When not all bits are equal: worth-based information flow

Mário S. Alvim[1], Andre Scedrov[1], and Fred B. Schneider[2]

[1] University of Pennsylvania, USA
[2] Cornell University, USA

Abstract. Only recently have approaches to quantitative information flow started to challenge the presumption that all leaks involving a given number of bits are equally harmful. This paper proposes a framework to capture the semantics of information, making the quantification of leakage independent of the syntactic representation of secrets. Secrets are defined in terms of fields, which are combined to form structures; and a worth assignment is introduced to associate each structure with a worth (perhaps in proportion to the harm that would result from disclosure). We show how worth assignments can capture inter-dependence among structures within a secret, allowing the modeling of: (i) secret sharing; (ii) information-theoretical predictors; and (iii) computational (as opposed to information-theoretic) guarantees for security. Using non-trivial worth assignments we generalize Shannon entropy, guessing entropy, and probability of guessing. For deterministic systems, we give a lattice of information to provide an underlying algebraic structure for the composition of attacks. Finally, we outline a design technique to capture into worth assignments relevant aspects of a scenario of interest.

1 Introduction

Quantitative information flow (QIF) is concerned with measuring how much information about a system's secrets leaks to an adversary. The adversary is presumed to have *a priori information* about the secrets before execution starts and to access *public observables* as execution proceeds. By combining a priori information and public observables, the adversary achieves *a posteriori information* about the secrets. The *leakage* from an execution is then computed as the difference between a posteriori and a priori information.

This definition of leakage depends on how information is measured. Cachin [1] advocates that such definitions not only include a way to calculate some numeric value but also offer an *operational interpretation*, which describes what aspect of the scenario of interest is quantified by the information measure. Popular definitions of information include: *Shannon entropy* [2–8], which measures how much information is leaked per guess; *guessing entropy* [9, 10], which measures how many tries are required before the secret is correctly guessed; and *probability of guessing* [11, 12], which measures how likely it is that the secret is correctly inferred in a certain number of tries.

These definitions are best suited to sets of monolithic and equally valuable secrets, and researchers have recently begun to consider richer scenarios. The *g-leakage* framework [13] of Alvim et al. makes use of gain functions to quantify the benefit of different guesses for the secret. The broad flexibility of gain-functions, however, makes it hard to determine appropriate instances for all cases of interest. Moreover, that framework generalizes probability of guessing, but not Shannon entropy or guessing entropy. Finally, it is not suitable to infinitely risk-averse adversaries. In this paper we propose an approach that addresses these limitations; a detailed comparison with g-leakage is given in Section 6.1.

We model a secret as partitioned into *fields*, which are combined to form *structures*. Since different structures might cause different harms, a *worth assignment* is introduced to associate a *worth* with each structure. For instance, the secret corresponding to a client's bank account might comprise two 7-digit structures: a pincode and a telephone number. Leaking the pincode has the potential to cause considerable harm, so that structure is assigned high worth; the telephone number would generally be public information, so this structure is assigned low worth.

Assuming that all structures are equally sensitive can lead to inadequate comparisons between systems that leak structures with different worths but the same numbers of bits. Conversely, ignoring the structure of secrets may lead to deceptive estimations of the harm from leaking different numbers of bits. Consider two systems that differ in the way they represent a house address. In system C_1, standard postal addresses are used (i.e., a number, street name, and zip-code); system C_2 uses GPS coordinates (i.e., a latitude and a longtitude, each a signed 10-digit numbers). Under Shannon entropy with plausible sizes[3] for address fields, C_1 requires 129 bits to represent a location that C_2 represents using 49 bits. Yet the same content is revealed whether C_1 leaks its 129 bits or C_2 leaks its 49 bits. (The a priori information for addresses in C_1 is not zero, since certain values for a house number, street name, and zip-code can be ruled out. And a similar argument can be made for C_2, given knowledge of habitable terrain. Accounting for idiosyncrasies in the syntactic representation of secrets, however, can be a complicated task, hence an opportunity to introduce analysis mistakes. Worth assignments avoid some of that complexity.)

Since secrets are no longer modeled as monolithic, distinct structures within a same secret may be correlated. A clever adversary, thus, might infer information about a structure with more worth (and presumably better protected) by attacking a correlated structure with less worth (and presumably less well protected). For instance, the location of a neighborhood is often correlated to the political preferences of its residents, so an adversary may target at a person's house address to estimate what party they support. Worth assignments can model such correlations and appropriately adjust the relative worth of structures. Moreover, they can capture the computational complexity of obtaining one structure from the other, which is a common limitation of information theoretical approaches

[3] Specifically, we assume a 4-digit house number, a 20-character alphabetic street name, and a 5-digit zip-code.

to QIF. As an example, a public RSA key is a perfect predictor, in an information theoretical sense, for the corresponding private key. In practice, however, learning the public key should not be assigned the same worth as learning the private key because no realistic adversary is expected to retrieve the latter from the former in viable time.

In this paper we propose *measures of information worth* that incorporate the structure and worth of secrets. As in other QIF literature, we assume the adversary performs attacks, controlling the low input to a probabilistic system execution and observing the low outputs. An attack induces a probability distributions on the space of secrets according to what the adversary observes. This characterization admits measures of information worth for the information contained in each distribution; leakage is then defined as the difference in information between two distributions. Our approach generalizes probability of guessing, guessing entropy, and Shannon entropy to admit non-trivial worth assignments. Yet our work remains consistent with the Lattice of Information [14] for deterministic systems, which is an underlying algebraic structure for sets of system executions. The main contributions of this paper are:

1. We propose a framework of structures and worth assignments to capture the semantics of information, making the quantification of leakage independent of the particular representation chosen for secrets.
2. We show how to use worth assignments to model the inter-dependability among structures within a same secret, capturing practical scenarios including: (i) secret sharing; (ii) information theoretical predictors; and (iii) computational (as opposed to information-theoretic) guarantees for security.
3. We generalize Shannon entropy and guessing entropy to incorporate worth explicitly, and we introduce other measures without traditional equivalents. We show that our theory of measures of information worth and the g-leakage framework are not comparable in general, although they do overlap.
4. We prove that our measures of information worth are consistent with respect to the Lattice of Information for deterministic systems, which allows sound reasoning about the composition of attacks in such systems.
5. We outline a design technique to capture into worth assignments the following aspects of the scenario of interest: (i) *sensitivity requirements* that determine what structures are intrinsically sensitive, and by how much; (ii) *consistency requirements* that ensure the adequacy of the worth assignment; and (iii) the adversary's *side knowledge* that may be of help in attacks.

Plan of the paper. The paper is organized as follows. Section 2 describes our model for the structure and worth of secrets in probabilistic systems. Section 3 uses worth assignments to propose measures of information worth. Section 4 shows that the proposed measures are consistent with respect to the Lattice of Information for deterministic systems under composite attacks. Section 5 outlines a technique for designing adequate worth assignments for a scenario of interest. Finally, Section 6 discusses related work, and Section 7 concludes the paper.

2 Modeling the structure and worth of secrets

We decompose secrets into elementary units called *fields*, each a piece of information with a domain. Let $\mathcal{F} = \{f_1, \ldots, f_m\}$ denote the (finite) set of fields in some scenario of interest, and for $1 \leq i \leq n$, let $domain(f_i)$ be the domain of values for field f_i. A *structure* is a subset $\mathfrak{f} \subseteq \mathcal{F}$, and if $\mathfrak{f} = \{f_{i_1}, \cdots, f_{i_k}\}$, its domain is given by $domain(\mathfrak{f}) = domain(f_{i_1}) \times \cdots \times domain(f_{i_k})$. The set of all possible structures is the power set $\mathcal{P}(\mathcal{F})$ of fields, and the structure $\mathfrak{f} = \mathcal{F}$ containing all fields is called the *maximal structure*.

A *secret* s is a mapping from the maximal structure to values, i.e., $s = \langle s[f_1], \ldots, s[f_m] \rangle$, where $s[f_i] \in domain(f_i)$ is the value assumed by field f_i. Hence the set $\mathcal{S}$ of possible secrets is $\mathcal{S} = domain(\mathcal{F})$. Given a secret s and a (not necessarily maximal) structure $\mathfrak{f} \subseteq \mathcal{F}$, we call a *sub-secret* $s[\mathfrak{f}]$ the projection of s on the domain of $\mathfrak{f}$, and the set of all possible sub-secrets associated with that structure is $\mathcal{S}[\mathfrak{f}] = domain(\mathfrak{f})$.

Structures may carry some valuable piece of information on their own. A *worth assignment* attributes to each structure a non-negative, real number. Worth may be seen as the utility obtained by an adversary who learns the contents of the structure, or as the damage suffered should the contents of the structure become known to that adversary.

Definition 1 (Worth assignment). *A* worth assignment *is a function* $\omega : \mathcal{P}(\mathcal{F}) \rightarrow \mathbb{R}$ *from the set of structures to reals, satisfying for all* $\mathfrak{f}, \mathfrak{f}' \in \mathcal{P}(\mathcal{F})$*:* (i) non-negativity*:* $\omega(\mathfrak{f}) \geq 0$*; and* (ii) monotonicity*:* $\mathfrak{f} \subseteq \mathfrak{f}' \implies \omega(\mathfrak{f}) \leq \omega(\mathfrak{f}')$*.*

We require non-negativity of ω because the knowledge of the contents of a structure should not carry a negative amount of information; and we require monotonicity because every structure should be at least as sensitive as any of its parts. Note that monotonicity implies that the worth of the maximal structure, $\omega(\mathcal{F})$, is an upper bound for the worth of every other structure.

The expressiveness of worth assignments The worth of a structure should appropriately represent the sensitivity of that structure in a scenario of interest. Consider a medical database where a secret is a patient's entire record, and structures are sub-sets of that record (e.g., a patient's name, age, smoking habits). The worth assigned to an individual's smoking habits should reflect: (i) how much the *protector* (i.e., the party interested in keeping the secret concealed) cares about hiding, in itself, whether an individual is a smoker; (ii) how much an adversary would benefit from learning, in itself, whether an individual is a smoker; and, more subtly, (iii) how effective (information-theoretically and/or computationally) of a predictor an individual's smoking habits are for other sensitive structures (e.g., heavy smokers are more likely to develop lung cancer, and insurance companies may deny them coverage based on that). Worth assignments can capture these factors. They can also model:

a) **Semantic-based leakage.** Worth assignments provide a natural means to abstract away from syntactic idiosyncrasies, treating structures according to their meaning. In the bank system of the introduction, for instance, we would assign a higher worth to the 7-digit pincode than to the 7-digit telephone number, thus discriminating eventual 7-digit leaks in terms of their relevance:

$$\omega(\{\mathsf{pincode}\}) > \omega(\{\mathsf{telephone\ number}\}).$$

Conversely, structures with equivalent meanings should be assigned the same worth, regardless of their representation. For instance, the worth of a structure corresponding to address should be the same, whether it is represented in GPS coordinates or in the standard postal address format:

$$\omega(\{\mathsf{GPS\ address}\}) = \omega(\{\mathsf{postal\ address}\}).$$

b) **Secret sharing.** The combination of two structures may convey more worth than the sum of their individual worths. In *secret sharing*, for instance, different persons retain distinct partial secrets (i.e., structures) that in isolation give no information about the secret as a whole (i.e., the maximal structure), but that reveal the entire secret when combined. As another example, a decryption key without any accompanying ciphertext is of little worth, so each corresponding structure should have, in isolation, a worth close to zero. When combined, however, the benefit these structures provide to the adversary substantially exceeds the sum of their individual worths:

$$\omega(\{\mathsf{ciphertext}, \mathsf{decryption\ key}\}) \gg \omega(\{\mathsf{ciphertext}\}) + \omega(\{\mathsf{decryption\ key}\}).$$

c) **Correlation of structures.** The knowledge of a particular structure may imply the knowledge of another one (e.g., if the adversary has access to tax files, learning someone's tax identification number implies learning their name as well); or may at least increase the probability of learning other structure (recall the correlation between smoking habits and lung cancer). An adversary might exploit correlations between different structures within a same secret to obtain information about a more important (and presumably better protected) structure through a less important (and presumably less well protected) structure. By considering the distribution on secrets and the capabilities of the adversary, we can adjust the relative worth of one structure with respect to any other, thus avoiding potentially harmful loopholes. In particular, worth assignments can model:

   (i) **Information theoretical predictors.** The worth of every structure should reflect the worth it carries, via correlation, from other structures. For instance, when an individual's identity can be recovered with 60% accuracy from the combination of his zip-code, date of birth, and gender [15], we ought to make the worth $\omega(\{\mathsf{zip\text{-}code}, \mathsf{date\ of\ birth}, \mathsf{gender}\})$ at least as great as 60% of the worth $\omega(\{\mathsf{identity}\})$. More generally, given any two structures $\mathfrak{f}, \mathfrak{f}' \in \mathcal{P}(\mathcal{F})$, the requirement

$$\omega(\mathfrak{f}) \geq \mathit{correlation}(\mathfrak{f}, \mathfrak{f}') \cdot \omega(\mathfrak{f}')$$

   may be imposed on a worth assignment ω. Here $\mathit{correlation}(\mathfrak{f}, \mathfrak{f}')$ is a function representing how precise of a predictor $\mathfrak{f}$ is for $\mathfrak{f}'$.

(ii) **Computational effort.** As the issue of retrieving a private RSA key from the corresponding public key attests, even perfect information-theoretic correlations among structures may not be of practical use for the adversary. Worth assignments can adjust the worth obtainable by computing one structure from another, given the effort involved. We can impose, on any two structures $\mathfrak{f}, \mathfrak{f}' \in \mathcal{P}(\mathcal{F})$, the requirement

$$\omega(\mathfrak{f}) > \omega(\mathfrak{f}')/\mathit{effort}(\mathfrak{f}, \mathfrak{f}'),$$

where $\mathit{effort}(\mathfrak{f}, \mathfrak{f}')$ is a function of the computational resources needed to obtain $\mathfrak{f}'$ from $\mathfrak{f}$.

2.1 A worth-based approach to QIF

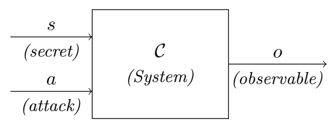

Fig. 1: A system with one high input, one low input, and one low output.

