Information and Computation 254 (2017) 84–104

Contents lists available at ScienceDirect

Information and Computation

www.elsevier.com/locate/yinco

Differential privacy in probabilistic systems

Jiannan Yang, Yongzhi Cao *, Hanpin Wang

Key Laboratory of High Confidence Software Technologies (MOE), School of Electronics Engineering and Computer Science, Peking University, Beijing 100871, China

ARTICLE INFO

Article history:
Received 20 November 2015
Received in revised form 1 December 2016
Available online 22 March 2017

Keywords:
Differential privacy
Probabilistic system
Metric
Probabilistic bisimilarity
Logical characterization

ABSTRACT

Ever since proposed by Dwork, differential privacy has been a hot topic in academia. However, few attempts have been made on reasoning about differential privacy at a system level. In this paper, we propose a formal framework to verify differential privacy in probabilistic systems. With a metric on the states of a system, we formalize differential privacy by the ratio of the probabilities in the distributions after the same labeled transitions of relevant states. We explain how traditional differential privacy can be embedded in our framework and raise an infimum metric, the least distance between two states, while not violating differential privacy. It is proven that the infimum metric is also a metric instance of differential privacy itself. Furthermore, we propose a two-level logic, a privacy variant of the familiar Hennessy–Milner logic, to characterize differential privacy in our framework. Our results have close relations to probabilistic bisimilarity as well.

© 2017 Elsevier Inc. All rights reserved.

1. Introduction

There has always been a conflict divergence between data publishers and their adversaries. Therefore, it is a hot topic in academia to efficiently protect the privacy of the participants in a dataset, and meanwhile publish some useful information [1–4]. Many protocols have been proposed in the literature to protect sensitive information. Among them, differential privacy, proposed by Dwork in [5], has gained widespread attention in many fields of computer science [6]. It describes a promise made by a data publisher that an adversary cannot gain much information about a particular individual using the exposed information. Specifically, a randomized algorithm on a dataset satisfies differential privacy, when it returns a result that can be regarded probabilistically unchanged if the dataset increases or decreases by one element. Many papers on differential privacy have been published [6–8] and most of them focus on the tasks of designing an algorithm which satisfies differential privacy and analyzing the trade-offs between privacy and utility [9–12]. In particular, some discuss the applications of differential privacy in terms of location protection [13,14], social network [15,16], and cloud computing [17].

Remarkably, there exist some works in the field of differential privacy verification in systems. Reed et al. proposed a functional language with a type system that automatically guarantees differential privacy in [18]. This functional language can help the programmer to write complex privacy-safe programs in a flexible way. Gaboardi et al. extended this language with a combination of linear indexed types and lightweight dependent types in [19]. This combination allows a richer sensitivity analysis that is able to certify a larger class of queries. Tschantz et al. extended differential privacy into interactive systems modeled by a kind of probabilistic automata and introduced the notion of differential noninterference for probabilistic automata in [20]. In their settings, actions are separated into input and output actions; the former are further

* Corresponding author.
E-mail addresses: yjn19920627@pku.edu.cn (J. Yang), caoyz@pku.edu.cn (Y. Cao), whpxhy@pku.edu.cn (H. Wang).

http://dx.doi.org/10.1016/j.ic.2017.03.002
0890-5401/© 2017 Elsevier Inc. All rights reserved.

separated into data and query actions, while the latter are divided based on whether they can be observed by the data examiner. A probabilistic automaton has ϵ-differential noninterference if the ratio of probabilities that adjacent paths produce the same observable output is at most e^{ϵ}, where two paths are adjacent if their input labels differ in only one data label. Xu et al. examined differential privacy in concurrent systems with a model of probabilistic process algebra and probabilistic automata in [21,22]. They concerned with the probabilities of a given finite trace in adjacent probabilistic automata. Additionally, they proposed three different metrics to verify their differential privacy and compared these metrics, proving that the latter two metrics are indeed more permissive than the first one, but incomparable with each other.

In this paper, we propose a formal framework to verify differential privacy in the context of probabilistic systems. Probabilistic systems [23,24] are a kind of systems where system dynamics encode the probability of making a transition between states rather than just the existence of such a transition. The main motivation behind the employment of probabilities in our approach is the need for quantitative information, as opposed to qualitative information, when reasoning about the non-functional aspects of systems such as throughput and resource utilization [23]. We utilize the model of probabilistic labeled transition system (or simply pLTS), which admits both non-deterministic and probabilistic behavior. Furthermore, we suppose a preset metric on its states which expresses the viewpoint of an observer on the difference between its states. The metric is similar to the difference between datasets in the traditional differential privacy. The notion of differential privacy in our framework is defined in terms of the probability ratio in the distributions after the same labeled transitions of relevant states. We then explain how traditional differential privacy can be embedded in our framework and raise an infimum metric, the least distance possibly between two states, while not violating differential privacy. It is proven that the infimum metric is also a metric instance of differential privacy itself, so the work of characterizing differential privacy focuses on this metric. We propose a two-level logic, which is a privacy variant of the familiar HML logic [25], and proceed to construct an extension for each formula with privacy and distance parameters. We succeed to characterize differential privacy with this logic and show that it provides an approach to measuring the distance between states in the infimum metric logically. In addition, we examine a real case, an extended Crowds protocol with different behavior members. We model it with a pLTS and verify our notions of differential privacy and infimum metric in this pLTS.

As mentioned above, Xu et al. also introduced three metrics to verify differential privacy in concurrent systems [22]. Compared to their work, our work differs in two main aspects. (1) In our framework, we establish differential privacy on the behavior of the system when performing a single transition or step. We focus on the distinction of probabilities between transitions of relevant states. After the transition, the whole system is still under the same privacy parameter. However, Xu et al. built differential privacy upon traces. They studied the probabilities of different probabilistic automata performing the same trace. So, they adopted a notion of privacy leakage which may increase or decrease when performing a transition. (2) In our framework, the metric distance is affected by the privacy parameter. As pointed in our Proposition 3.2, different privacy parameters may lead to different metrics. So, we have to determine the privacy parameter first and deduce the infimum metric with the privacy parameter. However, the distance in their metric is independent of the privacy parameter and also a limit of the privacy parameter. Part of their main theorems state that the privacy parameter is no less than the distance in their metrics.

On the other hand, probabilistic bisimilarity is a classical theory and has been well studied in probabilistic systems. Our work has a close relation to it; for example, the distance between two states in the infimum metric is 0 iff they are probabilistic bisimilar. Thus, our infimum metric can be considered to measure the difference between the equivalence classes of probabilistic bisimilarity. We notice that Desharnais et al. did some work on metric extensions of probabilistic bisimilarity [26–28]. The distance between two states in their metric is 0 iff they are probabilistic bisimilar. As a result, it is also equivalent to that the distance in our infimum metric is 0. The essential distinction between these two metrics is that our infimum metric originates from verification of differential privacy in probabilistic systems, which is a different view from their metrics. In addition, we focus on the quotients of probabilities in distributions, rather than the differences in their settings. However, further research is needed regarding the deeper and more specific relations between the two metrics.

The main contributions of the paper are listed as follows.

(1) We propose a notion of differential privacy in the context of probabilistic systems and show how traditional differential privacy can be embedded in our framework.
(2) We introduce an infimum metric and show that it is also a metric instance of differential privacy. Further, we raise a two-level logic as a privacy variant of the familiar HML logic and define an extension for formulae with privacy and distance parameters. With its help, we succeed to characterize differential privacy through the infimum metric.
(3) We explore the relation between our differential privacy and the traditional probabilistic bisimilarity and discover that the distance between two states in the infimum metric is 0 iff they are probabilistic bisimilar. Additionally, our privacy variant logic retains the ability to characterize probabilistic bisimilarity.

The remainder of the paper is structured as follows. After reviewing some preliminaries in Section 2, we introduce our notion of differential privacy for probabilistic systems and propose the infimum metric in Section 3. Section 4 is devoted to characterizing differential privacy logically, including the presentation of a new two-level logic and the extension for its formulae. We study a variant of Crowds protocol in Section 5 and conclude the paper in Section 6. For the convenience of the reader, we place all the proofs of theorems, propositions, corollaries, and lemmas in Appendix.

2. Preliminaries

In this section, we give the preliminaries that will be utilized in our paper. They are separated into three parts, on metric, on differential privacy, and on probabilistic bisimilarity.

2.1. Metric

We recall the notion of metric in this subsection (see, for example [29]).

Definition 2.1. A *metric* on a set X is a function (called the distance function),

$$d : X \times X \to [0, +\infty],$$

such that for all $x, y, z \in X$, the following conditions are satisfied:

(1) $d(x, y) = 0$ iff $x = y$ (coincidence axiom),
(2) $d(x, y) = d(y, x)$ (symmetry),
(3) $d(x, z) \leq d(x, y) + d(y, z)$ (triangle inequality),

where the interval $[0, +\infty]$ includes all non-negative real numbers and a special element of positive infinity.

For the neatness of our framework, we introduced an extension in this definition to include positive infinity into the value range of the distance function d. We will make a specified explanation on it in Remark 3.2.

Additionally, the "only if" direction of the first condition "coincidence axiom" is sometimes eliminated, that is, the distance between two different elements is allowed to be 0. Such a "weak metric" is called a *pseudometric*. In our framework, we actually adopt pseudometric, rather than metric. With a little abuse of notation, we still use metric in the paper.

2.2. Differential privacy

Differential privacy [9] formalizes the idea that a private algorithm should not expose too much information about a particular participant. A randomized private algorithm processes a dataset and returns a result that should remain probabilistically unchanged as one data element is added to or deleted from the dataset.

Definition 2.2. A randomized algorithm $\mathcal{A}$ is *ϵ-differential privacy* if for all datasets D_1 and D_2 that differ in a single element and all $S \subseteq \text{Range}(\mathcal{A})$,

$$\Pr[\mathcal{A}(D_1) \in S] \leq e^{\epsilon} \times \Pr[\mathcal{A}(D_2) \in S],$$

where the probability is taken over the coins of the algorithm and the set $\text{Range}(\mathcal{A})$ denotes the output range of the algorithm $\mathcal{A}$.

Formally, two datasets differ in a single element means that one dataset can be generated by adding an element into the other dataset.

Differential privacy has many pleasant properties. For example, when we query an ϵ-differential private algorithm on two datasets D_1 and D_2 that differ in n elements, then the probabilities of $\mathcal{A}(D_1)$ and $\mathcal{A}(D_2)$ being in the same set S will be within a factor of $e^{n\epsilon}$ of the other.

2.3. Probabilistic bisimilarity

In this subsection, we review some preliminaries about the theory of probabilistic bisimilarity (see, for example [30]). We begin with the model pLTS, since it is a common object of probabilistic bisimilarity.

Definition 2.3. A *probabilistic labeled transition system (pLTS)* is a triple $\langle S, \text{Act}, \to \rangle$, where

- S is a set of states,
- Act is a set of transition labels, and
- the relation $\to$ is a subset of $S \times \text{Act} \times \mathcal{D}(S)$,

where $\mathcal{D}(S)$ is the set of probabilistic distributions over S.

As usual, we shall use the more suggestive notation $s \xrightarrow{a} \mu$ in lieu of $(s, a, \mu) \in \rightarrow$, which means that s can afford an a-labeled transition and reach the distribution μ after the transition. In addition, a pLTS is *finitely branching* if, for each state s, the set $\{(a, \mu) \mid s \xrightarrow{a} \mu\}$ is finite. A pLTS is *finitary* if it has finite states and is finitely branching.

The model of pLTSs admits both non-deterministic and probabilistic behavior. The non-deterministic behavior of pLTSs lies in that one particular state can reach more than one distribution after the same labeled transition, while the probabilistic behavior lies in the probabilities of distributions.

Definition 2.4. Given a pLTS P, an equivalence relation $\mathcal{R}$ over the states of P is a *probabilistic bisimulation* if for any states s and t with $(s, t) \in \mathcal{R}$, $s \xrightarrow{a} \mu$ implies that there exists a distribution η, such that $t \xrightarrow{a} \eta$ and $\eta(E) = \mu(E)$ for every equivalence class E induced by $\mathcal{R}$.

As in the above definition, probabilistic bisimulation is a special equivalence relation on the states. It only admits the states with the same transitions to be equivalent with each other. While probabilistic bisimilarity is a special probabilistic bisimulation, it can be regarded as the "largest" probabilistic bisimulation.

Definition 2.5. Given a pLTS P and two states s and t of P, we say that s and t are *probabilistic bisimilar*, denoted by $s \sim t$, if there is a probabilistic bisimulation $\mathcal{R}$ of P, which contains the pair (s, t) of states.

It is proved that the relation $\sim$ of probabilistic bisimilarity is also a probabilistic bisimulation itself and every other probabilistic bisimulation is a subset of probabilistic bisimilarity. We set $\mathcal{R}_\sim$ to be equivalence classes of probabilistic bisimilarity. Obviously, the equivalence classes of any other probabilistic bisimulation is a division of $\mathcal{R}_\sim$.

