TRANSACTIONS ON DATA PRIVACY 6 (2013) 185–198

Semantic Security: Privacy Definitions Revisited

Jinfei Liu*, **Li Xiong***, **Jun Luo****

*Department of Mathematics & Computer Science, Emory University, Atlanta, USA

**Huawei Noah's Ark Laboratory, HongKong & Shenzhen Institutes of Advanced Technology, Chinese Academy of Sciences, China

E-mail: jinfei.liu@emory.edu, lxiong@mathcs.emory.edu, jun.luo@siat.ac.cn

Abstract. In this paper* we illustrate a privacy framework named Indistinguishable† Privacy. Indistinguishable privacy could be deemed as the formalization of the existing privacy definitions in privacy preserving data publishing as well as secure multi-party computation. We introduce three representative privacy notions in the literature, Bayes-optimal privacy for privacy preserving data publishing, differential privacy for statistical data release, and privacy w.r.t. semi-honest behavior in the secure multi-party computation setting, and prove they are equivalent. To the best of our knowledge, this is the first work that illustrates the relationships of these privacy definitions and unifies them through one framework.

Keywords. K-Anonymity, Bayes-optimal Privacy, Differential Privacy, Secure Multi-party Computation, Privacy w.r.t. Semi-honest Behavior, Indistinguishable Privacy

1 Introduction

In an age where the details of our life are recorded and stored in databases, a clear paradox is emerging between the need to preserve the privacy of individuals and the need to use these collected data for research or other purposes. Privacy preserving data analysis and publishing (PPDP) has received considerable attention in recent years [10, 8]. The goal is for a data custodian to release some views or statistical computations of the original private data, so that the released data remains practically useful while individual privacy for the data subjects is preserved. A related problem is secure multi-party computation (SMC) where a given number of participants wish to compute a public function on their private inputs without disclosing the private inputs to each other. With decades' development, there are three essential privacy principles in the literature on PPDP and SMC: Bayes-optimal privacy [29] in the PPDP setting, differential privacy [6] in the PPDP setting, and privacy w.r.t. semi-honest behavior [14] in the SMC setting.

L. Sweeney [38] [37] introduced the well-known k-anonymity principle. It is a syntactic property on anonymized databases: if only certain attributes known as quasi-identifiers

* Preliminary version of this paper in the Proceedings of the 2013 Joint EDBT/ICDT Workshops [28]

† We note that this notion came from [13] first and was developed further in [9].

(QIDs) are considered, each instance in the anonymized database should appear at least k times. However, it is generally considered too weak. Many other derivative privacy principles have been introduced since then, e.g., l-diversity [29] and t-closeness [24]. A. Machanavajjhala et al. [29] studied that k-anonymity is susceptible to homogeneity an background knowledge attacks. To address this problem, they show the notion of Bayes-optimal privacy that provides privacy even when the data publisher does not know what kind of knowledge is possessed by the adversary.

The notion of differential privacy was introduced by C. Dwork et al. [6, 9]. An "algorithm" (or, "mechanism") $\mathcal{M}$ satisfies ϵ-differential privacy if and only if for two datasets D and D' which differ at only one instance, the distributions of $\mathcal{M}(D)$ and $\mathcal{M}(D')$ differ at most by a multiplicative factor of e^{ϵ}. A relaxed version of ϵ-differential privacy, which we use (ϵ, δ)-differential privacy to denote, allows an error probability bounded by δ. Satisfying differential privacy ensures that even if the adversary has full knowledge of the values of an instance t, as well as full knowledge of other instances in the dataset, and is only uncertain about whether t is in the input dataset, the adversary is unlikely to have precise information about the instance's presence in the database. Differential privacy is achieved by introducing randomness into query answers. The original algorithm for achieving differential privacy, commonly called the Laplace mechanism [9], returns the sum of the true answer and random noise drawn form a Laplace distribution. The scale of the distribution is determined by a property of the query called sensitivity: roughly the maximum possible change to the query answer induced by the addition or removal of one instance. Higher sensitivity queries are more likely to reveal individual instances and thus they should receive greater noise.

Yao first introduced the two parties comparison problem (Yao's Millionaire Problem), where two millionaires want to find out who is richer without disclosing their actual wealth, and developed a provably secure solution [42]. This was extended to multi-party computation by Goldreich et al. [15]. They developed a framework for secure multi-party computation (SMC), and proved that computing a function privately is equivalent to computing it securely in [14]. The protocol is *secure* if the parties learn only the result of the function and nothing else.

1.1 Contributions

While there are extensive literature based on each of the privacy definitions, few works studied their inter relationship. We believe it is important and significant to understand their relationships and the underlying principles that unify these definitions. The main contributions of this paper are as follows:

1. We present a privacy framework named indistinguishable privacy that could unify existing privacy definitions for privacy preserving data publishing and secure multi-party computation.

2. We introduce the representative privacy principles in the literature, Bayes-optimal privacy and differential privacy in privacy preserving data publishing setting and privacy w.r.t. semi-honest behavior in the secure multi-party computation setting - and prove they are equivalent.

