Abstract—we present a comprehensive view of the relations among several privacy notions: differential privacy (DP) \[1\], Bayesian differential privacy (BDP) \[2\], semantic privacy (SP) \[3\], and membership privacy (MP) \[4\]. The results are organized into two parts. In part one, we extend the notion of semantic privacy (SP) to Bayesian semantic privacy (BSP) and show its essential equivalence with Bayesian differential privacy (BDP) in the quantitative sense. We prove the relations between BDP, BSP, and SP as follows: \( \epsilon \text{-BDP} \Leftrightarrow (\epsilon - \text{BDP}_{\text{SP}}) \), which improves the result of Kasiviswanathan and Smith \[3\] stating \( \epsilon \text{-DP} \Leftrightarrow \epsilon / 6 \text{-SP} \) for \( \epsilon \leq 1.35 \).

In part two, we establish the relations between BDP and MP. First, \( \text{BDP} \Rightarrow \epsilon \text{-MP} \). Second, for a family of distributions that are downward scalable in the sense of Li et al. \[4\], it is shown that \( \text{BDP} \Rightarrow \epsilon \text{-MP} \).

Key words—differential privacy, Bayesian differential privacy, semantic privacy, membership privacy.

I. INTRODUCTION

Differential privacy (DP). Differential privacy by Dwork et al. \[1\], \[5\] is a robust privacy standard that has been successfully applied to a range of data analysis tasks, since it provides a rigorous foundation for defining and preserving privacy. Differential privacy has received considerable attention in the literature \[6\]–\[15\]. Apple has incorporated differential privacy into its mobile operating system iOS 10 \[16\]. Google has implemented a differentially private tool called RAPPOR in the Chrome browser to collect information about clients \[17\].

A randomized algorithm \( Y \) satisfies \( \epsilon \)-differential privacy if for all adjacent databases \( x \) and \( x' \), it holds that \( \Pr[Y(x) \in E] \leq e^\epsilon \Pr[Y(x') \in E] \), where \( \Pr[\cdot] \) denotes the probability throughout this paper. Intuitively, under differential privacy, an adversary given access to the output do not have much confidence to determine whether it was sampled from the probability distribution generated by the algorithm when the database is \( x \) or when the database is \( x' \).

Bayesian differential privacy (BDP). Yang et al. \[2\] introduce the notion of Bayesian differential privacy as follows. Bayesian differential privacy broadens the application scenarios of differential privacy when data records have dependencies. For a database \( x \) with \( n \) tuples, let \( i \in \{1,2,\ldots,n\} \) be a tuple index in the database and \( S \subseteq \{1,2,\ldots,n\} \setminus i \) be a tuple index set. An adversary denoted by \( A(i,S) \) knows the values of all tuples in \( S \) (denoted by \( x_S \)) and attempts to attack the value of tuple \( i \) (denoted by \( x_i \)). For a randomized perturbation mechanism \( Y = \Pr[y \in Y | x] \) on database \( x \), the Bayesian differential privacy leakage (BDPL) of \( Y \) with respect to the adversary \( A(i,S) \) is \( \text{BDPL}_A(Y) = \sup_{x,x',x_S} \epsilon \text{-IDP} \).

Semantic privacy (SP). Kasiviswanathan and Smith \[3\] propose a Bayesian formulation of semantic privacy, inspired by the following interpretation of differential privacy explained in \[1\]: Regardless of external formulation, an adversary with access to the sanitized database draws the same conclusions whether or not any individual data is included in the original database. The phrases “external knowledge” and “drawing conclusions” are formulated as follows in \[3\]. The external knowledge is modeled by a prior probability distribution \( b \) on \( D^n \), where \( b \) is short for “belief”, and databases are assumed to be vectors in \( D^n \) for some domain \( D \). Conclusions are captured via the corresponding posterior distribution: given a transcript \( y \), the adversary updates his belief \( b \) about the database \( x \) using Bayes’ rule to obtain a posterior \( \overline{b} \) as defined in \[1\]:

\[
\overline{b}[x|y] = \frac{\Pr[Y(x) = y|b[x]]}{\sum_z \Pr[Y(x) = y|b[z]]}.
\]

For the database \( x \), Kasiviswanathan and Smith \[3\] further define \( x_{-i} \) to be the same vector except that the record at position \( i \) has been replaced by some fixed, default value \( \bot \) in \( D \).

Kasiviswanathan and Smith \[3\] define \( n + 1 \) related games, numbered 0 through \( n \). In Game 0, the adversary interacts with \( Y(x) \). This is the interaction that actually takes place between the adversary and the randomized mechanism \( Y \). Hence, the distribution \( \overline{b}_0 \) is just the distribution \( \overline{b} \) as defined in \[1\]: i.e.,

\[
\overline{b}_0[x|y] = \frac{\Pr[Y(x) = y|b_0[x]]}{\sum_z \Pr[Y(x) = y|b_0[z]]}.
\]

In Game \( i \) (for \( 1 \leq i \leq n \)), the adversary interacts with \( Y(x_{-i}) \). Game \( i \) describes the hypothetical scenario where person \( i \)’s record is not used. In Game \( i \) (for \( 1 \leq i \leq n \)), given a transcript \( y \), the adversary updates his belief \( b \) about database \( x \) again using Bayes’ rule to obtain a posterior \( \overline{b}_i \) as follows:

\[
\overline{b}_i[x|y] = \frac{\Pr[Y(x_{-i}) = y|b_0[x]]}{\sum_z \Pr[Y(x_{-i}) = y|b_0[z]]}.
\]

Given a transcript \( y \), Kasiviswanathan and Smith \[3\] say that privacy has been breached if the adversary would draw different conclusions about the world and, in particular, about a person \( i \), depending on whether or not \( i \)’s data was used. To this end, Kasiviswanathan and Smith \[3\] formally define \( \epsilon \)-semantic privacy below, where the statistical difference \( SD(X,Y) \) between random variables \( X \) and \( Y \) on the same discrete space \( D \) is defined
by \( \text{SD}(X, Y) = \max_{x \in D} \left| \mathbb{P}[X = x] - \mathbb{P}[Y = x] \right| \). A randomized mechanism \( Y \) is said to be \( \epsilon \)-semantically private if for all belief distributions \( b \) on \( D^n \), for all possible transcripts \( y \), and for all \( i = 1, \ldots, n \), it holds that \( \text{SD}(b_i[\cdot|y], b_i[\cdot|y]) \leq \epsilon \).