3. Differential privacy in probabilistic systems

In this section, we propose our notion of differential privacy in probabilistic systems. We discuss the pLTSs with metrics on their states. The metrics are initialized under an earlier impression on the states and will not change as the system evolves. They often reflect how much difference there is between states in the observer's opinion. Usually, zero distance means that two states are the "same", i.e., they should share the same behavior in the pLTS. Larger distance means that the behaviors of the states are "less similar" to each other. Furthermore, the distance of positive infinity means that two states are totally different, i.e., their behaviors in the pLTS may have no relation. In general, we say that two states are *relevant*, if the distance between them is a real number rather than positive infinity. That is, the behaviors of relevant states are more or less alike. Some metrics have been well studied in the literature and can be directly adopted in our framework. For example, Xu et al. proposed three metrics in [22]. In their framework, larger distance means larger ratio of the probabilities that two automata produce the same trace.

In Subsection 3.1, we introduce our definition of differential privacy in probabilistic systems and display two examples and some properties. We propose an infimum metric in terms of our differential privacy and show its relation to probabilistic bisimilarity in Subsection 3.2. With two preparation lemmas, we prove that this infimum metric is also a metric instance of differential privacy in Subsection 3.3.

3.1. Differential privacy

In this subsection, we define the notion of differential privacy in probabilistic systems and present some remarks about the reason why we define differential privacy in this way. Then, we give an example about how to embed the traditional differential privacy in our framework and another example on an ordinary probabilistic system. Finally, we present some basic properties on our notion of differential privacy.

Given a pLTS P with a preset metric m on its states, we first define a relation $\mathcal{R}_m$ on the states, such that $(s, t) \in \mathcal{R}_m$ iff $m(s, t) = 0$, where s and t are two states of P. Obviously, $\mathcal{R}_m$ is an equivalence relation. As stated in Subsection 2.1, we actually adopt pseudometrics in our framework, so the equivalence class may contain more than one state. The states in the same equivalence class are regarded as "identical" with each other.

Definition 3.1. Given a pLTS P with a metric m on its states and a privacy parameter $\epsilon \in \mathbb{R}^+$, we say that P satisfies *ϵ-differential privacy* on m if for any pair (s_1, s_2) of states of P, such that $m(s_1, s_2) < +\infty$, and any transition label a, if $s_1 \xrightarrow{a} \mu_1$, then there exists a transition $s_2 \xrightarrow{a} \mu_2$ such that

$$\mu_2(E) \leq e^{\epsilon m(s_1, s_2)} \mu_1(E),$$

for any equivalence class E of $\mathcal{R}_m$.

On this definition, we have the following two remarks, which explain why we define differential privacy in this form.

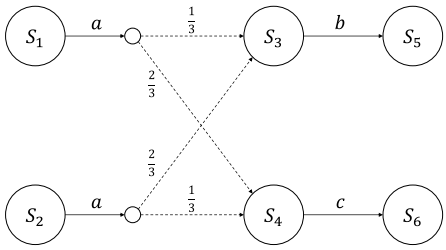

Fig. 1. A pLTS.

Remark 3.1. Compared to Definition 2.2, we formalize the computation of algorithm with the transition in pLTS, the range set with the equivalence class, and the neighborhood of datasets with the metric on states. Suppose that there is a black box with a button. The black box has several internal states and when we press the button, it alters the internal state and releases partial information about the current state. We want to make sure that the internal state is secret and no one can identify the previous state when presented with the latter information. The action of pressing the button causes the transition and if the previous states are relevant to each other, the current states should not be too much different in case that too much information about the previous states is revealed. We adopt the notion of differential privacy to express the restriction on the transition. Since the distance between states is a real number, not limited to either 0 or 1, it is a natural idea to add $m(s_1, s_2)$ to the exponent of e in our definition. We notice that a similar idea also appears in the work [31] of Chatzikokolakis et al.

Remark 3.2. As stated in Subsection 2.1, the value range of metric is extended to contain positive infinity. We will give an explanation in this remark. Technically, if we skip this extension and discard the limitation $m(s_1, s_2) < +\infty$ in Definition 3.1, then the notion of differential privacy is too powerful. It commands that if any state affords an a-labeled transition for some a, then all states should afford an a-labeled transition. Therefore, we should introduce a special element, i.e. positive infinity, into the value range of the metric, which denotes that the states are too different to be forced to share transitions of the same label. Actually, we first adopted a similar form to (ϵ, δ)-differential privacy. However, for the sake of easing the computation and simplifying our theorems, we eventually convert our definition to this form.

We now consider two examples of our notion of differential privacy. The first one shows the relation to the traditional differential privacy. The second one is about an ordinary pLTS and will be frequently utilized in our framework to illustrate our results.

Example 3.1. Given a randomized algorithm $\mathcal{A}$ with finite outputs, we can construct a pLTS P as follows. Its states consist of two kinds, dataset states S_D, each for an available dataset D, and output states S_o, each for a possible output o of the algorithm. It has one transition label a, standing for this algorithm, and the transition on this label is defined according to the behavior of this algorithm, that is, for any $s \in S_D$, we have a transition $s \xrightarrow{a} \mu$ and $\mu(t) = \Pr[\mathcal{A}(D) = o]$, for any $t \in S_o$.

We then set a metric m on this pLTS. The distance between two dataset states equals the count of elements that the corresponding datasets differ in. The distance between two output states or between one dataset state and one output state is set to be positive infinity. Then each equivalence class of $\mathcal{R}_m$ consists of one single state. It is not difficult to verify that the algorithm $\mathcal{A}$ is ϵ-differential privacy iff the pLTS P satisfies ϵ-differential privacy on m.

Example 3.2. Consider the pLTS P displayed in Fig. 1. The edges with labels on them denote the transitions of this pLTS. The a-labeled edge at the top denotes that s_1 can afford an a-labeled transition and arrive at s_3 or s_4 with probability $1/3$ or $2/3$, respectively. Similarly, s_2 can afford an a-labeled transition and arrive at s_3 or s_4 with probability $2/3$ or $1/3$, respectively. The b-labeled edge between s_3 and s_5 denotes that there is a transition $s_3 \xrightarrow{b} \mu_3$ and μ_3 is a Dirac distribution for s_5, that is, $\mu_3(s_5) = 1$ and $\mu_3(s) = 0$ for any other state s. Similarly, the c-labeled edge between s_4 and s_6 denotes that s_4 can afford a c-labeled transition and arrive at s_6 with probability 1.

We set a distance function m on the states of the pLTS, such that

$$m(s_1, s_2) = m(s_2, s_1) = \ln 2,$$
$$m(s_5, s_6) = m(s_6, s_5) = 0, \text{ and}$$
$$m(s, t) = +\infty$$

for any other pair (s, t) of states. Clearly, m is a metric and the equivalence classes of $\mathcal{R}_m$ are

$$\{\{s_1\}, \{s_2\}, \{s_3\}, \{s_4\}, \{s_5, s_6\}\}.$$

Now, let us check whether P satisfies 1-differential privacy on m. There are only two pairs of states that have real numbers as distance. Further, s_5 and s_6 do not afford any transition, so this pair does not violate differential privacy. For the pair (s_1, s_2) of states, s_1 affords a transition $s_1 \xrightarrow{a} \mu_1$ and s_2 affords a transition $s_2 \xrightarrow{a} \mu_2$, such that

$$\mu_1 = \frac{1}{3}s_3 + \frac{2}{3}s_4,\ \mu_2 = \frac{2}{3}s_3 + \frac{1}{3}s_4.$$

One can easily verify that the pair (s_1, s_2) does not violate differential privacy by Definition 3.1, as well. So we can conclude that P satisfies 1-differential privacy on m.

Now let us state some simple properties of our differential privacy. The first two properties can be achieved by some basic mathematical technologies.

Proposition 3.1. *Given a pLTS P with a metric m on its states, if P satisfies ϵ-differential privacy on m for some ϵ, then P also satisfies ϵ'-differential privacy on m for any $\epsilon' \geq \epsilon$.*

Proposition 3.2. *Given a pLTS P with a metric m on its states and a privacy parameter ϵ, if P satisfies ϵ-differential privacy on m, then P also satisfies $\frac{1}{\alpha}\epsilon$-differential privacy on αm for any $\alpha \in \mathbb{R}^+$.*

In the above proposition, αm is defined by

$$(\alpha m)(s, t) = \alpha \cdot m(s, t)$$

for any states s and t, which turns out to be a metric as well.

The following two propositions take the first step towards the relation between our differential privacy and probabilistic bisimilarity.

Proposition 3.3. *Given a pLTS P with a metric m on its states and a privacy parameter ϵ, if P satisfies ϵ-differential privacy on m, then $\mathcal{R}_m$ is a probabilistic bisimulation.*

Proposition 3.4. *Given a pLTS P with a metric m on its states and a privacy parameter ϵ, if P satisfies ϵ-differential privacy on m, then for any pair (s_1, s_2) of states of P, such that $m(s_1, s_2) < +\infty$, and any transition label a, if $s_1 \xrightarrow{a} \mu_1$, then there exists a transition $s_2 \xrightarrow{a} \mu_2$ such that $\mu_2(E) \leq e^{\epsilon m(s_1, s_2)}\mu_1(E)$, for any equivalence class E of $\mathcal{R}_\sim$.*

It should be noticed that in the above proposition, the equivalence class E is a member of $\mathcal{R}_\sim$, rather than R_m in Definition 3.1.

3.2. Infimum metric

In Example 3.2, we set a metric on the states of the pLTS displayed in Fig. 1 and proved that the pLTS satisfies 1-differential privacy on the metric. We know that smaller distance means more similarity, so a natural question is to what degree the distance between two given states could be small, while not violating differential privacy. In this subsection, we will give a specific definition of such a distance, called infimum distance, and show its relation to probabilistic bisimilarity.

Definition 3.2. Given a pLTS P and a privacy parameter ϵ, we define a distance function m_ϵ on the states of P, such that the distance between any two states is the infimum of distances between them in such metrics that P satisfies ϵ-differential privacy on them. Formally,

$$m_\epsilon(s, t) = \inf\{m(s, t) \mid P \text{ satisfies } \epsilon\text{-differential privacy on } m\}.$$

Additionally, we set $m_\epsilon(s, t) = +\infty$, if $m(s, t) = +\infty$ for every metric m such that P satisfies ϵ-differential privacy on m.

In this definition, m_ϵ is merely a distance function between states, but we will prove that it indeed satisfies the conditions of metric in Lemma 3.2. We call this distance function *infimum metric* or *ϵ-metric*, if we want to emphasize the privacy parameter, in the rest of the paper.

As stated in Propositions 3.3 and 3.4, we have obtained some properties of differential privacy that are related to probabilistic bisimilarity. Inspired by them, we are going to explore whether there exists close relation between infimum metric and probabilistic bisimilarity. To this end, we give a metric which will play an important role in the proofs of our subsequent results.

Definition 3.3. Given a pLTS P, we define a distance function m_p on its states as follows,

$$m_p(s,t) = \begin{cases} 0 & \text{if } s \sim t, \\ +\infty & \text{if } s \nsim t. \end{cases}$$

Obviously, m_p is a metric and $\mathcal{R}_{m_p}$ has the same equivalence class with $\mathcal{R}_\sim$. Furthermore, for any ϵ, P satisfies ϵ-differential privacy on metric m_p. The metric m_p is called *p-metric* (for probabilistic bisimilarity) in the rest of the paper.

The following theorem discloses the relation between the infimum metric and probabilistic bisimilarity and actually provides a method to show that two states are probabilistic bisimilar.

Theorem 3.1. *Given a finitary pLTS P and a privacy parameter ϵ, two states s and t of P are probabilistic bisimilar iff $m_\epsilon(s,t) = 0$. Therefore, $\mathcal{R}_{m_\epsilon} = \mathcal{R}_\sim$ for any ϵ.*

In the theorem, we placed a condition on pLTS, which has to be finitary. We now give an example extended from Example 3.2 to show the necessity of this condition.

Example 3.3. Consider a pLTS P_r, arisen from the pLTS in Example 3.2. We erase the existing a-labeled transitions from s_1 and s_2 and replace them with T_1 and T_2, respectively, where T_1 and T_2 are defined as follows.

$$T_1 = \{s_1 \xrightarrow{a} \mu_1 \mid \mu_1(s_3) = x \text{ and } \mu_1(s_4) = 1 - x, \text{ for some } \textit{rational} \text{ number } x \in (0,1)\},$$

$$T_2 = \{s_2 \xrightarrow{a} \mu_2 \mid \mu_2(s_3) = y \text{ and } \mu_2(s_4) = 1 - y, \text{ for some } \textit{irrational} \text{ number } y \in (0,1)\}.$$

Note that, x in T_1 is a rational number while y in T_2 is an irrational number. Having this revision, we can easily verify that P_r is no longer a finitary pLTS and the equivalence classes of $\mathcal{R}_\sim$ on P_r are $\{\{s_1\}, \{s_2\}, \{s_3\}, \{s_4\}, \{s_5, s_6\}\}$. Therefore, s_1 and s_2 are not probabilistic bisimilar.

However, $m_\epsilon(s_1, s_2)$ is indeed 0 for any $\epsilon \in \mathbb{R}^+$. Given a distance limit $d \in \mathbb{R}^+$, no matter how small d is, we can construct a distance function m by slightly editing m_p defined in Definition 3.3, setting $m(s_1, s_2) = m(s_2, s_1) = d/2$. Obviously, m is a metric. Additionally, it can be easily checked that P_r satisfies ϵ-differential privacy on m for any $\epsilon \in \mathbb{R}^+$, if we notice that there exist at least one rational number and one irrational number in any real interval.

