918–923, 1983.

[19] H. Yamamoto, "A rate-distortion problem for a communication system with a secondary decoder to be hindered," *IEEE Transactions on Information Theory*, vol. 34, no. 4, pp. 835–842, 1988.

[20] M. S. Alvim, M. E. Andrés, K. Chatzikokolakis, and C. Palamidessi, "On the relation between differential privacy and quantitative information flow," in *Automata, Languages and Programming* (L. Aceto, M. Henzinger, and J. Sgall, eds.), vol. 6756 of *Lecture Notes in Computer Science*, pp. 60–76, Springer Berlin Heidelberg, 2011.

[21] F. du Pin Calmon and N. Fawaz, "Privacy against statistical inference," in *Proceedings of the 50th Annual Allerton Conference onCommunication, Control, and Computing (Allerton)*, pp. 1401–1408, 2012.

[22] F. Farokhi, H. Sandberg, I. Shames, and M. Cantoni, "Quadratic Gaussian privacy games," in *Proceedings of the 54th IEEE Conference on Decision and Control*, pp. 4505–4510, 2015.

[23] F. Farokhi and G. Nair, "Privacy-constrained communication," *IFAC-PapersOnLine*, vol. 49, no. 22, pp. 43–48, 2016.

[24] M. J. Wainwright, M. I. Jordan, and J. C. Duchi, "Privacy aware learning," in *Proceedings of Advances in Neural Information Processing Systems (NIPS)*, pp. 1430–1438, 2012.

[25] Y. Liang, H. V. Poor, and S. Shamai, "Information theoretic security," *Foundations and Trends in Communications and Information Theory*, vol. 5, no. 4–5, pp. 355–580, 2009.

[26] L. Lai, S.-W. Ho, and H. V. Poor, "Privacy–security trade-offs in biometric security systems–Part I: Single use case," *IEEE Transactions on Information Forensics and Security*, vol. 6, no. 1, pp. 122–139, 2011.

[27] Z. Li and T. Oechtering, "Privacy on hypothesis testing in smart grids," in *IEEE Information Theory Workshop (ITW) 2015, Jeju, Korea, Oct. 11-15, 2015*, pp. 337–341, IEEE, 2015.

[28] G. Bassi, M. Skoglund, and P. Piantanida, "Lossy communication subject to statistical parameter privacy," in *2018 IEEE International Symposium on Information Theory (ISIT)*, pp. 1031–1035, IEEE, 2018.

[29] F. Farokhi and H. Sandberg, "Fisher information as a measure of privacy: Preserving privacy of households with smart meters using batteries," *IEEE Transactions on Smart Grid*, vol. 9, no. 5, pp. 4726–4734, 2018.

[30] P. Samarati, "Protecting respondents identities in microdata release," *IEEE transactions on Knowledge and Data Engineering*, vol. 13, no. 6, pp. 1010–1027, 2001.

[31] L. Sweeney, "k-anonymity: A model for protecting privacy," *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*, vol. 10, no. 05, pp. 557–570, 2002.

[32] A. Machanavajjhala, J. Gehrke, D. Kifer, and M. Venkitasubramaniam, "ℓ-diversity: privacy beyond k-anonymity," in *22nd International Conference on Data Engineering (ICDE'06)*, pp. 24–24, 2006.

[33] R. Bild, K. A. Kuhn, and F. Prasser, "SafePub: A truthful data anonymization algorithm with strong privacy guarantees," *Proceedings on Privacy Enhancing Technologies*, vol. 2018, no. 1, pp. 67–87, 2018.

[34] G. Poulis, A. Gkoulalas-Divanis, G. Loukides, S. Skiadopoulos, and C. Tryfonopoulos, *SECRETA: A Tool for Anonymizing Relational, Transaction and RT-Datasets*, pp. 83–109. Springer International Publishing, 2015.

[35] R. Bhaskar, A. Bhowmick, V. Goyal, S. Laxman, and A. Thakurta, "Noiseless database privacy," in *International Conference on the Theory and Application of Cryptology and Information Security*, pp. 215–232, Springer, 2011.

[36] S. U. Nabar, B. Marthi, K. Kenthapadi, N. Mishra, and R. Motwani, "Towards robustness in query auditing," in *Proceedings of the 32nd international conference on Very large data bases*, pp. 151–162, VLDB Endowment, 2006.

[37] F. K. Dankar and K. El Emam, "Practicing differential privacy in health care: A review.," *Transactions on Data Privacy*, vol. 6, no. 1, pp. 35–67, 2013.

[38] J. Mervis, "Researchers object to census privacy measure," *Science*, vol. 363, no. 6423, pp. 114–114, 2019.

[39] F. Farokhi, J. Milosevic, and H. Sandberg, "Optimal state estimation with measurements corrupted by Laplace noise," in *Decision and Control (CDC), 2016 IEEE 55th Conference on*, pp. 302–307, IEEE, 2016.