3. We discuss the relationship of those state of the art privacy definitions related to differential privacy. The map of those definitions to Indistinguishable Privacy framework is also presented.

4. We also show that the indistinguishable Privacy framework satisfies the two privacy axioms.

The rest of the paper is organized as follows. Section 2 presents the new privacy framework, and analyzes the relationship of these three definitions in the literature. The existing state of the art privacy definitions related to differential privacy are discussed in Section 3. We prove indistinguishable privacy satisfies privacy axioms in Section 4. We review the related work in Section 5. Section 6 concludes the paper.

2 Indistinguishable Privacy

In this section, we illustrate our privacy framework *indistinguishable privacy*. We first discuss the underlying principle followed by the formal definition of the framework.

Let us briefly describe Shannon's definition of "perfect secrecy" [34]. Consider an adversary with unlimited time and manpower available for analysis of intercepted cryptograms. Let the set of all possible messages be finite. These messages have a priori probability for each and are encoded and sent across the wire. When an adversary intercepts an encoded message, he can calculate its posteriori probabilities for the various messages. Perfect secrecy is achieved if for all encoded messages the posteriori probabilities are equal to the priori probabilities. Thus intercepting the message gives the adversary no information.

Compare with "perfect secrecy" that provably can not be broken even with unlimited time and manpower available, semantic security (computationally secure) is theoretically possible to break but it is infeasible to do so by any known practical means. Due to the use of cryptography knowledge, SMC is based on semantic security. Hence, in this paper, our privacy framework definition also is based on semantic security.

Dalenius [4] defined a similar privacy goal for statistical database: access to the published data should not enable the attacker to learn anything extra about any target victim compared to no access to the database, even with the presence of any attacker's background knowledge obtained from other sources. The literature on privacy preserving data publishing has attempted to formalize Dalenius' goal or define similar notions for privacy. Machanavajjhala et al. defined a Bayes-optimal privacy notion for privacy preserving data publishing based on the uninformative principle (for published data).

Uninformative Principle [29]. The *published table* should provide the adversary with little additional information beyond the background knowledge. In other words, there should not be a large difference between the prior and posterior beliefs.

2.1 Notations and Privacy Principle

We define a formal indistinguishable privacy framework based on a generalized uninformative principle and show that it can be used to unify the privacy definitions for both PPDP and SMC. Given an operation of private data (e.g. a data release, a statistical computation, or a multi-party secure-computation), intercepting the operation knowledge should give an adversary no or little (ϵ) new information about sensitive knowledge in private data.

We first define the notations below.

Background Knowledge (BK) Background knowledge is what adversary obtained before one operation.

Sensitive Information (SI) Individual sensitive information is the information that needs to be protected, such as the salary or state of health of an individual.

Table 1: Summary of Notations and Mapping with Existing Privacy Definitions

Notation \ Definition	Bayes-optimal Privacy	Differential Privacy	Privacy w.r.t Semi-honest Behavior in SMC
Background Knowledge (BK)	Dataset that can be linked with the quasi-identifying attributes in the original dataset	D_{n-1} from D_n without i	own input and output
Sensitive Information (SI)	Each individual's sensitive attributes	instance i's sensitive information	Other party's private input and output
Operation Knowledge (OK)	Anonymized data	$\mathcal{M}(D_n)$, where D_n differs only in i from dataset D_{n-1}	Intermediate result received during communication with the other party

Operation Knowledge (OK) Operation knowledge is the knowledge that a participant will obtain after an operation. For example, it can be the published data after the operation of data release.

We redefine the uninformative principle with a generalization from published data to the operation knowledge as follows:

Uninformative Principle for Operations. The *operation knowledge* should provide the adversary with little *sensitive information* beyond the *background knowledge*. In other words, the prior and posterior beliefs should be *indistinguishable*.

2.2 Indistinguishable Privacy Definition

Consider an adversary Alice, we denote her prior belief about the sensitive information as:

$$\alpha_{(BK,SI)} = P(SI|BK)$$

After an operation is executed, Alice's posterior belief is:

$$\beta_{(BK,SI,OK)} = P(SI|BK,OK)$$

Definition 1. (Indistinguishable Privacy). An operation satisfies indistinguishable privacy if the following holds for an adversary with polynomially bounded resources available:

$$\alpha_{(BK,SI)} \leq e^{\epsilon}\beta_{(BK,SI,OK)} \quad (1)$$

The Inequation (1) indicates that before and after the operation, the difference between the prior and posterior beliefs of the adversary about the ***sensitive information*** (not the complete information) differs by no more than a very small fraction ϵ. ϵ can be considered as the disclosure. When ϵ is small, $ln(1+\epsilon) \approx \epsilon$.

Given the above definition, we can show that each of the three existing privacy definitions can be mapped to the indistinguishable privacy framework. Table 1 shows a summary of the mapping.

Example 2. Bayes-optimal Privacy: Alice has background knowledge (BK), e.g. publicly available voter registration list, that can be used to link the quasi-identifying attributes in the datset and identify the individuals in order to compute the sensitive information (SI). After she obtains the published dataset (OK), she could compute the sensitive information (SI) based on both the background knowledge and the published data (BK, OK).

