

# Measuring the Effectiveness and the Fairness of Relation Hiding Systems

Andreas Pashalidis  
NEC Europe Ltd.  
Heidelberg, Germany  
Email: pashalidis@nw.neclab.de

**Abstract**—In this paper, we develop a framework for measuring the level of protection offered by relation hiding systems. The framework provides a uniform way to define a variety of privacy notions, including anonymity and unlinkability, by means of information-theoretic metrics. Moreover, based on the framework, a fairness metric for relation hiding systems is proposed. It is envisioned that, due to its generality, the framework will enable the analysis of privacy protecting systems in more detail, while the ability to measure a system’s fairness circumvents in some cases the need to evaluate the privacy level that is provided to individual users, thereby reducing the number of times the metrics need to be evaluated by a potentially significant factor.

## I. INTRODUCTION

It is often desirable to hide a relation. In an anonymous peer review system, for example, it is desirable to hide who has reviewed whose work. In a social network, it is sometimes desirable to hide who are whose friends. In the setting of anonymous communication, it is desirable to hide multiple relations, including who sent a message to whom, who received a message from whom, which messages have the same sender, and which messages have the same intended recipient.

In this paper, we develop a framework for measuring the opacity of a hidden relation, and propose a corresponding fairness metric. The framework enables one to ‘ask the right questions’ regarding the privacy protection that is provided by a system, and provides new insights into the relation among different privacy notions. It achieves this by providing information-theoretic metrics that measure how well a system hides (a) a relation on all elements in the system, (b) a relation with respect to only a subset of ‘interesting’ elements, and (c) a given predicate on a (hidden) relation, against an adversary with partial knowledge about the relation. It is envisioned that the framework will enable designers of privacy protecting systems to define the privacy notion(s) of interest to their systems, and to measure how well they are protected, and evaluators of privacy protecting systems to effectively analyse and compare different systems in terms of the privacy protection they offer. The ability to measure the fairness of a privacy protecting system may, on the other hand, have a positive impact on user acceptance. This is because, in some systems, users cannot obtain reliable feedback on their individual level of privacy. However, if the system they use has been shown to be ‘fair enough’ then they can be confident that their privacy is not significantly less well protected than

that of the ‘average’ user. If the system is also acceptable in terms of privacy protection, then users may be happy using it without being made aware of their individual level of privacy.

Due to the fact that our framework is agnostic to the adversary’s interaction with the system, it is furthermore straightforward to evaluate any given system in different adversarial models. Finally, the ability to measure the opacity of a predicate may prove useful in the design of interfaces that inform users about their individual level of privacy; using the metric proposed in this paper, it is not difficult to imagine intuitive *and* precise visualisations of the adversary’s uncertainty in answering ‘interesting’ questions such as ‘were these transactions initiated by the same user?’ or ‘is Bob a customer of Alice?’.

**Related Work:** The frameworks introduced in [1], [2] have certain commonalities with the framework presented in this paper; they support, for example, the specification of privacy notions against adversaries with partial knowledge. However, in the setting of the frameworks in [1], [2], any given privacy notion is either satisfied, or not satisfied. This is not true for framework presented in this paper, since it provides the tools to measure the extent to which any given privacy notion is satisfied (or not satisfied).

Other related work includes the literature on definitions and metrics for anonymity and unlinkability (e.g. [3]–[14]). From this literature it is evident that one is typically interested to measure multiple aspects of the protection of privacy that is provided by a system. For example, while [8], [12] introduce a way to measure the anonymity of a single element that is hidden in an ‘anonymity set’, [9] provides a metric for the anonymity that is provided by a system as a whole. Similarly, while [4] aims to measure the (un)linkability of the actions of an individual user, [10], [15] provide a metric for the overall (un)linkability provided by a system. In this paper, we do not aim to further diversify the already scattered landscape of privacy definitions and metrics. Instead, the framework proposed in this paper unifies some of the existing metrics under the umbrella of ‘relation hiding’, where anonymity and unlinkability are just two examples from a large universe of privacy notions.

Although it is sometimes claimed that ‘anonymity and unlinkability are technically the same property’ (see, for example, [16]), the application of our framework to these two

privacy notions demonstrates that they are, in fact, technically distinct.<sup>1</sup> Note that this is in line with previous findings (see, for example, sections 4.4 and 4.7 of [1]). In our framework, this distinction is made explicit by virtue of differing sets of candidate relations the adversary starts with. We also show that, for systems with at least three elements, it is not always possible to achieve the same level of protection for both notions – see Theorem 1.

The rest of this paper is organised as follows. The next section describes our framework and section III proposes a fairness metric for relation hiding systems. Section IV provides general definitions, metrics and numerical examples for unlinkability, anonymity and unrelateability, expressed in terms of relation hiding, and provides a proof that some anonymity instances on a set are not reducible to unlinkability instances on the same set. Finally, section V concludes.

## II. RELATION HIDING

Consider a set of elements  $S$  and the set of all binary relations over  $S$ , denoted  $\mathfrak{R} = \{R : R \subseteq S \times S\}$ .<sup>2</sup> In this paper, we consider the setting of a system that hides a particular relation, denoted the ‘target’ relation  $R_\tau \in \mathcal{R} \subseteq \mathfrak{R}$ , against an adversary that nevertheless tries to identify it. It is assumed that the adversary knows  $S$  and the set of ‘candidate’ relations  $\mathcal{R}$ , and that it tries to identify  $R_\tau$  through interaction with (or observation of) the system.<sup>3</sup> As a result of this interaction, the adversary, denoted by  $\mathcal{A}(\mathcal{R})$  in the sequel, assigns to each  $R \in \mathcal{R}$  a probability that  $R = R_\tau$ . We call the resulting probability distribution  $\mathcal{A}(\mathcal{R})$ ’s ‘view on  $\mathcal{R}$ ’ and use the entropy of this distribution [17] as a metric for the opaqueness of  $R_\tau$ . That is, the opaqueness of the relation  $R_\tau \in \mathcal{R}$  on the set of elements  $S$  against  $\mathcal{A}(\mathcal{R})$  is defined as

$$\mathcal{O}(\mathcal{A}(\mathcal{R})) = \sum_{R \in \mathcal{R}} \mathcal{H}(\Pr(R = R_\tau)),$$

where  $\Pr(R = R_\tau)$  refers to  $\mathcal{A}(\mathcal{R})$ ’s view on  $\mathcal{R}$  and  $\mathcal{H}(x)$  denotes the quantity  $-x \log_2(x)$ . Note that  $\mathcal{O}(\mathcal{A}(\mathcal{R}))$  measures the amount of information (in bits) that  $\mathcal{A}(\mathcal{R})$  still needs to obtain in order to identify  $R_\tau$ , i.e. in order to unambiguously establish the relation  $R_\tau$  over all elements in  $S$ . However, sometimes it is desirable to measure the amount of information that  $\mathcal{A}(\mathcal{R})$  has to obtain in order to establish the relation  $R_\tau$  on the elements *in a subset*  $S' \subseteq S$ . Establishing this may mean multiple things; we specify a set  $G = \{\triangleright, \triangleleft, \diamond, \circ\}$  of four potential goals that  $\mathcal{A}(\mathcal{R})$  may have in this respect, as follows.

<sup>1</sup>In the formalisations of [16], the adversary’s goal in a ‘full anonymity’ game is to identify one of only two users. This is sufficient as a privacy definition for the context of [16] (group signatures) because it, indeed, also guarantees unlinkability. However, in a real world system, the adversary is typically able to obtain additional information which may lead to a situation where breaching unlinkability is easier than breaching anonymity, or vice versa.

<sup>2</sup>In this paper, we restrict our attention to systems that hide a binary relation over a given set.

<sup>3</sup>We do not distinguish between passive and active adversaries.

- $\triangleright$ : Establish how the elements in  $S'$  are related to the elements in  $S$ . That is, for all  $(s_1, s_2) \in (S' \times S)$ , decide whether or not  $(s_1, s_2) \in R_\tau$ .
- $\triangleleft$ : Establish how the elements in  $S$  are related to the elements in  $S'$ . That is, for all  $(s_1, s_2) \in (S \times S')$ , decide whether or not  $(s_1, s_2) \in R_\tau$ .
- $\diamond$ : Establish both the above.
- $\circ$ : Establish how the elements in  $S'$  are related amongst themselves. That is, for all  $(s_1, s_2) \in (S' \times S')$ , decide whether or not  $(s_1, s_2) \in R_\tau$ .

Since these goals are distinct, the amount of information about  $R_\tau$  that  $\mathcal{A}(\mathcal{R})$  needs in order to achieve each of them may vary. In order to construct a metric for each goal, we define the following four notions of relation equivalence.

**Definition 1.** Two relations  $R_1, R_2 \in \mathfrak{R}$  are said to be outwards-equivalent (resp. inwards-equivalent, closed-equivalent) with respect to a subset  $S' \subseteq S$ , denoted  $R_1 \triangleright R_2$  (resp.  $R_1 \triangleleft R_2$ ,  $R_1 \circ R_2$ ), if and only if  $R_1 \cap (S' \times S) = R_2 \cap (S' \times S)$  (resp.  $R_1 \cap (S \times S') = R_2 \cap (S \times S')$ ,  $R_1 \cap (S' \times S') = R_2 \cap (S' \times S')$ ). Moreover,  $R_1, R_2$  are said to be totally equivalent with respect to  $S'$ , denoted  $R_1 \diamond R_2$ , if and only if  $R_1 \triangleright R_2$  and  $R_1 \triangleleft R_2$  with respect to  $S'$ .

