Measuring Information Leakage in Non-stochastic Brute-Force Guessing

Farhad Farokhi
Department of Electrical and Electronic Engineering
The University of Melbourne, Parkville, Australia
farhad.farokhi@unimelb.edu.au

Ni Ding
School of Computing and Information Systems
The University of Melbourne, Parkville, Australia
ni.ding@unimelb.edu.au

***Abstract*—We propose an operational measure of information leakage in a non-stochastic setting to formalize privacy against a brute-force guessing adversary. We use uncertain variables, non-probabilistic counterparts of random variables, to construct a guessing framework in which an adversary is interested in determining private information based on uncertain reports. We consider brute-force trial-and-error guessing in which an adversary can potentially check all the possibilities of the private information that are compatible with the available outputs to find the actual private realization. The ratio of the worst-case number of guesses for the adversary in the presence of the output and in the absence of it captures the reduction in the adversary's guessing complexity and is thus used as a measure of private information leakage. We investigate the relationship between the newly-developed measure of information leakage with maximin information and stochastic maximal leakage that are shown to arise in one-shot guessing.**

I. INTRODUCTION

Recently, maximal leakage based on one-shot guessing [1] and guessing leakage based on brute-force guessing [2] have been developed to provide operational information-leakage metrics for privacy analysis. These notions have started a new wave of research in information-theoretic privacy with interpretable or operational measure of private information leakage [3]. In some cases, however, probability distributions of the underlying variables or conditional probability of outputs given private data might not be known *a priori* or might change unpredictably over time. For instance, when considering small datasets, enough data might not be available to make probabilistic inference about the population and, thus, we may want to investigate whether an adversary can gain private information that is not based on statistics. Alternatively, we may need to avoid randomized policies for privacy preservation. For instance, this could be due to concerns about untruthfulness in privacy-preserving reports [4] or complications in financial auditing and fraud detection [5]. Therefore, in these cases, there is a need to investigate information leakage in non-stochastic frameworks.

In this paper, we propose a measure of information leakage in a non-stochastic framework. Doing so, we also provide an interpretation for the recent results on non-stochastic privacy [6], [7]. We use uncertain variables, non-stochastic counterparts of random variables introduced in [8], to construct a guessing framework in which an adversary is interested in determining private information based on available outputs. We consider brute-force guessing in which an adversary potentially checks all the possibilities of the private information that are compatible with the outputs to find the realization of the private information. This is similar to the interpretation of [1] for password guessing or side-channel attacks on cipher systems in which an adversary can repeatedly check all the possible combinations that are compatible with its observations. However, the approach of [1] is based on the probability of successful deduction/inference with just one guess while we use the number of guesses in a repeated scenario. This is similar to the brute-force guessing framework in [2] with the exception of avoiding distributions or statistics. The ratio of the worst-case number of guesses for the adversary in the presence of the outputs and in the absence of them captures the reduction in the adversary's guessing complexity and is thus used as a measure of information leakage.

Although a brute-force interpretation of leakage is used in this paper, we follow the axioms[1] of [1] for guiding the development of the information leakage metric. These axioms are, in fact, relevant to any notion of information leakage. Therefore, we require that the introduced information-leakage metric (R1) explain leakage in an operational manner (what leakage means in practice), (R2) require minimal assumptions about the privacy-intrusive adversary, (R3) satisfy properties, such as (R3.a) data-processing inequality (post processing does not increase leakage), (R3.b) independence property (independent outputs result in zero leakage), and (R3.c) additivity property (akin to composition rule in differential privacy), and finally, (R4) accord with intuition.

In summary, this paper makes the following contributions:

- Proposing a non-stochastic brute-force guessing framework for measuring information leakage in which the ratio of the worst-case number of guesses for the adversary in the presence of the output and in the absence of it is used to define a measure of information leakage;

The work of F. Farokhi is funded by the Melbourne School of Engineering. Aspects of this work was done while F. Farokhi was also affiliated with CSIRO's Data61. The work of Ni Ding is funded by the Doreen Thomas Postdoctoral Fellowship at the University of Melbourne.

---

[1] Not all the requirements in [1] are axioms, e.g., the requirement for the leakage to accord with intuition, but most can be regarded as fundamental properties required for private information leakage metric.