We adopt a probabilistic version of the model of deterministic systems and attacks proposed by Köpf and Basin [16]. Let $\mathcal{S}$ be a finite set of *secrets*, $\mathcal{A}$ be a finite set of adversary-controlled inputs or *attacks*, and $\mathcal{O}$ be a finite set of *observables*. A *(probabilistic computational) system* is a family $C = \{(\mathcal{S}, \mathcal{O}, C_a)\}_{a \in \mathcal{A}}$ of *(information-theoretic) channels* parametrized by the adversary-chosen input $a \in \mathcal{A}$. Each $(\mathcal{S}, \mathcal{O}, C_a)$ is a channel in which $\mathcal{S}$ is the *channel input*, $\mathcal{O}$ is the *channel output*, and C_a is a $|\mathcal{S}| \times |\mathcal{O}|$ matrix of conditional probability distributions called the *channel matrix*. Each entry $C_a(s, o)$ in the matrix represents the probability of the system producing observable o when the secret is s and the adversary-chosen low input is a. Given a probability distribution p_S on $\mathcal{S}$, the behavior of the system under attack a is described by the joint distribution $p_a(s, o) = p_S(s) \cdot C_a(s, o)$, with marginal $p_a(o) = \sum_s p_a(s, o)$, and conditional distribution $p_a(s|o) = p_a(s, o)/p_a(o)$ whenever $p_a(o) > 0$ (and similarly for $p_a(s)$ and $p_a(o|s)$).

As is usual in QIF, we assume that the adversary knows the probability distribution p_S on the set of secrets and the family of channel matrices C describing the system's behavior. Since the adversary controls the low input, he can use it in an attack as follows: by picking $a \in \mathcal{A}$ the channel matrix is set to C_a, thereby manipulating the behavior of the system. The adversary's goal is to infer as much information as possible from the secret, given knowledge about how the system works, the attack fed to the system, and the observations made as the system executes.

Let Ω be the set of all possible worth assignments for the structures of $\mathcal{S}$, $Pr(S)$ be the set of all probability distributions on $\mathcal{S}$, and $\mathcal{C}_{\mathcal{A}}$ be set of channel matrices induced by attacks $a \in \mathcal{A}$. A *measure of information worth* is a function $\nu : \Omega \times Pr(\mathcal{S}) \times \mathcal{C}_{\mathcal{A}} \to \mathbb{R}^+$. The quantity $\nu(\omega, p_S, C_a)$ represents the a posteriori information with respect to S revealed by attack $C_a \in \mathcal{C}_{\mathcal{A}}$, given probability distribution $p_S \in Pr(\mathcal{S})$ on secrets and worth assignment $\omega \in \Omega$. Before any attack is performed, the adversary has some a priori information about the secret due to his knowledge of p_S and ω only, and we represent this information by $\nu(\omega, p_S)$. Because the attack is expected to disclose secret information to the adversary, the leakage from an attack C_a is defined as the difference[4], between the a posteriori and a priori information associated with C_a.

3 Measures of information worth

3.1 Operational interpretation of measures revisited

One of Shannon's greatest insights, which ultimately led to the creation of the field of information theory, can be formulated as: *information is describable in terms of answers to questions*. The more information the adversary has about a random variable, the fewer questions of a certain type he needs to ask in order to infer its value, and the smaller the Shannon entropy of this random variable.

Formally, the *Shannon entropy* of a probability distribution p_S is defined as $SE(p_S) = -\sum_s p_S(s) \log p_S(s)$, and the *conditional Shannon entropy* of p_S given a channel C_a is defined as $SE(p_S, C_a) = \sum_{o \in \mathcal{O}} p_a(o) SE(p_a(\cdot|o))$. A possible operational interpretation of this measure is: The adversary can pose questions *Does* $S \in \mathcal{S}'$*?*, for some $\mathcal{S}' \subseteq \mathcal{S}$, to an oracle, and Shannon entropy quantifies the expected minimum number of guesses needed to infer the entire secret with certainty. The decrease in the Shannon entropy of the secret space caused by a system can be seen as the leakage from the system. This question-and-answer interpretation has an algorithmic equivalent: The set $\mathcal{S}$ is seen as a search space, and by repeatedly asking questions *Does* $S \in \mathcal{S}'$*?*, the adversary performs a binary search on the space of secrets. Shannon entropy corresponds to the average height of the optimal binary search tree.

However, Shannon entropy is not the unique meaningful measure of information. Guessing entropy allows the adversary to pose a different type of question; whereas probability of guessing quantifies a different aspect of the scenario of interest. Yet, the operational interpretation of also these measures can be described in terms of questions and answers as follows.

For simplicity, assume that elements of $\mathcal{S}$ are ordered by decreasing probabilities, i.e., if $1 \leq i < j \leq |\mathcal{S}|$ then $p_S(s_i) \geq p_S(s_j)$. Then the *guessing entropy* of p_S is defined as $NG(p_S) = \sum_{i=1}^{|\mathcal{S}|} i \cdot p_S(s_i)$, and the *conditional guessing entropy* of p_S given a channel C_a is defined as $NG(p_S, C_a) = \sum_{o \in \mathcal{O}} p_a(o) NG(p_a(\cdot|o))$. A operational interpretation of guessing entropy is: The adversary can pose questions *Is* $S = s$*?*, for some $s \in \mathcal{S}$, to an oracle, and the measure quantifies the expected number of guesses needed to learn the entire secret. Algorithmically, guessing entropy is the expected number of steps needed for the adversary to find the secret using linear search on the space of secrets.

[4] Braun et al. [12] make a distinction between this definition of leakage, called *additive leakage*, and *multiplicative leakage*, where the ratio (rather than the difference) of the a posteriori and a priori information is taken. Divisions by zero avoided, the results of this paper apply to both definitions. For simplicity, we stick to the first.

Measure	Type of question	Number of questions comprising attack	Probability of attack successful
Shannon entropy $SE(p_S)$	*Does* $S \subseteq \mathcal{S}'$*?*	?	S is inferred with prob. 1
Guessing entropy $NG(p_S)$	*Is* $S = s$*?*	?	S is inferred with prob. 1
Prob. of guessing $PG_n(p_S)$	*Is* $S = s$*?*	n questions allowed	?
Prob. of guessing under $\subseteq$ $PG^{\subseteq}_n(p_S)$	*Does* $S \subseteq s$*?*	n questions allowed	?

Table 1: Operational interpretation for three traditional information-flow measures, and a new measure. The question mark indicates the value of measure.

Still assuming that the elements of $\mathcal{S}$ are in decreasing order of probabilities, the *probability of guessing* the secret in n tries is defined as $PG_n(p_S) = \sum_{i=1}^{n} p_S(s_i)$. The *conditional probability of guessing* of p_S in n tries given a channel C_a is defined as $PG_n(p_S, C_a) = \sum_{o\in\mathcal{O}} p_a(o)PG_n(p_a(\cdot|o))$. A operational interpretation of probability of guessing in n tries is: The adversary can pose questions *Is* $S = s$*?*, for some $s \in \mathcal{S}$, and the measure quantifies the probability of guessing the entire secret in n tries. Algorithmically, the probability of guessing is the chance of success by an adversary performing a linear search on the space of secrets, after n steps.

The landscape of these traditional measures can be covered by varying the following three dimensions composing their operational interpretation:

d1: the *type of question* the adversary is allowed to pose;
d2: the *number of questions (guesses)* the adversary is allowed to pose;
d3: the *probability of success*, i.e., that of the adversary inferring the secret.

Table 1 summarizes the operational interpretation of Shannon entropy, guessing entropy and probability of guessing in terms of dimensions **d1**, **d2**, and **d3**. The type of question is fixed for each measure, and the two other dimensions have a dual behavior: one is fixed and the other one is quantified. In particular, Shannon entropy and guessing entropy fix the probability of guessing the secret to be 1 and quantify the number of questions necessary to do so; whereas probability of guessing fixes the number of guesses to be n and quantifies the probability of the secret being guessed.

We add a fourth row to Table 1 for a measure whose operational interpretation is: The adversary can pose questions *Does* $S \subseteq \mathcal{S}'$*?*, for some $\mathcal{S}' \subseteq \mathcal{S}$, to an oracle, and the measure quantifies the probability of guessing the entire secret in n tries. Algorithmically, this measure is analogous to the probability of guessing, but allowing the adversary to perform a binary (rather than linear) search on the space of secrets. Formally, we define the *probability of guessing under* $\subseteq$ of an element distributed according to p_S in n tries as $PG^{\subseteq}_n(p_S) = \max_{\mathsf{P}\in\mathtt{LoI}(\mathcal{S}),|\mathsf{P}|\leq 2^n} \sum_{\mathcal{S}'\in\mathsf{P},|\mathcal{S}'|=1} p_S(\cdot|\mathcal{S}')$, and the *conditional probability of guessing under* $\subseteq$ of p_S in n tries given a channel C_a is defined as $PG^{\subseteq}_n(p_S, C_a) = \sum_{o\in\mathcal{O}} p_a(o)PG^{\subseteq}_n(p_a(\cdot|o))$.

Worth as a new dimension The traditional measures in Table 1 presume all secrets to be monolithic and equally sensitive. We relax this restriction by introducing a new dimension to the operational interpretation of measures:

d4: the *worth* the adversary extracts from a guess.

We can enrich the landscape of measures of information with new definitions that exploit the freedom allowed by the extra dimension **d4**. As is done in the traditional case, for each measure we fix the type of question the adversary is allowed to pose and vary the role played by the other three dimensions. Hence we classify the measures into three groups:

- W**-measures** quantify the worth extracted from an attack when the following dimensions are fixed: (i) the type of question the adversary can pose; (ii) the number of questions that can be posed; and (iii) the required probability of success.
- N**-measures** quantify the number of guesses the adversary needs in order to succeed when the following dimensions are fixed: (i) the type of question the adversary can pose; (ii) the required probability of success; and (iii) a minimum worth threshold to extract as measured according to a W-measure ν modeling his preferences.
- P**-measures** quantify the probability of an attack being successful when the following dimensions are fixed: (i) the type of question the adversary can pose; (ii) the number of questions that can be posed; and (iii) a minimum worth threshold to extract as measured according to a W-measure ν modeling his preferences.

According to this classification, Shannon entropy and guessing entropy are N-measures, and probability of guessing is a P-measure (all of them implicitly using a trivial worth assignment). Table 2 organizes the measures of information worth we propose in this paper; because our results are more general, the new table subsumes Table 1 of traditional measures.

W-measures are used to specify the fixed worth threshold necessary to fully define P-measures and N-measures, and hence we will start our discussion with them. Before, though, we set some conventions.

Conventions and definitions Assume that the set $\mathcal{S}$ of secrets follows a probability distribution p_S, and that its fields are in the set $\mathcal{F}$. For any $\mathcal{S}' \subseteq \mathcal{S}$ we denote by $p_S(\cdot|\mathcal{S}')$ the normalization of p_S with respect to $\mathcal{S}'$, i.e., for every $s \in \mathcal{S}$, $p_S(s|\mathcal{S}') = p_S(s)/p_S(\mathcal{S}')$ if $s \in \mathcal{S}'$, and $p_S(s|\mathcal{S}') = 0$ otherwise. The support of a distribution p_S is denoted $supp(p_S)$.

Assume that an appropriate worth assignment ω is provided. For an attack C_a producing observables in a set $\mathcal{O}$, the information conveyed by each $o \in \mathcal{O}$ is the information contained in the probability distribution $p_a(\cdot|o)$ that o induces on secrets. A measure of information worth is *composable* if the value of an attack can be calculated as a function of information conveyed by each observable: $\nu(\omega, p_S, C_a) = \sum_{o \in \mathcal{O}} p_a(o)\nu(\omega, p_S(\cdot|o))$. In *worst-case measures* the

W-measures: quantifying worth	Type of question	Number of questions comprising attack	Probability of attack successful	Worth of payoff to attacker
Worth of certainty $WCER(\omega, p_S)$	*Does* $S \subseteq \mathcal{S}'$*?*	1 guess allowed	success with prob. 1	?
W-vulnerability $WV(\omega, p_S)$	*Does* $S \subseteq \mathcal{S}'$*?*	1 guess allowed	? (product prob. × worth)	
Worth of exp. = $WEXP^{=}_{n,\nu}(\omega, p_S)$	*Is* $S = s$*?*	n guesses allowed	success with prob. 1	? (using W-measure ν)

N-measures: quantifying number of guesses	Type of question	Number of questions comprising attack	Probability of attack successful	Worth of payoff to attacker
W-guessing entropy $WNG_{\mathsf{w},\nu}(\omega, p_S)$	*Is* $S = s$*?*	?	success with prob. 1	extracted worth w using W-measure ν
W-Shannon entropy $WSE_{\mathsf{w},\nu}(\omega, p_S)$	*Does* $S \subseteq \mathcal{S}'$*?*	?	success with prob. 1	extracted worth w using W-measure ν

P-measures: quantifying probability of success	Type of question	Number of questions comprising attack	Probability of attack successful	Worth of payoff to attacker
W-prob. of guessing $WPG^{\subseteq}_{\mathsf{w},n,\nu}(\omega, p_S)$	*Does* $S \subseteq \mathcal{S}'$*?*	n guesses allowed	?	extracted worth w (using W-measure ν)

Table 2: Operational interpretation for measures of information worth. The question mark indicates the value of the measure.

information contained in an attack is defined as the maximum value among all possible observables, that is, $\nu(\omega, p_S, C_a) = \max_{o \in \mathcal{O}} \nu(\omega, p_S(\cdot|o))$. All measures we propose in this paper are composable, but they easily extend to wort-case versions. Finally, define the *worth of a secret* $s \in \mathcal{S}$ to be the worth of learning all of its fields, i.e., $\omega(s) = \omega(\mathcal{F})$.

We will need to refer to a partition on the space of secrets. Formally, $\mathsf{P} = \{\mathcal{S}_1, \ldots, \mathcal{S}_n\}$ is a *partition* on $\mathcal{S}$ iff: (i) $\bigcup_{\mathcal{S}_i \in \mathsf{P}} \mathcal{S}_i = \mathcal{S}$; and (ii) for $1 \leq i \neq j \leq n$, $\mathcal{S}_i \cap \mathcal{S}_j = \emptyset$. Each $\mathcal{S}_i \in \mathsf{P}$ is called a *block* in the partition. We denote the set of all partitions in $\mathcal{S}$ by $\texttt{LoI}(\mathcal{S})$. Following [10], every partition $\mathsf{P}_a = \{\mathcal{S}_{o_1}, \ldots, \mathcal{S}_{o_n}\}$ on $\mathcal{S}$ induced by the attack a can be seen as a random variable with carrier $\{\mathcal{S}_{o_1}, \ldots, \mathcal{S}_{o_n}\}$ and probability distribution $p_S(\mathcal{S}_{o_i}) = \sum_{s \in \mathcal{S}_{o_i}} p_S(s)$.