Each of these four equivalence relations on  $\mathfrak{R}$ , which are induced by  $S'$ , corresponds to one of  $\mathcal{A}(\mathcal{R})$ ’s potential goals. In particular, outwards-equivalence, inwards-equivalence, total equivalence, and closed equivalence, correspond with  $\triangleright$ ,  $\triangleleft$ ,  $\diamond$ , and  $\circ$ , respectively. We denote these equivalence relations by  $\sim (S', \mathfrak{R}, g)$ , and the partitions they induce on  $\mathcal{R}$  by  $\mathcal{R}(S', \mathcal{R}, g)$ , where  $g \in G$  denotes  $\mathcal{A}(\mathcal{R})$ ’s corresponding goal. Note that, for all  $g \in G$ ,  $|\mathcal{R}(S', \mathcal{R}, g)| = |\mathcal{R}|$ , i.e. that, if  $S' = S$ , then each  $R \in \mathcal{R}$  constitutes an equivalence class in its own right, regardless of  $\mathcal{A}(\mathcal{R})$ ’s goal. Also note that  $|\mathcal{R}(S', \mathcal{R}, \diamond)| \geq |\mathcal{R}(S', \mathcal{R}, \cdot)|$ , i.e. that total equivalence implies all other equivalence types.

Establishing  $R_\tau$  over the elements in  $S'$  in the sense of  $g$  amounts to identifying the equivalence class  $\mathcal{R}' \in \mathcal{R}(S', \mathcal{R}, g)$  that contains  $R_\tau$ . We thus generalise the definition of opaqueness above, and introduce a definition for the *degree* of opaqueness of a relation, as follows.

**Definition 2.** The opaqueness of the relation  $R_\tau \in \mathcal{R}$  on the set of elements  $S$  against  $\mathcal{A}(\mathcal{R})$  with respect to a subset  $S' \subseteq S$  and a given goal  $g \in G$  is defined as

$$\mathcal{O}(\mathcal{A}(\mathcal{R}), S', g) = \sum_{\mathcal{R}' \in \mathcal{R}(S', \mathcal{R}, g)} \mathcal{H}\left(\sum_{R \in \mathcal{R}'} \Pr(R = R_\tau)\right).$$

**Definition 3.** The degree of opaqueness of the relation  $R_\tau \in \mathcal{R}$  with respect to a subset  $S' \subseteq S$  and a given goal  $g \in G$  against  $\mathcal{A}(\mathcal{R})$  is defined as

$$\mathcal{D}(\mathcal{A}(\mathcal{R}), S', g) = \frac{\mathcal{O}(\mathcal{A}(\mathcal{R}), S', g)}{\log_2(|\mathcal{R}(S', \mathcal{R}, g)|)}.$$

Note that, for all  $g_1, g_2 \in G$ , it holds that  $\mathcal{O}(\mathcal{A}(\mathcal{R}), S, g_1) = \mathcal{O}(\mathcal{A}(\mathcal{R}), S, g_2) = \mathcal{O}(\mathcal{A}(\mathcal{R}))$  and that  $\mathcal{D}(\mathcal{A}(\mathcal{R}), S, g_1) = \mathcal{D}(\mathcal{A}(\mathcal{R}), S, g_2) = \mathcal{O}(\mathcal{A}(\mathcal{R})) / \log_2(|\mathcal{R}|)$ . Therefore, for the

special case where  $S' = S$ , we use the short notation  $\mathcal{O}(\mathcal{A}(\mathcal{R}))$  and  $\mathcal{D}(\mathcal{A}(\mathcal{R}))$ .

$R_\tau$  is ‘optimally hidden’ with respect to  $S'$  and  $g$  if and only if  $\mathcal{D}(\mathcal{A}(\mathcal{R}), S', g) = 1$ , i.e. in the case where, according to  $\mathcal{A}(\mathcal{R})$ ’s view, it is equally likely that  $R_\tau$  is in any of the equivalence classes in  $\mathcal{R}(S', \mathcal{R}, g)$ . In other words, in order to unambiguously relate the elements in  $S'$  according to  $R_\tau$ ,  $\mathcal{A}(\mathcal{R})$  has to know  $\log_2(|\mathcal{R}(S', \mathcal{R}, g)|)$  bits of information about it.

*Remark 1.* The above metrics measure  $\mathcal{A}(\mathcal{R})$ ’s uncertainty in ‘fully’ relating the elements in  $S'$  according to  $g$  and  $R_\tau$ , i.e.  $\mathcal{A}(\mathcal{R})$ ’s uncertainty in identifying the ‘correct’ equivalence class in  $\mathcal{R}(S', \mathcal{R}, g)$ . However, since some equivalence classes may be significantly likelier than others, one may (also) be interested in the ‘worst’ case, i.e. in the probability of the most likely equivalence class, which is

$$\max_{\mathcal{R}' \in \mathcal{R}(S', \mathcal{R}, g)} \left( \sum_{R \in \mathcal{R}'} \Pr(R = R_\tau) \right).$$

However, while this information is indeed useful in some situations (see, for example, [14], [18]), it is not a measure of how well the relation is hidden since – quite simply – the likeliest equivalence class may not be the correct one.

*Remark 2.* One might be tempted to define the degree of opaqueness of  $R_\tau$  as the fraction  $\mathcal{O}_f/\mathcal{O}_i$  where  $\mathcal{O}_i$  and  $\mathcal{O}_f$  denote the initial and the final opaqueness of the hidden relation, respectively (representing the adversary’s ‘a priori’ and ‘a posteriori’ knowledge, respectively). However, if the adversary’s uncertainty has increased after its interaction with the system (see [19] for an example of such a situation), then  $\mathcal{O}_f/\mathcal{O}_i > 1$ , which is undesirable. In a similar line of thought, one might be tempted to define the degree of opaqueness of  $R_\tau$  as  $H(X|Y)/H(X)$ , where the random variables  $X$  and  $Y$  refer to the adversary’s a priori view on  $\mathcal{R}$  and its information gain from its interaction with the system, respectively, and  $H(X|Y)$  denotes equivocation [17]. However, although this expression always delivers a value between 0 and 1, and although it has been used to evaluate some systems (see, for example, [20]), it, too, is unsuitable for the purposes of our framework, mainly for the following two reasons. Firstly, it is only a statement on the average opaqueness of the hidden relation. In fact, it is the average value of  $\mathcal{O}_f/\mathcal{O}_i$ , over all possible values of  $Y$ . (This follows from the definition of  $H(X|Y)$ .) Secondly, due to the possibility that the adversary may start off with a different a priori view in each system, it cannot be used to compare different systems. By contrast, the metric in Definition 3, which follows the type of normalisation first proposed in [8], does not suffer from these drawbacks. That is, while it quantifies the degree of information leakage occurring in a given system, it is also suitable for comparing different systems because it rates them against the ideal system where the relation is optimally hidden.

Sometimes it is desirable to measure the amount of information that  $\mathcal{A}(\mathcal{R})$  has to obtain about  $R_\tau$  in order to evaluate  $L(R_\tau)$  for a given predicate  $L \in \mathcal{L}$ , where  $\mathcal{L} = \{L : L(R) \in$

$\{0, 1\}, R \in \mathcal{R}\}$ . We call this the ‘degree of opaqueness of  $L(R_\tau)$  against  $\mathcal{A}(\mathcal{R})$ ’ or, equivalently, the ‘degree of  $\mathcal{A}(\mathcal{R})$ ’s uncertainty about  $L(R_\tau)$ ’ and define it as follows.

**Definition 4.** The degree of  $\mathcal{A}(\mathcal{R})$ ’s uncertainty about  $L(R_\tau)$  is defined as

$$\mathcal{D}(\mathcal{A}(\mathcal{R}), L) = \sum_{b \in \{0, 1\}} \mathcal{H} \left( \sum_{R \in \mathcal{R}(L, b)} \Pr(R = R_\tau) \right),$$

where  $\mathcal{R}(L, b) = \{R \in \mathcal{R} : L(R) = b\}$ .

The best case from a privacy perspective, i.e. the case where  $\mathcal{D}(\mathcal{A}(\mathcal{R}), L) = 1$ , occurs if  $\mathcal{A}(\mathcal{R})$  has to obtain a full bit of information about  $R_\tau$  in order to evaluate  $L(R_\tau)$  i.e. if, in  $\mathcal{A}(\mathcal{R})$ ’s view,  $\Pr(L(R_\tau) = 0) = \Pr(L(R_\tau) = 1) = 1/2$ . Conversely, the worst case, i.e. the case where  $\mathcal{D}(\mathcal{A}(\mathcal{R}), L) = 0$ , occurs if  $\mathcal{A}(\mathcal{R})$  already has enough information about  $R_\tau$  in order to evaluate  $L(R_\tau)$  with certainty, i.e. if  $\Pr(L(R_\tau) = b) = 1$  for  $b \in \{0, 1\}$ .

Sometimes it is desirable to measure  $\mathcal{A}(\mathcal{R})$ ’s uncertainty about whether or not  $R_\tau$  has a given property with respect to a subset  $S' \subseteq S$ . Such a property is modelled by means of a ‘predicate function’  $f : \mathfrak{S} \rightarrow \mathcal{L}$ , where  $\mathfrak{S}$  denotes the power set of  $S$ . Measuring this uncertainty then amounts to evaluating  $\mathcal{D}(\mathcal{A}(\mathcal{R}), f(S'))$ .