Example 3. Differential Privacy: Alice has background knowledge (BK), in the worst case, about all but one record in the database, which is considered as D_{n-1}. After she obtains the query answer (OK) from the dataset D_n which only differs from D_{n-1} by one record, she could be able to compute the sensitive information (SI) based on D_{n-1} and $\mathcal{M}(D_n)$ (BK, OK).

Example 4. Privacy w.r.t. Semi-honest Behavior in SMC: Alice has some knowledge (BK) to compute sensitive information (SI). After she receives intermediate result (OK) from the other party during the execution of the protocol, she could compute the sensitive information (SI) based on her own background knowledge and the intermediate result (BK, OK).

2.3 Relationships of Existing Privacy Definitions

We present three existing privacy definitions and show their equality in this subsection.

2.3.1 Bayes-Optimal Privacy

We present Bayes-optimal privacy [29] that bounds the differences between the prior and posterior beliefs.

Consider an original table T which contains a instance t about Bob. Let S denote the set of all sensitive attributes and Q denote the set of all nonsensitive attributes. Alice's prior belief about Bob's sensitive information is denoted as $\alpha_{(q,s)}$, where s is Bob's sensitive attribute values and q is his nonsensitive attribute values:

$$\alpha_{(q,s)} = P(t[S] = s | t[Q] = q)$$

After the anonymization operation, Alice observes the anonymized table T^*, her posterior belief about Bob's sensitive attribute is denoted as $\beta_{(q,s,T^*)}$:

$$\beta_{(q,s,T^*)} = P(t[S] = s | t[Q] = q \wedge \exists t^* \in T^*, t \to t^*).$$

Definition 5. (ϵ-Bayes-optimal privacy for anonymized data). The anonymized table T^* satisfies ϵ-adversarial privacy if the following holds:

$$\alpha_{(q,s)} \leq e^{\epsilon} \beta_{(q,s,T^*)}.$$

2.3.2 Differential Privacy

We present differential privacy based on [19].

Definition 6. (ϵ-differential privacy). A randomized mechanism $\mathcal{M}$ satisfies ϵ-differential privacy if for any pair of database instances D, D' and for any set S,

$$P(\mathcal{M}(D) \in S) \leq e^{\epsilon} P(\mathcal{M}(D') \in S)$$

2.3.3 Privacy w.r.t. Semi-honest Behavior in SMC

We present the privacy definition w.r.t. Semi-honest Behavior in SMC based on [13].

Definition 7. (ϵ-privacy w.r.t Semi-honest Behavior for SMC). For a function f, we say that $\prod$ privately computes one operation f if there exist probabilistic polynomial time algorithms, denoted S_1 and S_2 for any ϕ and φ, such that

$$P(\{S_1(x, f_1(x, y)) = \phi\}_{x,y\in\{0,1\}^*}) \leq e^{\epsilon} P(\{view_1^{\prod}(x, y) = \phi\}_{x,y\in\{0,1\}^*}), \quad (2)$$

$$P(\{S_2(y, f_2(x, y)) = \varphi\}_{x,y\in\{0,1\}^*}) \leq e^{\epsilon} P(\{view_2^{\prod}(x, y) = \varphi\}_{x,y\in\{0,1\}^*}), \quad (3)$$

where x and y are the input, $f(x, y)$ is the output. $f_1(x, y)$ (resp., $f_2(x, y)$) denotes the first (resp., second) element of $f(x, y)$. The view of the first (resp., second) party during an execution of $\prod$ on (x, y), denoted $view_1^{\prod}(x, y)$ (resp., $view_2^{\prod}(x, y)$). "$\leq e^{\epsilon}$" is equivalent to "$\stackrel{c}{\equiv}$" in [13].

2.3.4 Equivalence

Theorem 8. *The three definitions: ϵ-Bayes-optimal privacy for anonymized data, ϵ-differential privacy for a randomized algorithm, and ϵ-privacy w.r.t. semi-honest behavior for SMC, are equivalent.*

Proof. From Bayes-optimal privacy's viewpoint:

$$\alpha_{(q,s)} \leq e^{\epsilon}\beta_{(q,s,T^*)}$$

$$\Leftrightarrow P(t[S] = s|t[Q] = q) \leq e^{\epsilon} P(t[S] = s|t[Q] = q \wedge \exists t^* \in T^*, t \to t^*)$$

$$\Leftrightarrow \alpha_{(BK,SI)} \leq e^{\epsilon}\beta_{(BK,SI,OK)}$$

where $SI = (t[S] = s)$, $BK = (t[Q] = q)$, and $OK = (\exists t^* \in T^*, t \to t^*)$.

From differential privacy's viewpoint:

$$P(\mathcal{M}(D) \in S) \leq e^{\epsilon} P(\mathcal{M}(D') \in S)$$

$$\Leftrightarrow \alpha_{(BK,SI)} \leq e^{\epsilon}\beta_{(BK,SI,OK)}$$

where $SI = instance\ i's\ sensitive\ information$, $BK = D_{n-1}$, and $OK = \mathcal{M}(D_n = D_{n-1} + i)$.