3.2 W-measures

Worth of certainty. Consider a risk-averse adversary allowed to guess any part of the secret—as opposed to the secret as a whole—but who will do so only when absolutely certain of the success of the guess. To model this scenario, we note that a field is deducible with certainty from p_S if its contents is the same in every secret in the support of the distribution. Formally, the *deducible fields* from

p_S are defined as $ded(p_S) = \mathcal{F} \setminus \{f \in \mathcal{F} \mid \exists s', s'' \in supp(p_S) \ : \ s'[f] \neq s''[f]\}$. For an attack C_a producing observables in a set $\mathcal{O}$, the deducible fields from each $o \in \mathcal{O}$ are the ones that can be inferred from the probability distribution that o induces on secrets, that is, $ded(p_a(\cdot|o))$. The information contained in a probability distribution is defined as its *worth of certainty*, i.e., the worth of its deducible fields. Because worth assignments are monotonic, the maximum information in a probability distribution is the worth of the structure formed by all deducible fields, i.e., $\omega(ded(p_S))$. The information conveyed by an attack C_a is defined as the expectation of the worth of certainty over all observations produced by this attack.

Definition 2 (Worth of certainty). *The* worth of certainty *of p_S is defined as $WCER(\omega, p_S) = \omega(ded(p_S))$. The* worth of certainty *of an attack C_a is a W-measure defined as $WCER(\omega, p_S, C_a) = \sum_{o\in\mathcal{O}} p_a(o)\, WCER(\omega, p_a(\cdot|o))$.*

***W*-vulneratiblity.** Consider an adversary who can guess a less likely structure, as long as this structure is worth enough to yield a higher overall expected gain. Formally we define, for every structure $\mathfrak{f} \in \mathcal{F}$, $p_S(\mathfrak{f})$ to be the probability that f can be deduced by an adversary knowing the distribution p_S: $p_S(\mathfrak{f}) = \max_{x\in\mathcal{S}[\mathfrak{f}]} \sum_{s\in\mathcal{S}, s[\mathfrak{f}]=x} p_S(s)$. A rational adversary maximizes the product of probability and worth, and hence we define W-vulnerability as follows.

Definition 3 (W-vulnerability). *The* W-vulnerability *of p_S is defined as $WV(\omega, p_S) = \max_{\mathfrak{f}\subseteq\mathcal{F}} (p_S(\mathfrak{f})\omega(\mathfrak{f}))$. The* W-vulnerability *of an attack C_a is a W-measure defined as $WV(\omega, p_S, C_a) = \sum_{o\in\mathcal{O}} p_a(o)\, WV(\omega, p_a(\cdot|o))$.*

Worth of expectation under =. Consider an adversary who can explore the space of secrets using brute force, i.e., by guessing the possible values of the secret one by one. Assume that this adversary is allowed $n \geq 0$ tries to guess the secret, and that he aims to extract as much worth as possible according to some W-measure ν modeling his preferences. This leads to the following measure.

Definition 4 (Worth of expectation under =). *Let $n \geq 0$ be the maximum number of tries allowed for the adversary. The* worth of expectation under = *of p_S is $WEXP^{=}_{n,\nu}(\omega, p_S) = \max_{\mathcal{S}'\subseteq\mathcal{S}, |\mathcal{S}'|\leq n} \left(p_S(\mathcal{S}')\omega(\mathcal{F}) + p_S(\bar{\mathcal{S}}')\nu(\omega, p_S(\cdot|\bar{\mathcal{S}}'))\right)$. The* worth of expectation under = *of an attack C_a is a W-measure defined as $WEXP^{=}_{n,\nu}(\omega, p_S, C_a) = \sum_{o\in\mathcal{O}} p_a(o)\, WEXP^{=}_{n,\nu}(\omega, p_a(\cdot|o))$*

3.3 *N*-measures

***W*-guessing entropy.** Guessing entropy quantifies the expected number of questions of the type *Is $S = s$?* needed for the adversary to guess the entire secret. Consider an adversary who can ask the same type of question, but who, instead of having to guess the secret as a whole, can fix a minimum worth $0 \leq \mathsf{w} \leq \omega(\mathcal{F})$ to obtain according to some W-measure ν modeling his preferences. The following measures quantifies the expected number of questions needed to obtain a minimum worth w from the attacks in this a scenario.

Definition 5 **(W-guessing entropy).** *Let $0 \le \mathsf{w} \le \omega(\mathcal{F})$ be a worth threshold quantified according to a W-measure ν. The* W-guessing entropy *of p_S is $WNG_{\mathsf{w},\nu}(\omega, p_S) = \min_{\mathcal{S}' \subseteq \mathcal{S}, \nu(\omega, p_S(\cdot|\mathcal{S}')) \ge \mathsf{w}} \left(p_S(\bar{\mathcal{S}}') NG(p_S(\cdot|\bar{\mathcal{S}}')) + p_S(\mathcal{S}')(|\bar{\mathcal{S}}'| + 1) \right)$, where $\bar{\mathcal{S}}' = \mathcal{S} \backslash \mathcal{S}'$. The* W-guessing entropy *of an attack C_a is a N-measure defined as $WNG_{\mathsf{w},\nu}(\omega, p_S, C_a) = \sum_{o \in \mathcal{O}} p_a(o)\, WNG_{\mathsf{w},\nu}(\omega, p_a(\cdot|o))$.*

***W*-Shannon entropy.** Shannon entropy allows the adversary to pose questions of the type *Does* $S \in \mathcal{S}'$*?*, and it quantifies the expected minimum number of guesses needed to infer the entire secret. Consider an adversary who is allowed the same type of question, but who, instead of having to guess the entire secret, can fix a minimum worth threshold $0 \le \mathsf{w} \le \omega(\mathcal{F})$ to extract according to a W-measure ν. A generalized measure quantifies the expected number of questions necessary to obtain worth w from the attacks.

Definition 6 **(W-Shannon entropy).** *Let $0 \le \mathsf{w} \le \omega(\mathcal{F})$ be a worth threshold quantified according to a W-measure ν. The* W-Shannon entropy *of p_S is defined as $WSE_{\mathsf{w},\nu}(\omega, p_S) = \min_{\mathsf{P} \in \mathtt{LoI}(\mathcal{S}), \forall \mathcal{S}' \in \mathsf{P}\ \nu(\omega, p_S(\cdot|\mathcal{S}')) \ge \mathsf{w}} SE(p_{\mathsf{P}})$, where $\mathtt{LoI}(\mathcal{S})$ is the set of all partitions on the set $\mathcal{S}$. The* W-Shannon entropy *of an attack C_a is a N-measure defined as $WSE_{\mathsf{w},\nu}(\omega, p_S, C_a) = \sum_{o \in \mathcal{O}} p_a(o)\, WSE_{\mathsf{w},\nu}(\omega, p_a(\cdot|o))$.*

3.4 *P*-measures

***W*-Probability of guessing.** The probability of guessing under $\subseteq$ allows an adversary to pose questions *Does* $S \subseteq \mathcal{S}'$*?*, and it quantifies the chances of guessing the entire secret in n tries. Consider an adversary also allowed to pose n questions *Does* $S \subseteq \mathcal{S}'$*?*, and a generalized measure quantifying the chances of him extracting worth $0 \le \mathsf{w} \le \omega(\mathcal{F})$, as measure by some W-measure ν, from an attack. Given n questions, at most 2^n blocks can be inspected, which leads to the following mathematical definition of a measure.

Definition 7 **(W-probability of guessing).** *Let $0 \le \mathsf{w} \le \omega(\mathcal{F})$ be a worth threshold quantified according to a W-measure ν, and $n \ge 0$ be the maximum number of tries allowed for the adversary. The* W-probability of guessing *of p_S is $WPG^{\subseteq}_{\mathsf{w},n,\nu}(\omega, p_S) = \max_{\mathsf{P} \in \mathtt{LoI}(\mathcal{S}), |\mathsf{P}| \le 2^n} \sum_{\mathcal{S}' \in \mathsf{P}, \nu(\omega, p_S(\cdot|\mathcal{S}')) \ge \mathsf{w}} p_S(\mathcal{S}')$. The* W-probability of guessing *of an attack C_a is a P-measure defined as follows: $WPG^{\subseteq}_{\mathsf{w},n,\nu}(\omega, p_S, C_a) = \sum_{o \in \mathcal{O}} p_a(o)\, WPG^{\subseteq}_{\mathsf{w},n,\nu}(\omega, p_a(\cdot|o))$.*

3.5 Mathematical properties of measures of information worth

Measures of information are expected to satisfy certain mathematical properties. It is immediate from the definitions that the proposed measures of information worth yield always non-negative values. It is a subtler matter, however, to show that they also always yield non-negative values for leakage. Theorem 1 below shows that non-negativity of leakage holds for our measures of information worth under certain conditions. Because N-measures and P-measures have a W-mesaure as an input parameter to model the preferences of the adversary, we restrict ourselves to W-measures presenting a consistent behavior with respect to the number of possible values for the secret. Intuitively, whenever some secret value is ruled out from the search space, the adversary's information about the secret, according to the measure, does not decrease. Formally:

Definition 8 (Monotonicity with respect to blocks). *Given a set $\mathcal{S}$ of secrets, a W-measure ν is said to be* monotonic with respect to blocks *if, for every worth assignment ω, every probability distribution p_S on $\mathcal{S}$, and all subsets (i.e., blocks) $\mathcal{S}', \mathcal{S}''$ of $\mathcal{S}$ such that $\mathcal{S}' \subseteq \mathcal{S}''$, it is the case that $\nu(\omega, p_S(\cdot|\mathcal{S}')) \geq \nu(\omega, p_S(\cdot|\mathcal{S}''))$. When ν quantifies uncertainty, the inequality is reversed.*

At first it might seem that monotonicity with respect to blocks holds for every W-measure. But this is not the case. It does hold for worth of certainty, for instance. But it does not hold for W-vulnerability, as shown in Example 1.

Example 1. The vulnerability of a probability distribution p_S is calculated as $V(p_S) = max_s p(s)$. Consider the block $S' = \{s_1, s_2, s_3, s_4\}$ of secrets where $p(s_1) = 1/2$ and $p(s_2) = p(s_3) = p(s_4) = 1/6$. Then $V(S') = 1/2$. Suppose that S' is split into blocks $S'' = \{s_1\}$ and $S''' = \{s_2, s_3, s_4\}$. Hence, even if $S''' \subseteq S'$, we have $V(S''') = 1/3 < V(S')$. Since traditional vulnerability is a particular case of W-vulnerability (Theorem 2), the example is also valid for the former.

In probabilistic systems the adversary's knowledge is not tied to blocks of secrets, but to probability distributions induced by observations. The concept of monotonicity is generalized accordingly.

Definition 9 (Monotonicity with respect to observations). *Given a set $\mathcal{S}$ of secrets, a measure of information worth ν is said to be* monotonic with respect to observations *if for every worth assignment ω, every probability distribution p_S on $\mathcal{S}$, and all observables $o \in \mathcal{O}$, it is the case that $\nu(\omega, p_S(\cdot|o)) \geq \nu(\omega, p_S(\cdot))$. When ν quantifies uncertainty, the inequality is reversed.*

From Example 1 it follows that W-vulnerability is not monotonic with respect to observations. It is easy to see, however, that worth of uncertainty is.

The following theorem establishes that, observed the regularity of the W-mesaures used as parameters, the adversary's information after an attack is never smaller than his a priori information, and hence leakage is non-negative.

Theorem 1. *Let $\mathcal{S}$ be a set of secrets composed by the fields in $\mathcal{F}$ and let C_a be an attack. Let ν be a W-measure that is monotonic with respect to observations, $n \geq 0$ be the number of guesses allowed for the adversary, and $0 \leq \mathsf{w} \leq \omega(\mathcal{F})$. For every distribution p_S on $\mathcal{S}$ and every worth assignment ω:*

$$WCER(\omega, p_S, C_a) \geq WCER(\omega, p_S) \tag{1}$$

$$WV(\omega, p_S, C_a) \geq WV(\omega, p_S) \tag{2}$$

$$WEXP^{=}_{n,\nu}(\omega, p_S, C_a) \geq WEXP^{=}_{n,\nu}(\omega, p_S) \tag{3}$$

$$WNG_{\mathsf{w},\nu}(\omega, p_S, C_a) \leq WNG_{\mathsf{w},\nu}(\omega, p_S) \tag{4}$$

$$WSE_{\mathsf{w},\nu}(\omega, p_S, C_a) \leq WSE_{\mathsf{w},\nu}(\omega, p_S) \tag{5}$$

$$WPG^{\subseteq}_{\mathsf{w},n,\nu}(\omega, p_S, C_a) \geq WPG^{\subseteq}_{\mathsf{w},n,\nu}(\omega, p_S) \tag{6}$$

3.6 Relation with traditional measures

We now substantiate our claim that Shannon entropy, guessing entropy, and probability of guessing (and, in particular, vulnerability) are measures of information that ignore the worth of structures. Define the *binary worth assignment* ω_{bin} that attributes zero worth to any proper structure, i.e., $\omega_{bin}(\mathfrak{f}) = 1$ if $\mathfrak{f} = \mathcal{F}$, $\omega_{bin}(\mathfrak{f}) = 0$ if $\mathfrak{f} \subset \mathcal{F}$. Theorem 2 asserts that the traditional measures implicitly use ω_{bin} as a worth assignment, which means that only the maximal structure is deemed to be conveying relevant information. For instance, the theorem states that Shannon entropy is the particular case of W-Shannon entropy in which the adversary must perform a binary search to the maximum level of granularity, i.e., until the secret is unequivocally identified.

Theorem 2. *Let $\mathcal{S}$ be a set of secrets distributed according to p_S, and C_a be an attack. Then the following hold:*

$$SE(p_S, C_a) = WSE_{1,WCER}(\omega_{bin}, p_S, C_a) \tag{7}$$

$$NG(p_S, C_a) = WNG_{1,WCER}(\omega_{bin}, p_S, C_a) \tag{8}$$

$$PG_n(p_S, C_a) = WEXP^{=}_{n,\nu_{null}}(\omega_{bin}, p_S, C_a) \qquad (\forall n \geq 0) \tag{9}$$

$$V(p_S|C_a) = WV(\omega_{bin}, p_S, C_a) \tag{10}$$

where WCER is the worth of certainty measure; and ν_{null} is the null W-measure such that $\nu_{null}(\omega, p_S) = 0$ for every ω and p_S.

4 Algebraic structure for measures of information worth in deterministic systems

4.1 Deterministic systems and attack sequences

In a deterministic system $\mathcal{C}$, for each pair of high input $s \in \mathcal{S}$ and and low input $a \in \mathcal{A}$, a single output $o \in \mathcal{O}$ is produced with probability 1. Therefore each attack $a \in \mathcal{A}$ induces a partition P_a on the set of secrets, where one block in the partition corresponds to each observable. The block $\mathcal{S}_{a,o} \in \mathsf{P}_a$ contains all secrets that are mapped to o when the low input to the system is a, i.e., $\mathcal{S}_{a,o} = \{s \in \mathcal{S} | \mathcal{C}(s,a) = o\}$. We omit the subscript corresponding to the attack when this is clear from the context, writing only $\mathcal{S}_o$ for $\mathcal{S}_{a,o}$. An attack step can be described mathematically as $\mathcal{C}(s,a) \in \mathsf{P}_a$, which is a two-phase process: (1) the adversary chooses a partition P_a on $\mathcal{S}$, corresponding to attack $a \in \mathcal{A}$; and (2) the system responds with the block $\mathcal{S}_o \in \mathsf{P}_a$ that contains the secret.