### III. FAIRNESS

Consider a ‘set of subsets’  $\mathcal{S} \subseteq \mathfrak{S}$ . For a given goal  $g$ , the degree of opaqueness of the relation  $R_\tau$  of the elements in a subset  $S' \in \mathcal{S}$  against  $\mathcal{A}(\mathcal{R})$  may differ depending on  $S'$ . However, if the system hides  $R_\tau$  in a fair – with respect to the subsets in  $\mathcal{S}$  and the goal  $g$  – manner, then this should not happen; instead, it should hold that  $\mathcal{D}(\mathcal{A}(\mathcal{R}), S'_1, g) = \mathcal{D}(\mathcal{A}(\mathcal{R}), S'_2, g)$  for all  $S'_1, S'_2 \in \mathcal{S}$ . Moreover, as the differences between the degrees of opaqueness with respect to the different subsets grows, the manner in which the relation  $R_\tau$  is hidden becomes less fair. In other words, privacy (as expressed by  $\mathcal{D}(\mathcal{A}(\mathcal{R}), S', g)$ ) may be viewed as a resource of which, ideally, all  $S' \in \mathcal{S}$  should be provided a fair share. We propose using the ‘fairness index’ introduced in [21] for measuring the fairness of relation hiding systems. Note that, in the past, this metric has been used with different resource types, including bandwidth [22], throughput [23], and the number of served requests per unit time [24].

**Definition 5.** The fairness of a system that hides a relation  $R_\tau$  on a set of elements  $S$  from an adversary  $\mathcal{A}(\mathcal{R})$  is, with respect to a set of subsets  $\mathcal{S} \subseteq \mathfrak{S}$  and a goal  $g \in \mathcal{G}$ , defined as

$$\mathcal{F}(\mathcal{A}(\mathcal{R}), \mathcal{S}, g) = \frac{\left( \sum_{S' \in \mathcal{S}} \mathcal{D}(\mathcal{A}(\mathcal{R}), S', g) \right)^2}{|\mathcal{S}| \sum_{S' \in \mathcal{S}} \mathcal{D}(\mathcal{A}(\mathcal{R}), S', g)^2}$$

More generally, the amount of information that  $\mathcal{A}(\mathcal{R})$  has to obtain about  $R_\tau$  in order to evaluate a given predicate function  $f(S')$  on  $R_\tau$ , where  $S' \in \mathcal{S}$ , may differ depending on  $S'$ .

**Definition 6.** The fairness of a system that hides a relation  $R_\tau$  on a set of elements  $S$  from an adversary  $\mathcal{A}(\mathcal{R})$ , with respect to a set of subsets  $\mathcal{S} \subseteq \mathfrak{S}$  and a predicate function  $f$ , is defined as

$$\mathcal{F}(\mathcal{A}(\mathcal{R}), \mathcal{S}, f) = \frac{\left( \sum_{S' \in \mathcal{S}} \mathcal{D}(\mathcal{A}(\mathcal{R}), f(S')) \right)^2}{|\mathcal{S}| \sum_{S' \in \mathcal{S}} \mathcal{D}(\mathcal{A}(\mathcal{R}), f(S'))^2}$$

The overall fairness of a system is given by  $\mathcal{F}(\mathcal{A}(\mathcal{R}), \mathfrak{S}, \diamond)$  and the overall fairness of a system with respect to a predicate function  $f$  is given by  $\mathcal{F}(\mathcal{A}(\mathcal{R}), \mathfrak{S}, f)$ . See sections IV-A1 and IV-B1 for two fairness calculation examples.

Note that the fairness is based on the (normalised) degree of opaqueness; this is because it may hold that  $|S'_1| \neq |S'_2|$  for some  $S'_1, S'_2 \in \mathcal{S}$ . Also note that, using this fairness metric, one can calculate each individual's 'perception of fairness'. That is, it is possible to calculate how fairly the relation  $R_\tau$  is hidden 'from the point of view' of each  $S' \in \mathcal{S}$ . It is furthermore possible to 'tweak' the definition of what is considered to be fair, for example if certain subsets (e.g. paying users) are supposed to be granted more privacy than others. For the corresponding expressions and a discussion on the interpretation of the metric, the reader is referred to [21].

*Remark 3.* The minimum (degree of) opaqueness regarding the subsets of interest could also be regarded as a form of 'fairness', as it guarantees that no subset in  $\mathcal{S}$  is 'worse off' than this minimum. However, in order to see why the minimum degree of opaqueness is insufficient as a fairness metric, suppose that  $\mathcal{S} = \{S'_1, S'_2\}$ , and consider, for example, a system where  $\mathcal{D}(\mathcal{A}(\mathcal{R}), S'_1, g) = \mathcal{D}(\mathcal{A}(\mathcal{R}), S'_2, g) = 0.6$ , and a system where  $\mathcal{D}(\mathcal{A}(\mathcal{R}), S'_1, g) = 0.6$ , and  $\mathcal{D}(\mathcal{A}(\mathcal{R}), S'_2, g) = 0.8$ . Although both systems have the same minimum degree of opaqueness, the first system is clearly more fair than the second and the fairness index proposed above reflects this. The fact that the second system, although less fair, provides a better privacy to the subsets in  $\mathcal{S}$ , also demonstrates that fairness should always be evaluated in conjunction with the degree of privacy protection. Note that, overall, the first system may be preferable because of other reasons (e.g. better performance). For more detailed comparisons of the fairness metric above to other fairness metrics, including variance, coefficient of variation, and min-max ratio, the reader is referred to [21].

#### IV. EXAMPLE PRIVACY NOTIONS

This section provides definitions and numerical examples for the privacy notions of unlinkability, anonymity, and unrelateability, all in terms of relation hiding. We also sketch how each of these notions may be applied in practice.

##### A. Unlinkability

**Definition 7.** The unlinkability of the elements in a set  $S' \subseteq S$  against an adversary  $\mathcal{A}(\mathcal{R}_{li})$  is defined as  $\mathcal{O}(\mathcal{A}(\mathcal{R}_{li}), S', \circ)$ , and the degree of their unlinkability as  $\mathcal{D}(\mathcal{A}(\mathcal{R}_{li}), S', \circ)$ , where  $\mathcal{R}_{li}$  is the set of all equivalence relations over  $S$ .

Note that  $|\mathcal{R}(S', \mathcal{R}_{li}, \circ)| = B_{|S'|}$ , where  $B_{|S'|}$ , which is a Bell number [25], is given by

$$B_{n+1} = \sum_{k=0}^n \binom{n}{k} B_k \quad (1)$$

with  $B_0 = 1$  and that, if  $S' = S$ , then  $|\mathcal{R}(S', \mathcal{R}_{li}, \circ)| = B_{|S|}$  and the definition above reduces to the one introduced in [10]. Moreover, the definition of  $\mathcal{D}(\mathcal{A}(\mathcal{R}_{li}), S', \circ)$  above matches the definitions given in section 3.1 of [15], as corrected in appendix A.

$\mathcal{O}(\mathcal{A}(\mathcal{R}_{li}), S', \circ)$  measures  $\mathcal{A}(\mathcal{R}_{li})$ 's uncertainty in dividing the elements in  $S'$  into equivalence classes according to  $R_\tau$ . However, sometimes it is desirable to measure the amount of information that  $\mathcal{A}(\mathcal{R}_{li})$  has to obtain about  $R_\tau$  in order to *decide whether or not* the elements in  $S'$  are linked or unlinked. In the following, we define two notions of such linking, namely a weak one and a strong one, and one notion of unlinking. Note that  $\Pi_\tau$  denotes the partition of  $S$  that is induced by  $R_\tau$  and that we write  $s_1 \equiv_{\Pi_\tau} s_2$  if the elements  $s_1, s_2 \in S$  lie in the same equivalence class of  $\Pi_\tau$ , and  $s_1 \not\equiv_{\Pi_\tau} s_2$  otherwise.

**Definition 8.** The protection against weak linking of the elements in a set  $S' \subseteq S$  against an adversary  $\mathcal{A}(\mathcal{R}_{li})$  is defined as  $\mathcal{D}(\mathcal{A}(\mathcal{R}_{li}), f_{wl}(S'))$ , where  $f_{wl}(S') = L_{wl, S'} \in \mathcal{L}$ , and

$$L_{wl, S'} = \begin{cases} 1, & \text{if } \forall \{s_1, s_2\} \subseteq S', s_1 \equiv_{\Pi_\tau} s_2 \\ 0, & \text{otherwise.} \end{cases}$$

If  $\mathcal{D}(\mathcal{A}(\mathcal{R}_{li}), f_{wl}(S')) = 0$ , i.e. if the elements in  $S'$  are not protected against weak linking, then  $\mathcal{A}(\mathcal{R}_{li})$  can tell whether or not they are equivalent in  $\Pi_\tau$ . If they are equivalent, then  $\mathcal{A}(\mathcal{R}_{li})$  may still be uncertain about whether or not other elements, i.e. elements in  $S - S'$  are also equivalent with those in  $S'$  (the notion of strong linking, defined below, does not allow for such uncertainty). If, on the other hand, they are not equivalent, then  $\mathcal{A}(\mathcal{R}_{li})$  may still be uncertain about whether or not they all belong to different equivalence classes (the notion of unlinking, defined below, does not allow for such uncertainty).

**Definition 9.** The protection against strong linking of the elements in a set  $S' \subseteq S$  against an adversary  $\mathcal{A}(\mathcal{R}_{li})$  is defined as  $\mathcal{D}(\mathcal{A}(\mathcal{R}_{li}), f_{sl}(S'))$ , where  $f_{sl}(S') = L_{sl, S'} \in \mathcal{L}$ , and

$$L_{sl, S'} = \begin{cases} 1, & \text{if } S' \in \Pi_\tau \\ 0, & \text{otherwise.} \end{cases}$$

If  $\mathcal{D}(\mathcal{A}(\mathcal{R}_{li}), f_{sl}(S')) = 0$ , i.e. if the elements in  $S'$  are not protected against strong linking, then  $\mathcal{A}(\mathcal{R}_{li})$  can tell whether or not  $S'$  constitutes an equivalence class in  $\Pi_\tau$ . If it does, then this means that  $\mathcal{A}(\mathcal{R}_{li})$  not only knows that all elements in  $S'$  are equivalent, but also that no other elements, i.e. no elements in  $S - S'$ , are also equivalent with those in  $S'$ . Finally, we define a notion of unlinking.