From privacy w.r.t semi-honest behavior's viewpoint:

$$P(\{S_1(x, f_1(x, y)) = \phi\}_{x,y\in\{0,1\}^*})$$

$$\leq e^{\epsilon} P(\{view_1^{\prod}(x, y) = \phi\}_{x,y\in\{0,1\}^*}),$$

$$\Leftrightarrow \alpha_{(BK,SI)} \leq e^{\epsilon}\beta_{(BK,SI,OK)}$$

where $SI = (y, f_2(x, y))$, $BK = (S_1(x, f_1(x, y)))$ and $OK = (view_1^{\prod}(x, y))$. Similarly, Inequation (3) satisfies the constraint.

Summing up the above, the theorem is correct. □

3 The State of the Art Privacy Definitions

In this section, we survey the existing state of the art privacy definitions. Furthermore, we show Indistinguishable Privacy Framework also could be deemed as the formalization of those privacy definitions. In addition, we discuss the relationship between free-lunch privacy, zero-knowledge privacy, differential privacy, and crowd-blending privacy.

3.1 Free-Lunch Privacy

D. Kifer et al. [19] addressed several popular misconceptions about differential privacy. They showed that, without further assumptions about the data, its privacy guarantees can degrade when applied to social networks or when deterministic statistics have been previously released. They presented a stricter privacy definition - free-lunch privacy.

Definition 9. (Free-Lunch Privacy)[19].
A randomized mechanism $\mathcal{M}$ satisfies ϵ-free-lunch privacy if for any pair of database instances D, D' (not just those differing in one instance) and for any set S,

$$P(\mathcal{M}(D) \in S) \leq e^{\epsilon} P(\mathcal{M}(D') \in S).$$

We show how to map free-lunch privacy to Indistinguishable Privacy framework.

$$P(\mathcal{M}(D) \in S) \leq e^{\epsilon} P(\mathcal{M}(D') \in S)$$

$$\Leftrightarrow \alpha_{(BK,SI)} \leq e^{\epsilon} \beta_{(BK,SI,OK)}$$

where $SI = instance\ i's\ sensitive\ information$, $BK = any\ subset\ D\ without\ i$, and $OK = \mathcal{M}(D')$. Free-lunch privacy guarantees any subset can simulate the view of whole database.

3.2 Zero-Knowledge Privacy

Let $\mathcal{D}$ be the class of all databases whose rows are instances from some relation/universe X. For convenience, we will assume that X contains a instance $\perp$, which can be used to conceal the true value of a row. Given a database D, let $|D|$ denote the number of rows in D. For any integer n, let $[n]$ denote the set $\{1, ..., n\}$. For any database $D \in \mathcal{D}$, any integer $i \in [|D|]$, and any $v \in X$, let D_{-i}, v denote the database D with row i replaced by the instance v. Let $\mathcal{M}$ be a mechanism that operates on database in $\mathcal{D}$. For any database $D \in \mathcal{D}$, any adversary A, and any $z \in \{0,1\}^*$, let $Out_A(A(z) \leftrightarrow \mathcal{M}(D))$ denote the random variable representing the output of A on input z after interacting with the mechanism $\mathcal{M}$ operating on the database D. J. Gehrke et al. [12] presented the Zero-Knowledge Privacy definition as follows:

Definition 10. (Zero-Knowledge Privacy)[12]. We say that $\mathcal{M}$ is ϵ-zero-knowledge private with respect to Aggregate Information [12] if there exists a $T \in$ Aggregate Information such that for every adversary A, there existing a simulator S such that for every database $D \in X^n$, every $z \in \{0,1\}^*$, every integer $i \in [n]$, and every $W \subseteq \{0,1\}^*$, the following hold:

$$\bullet Pr[Out_A(A(z) \leftrightarrow \mathcal{M}(D)) \in W] \leq e^{\epsilon} Pr[S(z, T(D_{-i}, \perp), i, n) \in W]$$

$$\bullet Pr[S(z, T(D_{-i}, \perp), i, n) \in W] \leq e^{\epsilon} Pr[Out_A(A(z) \leftrightarrow \mathcal{M}(D)) \in W]$$

The probabilities are over the random coins of $\mathcal{M}$ and A, and T and S, respectively.

Roughly speaking, zero-knowledge privacy requires that whatever an adversary learns about an individual i can be simulated given just some "aggregate information" about the remaining individuals in the database. For example, this aggregate information could be k random samples of the remaining individuals in the database. If the aggregate information contains all individuals, zero-knowledge privacy collapses down to differential privacy, but for more restrictive classes of aggregate information, such as k random samples, where k is smaller than the number of individual in the database, zero-knowledge privacy is strictly

stronger, and provides stronger privacy guarantees in contexts where there is correlation between individuals. That is, zero-knowledge privacy definition is a variant of differential privacy definition.

