# On the Fundamentals of Anonymity Metrics

Christer Andersson and Reine Lundin

Karlstad University, Department of Computer Science
Universitetsgatan 2, 651-88 Karlstad, Sweden
{christer.andersson, reine.lundin}@kau.se

**Abstract.** In recent years, a handful of anonymity metrics have been proposed that are either based on *(i)* the number participants in the given scenario, *(ii)* the probability distribution in an anonymous network regarding which participant is the sender / receiver, or *(iii)* a combination thereof. In this paper, we discuss elementary properties of metrics, and evaluate the behavior of a recent anonymity metrics in a set of application scenarios. Then, we define criteria for anonymity metrics and show than none of the studied metrics fulfill all criteria. Lastly, based on previous work on entropy-based anonymity metrics, we propose a new metric designed to fulfill these criteria – the so-called scaled anonymity set size.

## 1 Introduction

*Anonymity* can be defined as "the state of being not identifiable within a set of subjects, the anonymity set" [7]. Anonymity both involves preserving the confidentiality of user data (data level anonymity) and hiding with whom a user is communicating (communication level anonymity). *Sender anonymity* means that a message cannot be linked to the sender, while *receiver anonymity* implies that a certain message cannot be linked to the receiver of that message [7]. In this paper, we limit our scope to sender anonymity, although most ideas are also valid for receiver anonymity.

This paper discusses *anonymity metrics*, which can be applied to measure the degree of anonymity in a certain scenario. State-of-the-art metrics are normally based on either *(ii)* the number participants in the given scenario, *(ii)* the probability distribution in an anonymous network regarding which participant is the sender / receiver, or *(iii)* a combination thereof. In this paper, we first discuss the basics of measurements and anonymity metrics. Then, a basic model of anonymity attacks is proposed and some recent anonymity metrics are introduced. After this, we define a set of "typical" scenarios for anonymous communication, and then quantify the degree of anonymity in these scenarios using the earlier introduced metrics. On the basis of this evaluation – and taking elementary properties of each anonymity metric into account – we thereafter propose a set of criteria that an anonymity metric should fulfill and assess whether the studied anonymity metrics fulfill these criteria. In the scenarios, the Crowds system [9] is used – a theoretically well studied protocol that is easy to understand.

A subsequent result is that, although some metrics fulfill most criteria, there is none that fulfill all criteria. Using existing entropy-based metrics [3, 10] as a starting point, we thereafter propose and evaluate an adapted entropy-based metric that better fulfills the stated criteria. We denote this metric the *scaled anonymity set size*.

## 2 Preliminaries

### 2.1 Introduction to Crowds.

Later, four scenarios are presented that use the *Crowds system* – an anonymous communication mechanism based on traffic forwarding through virtual paths. The anonymity set is denoted a *crowd*, and all users in the crowd run a *jondo* application. In addition, a *blender* application administrates user membership. Path in Crowds are created randomly: first, a user extends to path to a random jondo, which, in turn, flips a biased coin (based on the probability of forwarding, $p_f$) to determine whether the path should be ended, or extended to another jondo (which repeats the same procedure).

### 2.2 A Model for Anonymity Attacks

An *anonymity attack* entails a attacker $\mathcal{A}$ trying to uniquely map a user $u_i$ in the anonymity set $\mathcal{U} = \{u_1, u_2, ..., u_n\}$ to an observed sender by gathering knowledge about the system, the user base / anonymity set $\mathcal{U}$ and the sender. These entities have attributes that can be modeled as sets of attribute types / values. The system has attributes such as $a_i$ = (*application*, "Crowds") and $a_j = (p_f, \frac{3}{4})$. One essential attribute in the system is the distribution $\mathcal{P}$ containing $\{p_1, p_2, \ldots, p_n\}$, a vector such that $p_i$ denotes the probability that $u_i$ is the sender for each communication. $\mathcal{U}$ has attribute sets about its users (or their devices), such as $a_i$ = {*name*, "Alice"} and $a_j$ ={*IP*, 192.168.10.20}. Lastly, the sender initially has only attribute types (same types as $\mathcal{U}$), but no values. Using this terminology, a strategy for an anonymity attack can be described as follows:

1. Initially, $\mathcal{A}$ can be assumed to know at least the public parameters of the system and some information about the users in $\mathcal{U}$.[1] $\mathcal{A}$ initially possess no knowledge about the sender. This entails that the distribution $\mathcal{P}$ is initially uniform;
2. Now, $\mathcal{A}$'s objective is to either passively observe or actively trigger events to learn information about the sender. The triggering can be accomplished using arbitrary active attacks, such as predecessor [13], intersection [8], or Sybil attack [5]. If $\mathcal{A}$ is successful, the events may enable him to learn one or more attribute values of the sender's attribute types, or at least restrict the corresponding value domains;
3. Then, $\mathcal{A}$ analyzes the collected attribute values of the sender, together with the attributes of the system and the users in $\mathcal{U}$. $\mathcal{A}$'s objective is to calculate a new (less uniform) $\mathcal{P}'$. The way $\mathcal{P}'$ is calculated varies from scenario to scenario; in this paper we base our calculations on the internal structure of Crowds [9];
4. $\mathcal{A}$'s goal is to map a single user in $\mathcal{U}$ to the sender. Depending on $\mathcal{P}'$, there are three possible next steps: *(i)* if any of $\mathcal{A}$'s resources are exhausted, he fails; *(ii)* if $\mathcal{P}'$ does not single out as the sender with a specifically large likelihood, repeat step two; and *(iii)* if there is a $p_i \in \mathcal{P}'$ that is close or equal to 1, the attacker succeeds.

When assessing a system's resistance against anonymity attacks, an analyst can simulate these steps. In step three, the analyst can use an anonymity metric to determine the degree of anonymity. In the next section, we thus discuss the basics of measurement and anonymity metrics, and give examples of anonymity metrics.

[1] Compare for example with the information distributed by the Blender in Crowds [9].

### 2.3 Anonymity Metrics

**The Basics of Measurements.** *Measurement* can be defined as "a mapping from the empirical world to the formal, relational world. Consequently, a *measure* is the number or symbol assigned to an entity by this mapping in order to characterize an attribute" where "the real world is the *domain* of the mapping, and the mathematical world is the *range*" [6]. One important rule is the *representation condition* which asserts that "a measurement mapping $M$ must map entities into numbers and empirical relations into numerical relations in such a way that the empirical relations preserve and are preserved by the numerical relations" [6]. Lastly, a *metric* is a standard of measurement.

**Introduction to Anonymity Metrics.** An anonymity metric is a mapping from the empirical world (the domain) to the mathematical world (the range), where numbers or symbols are assigned to entities in a system to describe the degree of anonymity: *(i)* the *domain* is the knowledge of the attacker $\mathcal{A}$ about the studied entities in the real world – the system and its anonymity set $\mathcal{U} = \{u_1, u_2, ..., u_n\}$. The attacker $\mathcal{A}$ is often a model defined to test the resistance of a system against anonymity attacks. The system can both be a real world instance or a theoretical model; *(ii)* the *range* is the mapping of an attribute in the real world to a mathematical system. Here, there are many options, as different anonymity metrics use different units for presenting the degree of anonymity; *(iii)* the *mapping* itself can be seen as a function behaving according to set of rules. An important parameter in the mapping is the probability distribution $\mathcal{P} = \{p_1, p_2, ..., p_n\}$ among the users in $\mathcal{U}$ regarding which user is the sender in a communication.

**Examples of Anonymity Metrics.** Below, we introduce some of the most notorious anonymity metrics that have been proposed in recent years.