**Membership privacy (MP).** Li et al. [4] propose membership privacy (MP) in consideration of the adversary’s prior beliefs. Let the adversary’s prior beliefs about the dataset be captured by a distribution \( D \). From the adversary’s point of view, the dataset is a random variable drawn according to the distribution \( D \). With \( x \) denoting the event that record \( x \) is not in the database, Li et al. [4] define membership privacy as follows. A mechanism \( Y \) achieves \( \epsilon \)-membership privacy under a family \( D \) of distributions, i.e., \( (\langle \mathcal{D}, \epsilon \rangle, \text{MP}) \), if and only if for any distribution \( D \in \mathcal{D} \) and for any record \( x_i \), any possible set \( Y \) for the output, we have \( \mathbb{P}_{D, Y}(x_i | Y) \leq e^\epsilon \mathbb{P}_D(x_i) \) and \( \mathbb{P}_{D, Y}(x_i | Y) \geq e^{-\epsilon} \mathbb{P}_D(x_i) \).

The rest of the paper is organized as follows. Section II presents the results on the relations among several privacy notions: differential privacy (DP), Bayesian differential privacy (BDP), semantic privacy (SP), and membership privacy (MP). We elaborate their proofs in Sections III. Section IV surveys related work, and Section V concludes the paper.

### II. The Results

Kasiviswanathan and Smith [3] introduce semantic privacy (SP) and show its essential equivalence with differential privacy (DP) in the quantitative sense (the notion of essential equivalence means \( \epsilon \)-DP \( \iff \) \( f(\epsilon) \)-SP and \( \epsilon \)-DP \( \implies \) \( g(\epsilon) \)-SP for some functions \( f \) and \( g \)). We extend their notion to Bayesian semantic privacy (BSP) and show its essential equivalence with Bayesian differential privacy (BDP) also in the quantitative sense. We prove the relations between BDP, BSP, and SP as follows:

(i) \( \epsilon \)-BDP \( \iff \) \( (\frac{1}{2} - \frac{1}{e^{\epsilon} + 1}) \)-BSP.

(ii) \( \epsilon \)-BDP \( \implies \) \( (e^{2\epsilon} - 1) \)-BSP \( \implies \) \( (e^{2\epsilon} - 1) \)-SP.

We prove results (i) and (ii) in Section III-A where we also obtain a minor result \( \epsilon \)-DP \( \iff \) \( (\frac{1}{2} - \frac{1}{e^{\epsilon} + 1}) \)-SP, which improves the result of Kasiviswanathan and Smith [3] stating \( \epsilon \)-DP \( \iff \) \( \epsilon / 6 \)-SP for \( \epsilon \leq 1.35 \).

Li et al. [4] propose membership privacy (MP), which is applicable to Bayesian data, in contrast to DP. However, no general algorithm has been proposed for this framework. We present the following relations between BDP and MP:

(iii) \( \epsilon \)-BDP \( \implies \) \( \epsilon \)-MP.

(iv) For a family of distributions that are downward scalable in the sense of Li et al. [4], \( \epsilon \)-BDP \( \iff \) \( \epsilon \)-MP (See [4] for the meaning of “downward scalable” distributions).

We prove results (iii) and (iv) in Section III-B.

### III. Proofs

#### A. Relations between our Bayesian differential privacy and Kasiviswanathan and Smith’s semantic privacy [3]

We extend the work of Kasiviswanathan and Smith [3] on semantic privacy to tackle the case of correlated tuples. Specifically, we will present Bayesian semantic privacy and prove that the notions of Bayesian differential privacy and Bayesian semantic privacy are essentially (i.e., quantitatively) equivalent (see Theorem 1 below). Our result resembles [3] Theorem 2.2, which shows that differential privacy and semantic privacy are essentially equivalent.

**Theorem 1.** \( \epsilon \)-Bayesian differential privacy implies \( (e^{2\epsilon} - 1) \)-Bayesian semantic privacy, and is implied by \( (\frac{1}{2} - \frac{1}{e^{\epsilon} + 1}) \)-Bayesian semantic privacy.

Theorem 1 is one of our novel results. The first part of Theorem 2 is obtained by Kasiviswanathan and Smith [3]. The second part of Theorem 2 improves the corresponding result of Kasiviswanathan and Smith [3], which states that \( \epsilon \)-differential privacy is implied by \( \epsilon / 6 \)-semantic privacy for \( \epsilon \leq 1.35 \). The improvement can be seen from \( \frac{1}{2} - \frac{1}{e^{\epsilon} + 1} > \epsilon / 6 \) for \( \epsilon \leq 1.35 \).

The rest of the discussion is organized as follows. We review semantic privacy and define Bayesian semantic privacy in Section III-A1. In Section III-A2, we recall Bayesian differential privacy. Finally, we prove the above Theorem 1 in Section III-A3. The proof of Theorem 2 is similar to that of Theorem 1.

1) **Reviewing semantic privacy and defining Bayesian semantic privacy:** In this section, we first review semantic privacy from Kasiviswanathan and Smith [3], before presenting Bayesian semantic privacy, which extends the notion of semantic privacy to address correlated tuples.

A review of Kasiviswanathan and Smith [3] for semantic privacy:

Kasiviswanathan and Smith [3] propose a Bayesian formulation of semantic privacy, inspired by the following interpretation of differential privacy explained in [1]: Regardless of external knowledge, an adversary with access to the sanitized database draws the same conclusions whether or not any individual data is included in the original database. The phrases “external knowledge” and “drawing conclusions” are formulated as follows in [3]. The external knowledge is modeled by a prior probability distribution \( b \) on \( D^n \), where \( b \) is short for “belief,” and databases are assumed to be vectors in \( D^n \) for some domain \( D \). Conclusions are captured via the corresponding posterior distribution: given a transcript \( y \), the adversary updates his belief \( b \) about the database.
For the database $x$, Kasiviswanathan and Smith [3] further define $x_i$ to be the same vector except that position $i$ has been replaced by some fixed, default value in $D$. Any valid value in $D$ will do for the default value. In addition, the default value can be understood as a special value (e.g., “no data”); see [3, Page 3–Footnote 2] for details. We will use $\perp$ whenever it is necessary to explicitly write out the default value.