- Measuring leakage from the private data to the outputs when we are aware of adversary's intentions (i.e., what sensitive attribute/data it wants to guess) and when we are not aware of the adversary's intentions, which is defined based on the maximal information leakage;
- Demonstrating that the non-stochastic brute-force leakage satisfies the axioms outlined for information leakage in [1], such as operational interpretation, minimality of assumptions on the adversary, data-processing inequality, independence property, and additivity;
- Presenting identifiability, a new notion of privacy based on the developed maximal measure of information leakage, in this paper;
- Relating the non-stochastic information leakage based on the presented brute-force guessing framework to maximin information [8], which we prove stems naturally from one-shot guessing with perfect accuracy, and stochastic maximal leakage, which is shown to relate to stochastic one-shot guessing [1].

II. UNCERTAIN VARIABLES

We borrow the following concepts from [8]. Consider uncertainty set Ω. An uncertain variable, uv in short, is a mapping on Ω. For example, for uv $X : \Omega \to \mathbb{X}$, $X(\omega)$ is the realization of uv X corresponding to uncertainty $\omega \in \Omega$. For any two uvs X and Y, the set $[\![X, Y]\!] := \{(X(\omega), Y(\omega)) : \omega \in \Omega\} \subseteq [\![X]\!] \times [\![Y]\!]$ is their *joint range*. For uv X, $[\![X]\!] := \{X(\omega) : \omega \in \Omega\}$ denotes its *marginal range*. The *conditional range* of uv X, conditioned on realizations of uv Y belonging to the set $\mathcal{Y}$, is $[\![X|Y(\omega) \in \mathcal{Y}]\!] := \{X(\omega) : \exists\omega \in \Omega \text{ such that } Y(\omega) \in \mathcal{Y}\} \subseteq [\![X]\!]$. If $\mathcal{Y} = \{y\}$ is a singleton, $[\![X|Y(\omega) \in \{y\}]\!] = [\![X|Y(\omega) \in \mathcal{Y}]\!]$ is replaced with $[\![X|Y(\omega) = y]\!]$ or $[\![X|y]\!]$ when it is clear from the context. For any two uvs X and Y, we define the notation $[\![Y|X]\!] := \{[\![Y|X(\omega) = x]\!], \forall x \in [\![X]\!]\}$. We sometimes refer to $[\![Y|X]\!]$ as a non-stochastic channel as $[\![Y|X]\!]$ fully characterizes the non-stochastic communication channel from X to Y. In this paper, we only deal with *discrete* uvs possessing finite[2] ranges.

Uvs X_1 and X_2 are unrelated if $[\![X_1|X_2(\omega) = x_2]\!] = [\![X_1]\!]$ for all $x_2 \in [\![X_2]\!]$ and *vice versa*. Similarly, X_1 and X_2 are conditionally unrelated given Y if $[\![X_1|X_2(\omega) = x_2, Y(\omega) = y]\!] = [\![X_1|Y(\omega) = y]\!]$ for all $(x_2, y) \in [\![X_2, Y]\!]$. Uvs X_i, $i = 1, \dots, n$, are *unrelated* if $[\![X_1, \dots, X_n]\!] = [\![X_1]\!] \times \cdots \times [\![X_n]\!]$ and *conditionally unrelated* given Y if $[\![X_1, \dots, X_n|Y(\omega) = y]\!] = [\![X_1|Y(\omega) = y]\!] \times \cdots \times [\![X_n|Y(\omega) = y]\!]$ for all $y \in [\![Y]\!]$. Uvs X, Y, and Z form a Markov (uncertainty) chain, denoted by $X - Y - Z$, if X and Z are unrelated conditioned on Y, that is, $[\![X|Z(\omega) = z, Y(\omega) = y]\!] = [\![X|Y(\omega) = y]\!]$ for all $(z, y) \in [\![Z, Y]\!]$. Note that, by symmetry of the definition of unrelated uvs, $X - Y - Z$ forms a Markov chain if and only if $Z - Y - X$ forms a Markov chain. We say $X_1 - X_2 - \cdots - X_n$ forms a Markov chain if $X_i - X_j - X_\ell$ forms a Markov chain for any $1 \le i < j < \ell \le n$.

Non-stochastic entropy of uncertain variable X is defined as $H_0(X) := \log_2(|[\![X]\!]|)$. This is often described as the Hartley entropy [8], [9], which coincides with the Rényi entropy of order 0 for discrete variables [10], [11]. Conditional (or relative) entropy of uv X given Y is given by $H_0(X|Y) := \max_{y \in [\![Y]\!]} \log_2(|[\![X|Y(\omega) = y]\!]|)$. This is the Arimoto-Rényi conditional entropy of order 0 [10], [12]. Based on this, we can define $I_0(X; Y) := H_0(X) - H_0(X|Y)$. This is equivalent to the 0-mutual information [10], [13].