We show how to map zero-knowledge privacy to Indistinguishable Privacy framework.

$$\epsilon - zero - knowledge\ privacy$$

$$\Leftrightarrow \alpha_{(BK,SI)} \leq e^{\epsilon}\beta_{(BK,SI,OK)}$$

where $SI = instance\ i's\ sensitive\ information$, $BK = any\ subset\ of\ n\ with\ k\ instances\ but\ i$, and $OK = \mathcal{M}(any\ subset\ of\ n\ with\ k\ instances)$. Zero-knowledge privacy guarantees any subset with k instances can simulate the view of whole database.

3.3 Crowd-Blending Privacy

In this subsection, we survey Crowd-Blending Privacy, a weaker version of zero-knowledge privacy. J. Gehrke et al. [11] proved crowd-blending privacy with "robust pre-sampling" equals to zero-knowledge privacy as well as differential privacy is the sufficient condition of crowd-blending privacy (differential privacy implies crowd-blending privacy).

Definition 11. (ϵ-blend in a crowd of k instances in D)[11]. Let D be any database. An individual $i \in D$ ϵ-blend in a crowd of k instances in D with respect to the mechanism $\mathcal{M}$ if $|\{i' \in D : i' \approx_{\epsilon,\mathcal{M}} i\}| \geq k$.

Intuitively, an individual $i \in D$ blends in a crowd of k instances in D if i is indistinguishable by $\mathcal{M}$ from at least $k-1$ other individuals in D. Note that by the definition of two individuals being indistinguishable by $\mathcal{M}$, $i \in D$ must be indistinguishable by $\mathcal{M}$ from each of these $k-1$ other individuals regardless of what the database is, as opposed to only when the database is D.

Definition 12. (Crowd-Blending Privacy)[11].

A mechanism $\mathcal{M}$ is (k, ϵ)-crowd-blending private if for every database D and every individual $i \in D$, either i ϵ-blends in a crowd of k instances in D, or $\mathcal{M}(D) \approx_{\epsilon} \mathcal{M}(D \setminus \{i\})$.

Crowd-blending privacy requires that for every individual i in the database, either i blends in a crowd of k instances in the database, or the mechanism essentially ignores individual i's data.

We show how to map crowd-blending privacy to Indistinguishable Privacy framework.

$$(k, \epsilon) - Crowd - Blending\ Privacy$$

$$\Leftrightarrow \alpha_{(BK,SI)} \leq e^{\epsilon}\beta_{(BK,SI,OK)}$$

where $SI = instance\ i's\ sensitive\ information$, $BK = particular\ subset\ of\ n\ with\ k-1\ instances$ and $OK = \mathcal{M}(particular\ subset\ of\ n\ with\ k-1\ instances+i)$. Crowd-blending privacy guarantees particular $k-1$ (i blends in a crowd of $k-1+i$ instances) instances can simulate the view of k instances.

3.4 Discussion

Generally speaking, free-lunch privacy requires any subset can simulate the view of whole database, zero-knowledge privacy requires any subset with k instances can simulate the view of whole database, differential privacy requires any subset with $n-1$ instances can simulate the view of whole database, crowd-blending privacy requires there exists particular $k-1$ instances can simulate the view of k instances. That is,

$$free-lunch\ privacy \succ zero-knowledge\ privacy$$

$$\succ differential\ privacy \succ crowd-blending\ privacy$$

where "$\succ$" means "stricter than".

3.5 Induced Neighbors Privacy

To account for prior deterministic data releases, D. Kifer and A. Machanavajjhala [19] [20] presented the Induced Neighbors Privacy.

Definition 13. (Induced Neighbors $\mathcal{N}_{\mathcal{Q}}$)[19].
Given a general constraint $\mathcal{Q}$, let $\mathcal{I}_{\mathcal{Q}}$ be the set of databases satisfying those constraints. Let D_a and D_b be two databases. Let n_{ab} be the smallest number of moves necessary to transform D_a into D_b and let $\{m_1, ..., m_{ab}\}$ be the set of those moves. We say that D_a and D_b are neighbors induced by $\mathcal{Q}$, denoted as $\mathcal{N}_{\mathcal{Q}}(D_a, D_b)$=true, if the following holds.
- $D_a \in \mathcal{I}_{\mathcal{Q}}$ and $D_b \in \mathcal{I}_{\mathcal{Q}}$.
- No subset of $\{m_1, ..., m_{ab}\}$ can transform D_a into some $D_c \in \mathcal{I}_{\mathcal{Q}}$.

Definition 14. (Induced Neighbors Privacy)[20]. An mechanism $\mathcal{M}$ satisfies induced neighbor privacy with constraint $\mathcal{Q}$, if for each output $w \in range(\mathcal{M})$ and for every pair D_a, D_b of neighbors induced by $\mathcal{Q}$, the following holds:

$$P(\mathcal{M}(D_a) = w) \leq e^{\epsilon} P(\mathcal{M}(D_b) = w)$$

We show how to map induced neighbors privacy to Indistinguishable Privacy framework.

$$P(\mathcal{M}(D_a) = w) \leq e^{\epsilon} P(\mathcal{M}(D_b) = w)$$

$$\Leftrightarrow \alpha_{(BK,SI)} \leq e^{\epsilon} \beta_{(BK,SI,OK)}$$

where $SI = instance\ i's\ sensitive\ information$, $BK = D_a$ and $OK = \mathcal{M}(D_b)$. Induced neighbor privacy guarantees any subset D can simulate the view of instance that different from its induced neighbors.