Kasiviswanathan and Smith [3] define $n + 1$ related games, numbered $0$ through $n$. In Game $0$, the adversary interacts with $Y(x)$. This is the interaction that actually takes place between the adversary and the randomized mechanism $Y$. Hence, the distribution $\mathbb{P}_0$ is just the distribution $\mathbb{P}$ as defined in (1); i.e.,

$$
\mathbb{P}_0[x|y] = \mathbb{P}[x|y] = \frac{\mathbb{P}[Y(x) = y] b[x]}{\sum_z \mathbb{P}[Y(z) = y] b[z]}. 
$$ (2)

In Game $i$ (for $1 \leq i \leq n$), the adversary interacts with $Y(x_{i-1})$. Game $i$ describes the hypothetical scenario where person $i$’s record is not used. In Game $i$ (for $1 \leq i \leq n$), given a transcript $y$, the adversary updates his belief $b$ about database $x$ again using Bayes’ rule to obtain a posterior $\mathbb{P}$ as follows:

$$
\mathbb{P}[b_i|x_{i-1}] = \mathbb{P}[b|x_{i-1}] = \frac{\mathbb{P}[Y(x_{i-1}) = y] b[x]}{\sum_z \mathbb{P}[Y(z_{i-1}) = y] b[z]}. 
$$ (3)

Given a transcript $y$, Kasiviswanathan and Smith [3] say that privacy has been breached if the adversary would draw different conclusions about the world and, in particular, about a person $i$, depending on whether or not $i$’s data was used. To this end, Kasiviswanathan and Smith [3] formally define $\epsilon$-semantic privacy below, where the statistical difference $\text{SD}(X, Y)$ between probability distributions (or random variables) $X$ and $Y$ on a discrete space $D$ is defined by

$$
\text{SD}(X, Y) = \max_{S \subseteq D} \left| \mathbb{P}[X \in S] - \mathbb{P}[Y \in S] \right|.
$$

Definition 1 ($\epsilon$-Semantical Privacy by [3, Definition 2.1]). A randomized mechanism $Y$ is said to be $\epsilon$-semantically private if for all database distributions $b$ on $D^n$, for all possible transcripts $y$, and for all $i = 1, \ldots, n$:

$$
\text{SD}(\mathbb{P}_0[\cdot|y], \mathbb{P}_i[\cdot|y]) \leq \epsilon. 
$$ (4)

From (3) and (4), the above definition of $\epsilon$-semantic privacy requires the use of $x_{i-1}$, $x_i$ is obtained after we replace position $i$ at $x$ by the default value $\perp$. If the tuples are correlated, changing position $i$ at $x$ might also result in changing other positions at $x$. Hence, $\epsilon$-semantic privacy may not work well under correlated tuples. Given this, we next extend $\epsilon$-semantic privacy to address correlated tuples and present $\epsilon$-Bayesian semantic privacy.

---

[2] For simplicity, only discrete probability distributions are discussed. The results can be readily extended to the continuous case.

---

Extending semantic privacy to Bayesian semantic privacy to address correlated tuples:

As will become clear, our extension of semantic privacy to Bayesian semantic privacy is similar to the extension of differential privacy to Bayesian differential privacy.

We let a statistical database be $[X_1, X_2, \ldots, X_n]$, where $X_j$ for each $j \in \{1, 2, \ldots, n\}$ is a random variable. We also let $\mathcal{N}$ be $\{1, 2, \ldots, n\}$. Then we consider the databases $x$ and $z$ used in (1)–(3) above to be

$$
x = [X_1 = x_1, X_2 = x_2, \ldots, X_n = x_n] = [X_j = x_j : j \in \mathcal{N}], 
$$ (5)

and

$$
z = [X_1 = z_1, X_2 = z_2, \ldots, X_n = z_n] = [X_j = z_j : j \in \mathcal{N}]. 
$$ (6)

When the data tuples are correlated, the adversary may gain more advantage in inferring $x_i$ by using random variables $X_j|_{j \in \mathcal{S}}$’s instantiations $x_j|_{j \in \mathcal{S}}$, and random variables $X_j|_{j \notin \mathcal{S}}$ for computation instead of using instantiations $x_j|_{j \notin \mathcal{S}}$ only, where $\mathcal{S} \subseteq \mathcal{N} \setminus \{i\}$ (note that $\mathcal{S}$ can be an arbitrary subset of $\mathcal{N} \setminus \{i\}$). For notation convenience, we define $x_{i+S}$ and $z_{i+S}$ by

$$
x_{i+S} = [X_i = x_i, X_j = x_j : j \in \mathcal{S}], X_j : j \in \mathcal{N} \setminus \{i\} \setminus \mathcal{S}], 
$$ (7)

and

$$
z_{i+S} = [X_i = z_i, X_j = z_j : j \in \mathcal{S}], X_j : j \in \mathcal{N} \setminus \{i\} \setminus \mathcal{S}]. 
$$ (8)

From (5)–(8), if $\mathcal{S} = \mathcal{N} \setminus \{i\}$, then $x_{i+S}$ and $z_{i+S}$ reduce to databases $x$ and $z$, respectively.