Thus, it is necessary to add the condition of finitary pLTS in this theorem.

We now give a corollary of Theorem 3.1 which specifies that m_ϵ treats the equivalence classes of probabilistic bisimilarity as a whole and describes the amount of difference between two equivalence classes.

Corollary 3.1. *Given a finitary pLTS P and a privacy parameter ϵ, if $s_1 \sim s_2$ and $t_1 \sim t_2$, then $m_\epsilon(s_1, t_1) = m_\epsilon(s_2, t_2)$, for any states s_1, s_2, t_1, and t_2 of P.*

3.3. Infimum metric satisfies differential privacy

In the last subsection, we introduced a distance function to specify the least distance between two states while not violating differential privacy. We wonder whether such a distance function is also a metric and if so, whether this metric is a metric instance of differential privacy. In this subsection, we show that the answers are both YES.

Before stating the main result, we first give a lemma which is an extension of Theorem 3.1, showing the relation between m_ϵ and ordinary metrics, which will be used when proving that m_ϵ is a metric.

Lemma 3.1. *Given a finitary pLTS P and a privacy parameter ϵ, for any two states s and t of P, there exists a metric m, such that $m(s,t) = m_\epsilon(s,t)$ and P satisfies ϵ-differential privacy on m.*

In a finitary pLTS, for any pair (s,t) of states, we have a metric m which has the same distance with m_ϵ between these two states. That is, the distance between each pair of states in m_ϵ is "reachable". Additionally, we would like to remark that for different pairs of states, the metric m may be different, so this lemma does not directly result that P satisfies ϵ-differential privacy on m_ϵ. Having this lemma, we are ready to show that m_ϵ is also a metric.

Lemma 3.2. *Given a finitary pLTS P, m_ϵ is a metric for any privacy parameter ϵ.*

We confirm that m_ϵ is also a metric in this lemma before m_ϵ becomes a candidate of a metric instance of ϵ-differential privacy. We continue to check whether the pLTS P satisfies ϵ-differential privacy on m_ϵ.

Theorem 3.2. *Given a finitary pLTS P and a privacy parameter ϵ, P satisfies ϵ-differential privacy on m_ϵ.*

With this theorem, we discover that the infimum metric m_ϵ owns a special position among all metric instances of ϵ-differential privacy. First, it is a metric instance of ϵ-differential privacy itself, as shown in this theorem. On the other hand, the distance between any pair of states in m_ϵ is no greater than that in any other metric instance of ϵ-differential privacy, according to the definition of m_ϵ. This is similar to the relation between probabilistic bisimilarity and probabilistic bisimulation. Probabilistic bisimilarity is a probabilistic bisimulation itself and contains any other probabilistic bisimulation as its subset. Since larger distance means less similarity, the studies of metric instances of ϵ-differential privacy can be focused on m_ϵ, including the logical characterization that we will introduce in the next section.

4. Logical characterization of differential privacy

In this section, we propose a logic, which is extending from the familiar HML logic proposed in [25], and characterize our notion of differential privacy with this logic. We introduce the formula structure of the logic and how they are satisfied by states in Subsection 4.1 and characterize probabilistic bisimilarity in Subsection 4.2. In Subsection 4.3, we give an extension of the formulae and present our main result on how we can characterize differential privacy through the infimum metric with our logic.

4.1. Logic for differential privacy

In this subsection, we define a logic extending from the HML logic [25] and illustrate how the formulae are satisfied by states and distributions over states.

We now define our logic, which is based on a set of transition labels Act. The set of its formulae is given by the following abstract syntax:

$$F ::= tt \mid ff \mid F_1 \wedge F_2 \mid F_1 \vee F_2 \mid \langle a \rangle \varphi \mid [a]\varphi,$$

$$\varphi ::= tt \mid ff \mid \varphi_1 \wedge \varphi_2 \mid \varphi_1 \vee \varphi_2 \mid \Diamond_p F \mid \Box_p F,$$

where $a \in Act$ and $p \in [0, 1]$. We call this logic *pHML logic*, for the privacy extension of the HML logic.

Remark 4.1. There have already existed a lot of variants of the HML logic, such as in these works [32–35]. However, we cannot follow them due to the following two reasons.

First, the semantics of our logic should be given in terms of a single state, rather than a distribution over states, because the infimum metric, as defined in Definition 3.2, is over states and we characterize differential privacy through the infimum metric. In some papers, for example [33], the semantics of the logic is given in terms of distributions, as they need to express probabilistic transitions. We also refer to probabilistic transitions in our framework, so we make a compromise and adopt a two-level logic, for states and distributions, respectively. This idea is taken from Jonsson et al. [36].

On the other hand, we have not introduced the negative symbol $\neg$ in our logic, because we need an extension of the formulae when characterizing differential privacy. However, the extensions of $\langle a \rangle \varphi$ and $[a]\varphi$ apply different rules. If we use the same way as Hennessy [35] and introduce $\neg$ in our logic, then $[a]\varphi$ would be expressed as $\neg\langle a \rangle \neg\varphi$. As a result, it would be impossible to distinguish them when generating extensions of formulae. The specific extension rules of the formulae can be found in Definition 4.1.

As seen, we have two kinds of formulae in this logic. The formulae with the form F, called *F-formulae*, are satisfied by states of a pLTS with the set Act of transition labels, while those with the form φ, called *φ-formulae*, are satisfied by distributions over states. Since we mainly concern about states rather than distributions in differential privacy, we will focus the study of this logic on F-formulae.

Formally, the satisfaction can be described as follows. For F-formulae,

- $s \vDash tt$ for all states s.
- $s \vDash ff$ for no state s.
- $s \vDash F_1 \wedge F_2$ iff $s \vDash F_1$ and $s \vDash F_2$.
- $s \vDash F_1 \vee F_2$ iff $s \vDash F_1$ or $s \vDash F_2$.
- $s \vDash \langle a \rangle \varphi$ iff there exists a distribution μ, such that $s \xrightarrow{a} \mu$ and $\mu \vDash \varphi$.
- $s \vDash [a]\varphi$ iff for any distribution μ, $s \xrightarrow{a} \mu$ results in $\mu \vDash \varphi$.

For φ-formulae,

- $\mu \vDash tt$ for all distributions μ.
- $\mu \vDash ff$ for no distribution μ.
- $\mu \vDash \varphi_1 \wedge \varphi_2$ iff $\mu \vDash \varphi_1$ and $\mu \vDash \varphi_2$.
- $\mu \vDash \varphi_1 \vee \varphi_2$ iff $\mu \vDash \varphi_1$ or $\mu \vDash \varphi_2$.

- $\mu \vDash \Diamond_p F$ iff the probability of those states that satisfy F in μ is no less than p, that is, $\sum_{s \vDash F} \mu(s) \geq p$.
- $\mu \vDash \Box_p F$ iff the probability of those states that satisfy F in μ is less than p, that is, $\sum_{s \vDash F} \mu(s) < p$.

The symbol $\vDash$ represents satisfaction for both F-formulae and φ-formulae. We write $\text{pHML}(s) = \{F \mid s \vDash F\}$ for the set of all F-formulae that are satisfied by the state s, and write $\text{state}(F) = \{s \mid s \vDash F\}$ for the set of all states that satisfy the given formula F. We give an example on the satisfaction of formulae.

Example 4.1. Consider the formula $F = \langle a \rangle tt \wedge [b]\Diamond_{\frac{1}{2}}(\langle c \rangle tt)$. If a state s satisfies the formula F, it should afford an a-labeled transition. Meanwhile, for any distribution after s performs a b-labeled transition, the probabilities of those states that can afford a c-labeled transition should be no less than $1/2$.

4.2. Characterizing probabilistic bisimilarity

In this subsection, we first construct the negations of the formulae in our pHML logic and then characterize probabilistic bisimilarity with our pHML logic.

Since the HML logic is proposed to characterize probabilistic bisimilarity, we desire that our pHML logic, as an extension of the HML logic, also has the ability. In addition, the techniques used in characterizing probabilistic bisimilarity are helpful to characterize differential privacy. Following the existing manner in probabilistic bisimilarity [30], the negation of a formula is necessary when we attempt to characterize probabilistic bisimilarity logically. However, we did not include a negation operator in our pHML logic. Thus, we need to construct an F-formula F^c for each F-formula F, which behaves like the negation of F. The construction method is defined by the structural recursion as follows:

- $tt^c = ff$, for both F-formulae and φ-formulae,
- $ff^c = tt$, for both F-formulae and φ-formulae,
- $(F_1 \wedge F_2)^c = F_1^c \vee F_2^c$,
- $(F_1 \vee F_2)^c = F_1^c \wedge F_2^c$,
- $(\langle a \rangle \varphi)^c = [a]\varphi^c$,
- $([a]\varphi)^c = \langle a \rangle \varphi^c$,
- $(\varphi_1 \wedge \varphi_2)^c = \varphi_1^c \vee \varphi_2^c$,
- $(\varphi_1 \vee \varphi_2)^c = \varphi_1^c \wedge \varphi_2^c$,
- $(\Diamond_p F)^c = \Box_p F$,
- $(\Box_p F)^c = \Diamond_p F$.

Now, we present an example to illustrate the construction method.

Example 4.2. Consider the formula in Example 4.1, $F = \langle a \rangle tt \wedge [b]\Diamond_{\frac{1}{2}}(\langle c \rangle tt)$. Applying the construction method for negation, we can get that $F^c = [a]ff \vee \langle b \rangle \Box_{\frac{1}{2}}(\langle c \rangle tt)$.

The following lemma shows that F^c indeed behaves in the way that is opposite to F.

Lemma 4.1. *Given a pLTS, for any state s and any F-formula F, $s \vDash F$ iff $s \nvDash F^c$.*

The existence of F^c will play a part in the proof of the following theorem, on the relation between our pHML logic and probabilistic bisimilarity.

Theorem 4.1. *Given a finitary pLTS P, two states s_1, s_2 of P are probabilistic bisimilar iff they satisfy the same formulae, i.e., $pHML(s_1) = pHML(s_2)$.*

With this theorem, we know that if two states are probabilistic bisimilar with each other, then they share the same formulae in our pHML logic. That is, given an equivalence class E of $\mathcal{R}_\sim$ and a formula F, either all states in E satisfy F or none of them satisfy F. We use $E \vDash F$ to denote the former case.

4.3. Characterizing differential privacy

In this subsection, we characterize differential privacy through the infimum metric defined in Definition 3.2 with our pHML logic. We first introduce an extension of the formulae, which is constructed with privacy and distance parameters, and give a property on the extension. Then, we present our main theorem which states that the distance between two states is no greater than a threshold if and only if the formulae satisfied by one state can be satisfied by the other state, after

extension constructed with the threshold as distance parameter. We derive a method to determine the distance between states in the infimum metric from the theorem and give an example to illustrate the method.

Since the infimum metric is a metric instance of differential privacy, the distance between two states in the infimum metric describes the difference between their behavior when performing the same labeled transition. Thus, if the distance between two states is d, the relation between the formulae satisfied by them should be relevant to the distance d. So, we define an extension of formulae which takes privacy and distance parameters.

Definition 4.1. Given an F-formula F, a privacy parameter ϵ, and a distance d, we define the *extension* of F, denoted by F^e, by the following construction method, which is according to the structural recursion on formulae.

For the extension F^e of F-formulae,

- $tt^e = tt$,
- $ff^e = ff$,
- $(F_1 \wedge F_2)^e = F_1^e \wedge F_2^e$,
- $(F_1 \vee F_2)^e = F_1^e \vee F_2^e$,
- $(\langle a\rangle\varphi)^e = \langle a\rangle\varphi^{e_1}$,
- $([a]\varphi)^e = [a]\varphi^{e_2}$.

As seen, when constructing F^e, we utilize the extension of φ-formulae, which has two kinds, φ^{e_1} and φ^{e_2}. They are applied to the cases $F = \langle a\rangle\varphi$ and $F = [a]\varphi$, respectively.

For the first extension φ^{e_1} of φ-formulae,

- $tt^{e_1} = tt$,
- $ff^{e_1} = ff$,
- $(\varphi_1 \wedge \varphi_2)^{e_1} = \varphi_1^{e_1} \wedge \varphi_2^{e_1}$,
- $(\varphi_1 \vee \varphi_2)^{e_1} = \varphi_1^{e_1} \vee \varphi_2^{e_1}$,
- $(\Diamond_p F)^{e_1} = \Diamond_{1-e^{\epsilon d}(1-p)} F$,
- $(\Box_p F)^{e_1} = \Box_{e^{\epsilon d}p} F$.

For the second extension φ^{e_2} of φ-formulae,

- $tt^{e_2} = tt$,
- $ff^{e_2} = ff$,
- $(\varphi_1 \wedge \varphi_2)^{e_2} = \varphi_1^{e_2} \wedge \varphi_2^{e_2}$,
- $(\varphi_1 \vee \varphi_2)^{e_2} = \varphi_1^{e_2} \vee \varphi_2^{e_2}$,
- $(\Diamond_p F)^{e_2} = \Diamond_{e^{-\epsilon d}p} F$,
- $(\Box_p F)^{e_2} = \Box_{1-e^{-\epsilon d}(1-p)} F$.