- *Anonymity set size:* a classic degree is the size of the anonymity set, $|\mathcal{U}| = n$ (anonymity set concept first used in [2]). Alteratively, this can be specified as $log_2(n)$ [1];
- *Crowds-based metric:* in this metric (initially developed for Crowds, but has since been used in other contexts), the degree of anonymity $A$ is measured on a continuum between 0 (`provably exposed`) and 1 (`absolute privacy`), were $A = 1 - p_i$ [9]. The continuum includes the intermediary points: `possible innocence`: $\overline{p_i}$ that $u_i$ is *not* the sender is non-negligible, thus $\overline{p_i} \geq 0 + \delta$, where the threshold $\delta > 0$. Hence,we get $A = 1 - p_i = \overline{p_i} \geq 0 + \delta$; `probable innocence`: $p_i$ that $u_i$ is the sender is less than $1/2$, thus $A \geq 1/2$; and `beyond suspicion`: $u_i$ is not more likely than any other $u_j \in \mathcal{U}$ to be the sender, and thus $A = \max\{A_1, A_2, ..., A_i, ..., A_n\}$ among $\mathcal{U}$.
- *Source-hiding property:* here, $\Theta$ is defined as the greatest probability you can assign to any user $u_i$ of being the sender of a message, thus $\Theta = \max(\mathcal{P})$ [12]. Naturally, $\Theta$ varies between $\frac{1}{n}$ and 1, where in this case $\Theta = \frac{1}{n}$ denotes maximum anonymity;
- *Entropy-based metrics:* in Serjantov / Danezis's metric [10], "the effective anonymity set size" $\mathcal{S}$ is defined as the uncertainty $H(\mathcal{P})$ regarding which user in $\mathcal{U}$ sent a message. Using Shannon's theories on entropy [11]), we get $\mathcal{S} = H(\mathcal{P}) = -\sum_{i=1}^{n} p_i log_2(p_i)$, where $0 \leq H(\mathcal{P}) \leq log_2(n)$. Díaz *et al.* [3] instead calculate the degree of anonymity $d$ as $\frac{H(\mathcal{P})}{log_2(n)}$. Here, $d$ varies between 0 and 1. Both $\mathcal{S}$ and $d$ output a maximum degree of anonymity when $\mathcal{P}$ equals the uniform distribution.

### 2.4 Measuring the Uniformness of Probability Distributions

To study how an anonymity metric behaves when the probability distribution $\mathcal{P}$ change, a function $d(\mathcal{P}, U)$ is needed, where the parameter $U$ is the uniform distribution. Such a function $d(\mathcal{P}, U)$ should by some means quantify the distance (or quotient) between $\mathcal{P}$ and $U$. There are several alternatives for $d(\mathcal{P}, U)$, such as $d(\mathcal{P}, U) = H(U) - H(\mathcal{P})$ or $d(\mathcal{P}, U) = \frac{H(\mathcal{P})}{H(U)}$. Another option that we think could be used as well is to calculate the $d(\mathcal{P}, U)$ as the Euclidean distance in $n$-space, according to the following:

$$d(\mathcal{P}, U) = \sqrt{\sum_{i=1}^{n}(p_i - u)^2} \tag{1}$$

Here, $u$ is the probability assigned to each user when $\mathcal{P}$ is the uniform distribution (that is, $\frac{1}{n}$, assuming $n$ users). Intuitively, Equation (1) outputs the ordinary distance between the two points $\mathcal{P}$ and $U$ when they are plotted in an $n$-dimensional space. Equation (1) varies between 0 (when $\mathcal{P} = U$) and $\sqrt{\left(\frac{n(n-1)}{n^2}\right)}$ (when there is a $p_i$ in $\mathcal{P}$ such that $p_i = 1$). For $n \to \infty$, the term $\left(\frac{n(n-1)}{n^2}\right)^{1/2}$ approaches 1.

## 3 Evaluation of Anonymity Metrics

### 3.1 Example Scenarios

This section evaluates the degree of anonymity in a set of example scenarios using *Crowds* [9]. The scenarios involves a user communicating with an external web server through the Crowds network. The following parameters are varied in the scenarios: the number of users $n$, the number of rogue users $c$ (note that $c$ is a subset of $n$), and $p_f$:

- In scenario one, $n = 10$, $c = 1$, and $p_f = 11/20$;
- In scenario two, $n = 1000$, $c = 10$, and $p_f = 11/20$;
- In scenario three, $n = 1000$, $c = 200$, and $p_f = 11/20$;
- In scenario four, $n = 1000$, $c = 200$, and $p_f = 3/4$.