We end this section by presenting the definition of maximin information from non-stochastic information theory [8]. Consider uvs X and Y. Any $x, x' \in [\![X]\!]$ are $[\![X|Y]\!]$-overlap connected if there exists a finite sequence of conditional ranges $\{[\![X|Y(\omega) = y_i]\!]\}_{i=1}^{n}$ such that $x \in [\![X|Y(\omega) = y_1]\!]$, $x' \in [\![X|Y(\omega) = y_n]\!]$, and $[\![X|Y(\omega) = y_i]\!] \cap [\![X|Y(\omega) = y_{i+1}]\!] \neq \emptyset$ for all $i = 1, \dots, n-1$. We say $\mathcal{A} \subseteq [\![X]\!]$ is $[\![X|Y]\!]$-overlap connected if all $x, x' \in \mathcal{A}$ are $[\![X|Y]\!]$-overlap connected. Further, $\mathcal{A}, \mathcal{B} \subseteq [\![X]\!]$ are $[\![X|Y]\!]$-overlap isolated if there does not exist $x \in \mathcal{A}, x' \in \mathcal{B}$ such that x, x' are $[\![X|Y]\!]$-overlap connected. An $[\![X|Y]\!]$-overlap partition is a partition of $[\![X]\!]$ such that each member set is $[\![X|Y]\!]$-overlap connected and any two member sets are $[\![X|Y]\!]$-overlap isolated. There always exists a unique $[\![X|Y]\!]$-overlap partition [8], which is denoted by $[\![X|Y]\!]_\star$. The maximin information is $I_\star(X; Y) := \log_2(|[\![X|Y]\!]_\star|)$. In [8], it is proved that $|[\![X|Y]\!]_\star| = |[\![Y|X]\!]_\star|$ and thus $I_\star(X; Y) = I_\star(Y; X)$. The overlap partition captures common uv [14], an extension of common random variable [15] to uvs. This relationship explains the relationship between entropy of the common uv, which is equal to the maximin information, and the zero-error capacity [8], [15].

III. INFORMATION LEAKAGE IN BRUTE-FORCE GUESSING

Consider uv X containing sensitive data U, which is interpreted as some attribute or feature of X that is computable by some function $g : [\![X]\!] \to [\![U]\!]$, i.e., $U = g \circ X$. Note that, by construction, $|[\![U]\!]| \le |[\![X]\!]|$. Let Y be an observable uv that depends on X, e.g., X and Y are the input and output, respectively, of a (privacy-preserving) channel.[3] These uvs form a Markov chain $U - X - Y$. An adversary wants to guess U correctly given Y. For instance, consider an example in which X captures weight and height of an individual, and U denotes body mass index. In such an example, insurance agencies might be interested in deducing the body mass index of an individual (due to its correlation with heart disease) based on publicly released data Y while they do not have any particular interest in learning an individual's height and weight separately.

We assume that the adversary can guess the value of U in a brute-force trial-and-error manner. That is, the adversary chooses a distinct element $u \in [\![U]\!]$ each time and tests[4] whether the actual value $U(\omega)$ equals u. The adversary repeats

---

[2] Extension to countably infinite sets is straightforward with extra care when manipulating extended real numbers (i.e., infinity).

[3] The conditional range $[\![Y|X]\!]$ characterizes this channel, which can also be regarded as a non-stochastic privacy-preserving scheme.

[4] We assume that the adversary has access to an oracle that can determine whether $U(\omega)$ is equal to u (for a given $u \in [\![U]\!]$) or not.

this procedure until the answer is 'yes'. We consider the number of trials before the successful guess. Without observations of Y, the adversary must try at most $|\llbracket U \rrbracket|$ times. However, with access to observation $Y(\omega) = y \in \llbracket Y \rrbracket$, the actual value of $U(\omega)$ lies in the conditional range $\llbracket U|Y(\omega) = y \rrbracket$ and therefore the maximum number of trials is $|\llbracket U|Y(\omega) = y \rrbracket|$. Since the number of trials is proportional to the inference cost/effort of the adversary, the ratio $|\llbracket U \rrbracket|/|\llbracket U|Y(\omega) = y \rrbracket|$ captures the reduction in the adversary's maximum cost for guessing U upon the observation $\llbracket U|Y(\omega) = y \rrbracket$. This coincides with the definition of the information gain $\log_2(|\llbracket U \rrbracket|/|\llbracket U|Y(\omega) = y \rrbracket|)$ in [16], where $\log_2(|\llbracket U|Y(\omega) = y \rrbracket|)$ denotes the 'combinatorial' conditional entropy. The adversary's reduction in guessing cost can be interpreted as the information gained about uv U from the observation $Y(\omega) = y$.