Similar to the previous subsection, here we also let the adversary play $n + 1$ related games with the randomized mechanism $Y$, and define $\mathbb{P}_0, \mathbb{P}_1, \ldots, \mathbb{P}_n$ as detailed below. In Game $0$, the adversary interacts with $Y(x_{i+S})$. We generalize $x$ and $z$ in (2) to $x_{i+S}$ and $z_{i+S}$, so that (2) becomes

$$
\mathbb{P}_0[x_{i+S} | y] = \mathbb{P}[x_{i+S} | y] = \frac{\mathbb{P}[Y(x_{i+S}) = y] b[x_{i+S}]}{\sum_{z_{i+S}} \mathbb{P}[Y(z_{i+S}) = y] b[z_{i+S}].} 
$$ (9)

For clarity, we explain the beliefs in (9). From (7) and (8), $b[x_{i+S}]$ and $b[z_{i+S}]$ in (9) are given by

$$
b[x_{i+S}] = b[X_i = x_i, X_j = x_j : j \in \mathcal{S}], X_j : j \in \mathcal{N} \setminus \{i\} \setminus \mathcal{S}], 
$$ (10)

and

$$
b[z_{i+S}] = b[X_i = z_i, X_j = z_j : j \in \mathcal{S}], X_j : j \in \mathcal{N} \setminus \{i\} \setminus \mathcal{S}], 
$$ (11)
Similar to (10), from (7), \( \tilde{b}_0[x_{i+S} | y] \) is given by
\[
\tilde{b}_0[x_{i+S} | y] = \frac{\Pr [Y(x_{i+S}) = y | b_{x_{i+S}]} \sum_{i \in S} \Pr [Y(z_{i+S}) = y | b_{z_{i+S}]}}. \tag{15}
\]
The beliefs \( b_{x_{i+S} | y} \) and \( b_{z_{i+S} | y} \) in (15) are already interpreted as (10) and (11). For clarity, we further explain \( \tilde{b}_0[x_{i+S} | y] \) in (15). Similar to (12), from (7), \( \tilde{b}_i[x_{i+S} | y] \) is given by
\[
\tilde{b}_i[x_{i+S} | y] = \frac{\Pr [Y(x_{i+S}) = y | b_{x_{i+S}]} \sum_{i \in S} \Pr [Y(z_{i+S}) = y | b_{z_{i+S}]}}. \tag{16}
\]

With the above notation, we define \( \epsilon \)-Bayesian semantical privacy below, in a way similar to that of \( \epsilon \)-semantical privacy in Definition 1:

**Definition 2 (\( \epsilon \)-Bayesian Semantical Privacy).** A randomized mechanism \( Y \) is said to have \( \epsilon \)-Bayesian semantical privacy if for all belief distributions \( b \) on \( D^n \), for all possible transcripts \( y \), for all \( i = 1, \ldots, n \), and for all \( x_{i+S} \) and \( z_{i+S} \) defined in (7) and (8) with \( S \subseteq N \setminus \{i\} \):
\[
\text{SD}(\tilde{b}_0[x_{i+S} | y], \tilde{b}_i[x_{i+S} | y]) \leq \epsilon. \tag{17}
\]

To understand the beliefs \( \tilde{b}_0[x_{i+S} | y] \) and \( \tilde{b}_i[x_{i+S} | y] \) in (17), we use their interpretations in (12) and (16). In Definition 2 for \( \epsilon \)-Bayesian semantical privacy, we consider all possible \( S \subseteq N \setminus \{i\} \). In the hypothetical scenario where we consider \( S \) only as \( N \setminus \{i\} \) in Definition 2, Definition 2 would reduce to Definition 1 for \( \epsilon \)-semantical privacy.

2) Recalling Bayesian differential privacy: In this section, we recall Bayesian differential privacy and express its definition using some new notation.

With \( x_{i+S} \) defined in (7) (i.e., \( x_{i+S} = [X_i = x_i, X_j = x_j : j \in S, X_j : j \in N \setminus \{i\} \setminus S] \)), for notation convenience, we further define \( x'_{i+S} \) by
\[
x'_{i+S} = [X_i = x'_i, X_j = x_j : j \in S, X_j : j \in N \setminus \{i\} \setminus S]. \tag{18}
\]

Note that the only difference between \( x_{i+S} \) and \( x'_{i+S} \) is that the former has \( X_i = x_i \), while the latter enforces \( X_i = x'_i \). Then \( \epsilon \)-Bayesian differential privacy means
\[
\Pr [Y(x_{i+S}) = y] \leq \epsilon \Pr [Y(x'_{i+S}) = y]. \tag{19}
\]

3) Proving Theorem 1 on the relations between Bayesian differential privacy and Bayesian semantic privacy: Our Theorem 1 restated below presents the relations between Bayesian differential privacy and Bayesian semantic privacy.

**Theorem 1 (Restated).** \( \epsilon \)-Bayesian differential privacy implies \( (e^{\epsilon} - 1) \)-Bayesian semantic privacy, and is implied by \( \frac{1}{2} - \frac{\epsilon}{1 + \epsilon} \)-Bayesian semantic privacy.

Theorem 1 shows that the notions of Bayesian differential privacy and Bayesian semantic privacy are essentially equivalent (of course, the parameters should be set appropriately). The proof of Theorem 1 below is just an extension of the reasoning by Kasiviswanathan and Smith [3].

**Proof of Theorem 1** We show Theorem 1 in two parts below. We will use the following definition of point-wise \((\epsilon, 0)\)-indistinguishability from (3) Definition 3.2: Two discrete random variables \( X \) and \( Y \) are point-wise \((\epsilon, 0)\)-indistinguishable if it holds for a drawn from either \( X \) or \( Y \) that \( e^{-\epsilon} \Pr [Y = a] \leq \Pr [X = a] \leq e^{\epsilon} \Pr [Y = a]. \)