*Attacker Model.* As Crowds does not provide anonymity against global observers or eavesdroppers directly observing the sender, we omit these entities from the attacker model, and instead only include *(i)* the $c$ corrupted users and *(ii)* the web server. In the analysis, we assume that a corrupted user is succeeding the sender in the virtual path.

### 3.2 Anonymity Evaluations

Below, we evaluate the above scenarios against the metrics introduced in Section 2.3. We provide the details of the calculations only for scenario one. For the entropy-based metrics and the source-hiding property, we need the probability distribution $\mathcal{P}$. From the perspective of the $c$ corrupted users, $\mathcal{P}$ is $\{0.56, \frac{0.44}{8}, \frac{0.44}{8}, \frac{0.44}{8}, \frac{0.44}{8}, \frac{0.44}{8}, \frac{0.44}{8}, \frac{0.44}{8}, \frac{0.44}{8}, 0\}$, while $\mathcal{P}$ from the perspective of the web server is uniform. The probability $p_i = 0.56$ is calculated as: $p_i = \frac{n - p_f(n-c-1)}{n} = \frac{10 - 0.55*8}{10} = 0.56$ [9].

– *Anonymity set size:* the set size evaluates to $|\mathcal{U}| = 10$ (or $log_2(|\mathcal{U}|) = 3.32$ bits);
– *Crowds-based metric: A* against the web server is `beyond suspicion`, as all users in $\mathcal{U}$ are equally likely of being the sender. If expressing $A$ as $1 - p_i$, we get $A = \frac{9}{10}$, as $p_i$ that any $u_i$ is the sender is $\frac{1}{10}$. Assuming that one of the $c$ corrupted users succeeds the user $u_i$ in the path, $A$ against the corrupted users is `possible innocence`. This is because the following inequality does not hold [9]: $n \geq \frac{p_f}{(p_f - 1/2)} * (c + 1)$. Instead, the corrupted users can say with $p_i = 0.56$ that $u_i$ is the sender (i.e., $A = 1 - p_i = 0.44$);
– *Entropy-based metrics:* according to Serjantov / Danezis [10], the effective anonymity set size $\mathcal{S}$ against the corrupted users is calculated as: $\mathcal{S} = H(\mathcal{P}) = -\sum_{i=1}^{n}(p_i * log_2 p_i) = 1.83477 \approx 1.83$ bits. According to the metric proposed by Díaz *et al.* [3], the degree of anonymity $d$ is instead calculated as follows (using $H(\mathcal{P})$ from above): $d = \frac{H(\mathcal{P})}{log_2(n)} = \frac{1.834767}{3.321928} \approx 0.55$. Regarding the web server, Díaz *et al.*'s metric gives us $d = 1$, as $\mathcal{P}$ is uniform, and for this reason $H(\mathcal{P}) = log_2(n)$. Using Serjantov / Danezis's metric, we get the following effective anonymity set size: $\mathcal{S} = H(\mathcal{P}) = -\sum_{i=1}^{n}(p_i * log_2(p_i)) = 10 * (\frac{1}{10} * log_2 10) \approx 3.32$ bits;
– *The source-hiding property:* the greatest $p_i$ the corrupted users can assign to any $u_i$ is $\max(\mathcal{P}) = 0.56$, and thus $\Theta = 0.56$. Against the web server, $\Theta = \max(\mathcal{P}) = \frac{1}{10}$.

In Table 1, we list the degrees of anonymity for the above scenarios. For comparison, we also include $d(\mathcal{P}, U)$ according the the Euclidean distance in $n$-space.