Note that the measure $\log_2(|\llbracket U \rrbracket|/|\llbracket U|Y(\omega) = y \rrbracket|)$ is also consistent with the *stochastic brute-force guessing leakage* $H_G(U) - \mathbb{E}_Y[H_G(U|Y(\omega) = y)]$ proposed in [2, Definition 3] for rvs U and X. This measure is based on the guessing entropy[5] in [17] defined as $H_G(U) := \sum_{i=1}^{|\llbracket U \rrbracket|} i\mathbb{P}\{U(\omega) = u_i\}$, where $(u_i)_{i=1}^{|\llbracket U \rrbracket|}$ are ordered elements such that $\mathbb{P}\{U(\omega) = u_1\} \geq \mathbb{P}\{U(\omega) = u_2\} \geq \ldots \geq \mathbb{P}\{U(\omega) = u_{|\llbracket U \rrbracket|}\}$. Similarly, the conditional guessing entropy is $H_G(U|Y(\omega) = y) = \sum_{i=1}^{|\llbracket U|Y(\omega)=y \rrbracket|} i\mathbb{P}\{U(\omega) = \tilde{u}_i|Y(\omega) = y\}$ for each $y \in \llbracket Y \rrbracket$, where $(\tilde{u}_i)_{i=1}^{|\llbracket U|Y(\omega)=y \rrbracket|}$ are again ordered elements such that $\mathbb{P}\{U(\omega) = \tilde{u}_1|Y(\omega) = y\} \geq \mathbb{P}\{U(\omega) = \tilde{u}_2|Y(\omega) = y\} \geq \ldots \geq \mathbb{P}\{U(\omega) = \tilde{u}_{|\llbracket U|Y(\omega)=y \rrbracket|}|Y(\omega) = y\}$. When there is no σ-field or probability measure over $\llbracket U \rrbracket$, $H_G(U)$ and $H_G(U|Y(\omega) = y)$ reduce to the prior guessing cost $\log_2(|\llbracket U \rrbracket|)$ and posterior guessing cost $\log_2(|\llbracket U|Y(\omega) = y \rrbracket|)$, respectively, by replacing the expectation with the worst-case. To quantify the *non-stochastic brute-force guessing leakage*, we consider the difference between $\log_2(|\llbracket U \rrbracket|)$ and the minimum guessing cost $\min_{y \in \llbracket Y \rrbracket} \log_2(|\llbracket U|Y(\omega) = y \rrbracket|)$ as follows.

Definition 1 (Non-Stochastic Brute-force Guessing Leakage)**.** *For a given uv U, the non-stochastic leakage from U to Y is*

$$\begin{aligned}\mathcal{L}(U \to Y) &= \log_2 \left(\frac{|\llbracket U \rrbracket|}{\min\limits_{y \in \llbracket Y \rrbracket} |\llbracket U|Y(\omega) = y \rrbracket|} \right) \\ &= \max_{y \in \llbracket Y \rrbracket} \log_2 \left(\frac{|\llbracket U \rrbracket|}{|\llbracket U|Y(\omega) = y \rrbracket|} \right).\end{aligned}$$

The measure $\mathcal{L}(U \to Y)$ quantifies the maximum reduction in the guessing cost of the adversary after observing Y, which indicates the most information gained by the adversary in the sense of [16]. This measure has been previously used as the non-stochastic information leakage in [6], [7] for privacy analysis, e.g., in the case of k-anonymity [6]. Hence, this definition provides an operative meaning to the non-stochastic information leakage and can be used as its interpretation for privacy analysis.

In the following proposition, we show that non-stochastic leakage satisfies the data-processing inequality. This implies that, for a given uv X and a specified attribute U of X, the leakage is non-increasing along cascading channels $\llbracket Y|X \rrbracket$ and $\llbracket Z|Y \rrbracket$. This is in line with axiom R3.a of an operational notion of information leakage in [1]. This is an important requirement as it shows that a curator does not need to worry about an increased risk incurred by any post processing after releasing outputs.