4 Privacy Axioms

Modern design guidelines for privacy definitions include two fundamental axioms known as transformation invariance and convexity [18]. While the ideas contained in the axioms have been accepted by the privacy community for a long time, only recently there has been an insistence that privacy definitions should satisfy them.

In this section we show indistinguishable privacy framework satisfies both fundamental axioms, thus ensuring that it satisfies modern design guidelines.

The axioms are:

Axiom 15. *(Transformation Invariance [18]). If an algorithm $\mathcal{M}$ satisfies a privacy definition and $\mathcal{A}$ is any algorithm such that (1) its domain contains the range of M and (2) its random bits (if any) are statistically independent from the random bits (if any) of $\mathcal{M}$, then the algorithm $\mathcal{A} \circ \mathcal{M}$, which first runs M on the data and then runs A on the output should also satisfy the same privacy definition.*

Axiom 16. *(Convexity [18]). If $\mathcal{M}_1$ and $\mathcal{M}_2$ both satisfy a privacy definition, and $p \in [0, 1]$, then the algorithm $\mathcal{M}^p$ which runs $\mathcal{M}_1$ with probability p and $\mathcal{M}_2$ with probability $1 - p$ should also satisfy the privacy definition.*

The following theorem confirms that the indistinguishable privacy framework satisfies modern privacy design guidelines.

Theorem 17. *Indistinguishable privacy satisfies the axioms of convexity and transformation invariance.*

Proof. Let $\mathcal{M}$ be an algorithm that satisfies indistinguishable privacy, for any s we have:

$$P(SI = s|BK) \leq e^{\epsilon} P(SI = s|BK, OK(\mathcal{M}))$$

where $OK(\mathcal{M})$, the operation knowledge of $\mathcal{M}$, is what you obtain after the operation $\mathcal{M}$.

Step 1: First we prove it satisfies the axiom of transformation invariance. Let $\mathcal{A}$ be any algorithm whose domain contains the range of $\mathcal{M}$ and whose random bits are independent from those of $\mathcal{M}$.

$$\begin{aligned} P(SI = s|BK) &\leq e^{\epsilon} P(SI = s|BK, OK(\mathcal{M})) \\ &= e^{\epsilon} \frac{P(SI = s, BK, OK(\mathcal{M}))}{P(BK, OK(\mathcal{M}))} \\ &= e^{\epsilon} \frac{P(SI = s, BK, OK(\mathcal{M})) \times P(OK(\mathcal{A} \circ \mathcal{M}))}{P(BK, OK(\mathcal{M})) \times P(OK(\mathcal{A} \circ \mathcal{M}))} \\ &= e^{\epsilon} \frac{P(SI = s, BK, OK(\mathcal{A} \circ \mathcal{M}), OK(\mathcal{M}))}{P(BK, OK(\mathcal{A} \circ \mathcal{M}), OK(\mathcal{M}))} \\ &= e^{\epsilon} P(SI = s|BK, OK(\mathcal{A} \circ \mathcal{M}), OK(\mathcal{M})) \end{aligned}$$

Thus $\mathcal{A} \circ \mathcal{M}$ also satisfies the privacy definition.

Step 2: Now we prove that it satisfies that axiom of convexity. Let $\mathcal{M}_1$ and $\mathcal{M}_2$ be algorithms that satisfy the axiom of convexity. Let $\mathcal{M}_1$ and $\mathcal{M}_2$ be algorithms that satisfy the privacy definition indistinguishable privacy, let $p \in [0, 1]$ and let $\mathcal{M}^p$ be the algorithm that runs $\mathcal{M}_1$ with probability p and $\mathcal{M}_2$ with probability $1 - p$.

$$\begin{aligned} &P(SI = s|BK) \\ &= pP(SI = s|BK) + (1 - p)P(SI = s|BK) \\ &\leq e^{\epsilon} pP(SI = s|BK, OK(\mathcal{M}_1)) + e^{\epsilon}(1 - p)P(BK, OK(\mathcal{M}_2)) \\ &= e^{\epsilon} P(SI = s|BK, OK(\mathcal{M}^p)) \end{aligned}$$

Thus $\mathcal{M}^p$ also satisfies the privacy definition. □

5 Related Work

In a k-anonymized dataset, each record is *indistinguishable* from at least $k-1$ other records with respect to certain identifying attributes. Some follow-up notions include l-diversity [29], which requires that the distribution of a sensitive attribute in each equivalence class has at least l "well represented" values. l-diversity is based on the Bayes-optimal privacy which involves modeling background knowledge as a probability distribution over the attributes and uses Bayesian inference techniques to reason about privacy. t-closeness [24], which requires that the distribution of a sensitive attribute in any equivalent class is close to the distribution of the attribute in the overall table. A series [23] [35] [1] [36] [40] of papers based on k-anonymity are presented. For a detailed survey, please see [10].