Table 1: Anonymity evaluation of scenarios (incl. Euclidean distance).

| | Scen. | $c$ corrupted users | Web server |
|---|---|---|---|
| *Anonymity* | S1 | $\|\mathcal{U}\| = 10$ / 3.32 bits | $\|\mathcal{U}\| = 10$ / 3.32 bits |
| *set size* | S2-4 | $\|\mathcal{U}\| = 1000$ / 9.97 bits | $\|\mathcal{U}\| = 1000$ / 9.97 bits |
| *Crowds-* | S1 & S3 | `possible innocence` | `beyond suspicion` |
| *based m.* | S2 & S4 | `probable innocence` | `beyond suspicion` |
| *Entropy-* | S1 | $\mathcal{S} = 1.83$ bits | $\mathcal{S} = 3.32$ bits |
| *based* | S2 | $\mathcal{S} = 6.37$ bits | $\mathcal{S} = 9.97$ bits |
| *metric* | S3 | $\mathcal{S} = 5.23$ bits | $\mathcal{S} = 9.97$ bits |
| (Serjantov / Danezis) | S4 | $\mathcal{S} = 6.75$ bits | $\mathcal{S} = 9.97$ bits |
| *Entropy-* | S1 | $d = 0.55$ | $d = 1$ |
| *based* | S2 | $d = 0.63$ | $d = 1$ |
| *metric* | S3 | $d = 0.52$ | $d = 1$ |
| (Díaz *et al.*) | S4 | $d = 0.68$ | $d = 1$ |
| *Source-* | S1 | $\Theta = 0.56$ | $\Theta = 1/10$ |
| *hiding* | S2 | $\Theta = 0.46$ | $\Theta = 1/1000$ |
| *property* | S3 | $\Theta = 0.56$ | $\Theta = 1/1000$ |
| | S4 | $\Theta = 0.40$ | $\Theta = 1/1000$ |
| *Euclidean-* | S1 | $d(\mathcal{P}, U) = 0.49$ (max: 0.95) | $d(\mathcal{P}, U) = 0$ |
| *distance in* | S2 | $d(\mathcal{P}, U) = 0.46$ (max: 0.995) | $d(\mathcal{P}, U) = 0$ |
| *in n-space* | S3 | $d(\mathcal{P}, U) = 0.56$ (max: 0.995) | $d(\mathcal{P}, U) = 0$ |
| | S4 | $d(\mathcal{P}, U) = 0.40$ (max: 0.995) | $d(\mathcal{P}, U) = 0$ |

**Some Observations from the Evaluation Results.**

- All metrics except the anonymity set size metric consider probabilities;
- All metrics except anonymity set size scored higher against the web server than against the corrupted users, as $\mathcal{P}$ was uniform from the perspective of the web server;
- Although stated in [10], we do not think that Serjantov / Danezis's metrics reflect the "effective anonymity set size" (as the endpoints do not overlap with those of the anonymity set size metric). We also think that the max anonymity (given $n$) should be made explicit. That is, $\mathcal{S}$ could be expressed as $H(P)$ out of $log_2(n)$ bits;
- Against the corrupted users, most metrics yielded the highest anonymity in $S4$;
- $d(\mathcal{P}, U)$ according to the Euclidean distance in $n$-space seems to be fairly alike measuring distance based on entropy, although not exactly similar. Further analysis on the deviation between these different measures of $d(\mathcal{P}, U)$ is left as future research.

### 3.3 Criteria for Anonymity Metrics

As it is essential that an anonymity metric gives an accurate picture about the degree of anonymity, we below state a set of criteria an anonymity metric should meet.