The adversary may perform multiple attack steps for the same secret. The adversary combines information acquired from an *attack sequence* $\hat{a} = a_{t_1}, \ldots, a_{t_k}$ of k steps by intersecting the partitions corresponding to each step in the sequence, thereby obtaining a refined partition[5] $\mathsf{P}_{\hat{a}} = \bigcap_{a \in \hat{a}} \mathsf{P}_a$. Hence an attack sequence $\hat{a}$ can be modeled as a single attack where the adversary chooses the partition $\mathsf{P}_{\hat{a}}$ as the low input to the system, and obtains as an observable the block the secret s belongs to. Formally, $\mathcal{C}(s, \hat{a}) \in \mathsf{P}_{\hat{a}}$.

[5] The intersection of partitions is defined as $\mathsf{P} \cap \mathsf{P}' = \bigcup_{\mathcal{S}_o \in \mathsf{P}, \mathcal{S}_{o'} \in \mathsf{P}'} \mathcal{S}_o \cap \mathcal{S}_{o'}$.

4.2 The Lattice of Information and the leakage from attack sequences

The set of all partitions on a finite set $\mathcal{S}$ forms a *complete lattice* called *Lattice of Information* (`LoI`) [14]. The order on the lattice elements is the *refinement order* $\sqsubseteq$ on partitions:

$$\mathsf{P} \sqsubseteq \mathsf{P}' \quad \Leftrightarrow \quad \forall \mathcal{S}_j \in \mathsf{P}' \;\; \exists \mathcal{S}_i \in \mathsf{P} \text{ such that } \mathcal{S}_j \subseteq \mathcal{S}_i.$$

The relation $\sqsubseteq$ is a partial order on the set of all partitions on $\mathcal{S}$. Intuitively, each block in a partition groups indistinguishable elements. The finer the partition, the more elements it can distinguish, and the more information it should carry about $\mathcal{S}$. The *join* $\sqcup$ of two elements in the `LoI` is the intersection of partitions, and their *meet* $\sqcap$ is the transitive closure union of partitions. Given two partitions P and P', both $\mathsf{P} \sqcup \mathsf{P}'$ and $\mathsf{P} \sqcap \mathsf{P}'$ are partitions as well.

In our model, we fix the deterministic system and let the elements in the `LoI` model possible executions. By controlling the low input to the system, the adversary chooses among executions, so the `LoI` serves as an algebraic representation of the partial order on the attack sequences the adversary can perform. Each attack sequence $\hat{a}$ corresponds to one element $\mathsf{P}_{\hat{a}}$—i.e., the partition it induces—in the `LoI` for $\mathcal{S}$.

The execution of an attack sequence can be seen as a path in the `LoI`. By performing an attack step the adversary may obtain a finer partition on the space of secrets, therefore moving up in the lattice to a state with more information. The leakage of information from an attack sequence is, thus, the difference in the measures of information worth between the initial and final partition in the path. Formally, given a distribution p_S on $\mathcal{S}$, if P and P' are two partitions in the `LoI` for $\mathcal{S}$ such that $\mathsf{P} \sqsubseteq \mathsf{P}'$, then the *leakage* from P' with respect to P under the measure of information worth ν is defined as $\mathcal{L}_\nu(\omega, p_S, \mathsf{P} \to \mathsf{P}') = \nu(\omega, p_S, \mathsf{P}') - \nu(\omega, p_S, \mathsf{P})$, where the right-hand side of the equation is negated in case ν is a measure of uncertainty. This definition of leakage encompasses the traditional definitions for Shannon entropy, guessing entropy, and probability of guessing.

4.3 Consistency with respect to the `LoI`

The Lattice of Information has been used as an underlying algebraic structure for deterministic systems, and it provides an elegant way to reason about leakage under composition of attacks. Yasuoka and Terauchi [17] showed that the orderings based on probability of guessing, guessing entropy, and Shannon entropy are all equivalent, and Malacaria [10] showed that they coincide with the refinement order in the `LoI`. These results establish that the traditional measures behave well with respect to the `LoI`: the finer a partition is, the more information (or the less uncertainty) the measures attribute to it.

All measures of information worth proposed in Section 3 behave in a similar way, that is, they are *consistent with respect to the `LoI`*. This is formally established in the following theorem.

Theorem 3. *Let $\mathcal{S}$ be a set of secrets composed by the fields in $\mathcal{F}$. For all* P *and* P' *in the* `LoI` *for* $\mathcal{S}$*, the following are equivalent:*

$$\mathsf{P} \sqsubseteq \mathsf{P}' \tag{11}$$

$$\forall \omega\ \forall p_S \quad WCER(\omega, p_S, \mathsf{P}) \leq WCER(\omega, p_S, \mathsf{P}') \tag{12}$$

$$\forall \omega\ \forall p_S\ WV(\omega, p_S, \mathsf{P}) \leq WV(\omega, p_S, \mathsf{P}') \tag{13}$$

$$\forall n\ \forall \nu\ \forall \omega\ \forall p_S \quad WEXP^{=}_{n,\nu}(\omega, p_S, \mathsf{P}) \leq WEXP^{=}_{n,\nu}(\omega, p_S, \mathsf{P}') \tag{14}$$

$$\forall \mathsf{w}\ \forall \nu\ \forall \omega\ \forall p_S \quad WNG_{\mathsf{w},\nu}(\omega, p_S, \mathsf{P}) \geq WNG_{\mathsf{w},\nu}(\omega, p_S, \mathsf{P}') \tag{15}$$

$$\forall \mathsf{w}\ \forall \nu\ \forall \omega\ \forall p_S \quad WSE_{\mathsf{w},\nu}(\omega, p_S, \mathsf{P}) \geq WSE_{\mathsf{w},\nu}(\omega, p_S, \mathsf{P}') \tag{16}$$

$$\forall \mathsf{w}\ \forall n\ \forall \nu\ \forall \omega\ \forall p_S\ WPG^{\subseteq}_{\mathsf{w},n,\nu}(\omega, p_S, \mathsf{P}) \leq WPG^{\subseteq}_{\mathsf{w},n,\nu}(\omega, p_S, \mathsf{P}') \tag{17}$$

where $n \geq 0$; $0 \leq \mathsf{w} \leq \omega(\mathfrak{f})$; and ν ranges over all composable W-measures that are consistent with respect to the `LoI` *plus the worth of certainty measure WCER. In (15) and (16) ν is restricted to be monotonic with respect to blocks.*

5 A design technique for worth assignments

We now outline a general technique to capture into worth assignments relevant aspects of the scenario of interest.

The domain of worth assignments is the power set $\mathcal{P}(\mathcal{F})$ of the set $\mathcal{F}$ of fields. By endowing $\mathcal{P}(\mathcal{F})$ with the set-inclusion ordering, we obtain a (complete) *lattice of structures* $\mathtt{L}_{\mathcal{F}}$. For every structure $\mathfrak{f} \in \mathcal{P}(\mathcal{F})$ we can identify a partition $\mathsf{P}_{\mathfrak{f}}$ belonging to the `LoI` that discriminates exactly the structure $\mathfrak{f}$. Formally, $\mathsf{P}_{\mathfrak{f}} = \{\mathcal{S}_{s[\mathfrak{f}]=x} \mid x \in \mathcal{S}[\mathfrak{f}]\}$ where to every $x \in \mathcal{S}[\mathfrak{f}]$ corresponds the block $\mathcal{S}_{s[\mathfrak{f}]=x} = \{s \in \mathcal{S} \mid s[\mathfrak{f}] = x\}$. Proposition 1 shows that the set-inclusion ordering on structures coincides with the refinement relation on the corresponding partitions, thereby establishing that the space of structures is a sub-lattice of the `LoI`.

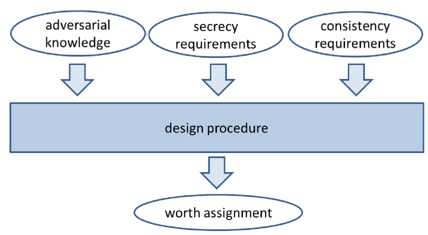

Fig. 2: The inputs and output of our design technique for worth assignments.

Proposition 1. *For every $\mathfrak{f}, \mathfrak{f}' \in \mathcal{P}(\mathcal{F})$, $\mathfrak{f} \subseteq \mathfrak{f}'$ iff $\mathsf{P}_{\mathfrak{f}} \sqsubseteq \mathsf{P}_{\mathfrak{f}'}$.*

Hence, space of structures $\mathtt{L}_{\mathcal{F}}$ is isomorphic to the complete lattice formed by all partitions $\mathsf{P}_{\mathfrak{f}}$ for $\mathfrak{f} \subseteq \mathcal{F}$, ordered by the refinement relation $\sqsubseteq$.

Figure 2 depicts our design technique, which constructs a worth assignment having as input the following three parameters describing a scenario of interest.

a) **Side knowledge** is any piece of information the adversary has about the secret space coming from sources external to the system (e.g., newspapers, common-sense, other systems). As usual in QIF and privacy, side knowledge can be modeled as a probability distribution on the space of secrets [18–20].

b) **Sensitivity requirements** reflect the protector's (i.e., the party interested in hiding the secret) interests, specifying which structures are *intrinsically sensitive* and which are only *contingently sensitive*, that is, sensitive only to the extent they possibly reveal information about other intrinsically sensitive structures. (As we have discussed, a patient's lung cancer status may be considered intrinsically sensitive, whereas his smoking habits are considered sensitive only to the extent they reveal information about the patient's cancer status.) Sensitivity requirements are represented as a partial function from the space of structures to non-negative reals that associates every intrinsically sensitive structures with an appropriate, a priori, worth.
c) **Consistency requirements** are mathematical properties that worth assignments must satisfy in a scenario of interest. Non-negativity and monotonicity are *syntactic* consistency requirements, in that they depend only on the representation of secrets, not on their meaning. Even if arguably universal—one can hardly find a scenario where they should not hold—syntactic requirements alone are often not sufficient to guarantee the consistency of worth assignments. In general some semantic requirements need also to be considered. The adjustments for information theoretical predictors and computational cost from Section 2 are examples of such semantic requirements. Other examples are:
   - *Inclusion-exclusion consistency:* analogously set theory principle, the worth of the composition of two structures is equal to the sum of their individual worths, minus the worth they share: $\omega(\mathfrak{f} \sqcup \mathfrak{f}') = \omega(\mathfrak{f}) + \omega(\mathfrak{f}') - \omega(\mathfrak{f} \sqcap \mathfrak{f}')$.
   - *Independency:* statistically independent structures add their worth: if $\mathsf{P}_{\mathfrak{f}'}$ and $\mathsf{P}_{\mathfrak{f}'}$ are independent then $\omega(\mathfrak{f} \sqcup \mathfrak{f}') = \omega(\mathfrak{f}) + \omega(\mathfrak{f}')$.

Once the inputs are provided, the design technique proceeds as follows:

1. Construct the complete lattice $\mathtt{L}_{\mathcal{F}}$ of structures.
2. Use the sensitivity requirements to annotate each element $\mathsf{P}_{\mathfrak{f}}$ in $\mathtt{L}_{\mathcal{F}}$, where $\mathfrak{f} \in \mathcal{P}(\mathcal{F})$ is a intrinsically sensitive structure, with the appropriate a priori worth in accordance to the protector's interests.
3. Using the adversary's side knowledge, derive a probability distribution p_S. Recalling that partitions in the `LoI` can be seen as random variables, use p_S to derive the probability distribution in the elements of $\mathtt{L}_{\mathcal{F}}$.
4. Take some well established measure of information ν (e.g., guessing entropy), and for every structure $\mathfrak{f}' \in \mathcal{P}(\mathcal{F})$ update its worth according to $\omega(\mathfrak{f}') = \max_{\mathfrak{f} \in \mathcal{P}(\mathcal{F})} \nu(\mathsf{P}_{\mathfrak{f}'} | \mathsf{P}_{\mathfrak{f}})$. Repeat until all structures respect the adequacy requirements.

This design technique captures the adversary's side knowledge into the worth assignment, and the worth of structures will inherit the operational interpretation of the measure ν chosen in step 4. However, because the procedure depends on the probability distribution on the elements of $\mathtt{L}_{\mathcal{F}}$, some semantic requirements can only be approximated. An example is the inclusion-exclusion principle: if it were to be preserved for all probability distributions p_S, it would be a valuation on the lattice, which is known not to exist [21].

6 Related work

6.1 Relation with g-leakage

We start by reviewing g-leakage [13]. Given a set $\mathcal{S}$ of possible secrets and a finite, nonempty set $\mathcal{Z}$ of allowable guesses, a *gain function* is a function $g : \mathcal{Z} \times \mathcal{S} \rightarrow [0,1]$. Given a gain function g and a probability distribution p_S, the *prior g-vulnerability* is $V_g(p_S) = \max_{z \in \mathcal{Z}} \sum_{s \in \mathcal{S}} p_S(s) g(z,s)$, and given also a channel C_a from secrets in $\mathcal{S}$ to observables in $\mathcal{O}$, the *posterior g-vulnerability* is defined as $V_g(p_S, C_a) = \sum_{o \in \mathcal{O}} p(o) V_g(p_a(\cdot|o))$. The g-vulnerability is converted into g-entropy by taking its logarithm: $H_g(p_S) = -\log V_g(p_S)$ and $H_g(p_S, C_a) = -\log V_g(p_S, C_a)$. Finally, g-leakage is defined as the difference between prior and posterior g-entropies: $\mathcal{L}_g(p_S, C_a) = H_g(p_S) - H_g(p_S, C_a)$.

Comparing our work with g-leakage, we can emphasize two main points:

(i) g-leakage as defined in [13] cannot capture scenarios where the worth of a structure depends on the probability of that structure. Hence worth of certainty and W-Shannon entropy cannot be modeled using g-leakage.