Proposition 1 (Post Processing Inequality)**.** *If Markov chain $U - X - Y - Z$ holds, $\mathcal{L}(U \to Z) \leq \mathcal{L}(U \to Y)$.*

Proof: Due to page limits, the proofs are presented in a technical note online [18]. ■

The following result shows the leakage is equal to zero if two uvs are unrelated. Evidently, the most private case arises from ensuring that X and Y are unrelated because the leakage is always greater and equal to zero. In this case, the realizations of Y do not provide any useful information about X or its derivatives, e.g., U. This is again in line with axiom R3.b of an operational notion of information leakage [1].

Proposition 2 (Bounding Leakage)**.** $\mathcal{L}(U \to Y) \geq 0$ *with equality if X and Y are unrelated.*

Proof: See our online technical note [18]. ■

For the Markov chain $U - X - Y$, the measure $\mathcal{L}(U \to Y)$ can be used to quantify the non-stochastic brute-force guessing leakage if we know attribute U of X that is targeted by the adversary. However, there are some real-world situations that we do not know *a priori* the intention of the adversary, i.e., the attribute U of X that the adversary is trying to infer. In some cases, more than one user may observe Y and each user might be interested in guessing/estimating a different attribute of X. In these situations, it is required to consider the brute-force guessing leakage $\mathcal{L}(U \to Y)$ when the attribute U varies. Therefore, we need to define a maximal non-stochastic guessing leakage. This is in-line with axiom R2 in [1]. We consider such situations in the next section.

IV. MAXIMAL NON-STOCHASTIC LEAKAGE

For given uv X and the released output Y, we define the maximal non-stochastic brute-force guessing leakage over all attributes U as follows.

Definition 2 (Maximal Non-Stochastic Brute-Force Leakage)**.** *The maximal non-stochastic leakage from X to Y is defined as*

$$\mathcal{L}_\star(X \to Y) = \sup_{U:\, U - X - Y} \mathcal{L}(U \to Y), \tag{1}$$

where the supremum is taken over all functions $g : \llbracket X \rrbracket \to \llbracket U \rrbracket$ with $\llbracket U \rrbracket$ containing finite arbitrary alphabets.

The maximal non-stochastic brute-force leakage only depends on uvs X and Y. The maximizer of (1) denotes the

---

[5] The guessing entropy $H_G(U)$ denotes the minimum average number of trials for guessing the realization of U. This results from the optimal brute-force guessing strategy of the adversary to pick $u_i \in \llbracket U \rrbracket$, i.e., the element in $\llbracket U \rrbracket$ with the i-th largest probability $\mathbb{P}\{U(\omega) = u_i\}$, at the i-th trial [17].

most vulnerable attributes U to the brute-force guessing over $\llbracket Y|X\rrbracket$; The supremum of (1) indicates the lowest data privacy level the channel $\llbracket Y|X\rrbracket$ provides.

Now, we can show that maximal non-stochastic leakage admits axiom R3 in the axiomatic approach to operational information leakage in [1]. That is, maximal non-stochastic leakage satisfies post processing inequality (post processing does not increase leakage), unrelatedness (unrelated outputs result in zero leakage, c.f., independence in maximal stochastic leakage), and additivity.

Proposition 3 (Properties of Maximal Leakage)**.** *The following holds:*

a) $\mathcal{L}_\star(X \to Y) \geq 0$;
b) $\mathcal{L}_\star(X \to Y) = 0$ *if and only if* X *is unrelated to* Y;
c) $\mathcal{L}_\star(X \to Y) \leq H_0(X)$ *with the equality if* $Y = X$;
d) $\mathcal{L}_\star(X \to Z) \leq \mathcal{L}_\star(X \to Y)$ *if Markov chain* $X - Y - Z$ *holds;*
e) *If* (X_i, Y_i), $\forall i$, *are unrelated, i.e.,* (X_i, Y_i) *and* $(X_{i'}, Y_{i'})$ *are unrelated* $\forall i \neq i'$, *then* $\mathcal{L}_\star((X_1, \dots, X_n) \to (Y_1, \dots, Y_n)) = \sum_{i=1}^n \mathcal{L}(X_i \to Y_i)$.

Proof: See our online technical note [18]. ■

Now, we are ready to present a formula for computing the maximal non-stochastic leakage in the next proposition.