- A user can be said to be de-anonymized when an attacker can, beyond reasonable doubt, pinpoint a user as the sender of a message (step three in Section 2.2). Thus, the analyst must, in one way or another, consider probabilities;
  $\Rightarrow$ *C1: An anonymity metric should base its analysis on probabilities.*
- The endpoints in an anonymity metric are "no anonymity" and "max anonymity". E.g., in metrics solely based on $\mathcal{P}$, max anonymity happens when $\mathcal{P}$ is uniform, and no anonymity occurs if there is a $p_i \in \mathcal{P}$ such that $p_i >> \max\{\mathcal{P} - p_i\}$. An anonymity metric should model these two endpoints in a well defined and intuitive manner;
  $\Rightarrow$ *C2: An anonymity metric must have well defined and intuitive endpoints.*
- Intuitively, the more uniform the $\mathcal{P}$, the more uncertain the attacker is. A metric should preserve this relation (recall the representation condition [8]). Thus, a degree of anonymity should increase if the uniformness of $\mathcal{P}$ increases, and vice verse;
  $\Rightarrow$ *C3: The more uniform the distribution $\mathcal{P}$, the higher the anonymity.*
- Assuming a static degree of uniformness of $\mathcal{P}$: the more the users in $\mathcal{U}$, the more the potential senders, and thus the higher the uncertainty of the attacker. A metric should preserve this relation according to the representation condition. Thus, the degree of anonymity should increase if the number of users increases, and vice verse;
  $\Rightarrow$ *C4: The more the users in the anonymity set, the higher the anonymity.*
- By studying the degree of anonymity in a scenario, an analyst should be able to judge where in between the two endpoints (no & max anonymity) the current degree is. Thus, all values in the value domain of an anonymity metric should be well defined;
  $\Rightarrow$ *C5: The elements in the metric's value domain should be well defined.*
- An anonymity metric should use a scale that preserves the ordering among elements, such as ordinal, interval, ratio, or absolute scale [8]. Moreover, the metric should be fined-grained enough to differ between similar, but not equal, scenarios.
  $\Rightarrow$ *C6: The value domain of the metric should be ordered and not too coarse.*

Next, we evaluate the aforementioned anonymity metrics against these criteria.

### 3.4 Evaluation of Anonymity Metrics against Criteria

In Table 2, we assess whether the studied metrics fulfill the earlier stated criteria.

Table 2: Evaluation against criteria.

| | | | |
|---|---|---|---|
| *Anonymity set size metric* | C1 | - | Neither $\|\mathcal{U}\| = n$ nor $log_2(\|\mathcal{U}\|)$ consider probabilities. |
| | C2 | - | As this is an absolute measure, the metric always outputs $n$, which can vary between 1 and $\infty$. Difficult to state a "good-enough" value for $n$. |
| | C3 | - | Not fulfilled, as this metric does not consider probabilities. |
| | C4 | + | Fulfilled, as the degree of anonymity is $\|\mathcal{U}\| = n$. |
| | C5 | + | $n$ simply entails the number of users in the anonymity set ($\|\mathcal{U}\|$). |
| | C6 | + | Fulfilled, as this metric uses absolute scale. |
| *Crowds-based metric* | C1 | + | Fulfilled, as output corresponds directly to the probability of being the sender an attacker can assign to the sending user in a system. |
| | C2 | + | The metric varies between `provably exposed` and `absolute privacy`, where each intermediary category is semantically mapped to probabilities. |
| | C3 | - | Not always true as individual probabilities are quantified. |
| | C4 | + | In general fulfilled, assuming that the corresponding $p_i > 0$. Specifically, increasing $n$ helps fulfilling $n \geq \frac{p_f}{(p_f - 1/2)} * (c + 1)$ in the scenarios. |
| | C5 | + | Categories are based on the underlying probability of being the sender. |
| | C6 | - | Although ordinal scale is used, the output is fairly coarse. |
| *Entropy-based metric* (Serjantov / Danezis) | C1 | + | Based on the entropy of the probability distribution. |
| | C2 | - | The endpoints are 0 and $log_2(n)$. The latter is hard to calculate by hand. |
| | C3 | + | Fulfilled, if we assume $d(\mathcal{P}, U) = H(U) - H(\mathcal{P})$. |
| | C4 | + | Fulfilled. Note that the maximum increases with an increasing $n$. |
| | C5 | + | States that an attacker on average has to find the answer for $H(P)$ binary questions to identity the sender. |
| | C6 | + | This criterion is fulfilled as ratio scale is used. |
| *Entropy-based metric* (Díaz *et al.*) | C1 | + | Based on the entropy of the probability distribution. |
| | C2 | + | Clear endpoints: 0 (no anonymity) and 1 (max anonymity). |
| | C3 | + | Fulfilled, if we assume $d(\mathcal{P}, U) = \frac{H(\mathcal{P})}{H(U)}$. |
| | C4 | - | This criterion is not fulfilled, as the resulting $d$ is normalized. |
| | C5 | + | Easy to interpret as $d$ denotes the quotient between $H(\mathcal{P})$ and $H(U)$. |
| | C6 | + | This criterion is fulfilled as ratio scale is used. |
| *Source-hiding property* | C1 | + | $\Theta$ is directly based on the greatest probability in $\mathcal{P}$, as $\Theta = \max(\mathcal{P})$. |
| | C2 | - | The use of an inverted scale is somewhat confusing (best case: $\Theta = 0$). |
| | C3 | - | Although it can be expected to be true in many real scenarios, it may not coincide as the output is merely an individual probability. |
| | C4 | + | Fulfilled, assuming corresponding $p_i > 0$ for added users. |
| | C5 | + | $\Theta$ is the max probability (of being the sender) any user in the anonymity set can be assigned of by the attacker. In real scenarios, it will probably often overlap with the probability assigned to the real sender. |
| | C6 | + | This criterion is fulfilled as ratio scale is used. |