**Proving \( \epsilon \)-Bayesian differential privacy \( \implies \) \( (e^{\epsilon} - 1) \)-Bayesian semantic privacy:** To prove this part, we consider any database \( x \in D^n \). Let \( Y \) be an \( \epsilon/2 \)-Bayesian differentially private algorithm. Consider any belief distribution \( b \). Let the posterior distributions \( \tilde{b}_0[x_{i+S} | y] \) and \( \tilde{b}_i[x_{i+S} | y] \) for some fixed \( i \), \( S \) and \( y \) be defined in (9) and (15). From (19), \( \epsilon \)-Bayesian differential privacy implies that for every \( z_{i+S} \),
\[
e^{-\epsilon} \Pr [Y(z_{i+S}) = y] \leq \Pr [Y(z_{i+S}) = y] \leq e^{\epsilon} \Pr [Y(z_{i+S}) = y].
\]
These inequalities imply that the ratio of \( \tilde{b}_0[x_{i+S} | y] \) and \( \tilde{b}_i[x_{i+S} | y] \) (defined in (9) and (15)) is within \( e^{\pm 2\epsilon} \). Since these inequalities hold for every \( x_{i+S} \), we get:
\[
e^{-2\epsilon} \tilde{b}_i[x_{i+S} | y] \leq \tilde{b}_0[x_{i+S} | y] \leq e^{2\epsilon} \tilde{b}_i[x_{i+S} | y], \quad \forall x_{i+S}.
\]
This implies that the random variables \( \tilde{b}_0[x_{i+S} | y] \) and \( \tilde{b}_i[x_{i+S} | y] \) are point-wise \((2\epsilon, 0)\)-indistinguishable. Applying (3) Lemma 3.3-Property 5, we obtain \( \text{SD}(\tilde{b}_0[x_{i+S} | y], \tilde{b}_i[x_{i+S} | y]) \leq (e^{2\epsilon} - 1) \).

Repeating the above arguments for every belief distribution, for every \( i \), and for every \( y \), we thus show that the mechanism \( Y \) is \( (e^{2\epsilon} - 1) \)-Bayesian semantic private.
Since this relation holds for every pair of $(x_i, x_j)$, the dataset is a random variable drawn according to the distribution $D$. Fix a transcript $y$ and, by Definition $2$, $D$ and $D'$ have the same distribution if and only if for any distribution $D$ and any distribution $D'$ such that $D'$ is non-zero, $D'$ assigns probabilities in the interval $[1/2, 1/2 + \frac{1}{4\cdot1+x^2}]$ to each of $x_i$ and $x_j$. Working through Bayes’ rule shows that (note that $b(x_i, x_j) = b(x'_i, x'_j)$)

$$b(x_i, x_j) = \frac{P(y|x_i)}{P(y|x'_i)} = \frac{P(y|x_i)}{P(y|x'_i)} = e^\epsilon.$$ (20)

Since the bound in (20) holds for every $y$, $Y(x_i)$ and $Y(x'_i)$ are point-wise $(\epsilon, 0)$-indistinguishable. From [3, Lemma 3.3-Property 5], $Y(x_i)$ and $Y(x'_i)$ are $(\epsilon, 0)$-indistinguishable. Since this relation holds for every pair of $x_i$ and $x_j$, the mechanism $Y$ is $\epsilon$-Bayesian differentially private.

B. Relations between Bayesian differential privacy and membership privacy

The adversary may have prior beliefs about what the dataset is; this is captured by a distribution $D$. From the adversary’s point of view, the dataset is a random variable drawn according to the distribution $D$. With $\mathcal{D}_k$ denoting the event that record $x_i$ is not in the database, Li et al. [4] define membership privacy as follows, where we reuse some notation of Li et al. [4].

**Definition 3** (Li et al. [4]). A mechanism $Y$ achieves $\epsilon$-membership privacy under a family of distributions, i.e., $(\epsilon, \gamma)$-membership privacy, if and only if for any distribution $D \in \mathcal{D}$ and for any record $x_i$, any possible set $Y$ for the output, we have:

$$P_y[x_i \in Y] \leq e^\epsilon P_D[x_i]$$ (21)

and

$$P_y[y \in Y | x_i] \geq e^{-\epsilon} P_D[y | x_i].$$ (22)

We discuss the adversary model considered here. Let $D_{i,k}$ denote a distribution where $P[x_i, x_k] = p$ and $P[x'_i, x_k] = 1 - p$ for some $p$. Define $D_{\epsilon} \equiv \cup_{\epsilon \in (1,...,n)} D_{i,k}$. The adversary model will be captured by the family $D_{\epsilon}$ of distributions. For simplicity, we will refer to $(\mathcal{D}_\epsilon, \gamma)$-membership privacy as $\epsilon$-membership privacy.

1) From membership privacy to membership privacy:

**Theorem 3.** $\epsilon$-Bayesian differential privacy implies $\epsilon$-membership privacy.

**Lemma 1.** A mechanism $Y$ achieves $\epsilon$-membership privacy under a family of distributions, i.e., $(\mathcal{D}, \epsilon)$-MP, if and only if for any distribution $D \in \mathcal{D}$ that

$$P_D[Y | x_i] \leq \left\{ \begin{array}{ll}
1 - P_D[x_i], & \text{if } 0 \leq P_D[x_i] \leq \frac{1}{1+e^\epsilon}, \quad (23a) \\
\frac{P_D[x_i]}{e^\epsilon - P_D[x_i]}, & \text{if } \frac{1}{1+e^\epsilon} < P_D[x_i] \leq 1. \quad (23b)
\end{array} \right.$$ (23)

We will explain that Lemma 1 implies the following corollary, which will be used to show Theorem 3.

**Corollary 1.** A mechanism $Y$ achieves $\epsilon$-membership privacy under a family of distributions, i.e., $(\mathcal{D}, \epsilon)$-MP, if and only if for any distribution $D \in \mathcal{D}$ that

$$P_D[Y | x_i] \leq e^\epsilon.$$ (24)

**Proof of Theorem 3 using Corollary 1** Under distribution $D_{i,k}$ where $P[x_i, x_k] = p$ and $P[x'_i, x_k] = 1 - p$ for some $p$, we have

$$P_{D_{i,k}, Y}[y | x_i] = P[Y(x_i, x_k, X_K) \in Y],$$ (25)

Under $\epsilon$-Bayesian differential privacy, we have

$$P_{D_{i,k}, Y}[y | x_i] \leq e^\epsilon,$$ (26)

which along with (24) and (25) yields $P_{D_{i,k}, Y}[y | x_i] \leq e^\epsilon$, then $(\mathcal{D}_\epsilon, \epsilon)$-membership privacy (i.e., $\epsilon$-membership privacy) follows for $D_{\epsilon} \equiv \cup_{\epsilon \in (1,...,n)} D_{i,k}$.