**Definition 10.** The protection against (complete) unlinking of the elements in a set  $S' \subseteq S$  against an adversary  $\mathcal{A}(\mathcal{R}_{li})$  is

defined as  $\mathcal{D}(\mathcal{A}(\mathcal{R}_{\text{li}}), f_{\text{ul}}(S'))$ , where  $f_{\text{ul}}(S') = L_{\text{ul}, S'} \in \mathcal{L}$ , and

$$L_{\text{ul}, S'} = \begin{cases} 1, & \text{if } \forall \{s_1, s_2\} \subseteq S', s_1 \not\equiv_{\Pi_\tau} s_2 \\ 0, & \text{otherwise.} \end{cases}$$

If  $\mathcal{D}(\mathcal{A}(\mathcal{R}_{\text{li}}), f_{\text{ul}}(S')) = 0$ , i.e. if the elements in  $S'$  are not protected against unlinking, then  $\mathcal{A}(\mathcal{R}_{\text{li}})$  can tell whether or not each element in  $S'$  belongs to a different equivalence class. Note that  $L_{\text{sl}, S'} \Rightarrow L_{\text{wl}, S'} \Rightarrow \overline{L_{\text{ul}, S'}}$  and  $L_{\text{ul}, S'} \Rightarrow \overline{L_{\text{wl}, S'}} \Rightarrow \overline{L_{\text{sl}, S'}}$ .

*Practical Example 1.* As an example, consider the setting of anonymous transactions [26], and suppose that  $S = \{\alpha, \beta, \gamma, \delta\}$  is the set of transactions occurring in the system. The unlinkability metric above can be used to measure the unlinkability of these transactions, or any subset thereof (say, e.g.  $\{\alpha, \beta, \gamma\}$ ). In this respect, the metric is identical to the one introduced in [10], because, the one introduced in [10] can be used for subsets, too. However, measuring the protection against weak and strong linking, as well as against unlinking, is not possible with previous metrics. Note that, while some scenarios require protection against weak linking, for others protection against strong linking may suffice. A user of a pseudonym system [27], [28], for example, that uses one pseudonym for business purposes, and another one for private activities, is likely to require protection against weak linking because linking the two pseudonyms is undesirable, even if uncertainty remains as to whether or not other pseudonyms also belong to the user. As an example of a scenario where protection against strong linking may suffice, consider a user that regularly visits a news website that supports a certain political view. If an adversary can tell that different web sessions of that site originate from this user, then the system clearly does not provide protection against weak linking. However, the impact of this privacy breach may depend on whether or not the user can claim that he also regularly visits other websites, e.g. those in support of opposing political views, without the adversary knowing better. If the system provides protection against strong linking, then making such a claim remains possible, even if the user has never visited any such websites (as long as other users have).

Finally, we define the ‘effective fairness’ of an unlinkability-protecting system. Note that this can only be calculated if  $R_\tau$  is known.

**Definition 11.** The effective fairness of a system that protects the unlinkability of the elements in a set  $S$  against an adversary  $\mathcal{A}(\mathcal{R}_{\text{li}})$  is defined as  $\mathcal{F}(\mathcal{A}(\mathcal{R}_{\text{li}}), \Pi_\tau, \circ)$ , where  $\Pi_\tau$  denotes the partition of  $S$  that is induced by  $R_\tau$ .

1) *Numerical unlinkability example:* As an example, consider the set  $S = \{\alpha, \beta, \gamma, \delta\}$ .  $\mathcal{R}_{\text{li}}$  consists of  $B_{|S|} = 15$  relations shown in the table below. Note that, in a slight abuse of notation, each relation is depicted in terms of the partition it induces on the elements in  $S$ . The number after each relation  $R_i$  in the table represents the probability  $\Pr(R_i = R_\tau)$ , i.e.

the probability that, in  $\mathcal{A}(\mathcal{R}_{\text{li}})$ ’s view, the relation  $R_i$  is the target relation  $R_\tau$ .

$$\begin{array}{ll} R_1 = \{\{\alpha, \beta, \gamma, \delta\}\} & 02\% \quad R_8 = \{\{\alpha, \delta\}, \{\beta, \gamma\}\} & 05\% \\ R_2 = \{\{\alpha\}, \{\beta, \gamma, \delta\}\} & 15\% \quad R_9 = \{\{\alpha\}, \{\beta\}, \{\gamma, \delta\}\} & 16\% \\ R_3 = \{\{\beta\}, \{\alpha, \gamma, \delta\}\} & 15\% \quad R_{10} = \{\{\alpha\}, \{\gamma\}, \{\beta, \delta\}\} & 08\% \\ R_4 = \{\{\gamma\}, \{\alpha, \beta, \delta\}\} & 02\% \quad R_{11} = \{\{\alpha\}, \{\delta\}, \{\beta, \gamma\}\} & 02\% \\ R_5 = \{\{\delta\}, \{\alpha, \beta, \gamma\}\} & 02\% \quad R_{12} = \{\{\beta\}, \{\gamma\}, \{\alpha, \delta\}\} & 02\% \\ R_6 = \{\{\alpha, \beta\}, \{\gamma, \delta\}\} & 02\% \quad R_{13} = \{\{\beta\}, \{\delta\}, \{\alpha, \gamma\}\} & 02\% \\ R_7 = \{\{\alpha, \gamma\}, \{\beta, \delta\}\} & 10\% \quad R_{14} = \{\{\gamma\}, \{\delta\}, \{\alpha, \beta\}\} & 02\% \\ & & R_{15} = \{\{\alpha\}, \{\beta\}, \{\gamma\}, \{\delta\}\} & 15\% \end{array}$$

Based on the view above, the unlinkability of the elements in  $S$  is  $\mathcal{O}(\mathcal{A}(\mathcal{R}_{\text{li}})) \approx 3.40$  bits. This means that  $\mathcal{A}(\mathcal{R}_{\text{li}})$  still needs to obtain approximately 3.40 bits of information about  $R_\tau$  in order to divide all elements in  $S$  into non-overlapping groups according to  $R_\tau$ . As the theoretical maximum is  $\log_2(|B_S|) = \log_2(B_4) = \log_2(15) \approx 3.9$  bits, the degree of unlinkability of the elements in  $S$  is  $\mathcal{D}(\mathcal{A}(\mathcal{R}_{\text{li}})) \approx 0.87$ .

Next, we calculate the unlinkability of the elements in  $\{\alpha, \beta, \gamma\}$ . The equivalence relation  $\sim (\{\alpha, \beta, \gamma\}, \mathfrak{R}, \circ)$  divides  $\mathcal{R}_{\text{li}}$  into the following  $B_{|\{\alpha, \beta, \gamma\}|} = B_3 = 5$  equivalence classes.

	eq. class	condition
$\mathcal{R}_1$	$= \{R_1, R_5\}$	$\alpha \equiv \beta \equiv \gamma$
$\mathcal{R}_2$	$= \{R_2, R_8, R_{11}\}$	$\alpha \not\equiv \beta \equiv \gamma$
$\mathcal{R}_3$	$= \{R_3, R_7, R_{13}\}$	$\beta \not\equiv \alpha \equiv \gamma$
$\mathcal{R}_4$	$= \{R_4, R_6, R_{14}\}$	$\gamma \not\equiv \alpha \equiv \beta$
$\mathcal{R}_5$	$= \{R_9, R_{10}, R_{12}, R_{15}\}$	$\alpha \not\equiv \beta \not\equiv \gamma$

We now have that  $\mathcal{O}(\mathcal{A}(\mathcal{R}_{\text{li}}), \{\alpha, \beta, \gamma\}, \circ) = \mathcal{H}(4/100) + \mathcal{H}(22/100) + \mathcal{H}(27/100) + \mathcal{H}(6/100) + \mathcal{H}(41/100) \approx 1.947$  bits. As the theoretical maximum is  $\log_2(5) \approx 2.32$  bits,  $\mathcal{D}(\mathcal{A}(\mathcal{R}_{\text{li}}), \{\alpha, \beta, \gamma\}, \circ) \approx 0.84$ .

Next, we calculate the protection against weak linking for the elements in  $\{\alpha, \beta\}$ . Since  $f_{\text{wl}}(\{\alpha, \beta\})$  evaluates to 1 for the relations  $R_1, R_4, R_5$ , and  $R_6$ , and  $R_{14}$ , and to 0 for all other relations, we have  $\mathcal{D}(\mathcal{A}(\mathcal{R}_{\text{li}}), f_{\text{wl}}(\{\alpha, \beta\})) = \mathcal{H}(10/100) + \mathcal{H}(90/100) \approx 0.47$ ; this means that  $\mathcal{A}(\mathcal{R}_{\text{li}})$  still needs to obtain approximately 0.47 bits of information about  $R_\tau$  in order to decide whether or not  $\alpha$  and  $\beta$  are equivalent.