In the construction of φ^{e_1} and φ^{e_2}, the probability parameters of the operators $\Diamond$ and $\Box$ are modified. However, we command that the probability parameters should be between 0 and 1 when defining our pHML logic and the modification may break this limitation. We observe that in both extensions of φ-formulae, the probability parameters of $\Diamond$ become lesser and the probability parameters of $\Box$ become larger. So, if the parameters break the limitation of $[0, 1]$, it must be a $\Diamond$-formula with negative probability parameter or a $\Box$-formula with probability parameter which is greater than 1. Intuitively, these φ-formulae are satisfied by all distributions, which helps us to make a simple rule. In both situations, we can set the corresponding extensions to be tt directly. We will specify this rule in the following example. However, since it is an intuitive solution under the idea of this construction, we will not give a detailed discussion on it in our subsequent proofs.

Example 4.3. Consider the formula

$$F = \langle a\rangle(\Box_{\frac{3}{4}}(\langle b\rangle tt \vee \langle c\rangle tt)) \wedge [b](\Diamond_{\frac{3}{4}}(\langle a\rangle\Box_{\frac{1}{6}}([c]ff)))$$

and its extension with privacy parameter $\epsilon = \ln 2$ and distance $d = 1$. According to the construction method, its extension is

$$F^e = \langle a\rangle(\Box_{\frac{3}{2}}(\langle b\rangle tt \vee \langle c\rangle tt)) \wedge [b](\Diamond_{\frac{3}{8}}(\langle a\rangle\Box_{\frac{1}{6}}([c]ff))).$$

However, the probability parameter under the first operator $\Box$ is $3/2$, larger than 1. With the special rule, we should make a modification and set it tt directly. Thus, it turns out that

$$F^e = \langle a\rangle tt \wedge [b](\Diamond_{\frac{3}{8}}(\langle a\rangle\Box_{\frac{1}{6}}([c]ff))).$$

With this example, we can discover that the extension of F-formulae does not change the structure. It only modifies some probability parameters of the operators $\Diamond$ and $\Box$, if the aforementioned special rule is not applied.

Proposition 4.1. *Given an F-formula F, a φ-formula φ, a privacy parameter ϵ, a distance d, a pLTS P, a state s of P, and a distribution μ over states of P,*

(1) *if $s \vDash F$, then $s \vDash F^e$;*
(2) *if $\mu \vDash \varphi$, then $\mu \vDash \varphi^{e_1}$;*
(3) *if $\mu \vDash \varphi$, then $\mu \vDash \varphi^{e_2}$,*

where the extensions F^e, φ^{e_1}, and φ^{e_2} are all constructed with ϵ and d.

This proposition specifies that F^e, φ^{e_1}, and φ^{e_2} are indeed extensions of F and φ, because they extend the sets of states and distributions that satisfy F and φ, respectively.

With the extension of formulae, we are ready to characterize differential privacy now.

Lemma 4.2. *Given a φ-formula φ, a privacy parameter ϵ, a distance d, a finitary pLTS P, and two distributions μ_1 and μ_2 over its states, such that $\mu_2(E) \leq e^{\epsilon d}\mu_1(E)$ for all equivalence classes E of $\mathcal{R}_\sim$ on P,*

(1) *if $\mu_1 \vDash \varphi$, then $\mu_2 \vDash \varphi^{e_1}$;*
(2) *if $\mu_2 \vDash \varphi$, then $\mu_1 \vDash \varphi^{e_2}$,*

where the extensions φ^{e_1} and φ^{e_2} are both constructed with ϵ and d.

The above lemma shows the relation between distributions over states and two extensions of φ-formulae. With this lemma, we state the final result on how to characterize differential privacy with our pHML logic, in the following theorem.

Theorem 4.2. *Given a privacy parameter ϵ, a distance d, a finitary pLTS P, and two states s_1 and s_2 of P, the following two statements are equivalent.*

(1) $m_\epsilon(s_1, s_2) \leq d$.
(2) *$s_1 \vDash F$ results in $s_2 \vDash F^e$ and $s_2 \vDash F$ results in $s_1 \vDash F^e$, for any F-formula F,*

where F^e is constructed with ϵ and d.

Comparing this theorem with Theorem 4.1, the first statement "$m_\epsilon(s_1, s_2) \leq d$" is similar to that $s_1 \sim s_2$, both describing the relation between two states. The distinction is that in Theorem 4.1, we only concern whether these two states are probabilistic bisimilar, while in this theorem, we still concern how much difference they have if the distance between them is not 0, which is equivalent to that they are not probabilistic bisimilar.

The second statement "$s_1 \vDash F$ results in $s_2 \vDash F^e$ and $s_2 \vDash F$ results in $s_1 \vDash F^e$" is similar to that s_1 and s_2 satisfy the same formulae, both describing the relation between the formulae satisfied by them. Since we introduce a measure on the difference between these two states, the formulae satisfied by them naturally need a transformation, exactly the extension of formula that we defined in Definition 4.1.

In this theorem, we only give an upper bound of the distance between two states, rather than the precise value. However, we may still acquire the distance in the infimum metric with this theorem. The first statement of the theorem gives an upper bound of the distance, but if we use the theorem conversely, that is, we construct an extension of formula with a distance parameter such that the extension violates the second statement, then we can see that the first statement is also wrong, which gives us a lower bound of the distance. That is, the logical characterization can help us to find a witness formula when the distance of two states cannot be less than a distance threshold. Combining the lower and upper bounds, we can possibly determine the exact distance between two states in the infimum metric. The following is an example of the method.

Example 4.4. Consider the pLTS P displayed in Fig. 1. We have constructed a metric m on the states of this pLTS and shown that P satisfies 1-differential privacy on m in Example 3.2. That is, we have known that $m_1(s_1, s_2) \leq m(s_1, s_2) = \ln 2$. Here, m_1 is the ϵ-metric for $\epsilon = 1$. We wonder whether $m_1(s_1, s_2)$ can be less or what the value of $m_1(s_1, s_2)$ is.

Suppose that there is another distance limitation $d' < \ln 2$. According to Theorem 4.2, if $m_1(s_1, s_2) \leq d'$, then for any formula F with $s_1 \vDash F$, we have that $s_2 \vDash F^e$, where F^e is constructed with 1 and d'. We notice that $s_1 \vDash F = [a](\Diamond_{\frac{2}{3}}(\langle c\rangle tt))$, and its extension $F^e = [a](\Diamond_{\frac{2}{3}e^{-d'}}(\langle c\rangle tt))$. Since $d' < \ln 2$, we have that $\frac{2}{3}e^{-d'} > \frac{1}{3}$. However, s_2 has an a-labeled transition and reaches a distribution with only $1/3$ probability to afford a c-labeled transition, that is, $s_2 \nvDash F^e$.

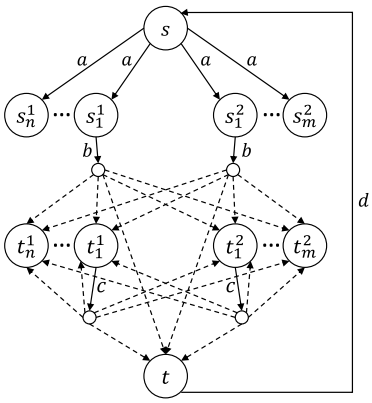

Fig. 2. The pLTS for Crowds.

After this discussion, we see that it does not hold that $m_1(s_1, s_2) \leq d'$, for any distance limit $d' < \ln 2$. That is, $m_1(s_1, s_2) = \ln 2$.

We notice that the method in the last example is not a general method. The method requires us to find the logic and verify the satisfaction manually. So, we desire a more automated method which can determine the distance in the infimum metric logically without too much intervention. To achieve such a method, we investigate some work on the automatic verification of finite-state processes [37–39]. They provided a workbench to check whether two processes are equivalent to each other in the sense of having the same behavior and whether a process satisfies a particular logic formula. But the equivalence checking is through an algorithm, which maintains partitioning of states and refines it with the bisimulation restriction [40]. Since they does not check equivalence logically, we need some further study to acquire a method that can determine the distance in the infimum metric logically and we would like to defer it to our future work.

5. Case study: crowds protocol

In this section, we study a real case, an extended Crowds protocol with different behavior members. We build a pLTS for the protocol and preset a metric on its states following an intuitive idea. We prove that the system satisfies differential privacy on the metric under some privacy parameter, and deduce the infimum metric of the privacy parameter.

The Crowds protocol, proposed by Reiter et al. in [41], is a network protocol for anonymous web browsing. The main idea behind Crowds is to hide each member's communications by routing them randomly within a group of similar members. So, the message receiver and the other group members cannot distinguish the true sender of this message. Therefore, the Crowds protocol performs well when defending against corrupt internal attackers and receiver.

Technically, the protocol works as follows.

(1) When a member in the network, called sender, wants to send a message, she does not directly send it to the receiver. However, she selects a member randomly (possibly herself) and sends this message to this member.
(2) When a member receives a message, she first checks whether she is the receiver. If not, she tosses a coin. If getting "Heads", she selects a member randomly (possibly herself) and forwards the message to that member. If getting "Tails", she forwards the message to the receiver.

The coin used here is not fair, which turns out "Head" with probability $p_f > \frac{1}{2}$.

Members in the network are not allowed to get any knowledge about the route of this message. They have only access to the identifier of their predecessors and message receiver. In this way, even though the message is caught by a corrupt internal member or message receiver, they cannot make sure who sends this message, because their predecessor may only be a forwarder. We notice that Xu studied an extended Crowds protocol with member-wise trusted forwarders in [21], and applied the compositionality result in that extended protocol.

We study another variant of the Crowds protocol with different behavior members. In our framework of differential privacy, we concern about the difference between behaviors of relevant states. So we suppose that there are two kinds of members in the network, who differ in the probabilities of their coins. Specifically, there are n members tossing a coin which turns out "Head" with probability p_1, and m members with probability p_2 ($p_1 > p_2 > \frac{1}{2}$). Additionally, there is another member playing the role of message receiver. Since this member does not forward messages, we do not care the probability of her coin.

We build a pLTS P_c for our variant of the Crowds protocol and display it in Fig. 2. There are totally $2n + 2m + 2$ states in this pLTS and their implications are listed as follows.

Table 1
Transitions in the pLTS for Crowds.

state	label	distribution
s	a	$1 \cdot s_i^1$ for each i
s	a	$1 \cdot s_j^2$ for each j
s_i^1 or s_j^2	b	$\sum_i \frac{1}{n+m+1} t_i^1 + \sum_j \frac{1}{n+m+1} t_j^2 + \frac{1}{n+m+1} t$
t_i^1	c	$\sum_i \frac{p_1}{n+m} t_i^1 + \sum_j \frac{p_1}{n+m} t_j^2 + (1-p_1)t$
t_j^2	c	$\sum_i \frac{p_2}{n+m} t_i^1 + \sum_j \frac{p_2}{n+m} t_j^2 + (1-p_2)t$
t	d	$1 \cdot s$

Table 2
Metric on states of the pLTS for Crowds.

state 1	state 2	distance
s	X	$+\infty$
t	X	$+\infty$
s_i^1 or s_j^2	t_i^1 or t_j^2	$+\infty$
s_i^1	s_j^2	2
$s_{i_1}^1$	$s_{i_2}^1$	0
$s_{j_1}^2$	$s_{j_2}^2$	0
t_i^1	t_j^2	2
$t_{i_1}^1$	$t_{i_2}^1$	0
$t_{j_1}^2$	$t_{j_2}^2$	0

(1) The state s means that currently, this system is idle and no message is forwarding.
(2) The state s_i^1 or s_j^2 means that a member wants to send a message to the receiver. The parameters i and j denote the index of the member.
(3) The state t_i^1 or t_j^2 means that a member has received a message and is going to forward it. The parameters i and j still denote the index of the member.
(4) The state t means that a message has been delivered to the receiver.

The subscripts i and j are in ranges that $i \in \{1, 2, \ldots, n\}$ and $j \in \{1, 2, \ldots, m\}$. Transitions in this pLTS are divided into four kinds and labeled with a, b, c, and d. The state s can afford an a-labeled transition and arrive at some s_i^1 or s_j^2 with probability 1, standing for that the corresponding member wants to send a message. The state s_i^1 or s_j^2 can afford a b-labeled transition and arrive at some t_i^1, t_j^2, or t with the same probability, standing for the random selection in the first step of the protocol. The state t_i^1 or t_j^2 can afford a c-labeled transition and arrive at t with probability $1 - p_j$ and some t_i^1 or t_j^2 with probability $p_j/(n+m)$, standing for the forwarding stage in the second step. The state t can afford a d-labeled transition and arrive at s with probability 1, meaning the completeness of this sending. For the neatness of the figure, we omit some states, all probabilities in distributions, and the transitions of s_n^1, s_m^2, t_n^1, and t_m^2, while fill all the transitions of P_c in Table 1.