**Proof of Corollary 1 using Lemma 1** Note that (23a) and (23b) in Lemma 1 can be written as $P_D[Y | x_i] \leq g(P_D[x_i])$, where $g(b)$ is a function defined as follows:

$$g(b) = \left\{ \begin{array}{ll}
\frac{1-b}{1+e^\epsilon}, & \text{if } 0 \leq b \leq \frac{1}{1+e^\epsilon}, \\
\frac{e^\epsilon - b}{e^\epsilon}, & \text{if } \frac{1}{1+e^\epsilon} < b \leq 1.
\end{array} \right.$$ (27)

The function $g(b)$ increases as $b$ increases for $0 \leq b \leq \frac{1}{1+e^\epsilon}$ and decreases as $b$ increases for $\frac{1}{1+e^\epsilon} < b \leq 1$. Hence, at $b = 0$ or $b = 1$, $g(b)$ takes its minimum $g(0) = g(1) = e^\epsilon$. Then $P_{D, Y}[y | x_i] \leq e^\epsilon$ implies $P_{D, Y}[y | x_i] \leq g(P_D[x_i])$ for any $P_D[x_i]$.

In view of this, we obtain Corollary 1 from Lemma 1.

---

1 We let $D_{i,k} = 1$ and $\frac{\text{non-zero}}{0} = \infty$ to address the degenerate cases.
Proof of Lemma 1. For simplicity, we define
\[ A \overset{\text{def}}{=} \frac{P_{D,Y}[Y \mid x_i]}{P_{D,Y}[Y \mid \bar{x}_i]}, \] (27)

Then the goal of Lemma 1 is to show the combination of (21) and (22) is equivalent to \( A \leq g(P_D[x_i]) \). Hence, we will establish Lemma 1 once proving the following three results:

\[ 1 - P_{D}[x_i] \geq A(e^{-\epsilon} - P_{D}[x_i]) \] (28)
\[ \text{and} \quad A \times P_{D}[x_i] + 1 - P_{D}[x_i] \leq e^{\epsilon} \] (29)

and
\[ A \times P_{D}[x_i] + 1 - P_{D}[x_i] \leq e^{\epsilon} \] (30)

Below we demonstrate (28), (29) and (30), respectively.

Proving (28):

By Bayes’ theorem, it holds that
\[ P_{D,Y}[x_i \mid Y] = \frac{P_{D,Y}[Y \mid x_i] P_{D}[x_i]}{P_{D,Y}[Y]} \] (31)

Given (31), we have
\[ 1 - P_{D}[x_i] \geq A(e^{-\epsilon} - P_{D}[x_i]) \] (32)
To prove (28), we express \( P_{D,Y}[Y] \) by the law of total probability, and find
\[ P_{D,Y}[Y] = P_{D,Y}[Y \mid x_i] P_{D}[x_i] + P_{D,Y}[Y \mid \bar{x}_i] P_{D}[\bar{x}_i] \] (33)

Applying (27) to (33), we obtain
\[ P_{D,Y}[Y] = P_{D,Y}[Y \mid x_i] \left( P_{D}[x_i] + A^{-1} \times P_{D}[\bar{x}_i] \right) \] (34)

Then it follows from (32) and (34) that
\[ 1 - P_{D}[x_i] \geq A(e^{-\epsilon} - P_{D}[x_i]) \] (35)

i.e., (28) is established.

Proving (29):

By Bayes’ theorem, it holds that
\[ P_{D,Y}[x_i \mid Y] = \frac{P_{D,Y}[Y \mid x_i] P_{D}[x_i]}{P_{D,Y}[Y]} \] (35)

Given (35), we have
\[ A \times P_{D}[x_i] + 1 - P_{D}[x_i] \leq e^{\epsilon} \] (36)

We recall (34). Applying (27) to (34), we obtain
\[ P_{D,Y}[Y] = A \times P_{D,Y}[Y \mid \bar{x}_i] \times \left( P_{D}[x_i] + A^{-1} \times P_{D}[\bar{x}_i] \right) \] (37)

Then it follows from (35) and (36) that
\[ P_{D}[x_i] + A^{-1} \times P_{D}[\bar{x}_i] \leq e^{\epsilon} \]
\[ \text{i.e., (29) is established.} \]

Proving (30):

With \( P_D[x_i] \) replaced by real \( x \in [0,1] \), (30) will follow once we show for \( x \in [0,1] \) that
\[ 1 - x \geq A(e^{-\epsilon} - x) \] (28)

and
\[ A \times x + 1 - x \leq e^{\epsilon} \] (29)

We first prove the “\( \Longrightarrow \)” part in (38). If \( 0 \leq x < e^{-\epsilon} \), we obtain from \( 1 - x \geq A(e^{-\epsilon} - x) \) that \( A \leq \frac{1-e^{-x}}{x} \). If \( 0 \leq x < 1 \), we obtain from \( A \times x + 1 - x \leq e^{\epsilon} \) that \( A \leq \frac{e^{x}-1+x}{x} \). With \( g_1(x) \) denoting \( \frac{1-e^{-x}}{x} \), we see that \( (g_1(x) \) is defined for \( 0 \leq x < \frac{1}{1+e^{-\epsilon}} \) and equals \( g_2(x) \) if \( \frac{1}{1+e^{-\epsilon}} < x \leq 1 \). Given the above, if \( 0 \leq x \leq \frac{1}{1+e^{-\epsilon}} \), we have \( A \leq g_1(x) = g(x) \), and if \( \frac{1}{1+e^{-\epsilon}} < x \leq 1 \), we have \( A \leq g_2(x) = g(x) \). Hence, the “\( \Longrightarrow \)” part in (38) immediately follows.