Next, we calculate the protection against strong linking for the elements  $\{\alpha, \beta\}$ . Since  $f_{\text{sl}}(\{\alpha, \beta\}) = 1$  only for the relations  $R_6$  and  $R_{14}$ , we have that  $\mathcal{D}(\mathcal{A}(\mathcal{R}_{\text{li}}), f_{\text{sl}}(\{\alpha, \beta\})) = \mathcal{H}(4/100) + \mathcal{H}(96/100) \approx 0.24$ ; this means that  $\mathcal{A}(\mathcal{R}_{\text{li}})$  still needs to obtain approximately 0.24 bits of information about  $R_\tau$  in order to decide whether or not  $\{\alpha, \beta\}$  constitutes an equivalence class in  $R_\tau$ .

Supposing that  $R_\tau$  is known, and that  $R_\tau = R_6$ , i.e. that  $\{\alpha, \beta\}$  and  $\{\gamma, \delta\}$  is the ‘correct’ way to divide the elements in  $S$  into non-overlapping groups, we calculate the effective fairness of the system that led to  $\mathcal{A}(\mathcal{R}_{\text{li}})$ ’s view:

$$\begin{aligned} & \mathcal{F}(\mathcal{A}(\mathcal{R}_{\text{li}}), \{\{\alpha, \beta\}, \{\gamma, \delta\}\}, \circ) \\ &= \frac{[\mathcal{H}(\frac{1}{10}) + \mathcal{H}(\frac{9}{10}) + \mathcal{H}(\frac{5}{10}) + \mathcal{H}(\frac{5}{10})]^2}{2[(\mathcal{H}(\frac{1}{10}) + \mathcal{H}(\frac{9}{10}))^2 + (\mathcal{H}(\frac{5}{10}) + \mathcal{H}(\frac{5}{10}))^2]} \approx 0.73 \end{aligned}$$

Note that  $\{\gamma, \delta\}$  enjoys a 100% degree of unlinkability, while the degree of unlinkability of  $\{\alpha, \beta\}$  is just about 47%. Thinking about (the degree of) unlinkability as a resource that the system shares between  $\{\alpha, \beta\}$  and  $\{\gamma, \delta\}$ , and since in this case (i.e. in the presence of  $\mathcal{A}(\mathcal{R}_{li})$ ) the system provides 147% of this resource to both subsets, absolute fairness would demand that both degrees are about 73.5%. However, as in fact  $\{\gamma, \delta\}$  enjoys slightly more than two thirds of this resource, while  $\{\alpha, \beta\}$  just about the remaining third, we have an effective fairness of 73%.

## B. Anonymity

This section defines anonymity in terms of a binary relation  $R_\tau$  on the elements in an ‘anonymity set’  $S$ . Similar to other instances of relation hiding, the adversary’s goal is to identify  $R_\tau$  from a set of relations in which it is hidden. Let us briefly describe the intuition behind this model.

It is assumed that the adversary knows as many ‘de-anonymising labels’ as there are elements in  $S$ . The labels represent the semantics of breaking the anonymity of the elements in  $S$ . There exists a one-to-one correspondence between the labels and the elements in  $S$ ; the adversary’s goal is to identify this correspondence. Consider, for example, the case where  $S$  contains the actions ‘stole fire’, ‘held the skies’ and ‘was blinded’, and the de-anonymising labels are the names ‘Atlas’, ‘Prometheus’, and ‘Polyphemus’.<sup>4</sup> The action ‘stole fire’, for example, is then anonymous if the adversary cannot tell whether the fire thief was Atlas, Prometheus, or Polyphemus. Moreover, the elements of the entire set  $S$  are anonymous as long as the adversary cannot associate all three actions with the name of their corresponding perpetrator (of course, if the adversary can associate some of them, then their anonymity is reduced).

In other words, given an ordering of the labels, the adversary’s goal is to find the matching permutation of  $S$ , where a permutation is said to ‘match’ a sequence of labels if the position of each of the elements in the permutation is identical to the position of the corresponding label in the sequence. Another way to think about this problem is as follows. Suppose that the adversary attaches to each element in  $S$  a de-anonymising label. (How this is done does not matter; it could be done, for example, randomly.) The adversary’s goal is now to determine, for each element  $s_1 \in S$ , the identity of the element  $s_2 \in S$  that carries the correct label for  $s_1$  (it could be that  $s_1 = s_2$  or that  $s_1 \neq s_2$ ). The binary relation  $R_\tau$  models exactly this mapping of elements to labels. If, for example,  $s_1$  is related to  $s_2$  according to  $R_\tau$ , then this means that  $s_2$  carries the label that corresponds to  $s_1$ . We now define anonymity in terms of a hidden binary relation.

**Definition 12.** The anonymity of the elements in a set  $S' \subseteq S$  against an adversary  $\mathcal{A}(\mathcal{R}_{an})$  is defined as  $\mathcal{O}(\mathcal{A}(\mathcal{R}_{an}), S', \triangleright)$  and the degree of their anonymity as  $\mathcal{D}(\mathcal{A}(\mathcal{R}_{an}), S', \triangleright)$ , where  $\mathcal{R}_{an} = \{\{(s, \pi(s)) : s \in S\} : \pi \text{ permutation of } S\}$ .

<sup>4</sup>It is assumed that it is known that each action corresponds to exactly one label.

Note that  $|\mathcal{R}(S', \mathcal{R}_{an}, \triangleright)| = |S|! / (|S| - |S'|)!$  and that, if  $S' = S$ , then  $|\mathcal{R}(S', \mathcal{R}_{an}, \triangleright)| = |\mathcal{R}_{an}| = |S|!$ , and the anonymity metric above reduces to the one in section 2 of [9]. Similarly, if  $|S'| = 1$ , then  $|\mathcal{R}(S', \mathcal{R}_{an}, \triangleright)| = |S|$  and the metric effectively reduces to the one introduced in [8], [12]. This means that our metric can be used to measure the overall anonymity provided by a system as well as the anonymity of individual elements.

Moreover, the fact that our metric enables one to measure the anonymity of the elements in any subset  $S' \subset S$ , enables one to make more targeted anonymity measurements. Note that such measurements are not possible by isolating  $S'$  from the rest of the system (for example, by applying the metric from [9] to  $S'$ ), because  $|\mathcal{R}(S', \mathcal{R}_{an}, \triangleright)|$  depends on *both*  $|S'|$  and  $|S|$ . Similarly, measuring the anonymity of each element in  $S'$  does not help in determining the anonymity of  $S'$  because  $\mathcal{O}(\mathcal{A}(\mathcal{R}_{an}), S', \triangleright) \leq \sum_{s \in S'} \mathcal{O}(\mathcal{A}(\mathcal{R}_{an}), \{s\}, \triangleright)$ , with equality only in the special case where the adversary assigns all elements in  $S'$  to labels in an independent manner. If an attack is deemed successful only if the anonymity of  $S'$  drops below a threshold, then the fact that the above is usually an inequality, makes single-element anonymity measurements irrelevant.

*Practical Example 2.* Consider, for example, the setting of a mix network [29] where  $S = \{\alpha, \beta, \gamma, \delta\}$  is the set of messages that leave the network in a particular time interval, and the de-anonymising labels are the IP addresses that injected messages into the network in this interval; both sets are available to a ‘global passive adversary’. Being able to measure the anonymity of the messages in, say,  $S' = \{\beta, \gamma\}$  is desirable because it may be the case that these (and only these) messages are destined to ‘interesting’ recipients, for example servers hosting politically controversial material. Moreover, if  $\mathcal{O}(\mathcal{A}(\mathcal{R}_{an}), S', \triangleright)$  drops below a certain threshold, then this event may trigger the process of identifying the users behind the affected IP addresses. Practical reasons may furthermore require that  $|S'| > n$  for some threshold  $n$ . For example, the budget required to identify the affected users and to crossexamine other evidence may only be approved if there is promising evidence that at least  $n$  ‘perpetrators’ will be identified;  $\mathcal{O}(\mathcal{A}(\mathcal{R}_{an}), S', \triangleright)$  dropping below a well-defined threshold would amount to such evidence.

We now show that some anonymity instances on a set are not reducible to any unlinkability instance on the same set. Although this is a somewhat trivial observation, it provides insight into the relation between these two privacy notions.

**Theorem 1.** *Some anonymity instances on a set  $S$  with at least three elements are not reducible to any unlinkability instance on that set.*

*Proof:* In order to reduce an anonymity instance on a set  $S$  to an unlinkability instance on the same set, it is necessary to provide a transformation of the adversary’s view on  $\mathcal{R}_{an}$  to a view on  $\mathcal{R}_{li}$  without loss of information. However, while  $\mathcal{R}_{an}$  contains  $|S|!$  relations,  $\mathcal{R}_{li}$  contains only  $B_{|S|}$

relations (see (1)). Since  $B_{|S|} < |S|!$  for all  $|S| > 2$  (by Lemma 1, see appendix A), there exist some views on  $\mathcal{R}_{\text{an}}$  where  $\mathcal{O}(\mathcal{A}(\mathcal{R}_{\text{an}})) > \log_2(B_{|S|})$ . These views contain more entropy than can be accommodated by a view on  $\mathcal{R}_{\text{li}}$ , and, therefore, there exists no way to transform any of these views to a view on  $\mathcal{R}_{\text{li}}$  without information loss. ■

*Remark 4.* While an adversary on unlinkability tries to divide the elements in a given set into non-overlapping groups (according to a hidden equivalence relation), an adversary on anonymity tries to permute the elements in a given set (according to a hidden ordering) such that they match a given sequence of labels. If an adversary is uncertain as to whether or not the elements in a set all represent different labels, then it should first group the elements into equivalence classes (which requires solving an unlinkability instance). Then each equivalence class can be given a different label and an anonymity instance can be solved on the set of equivalence classes. If this is done, then the requirement that each element must correspond to exactly one de-anonymising label is not violated, and the issues observed in [30] are circumvented.