Proposition 4 (Computing Maximal Leakage)**.** $\mathcal{L}_\star(X \to Y) = \log_2(|\llbracket X\rrbracket| - \min_{y\in\llbracket Y\rrbracket} |\llbracket X|Y(\omega) = y\rrbracket| + 1)$.

Proof: See our online technical note [18]. ■

Corollary 5. *$\mathcal{L}_\star(X \to Y)$ is not symmetric in general.*

Proof: See our online technical note [18]. ■

In the next section, we introduce non-stochastic identifiability as a new notion of privacy, motivated by the expression for the maximal leakage in Proposition 4.

V. NON-STOCHASTIC IDENTIFIABILITY

We define non-stochastic identifiability by requiring that the ratio of the cardinality of the set of compatible realization of uv X with access to the measurements of uv Y over the cardinality of the set of compatible realization of uv X without this auxiliary information is lower bounded by an exponential of the privacy budget. This implies that access to the realizations of Y does not significantly reduce the cardinality of the set of possibilities that must be tested for guessing the realization of X. This definition is in consistent with stochastic identifiability in [19], [20] which requires that the posterior distribution (instead of the conditional range) to remain similar with and without access to privacy-preserving measurements.

Definition 3 (Non-Stochastic Identifiability)**.** *Any mapping $\mathfrak{M}$ is ϵ-identifiable, for $\epsilon > 0$, if*

$$|\llbracket X|Y(\omega) = y\rrbracket| \geq |\llbracket X\rrbracket| 2^{-\epsilon}, \quad \forall y \in \llbracket Y\rrbracket, \tag{2}$$

with $Y = \mathfrak{M} \circ X$.

We refer to ϵ in the non-stochastic identifiability as the *privacy budget*. By decreasing the privacy budget, we ensure a higher level of privacy (cf., differential privacy [21] and identifiability [19]). This is intuitively because, by decreasing the privacy budget, the size of the set $\llbracket X|Y(\omega) = y\rrbracket$ increases and thus guessing the actual realization of uv X becomes more complex.

Corollary 6. *For any ϵ-identifiable mapping $\mathfrak{M}$, $\mathcal{L}_\star(X \to Y) \leq \log_2(|\llbracket X\rrbracket|(1 - 2^{-\epsilon}) + 1)$.*

Proof: See our online technical note [18]. ■

Corollary 6 shows that, as expected, the maximal non-stochastic brute-force guessing leakage $\mathcal{L}_\star(X \to Y)$ goes to zero as the privacy budget approaches zero. By increasing the privacy budget, however, we increase the bound on the maximal non-stochastic brute-force guessing leakage $\mathcal{L}_\star(X \to Y)$ and therefore more private information could be potentially leaked.

VI. BRUTE-FORCE TO ONE-SHOT GUESS

In the previous section, we considered a brute-force guessing adversary that can potentially check all the possibilities. In this section, we restrict ourselves to one-shot guesses. We first analyze the non-stochastic case and its relationship with the non-stochastic brute-force guessing.

A. Non-Stochastic One-Shot Guessing

Let us consider an adversary with only a single opportunity for guessing the private realization of uv U by observing the realization of uv Y. For instance, consider the problem of guessing a person's password based on side-channel information (e.g., inter-keystroke delay as in [1]) while the system locks immediately after one wrong guess. Therefore, the adversary is interested in finding the largest amount of information that can be deduced correctly with one guess. This happens when $|\llbracket U|Y(\omega) = 1\rrbracket| = 1$ for all $y \in \llbracket Y\rrbracket$. In the next proposition, we show that the maximum information is the largest amount of information can be leaked to such an adversary. We further relate this notion of leakage to maximal non-stochastic leakage with brute-force guessing.

Proposition 7 (Maximal Leakage Bounds Maximin Info)**.** *For uvs X and Y,*

$$I_\star(X;Y) = \sup_{\substack{U:\, U - X - Y,\\ |\llbracket U|Y(\omega) = y\rrbracket| = 1,\\ \forall y \in \llbracket Y\rrbracket}} \mathcal{L}(U \to Y) \leq \mathcal{L}_\star(X \to Y),$$

where the supremum is taken over all $g : \llbracket X\rrbracket \to \llbracket U\rrbracket$ such that $|\{g(x) \colon x \in \llbracket X|Y(\omega) = y\rrbracket\}| = |\llbracket U|Y(\omega) = y\rrbracket| = 1$.