Proposition 2. *Given a set of secrets $\mathcal{S}$ and a set of guesses $\mathcal{Z}$, there is no gain function $g : \mathcal{Z} \times \mathcal{S} \rightarrow \mathbb{R}^+$ such that, for all priors p_S on $\mathcal{S}$, and all partitions P on the `LoI` for $\mathcal{S}$, it is the case that: (i) $V_g(p_S) = WCER(\omega, p_S)$; or (ii) $V_g(p_S) = SE(p_S)$; or (iii) $H_g(p_S) = SE(p_S)$.*

(ii) g-leakage and measures of information worth coincide in some scenarios, and when it happens, our approach can be used to give practical operational interpretations to gain functions—in fact, a common criticism of the g-leakage framework concerns the challenge of identifying adequate functions for a scenario of interest. Take guessing entropy as an example. Make an allowable guess z be a permutation $\Pi(\mathcal{S}')$ of the secret elements of a subset $\mathcal{S}' \subseteq \mathcal{S}$ of secrets. Let an index function $i_{\Pi(\mathcal{S}')} : \mathcal{S} \rightarrow [0, \ldots, |\mathcal{S}'|]$ return the position of s within the permutation $\Pi(\mathcal{S}')$ if $s' \in \mathcal{S}'$, and be undefined otherwise. A guess $\Pi(\mathcal{S}')$ means that the adversary believes that the secret belongs to the set $\mathcal{S}'$, and, moreover, that in a brute-force attack he would guess secrets in the same order they appear in the permutation. Then, for a worth assignment ω of interest, define a gain function $g_\omega(\Pi(\mathcal{S}'), s) = -i_{\Pi(\mathcal{S}')}(s)$ if $s \in \mathcal{S}'$, and $g_\omega(\Pi(\mathcal{S}'), s) = -(|\bar{\mathcal{S}}'| + 1)$ otherwise. It can be shown that the W-guessing entropy captures the g-vulnerability of an adversary guided by the gain function g_ω, i.e., that $WNG_{\mathsf{w},\nu}(\omega, p_S) = V_{g_\omega}(p_S)$. However, g_ω ranges over negative values, which is not allowed by the original g-vulnerability framework.[6] Fortunately we do not run into the same type of problem when using W-vulnerability, worth of expectation under $=$, and W-probability of guessing to provide operational interpretations for g-functions.[7]

[6] If we try to capture W-guessing entropy using g-entropy instead of g-vulnerability, the situation becomes even worth: no gain function exists, even with negative values.

[7] The interested reader can find the corresponding derivations in the accompanying technical report [22].

6.2 Other related work

Köpf and Basin [16] proposed the model for deterministic systems we extended in this paper. Their goal, however, was to derive bounds automatically for attacks, rather than finding an algebraic foundation for the measures they use.

Shannon [23] points out the independence of the information contents with respect to its representation, and gives the first steps in trying to understand how Shannon entropy would behave in a lattice of partitions.

The Lattice of Information is introduced by Landauer and Redmond [14]. Yasuoka and Terauchi [17] show the equivalence of the ordering on traditional measures, and Malacaria [10] uses the `LoI` as an algegraic foundation to unify all these orderings. Whereas their work focuses on the comparison of already existing measures, ours proposes new measures taking into account the worth of secrets. Backes, Köpf and Rybalchenko [24], and Heusser and Malacaria [25] use model checkers and sat-solvers to determine the partitions induced by deterministic programs.

Adão et al. [26] relax the assumption of perfect cryptography by allowing the adversary to infer a key at some (possibly computational) cost, and introduce a quantitative extension of the usual Dolev-Yao intruder model to analyze implementations of security protocols. Their work focuses on cryptography, whereas ours is applied to QIF.

Askarov et al. [27] show that, contrary to prior belief, termination-insensitive noninterference can leak an unbounded amount of information, but the problem can me mitigated by making the secret sufficiently random and large. Demange and Sands [28] point out that not always secrets can be chosen to fulfill such requirements, and they develop a framework in which "small" secrets are handled more carefully than "big" ones. They focus on preventing leakage, whereas we aim at providing rigorous information-theoretic measures for quantifying leakage.

7 Conclusion and future work

This paper proposed a framework to incorporate the worth of structures into information-flow measures. We introduced worth assignments to associate structures to a numerical value—possibly representing their sensitivity—and we used these worth assignments to enrich the landscape of measures of information. We generalized Shannon entropy, guessing entropy and probability of guessing, and we proved that the generalizations are consistent with respect to the Lattice of Information for deterministic systems. We also outlined a design technique for worth assignments that captures important aspects of a scenario of interest.

We are currently refining the design technique for worth assignments to make it fully automated. We are also investigating scenarios where every attack incurs in some *resource expenditure*, representing the effort demanded by each attack. The resulting theory would enable the study of the economics of attacks and the trade-off between the information yielded by an attack versus its cost.

Acknowledgements. The authors would like to thank Santosh S. Venkatesh for helpful discussions. Mário S. Alvim and Andre Scedrov are supported in part by the AFOSR MURI "Science of Cyber Security: Modeling, Composition, and Measurement" as AFOSR grant FA9550-11-1-0137. Additional support for Scedrov comes from NSF grant CNS-0830949 and from ONR grant N00014-11-1-0555. Fred Schneider is supported in part by AFOSR grant F9550-06-0019, by the AFOSR MURI "Science of Cyber Security: Modeling, Composition, and Measurement" as AFOSR grant FA9550-11-1-0137, by NSF grants 0430161, 0964409, and CCF-0424422 (TRUST), by ONR grants N00014-01-1-0968 and N00014-09-1-0652, and by grants from Microsoft.

References

1. Cachin, C.: Entropy Measures and Unconditional Security in Cryptography. PhD thesis, ETH Zürich (1997) Reprint as vol. 1 of *ETH Series in Information Security and Cryptography*, ISBN 3-89649-185-7, Hartung-Gorre Verlag, Konstanz, 1997.
2. Clark, D., Hunt, S., Malacaria, P.: Quantitative information flow, relations and polymorphic types. J. of Logic and Computation **18**(2) (2005) 181–199
3. Malacaria, P.: Assessing security threats of looping constructs. In Hofmann, M., Felleisen, M., eds.: Proceedings of the 34th ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages, POPL 2007, Nice, France, January 17-19, 2007, ACM (2007) 225–235
4. Malacaria, P., Chen, H.: Lagrange multipliers and maximum information leakage in different observational models. In Úlfar Erlingsson and Marco Pistoia, ed.: Proceedings of the 2008 Workshop on Programming Languages and Analysis for Security (PLAS 2008), Tucson, AZ, USA, ACM (June 2008) 135–146
5. Moskowitz, I.S., Newman, R.E., Syverson, P.F.: Quasi-anonymous channels. In: Proc. of CNIS, IASTED (2003) 126–131
6. Moskowitz, I.S., Newman, R.E., Crepeau, D.P., Miller, A.R.: Covert channels and anonymizing networks. In Jajodia, S., Samarati, P., Syverson, P.F., eds.: Workshop on Privacy in the Electronic Society 2003, ACM (2003) 79–88
7. Chatzikokolakis, K., Palamidessi, C., Panangaden, P.: Anonymity protocols as noisy channels. Inf. and Comp. **206**(2–4) (2008) 378–401
8. Alvim, M.S., Andrés, M.E., Palamidessi, C.: Information Flow in Interactive Systems. In Gastin, P., Laroussinie, F., eds.: Proceedings of the 21th International Conference on Concurrency Theory (CONCUR 2010), Paris, France, August 31-September 3. Volume 6269 of Lecture Notes in Computer Science., Springer (2010) 102–116
9. Massey: Guessing and entropy. In: Proceedings of the IEEE International Symposium on Information Theory, IEEE (1994) 204
10. Malacaria, P.: Algebraic foundations for information theoretical, probabilistic and guessability measures of information flow. CoRR **abs/1101.3453** (2011)
11. Smith, G.: On the foundations of quantitative information flow. In: FOSSACS. (2009) 288–302
12. Braun, C., Chatzikokolakis, K., Palamidessi, C.: Quantitative notions of leakage for one-try attacks. In: Proceedings of the 25th Conf. on Mathematical Foundations of Programming Semantics. Volume 249 of Electronic Notes in Theoretical Computer Science., Elsevier B.V. (2009) 75–91

13. Alvim, M.S., Chatzikokolakis, K., Palamidessi, C., Smith, G.: Measuring information leakage using generalized gain functions. Volume 0., Los Alamitos, CA, USA, IEEE Computer Society (2012) 265–279
14. Landauer, J., Redmond, T.: A lattice of information. In: Proc. Computer Security Foundations Workshop VI. (June 1993) 65 –70
15. Sweeney, L.: Uniqueness of simple demographics in the u.s. population (2000)
16. Köpf, B., Basin, D.: Automatically deriving information-theoretic bounds for adaptive side-channel attacks. J. Comput. Secur. **19**(1) (January 2011) 1–31
17. Yasuoka, H., Terauchi, T.: Quantitative information flow — verification hardness and possibilities. In: Proc. 23nd IEEE Computer Security Foundations Symposium (CSF '10). (2010) 15–27
18. Dwork, C.: Differential privacy. In: Automata, Languages and Programming, 33rd Int. Colloquium, ICALP 2006, Venice, Italy, July 10-14, 2006, Proc., Part II. Volume 4052 of LNCS., Springer (2006) 1–12
19. Ghosh, A., Roughgarden, T., Sundararajan, M.: Universally utility-maximizing privacy mechanisms. In: Proceedings of the 41st annual ACM symposium on Theory of computing. STOC '09, New York, NY, USA, ACM (2009) 351–360
20. Alvim, M.S., Andrés, M.E., Chatzikokolakis, K., Palamidessi, C.: On the relation between differential privacy and quantitative information flow. In: Proceedings of the 38th International Colloquium on Automata, Languages and Programming (ICALP 2011), Zürich, Switzerland, July 4th-8th 2011. (2011) to appear.
21. Nakamura, Y.: Entropy and semivaluations on semilattices. Kodai Math. Sem. (1970)
22. Alvim, M.S., Scedrov, A., Schneider, F.B.: When not all bits are equal: worth-based information flow. Technical report (2013) http://hans.math.upenn.edu/~msalvim/papers/nabae-TechRep.pdf.
23. Shannon, C.: The lattice theory of information. Information Theory, IRE Professional Group on **1**(1) (feb. 1953) 105 –107
24. Backes, M., Köpf, B., Rybalchenko, A.: Automatic discovery and quantification of information leaks. In: IEEE Symposium on Security and Privacy. (2009) 141–153
25. Heusser, J., Malacaria, P.: Quantifying information leaks in software. In: Proceedings of the 26th Annual Computer Security Applications Conference. ACSAC '10, New York, NY, USA, ACM (2010) 261–269
26. Adão, P., Mateus, P., Reis, T., Viganò, L.: Towards a quantitative analysis of security protocols. QAPL 2006, ENTCS **164**(3) (2006) 3–25
27. Askarov, A., Hunt, S., Sabelfeld, A., Sands, D.: Termination-insensitive noninterference leaks more than just a bit. In: Proceedings of the 13th European Symposium on Research in Computer Security: Computer Security. ESORICS '08, Berlin, Heidelberg, Springer-Verlag (2008) 333–348
28. Demange, D., Sands, D.: All secrets great and small. In: Proceedings of the 18th European Symposium on Programming Languages and Systems: Held as Part of the Joint European Conferences on Theory and Practice of Software, ETAPS 2009. ESOP '09, Berlin, Heidelberg, Springer-Verlag (2009) 207–221

Appendix A: Proofs

A.I Definitions and conventions

For some of our results we need a particular type of worth assignment called $\mathcal{F}$-*roofed*, in which every proper sub-structure has a strictly smaller worth than the entire secret. That means that there is no redundancy in the collection of fields composing the secret.

Definition 10 ($\mathcal{F}$-roofed worth assignment). *Given a set of fields $\mathcal{F}$, a worth assignment $\omega : \mathcal{P}(\mathcal{F}) \to \mathbb{R}$ is said to be $\mathcal{F}$-*roofed *if for every structure $\mathfrak{f} \subset \mathcal{F}$, $\omega(\mathfrak{f}) < \omega(\mathcal{F})$.*

The following theorem states the results of Yasuoka and Terauchi [17] and of Malacaria [10] using terminology in our paper. This theorem shows that showed the orders on probability of guessing, guessing entropy, and Shannon entropy, and the order on the `LoI` all coincide.

Theorem 4 ([10, 17]). *Let $\mathcal{S}$ be a set with probability distribution p_S. For any two partitions P and P' on $\mathcal{S}$, the following are equivalent:*

$$\mathsf{P} \sqsubseteq \mathsf{P}' \tag{18}$$

$$\forall p_S \quad SE(p_S|\mathsf{P}) \geq SE(p_S|\mathsf{P}') \tag{19}$$

$$\forall n \geq 1\ \forall p_S \quad PG_n(p_S|\mathsf{P}) \leq PG_n(p_S|\mathsf{P}') \tag{20}$$

$$\forall p_S \quad NG(p_S|\mathsf{P}) \geq NG(p_S|\mathsf{P}') \tag{21}$$

A.II Main results

Theorem 1. *Let $\mathcal{S}$ be a set of secrets composed by the fields in $\mathcal{F}$ and let C_a be an attack. Let ν be a W-measure that is monotonic with respect to observations, $n \geq 0$ be the number of guesses allowed for the adversary, and $0 \leq \mathsf{w} \leq \omega(\mathcal{F})$. For every distribution p_S on $\mathcal{S}$ and every worth assignment ω:*

$$WCER(\omega, p_S, C_a) \geq WCER(\omega, p_S) \tag{1}$$

$$WV(\omega, p_S, C_a) \geq WV(\omega, p_S) \tag{2}$$

$$WEXP^{=}_{n,\nu}(\omega, p_S, C_a) \geq WEXP^{=}_{n,\nu}(\omega, p_S) \tag{3}$$

$$WNG_{\mathsf{w},\nu}(\omega, p_S, C_a) \leq WNG_{\mathsf{w},\nu}(\omega, p_S) \tag{4}$$

$$WSE_{\mathsf{w},\nu}(\omega, p_S, C_a) \leq WSE_{\mathsf{w},\nu}(\omega, p_S) \tag{5}$$

$$WPG^{\subseteq}_{\mathsf{w},n,\nu}(\omega, p_S, C_a) \geq WPG^{\subseteq}_{\mathsf{w},n,\nu}(\omega, p_S) \tag{6}$$

Proof. It follows from Propositions 5, 7, 10, 13, 16, and 19.

Theorem 2. *Let $\mathcal{S}$ be a set of secrets distributed according to p_S, and C_a be an attack. Then the following hold:*

$$SE(p_S, C_a) = WSE_{1,WCER}(\omega_{bin}, p_S, C_a) \tag{7}$$

$$NG(p_S, C_a) = WNG_{1,WCER}(\omega_{bin}, p_S, C_a) \tag{8}$$

$$PG_n(p_S, C_a) = WEXP^{=}_{n,\nu_{null}}(\omega_{bin}, p_S, C_a) \qquad (\forall n \geq 0) \tag{9}$$

$$V(p_S|C_a) = WV(\omega_{bin}, p_S, C_a) \tag{10}$$

where WCER is the worth of certainty measure; and ν_{null} is the null W-measure such that $\nu_{null}(\omega, p_S) = 0$ for every ω and p_S.

Proof. It follows from Propositions 9, 12, 15, 18, and 21.