We then prove the “\( \Longleftarrow \)” part in (38). For any \( x \in [0,1] \), we will establish i) \( 1 - x \geq A(e^{-\epsilon} - x) \), and ii) \( A \times x + 1 - x \leq e^{\epsilon} \), respectively. We still use \( g_1(x) \) and \( g_2(x) \) defined above. Note that \( g_1(x) \) is only defined for \( 0 \leq x < e^{-\epsilon} \) and \( g_2(x) \) is only defined for \( 0 < x \leq 1 \). It is straightforward to show \( g_1(x) \leq g_2(x) \) if \( 0 \leq x < \frac{1}{1+e^{-\epsilon}} \), and \( g_1(x) \leq g_2(x) \) if \( \frac{1}{1+e^{-\epsilon}} < x \leq e^{-\epsilon} \).

i) If \( 0 \leq x \leq \frac{1}{1+e^{-\epsilon}} \), we obtain from \( A \leq g(x) = g_1(x) \) that \( A \leq \frac{1-e^{-x}}{x} \), implying \( 1 - x \geq A(e^{-\epsilon} - x) \). If \( \frac{1}{1+e^{-\epsilon}} < x < e^{-\epsilon} \), we obtain from \( A \leq g(x) = g_2(x) \) that \( A \leq \frac{e^{x}-1+x}{x} \), implying \( 1 - x \geq A(e^{-\epsilon} - x) \). If \( e^{-\epsilon} \leq x \leq 1 \), it holds that \( 1 - x \geq A(e^{-\epsilon} - x) \). To summarize, for any \( x \in [0,1] \), it follows that \( 1 - x \geq A(e^{-\epsilon} - x) \).

ii) If \( \frac{1}{1+e^{-\epsilon}} < x \leq 1 \), we obtain from \( A \leq g(x) = g_2(x) \) that \( A \leq \frac{e^{x}-1+x}{x} \), implying \( A \times x + 1 - x \leq e^{\epsilon} \). If \( 0 < x < \frac{1}{1+e^{-\epsilon}} \), we obtain from \( A \leq g(x) = g_1(x) \leq g_2(x) \) that \( A \leq \frac{e^{x}-1+x}{x} \), implying \( A \times x + 1 - x \leq e^{\epsilon} \). If \( x = 0 \), we have \( A \leq g(x) = g_1(x) \leq g_2(x) \), and if \( x \geq \frac{1}{1+e^{-\epsilon}} \), it follows that \( 1 - x \geq A(e^{-\epsilon} - x) \).

(38) is proved since its “\( \Longrightarrow \)” and “\( \Longleftarrow \)” both hold. 

2) From membership privacy to Bayesian differential privacy:

Theorem 4. For a family of distributions that are downward scalable in the sense of Li et al. [4], \( \epsilon \)-membership privacy implies \( \epsilon \)-Bayesian differential privacy.

Proof of Theorem 4. The proof is similar to that of [4] Theorem 3.6. For completeness, we still present the details below.

Assume, for the sake of contradiction, that mechanism \( Y \) achieves \( \epsilon \)-membership privacy yet does not satisfy \( \epsilon \)-Bayesian
differential privacy. Then there exists a distribution $D$ and entity $x_i$ such that $0 < P_D[x_i] < 1$ and $P_{D,Y}[Y|x_i] > e^\alpha P_{D,Y}[Y|x_i]$. We discuss two cases below.

Case one: $P_{D,Y}[Y|\bar{x}_i] = 0$ and $P_{D,Y}[Y|x_i] > 0$. Since $D$ is downward scalable, by definition $D$ contains some $D'$ which is $x_i$-scaled from $D$ such that $P_D[x_i] < e^{-\epsilon}$. From [4] Lemma 3.4, we have $P_{D',Y}[Y|\bar{x}_i] = P_{D,Y}[Y|\bar{x}_i]$, which with the case condition $P_{D,Y}[Y|\bar{x}_i] = 0$ means $P_{D,Y}[Y|\bar{x}_i] = 0$, further yielding $P_{D,Y}[x_i|Y] = 1$. Therefore, $P_{D,Y}[x_i|Y] = 1 > e^\alpha P_{D,Y}[x_i]$, which contradicts the fact that $Y$ achieves $\epsilon$-membership privacy.

Case two: $P_{D,Y}[Y|x_i] = \alpha P_{D,Y}[Y|\bar{x}_i]$, where $\alpha > e^\epsilon$. Since $D$ is downward scalable, by definition $D$ contains some $D'$ which is $x_i$-scaled from $D$ such that $P_D[x_i] = q$ for an arbitrarily small $q$ (see [4] for the meaning of “*-scaled”). From [4] Lemma 3.4, we have $P_{D',Y}[Y|x_i] = P_{D,Y}[Y|x_i]$ and $P_{D,Y}[Y|\bar{x}_i] = P_{D,Y}[Y|\bar{x}_i]$. These with the case condition $P_{D,Y}[Y|x_i] = \alpha P_{D,Y}[Y|\bar{x}_i]$ gives $P_{D',Y}[Y|x_i] = \alpha P_{D,Y}[Y|\bar{x}_i]$. Then, under $D'$, we have

$$\frac{P_{D',Y}[x_i|Y]}{P_{D',Y}[x_i]} = \frac{P_{D,Y}[Y|x_i]}{P_{D,Y'}[Y]} = \frac{P_{D,Y}[Y|x_i]}{\alpha P_{D,\bar{x}_i}[Y|\bar{x}_i]} = \frac{\alpha}{\alpha q + 1 - q}. \hspace{1cm} (39)$$

The above ratio $\frac{\alpha}{\alpha q + 1 - q}$ is greater than $e^\epsilon$ given $\alpha > e^\epsilon$, once we ensure $q < \frac{\alpha - e^\epsilon}{\epsilon(\alpha - 1)}$. This will give $P_{D',Y}[x_i|Y] > e^\epsilon P_{D,Y}[x_i]$, which contradicts the fact that $Y$ achieves $\epsilon$-membership privacy.

Summarizing the above two cases, we have proved the desired result.