We can note in Table 2 above that there is no metric that fulfill all criteria.

## 4 Proposal: Scaled Anonymity Set Size

In Section 3.4, we saw that no metric fulfilled all criteria. Thus, we propose a entropy-based anonymity metric $A$ that, in particular, avoids the following problems: *(i)* in the Díaz *et al.* metric, the number of users does not contribute to $d$, and *(ii)* the Serjantov / Danezis metric has nonintuitive endpoints. We propose to quantify $A$ as follows:

$$A = 2^{H(\mathcal{P})} \tag{2}$$

Equation (2) grows with an increasing uniformity of $H(\mathcal{P})$ and varies between 1 (when there is one $p_i \in \mathcal{P}$, where $p_i = 1$) and $n$ (when $\mathcal{P} = U$). Semantically, $A = 2^{H(\mathcal{P})}$ can be explained as follows – given that $H(\mathcal{P})$ denotes the average number of binary questions an attacker needs to find the answer to in order to identity the sender:

$2^{H(\mathcal{P})}$ *is the number of possible outcomes given the expected amount of binary questions the attacker needs to answer to identify the sender*.

For instance, if $H(\mathcal{P}) = 2$, then $2^{H(\mathcal{P})} = 4$, the possible outputs are: $\{0,0\}, \{0,1\}$, $\{1,0\}$, and $\{1,1\}$. Equation (2) has a desirable property: the max value ($n$) overlaps with the actual size of the anonymity set, while the min value (1) denotes a singleton anonymity set, i.e. no anonymity. For this reason, we denote this metric the *scaled anonymity set size*. In Table 3, we calculate $A$ for the four aforementioned scenarios, while in Table 4, we evaluate the proposed metric against the aforementioned criteria.

Table 3: Degrees of anonymity for the scaled anonymity set size.

| | Scen. | $c$ corrupted users | Web server |
|---|---|---|---|
| *Scaled* | S1 | $A = 2^{1.83} = 3.6$ (for $n = 10$) | $A = 2^{log_2(10)} = 10$ |
| *anonymity* | S2 | $A = 2^{6.37} = 83$ (for $n = 1000$) | $A = 2^{log_2(1000)} = 1000$ |
| *set size* | S3 | $A = 2^{5.23} = 38$ (for $n = 1000$) | $A = 2^{log_2(1000)} = 1000$ |
| | S4 | $A = 2^{6.75} = 108$ (for $n = 1000$) | $A = 2^{log_2(1000)} = 1000$ |

In Table 3, we can note that the ordering among the scenarios according to $A$ overlaps with that of the Serjantov / Danezis metric. However, we think that the linear scale more clearly shows e.g. that $A$ in scenario one is far lower than in the other scenarios.