Theorem 3. *Let $\mathcal{S}$ be a set of secrets composed by the fields in $\mathcal{F}$. For all P and P' in the* `LoI` *for $\mathcal{S}$, the following are equivalent:*

$$\mathsf{P} \sqsubseteq \mathsf{P}' \tag{11}$$

$$\forall\omega\ \forall p_S \quad WCER(\omega, p_S, \mathsf{P}) \leq WCER(\omega, p_S, \mathsf{P}') \tag{12}$$

$$\forall\omega\ \forall p_S\ WV(\omega, p_S, \mathsf{P}) \leq WV(\omega, p_S, \mathsf{P}') \tag{13}$$

$$\forall n\ \forall\nu\ \forall\omega\ \forall p_S \quad WEXP^{=}_{n,\nu}(\omega, p_S, \mathsf{P}) \leq WEXP^{=}_{n,\nu}(\omega, p_S, \mathsf{P}') \tag{14}$$

$$\forall \mathsf{w}\ \forall\nu\ \forall\omega\ \forall p_S \quad WNG_{\mathsf{w},\nu}(\omega, p_S, \mathsf{P}) \geq WNG_{\mathsf{w},\nu}(\omega, p_S, \mathsf{P}') \tag{15}$$

$$\forall \mathsf{w}\ \forall\nu\ \forall\omega\ \forall p_S \quad WSE_{\mathsf{w},\nu}(\omega, p_S, \mathsf{P}) \geq WSE_{\mathsf{w},\nu}(\omega, p_S, \mathsf{P}') \tag{16}$$

$$\forall \mathsf{w}\ \forall n\ \forall\nu\ \forall\omega\ \forall p_S\ WPG^{\subseteq}_{\mathsf{w},n,\nu}(\omega, p_S, \mathsf{P}) \leq WPG^{\subseteq}_{\mathsf{w},n,\nu}(\omega, p_S, \mathsf{P}') \tag{17}$$

where $n \geq 0$; $0 \leq \mathsf{w} \leq \omega(\mathfrak{f})$; and ν ranges over all composable W-measures that are consistent with respect to the `LoI` *plus the worth of certainty measure WCER. In (15) and (16) ν is restricted to be monotonic with respect to blocks.*

Proof. It follows from Propositions 6, 8, 11, 14, 17, and 20.

A.III Results regarding probability of guessing under $\subseteq$

Proposition 3. *Let $\mathcal{S}$ be a set of secrets and C_a be an attack. For every distribution p_S on $\mathcal{S}$ and every $n \geq 0$ the following holds.*

$$PG^{\subseteq}_{n}(p_S, C_a) \geq PG^{\subseteq}_{n}(p_S)$$

Proof. By definition:

$$\begin{aligned}
PG^{\subseteq}_{n}(p_S, C_a) &= \sum_{o \in \mathcal{O}} p_a(o) \max_{\substack{\mathsf{P} \in \mathtt{LoI}(\mathcal{S}) \\ |\mathsf{P}| \leq 2^n}} \sum_{\substack{\mathcal{S}' \in \mathsf{P} \\ |\mathcal{S}'|=1}} p_S(\mathcal{S}'|o) \\
&\geq \max_{\substack{\mathsf{P} \in \mathtt{LoI}(\mathcal{S}) \\ |\mathsf{P}| \leq 2^n}} \sum_{o \in \mathcal{O}} p_a(o) \sum_{\substack{\mathcal{S}' \in \mathsf{P} \\ |\mathcal{S}'|=1}} p_S(\mathcal{S}'|o) \\
&= \max_{\substack{\mathsf{P} \in \mathtt{LoI}(\mathcal{S}) \\ |\mathsf{P}| \leq 2^n}} \sum_{\substack{\mathcal{S}' \in \mathsf{P} \\ |\mathcal{S}'|=1}} p_S(\mathcal{S}') \\
&= PG^{\subseteq}_{n}(p_S)
\end{aligned}$$

□

Proposition 4. *Let $\mathcal{S}$ be a set of secrets composed by the fields in $\mathcal{F}$. Then for every two partitions* P *and* P' *in the* `LoI` *of* $\mathcal{S}$ *the following holds:*

$$\mathsf{P} \sqsubseteq \mathsf{P}' \quad \Leftrightarrow \quad \forall n\ \forall p_S PG_n^{\subseteq}(p_S, \mathsf{P}) \leq PG_n^{\subseteq}(p_S, \mathsf{P}')$$

Proof. 1. ($\Rightarrow$) By definition, $PG_n^{\subseteq}(p_S, \mathsf{P})$ is given by:

$$\sum_{\mathcal{S}_o \in \mathsf{P}} p_S(\mathcal{S}_o) \max_{\substack{\mathsf{P}^* \in \mathtt{LoI}(\mathcal{S}) \\ |\mathsf{P}^*| \leq 2^n}} \sum_{\substack{\mathcal{S}^* \in \mathsf{P}^* \\ |\mathcal{S}^*|=1}} p_S(\mathcal{S}^* | \mathcal{S}_o) \tag{22}$$

Since each block of P is split into blocks of P', (22) can be rewritten as:

$$\sum_{\mathcal{S}_o \in \mathsf{P}} \sum_{\substack{\mathcal{S}_{o'} \in \mathsf{P}' \\ \mathcal{S}_{o'} \mathcal{S}_o}} p_S(\mathcal{S}_{o'}) \max_{\substack{\mathsf{P}^* \in \mathtt{LoI}(\mathcal{S}) \\ |\mathsf{P}^*| \leq 2^n}} \sum_{\substack{\mathcal{S}^* \in \mathsf{P}^* \\ |\mathcal{S}^*|=1}} p_S(\mathcal{S}^* | \mathcal{S}_o) \tag{23}$$

Because $\mathcal{S}_{o'} \subseteq \mathcal{S}_o$, $p_S(\mathcal{S}^* | \mathcal{S}_{o'}) \geq p_S(\mathcal{S}^* | \mathcal{S}_o)$, and (23) must be greater or equal than:

$$\sum_{\mathcal{S}_o \in \mathsf{P}} \sum_{\substack{\mathcal{S}_{o'} \in \mathsf{P}' \\ \mathcal{S}_{o'} \mathcal{S}_o}} p_S(\mathcal{S}_{o'}) \max_{\substack{\mathsf{P}^* \in \mathtt{LoI}(\mathcal{S}) \\ |\mathsf{P}^*| \leq 2^n}} \sum_{\substack{\mathcal{S}^* \in \mathsf{P}^* \\ |\mathcal{S}^*|=1}} p_S(\mathcal{S}^* | \mathcal{S}_{o'}) \tag{24}$$

Grouping the summations in (24), we obtain:

$$\sum_{\mathcal{S}_{o'} \in \mathsf{P}'} p_S(\mathcal{S}_{o'}) \max_{\substack{\mathsf{P}^* \in \mathtt{LoI}(\mathcal{S}) \\ |\mathsf{P}^*| \leq 2^n}} \sum_{\substack{\mathcal{S}^* \in \mathsf{P}^* \\ |\mathcal{S}^*|=1}} p_S(\mathcal{S}^* | \mathcal{S}_{o'}) \tag{25}$$

And noting that (25) is the definition of $PG_n^{\subseteq}(p_S, \mathsf{P}')$ concludes the proof.

2. ($\Leftarrow$) We reason by counter-positive and show that if $\mathsf{P} \not\sqsubseteq \mathsf{P}'$, then there exists a probability distribution p_S on secrets and a value $n \geq 0$ that make $PG_n^{\subseteq}(p_S, \mathsf{P}') < PG_n^{\subseteq}(p_S, \mathsf{P})$.
If $\mathsf{P} \not\sqsubseteq \mathsf{P}'$, then there exist two secrets s_1, s_2 that are in the same block of partition P', but in different blocks in partition P. Take p_S to be the distribution on secrets that is zero in every secret with exception of $p_S(s_1) > 0$ and $p_S(s_2) > 0$. Then there are only two blocks in P with non-zero probability, one block $\mathcal{S}_1$ containing s_1 and the other one $\mathcal{S}_2$ containing s_2. Let us pick $n = 0$, and calculate $PG_0^{\subseteq}(p_S, \mathsf{P}')$ to be:

$$p_S(\mathcal{S}_1) \max_{\substack{\mathsf{P}^* \in \mathtt{LoI}(\mathcal{S}) \\ |\mathsf{P}^*| \leq 1}} \sum_{\substack{\mathcal{S}^* \in \mathsf{P}^* \\ |\mathcal{S}^*|=1}} p_S(\mathcal{S}^* | \mathcal{S}_1) + p_S(\mathcal{S}_2) \max_{\substack{\mathsf{P}^* \in \mathtt{LoI}(\mathcal{S}) \\ |\mathsf{P}^*| \leq 1}} \sum_{\substack{\mathcal{S}^* \in \mathsf{P}^* \\ |\mathcal{S}^*|=1}} p_S(\mathcal{S}^* | \mathcal{S}_2) \tag{26}$$

On the right-hand side of (26), in order to satisfy the maximizations the partition P^* must have at most one block, i.e., the sets $\mathcal{S}_1$ and $\mathcal{S}_2$ are not split. But because both $\mathcal{S}_1$ and $\mathcal{S}_2$ are singletons, they will satisfy the condition for the summations, and hence (26) becomes simply:

$$p_S(\mathcal{S}_1) + p_S(\mathcal{S}_2) = 1 \tag{27}$$

On the other hand, the partition P' must have a single block $\mathcal{S}_3$ containing both s_1 and s_2. So $PG_0^{\subseteq}(p_S, \mathsf{P}')$ is given by:

$$p_S(\mathcal{S}_3) \max_{\substack{\mathsf{P}^* \in \mathtt{LoI}(\mathcal{S}) \\ |\mathsf{P}^*| \leq 1}} \sum_{\substack{\mathcal{S}^* \in \mathsf{P}^* \\ |\mathcal{S}^*| = 1}} p_S(\mathcal{S}^* | \mathcal{S}_3) \tag{28}$$

Again, in (28) the partition P^* must have at most one block, meaning that the set $\mathcal{S}_3$ cannot be split. This implies that the only block $\mathcal{S}^* \in \mathsf{P}^*$ will have size 2, so the summation inẽqrefeq:pgalt-loi-7 is actually zero. Comparing that to (27), we conclude that for the particular p_S and n we constructed it is the case that $PG_n^{\subseteq}(p_S, \mathsf{P}') < PG_n^{\subseteq}(p_S, \mathsf{P})$.

□

A.IV Results regarding worth of certainty

Lemma 1. *Let $\mathcal{S}$ be a set of secrets composed by the fields in $\mathcal{F}$ and distributed according to p_S, and let C_a be an attack with observables in $\mathcal{O}$. Then for all $o \in \mathcal{O}$:*

$$supp(p_S(\cdot|o)) \subseteq supp(p_S)$$

Proof. If $s \in \mathcal{S}$ is in the support of $p_S(\cdot|o)$, then $p_S(s|o) = \frac{p_S(s)C_a(s,o)}{p_a(o)} > 0$. Hence it must be the case that also $p_S(s) > 0$, and $s \in supp(p_S)$. □

Lemma 2. *Let $\mathcal{S}$ be a set of secrets composed by the fields in $\mathcal{F}$, and let p'_S, p''_S be two probability distributions on $\mathcal{S}$. Then:*

$$supp(p'_S) \subseteq supp(p''_S) \implies ded(p''_S) \subseteq ded(p'_S)$$

Proof. By definition of deducible fields, $f \in ded(p''_S)$ if there is no pair of secrets $s', s'' \in supp(p''_S)$ such that $s'[f] \neq s''[f]$. It is easy to see that if $supp(p'_S) \subseteq supp(p''_S)$, no such a pair of secrets belong to $supp(p'_S)$ either, and therefore $f \in ded(p'_S)$. □

Proposition 5. *Let $\mathcal{S}$ be a set of secrets composed by the fields in $\mathcal{F}$ and C_a be an attack. For every distribution p_S on $\mathcal{S}$ and every worth assignment ω, the following holds.*

$$WCER(\omega, p_S, C_a) \geq WCER(\omega, p_S)$$

Proof. By Lemma 1, for every $o \in \mathcal{O}$, $supp(p_S(\cdot|o)) \subseteq supp(p_S)$. That means, by Lemma 2, that $ded(p_S(\cdot|o)) \geq ded(\omega(p_S))$. Because of the monotonicity of worth assignment ω, it follows that for every $o \in \mathcal{O}$, $\omega(ded(p_S(\cdot|o))) \geq \omega(ded(\omega(p_S)))$.

Using this fact in the definition of worth of certainty:

$$
\begin{aligned}
WCER(\omega, p_S, C_a) = &\sum_{o\in\mathcal{O}} p_a(o)\omega(ded(p_S(\cdot|o))) \\
\geq &\sum_{o\in\mathcal{O}} p_a(o)\omega(ded(p_S)) \\
= &\omega(ded(p_S)) \sum_{o\in\mathcal{O}} p_a(o) \\
= &\omega(ded(p_S)) \\
= &WCER(\omega, p_S)
\end{aligned}
$$

□

Proposition 6. *Let $\mathcal{S}$ be a set of secrets composed by the fields in $\mathcal{F}$. For every two partitions P and P' in the* `LoI` *of $\mathcal{S}$ the following holds:*

$$
\mathsf{P} \sqsubseteq \mathsf{P}' \quad \Leftrightarrow \quad \forall\omega\ \forall p_S\, WCER(\omega, p_S, \mathsf{P}) \leq WCER(\omega, p_S, \mathsf{P}')
$$

Proof. 1. (⇒) By definition, the value of $WCER(\omega, p_S, \mathsf{P})$ is given by:

$$
\sum_{\mathcal{S}_o\in\mathsf{P}} p_a(\mathcal{S}_o)\, WCER(\omega, p_a(\cdot|\mathcal{S}_o)) \tag{29}
$$

Since each block of P is split into blocks of P', (29) can be rewritten as:

$$
\begin{aligned}
\sum_{\mathcal{S}_o\in\mathsf{P}} \left(\sum_{\mathcal{S}_{o'}\in\mathsf{P}'} p(\mathcal{S}_{o'}|\mathcal{S}_o) \right) p_a(\mathcal{S}_o)\, WCER(\omega, p_a(\cdot|\mathcal{S}_o)) = \\
\sum_{\mathcal{S}_{o'}\in\mathsf{P}'} \sum_{\mathcal{S}_o\in\mathsf{P}} p(\mathcal{S}_{o'}, \mathcal{S}_o)\, WCER(\omega, p_a(\cdot|\mathcal{S}_o))
\end{aligned} \tag{30}
$$