IV. RELATED WORK

The notion of differential privacy (DP) [11, 5] provides a rigorous foundation for privacy protection. Intuitively, DP implies that changing one entry in the database does not significantly change the query output, so that an adversary, seeing the query output and knowing all records except the one to be inferred, draws almost the same conclusion on whether or not a record is in the database. Differential privacy has received considerable interest in the literature [17–26]. Yang et al. [2] and Liu et al. [27] propose Bayesian differential privacy and dependent differential privacy respectively to generalize differential privacy for correlated data. Kasiviswanathan and Smith [11] propose a Bayesian formulation of semantic privacy, inspired by the following interpretation of differential privacy explained in [11]: Regardless of external knowledge, an adversary with access to the sanitized database draws the same conclusions whether or not any individual data is included in the original database. To present the notion of semantic privacy, Kasiviswanathan and Smith model the external knowledge via a prior probability distribution, and model conclusions via the corresponding posterior distribution. Li et al. [4] introduce membership privacy (MP) in consideration of the adversary’s prior beliefs.

Dwork and Rothblum [28] recently proposed the notion of concentrated differential privacy, a relaxation of differential privacy achieving better accuracy than differential privacy without compromising on cumulative privacy cost over multiple computations. Motivated by [28], Bun and Steinke [29] suggest a relaxation of concentrated differential privacy. Instead of treating the privacy loss as a subgaussian random variable as [28] does, Bun and Steinke [29] instead formulate the problem in terms of Renyi entropy, giving a relaxation of concentrated differential privacy. Jorgensen et al. [30] introduce a new privacy definition called personalized differential privacy, a generalization of differential privacy in which users specify a personal privacy level for their data. They show that by accepting that not all users demand the same level of privacy, a higher level of utility can often be obtained by not providing excess privacy budget to those who do not need it. They present a mechanism for achieving personalized differential privacy, inspired by the well-known exponential mechanism of differential privacy. Hall et al. [31] introduce additional randomness to extend differential privacy to the notion of random differential privacy. Compared with differential privacy, Lee and Clifton [32] give an alternate formulation, differential identifiability, parameterized by the probability of individual identification. Their notion provides the strong privacy guarantees of differential privacy, while allowing policy makers to set parameters based on the privacy concept of individual identifiability.

Bohli and Andreas [33] discuss the relations among several privacy definitions, but the discussion does not cover differential privacy. Li et al. [34] present the relation between $k$-anonymization and differential privacy, where the $k$-anonymity notion by [35, 36] means that when only quasi-identifiers are considered, each record in a $k$-anonymized dataset should appear at least $k$ times. Wang et al. [37] analyze the relation between differential privacy, mutual-information privacy, and identifiability. Mironov et al. [38] present several relaxations of differential privacy by requiring privacy guarantees to hold only against computationally bounded adversaries. They establish various relations among these notions, and show that the notions exhibit close connection with the theory of pseudodense sets [39].

V. CONCLUSION

In this paper, we present a comprehensive view of the relations among different privacy notions: differential privacy (DP), Bayesian differential privacy (BDP), semantic privacy (SP), and membership privacy (MP). In particular, we extend the notion of semantic privacy (SP) to Bayesian semantic privacy (BSP) and prove its essential equivalence with Bayesian differential privacy (BDP) in the quantitative sense. We show the relations between BDP, BSP, and SP as follows: $\epsilon$-BDP $\iff (\epsilon^{-1} - \frac{1}{e})$-SP, and $\epsilon$-BDP $\iff (\epsilon^2 - 1)$-SP. Moreover, we derive the following relations between BDP and MP: First, $\epsilon$-BDP $\implies \epsilon$-MP. Second, for a family of...
distributions that are downward scalable in the sense of Li et al. [4], it holds that $\epsilon$-BDP $\iff$ $\epsilon$-MP.

**REFERENCES**

[1] 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.

[2] B. Yang, I. Sato, and H. Nakagawa, “Bayesian differential privacy on correlated data,” in *ACM SIGMOD International Conference on Management of Data (SIGMOD)*, 2015, pp. 747–762.

[3] J. Tang, A. Korolova, X. Bai, X. Wang, and X. Wang, “Privacy loss in Apple’s implementation of differential privacy,” in *IEEE Symposium on Foundations of Computer Science (FOCS)*, 2013, pp. 439–448.

[4] G. Acuña, L. Melis, C. Castelluccia, and E. De Cristofaro, “Differentially private mixtures of generative neural networks,” in *IEEE International Conference on Data Mining series (ICDM)*, 2017.

[5] J. Zhang, T. Yu, I. Khalil, X. Xiao, and K. Ren, “Heavy hitter estimation over set-valued data with local differential privacy,” in *ACM Conference on Computer and Communications Security (CCS)*, 2016, pp. 192–203.

[6] K. Jiang, D. Shao, S. Bressan, T. Kister, and K.-L. Tan, “Publishing trajectories with differential privacy guarantees,” in *International Conference on Scientific and Statistical Database Management (SSDBM)*, 2013, pp. 12:1–12:12.

[7] C. Dwork and A. Roth, “The algorithmic foundations of differential privacy: A Bayesian formulation,” *Journal of Privacy and Confidentiality*, vol. 6, no. 1, pp. 1–16, 2014.

[8] J. Zhang, X. Xiao, and X. Xie, “PrivTree: A differentially private algorithm for hierarchical decompositions,” in *ACM SIGMOD International Conference on Management of Data (SIGMOD)*, 2016, pp. 155–170.

[9] J. Zhang, G. Cormode, C. M. Procopiuc, D. Srivastava, and X. Xiao, “Private release of graph statistics using ladder functions,” in *ACM SIGMOD International Conference on Management of Data (SIGMOD)*, 2015, pp. 731–745.

[10] F. Tramèr, Z. Huang, J.-P. Huabux, and E. Ayday, “Differential privacy with bounded priors: Reconciling utility and privacy in genome-wide association studies,” in *ACM Conference on Computer and Communications Security (CCS)*, 2015, pp. 1286–1297.

[11] G. Erlingsson, V. Pihur, and A. Korolova, “RAPPOR: Randomized aggregated privacy-preserving ordinal response,” in *ACM Conference on Computer and Communications Security (CCS)*, 2014, pp. 1054–1067.

[12] R. Bassily, A. Groce, J. Katz, and A. Smith, “Coupled-worlds privacy: Exploiting adversarial uncertainty in statistical data privacy,” in *IEEE Symposium on Foundations of Computer Science (FOCS)*, 2013, pp. 439–448.