We then set a distance function m_c on the states of the pLTS P_c, specified in Table 2, where the symbol X stands for any state in the pLTS. Clearly, m_c is a metric and the equivalence classes of $\mathcal{R}_{m_c}$ are

$$\{\{s\}, \{s_1^1, \ldots, s_n^1\}, \{s_1^2, \ldots, s_m^2\}, \{t_1^1, \ldots, t_n^1\}, \{t_1^2, \ldots, t_m^2\}, \{t\}\}.$$

The metric m_c is set according to the following idea. First, the distance between the states of different kinds should be positive infinity for their totally different behavior. Second, the distance between the states in the same kind should be 0, if their corresponding members toss the coins with the same probability of "Head", and 2 otherwise, because one can transform between these two states by erasing a message from some member and adding it to another member.

With the metric on its states, we can verify our notion of differential privacy in this pLTS.

Proposition 5.1. *The pLTS P_c satisfies $(\frac{1}{2} \ln \frac{1-p_2}{1-p_1})$-differential privacy on the metric m_c.*

As stated in Remark 3.1, our notion of differential privacy in probabilistic systems prevents the previous internal states from being revealed by the later information. Since the Crowds protocol satisfies differential privacy, we conclude that the initial member who sends the message, as a previous internal state, is protected and cannot be known by any malicious member of the system if he only knows whether or not he is on the transition route, which is exactly the purpose of the Crowds protocol.

We also remark that our notion of differential privacy is a guarantee at system level. The privacy parameter ϵ is a property of the system, regardless of which state the system is in. If a system is ϵ-differential private, then it is still ϵ-differential private after it executes some steps. As mentioned in Introduction, we do not involve privacy budget and privacy leakage in our framework. For example, in our Crowds case, the system keeps executing forever and no matter which state it is in, it is always $(\frac{1}{2}\ln\frac{1-p_2}{1-p_1})$-differential private.

However, here comes another question: Is the metric m_c identical to the infimum metric m_ϵ under the privacy parameter $\epsilon = \frac{1}{2}\ln\frac{1-p_2}{1-p_1}$? By the definition of infimum metric, those pairs of states with the distance of 0 in m_c must also have the distance of 0 in m_ϵ. For those pairs of states with the distance of $+\infty$ in m_c, they have totally different behaviors and afford transitions with different labels. It is not difficult to verify that the distances between them are all $+\infty$ under every metric that the pLTS P_c satisfies ϵ-differential privacy on. That is, the distances between them are also $+\infty$ under the metric m_ϵ. Excluding these two kinds of pairs of states, we only need to check the distance between s_i^1 and s_j^2 and the distance between t_i^1 and t_j^2 in the infimum metric.

On the pair of s_i^1 and s_j^2, we can observe from Table 1 that they actually afford the transition with the same label and arrive at the same distribution. When we apply the observation to Definition 3.1, we have that μ_1 and μ_2 are the same distribution and $\mu_1(E)$ equals $\mu_2(E)$ for any set E of states, which shows that even though the distance between them is 0, the inequality still holds. This suggests that we should check whether the pLTS P_c satisfies ϵ-differential privacy on m_c', where m_c' is acquired from m_c by modifying the distance between s_i^1 and s_j^2 to 0. It is routine to check that the pLTS P_c indeed satisfies ϵ-differential privacy on m_c', and we do not go into the details here. So the distance between s_i^1 and s_j^2 in the infimum metric m_ϵ is 0. Then we look back to the behaviors of members in Crowds protocol. Although we assume two different kinds of members with coins of different probabilities, their behaviors are the same in the first step because when a member wants to send a message, she just selects a member randomly without tossing her coin. Since the states s_i^1 and s_j^2 denote that a member wants to send a message, it is not surprising that the distance between them in the infimum metric m_ϵ is 0.

On the pair of t_i^1 and t_j^2, we suppose that $m_\epsilon(t_i^1, t_j^2) = d$ for some $d < 2$. According to Theorem 4.2, if t_i^1 satisfies some formula F, then t_j^2 satisfies F_e constructed with ϵ and d. With the transitions in the pLTS P_c, we notice that $t_i^1 \vDash \langle c\rangle(\Box_p\langle d\rangle tt)$ iff $p > 1-p_1$ and $t_j^2 \vDash \langle c\rangle(\Box_{p'}\langle d\rangle tt)$ iff $p' > 1-p_2$. To make a contradiction, we set $p = (1-p_2)\cdot(\frac{1-p_1}{1-p_2})^{\frac{d}{2}}$. With $p_1 > p_2 > \frac{1}{2}$ and $d < 2$, we have that $\frac{1-p_1}{1-p_2} < 1$ and $p > (1-p_2)\cdot\frac{1-p_1}{1-p_2} = 1-p_1$, so $t_i^1 \vDash F = \langle c\rangle(\Box_p\langle d\rangle tt)$. Then we get the extension of F, $F^e = \langle c\rangle(\Box_{e^{\epsilon d}p}\langle d\rangle tt) = \langle c\rangle(\Box_{1-p_2}\langle d\rangle tt)$, which is not satisfied by t_j^2. This shows that $m_\epsilon(t_i^1, t_j^2) = d$ does not hold for any $d < 2$, so $m_\epsilon(t_i^1, t_j^2) = 2$. That is, the metric m_c' in the last paragraph is actually the infimum metric m_ϵ of the pLTS P_c, under the privacy parameter $\epsilon = \frac{1}{2}\ln\frac{1-p_2}{1-p_1}$.

6. Conclusion and future work

In this paper, we have proposed a formal framework for the analysis of differential privacy in the context of probabilistic systems. More specifically, based on the model of pLTSs, admitting both non-deterministic and probabilistic behavior, and a preset metric on its states, we have defined differential privacy by the probability difference of the distributions after the same labeled transitions of relevant states. We have explained how traditional differential privacy could be embedded in our framework and raised an infimum metric, the minimum distance between states, while not violating differential privacy. The infimum metric holds some desirable properties, such as the distance between states in the infimum metric is 0 iff they are probabilistic bisimilar. So, this metric can be regarded as a measure of the difference among equivalence classes of probabilistic bisimilarity. Moreover, the infimum metric is also a metric instance of differential privacy itself, so the work of characterizing differential privacy logically is carried out via this metric. We have developed a new two-level logic, called pHML, which is a privacy variant of the traditional HML logic. With this logic, we have initially characterized probabilistic bisimilarity after the construction of negation for each formula. In addition, we have proposed the extension of each formula, which is constructed with privacy and distance parameters. This extension enables us to characterize differential privacy. We have also succeeded to provide a method to measure the distance in the infimum metric with our pHML logic. Further, we have discussed a real case, an extended Crowds protocol with different behavior members. We have modeled this protocol with a pLTS, built a metric on its states, and investigated our concepts of differential privacy and infimum metric on this pLTS.

There are several problems worth further studying in our framework. First, we plan to extend some properties of the traditional differential privacy into our framework and discuss the relations to the computational differential privacy [42], where the adversary of system is computationally-bounded. Secondly, we are going to verify our notion of differential privacy in other existing systems, such as the mobile systems with noisy channels [43], the protocol of Mix Networks [44], and Onion Routing in anonymous network communications [45]. Lastly, as stated earlier in the paper, the deeper relation between our infimum metric and the metric extensions of probabilistic bisimilarity by Desharnais et al. [26–28] and an automated method to determine the distance in the infimum metric logically need further exploration.

Acknowledgments

The authors are very grateful to the anonymous reviewers for their invaluable suggestions. This work was supported by the National Natural Science Foundation of China (Grant Numbers 61370053, 61572003, and 61421091).

Appendix. Proofs in the paper

Proof of Proposition 3.1. For any pair (s_1, s_2) of states of P, such that $m(s_1, s_2) < +\infty$, and any transition label a, if $s_1 \xrightarrow{a} \mu_1$, according to that P satisfies ϵ-differential privacy on m, then there exists a transition $s_2 \xrightarrow{a} \mu_2$ such that $\mu_2(E) \leq e^{\epsilon m(s_1,s_2)}\mu_1(E)$ for any equivalence class E of $\mathcal{R}_m$. Since $\epsilon' \geq \epsilon$, we see that $\mu_2(E) \leq e^{\epsilon' m(s_1,s_2)}\mu_1(E)$, and thus P also satisfies ϵ'-differential privacy on m. □

Proof of Proposition 3.2. For any pair (s_1, s_2) of states of P, such that $(\alpha m)(s_1, s_2) < +\infty$, we also have that $m(s_1, s_2) < +\infty$. If $s_1 \xrightarrow{a} \mu_1$ for some transition label a and distribution μ_1, then there exists a transition $s_2 \xrightarrow{a} \mu_2$ such that $\mu_2(E) \leq e^{\epsilon m(s_1,s_2)}\mu_1(E)$ for any equivalence class E of $\mathcal{R}_m$. We observe that E is also an equivalence class of $\mathcal{R}_{\alpha m}$ and $\mu_2(E) \leq e^{(\frac{1}{\alpha}\epsilon)(\alpha m)(s_1,s_2)}\mu_1(E)$, so P satisfies $\frac{1}{\alpha}\epsilon$-differential privacy on αm. □

Proof of Proposition 3.3. For any two states s_1 and s_2 in the same equivalence class of $\mathcal{R}_m$, we have that $m(s_1, s_2) = 0$. If $s_1 \xrightarrow{a} \mu_1$ for some transition label a and distribution μ_1, then there exists a transition $s_2 \xrightarrow{a} \mu_2$ such that $\mu_2(E) \leq e^{\epsilon m(s_1,s_2)}\mu_1(E) = \mu_1(E)$ for any equivalence class E of $\mathcal{R}_m$. Since $\sum_E \mu_1(E) = \sum_E \mu_2(E) = 1$, we have that $\mu_2(E) = \mu_1(E)$ for any E. So, $\mathcal{R}_m$ is a probabilistic bisimulation. □

Proof of Proposition 3.4. According to Proposition 3.3, $\mathcal{R}_m$ is a probabilistic bisimulation, so any two states s_1 and s_2 in the same equivalence class of $\mathcal{R}_m$ are probabilistic bisimilar, that is, in the same equivalence class of $\mathcal{R}_\sim$. Consequently, any equivalence class E of $\mathcal{R}_\sim$ is a combination of several equivalence classes of $\mathcal{R}_m$. For any pair (s_1, s_2) of states of P, such that $m(s_1, s_2) < +\infty$, and any transition label a, if $s_1 \xrightarrow{a} \mu_1$, according to that P satisfies ϵ-differential privacy on m, there exists a transition $s_2 \xrightarrow{a} \mu_2$ such that $\mu_2(E_i) \leq e^{\epsilon m(s_1,s_2)}\mu_1(E_i)$ for any equivalence class E_i of $\mathcal{R}_m$. Considering any equivalence class E of $\mathcal{R}_\sim$,

$$\mu_2(E) = \sum_{\{E_i \text{ is a block of } E\}} \mu_2(E_i) \leq e^{\epsilon m(s_1,s_2)} \sum_{\{E_i \text{ is a block of } E\}} \mu_1(E_i) = e^{\epsilon m(s_1,s_2)}\mu_1(E),$$

as desired. This finishes the proof. □

Proof of Theorem 3.1. The "only if" direction is obvious, if we notice that P satisfies ϵ-differential privacy on p-metric defined in Definition 3.3.

Now, let us focus on the "if" direction. By contradiction, suppose that s and t are not probabilistic bisimilar. Then there must exist a transition $s \xrightarrow{a} \mu$ which has no corresponding transition $t \xrightarrow{a} \eta$.

Consider the set of distributions $\mathcal{D} = \{\eta \mid t \xrightarrow{a} \eta\}$. Since P is finitary, $\mathcal{D}$ is a finite set. We use η_i to range over $\mathcal{D}$. As a result of that no $t \xrightarrow{a} \eta$ is corresponding to $s \xrightarrow{a} \mu$, μ is not the same distribution with any η_i. However, $\sum_E \mu(E) = \sum_E \eta_i(E) = 1$, for all equivalence classes E of $\mathcal{R}_\sim$, so there must exist an equivalence classes E_i for each distribution η_i, such that $\eta_i(E_i) > \mu(E_i)$. We set a few variables r_i's as follows.

$$r_i = \begin{cases} \eta_i(E_i)/\mu(E_i) & \text{if } \mu(E_i) > 0, \\ 2 & \text{otherwise,} \end{cases}$$

and $r = \min_i r_i$. Clearly, $r > 1$ and for any distribution η_i, there exists an equivalence class E_i of $\mathcal{R}_\sim$, such that $\eta_i(E_i) \geq r\mu(E_i)$.

We continue to set $d = \frac{1}{\epsilon}\ln r$. Since $m_\epsilon(s, t) = 0$, there exists a metric m, such that $m(s, t) < d$ and P satisfies ϵ-differential privacy on m. So, for the transition $s \xrightarrow{a} \mu$, there exists a transition $t \xrightarrow{a} \eta$, such that

$$\eta(E_i) \leq e^{\epsilon m(s,t)}\mu(E_i) < e^{\epsilon d}\mu(E_i) = r\mu(E_i),$$

for any equivalence class E_i of $\mathcal{R}_\sim$. The first inequality is a result of Proposition 3.4. However, none of distributions in $\mathcal{D}$ satisfies this condition, so we get a contradiction. That is, s and t are probabilistic bisimilar.