1) *Numerical anonymity example:* As an example, consider the ‘anonymity set’  $S = \{\alpha, \beta, \gamma, \delta\}$ .  $\mathcal{R}_{\text{an}}$  consists of the  $|S|! = 4! = 24$  relations shown in the table below. The number after each relation  $R_i$  in the table represents the probability  $\Pr(R_i = R_\tau)$ , i.e. the probability that, in  $\mathcal{A}(\mathcal{R}_{\text{an}})$ ’s view,  $R_i$  is the target relation  $R_\tau$ .

$R_1$	$= \{(\alpha, \alpha), (\beta, \beta), (\gamma, \gamma), (\delta, \delta)\}$	0
$R_2$	$= \{(\alpha, \alpha), (\beta, \beta), (\gamma, \delta), (\delta, \gamma)\}$	0
$R_3$	$= \{(\alpha, \alpha), (\beta, \gamma), (\gamma, \beta), (\delta, \delta)\}$	0
$R_4$	$= \{(\alpha, \alpha), (\beta, \gamma), (\gamma, \delta), (\delta, \beta)\}$	0
$R_5$	$= \{(\alpha, \alpha), (\beta, \delta), (\gamma, \beta), (\delta, \gamma)\}$	0
$R_6$	$= \{(\alpha, \alpha), (\beta, \delta), (\gamma, \gamma), (\delta, \beta)\}$	0
$R_7$	$= \{(\alpha, \beta), (\beta, \alpha), (\gamma, \gamma), (\delta, \delta)\}$	0
$R_8$	$= \{(\alpha, \beta), (\beta, \alpha), (\gamma, \delta), (\delta, \gamma)\}$	0
$R_9$	$= \{(\alpha, \beta), (\beta, \gamma), (\gamma, \alpha), (\delta, \delta)\}$	0
$R_{10}$	$= \{(\alpha, \beta), (\beta, \gamma), (\gamma, \delta), (\delta, \alpha)\}$	1/6
$R_{11}$	$= \{(\alpha, \beta), (\beta, \delta), (\gamma, \alpha), (\delta, \gamma)\}$	0
$R_{12}$	$= \{(\alpha, \beta), (\beta, \delta), (\gamma, \gamma), (\delta, \alpha)\}$	1/6
$R_{13}$	$= \{(\alpha, \gamma), (\beta, \alpha), (\gamma, \beta), (\delta, \delta)\}$	0
$R_{14}$	$= \{(\alpha, \gamma), (\beta, \alpha), (\gamma, \delta), (\delta, \beta)\}$	0
$R_{15}$	$= \{(\alpha, \gamma), (\beta, \beta), (\gamma, \alpha), (\delta, \delta)\}$	0
$R_{16}$	$= \{(\alpha, \gamma), (\beta, \beta), (\gamma, \delta), (\delta, \alpha)\}$	1/6
$R_{17}$	$= \{(\alpha, \gamma), (\beta, \delta), (\gamma, \alpha), (\delta, \beta)\}$	0
$R_{18}$	$= \{(\alpha, \gamma), (\beta, \delta), (\gamma, \beta), (\delta, \alpha)\}$	1/6
$R_{19}$	$= \{(\alpha, \delta), (\beta, \alpha), (\gamma, \beta), (\delta, \gamma)\}$	0
$R_{20}$	$= \{(\alpha, \delta), (\beta, \alpha), (\gamma, \gamma), (\delta, \beta)\}$	0
$R_{21}$	$= \{(\alpha, \delta), (\beta, \beta), (\gamma, \alpha), (\delta, \gamma)\}$	0
$R_{22}$	$= \{(\alpha, \delta), (\beta, \beta), (\gamma, \gamma), (\delta, \alpha)\}$	1/6
$R_{23}$	$= \{(\alpha, \delta), (\beta, \gamma), (\gamma, \alpha), (\delta, \beta)\}$	0
$R_{24}$	$= \{(\alpha, \delta), (\beta, \gamma), (\gamma, \beta), (\delta, \alpha)\}$	1/6

According to this view, the anonymity of the elements in  $S$  is  $\mathcal{O}(\mathcal{A}(\mathcal{R}_{\text{an}})) \approx 2.58$  bits. This means that  $\mathcal{A}(\mathcal{R}_{\text{an}})$  still needs to obtain approximately 2.58 bits of information about  $R_\tau$  in order to de-anonymise all elements in  $S$ . As the theoretical

maximum is  $\log_2(|S|!) = \log_2(4!) = \log_2(24) \approx 4.56$  bits, the degree of anonymity of the elements in  $S$  is  $\mathcal{D}(\mathcal{A}(\mathcal{R}_{\text{an}})) \approx 0.56$ .

We now calculate the anonymity of the elements in  $S' = \{\beta, \gamma\}$ . The equivalence relation  $\sim (\{\beta, \gamma\}, \mathfrak{R}, \triangleright)$  divides  $\mathcal{R}_{\text{an}}$  into the following  $|S|!/(|S| - |S'|)! = 4!/(4 - 2)! = 12$  equivalence classes.

eq. class	condition
$\mathcal{R}_1$	$= \{R_{13}, R_{19}\} \quad (\beta, \alpha), (\gamma, \beta)$
$\mathcal{R}_2$	$= \{R_7, R_{20}\} \quad (\beta, \alpha), (\gamma, \gamma)$
$\mathcal{R}_3$	$= \{R_8, R_{14}\} \quad (\beta, \alpha), (\gamma, \delta)$
$\mathcal{R}_4$	$= \{R_{15}, R_{21}\} \quad (\beta, \beta), (\gamma, \alpha)$
$\mathcal{R}_5$	$= \{R_1, R_{22}\} \quad (\beta, \beta), (\gamma, \gamma)$
$\mathcal{R}_6$	$= \{R_2, R_{16}\} \quad (\beta, \beta), (\gamma, \delta)$
$\mathcal{R}_7$	$= \{R_9, R_{23}\} \quad (\beta, \gamma), (\gamma, \alpha)$
$\mathcal{R}_8$	$= \{R_3, R_{24}\} \quad (\beta, \gamma), (\gamma, \beta)$
$\mathcal{R}_9$	$= \{R_4, R_{10}\} \quad (\beta, \gamma), (\gamma, \delta)$
$\mathcal{R}_{10}$	$= \{R_{11}, R_{17}\} \quad (\beta, \delta), (\gamma, \alpha)$
$\mathcal{R}_{11}$	$= \{R_5, R_{18}\} \quad (\beta, \delta), (\gamma, \beta)$
$\mathcal{R}_{12}$	$= \{R_6, R_{12}\} \quad (\beta, \delta), (\gamma, \gamma)$

We now have that  $\mathcal{O}(\mathcal{A}(\mathcal{R}_{\text{an}}), \{\beta, \gamma\}, \triangleright) = \mathcal{H}(0) + \mathcal{H}(0) + \mathcal{H}(0) + \mathcal{H}(0) + \mathcal{H}(1/6) + \mathcal{H}(1/6) + \mathcal{H}(0) + \mathcal{H}(1/6) + \mathcal{H}(1/6) + \mathcal{H}(0) + \mathcal{H}(1/6) + \mathcal{H}(1/6) \approx 2.58$  bits. As the theoretical maximum is  $\log_2(12) \approx 3.58$  bits, the degree of anonymity of the elements  $\{\beta, \gamma\}$  is  $\mathcal{D}(\mathcal{A}(\mathcal{R}_{\text{an}}), \{\beta, \gamma\}, \triangleright) \approx 0.72$ .

Finally, we calculate the fairness of the system that led to  $\mathcal{A}(\mathcal{R}_{\text{an}})$ ’s view, with respect to all single-element subsets of  $S$ , i.e. with respect to  $\mathcal{S} = \{\{\alpha\}, \{\beta\}, \{\gamma\}, \{\delta\}\}$ . Proceeding as above, we have that  $\mathcal{D}(\mathcal{A}(\mathcal{R}_{\text{an}}), \{\alpha\}, \triangleright) \approx 0.79$ ,  $\mathcal{D}(\mathcal{A}(\mathcal{R}_{\text{an}}), \{\beta\}, \triangleright) \approx 0.79$ ,  $\mathcal{D}(\mathcal{A}(\mathcal{R}_{\text{an}}), \{\gamma\}, \triangleright) \approx 0.79$ , and  $\mathcal{D}(\mathcal{A}(\mathcal{R}_{\text{an}}), \{\delta\}, \triangleright) = 0$ . Therefore,

$$\mathcal{F}(\mathcal{A}(\mathcal{R}_{\text{an}}), \mathcal{S}, \triangleright) \approx \frac{(0 + 0.79 + 0.79 + 0.79)^2}{4[0^2 + 0.79^2 + 0.79^2 + 0.79^2]} \approx 0.75.$$

Indeed, the above system is only ‘75% fair’, as three out of four elements enjoy an equal degree of anonymity, while one element is not anonymous at all.

### C. Unrelateability

Unrelateability represents a situation where, from the adversary’s point of view, the elements in  $S$  could be related in all possible ways.

**Definition 13.** The unrelateability of the elements in a set  $S' \subseteq S$  against an adversary  $\mathcal{A}(\mathfrak{R})$  is defined as  $\mathcal{O}(\mathcal{A}(\mathfrak{R}), S', \diamond)$ , and the degree of their unrelateability as  $\mathcal{D}(\mathcal{A}(\mathfrak{R}), S', \diamond)$ .