Noting that $supp(p(\cdot|\mathcal{S}_{o'}, \mathcal{S}_o)) \subseteq supp(p(\cdot|\mathcal{S}_{o'}))$, we can use Lemma 2 to deduce that

$$
\begin{aligned}
WCER(\omega, p_a(\cdot|\mathcal{S}_o)) \leq &WCER(\omega, p_a(\cdot|\mathcal{S}_{o'}, \mathcal{S}_o)) \\
= &WCER(\omega, p_a(\cdot|\mathcal{S}_{o'}))
\end{aligned} \tag{31}
$$

where the equality follows because P' is a refinement of P and therefore $p(\cdot|\mathcal{S}_{o'}, \mathcal{S}_o) = p(\cdot|\mathcal{S}_{o'})$. Using (31), we deduce that (30) must be smaller or equal than:

$$
\begin{aligned}
\sum_{\mathcal{S}_{o'}\in\mathsf{P}'} \sum_{\mathcal{S}_o\in\mathsf{P}} p(\mathcal{S}_{o'}, \mathcal{S}_o)\, WCER(\omega, p_a(\cdot|\mathcal{S}_{o'})) = \\
\sum_{\mathcal{S}_{o'}\in\mathsf{P}'} p(\mathcal{S}_{o'})\, WCER(\omega, p_a(\cdot|\mathcal{S}_{o'})) = \\
WCER(\omega, \mathsf{P}')
\end{aligned}
$$

2. ($\Leftarrow$) We reason by counter-positive and show that if $\mathsf{P} \not\sqsubseteq \mathsf{P}'$, then there exists a probability distribution p_S on secrets and a worth assignment ω that make $WCER(\omega, p_S, \mathsf{P}') < WCER(\omega, p_S, \mathsf{P})$.
If $\mathsf{P} \not\sqsubseteq \mathsf{P}'$, then there exist two secrets s_1, s_2 that are in the same block of partition P', but in different blocks in partition P. Take p_S to be the distribution on secrets that is zero in every secret with exception of $p_S(s_1) > 0$ and $p_S(s_2) > 0$. Then there are only two blocks in P with non-zero probability, one block $\mathcal{S}_1$ containing s_1 and the other one $\mathcal{S}_2$ containing s_2. Noting that $ded(p_S(\cdot|\mathcal{S}_1)) = ded(p_S(\cdot|\mathcal{S}_2)) = \mathcal{F}$, we can calculate:

$$\begin{aligned} WCER(\omega, p_S, \mathsf{P}) =& p(\mathcal{S}_1)\omega(ded(p_S(\cdot|\mathcal{S}_1))) + p(\mathcal{S}_2)\omega(ded(p_S(\cdot|\mathcal{S}_2))) \\ =& p(\mathcal{S}_1)\omega(\mathcal{F}) + p(\mathcal{S}_2)\omega(\mathcal{F}) \\ =& \omega(\mathcal{F}) \end{aligned}$$

On the other hand, the partition P' must have a single block $\mathcal{S}_3$ containing both s_1 and s_2. Note that since $s_1 \neq s_2$, they must differ in at least one field, and therefore $ded(p_S(\cdot|\mathcal{S}_3))$ is a proper subset of $\mathcal{F}$. By choosing a $\mathcal{F}$-roofed worth assignment ω, we have that $\omega(ded(p_S(\cdot|\mathcal{S}_3))) < \omega(\mathcal{F})$ and consequently for the particular p_S we constructed it is the case that $WCER(\omega, p_S, \mathsf{P}') < WCER(\omega, p_S, \mathsf{P})$.

□

A.V Results regarding *W*-vulneratiblity

Lemma 3. *Let $\mathcal{S}$ be a set of secrets composed by the fields in $\mathcal{F}$, distributed according to p_S, and let P and P' be partitions in the `LoI` of $\mathcal{S}$ such that $\mathsf{P} \sqsubseteq \mathsf{P}'$. Then, for every block $\mathcal{S}_o$ of secrets belonging to partition P the following holds:*

$$\sum_{\mathcal{S}_{o'} \in \mathsf{P}'} p(\mathcal{S}_{o'}|\mathcal{S}_o) p_S(\mathfrak{f}|\mathcal{S}_{o'}) \geq p_S(\mathfrak{f}|\mathcal{S}_o)$$

Proof.

$$\begin{aligned} \sum_{\mathcal{S}_{o'} \in \mathsf{P}'} p(\mathcal{S}_{o'}|\mathcal{S}_o) p_S(\mathfrak{f}|\mathcal{S}_{o'}) &= \sum_{\mathcal{S}_{o'} \in \mathsf{P}'} p(\mathcal{S}_{o'}|\mathcal{S}_o) \max_{x \in \mathcal{S}[\mathfrak{f}]} \sum_{\substack{s \in \mathcal{S} \\ s[\mathfrak{f}]=x}} p_S(s|\mathcal{S}_{o'}) \\ &= \sum_{\substack{\mathcal{S}_{o'} \in \mathsf{P}' \\ \mathcal{S}_{o'} \subseteq \mathcal{S}_o}} \frac{p(\mathcal{S}_{o'})}{p(\mathcal{S}_o)} \max_{x \in \mathcal{S}[\mathfrak{f}]} \sum_{\substack{s \in \mathcal{S}_{o'} \\ s[\mathfrak{f}]=x}} \frac{p_S(s)}{p(\mathcal{S}_{o'})} \\ &\geq \max_{x \in \mathcal{S}[\mathfrak{f}]} \sum_{\substack{\mathcal{S}_{o'} \in \mathsf{P}' \\ \mathcal{S}_{o'} \subseteq \mathcal{S}_o}} \sum_{\substack{s \in \mathcal{S}_{o'} \\ s[\mathfrak{f}]=x}} \frac{p_S(s)}{p(\mathcal{S}_o)} \\ &= \max_{x \in \mathcal{S}[\mathfrak{f}]} \sum_{\substack{s \in \mathcal{S}_o \\ s[\mathfrak{f}]=x}} \frac{p_S(s)}{p(\mathcal{S}_o)} \\ &= p_S(\mathfrak{f}|\mathcal{S}_o) \end{aligned}$$

□

Proposition 7. *Let $\mathcal{S}$ be a set of secrets composed by the fields in $\mathcal{F}$ and C_a be an attack. For every distribution p_S on $\mathcal{S}$ and every worth assignment ω, the following holds.*

$$WV(\omega, p_S, C_a) \geq WV(\omega, p_S)$$

Proof. By definition of W-vulnerability, $WV(\omega, p_S, C_a)$ is given by:

$$\sum_{o \in \mathcal{O}} p_a(o) \max_{\mathfrak{f} \subseteq \mathcal{F}} (p_S(\mathfrak{f}|o)\omega(\mathfrak{f})) \tag{32}$$

By taking the max out of the summation, and then applying the definition of $p_S(\mathfrak{f}|o)$, we make (32) greater or equal than:

$$\max_{\mathfrak{f} \subseteq \mathcal{F}} \omega(\mathfrak{f}) \sum_{o \in \mathcal{O}} p_a(o) p_S(\mathfrak{f}|o) =$$
$$\max_{\mathfrak{f} \subseteq \mathcal{F}} \omega(\mathfrak{f}) \sum_{o \in \mathcal{O}} p_a(o) \max_{x \in \mathcal{S}[\mathfrak{f}]} \sum_{\substack{s \in \mathcal{S} \\ s[\mathfrak{f}]=x}} p_S(s|o) \tag{33}$$

Again taking the max out of the summation makes (33) greater or equal than:

$$\max_{\mathfrak{f} \subseteq \mathcal{F}} \omega(\mathfrak{f}) \max_{x \in \mathcal{S}[\mathfrak{f}]} \sum_{\substack{s \in \mathcal{S} \\ s[\mathfrak{f}]=x}} \sum_{o \in \mathcal{O}} p_S(s, o) =$$
$$\max_{\mathfrak{f} \subseteq \mathcal{F}} \omega(\mathfrak{f}) \max_{x \in \mathcal{S}[\mathfrak{f}]} \sum_{\substack{s \in \mathcal{S} \\ s[\mathfrak{f}]=x}} p_S(s) \tag{34}$$

And noting that (34) is exactly the definition of $WV(\omega, p_S)$ concludes the proof.
□

Proposition 8. *Let $\mathcal{S}$ be a set of secrets composed by the fields in $\mathcal{F}$. For every two partitions P and P' in the* `LoI` *of $\mathcal{S}$ the following holds:*

$$\mathsf{P} \sqsubseteq \mathsf{P}' \quad \Leftrightarrow \quad \forall \omega \ \forall p_S \, WV(\omega, p_S, \mathsf{P}) \leq WV(\omega, p_S, \mathsf{P}')$$

Proof. 1. ($\Rightarrow$) By definition, the value of $WV(\omega, p_S, \mathsf{P})$ is given by:

$$\sum_{\mathcal{S}_o \in \mathsf{P}} p_a(\mathcal{S}_o) \, WV(\omega, p_a(\cdot|\mathcal{S}_o)) \tag{35}$$

Since each block of P is split into blocks of P', and by applying the definition of $p_S(\mathfrak{f}|o)$, (35) can be rewritten as:

$$\sum_{\mathcal{S}_o \in \mathsf{P}} \left(\sum_{\mathcal{S}_{o'} \in \mathsf{P}'} p(\mathcal{S}_{o'}|\mathcal{S}_o) \right) \max_{\mathfrak{f} \subseteq \mathcal{F}} (p_S(\mathfrak{f}|\mathcal{S}_o)\omega(\mathfrak{f})) \tag{36}$$

By taking the max out of the summation, we infer that (36) must be greater or equal than:

$$\sum_{\mathcal{S}_o \in \mathsf{P}} \max_{\mathfrak{f} \subseteq \mathcal{F}} \omega(\mathfrak{f}) \sum_{\mathcal{S}_{o'} \in \mathsf{P}'} p(\mathcal{S}_{o'}|\mathcal{S}_o) p_S(\mathfrak{f}|\mathcal{S}_o) \tag{37}$$

Using Lemma 3, (37) is greater or equal than:

$$\sum_{\mathcal{S}_o \in \mathsf{P}} \max_{\mathfrak{f} \subseteq \mathcal{F}} \omega(\mathfrak{f}) p_S(\mathfrak{f}|\mathcal{S}_o) \tag{38}$$

And noting that (38) is the definition of $WV(\omega, p_S)$ concludes the proof.

2. ($\Leftarrow$) We reason by counter-positive and show that if $\mathsf{P} \not\sqsubseteq \mathsf{P}'$, then there exists a probability distribution p_S on secrets and a worth assignment ω that make $WV(\omega, p_S, \mathsf{P}') < WV(\omega, p_S, \mathsf{P})$. If $\mathsf{P} \not\sqsubseteq \mathsf{P}'$, then there exist two secrets s_1, s_2 that are in the same block of partition P', but in different blocks in partition P. Take p_S to be the distribution on secrets that is zero in every secret with exception of $p_S(s_1) > 0$ and $p_S(s_2) > 0$. Then there are only two blocks in P with non-zero probability, one block $\mathcal{S}_1$ containing s_1 and the other one $\mathcal{S}_2$ containing s_2. We can then calculate:

$$WV(\omega, p_S, \mathsf{P}) = p_S(\mathcal{S}_1) \max_{\mathfrak{f} \subseteq \mathcal{F}} p_S(\mathfrak{f}|\mathcal{S}_1)\omega(\mathfrak{f}) + p_S(\mathcal{S}_2) \max_{\mathfrak{f} \subseteq \mathcal{F}} p_S(\mathfrak{f}|\mathcal{S}_2)\omega(\mathfrak{f}) \tag{39}$$

Since $\mathcal{S}_1$ and $\mathcal{S}_2$ have one non-zero element each, both maximizations are realized on $\mathfrak{f} = \mathcal{F}$, which makes $p_S(\mathfrak{f}|\mathcal{S}_1) = p_S(\mathfrak{f}|\mathcal{S}_2) = 1$. Therefore (39) becomes:

$$\begin{aligned} WV(\omega, p_S, \mathsf{P}) =& p_S(\mathcal{S}_1) \cdot 1 \cdot \omega(\mathcal{F}) + p_S(\mathcal{S}_2) \cdot 1 \cdot \omega(\mathcal{F}) \\ =& \omega(\mathcal{F}) \end{aligned} \tag{40}$$

On the other hand, the partition P' must have a single block $\mathcal{S}_3$ containing both s_1 and s_2. We then derive:

$$\begin{aligned} WV(\omega, p_S, \mathsf{P}') =& p_S(\mathcal{S}_3) \max_{\mathfrak{f} \subseteq \mathcal{F}} p_S(\mathfrak{f}|\mathcal{S}_3)\omega(\mathfrak{f}) \\ =& \max_{\mathfrak{f} \subseteq \mathcal{F}} p_S(\mathfrak{f}|\mathcal{S}_3)\omega(\mathfrak{f}) && (41) \\ =& p_S(\mathfrak{f}^*|\mathcal{S}_3)\omega(\mathfrak{f}^*) && (42) \end{aligned}$$

where (41) follows because $p_S(\mathcal{S}_3) = 1$, and in (41) $\mathfrak{f}^*$ is the *argmax*. To conclude the proof, we show that (40) > (42), since we have found some $p_S(\cdot)$ that makes $WV(\omega, p_S, \mathsf{P}) > WV(\omega, p_S, \mathsf{P}')$. Let us choose an $\mathcal{F}$-roofed worth assignment ω and analyze the two possible cases:

i. In the case $\mathfrak{f}^* = \mathcal{F}$, we have:

$$\begin{aligned}
WV(\omega, p_S, \mathsf{P}') =& p_S(\mathcal{F}|\mathcal{S}_3)\omega(\mathcal{F}) \\
=& \omega(\mathcal{F}) \frac{1}{p_S(\mathcal{S}_3)} \max_{x \in \mathcal{S}[\mathcal{F}]} \sum_{\substack{s \in \mathcal{S}_3 \\ s[\mathcal{F}]=x}} p_S(s) \\
=& \omega(\mathcal{F}) \max_{x \in \mathcal{S}[\mathcal{F}]} \sum_{\substack{s \in \mathcal{S}_3 \\ s[\mathcal{F}]=x}} p_S(s) \qquad (43)
\end{aligned}$$

But note that since $s_1 \neq s_2$, it is impossible that $s_1[\mathcal{F}] = s_2[\mathcal{F}]$. Therefore at least one among s_1 and s_2 does not satisfy the condition on the summation in (43), and its result is necessarily smaller than 1. Hence $WV(\omega, p_S, \mathsf{P}') < \omega(\mathcal{F})$

ii. In the case $\mathfrak{f}^* \subset \mathcal{F}$, we have:

$$\begin{aligned}
WV(\omega, p_S, \mathsf{P}') =& p_S(\mathfrak{f}^*|\mathcal{S}_3)\omega(\mathfrak{f}^*) \\
\leq& 1 \cdot \omega(\mathfrak{f}^*) \qquad (44) \\
<& \omega(\mathcal{F}) \qquad (45)
\end{aligned}$$

where (44) follows because for every $\mathfrak{f}*$ it is the case that $p_S(\mathfrak{f}^*|\mathcal{S}_3) \leq 1$, and (45) follows because ω is $\mathcal{F}$-roofed.