We thus complete the proof of the theorem. □

In the proof of Corollary 3.1, we will use the result of Lemma 3.2, so we place the proof of Corollary 3.1 after the proof of Lemma 3.2.

Proof of Lemma 3.1. The idea in this proof is similar to that of the "if" direction of Theorem 3.1.

We first set $d = m_\epsilon(s,t)$. According to Theorem 3.1, if $d = 0$, then $s \sim t$. So m_p defined in Definition 3.3 is a metric as desired. If $d = +\infty$, then $s \nsim t$. So m_p is still a metric that we need.

If $d \in (0, +\infty)$, we also have that $s \nsim t$. We construct a metric m by slightly modifying m_p, setting $m(s,t) = m(t,s) = d$. Clearly, m is a metric and $\mathcal{R}_m = \mathcal{R}_\sim$. So any equivalence class E of $\mathcal{R}_m$ is also an equivalence class of $\mathcal{R}_\sim$.

By contradiction, suppose that no metric satisfies that the distance between s and t is d and P satisfies ϵ-differential privacy on it. So P does not satisfy ϵ-differential privacy on m. That is, there must exist a transition $s \xrightarrow{a} \mu$ which has no corresponding transition $t \xrightarrow{a} \eta$.

Consider the set of distributions $\mathcal{D} = \{\eta \mid t \xrightarrow{a} \eta\}$. Since P is finitary, $\mathcal{D}$ is a finite set. We use η_i to range over $\mathcal{D}$. As a result of that no $t \xrightarrow{a} \eta$ is corresponding to $s \xrightarrow{a} \mu$, there must exist an equivalence class E_i of $\mathcal{R}_m$, such that $\eta_i(E_i) > e^{\epsilon d}\mu(E_i)$, for each distribution η_i. We set a few variables r_i's as follows:

$$r_i = \begin{cases} \eta_i(E_i)/\mu(E_i) & \text{if } \mu(E_i) > 0, \\ e^{\epsilon d} + 1 & \text{otherwise,} \end{cases}$$

and $r = \min_i r_i$. Clearly, $r > e^{\epsilon d}$ and for any distribution η_i, there exists an equivalence class E_i of $\mathcal{R}_m$, such that $\eta_i(E_i) \geq r_i\mu(E_i) \geq r\mu(E_i)$.

We continue to set $d' = \frac{1}{\epsilon}\ln\frac{r+e^{\epsilon d}}{2}$. Obviously, $d < d' < \frac{1}{\epsilon}\ln r$. Since $m_\epsilon(s,t) = d$, there exists a metric m', such that $m'(s,t) < d'$ and P satisfies ϵ-differential privacy on m'. So, for the transition $s \xrightarrow{a} \mu$, there exists a transition $t \xrightarrow{a} \eta$, such that

$$\eta(E_i) \leq e^{\epsilon m'(s,t)}\mu(E_i) < e^{\epsilon d'}\mu(E_i) < r\mu(E_i),$$

for any equivalence class E_i of $\mathcal{R}_m$. The first inequality is a result of Proposition 3.4 and $\mathcal{R}_\sim = \mathcal{R}_m$. However, none of distributions in $\mathcal{D}$ satisfies this condition, so we get a contradiction. That is, there exists a metric m such that $m(s,t) = m_\epsilon(s,t)$ and P satisfies ϵ-differential privacy on m. □

Proof of Lemma 3.2. We can easily verify that $m_\epsilon(s,s) = 0$ and $m_\epsilon(s_1,s_2) = m_\epsilon(s_2,s_1) \geq 0$. It remains to check that m_ϵ satisfies the triangle inequality, that is, $m_\epsilon(s_1,s_2) + m_\epsilon(s_2,s_3) \geq m_\epsilon(s_1,s_3)$, for any states s_1, s_2, and s_3 of P.

Suppose that $m_\epsilon(s_1,s_2) = d_1$ and $m_\epsilon(s_2,s_3) = d_2$. Then there exist two metrics m_1 and m_2 such that $m_1(s_1,s_2) = d_1$, $m_2(s_2,s_3) = d_2$, and P satisfies ϵ-differential privacy on both m_1 and m_2, according to Lemma 3.1. We need to explain why $m_\epsilon(s_1,s_3) \leq d_1 + d_2$, which can be deduced by constructing a metric that satisfies this distance limit and P satisfies ϵ-differential privacy on it.

We construct a distance function m_3 as follows.

(1) Set $m_3(s,t) = \min\{m_1(s,t), m_2(s,t)\}$, for all pairs (s,t) of states.
(2) While there exist three states s_1, s_2, s_3, such that $m_3(s_1,s_3) > m_3(s_1,s_2) + m_3(s_2,s_3)$, set $m_3(s_1,s_3) = m_3(s_3,s_1) = m_3(s_1,s_2) + m_3(s_2,s_3)$.

Now, we will explain why this mechanism will eventually stop. After the first step, $m_3(s,t)$ has a value of real number or positive infinity, for each pair (s,t) of states. We select all the values of real numbers and construct a set S to involve them. Since P is a finitary pLTS, the set S is also a finite set. According to the update rule of the second step, the updated distance between states s and t must be the sum of some numbers in S. So the possible distances between s and t are only finitely many (at most the size of the power set of S). Furthermore, the distance is updated in descending order, so there are only finitely many steps to update the distance between s and t. When we consider all the pairs of states, this still holds, so the mechanism will always stop after finitely many steps.

When this mechanism stops, it produces a metric m_3 which satisfies

$$m_3(s_1,s_3) \leq m_3(s_1,s_2) + m_3(s_2,s_3) \leq m_1(s_1,s_2) + m_2(s_2,s_3) = d_1 + d_2.$$

That is, we only need to show that P satisfies ϵ-differential privacy on m_3.

Consider two states s,t such that $m_3(s,t)$ is a real number. If $m_3(s,t)$ is not updated in the second step, then $m_3(s,t) = \min\{m_1(s,t), m_2(s,t)\}$. Without loss of generality, suppose that $m_3(s,t) = m_1(s,t)$. Then, for any transition $s \xrightarrow{a} \mu$, there exists a transition $t \xrightarrow{a} \eta$, such that $\eta(E_1) \leq e^{\epsilon m_1(s,t)}\mu(E_1)$, for any equivalence class E_1 of $\mathcal{R}_{m_1}$, according to that P satisfies ϵ-differential privacy on m_1. For any two states s', t' in the same E_1, $m_1(s',t') = 0$, and we have that $m_3(s',t') = 0$ according to the first step of the previous algorithm. That is, any equivalence class E_3 of $\mathcal{R}_{m_3}$ is a combination of several equivalence classes of $\mathcal{R}_{m_1}$. So $\mu(E_3) = \sum_i \mu(E_{1i})$ and $\eta(E_3) = \sum_i \eta(E_{1i})$, where E_{1i}'s are all equivalence classes of $\mathcal{R}_{m_1}$. Consequently,

$$\eta(E_3) = \sum_i \eta(E_{1i}) \leq \sum_i e^{\epsilon m_1(s,t)}\mu(E_{1i}) = e^{\epsilon m_3(s,t)} \sum_i \mu(E_{1i}) = e^{\epsilon m_3(s,t)}\mu(E_3),$$

for any equivalence class E_3 of $\mathcal{R}_{m_3}$.

If $m_3(s,t)$ is updated in the second step, then suppose that $m_3(s,t)$ is last updated by $m_3(s,r)+m_3(r,t)$. Obviously, $m_3(s,r)$ and $m_3(r,t)$ will not be updated any more. For any transition $s \xrightarrow{a} \mu_s$, we can deduce, by induction on the last-update time of pairs of states, that there exist two transitions $r \xrightarrow{a} \mu_r$ and $t \xrightarrow{a} \mu_t$, such that $\mu_r(E_3) \le e^{\epsilon m_3(s,r)}\mu_s(E_3)$ and $\mu_t(E_3) \le e^{\epsilon m_3(r,t)}\mu_r(E_3)$. Consequently,

$$\mu_t(E_3) \le e^{\epsilon(m_3(r,t)+m_3(s,r))}\mu_s(E_3) = e^{\epsilon m_3(s,t)}\mu_s(E_3),$$

for any equivalence class E_3 of $\mathcal{R}_{m_3}$.

Thus, P satisfies ϵ-differential privacy on m_3. So, m_ϵ satisfies the triangle inequality. □

Proof of Corollary 3.1. Combining Theorem 3.1 and Lemma 3.2, we can immediately get that $m_\epsilon(s_2,s_1)=0$ and $m_\epsilon(s_2,t_1) \le m_\epsilon(s_2,s_1)+m_\epsilon(s_1,t_1)$, so $m_\epsilon(s_2,t_1) \le m_\epsilon(s_1,t_1)$. Similarly, $m_\epsilon(s_1,t_1) \le m_\epsilon(s_2,t_1)$, which results in that $m_\epsilon(s_2,t_1) = m_\epsilon(s_1,t_1)$. In the same way, $m_\epsilon(s_2,t_1) = m_\epsilon(s_2,t_2)$, which yields that $m_\epsilon(s_1,t_1) = m_\epsilon(s_2,t_2)$, finishing the proof. □

Proof of Theorem 3.2. Given two states s and t, such that $m_\epsilon(s,t) < +\infty$, there exists a metric m such that $m(s,t) = m_\epsilon(s,t)$, and P satisfies ϵ-differential privacy on m, according to Lemma 3.1. So, for any transition $s \xrightarrow{a} \mu$, there exists another transition $t \xrightarrow{a} \eta$, such that $\eta(E_m) \le e^{\epsilon m(s,t)}\mu(E_m)$, for any equivalence class E_m of $\mathcal{R}_m$.

On the other hand, if $m(s_1,s_2)=0$ for two states s_1 and s_2, then $m_\epsilon(s_1,s_2)=0$ by the definition of m_ϵ. That is, any equivalence class E_ϵ of $\mathcal{R}_{m_\epsilon}$ is a combination of several equivalence classes of $\mathcal{R}_m$. So $\mu(E_\epsilon) = \sum_i \mu(E_{mi})$ and $\eta(E_\epsilon) = \sum_i \eta(E_{mi})$, where E_{mi}'s are all equivalence classes of $\mathcal{R}_m$. Consequently,

$$\eta(E_\epsilon) = \sum_i \eta(E_{mi}) \le \sum_i e^{\epsilon m(s,t)}\mu(E_{mi}) = e^{\epsilon m_\epsilon(s,t)} \sum_i \mu(E_{mi}) = e^{\epsilon m_\epsilon(s,t)}\mu(E_\epsilon),$$

for any equivalence class E_ϵ of $\mathcal{R}_{m_\epsilon}$.

Thus, P also satisfies ϵ-differential privacy on m_ϵ. □

Proof of Lemma 4.1. We first prove the claim

$$\mu \vDash \varphi \text{ iff } \mu \nvDash \varphi^c$$

by the structural induction on φ, where μ is a distribution over the states of the pLTS and φ is a φ-formula. We omit the cases that $\varphi = tt, ff, \varphi_1 \vee \varphi_2$, and $\Box_p F$, and give detailed proofs for the following two cases.

- Case 1: $\varphi = \varphi_1 \wedge \varphi_2$ and $\varphi^c = \varphi_1^c \vee \varphi_2^c$. Supposing that $\mu \nvDash \varphi^c$, we have that $\mu \nvDash \varphi_1^c$ and $\mu \nvDash \varphi_2^c$, which leads to that $\mu \vDash \varphi_1$ and $\mu \vDash \varphi_2$, so $\mu \vDash \varphi_1 \wedge \varphi_2 = \varphi$. Conversely, there is no difficult to verify that $\mu \nvDash \varphi^c$ from $\mu \vDash \varphi$.
- Case 2: $\varphi = \Diamond_p F$ and $\varphi^c = \Box_p F$. For the two formulae, we have that $\mu \vDash \varphi$ iff $\sum_{s \vDash F} \mu(s) \ge p$ and $\mu \vDash \varphi^c$ iff $\sum_{s \vDash F} \mu(s) < p$. So we can easily get that $\mu \vDash \varphi$ iff $\mu \nvDash \varphi^c$.

Now, we prove this lemma by the structural induction on F. We omit the cases that $F = tt, ff$, $F_1 \wedge F_2$, and $F_1 \vee F_2$, and give detailed proofs for the following two cases.

- Case 1: $F = \langle a \rangle \varphi$ and $F^c = [a]\varphi^c$. This leads to that $s \vDash F^c$ iff for any distribution μ, $s \xrightarrow{a} \mu$ results $\mu \vDash \varphi^c$. Consequently, $s \nvDash F^c$ iff there exists a distribution μ, such that $s \xrightarrow{a} \mu$ and $\mu \nvDash \varphi^c$ iff there exists a distribution μ, such that $s \xrightarrow{a} \mu$ and $\mu \vDash \varphi$ iff $s \vDash \langle a \rangle \varphi = F$.
- Case 2: $F = [a]\varphi$ and $F^c = \langle a \rangle \varphi^c$. This leads to that $s \vDash F^c$ iff there exists a distribution μ, such that $s \xrightarrow{a} \mu$ and $\mu \vDash \varphi^c$. Consequently, $s \nvDash F^c$ iff for any distribution μ, $s \xrightarrow{a} \mu$ results $\mu \nvDash \varphi^c$ iff for any distribution μ, $s \xrightarrow{a} \mu$ results $\mu \vDash \varphi$ iff $s \vDash [a]\varphi = F$.