Table 4: Evaluation of scaled anonymity set size against criteria.

| | | | |
|---|---|---|---|
| *Scaled* | C1 | + | Fulfilled, as this metric is based on probabilities. |
| *anonymity* | C2 | + | Intuitive and well defined endpoints where $A$ varies between 1 and $n$. |
| *set size* | C3 | + | This criterion is fulfilled as $A$ is based on the uniformity of $\mathcal{P}$. |
| | C4 | + | Fulfilled, as max anonymity increases with $n$: $\max(2^{H(\mathcal{P})}) = 2^{log_2(n)}$. |
| | C5 | + | $A = 2^{H(\mathcal{P})}$ is the number of possible outcomes given the expected number of binary questions an attacker has to answer to identify the sender. |
| | C6 | + | Fulfilled, as the scaled anonymity set size metric uses ratio scale. |

In Table 4, we can see that all criteria are fulfilled for the scaled anonymity set size.

## 5 Summary & Outlook

In this paper we discussed elementary properties of anonymity metrics. We defined a set of example scenarios using Crowds, and then quantified the degree of anonymity in these scenarios for some recent anonymity metrics. Based on this evaluation and elementary properties of metrics, we then defined a set of criteria for anonymity metrics. We then assessed whether these metrics fulfilled the earlier defined criteria. Lastly, we proposed a new metric: the scaled anonymity set size, defined as $A = 2^{H(\mathcal{P})}$. Future work includes further analyzing the scaled anonymity set size, as well as studying the correlation between different ways of expressing the degree of uniformity in probability distributions and their relation to different anonymity metrics.

## References


1. O. Berthold, H. Federrath, and S. Köpsell. Web MIXes: A System for Anonymous and Unobservable Internet Access. In H. Federrath, editor, *Proceedings of Designing Privacy Enhancing Technologies: Workshop on Design Issues in Anonymity and Unobservability*, pages 115–129. Springer-Verlag, LNCS 2009, Jul 2000.
2. D. Chaum. The Dining Cryptographers Problem: Unconditional Sender and Recipient Untraceability. *J. Cryptography*, 1(1):65–75, 1988.
3. C. Díaz, S. Seys, J. Claessens, and B. Preneel. Towards Measuring Anonymity. In Dingledine and Syverson [4].
4. R. Dingledine and P. Syverson, editors. *Proceedings of the Workshop on Privacy Enhancing Technologies (PET 2002)*. Springer-Verlag, LNCS 2482, Apr 2002.
5. J. R. Douceur. The Sybil Attack. In P. Druschel, F. Kaashoek, and A. Rowstron, editors, *Peer-to-Peer Systems: Proceedings of the 1st International Peer-to-Peer Systems Workshop (IPTPS)*, volume 2429, pages 251–260. Springer-Verlag, 7–8 Mar 2002.
6. N. E. Fenton and S. L. Pfleeger. *Software Metrics – A Rigorous & Practical Approach*. PWS Publishing Company, 20 Park Plaza, Boston, MA 02116-4324, second edition, 1997.
7. A. Pfitzmann and M. Hansen. Anonymity, Unlinkability, Unobservability, Pseudonymity, and Identity Management - A Consolidated Proposal for Terminology v0.27, 20 Feb 2006. See `http://dud.inf.tu-dresden.de/literatur/`.
8. J.-F. Raymond. Traffic Analysis: Protocols, Attacks, Design Issues, and Open Problems. In H. Federrath, editor, *Proceedings of Designing Privacy Enhancing Technologies: Workshop on Design Issues in Anonymity and Unobservability*, pages 10–29. Springer-Verlag, LNCS 2009, July 2000.
9. M. Reiter and A. Rubin. Crowds: Anonymity for Web Transactions. In *DIMACS Technical report*, pages 97–115, 1997.
10. A. Serjantov and G. Danezis. Towards and Information Theoretic Metric for Anonymity. In Dingledine and Syverson [4].
11. C. E. Shannon. A Mathematical Theory of Communication. *The Bell System Technical Journal*, 27:379–423, Jul 1948.
12. G. Tóth and Z. Hornák. Measuring Anonymity in a Non-Adaptive, Real-Time System. In *Proceedings of the Workshop on Privacy Enhancing Technologies (PET 2004)*, 26–28 May 2004.
13. M. K. Wright, M. Adler, and B. N. Levine. The Predecessor Attack: An Analysis of a Threat to Anonymous Communication Systems. *ACM Transactions on Information and System Security*, 7(4):489–522, Nov, 2004.