[40] J. Bambauer, K. Muralidhar, and R. Sarathy, "Fool's gold: an illustrated critique of differential privacy," *Vanderbilt Journal of Entertainment & Technology Law*, vol. 16, p. 701, 2013.

[41] C. E. Shannon, "A mathematical theory of communication," *Bell System Technical Journal*, vol. 27, no. 3, pp. 379–423, 1948.

[42] J. A. Thomas and T. M. Cover, *Elements of Information Theory*. Wiley Series in Telecommunications and Signal Processing, Wiley-Interscience, 2 ed., 2006.

[43] R. V. L. Hartley, "Transmission of information," *Bell System Technical Journal*, vol. 7, no. 3, pp. 535–563, 1928.

[44] A. N. Kolmogorov and V. M. Tikhomirov, "ε-entropy and ε-capacity of sets in function spaces," *Uspekhi Matematicheskikh Nauk*, vol. 14, no. 2, pp. 3–86, 1959. English translation American Mathematical Society Translations, series 2, vol. 17, pp. 277–364.

[45] A. Renyi, "On measures of entropy and information," in *Proc. of the Fourth Berkeley Symp. on Math. Statist. and Prob.*, vol. 1, pp. 547–561, 1961.

[46] G. N. Nair, "A nonstochastic information theory for communication and state estimation," *IEEE Transactions on Automatic Control*, vol. 58, no. 6, pp. 1497–1510, 2013.

[47] D. Jagerman, "ε-entropy and approximation of bandlimited functions," *SIAM Journal on Applied Mathematics*, vol. 17, no. 2, pp. 362–377, 1969.

[48] G. N. Nair, "A nonstochastic information theory for feedback," in *Decision and Control (CDC), 2012 IEEE 51st Annual Conference on*, pp. 1343–1348, IEEE, 2012.

[49] P. Duan, F. Yang, S. L. Shah, and T. Chen, "Transfer zero-entropy and its application for capturing cause and effect relationship between variables," *IEEE Transactions on Control Systems Technology*, vol. 23, no. 3, pp. 855–867, 2015.

[50] M. Wiese, K. H. Johansson, T. J. Oechtering, P. Papadimitratos, H. Sandberg, and M. Skoglund, "Uncertain wiretap channels and secure estimation," in *Information Theory (ISIT), 2016 IEEE International Symposium on*, pp. 2004–2008, IEEE, 2016.

[51] L. Ambrosio and P. Tilli, *Topics on Analysis in Metric Spaces*. Oxford Lecture Series in Mathematics, Oxford University Press, 2004.

[52] J. L. Massey, "Guessing and entropy," in *Information Theory, 1994. Proceedings., 1994 IEEE International Symposium on*, p. 204, IEEE, 1994.

[53] G. Smith, "On the foundations of quantitative information flow," in *International Conference on Foundations of Software Science and Computational Structures*, pp. 288–302, Springer, 2009.

[54] C. Braun, K. Chatzikokolakis, and C. Palamidessi, "Quantitative notions of leakage for one-try attacks," *Electronic Notes in Theoretical Computer Science*, vol. 249, pp. 75–91, 2009.

[55] S. A. M'rio, K. Chatzikokolakis, C. Palamidessi, and G. Smith, "Measuring information leakage using generalized gain functions," in *Computer Security Foundations Symposium (CSF), 2012 IEEE 25th*, pp. 265–279, IEEE, 2012.

[56] G. J. Klir, *Uncertainty and information: Foundations of generalized information theory*. John Wiley & Sons, 2005.

[57] S. Levy, F. Hirsch, and G. Lacombe, *Elements of Functional Analysis*. Graduate Texts in Mathematics, Springer New York, 2012.

[58] H. Konno and T. Kuno, "Best piecewise constant approximation of a function of single variable," *Operations Research Letters*, vol. 7, no. 4, pp. 205–210, 1988.

[59] P. Samarati and L. Sweeney, "Protecting privacy when disclosing information: k-anonymity and its enforcement through generalization and suppression," tech. rep., Harvard Data Privacy Lab, 1998.

Farhad Farokhi is a Research Scientist at the Information Security and Privacy Group at CSIRO's Data61 and a Research Fellow at the Department of Electrical and Electronic Engineering at the University of Melbourne. In 2014, he received his PhD degree in Automatic Control from KTH Royal Institute of Technology, Sweden. During his PhD studies, he was a visiting researcher at the University of California at Berkeley and the University of Illinois at Urbana-Champaign. Farhad has been the recipient of the VESKI Victoria Fellowship from the Victorian State Government as well as the McKenzie Fellow and the 2015 Early Career Researcher Award from the University of Melbourne. He was a finalist in the 2014 European Embedded Control Institute (EECI) PhD Award. His research interests include security and privacy in cyber-physical systems, such as smart grids and intelligent transportation systems.