Thus, this lemma is proven. □

Proof of Theorem 4.1. We first prove the "only if" direction. We prove the following two claims by the structural induction on F and φ.

$$\begin{cases} \text{If } s_1 \sim s_2 \text{ and } s_1 \vDash F, \text{ then } s_2 \vDash F; \\ \text{If } \mu_1(E) = \mu_2(E) \text{ for all } E \text{ and } \mu_1 \vDash \varphi, \text{ then } \mu_2 \vDash \varphi; \end{cases}$$

where F is an F-formula, φ is a φ-formula, and E is an equivalence class of $\mathcal{R}_\sim$.

We omit the cases that $F = tt, ff$, $F_1 \vee F_2$, $F_1 \wedge F_2$ and $\varphi = tt, ff$, $\varphi_1 \wedge \varphi_2$, $\varphi_1 \vee \varphi_2$, $\Box_p F$, and give detailed proofs for the following three cases.

- Case 1: $F = \langle a\rangle\varphi$. Since $s_1 \vDash F$, there exists a distribution μ_1, such that $s_1 \xrightarrow{a} \mu_1$ and $\mu_1 \vDash \varphi$. According to $s_1 \sim s_2$, there exists a distribution μ_2, such that $s_2 \xrightarrow{a} \mu_2$ and $\mu_2(E) = \mu_1(E)$ for any equivalence class E of $\mathcal{R}_\sim$. By induction, $\mu_2 \vDash \varphi$, so $s_2 \vDash \langle a\rangle\varphi = F$.
- Case 2: $F = [a]\varphi$. We consider a distribution μ_2, which satisfies $s_2 \xrightarrow{a} \mu_2$. According to $s_1 \sim s_2$, there exists a distribution μ_1, such that $s_1 \xrightarrow{a} \mu_1$ and $\mu_1(E) = \mu_2(E)$ for any equivalence class E of $\mathcal{R}_\sim$. Since $s_1 \vDash F = [a]\varphi$, we have that $\mu_1 \vDash \varphi$. By induction, $\mu_2 \vDash \varphi$, so $s_2 \vDash [a]\varphi = F$.
- Case 3: $\varphi = \Diamond_p F$. By induction, for this F and two states s_1, s_2 in the same equivalence class E of $\mathcal{R}_\sim$, $s_1 \vDash F$ iff $s_2 \vDash F$. So for any distribution μ, we have that $\sum_{s\vDash F}\mu(s) = \sum_{\{E|s\vDash F, \text{ for some } s\in E\}}\mu(E)$. Since $\mu_1(E) = \mu_2(E)$ for any equivalence class E, we have $\sum_{s\vDash F}\mu_1(s) = \sum_{s\vDash F}\mu_2(s)$. According to $\mu_1 \vDash \varphi = \Diamond_p F$, we have that $\sum_{s\vDash F}\mu_1(s) \geq p$, so $\sum_{s\vDash F}\mu_2(s) \geq p$, which results in that $\mu_2 \vDash \Diamond_p F = \varphi$.

Thus, the "only if" direction, as the first claim, is proven.

Now, let us focus on the "if" direction. First we construct a relation $\mathcal{R}$ on the states of P:

$$\mathcal{R} = \{(s,t) \mid s \text{ and } t \text{ satisfy the same formulae}\}.$$

Obviously, $\mathcal{R}$ is an equivalence relation and it is sufficient for us to prove that $\mathcal{R}$ is a probabilistic bisimulation.

Set $S/\mathcal{R} = \{E_1, E_2, \ldots, E_n\}$, where E_i's are all equivalence classes of $\mathcal{R}$. For any two equivalence classes E_i and E_j, they satisfy different formulae, so there must exist a formula F_{ij}, such that $E_i \vDash F_{ij}$, while $E_j \nvDash F_{ij}$. If F_{ij} is satisfied by E_j, not by E_i, then F_{ij}^c is a formula that we need. (Since the states in E_i share the same formulae, we use $E_i \vDash F$ to simply express that $s \vDash F$ for some $s \in E_i$.) For equivalence class E_i, we set $F_i = \wedge_{j\neq i} F_{ij}$. Clearly, F_i is satisfied by E_i, but not by any other equivalence class E_j.

Let us focus on the relation $\mathcal{R}$ again. Given $(s,t) \in R$ and $s \xrightarrow{a} \mu$, we set $p_i = \mu(E_i)$ for each equivalence class E_i, so $s \vDash \langle a\rangle(\wedge_i \Diamond_{p_i} F_i)$. Since s and t satisfy the same formulae, we have that $t \vDash \langle a\rangle(\wedge_i \Diamond_{p_i} F_i)$, that is, there exists a distribution η, such that $t \xrightarrow{a} \eta$ and $\eta \vDash \wedge_i \Diamond_{p_i} F_i$. Setting $q_i = \eta(E_i)$, we get that $q_i \geq p_i$ for each equivalence class E_i, because F_i is only satisfied by E_i. On the other hand, $\sum_i p_i = \sum_i q_i = 1$, which results that $q_i = p_i$, that is, $\mu(E_i) = \eta(E_i)$ for any equivalence class E_i of $\mathcal{R}$. So $\mathcal{R}$ is a probabilistic bisimulation.

Thus, any pair of states in $\mathcal{R}$, including (s_1, s_2), is probabilistic bisimilar and the "if" direction is also proven. □

Proof of Proposition 4.1. We first prove the second assertion by the structural induction on φ and the third assertion can be proven in the similar way. We omit the cases that $\varphi = tt$, ff, $\varphi_1 \wedge \varphi_2$, and $\varphi_1 \vee \varphi_2$, and give detailed proofs for the following two cases.

- Case 1: $\varphi = \Diamond_p F$. Since $\mu \vDash \varphi$, we have that $\sum_{s\vDash F}\mu(s) \geq p \geq 1 - e^{\epsilon d}(1-p)$. So, $\mu \vDash \Diamond_{1-e^{\epsilon d}(1-p)} F = \varphi^{e_1}$.
- Case 2: $\varphi = \Box_p F$. Since $\mu \vDash \varphi$, we have that $\sum_{s\vDash F}\mu(s) < p \leq e^{\epsilon d} p$. So, $\mu \vDash \Box_{e^{\epsilon d} p} F = \varphi^{e_1}$.

Then, we prove the first assertion by the structural induction on F. We omit the cases that $F = tt$, ff, $F_1 \wedge F_2$, and $F_1 \vee F_2$, and give detailed proofs for the following two cases.

- Case 1: $F = \langle a\rangle\varphi$. Since $s \vDash F$, there exists a distribution μ, such that $s \xrightarrow{a} \mu$ and $\mu \vDash \varphi$. According to the second assertion, $\mu \vDash \varphi^{e_1}$. Consequently, $s \vDash \langle a\rangle\varphi^{e_1} = F^e$.
- Case 2: $F = [a]\varphi$. Since $s \vDash F$, for any distribution μ, $s \xrightarrow{a} \mu$ results $\mu \vDash \varphi$. According to the third assertion, $\mu \vDash \varphi^{e_2}$. Consequently, $s \vDash [a]\varphi^{e_2} = F^e$.

Thus, three assertions of this proposition are all proven. □

Proof of Lemma 4.2. We prove the first assertion by the structural induction on φ and omit the proof of the second assertion. For the cases that $\varphi = tt$, ff, $\varphi_1 \wedge \varphi_2$, and $\varphi_1 \vee \varphi_2$, the proofs are trivial.

- Case 1: $\varphi = \Diamond_p F$. We first divide all the equivalence classes of $\mathcal{R}_\sim$ by whether they satisfy F:

  $$E_1, E_2, \ldots, E_j \vDash F,$$
  $$E_{j+1}, E_{j+2}, \ldots, E_n \nvDash F.$$

  So, for any distribution μ, $\sum_{s\vDash F}\mu(s) = \sum_{i=1}^{j}\mu(E_i)$.
  Focusing on μ_1 and μ_2, we have that

  $$\sum_{i=1}^{j}\mu_2(E_i) = 1 - \sum_{i=j+1}^{n}\mu_2(E_i)$$

$$\geq 1 - \sum_{i=j+1}^{n} e^{\epsilon d}\mu_1(E_i)$$

$$= 1 - e^{\epsilon d}(1 - \sum_{i=1}^{j} \mu_1(E_i))$$

$$= 1 - e^{\epsilon d} + e^{\epsilon d} \sum_{i=1}^{j} \mu_1(E_i),$$

that is, $\sum_{s\vDash F} \mu_2(s) \geq 1 - e^{\epsilon d} + e^{\epsilon d} \sum_{s\vDash F} \mu_1(s)$. Since $\mu_1 \vDash \varphi = \Diamond_p F$, we see that $\sum_{s\vDash F} \mu_1(s) \geq p$, which leads to that $\sum_{s\vDash F} \mu_2(s) \geq 1 - e^{\epsilon d} + e^{\epsilon d} p$. Consequently, $\mu_2 \vDash \Diamond_{1-e^{\epsilon d}(1-p)} F = \varphi^{e_1}$.

- Case 2: $\varphi = \Box_p F$. Since $\mu_1 \vDash \varphi$, we obtain that $\sum_{s\vDash F} \mu_1(s) < p$, which leads to that $\sum_{s\vDash F} \mu_2(s) = \sum_{i=1}^{j} \mu_2(E_i) \leq \sum_{i=1}^{j} e^{\epsilon d}\mu_1(E_i) = e^{\epsilon d} \sum_{s\vDash F} \mu_1(s) < pe^{\epsilon d}$. So $\mu_2 \vDash \Box_{e^{\epsilon d} p} F = \varphi^{e_1}$.

Thus, we have proven all the cases of the first assertion. □

Proof of Theorem 4.2. (1) ⇒ (2): We prove this assertion by the structural induction on F, and by symmetry, it is sufficient to prove that $s_1 \vDash F$ results in $s_2 \vDash F^e$. We omit the cases that $F = tt$, ff, $F_1 \wedge F_2$, and $F_1 \vee F_2$ here.

- Case 1: $F = \langle a\rangle\varphi$. Since $s_1 \vDash F$, there exists a distribution μ_1, such that $s_1 \xrightarrow{a} \mu_1$ and $\mu_1 \vDash \varphi$. According to Theorem 3.2, we know that P satisfies ϵ-differential privacy on m_ϵ, so there exists a distribution μ_2, such that $s_2 \xrightarrow{a} \mu_2$ and $\mu_2(E) \leq e^{\epsilon m_\epsilon(s_1,s_2)}\mu_1(E) \leq e^{\epsilon d}\mu_1(E)$, for any equivalence class E of $\mathcal{R}_{m_\epsilon}$. Noticing that E is also an equivalence class of $\mathcal{R}_\sim$, we have that $\mu_2 \vDash \varphi^{e_1}$, with the help of Lemma 4.2. Thus, $s_2 \vDash \langle a\rangle\varphi^{e_1} = F^e$.
- Case 2: $F = [a]\varphi$. We first consider all distributions μ_2's, such that $s_2 \xrightarrow{a} \mu_2$. According to Theorem 3.2, we know that P satisfies ϵ-differential privacy on m_ϵ, so for any distribution μ_2, there exists a distribution μ_1, such that $s_1 \xrightarrow{a} \mu_1$ and $\mu_1(E) \leq e^{\epsilon m_\epsilon(s_1,s_2)}\mu_2(E) \leq e^{\epsilon d}\mu_2(E)$, for any equivalence class E of $\mathcal{R}_{m_\epsilon}$. Since $s_1 \vDash F = [a]\varphi$, we see that $\mu_1 \vDash \varphi$. Noticing that E is also an equivalence class of $\mathcal{R}_\sim$, we have that $\mu_2 \vDash \varphi^{e_2}$, due to Lemma 4.2. Thus, $s_2 \vDash [a]\varphi^{e_2} = F^e$.

We finish the proof of this assertion.

(2) ⇒ (1): We start by considering the equivalence classes of probabilistic bisimilarity. Set $R_\sim = \{E_1, E_2, \ldots, E_n\}$. If s_1 and s_2 are in the same E_i, then s_1 and s_2 are probabilistic similar. By Theorem 3.1, $m_\epsilon(s_1, s_2) = 0 \leq d$.

If s_1 and s_2 are not in the same E_i, suppose that $s_1 \in E_1$ and $s_2 \in E_2$ without loss of generality. To prove that $m_\epsilon(s_1, s_2) \leq d$, it is sufficient to construct a metric such that the distance between s_1 and s_2 is d and P satisfies ϵ-differential privacy on it.

We construct a distance function m on states of P as follows,

$$m(s,t) = \begin{cases} 0 & \text{if } s,t \text{ are in the same } E_i, \\ d & \text{if either (i) } s \in E_1 \text{ and } t \in E_2 \text{ or (ii) } t \in E_1 \text{ and } s \in E_2, \\ +\infty & \text{otherwise.} \end{cases}$$

Obviously, m is a metric, $m(s_1, s_2) = d$, and $\mathcal{R}_m = \mathcal{R}_\sim = \{E_1, E_2, \ldots E_n\}$.