The principle of differential privacy was developed in a series of works [6] [9] [2] [22] [19] [5] [3] [41] [16]. Differential privacy requires that computations be insensitive to changes in any particular individual's record, thereby restricting data leaks through the results. It represents a major breakthrough in privacy preserving data analysis. In an attempt to make differential privacy more amenable to more sensitive queries, several relaxations have been developed, including (ϵ, δ)-differential privacy [2] [9]. Three basic general approaches to achieve differential privacy add Laplace noise proportional to the query's global sensitivity [6] [9], adding noise related to the smooth bound of the query's local sensitivity [32], and the exponential mechanism to select a result among all possible results [31]. A survey on these results can be found in [7].

Secure two party computation was first investigated by Yao [42], and was later generalized to multi-party computation in [13] [14]. The basic problem is Yao's Millionaires' problem that two millionaires would like to know who is richer, but neither wants to reveal their real worth. Abstractly, the problem is simply comparing two numbers, each held by one party,however, without either party revealing its number to the other. Yao presented a solution for any efficiently computable function restricted to two parties and semi-honest adversaries. Goldreich first [14] introduced the privacy w.r.t semi-honest behavior. Due to the inefficiency of generic protocols, some research has focused on finding efficient protocols for specific problem of secure computation. See privacy preserving SVM [26], privacy preserving DBSCAN [27], and privacy preserving k-means [39] [17] for just a few examples.

The work closest to ours are V. Rastogi et al. [33], A. McGregor et al. [30], and N. Li et al. [25]. [33] has the original equivalent result on adversarial privacy and differential privacy, which is of independent interest: an algorithm is ϵ-indistinguishable if and only if it is private for a particular class of adversaries. [30] demonstrates a connection between differential privacy and deterministic extraction from Santha-Vazirani sources. [25] uses the random sampling step to bridge the gap between k-anonymity and differential privacy. D. Kifer et al. [21] introduced a rigorous and customizable framework for privacy which is the most closest work to ours. The main difference between our paper and others is that we consider the privacy w.r.t. semi-honest behavior while others' work like D. Kifer et al. only consider the k-anonymity and differential privacy. We prove that Bayes-optimal privacy, differential privacy are similar with privacy w.r.t. semi-honest behavior which is the original idea (three definitions in our paper).

6 Conclusions and Discussions

In this paper, we illustrate a new privacy framework named indistinguishable privacy and introduce Bayes-optimal privacy, differential privacy and privacy w.r.t. semi-honest behav-

ior, and prove they are equivalent. This is the first work to unify the existing definitions: Bayes-optimal privacy, differential privacy and privacy w.r.t. semi-honest behavior into one framework.

We also note that this is only a first step towards unifying the distinct privacy notions and many challenging issues remain to be solved. While the framework allows the framing of similar sets of equations for each of the privacy definition, it is also important to devise ways to capture numerically the various parameters. For instance, finding expressions to represent the background knowledge BK in the context of k-anonymity or syntactic privacy is itself a challenging issue. We hope there will be more work in this direction from the community that help us understand the foundations of the privacy definitions.

7 Acknowledgments

This research has been partially supported by the NSF under grant CNS-1117763 and NSF of China under project 11271351.

References

[1] M. M. Baig, J. Li, J. Liu, and H. Wang. Cloning for privacy protection in multiple independent data publications. In *CIKM*, pages 885–894, 2011.

[2] A. Blum, C. Dwork, F. McSherry, and K. Nissim. Practical privacy: the sulq framework. In *PODS*, pages 128–138, 2005.

[3] R. Chen, N. Mohammed, B. C. M. Fung, B. C. Desai, and L. Xiong. Publishing set-valued data via differential privacy. *PVLDB*, 4(11):1087–1098, 2011.

[4] T. Dalenius. Towards a methodology for statistical disclosure control. *Statistik Tidskrift*, (15), 1977.

[5] B. Ding, M. Winslett, J. Han, and Z. Li. Differentially private data cubes: optimizing noise sources and consistency. In *SIGMOD Conference*, pages 217–228, 2011.

[6] C. Dwork. Differential privacy. In *ICALP (2)*, pages 1–12, 2006.

[7] C. Dwork. Differential privacy: A survey of results. In *TAMC*, pages 1–19, 2008.

[8] C. Dwork. A firm foundation for private data analysis. *Commun. ACM*, 54(1):86–95, Jan. 2011.

[9] C. Dwork, F. McSherry, K. Nissim, and A. Smith. Calibrating noise to sensitivity in private data analysis. In *TCC*, pages 265–284, 2006.

[10] B. C. M. Fung, K. Wang, R. Chen, and P. S. Yu. Privacy-preserving data publishing: A survey of recent developments. *ACM Comput. Surv.*, 42(4), 2010.

[11] J. Gehrke, M. Hay, E. Lui, and R. Pass. Crowd-blending privacy. In *CRYPTO*, pages 479–496, 2012.