Proof: See our online technical note [18]. ■

Remark 1 (Relationship with Zero-Error Capacity)**.** *Following Proposition 7 and [8], the zero-error capacity of any memoryless uncertain channel satisfies $C_0 = \sup_{\llbracket X\rrbracket \subseteq \mathbb{X}} I_\star(X;Y) \leq \sup_{\llbracket X\rrbracket \subseteq \mathbb{X}} \mathcal{L}_\star(X \to Y)$. Therefore, based on Corollary 6, the zero-error capacity of any memoryless ϵ-identifiable channel* *is upper bounded by* $\log_2(|\mathbb{X}|(1-2^{-\epsilon})+1)$*, where* $|\mathbb{X}|$ *is the number of the input alphabets. This constraints dynamical systems that can be estimated or stabilized through privacy-preserving communication channels [8], [22].*

In the next subsection, we consider one-shot guessing in the stochastic sense of [1] and investigate its relationship with the maximal non-stochastic leakage with brute-force guessing.

B. Maximal Stochastic Leakage

We can recreate the stochastic framework for information leakage in [1] by endowing all the uncertain variables in this paper with a measure.

Definition 4 (Maximal Stochastic Leakage)**.** *For jointly distributed rvs* X *and* Y*, the maximal stochastic leakage from* X *to* Y *is given by*

$$\begin{aligned}&\widetilde{\mathcal{L}}(X \to Y)\\&\quad= \sup_{U:\, U-X-Y} \log_2\left(\frac{\mathbb{E}\left\{\max\limits_{u\in[\![U]\!]} \mathbb{P}\{U=u|Y=y\}\right\}}{\max\limits_{u\in[\![U]\!]} \mathbb{P}\{U=u\}}\right),\end{aligned}$$

where supremum is taken over all random variables (rvs) U *taking values in finite arbitrary alphabets. It was shown in [1] that*

$$\begin{aligned}\widetilde{\mathcal{L}}(X \to Y) &= \log_2\left(\sum_{y\in[\![Y]\!]} \max_{x\in[\![X]\!]} \mathbb{P}\{Y=y|X=x\}\right)\\&= I_\infty(X;Y),\end{aligned}$$

where I_∞ *is the Sibson mutual information* I_α *with* $\alpha \to \infty$ *[13], [23]. Note the fact that* $\{x\colon \mathbb{P}\{X=x\}>0\} = [\![X]\!]$*.*

In the next proposition, we show that the worst-case maximal stochastic leakage provides a bound for the maximal non-stochastic brute-force leakage. Therefore, we can interpret the maximal non-stochastic brute-force leakage as a robust non-stochastic counterpart of the maximal stochastic leakage.

Proposition 8 (Relating Maximal Leakages)**.** $\mathcal{L}_\star(X \to Y) \le \sup_{\mathbb{P}\{Y=y|X=x\}} \widetilde{\mathcal{L}}(X \to Y) + H_0(X|Y)$*.*

Proof: See our online technical note [18]. ■

VII. CONCLUSIONS AND FUTURE WORK

We developed an interpretable notion of non-stochastic information leakage based on guessing in a non-stochastic framework. We considered brute-force guessing in which an adversary can potentially check all the possibilities of the private information that are compatible with the available outputs to find the actual private realization. The ratio of the worst-case number of guesses for the adversary in the presence of the output and in the absence of it captures the reduction in the adversary's guessing complexity and is thus used as a measure of information leakage. We computed the maximal non-stochastic leakage over all sensitive attributes that could be targeted by the adversary and compared it with non-stochastic identifiabiliy, maximin information, and stochastic maximal leakage. Future work can focus on extending this definition to a dynamic framework with continual observations.

REFERENCES

[1] I. Issa, A. B. Wagner, and S. Kamath, "An operational approach to information leakage," *IEEE Transactions on Information Theory*, vol. 66, no. 3, pp. 1625–1657, 2020.

[2] S. A. Osia, B. Rassouli, H. Haddadi, H. R. Rabiee, and D. Gündüz, "Privacy against brute-force inference attacks," in *2019 IEEE International Symposium on Information Theory (ISIT)*, pp. 637–641, 2019.

[3] J. Liao, O. Kosut, L. Sankar, and F. P. Calmon, "A tunable measure for information leakage," in *2018 IEEE International Symposium on Information Theory (ISIT)*, pp. 701–705, IEEE, 2018.