Note that  $|\mathcal{R}(S', \mathfrak{R}, \diamond)| = 2^{|S|^2 - (|S| - |S'|)^2}$  and that, for the special case where  $S' = S$ ,  $|\mathcal{R}(S', \mathfrak{R}, \diamond)| = 2^{|S|^2}$  [31]. The elements in  $S'$  are optimally unrelateable if  $\Pr(R_\tau \in \mathcal{R}_1) = \Pr(R_\tau \in \mathcal{R}_2)$  for all  $\mathcal{R}_1, \mathcal{R}_2 \in \mathcal{R}(S', \mathfrak{R}, \diamond)$ , i.e. if the adversary still needs to obtain  $\mathcal{O}(\mathcal{A}(\mathfrak{R}), S', \diamond) = |S|^2 - (|S| - |S'|)^2$  bits of information in order to identify  $R_\tau$ . Identifying  $R_\tau$ , however, amounts to breaching the privacy of the elements in  $S'$  in the strongest possible sense.

*Practical Example 3.* As an application of unrelateability, consider the set  $S$  of email users, and an adversary that tries to

establish the relation ‘has sent an email to’ over that set. Since it is possible for everyone to have sent an email to anyone (including one’s self), all relations in  $\mathfrak{R}$  are, in principle, candidates. One way to establish the relation is by examining the log files of all involved email servers.

*Remark 5.* Unrelateability is the most general privacy notion that can be formulated in our framework, in the sense that all other privacy notions can be expressed as unrelateability instances. However, if the adversary is starting off with a more restricted set of candidate relations – and this is usually the case –, then an appropriate privacy notion should be defined and used instead. In fact, we expect this general form of unrelateability to be mainly of academic interest, because, in practice, more restricted privacy notions tend to be of interest.

1) *Numerical unrelateability example:* Consider the set  $S = \{\alpha, \beta, \gamma, \delta\}$ .  $\mathfrak{R}$  consists of  $2^{|S|^2} = 2^{4^2} = 65536$  relations denoted  $R_1, R_2, \dots, R_{65536}$ . Suppose that, in  $\mathcal{A}(\mathfrak{R})$ ’s view,  $\Pr(R_\tau = R_i) = 1/1024$  for all  $1 \leq i \leq 1024$  and that  $\Pr(R_\tau = R_j) = 0$  for all other relations. According to this view, the unrelateability of the elements in  $S$  is  $\mathcal{O}(\mathcal{A}(\mathfrak{R})) = -\mathcal{H}(1/1024) = 10$  bits. This means that  $\mathcal{A}(\mathfrak{R})$  still needs to obtain approximately 10 bits of information about  $R_\tau$  in order to relate all elements in  $S$ . As the theoretical maximum is  $\log_2(2^{4^2}) = \log_2(2^{16}) = 16$  bits, the degree of unrelateability of the elements in  $S$  is  $\mathcal{D}(\mathcal{A}(\mathfrak{R})) = 10/16 = 0.625$ .

We now calculate the unrelateability of the elements in  $S' = \{\alpha, \beta\}$ . The equivalence relation  $\sim (\{\alpha, \beta\}, \mathfrak{R}, \diamond)$  divides  $\mathfrak{R}$  into  $2^{4^2 - (4-2)^2} = 2^{16-4} = 2^{12} = 4096$  equivalence classes, denoted  $\mathcal{R}_1, \mathcal{R}_2, \dots, \mathcal{R}_{4096}$ . Assuming that, for example,  $R_1, R_2 \in \mathcal{R}_1, R_3, R_4 \in \mathcal{R}_2, \dots, R_{1023}, R_{1024} \in \mathcal{R}_{512}$ , we have that  $\mathcal{O}(\mathcal{A}(\mathfrak{R}), \{\alpha, \beta\}, \diamond) = -\mathcal{H}(1/512) = 9$  bits. As the theoretical maximum is  $\log_2(2^{4^2 - 2^2}) = \log_2(2^{12}) = 12$  bits, the degree of unrelateability of the elements  $\{\alpha, \beta\}$  is  $\mathcal{D}(\mathcal{A}(\mathfrak{R}), \{\alpha, \beta\}, \diamond) = 9/12 = 0.75$ .

## V. CONCLUSION

This paper introduced a framework for the derivation of information-theoretic metrics that measure how well a relation is hidden from an adversary. Although only binary relations on a single set have been considered, it is straight-forward to extend the framework to  $k$ -ary relations, and to relations between the elements of multiple sets. Furthermore, definitions of unlinkability, anonymity, and unrelateability were given, all in terms of relation hiding. The definitions generalise previously known definitions, and the resulting metrics unify some of those proposed in the literature within a consistent theory. It is, of course, possible to define many other privacy notions within the framework. Consider, for example, a social networking system that hides the relation ‘is a friend of’ on the set of its users  $S$  (such as, for example, the system described in [32]). Assuming that friendship is a mutual relationship, measuring how well the system hides this relation with respect to a subset of users is obvious; the corresponding metrics are  $\mathcal{O}(\mathcal{A}(\mathcal{R}_{sy}), S', \diamond)$ , and  $\mathcal{D}(\mathcal{A}(\mathcal{R}_{sy}), S', \diamond)$ , where  $\mathcal{R}_{sy}$  is the set

of all symmetric relations over  $S$ .

Since the framework enables measuring the privacy of any subset of ‘interesting’ elements within a system, and thereby make more targeted privacy measurements, it is envisioned that it will enable the analysis of privacy protecting systems in more detail. Furthermore, the ability of the metrics to measure the adversary’s uncertainty in answering arbitrary yes/no questions about a hidden relation is likely to make the delivery of feedback to users on their individual level of privacy more effective. This is because, on the one hand, it enables the development of interfaces that are intuitive *and* precise. On the other hand, a measurement that is based on a concrete question (e.g. “‘does the value of these transactions exceed \$10.000?’” can be answered with 52% uncertainty’), is better understood compared to, say, a measurement that indicates the more abstract degree of opaqueness (e.g. ‘the degree of unlinkability of these pseudonyms is 37%’).

However, one should keep in mind that calculating privacy metrics is typically expensive, both in terms of required storage and computational power; of course, this does not only apply to the metrics derived from our framework, but to privacy metrics in general; it is a challenge to find efficient algorithms for the calculation of these metrics (or good approximations). Measuring the fairness of a system at design time avoids the need to perform such expensive calculations in order to derive the individual privacy level for every user at runtime. This is because, if a system, or a particular operational environment of a system, has been shown to be ‘fair enough’ (and, of course, acceptable in terms of the privacy protection it offers), then most users may be happy using the system without being made aware of their individual level of privacy.

## ACKNOWLEDGEMENTS

The author would like to thank Matthias Franz for his insightful comments which substantially improved the quality of this paper, and Brigitta Lange for her corrections on Theorem 1. Part of this work was conducted within the framework of the European Project ‘SWIFT’.

## APPENDIX

Definition 2 of [15], which covers the special case where  $|S'| = 2$ , matches definition of  $\mathcal{D}(\mathcal{A}(\mathcal{R}_{ii}), S', \diamond)$  for that case. Definition 3 of [15], which aims to generalise Definition 2, defines the degree of unlinkability of the elements in a set  $S' \subseteq S$  with  $|S'| = k$  as

$$\sum_{j \in I_k} \frac{1}{|I_k|} \mathcal{H}(\Pr(R_j = R_\tau)),$$

where  $I_k$  denotes an index set enumerating all equivalence relations on  $S'$ ,  $R_j$  is the  $j$ th equivalence relation on  $S'$ ,  $R_\tau$  is the hidden (‘target’) relation, and  $\Pr(R_j = R_\tau)$  denotes the probability that, in the adversary’s view,  $R_j = R_\tau$ . There are two corrections that must be done in order for this definition to match  $\mathcal{D}(\mathcal{A}(\mathcal{R}_{ii}), S', \diamond)$ , as defined in this paper: firstly,  $|I_k|$  must be replaced with  $\log_2(|I_k|)$ . Secondly, [15] states that  $|I_k| = 2^{k-1}$ . This is wrong since  $|I_k| = B_k$  (see (1)).

**Lemma 1.** For all integers  $n \geq 3$ ,  $n! > B_n$ .

Note that this result is not new; see, for example, the remark on page 478 of [33]. The following proof is, however, perhaps more accessible.

*Proof:* Consider two ordered sets  $S$  and  $S^+$  where  $|S| = n \geq 3$ , and where  $S^+$  contains the same elements as  $S$ , plus an additional element denoted  $s$ . The `PermutationGen` algorithm shown below constructs all  $(n+1)!$  permutations of  $S^+$ , given as input the permutations of  $S$ . Note that, for each input permutation, the algorithm outputs  $n+1$  permutations. The `PartitionGen` algorithm, also shown below, constructs all  $B_{n+1}$  partitions of  $S^+$ , given as input the partitions of  $S$ . Note that, for each input partition except one, the algorithm outputs less than  $n+1$  partitions. The exception is the partition of singletons, which has  $n$  equivalence classes; all other input partitions have less than  $n$  equivalence classes. Thus,  $n!$  grows faster than  $B_n$ . Since  $2! = B_2 = 2$ , the result follows. ■

**PermutationGen algorithm** (input: the permutations of  $S$ ):

- 1) For each permutation  $p(S)$  of  $S$ , do the following.
  - a) For values of  $k$  from 1 until  $n+1$ , do the following.
    - i) Output  $p(S)$ , augmented with  $s$  in the  $k$ th position.

**PartitionGen algorithm** (input: the partitions of  $S$ ):

- 1) For each partition  $\Pi(S)$  of  $S$ , do the following.
  - a) Output  $\Pi(S)$ , augmented with an additional equivalence class containing only  $s$ .
  - b) For each equivalence class  $c$  in  $\Pi(S)$ , output  $\Pi(S)$  where  $c$  is augmented such that it contains  $s$ .