[12] J. Gehrke, E. Lui, and R. Pass. Towards privacy for social networks: A zero-knowledge based definition of privacy. In *TCC*, pages 432–449, 2011.

[13] O. Goldreich. *Secure Multi-party Computation (working draft)*. 1998.

[14] O. Goldreich. *The Foundations of Cryptography - Volume 2, Basic Applications*. Cambridge University Press, 2004.

[15] O. Goldreich, S. Micali, and A. Wigderson. How to play any mental game or a completeness theorem for protocols with honest majority. In *STOC*, pages 218–229, 1987.

[16] A. Inan, M. Kantarcioglu, G. Ghinita, and E. Bertino. Private record matching using differential privacy. In *EDBT*, pages 123–134, 2010.

[17] G. Jagannathan and R. N. Wright. Privacy-preserving distributed k-means clustering over arbitrarily partitioned data. In *KDD*, pages 593–599, 2005.

[18] D. Kifer and B. Lin. An axiomatic view of statistical privacy and utility. *Journal of Privacy and Confidentiality*, 4(1):2, 2012.

[19] D. Kifer and A. Machanavajjhala. No free lunch in data privacy. In *SIGMOD Conference*, pages 193–204, 2011.

[20] D. Kifer and A. Machanavajjhala. A rigorous and customizable framework for privacy. In *PODS*, pages 77–88, 2012.

[21] D. Kifer and A. Machanavajjhala. A rigorous and customizable framework for privacy. In *Proceedings of the 31st symposium on Principles of Database Systems*, pages 77–88. ACM, 2012.

[22] C. Li, M. Hay, V. Rastogi, G. Miklau, and A. McGregor. Optimizing linear counting queries under differential privacy. In *PODS*, pages 123–134, 2010.

[23] J. Li, R. C.-W. Wong, A. W.-C. Fu, and J. Pei. Anonymization by local recoding in data with attribute hierarchical taxonomies. *IEEE Trans. Knowl. Data Eng.*, 20(9):1181–1194, 2008.

[24] N. Li, T. Li, and S. Venkatasubramanian. t-closeness: Privacy beyond k-anonymity and l-diversity. In *ICDE*, pages 106–115, 2007.

[25] N. Li, W. H. Qardaji, and D. Su. Provably private data anonymization: Or, k-anonymity meets differential privacy. *CoRR*, abs/1101.2604, 2011.

[26] K.-P. Lin and M.-S. Chen. Privacy-preserving outsourcing support vector machines with random transformation. In *KDD*, pages 363–372, 2010.

[27] J. Liu, J. Z. Huang, J. Luo, and L. Xiong. Privacy preserving distributed dbscan clustering. In *EDBT/ICDT Workshops*, pages 177–185, 2012.

[28] J. Liu, L. Xiong, and J. Luo. A privacy framework: indistinguishable privacy. In *EDBT/ICDT Workshops*, pages 131–136, 2013.

[29] A. Machanavajjhala, D. Kifer, J. Gehrke, and M. Venkitasubramaniam. l-diversity: Privacy beyond k-anonymity. *TKDD*, 1(1), 2007.

[30] A. McGregor, I. Mironov, T. Pitassi, O. Reingold, K. Talwar, and S. P. Vadhan. The limits of two-party differential privacy. In *FOCS*, pages 81–90, 2010.

[31] F. McSherry and K. Talwar. Mechanism design via differential privacy. In *FOCS*, pages 94–103, 2007.

[32] K. Nissim, S. Raskhodnikova, and A. Smith. Smooth sensitivity and sampling in private data analysis. In *STOC*, pages 75–84, 2007.

[33] V. Rastogi, M. Hay, G. Miklau, and D. Suciu. Relationship privacy: output perturbation for queries with joins. In *PODS*, pages 107–116, 2009.

[34] C. Shannon. Communication theory of secrecy systems. *Bell system technical journal*, 28(4):656–715, 1949.

[35] P. Shi, L. Xiong, and B. C. M. Fung. Anonymizing data with quasi-sensitive attribute values. In *CIKM*, pages 1389–1392, 2010.

[36] X. Sun, H. Wang, J. Li, and J. Pei. Publishing anonymous survey rating data. *Data Min. Knowl. Discov.*, 23(3):379–406, 2011.

[37] L. Sweeney. Achieving k-anonymity privacy protection using generalization and suppression. *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*, 10(5):571–588, 2002.

[38] L. Sweeney. k-anonymity: A model for protecting privacy. *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*, 10(5):557–570, 2002.

[39] J. Vaidya and C. Clifton. Privacy-preserving k-means clustering over vertically partitioned data. In *KDD*, pages 206–215, 2003.

[40] R. C.-W. Wong, J. Li, A. W.-C. Fu, and K. Wang. (*alpha*, *k*)-anonymous data publishing. *J. Intell.*

Inf. Syst., 33(2):209–234, 2009.

[41] X. Xiao, G. Wang, and J. Gehrke. Differential privacy via wavelet transforms. In *ICDE*, pages 225–236, 2010.

[42] A. C.-C. Yao. How to generate and exchange secrets (extended abstract). In *FOCS*, pages 162–167, 1986.