[4] R. Bild, K. A. Kuhn, and F. Prasser, "SafePub: A truthful data anonymization algorithm with strong privacy guarantees," *Proceedings on Privacy Enhancing Technologies*, vol. 2018, no. 1, pp. 67–87, 2018.

[5] R. Bhaskar, A. Bhowmick, V. Goyal, S. Laxman, and A. Thakurta, "Noiseless database privacy," in *International Conference on the Theory and Application of Cryptology and Information Security*, pp. 215–232, 2011.

[6] F. Farokhi, "Development and analysis of deterministic privacy-preserving policies using non-stochastic information theory," *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 10, pp. 2567–2576, 2019.

[7] N. Ding and F. Farokhi, "Developing non-stochastic privacy-preserving policies using agglomerative clustering," *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 3911–3923, 2020.

[8] G. N. Nair, "A nonstochastic information theory for communication and state estimation," *IEEE Transactions on Automatic Control*, vol. 58, no. 6, pp. 1497–1510, 2013.

[9] R. V. L. Hartley, "Transmission of information," *Bell System Technical Journal*, vol. 7, no. 3, pp. 535–563, 1928.

[10] I. Sason and S. Verdú, "Arimoto–Rényi conditional entropy and bayesian m-ary hypothesis testing," *IEEE Transactions on Information Theory*, vol. 64, no. 1, pp. 4–25, 2017.

[11] A. Rényi, "On measures of entropy and information," in *Proceedings of the 4th Berkeley Symposium on Mathematical Statistics and Probability, Volume 1: Contributions to the Theory of Statistics*, 1961.

[12] S. Arimoto, "Information measures and capacity of order α for discrete memoryless channels," in *Proceedings of the 2nd Colloquium on Topics on Information Theory, Keszthely, Hungary*, vol. 16, p. 1975.

[13] S. Verdú, "α-mutual information," in *2015 Information Theory and Applications Workshop (ITA)*, pp. 1–6, 2015.

[14] A. Mahajan, "On the relationship between maximin information and common knowledge," 2014. Technical Note, http://www.ece.mcgill.ca/~amahaj1/projects/information/preprint/maximin-information.pdf.

[15] S. Wolf and J. Wultschleger, "Zero-error information and applications in cryptography," in *Information Theory Workshop*, pp. 1–6, 2004.

[16] A. N. Kolmogorov and V. M. Tikhomirov, "ε-entropy and ε-capacity of sets in function spaces," *Uspekhi Matematicheskikh Nauk*, vol. 14, no. 2, pp. 3–86, 1959. English translation American Mathematical Society Translations, series 2, vol. 17, pp. 277–364.

[17] J. L. Massey, "Guessing and entropy," in *Proceedings of 1994 IEEE International Symposium on Information Theory*, pp. 204–, June 1994.

[18] F. Farokhi and N. Ding, "Measuring information leakage in non-stochastic brute-force guessing," 2020. Technical Note, arXiv:2004.10911 [cs.IT], https://arxiv.org/abs/2004.10911.

[19] W. Wang, L. Ying, and J. Zhang, "On the relation between identifiability, differential privacy, and mutual-information privacy," *IEEE Transactions on Information Theory*, vol. 62, no. 9, pp. 5018–5029, 2016.

[20] J. Lee and C. Clifton, "Differential identifiability," in *Proceedings of the 18th ACM SIGKDD international conference on Knowledge discovery and data mining*, pp. 1041–1049, 2012.

[21] C. Dwork, F. McSherry, K. Nissim, and A. Smith, "Calibrating noise to sensitivity in private data analysis," in *Theory of Cryptography Conference*, pp. 265–284, Springer, 2006.

[22] A. S. Matveev and A. V. Savkin, "Shannon zero error capacity in the problems of state estimation and stabilization via noisy communication channels," *International Journal of Control*, vol. 80, no. 2, pp. 241–255, 2007.

[23] R. Sibson, "Information radius," *Zeitschrift für Wahrscheinlichkeitstheorie und Verwandte Gebiete*, vol. 14, pp. 149–160, June 1969.

Author/s:
Farokhi, F;Ding, N

Title:
Measuring Information Leakage in Non-stochastic Brute-Force Guessing

Date:
2021-04-11

Citation:
Farokhi, F. & Ding, N. (2021). Measuring Information Leakage in Non-stochastic Brute-Force Guessing. 2020 IEEE Information Theory Workshop (ITW), 00, IEEE. https://doi.org/10.1109/itw46852.2021.9457602.

Persistent Link:
http://hdl.handle.net/11343/278811