## REFERENCES

- [1] D. Hughes and V. Shmatikov, "Information hiding, anonymity and privacy: a modular approach," *Journal of Computer Security*, vol. 12, no. 1, pp. 3–36, 2004.
- [2] A. Hevia and D. Micciancio, "An indistinguishability-based characterization of anonymous channels," in *Privacy Enhancing Technologies, 8th International Symposium, PETS 2008, Leuven, Belgium, July 23–25, 2008, Proceedings*, ser. Lecture Notes in Computer Science, N. Borisov and I. Goldberg, Eds., vol. 5134. Springer, 2008, pp. 24–43.
- [3] C. Andersson and R. Lundin, "On the fundamentals of anonymity metrics," in *The Future of Identity in the Information Society*, ser. IFIP International Federation for Information Processing. Springer Science & Business Media, 2008.
- [4] S. Clauß, "A framework for quantification of linkability within a privacy-enhancing identity management system," in *Emerging Trends in Information and Communication Security, International Conference, ETRICS 2006, Freiburg, Germany, June 6–9, 2006, Proceedings*, ser. Lecture Notes in Computer Science, G. Müller, Ed., vol. 3995. Springer Verlag, 2006, pp. 191–205.
- [5] S. Clauß and S. Schiffner, "Structuring anonymity metrics," in *DIM '06: Proceedings of the second ACM workshop on Digital identity management*. New York, NY, USA: ACM Press, 2006, pp. 55–62.
- [6] C. Díaz, "Anonymity metrics revisited," in *Anonymous Communication and its Applications, number 05411 in Dagstuhl Seminar Proceedings*, 2005.
- [7] C. Díaz, J. Claessens, S. Seys, and B. Preneel, "Information theory and anonymity," in *Proceedings of the 23rd Symposium on Information Theory in the Benelux*, B. Macq and J. Quisquater, Eds., 2002, pp. 179–186.
- [8] C. Díaz, S. Seys, J. Claessens, and B. Preneel, "Towards measuring anonymity," in *Privacy Enhancing Technologies, Second International Workshop, PET 2002, San Francisco, CA, USA, April 14–15, 2002, Revised Papers*, ser. Lecture Notes in Computer Science, R. Dingleline and P. F. Syverson, Eds., no. 2482. Springer Verlag, Berlin, 2002, pp. 54–68.
- [9] M. Edman, F. Sivrikaya, and B. Yener, "A combinatorial approach to measuring anonymity," in *Proceedings of the 2007 IEEE International Conference on Intelligence and Security Informatics*. IEEE, 2007.
- [10] M. Franz, B. Meyer, and A. Pashalidis, "Attacking unlinkability: The importance of context," in *Privacy Enhancing Technologies, 7th International Symposium, PET 2007 Ottawa, Canada, June 20–22, 2007, Revised Selected Papers*, ser. Lecture Notes in Computer Science, N. Borisov and P. Golle, Eds., vol. 4776. Springer Verlag, Berlin, 2007, pp. 1–16.
- [11] G. Maitland, J. Reid, E. Foo, C. Boyd, and E. Dawson, "Linkability in practical electronic cash design," in *Information Security, Third International Workshop, ISW 2000, Wollongong, NSW, Australia, December 20–21, 2000, Proceedings*, ser. Lecture Notes in Computer Science, J. Pieprzyk, E. Okamoto, and J. Seberry, Eds., vol. 1975. Springer Verlag, 2000, pp. 149–163.
- [12] A. Serjantov and G. Danezis, "Towards an information theoretic metric for anonymity," in *Privacy Enhancing Technologies, Second International Workshop, PET 2002, San Francisco, CA, USA, April 14–15, 2002, Revised Papers*, ser. Lecture Notes in Computer Science, R. Dingleline and P. F. Syverson, Eds., vol. 2482. Springer Verlag, Berlin, 2002, pp. 41–53.
- [13] V. Shmatikov and M.-H. Wang, "Measuring relationship anonymity in mix networks," in *WPES '06: Proceedings of the 5th ACM workshop on Privacy in electronic society*. New York, NY, USA: ACM Press, 2006, pp. 59–62.
- [14] G. Tóth, Z. Hornák, and F. Vajda, "Measuring anonymity revisited," in *Proceedings of the Ninth Nordic Workshop on Secure IT Systems*, S. Liimatainen and T. Virtanen, Eds., Espoo, Finland, November 2004, pp. 85–90.
- [15] S. Steinbrecher and S. Köpsell, "Modelling unlinkability," in *Privacy Enhancing Technologies, Third International Workshop, PET 2003, Dresden, Germany, March 26–28, 2003, Revised Papers*, ser. Lecture Notes in Computer Science, R. Dingleline, Ed., vol. 2760. Springer Verlag, Berlin, 2003, pp. 32–47.
- [16] M. Bellare, D. Micciancio, and B. Warinschi, "Foundations of group signatures: Formal definitions, simplified requirements, and a construction based on general assumptions," in *Advances in Cryptology – EUROCRYPT 2003, International Conference on the Theory and Applications of Cryptographic Techniques, Warsaw, Poland, May 4–8, 2003, Proceedings*, ser. Lecture Notes in Computer Science, E. Biham, Ed., vol. 2656. Springer, 2003, pp. 614–629.
- [17] C. E. Shannon, "Communication theory of secrecy systems," *Bell System Technical Journal*, vol. 28, no. 4, pp. 656–715, 1949. [Online]. Available: <http://netlab.cs.ucla.edu/wiki/files/shannon1949.pdf>
- [18] G. Tóth and Z. Hornák, "Measuring anonymity in a non-adaptive, real-time system," in *Privacy Enhancing Technologies, 4th International Workshop, PET 2004, Toronto, Canada, May 26–28, 2004, Revised Selected Papers*, ser. Lecture Notes in Computer Science, D. Martin and A. Serjantov, Eds., vol. 3424. Springer Verlag, Berlin, 2004, pp. 226–241.
- [19] C. Díaz, C. Troconso, and G. Danezis, "Does additional information always decrease anonymity?" in *Proceedings of the 6th ACM Workshop on Privacy in the Electronic Society (WPES'07)*, T. Yu, Ed. ACM Press, 2007, pp. 72–75.
- [20] P. Venkitasubramanian, T. He, and L. Tong, "Anonymous networking amidst eavesdroppers," *The Computing Research Repository*, vol. abs/0710.4903, 2007.
- [21] R. Jain, D. Chiu, and W. Hawe, "A quantitative measure of fairness and discrimination for resource allocation in shared computer systems," DEC, Research Report TR-301, 1984.
- [22] Z. Fang and B. Bensaou, "Fair bandwidth sharing algorithms based on game theory frameworks for wireless ad-hoc networks," in *Proceedings of IEEE INFOCOM 2004, The 23rd Annual Joint Conference of the IEEE Computer and Communications Societies, Hong Kong, China, March 7–11, 2004*. IEEE, 2004.
- [23] Z. Fu, P. Zerfos, H. Luo, S. Lu, L. Zhang, and M. Gerla, "The impact of multihop wireless channel on tcp throughput and loss," in *Proceedings of IEEE INFOCOM 2003, The 22nd Annual Joint Conference of the*

*IEEE Computer and Communications Societies, San Francisco, CA, USA, March 30–April 3, 2003.* IEEE, 2003.

- [24] M. D. Welsh, “An architecture for highly concurrent, well-conditioned internet services,” PhD thesis, University of California at Berkeley, 2002.
- [25] E. T. Bell, “Exponential numbers,” *American Mathematical Monthly*, vol. 41, pp. 411–419, 1934.
- [26] D. Chaum, “Security without identification: transaction systems to make big brother obsolete,” *Communications of the ACM*, vol. 28, no. 10, pp. 1030–1044, 1985.
- [27] —, “Showing credentials without identification: transferring signatures between unconditionally unlinkable pseudonyms,” in *Advances in Cryptology – AUSCRYPT 90*, ser. Lecture Notes in Computer Science, J. Seberry and J. Pieprzyk, Eds., vol. 453. Springer Verlag, Berlin, 1990, pp. 246–264.
- [28] L. Chen, “Access with pseudonyms,” in *Cryptography: Policy and Algorithms, International Conference, Brisbane, Queensland, Australia, July 3-5, 1995, Proceedings*, ser. Lecture Notes in Computer Science, E. Dawson and J. D. Golic, Eds., no. 1029. Springer Verlag, Berlin, 1995, pp. 232–243.
- [29] D. Chaum, “Untraceable electronic mail, return addresses, and digital pseudonyms,” *Communications of the ACM*, vol. 24, no. 2, pp. 84–90, 1981.
- [30] B. Gierlichs, C. Troncoso, C. Díaz, B. Preneel, and I. Verbauwhede, “Revisiting a combinatorial approach toward measuring anonymity,” in *Proceedings of the 2008 ACM Workshop on Privacy in the Electronic Society, WPES 2008, Alexandria, Virginia, USA, October 27, 2008 (to be published)*. ACM, 2008.
- [31] F. Harary and R. W. Robinson, “Labeled bipartite blocks,” *Canadian Journal of Mathematics*, vol. 31, pp. 60–68, 1979.
- [32] K. B. Frikken and P. Golle, “Private social network analysis: How to assemble pieces of a graph privately,” in *2006 Workshop on Privacy in the Electronic Society*. ACM Press, 2006, pp. 89–97.
- [33] P. Erdős and R. Rado, “A partition calculus in set theory,” *Bulletin of the American Mathematical Society*, vol. 62, no. 5, pp. 427–489, 1956.