It remains to verify that P satisfies ϵ-differential privacy on m. Let s and t be two states, such that $m(s,t) < +\infty$.

- If s,t are in the same E_i, then $s \sim t$. For any transition $s \xrightarrow{a} \mu$, there exists a distribution η, such that $t \xrightarrow{a} \eta$ and $\eta(E_i) = \mu(E_i)$ for any equivalence class E_i. Immediately, it also holds that $\eta(E_i) \leq e^{\epsilon m(s,t)}\mu(E_i)$ for any equivalence class E_i.
- If $s \in E_1$ and $t \in E_2$, given a transition $s \xrightarrow{a} \mu$, we set $p_i = \mu(E_i)$. So $s \vDash \langle a\rangle(\wedge_i \Box_{r_i} F_i)$ if $r_i > p_i$, where F_i is a formula satisfied by E_i, but not satisfied by any other E_j for $j \neq i$. Such formulae F_i's can be constructed by the same way in the proof of the "if" direction of Theorem 4.1.
  Since s and s_1 are both in E_1, they are probabilistic bisimilar and accordingly satisfy the same formulae. Here, $s_1 \vDash \langle a\rangle(\wedge_i \Box_{r_i} F_i)$, which results in that $s_2 \vDash (\langle a\rangle(\wedge_i \Box_{r_i} F_i))^e = \langle a\rangle(\wedge_i \Box_{r_i} F_i)^{e_1} = \langle a\rangle(\wedge_i \Box_{r_i e^{\epsilon d}} F_i)$. Noticing that t and s_2 are both in E_2, we have that $t \vDash \langle a\rangle(\wedge_i \Box_{r_i e^{\epsilon d}} F_i)$.

  Consequently, there exists a distribution η such that $t \xrightarrow{a} \eta$ and $\eta \vDash \wedge_i \Box_{r_i e^{\epsilon d}} F_i$. Setting $q_i = \eta(E_i)$, we have that $q_i < r_i e^{\epsilon d}$. Let r_i be close to p_i and we will finally get that $q_i \leq p_i e^{\epsilon d}$, that is, $\eta(E_i) \leq \mu(E_i) e^{\epsilon m(s,t)}$ for any equivalence class E_i.
- For the case of $s \in E_2$ and $t \in E_1$, the proof is similar to that of the last case.

Putting these together, we find that P satisfies ϵ-differential privacy on m. That is, we have proven that $m_\epsilon(s_1, s_2) \leq m(s_1, s_2) = d$. □

Proof of Proposition 5.1. We can verify this proposition by checking the pairs of states with distance less than positive infinity in the metric m_c. However, we only discuss the pair (t_i^1, t_j^2) in this proof and omit the other pairs for their simplicities.

We first name the equivalence classes of $\mathcal{R}_{m_c}$:

$$E_1 = \{s\},$$
$$E_2 = \{s_1^1, \ldots, s_n^1\},$$
$$E_3 = \{s_1^2, \ldots, s_m^2\},$$
$$E_4 = \{t_1^1, \ldots, t_n^1\},$$
$$E_5 = \{t_1^2, \ldots, t_m^2\},$$
$$E_6 = \{t\}.$$

The transitions from t_i^1 and t_j^2 are $t_i^1 \xrightarrow{c} \mu_i$ and $t_j^2 \xrightarrow{c} \eta_j$, respectively. Further,

$$\mu_i(E_4) = \frac{n}{n+m}p_1, \mu_i(E_5) = \frac{m}{n+m}p_1, \mu_i(E_6) = 1 - p_1$$
$$\eta_j(E_4) = \frac{n}{n+m}p_2, \eta_j(E_5) = \frac{m}{n+m}p_2, \eta_j(E_6) = 1 - p_2.$$

Considering $m_c(t_i^1, t_j^2) = 2$ and $\epsilon = \frac{1}{2}\ln\frac{1-p_2}{1-p_1}$, it is sufficient to prove that $\mu_i(E) \leq \frac{1-p_2}{1-p_1}\eta_j(E)$ and $\eta_j(E) \leq \frac{1-p_2}{1-p_1}\mu_i(E)$ for any equivalence class E. We observe that $p_1 > p_2 > \frac{1}{2}$, leading to that $p_2(1-p_2) > p_1(1-p_1)$. Consequently, $\frac{1-p_2}{1-p_1} > \frac{p_1}{p_2} > \frac{p_2}{p_1} > \frac{1-p_1}{1-p_2}$, proving that $\mu_i(E) \leq \frac{1-p_2}{1-p_1}\eta_j(E)$ and $\eta_j(E) \leq \frac{1-p_2}{1-p_1}\mu_i(E)$ for any E. Thus, the pair (t_i^1, t_j^2) does not violate ϵ-differential privacy for $\epsilon = \frac{1}{2}\ln\frac{1-p_2}{1-p_1}$. □

References

[1] C.C. Aggarwal, P.S. Yu, A General Survey of Privacy-Preserving Data Mining Models and Algorithms, Springer, 2008.
[2] B.C.M. Fung, K. Wang, R. Chen, P.S. Yu, Privacy-preserving data publishing: a survey of recent developments, ACM Comput. Surv. 42 (4) (2010) 14:1–14:53.
[3] S. Hartung, A. Nichterlein, R. Niedermeier, O. Suchý, A refined complexity analysis of degree anonymization in graphs, Inf. Comput. 243 (2015) 249–262.
[4] A. Giurgiu, R. Guerraoui, K. Huguenin, A. Kermarrec, Computing in social networks, Inf. Comput. 234 (2014) 3–16.
[5] C. Dwork, Differential privacy, in: Proceedings of the 33rd International Colloquium on Automata, Languages and Programming, 2006, pp. 1–12.
[6] Y. Yang, Z. Zhang, G. Miklau, M. Winslett, X. Xiao, Differential privacy in data publication and analysis, in: Proceedings of the 2012 International Conference on Management of Data, 2012, pp. 601–606.
[7] C. Dwork, Differential privacy: a survey of results, in: Proceedings of the 5th International Conference on Theory and Applications of Models of Computation, 2008, pp. 1–19.
[8] C. Dwork, Differential privacy in new settings, in: Proceedings of the 21st Annual Symposium on Discrete Algorithms, 2010, pp. 174–183.
[9] C. Dwork, A. Roth, The algorithmic foundations of differential privacy, Found. Trends Theor. Comput. Sci. 9 (3–4) (2014) 211–407.
[10] Z. Huang, S. Kannan, The exponential mechanism for social welfare: private, truthful, and nearly optimal, in: Proceedings of the 53rd Annual Symposium on Foundations of Computer Science, 2012, pp. 140–149.
[11] F. McSherry, K. Talwar, Mechanism design via differential privacy, in: Proceedings of the 48th Annual Symposium on Foundations of Computer Science, IEEE, 2007, pp. 94–103.
[12] M. Hardt, A. Roth, Beating randomized response on incoherent matrices, in: Proceedings of the 44th Annual Symposium on Theory of Computing, ACM, 2012, pp. 1255–1268.
[13] R. Chen, B.C.M. Fung, B.C. Desai, N.M. Sossou, Differentially private transit data publication: a case study on the montreal transportation system, in: Proceedings of the 18th International Conference on Knowledge Discovery and Data Mining, 2012, pp. 213–221.
[14] W.H. Qardaji, W. Yang, N. Li, Differentially private grids for geospatial data, in: Proceedings of the 29th International Conference on Data Engineering, 2013, pp. 757–768.
[15] C. Task, C. Clifton, A guide to differential privacy theory in social network analysis, in: Proceedings of the 2012 International Conference on Advances in Social Networks Analysis and Mining, 2012, pp. 411–417.
[16] F.M. Naini, J. Unnikrishnan, P. Thiran, M. Vetterli, Privacy-preserving function computation by exploitation of friendships in social networks, in: Proceedings of the 2014 International Conference on Acoustics, Speech and Signal Processing, 2014, pp. 6250–6254.
[17] Y. Shin, K. Kim, Differentially private client-side data deduplication protocol for cloud storage services, J. Secur. Commun. Netw. 8 (12) (2015) 2114–2123.
[18] J. Reed, B.C. Pierce, Distance makes the types grow stronger: a calculus for differential privacy, in: Proceeding of the 15th International Conference on Functional Programming, ACM, 2010, pp. 157–168.
[19] M. Gaboardi, A. Haeberlen, J. Hsu, A. Narayan, B.C. Pierce, Linear dependent types for differential privacy, in: Proceeding of the 40th Annual Symposium on Principles of Programming Languages, 2013, pp. 357–370.
[20] M.C. Tschantz, D.K. Kaynar, A. Datta, Formal verification of differential privacy for interactive systems (extended abstract), Electron. Notes Theor. Comput. Sci. 276 (2011) 61–79.

[21] L. Xu, Modular reasoning about differential privacy in a probabilistic process calculus, in: Proceedings of the 7th International Symposium on Trustworthy Global Computing, 2012, pp. 198–212.
[22] L. Xu, K. Chatzikokolakis, H. Lin, Metrics for differential privacy in concurrent systems, in: Proceedings of the 34th International Conference on Formal Techniques for Distributed Objects, Components, and Systems, 2014, pp. 199–215.
[23] F. Bartels, A. Sokolova, E. de Vink, A hierarchy of probabilistic system types, Theor. Comput. Sci. 327 (1) (2004) 3–22.
[24] N. Trcka, S. Georgievska, Branching bisimulation congruence for probabilistic systems, Electron. Notes Theor. Comput. Sci. 220 (3) (2008) 129–143.
[25] M. Hennessy, R. Milner, Algebraic laws for nondeterminism and concurrency, J. ACM 32 (1) (1985) 137–161.
[26] J. Desharnais, V. Gupta, R. Jagadeesan, P. Panangaden, Metrics for Labeled Markov Systems, Lect. Notes Comput. Sci., vol. 1664, 1999.
[27] J. Desharnais, R. Jagadeesan, V. Gupta, P. Panangaden, The metric analogue of weak bisimulation for probabilistic processes, in: Proceedings of the 17th Symposium on Logic in Computer Science, 2002, pp. 413–422.
[28] J. Desharnais, V. Gupta, R. Jagadeesan, P. Panangaden, Metrics for labelled Markov processes, Theor. Comput. Sci. 318 (3) (2004) 323–354.
[29] P.M.B. Vitányi, Information distance in multiples, IEEE Trans. Inf. Theory 57 (4) (2011) 2451–2456.
[30] L. Aceto, A. Ingólfsdóttir, K.G. Larsen, J. Srba, Reactive Systems: Modelling, Specification and Verification, Cambridge University Press, 2007.
[31] K. Chatzikokolakis, M.E. Andrés, N.E. Bordenabe, C. Palamidessi, Broadening the scope of differential privacy using metrics, in: Proceedings of the 13th International Symposium on Privacy Enhancing Technologies, Springer, 2013, pp. 82–102.
[32] K.G. Larsen, A. Skou, Bisimulation through probabilistic testing, Inf. Comput. 94 (1) (1991) 1–28.
[33] A. Parma, R. Segala, Logical characterizations of bisimulations for discrete probabilistic systems, in: Proceedings of the 10th International Conference on Foundations of Software Science and Computational Structures, 2007, pp. 287–301.
[34] H. Hermanns, A. Parma, R. Segala, B. Wachter, L. Zhang, Probabilistic logical characterization, Inf. Comput. 209 (2) (2011) 154–172.
[35] M. Hennessy, Exploring probabilistic bisimulations, part I, Form. Asp. Comput. 24 (4–6) (2012) 749–768.
[36] B. Jonsson, W. Yi, K.G. Larsen, Probabilistic extensions of process algebras, in: Handbook of Process Algebra, 2001, pp. 685–710.
[37] R. Cleaveland, J. Parrow, B. Steffen, The concurrency workbench: a semantics-based tool for the verification of concurrent systems, ACM Trans. Program. Lang. Syst. 15 (1) (1993) 36–72.
[38] F. Moller, P. Stevens, The Edinburgh concurrency workbench (version 7), Laboratory for Foundations of Computer Science, University of Edinburgh, UK.
[39] R. Cleaveland, S. Sims, The NCSU concurrency workbench, in: Proceedings of the 8th International Conference on Computer Aided Verification, Springer, 1996, pp. 394–397.
[40] P.C. Kanellakis, S.A. Smolka, CCS expressions, finite state processes, and three problems of equivalence, in: Proceedings of the 2nd Annual ACM SIGACT-SIGOPS Symposium on Principles of Distributed Computing, ACM, 1983, pp. 228–240.
[41] M.K. Reiter, A.D. Rubin, Crowds: anonymity for web transactions, ACM Trans. Inf. Syst. Secur. 1 (1) (1998) 66–92.
[42] I. Mironov, O. Pandey, O. Reingold, S.P. Vadhan, Computational differential privacy, in: Proceedings of the 29th Annual International Cryptology Conference, 2009, pp. 126–142.
[43] Y. Cao, Reliability of mobile processes with noisy channels, IEEE Trans. Comput. 61 (9) (2012) 1217–1230.
[44] S. Zhioua, Analyzing anonymity attacks through noisy channels, Inf. Comput. 244 (2015) 76–112.
[45] K. Peng, Anonymous Communication Networks: Protecting Privacy on the Web, CRC Press, 2014.