□

Proposition 9. *Let $\mathcal{S}$ be a set of secrets distributed according to p_S, and C_a be an attack. Then the following holds:*

$$V(p_S, C_a) = WV(\omega_{bin}, p_S, C_a)$$

Proof. By definition:

$$\begin{aligned}
WV(\omega_{bin}, p_S) =& \max_{\mathfrak{f} \subseteq \mathcal{F}} (p_S(\mathfrak{f})\omega_{bin}(\mathfrak{f})) \\
=& p_S(\mathcal{F}) \qquad (46) \\
=& \max_{x \in \mathcal{S}[\mathcal{F}]} \sum_{\substack{s \in \mathcal{S} \\ s[\mathcal{F}]=x}} p_S(s) \qquad (47)
\end{aligned}$$

where (46) follows because $\omega_{bin}(\mathfrak{f}) > 0$ only for $\mathfrak{f} = \mathcal{F}$; and in (47) we apply the definition of $p_S(\mathcal{F})$. Since finding an element such that $s[\mathcal{F}] = x$ is the same as finding the (unique) element $s = x$ itself, (47) can be rewritten as follows:

$$\begin{aligned}
WV(\omega_{bin}, p_S) =& \max_{s \in \mathcal{S}} p_S(s) \\
=& V(p_S) \qquad (48)
\end{aligned}$$

From (48), and from Definition 3, for every C_a it follows immediately that $V(p_S, C_a) = WV(\omega_{bin}, p_S, C_a)$. □

A.VI Results regarding worth of expectation under =

Lemma 4. *Let $\mathcal{S}$ be a set of secrets composed by the fields in $\mathcal{F}$, and let ν be a composable measure of information worth consistent with respect to the* `LoI`*. Then for every probability distribution p_S on secrets, and for any sets $\mathcal{X}, \mathcal{Y}_1, \ldots, \mathcal{Y}_n \subseteq \mathcal{S}$ such that $\mathcal{X} = \bigcup_{i=1}^{n} \mathcal{Y}_i$ and $\bigcap_{i=1}^{n} \mathcal{Y}_i = \emptyset$:*

$$p_S(\mathcal{X})\nu(\omega, p_S(\cdot|\mathcal{X}), \mathcal{X}) \leq \sum_{i=1}^{n} p_S(\mathcal{Y}_i)\nu(\omega, p_S(\cdot|\mathcal{Y}_i), \mathcal{Y}_i)$$

Proof. Consider the probability distribution $p_S(\cdot|\mathcal{X})$. Since for every $1 \leq i \leq n$ we have $\mathcal{Y}_i \subseteq \mathcal{X}$, it follows that $p_S(\mathcal{Y}_i|\mathcal{X}) = \frac{p_S(\mathcal{Y}_i)}{p_S(\mathcal{X})}$, and $p_S(s|\mathcal{X}) = 0$ for any $s \notin \mathcal{X}$. Consider now partitions P, P' such that every block in P is exactly the same as every block in P', with the exception that $\mathcal{X}$ is a block in P and the corresponding blocks on P' are $\mathcal{Y}_i, \ldots, \mathcal{Y}_n$. Note that, by construction, $\mathsf{P} \sqsubseteq \mathsf{P}'$. We can derive:

$$\nu(\omega, p_S(\cdot|\mathcal{X}), \mathsf{P}) = \nu(\omega, p_S(\cdot|\mathcal{X}), \mathcal{X}) \tag{49}$$

On the other hand:

$$\nu(\omega, p_S(\cdot|\mathcal{X}), \mathsf{P}') = \sum_{i=1}^{n} p_S(\mathcal{Y}_i|\mathcal{X})\nu(\omega, p_S(\cdot|\mathcal{Y}_i), \mathcal{Y}_i) \tag{50}$$

Since ν is consistent with respect to the `LoI`, for every distribution $p'(\cdot)$ on secrets it is the case that $\nu(\omega, p'(\cdot), \mathsf{P}) \leq \nu(\omega, p'(\cdot), \mathsf{P}')$. In particular, that is true for the probability distribution $p_S(\cdot|\mathcal{X})$. Then we can compare (49) and (50) as follows:

$$\begin{aligned}\nu(\omega, p_S(\cdot|\mathcal{X}), \mathcal{X}) \leq& \sum_{i=1}^{n} p_S(\mathcal{Y}_i|\mathcal{X})\nu(\omega, p_S(\cdot|\mathcal{Y}_i), \mathcal{Y}_i)\\ =& \frac{1}{p_S(\mathcal{X})} \sum_{i=1}^{n} p_S(\mathcal{Y}_i)\nu(\omega, p_S(\cdot|\mathcal{Y}_i), \mathcal{Y}_i)\end{aligned}$$

From which the proposition follows immediately. $\square$

Proposition 10. *Let $\mathcal{S}$ be a set of secrets composed by the fields in $\mathcal{F}$ and C_a be an attack. Let ν be a (valid) composable W-measure, and $n \geq 0$ be the number of guesses allowed for the adversary. For every distribution p_S on $\mathcal{S}$ and every worth assignment ω the following holds.*

$$WEXP^{=}_{n,\nu}(\omega, p_S, C_a) \geq WEXP^{=}_{n,\nu}(\omega, p_S)$$

Proof. By definition of worth of expectation under $=$, $WEXP^{=}_{n,\nu}(\omega, p_S, C_a)$ is given by:

$$\sum_{o \in \mathcal{O}} p_a(o) \max_{\substack{\mathcal{S}' \subseteq \mathcal{S} \\ |\mathcal{S}'| \leq n}} \left(p_S(\mathcal{S}'|o)\omega(\mathcal{F}) + p_S(\bar{\mathcal{S}}'|o)\nu(\omega, p_S(\cdot|\bar{\mathcal{S}}', o))\right) \tag{51}$$

By taking the max out of the summation, we make (51) greater or equal than:

$$\max_{\substack{\mathcal{S}'\subseteq\mathcal{S}\\|\mathcal{S}'|\leq n}} \sum_{o\in\mathcal{O}} p_a(o)\left(p_S(\mathcal{S}'|o)\omega(\mathcal{F}) + p_S(\bar{\mathcal{S}}'|o)\nu(\omega, p_S(\cdot|\bar{\mathcal{S}}', o))\right) =$$

$$\max_{\substack{\mathcal{S}'\subseteq\mathcal{S}\\|\mathcal{S}'|\leq n}} \left(p_S(\mathcal{S}')\omega(\mathcal{F}) + p_S(\bar{\mathcal{S}}')\sum_{o\in\mathcal{O}} p_a(o|\bar{\mathcal{S}}')\nu(\omega, p_S(\cdot|\bar{\mathcal{S}}', o))\right) \tag{52}$$

By hypothesis, ν is a composable measure, and hence (52) can be rewritten as:

$$\max_{\substack{\mathcal{S}'\subseteq\mathcal{S}\\|\mathcal{S}'|\leq n}} \left(p_S(\mathcal{S}')\omega(\mathcal{F}) + p_S(\bar{\mathcal{S}}')\nu(\omega, p_S(\cdot|\bar{\mathcal{S}}'), C_a)\right) \tag{53}$$

Because ν is a valid measure, $\nu(\omega, p_S(\cdot|\bar{\mathcal{S}}'), C_a) \geq \nu(\omega, p_S(\cdot|\bar{\mathcal{S}}'))$ and hence (53) is greater or equal than:

$$\max_{\substack{\mathcal{S}'\subseteq\mathcal{S}\\|\mathcal{S}'|\leq n}} \left(p_S(\mathcal{S}')\omega(\mathcal{F}) + p_S(\bar{\mathcal{S}}')\nu(\omega, p_S(\cdot|\bar{\mathcal{S}}'))\right) \tag{54}$$

And noting that (54) is exactly the definition of $WEXP^{=}_{n,\nu}(\omega, p_S)$ concludes the proof. □

Proposition 11. *Let $\mathcal{S}$ be a set of secrets composed by the fields in $\mathcal{F}$. For every two partitions P and P' in the* `LoI` *of $\mathcal{S}$ the following holds:*

$$\mathsf{P} \sqsubseteq \mathsf{P}' \quad \Leftrightarrow \quad \forall n\ \forall \nu\ \forall \omega\ \forall p_S\ WEXP^{=}_{n,\nu}(\omega, p_S, \mathsf{P}) \leq WEXP^{=}_{n,\nu}(\omega, p_S, \mathsf{P}')$$

where $n \geq 0$ and ν is any composable W-measure consistent with respect to the `LoI`*.*

Proof.

1. ($\Rightarrow$) It is enough to consider one block $\mathcal{S}_o$ in the partition P that is split into blocks $\mathcal{S}_{o'}$ and $\mathcal{S}_{o''}$ in partition P'. Let us derive the value of:

$$WEXP^{=}_{n,\nu}(\omega, p_S(\cdot|\mathcal{S}_o), \mathcal{S}_o) \tag{55}$$

Using the definition of worth of expectation under $=$, (55) can be rewritten as:

$$\max_{\substack{\mathcal{X}\subseteq\mathcal{S}_o\\|\mathcal{X}|\leq n}} \left(p_S(\mathcal{X}|\mathcal{S}_o)\omega(\mathcal{F}) + p_S(\bar{\mathcal{X}}|\mathcal{S}_o)\nu(\omega, p_S(\cdot|\bar{\mathcal{X}}), \bar{\mathcal{X}})\right) \tag{56}$$

where $\bar{\mathcal{X}} = \mathcal{S}_o \backslash \mathcal{X}$.
Calling $\mathcal{X}_o$ the subset of $\mathcal{X}$ that realizes the maximization, (56) can be rewritten as:

$$p_S(\mathcal{X}_o|\mathcal{S}_o)\omega(\mathcal{F}) + p_S(\bar{\mathcal{X}}_o|\mathcal{S}_o)\nu(\omega, p_S(\cdot|\bar{\mathcal{X}}_o), \bar{\mathcal{X}}_o) \tag{57}$$

where $\bar{\mathcal{X}}_o = \mathcal{S}_o \backslash \mathcal{X}_o$.
Let $\mathcal{X}_{o'}$ and $\mathcal{X}_{o''}$ be the projection of $\mathcal{X}_o$ onto $\mathcal{S}_{o'}$ and $\mathcal{S}_{o''}$, respectively. Similarly, let $\bar{\mathcal{X}}_{o'}$ and $\bar{\mathcal{X}}_{o''}$ be the projection of $\bar{\mathcal{X}}_o$ onto $\mathcal{S}_{o'}$ and $\mathcal{S}_{o''}$, respectively. Then we can split the summations and (57) becomes:

$$\begin{aligned} p_S(\mathcal{X}_{o'}|\mathcal{S}_o)\omega(\mathcal{F}) + p_S(\mathcal{X}_{o''}|\mathcal{S}_o)\omega(\mathcal{F}) + \\ + p_S(\bar{\mathcal{X}}_{o'} \cup \bar{\mathcal{X}}_{o''}|\mathcal{S}_o)\nu(\omega, p_S(\cdot|\bar{\mathcal{X}}_{o'} \cup \bar{\mathcal{X}}_{o''}), \bar{\mathcal{X}}_{o'} \cup \bar{\mathcal{X}}_{o''}) \end{aligned} \tag{58}$$

Let us call $n^* \leq n$ the number that maximizes $WEXP^{=}_{n,\nu}(\omega, p_S(\cdot|\mathcal{S}_o), \mathcal{S}_o)$ together with $\mathcal{X}_o$. Now we explicit an arbitrary subset $\bar{\mathcal{X}}^n_{o'} \in \bar{\mathcal{X}}_{o'}$ such that $\bar{\mathcal{X}}^n_{o'} = n^* - |\mathcal{X}_{o'}|$. Note that it is always possible because $\mathcal{X}_{o'} \subseteq \mathcal{X}_o$ and $|\mathcal{X}_o| = n^*$. We proceed similarly for a set $\bar{\mathcal{X}}^n_{o''} \in \bar{\mathcal{X}}_{o''}$ such that $\bar{\mathcal{X}}^n_{o''} = n^* - |\mathcal{X}_{o''}|$. Then we can rewrite $\bar{\mathcal{X}}_{o'} \cup \bar{\mathcal{X}}_{o''}$ as $\bar{\mathcal{X}}^n_{o'} \cup \bar{\mathcal{X}}_{o'} \backslash \bar{\mathcal{X}}^n_{o'} \cup \bar{\mathcal{X}}^n_{o''} \cup \bar{\mathcal{X}}_{o''} \backslash \bar{\mathcal{X}}^n_{o''}$. Since ν is a composable measure that is consistent with respect to `LoI` (or the worth of certainty measure), we can use Lemma 4 to split $p_S(\bar{\mathcal{X}}_{o'} \cup \bar{\mathcal{X}}_{o''})\nu(\omega, p_S(\cdot|\bar{\mathcal{X}}_{o'} \cup \bar{\mathcal{X}}_{o''}), \bar{\mathcal{X}}_{o'} \cup \bar{\mathcal{X}}_{o''})$ and we can deduce that (58) is smaller or equal than the following:

$$\begin{aligned} p_S(\mathcal{X}_{o'}|\mathcal{S}_o)\omega(\mathcal{F}) + p_S(\mathcal{X}_{o''}|\mathcal{S}_o)\omega(\mathcal{F}) + \\ + p_S(\bar{\mathcal{X}}^n_{o'}|\mathcal{S}_o)\nu(\omega, p_S(\cdot|\bar{\mathcal{X}}_{o'}), \bar{\mathcal{X}}_{o'}) + \\ + p_S(\bar{\mathcal{X}}_{o'} \backslash \bar{\mathcal{X}}^n_{o'}|\mathcal{S}_o)\nu(\omega, p_S(\cdot|\bar{\mathcal{X}}_{o'} \backslash \bar{\mathcal{X}}^n_{o'}), \bar{\mathcal{X}}_{o'} \backslash \bar{\mathcal{X}}^n_{o'}) + \\ + p_S(\bar{\mathcal{X}}^n_{o''}|\mathcal{S}_o)\nu(\omega, p_S(\cdot|\bar{\mathcal{X}}_{o''}), \bar{\mathcal{X}}_{o''}) + \\ + p_S(\bar{\mathcal{X}}_{o''} \backslash \bar{\mathcal{X}}^n_{o''}|\mathcal{S}_o)\nu(\omega, p_S(\cdot|\bar{\mathcal{X}}_{o''} \backslash \bar{\mathcal{X}}^n_{o''}), \bar{\mathcal{X}}_{o''} \backslash \bar{\mathcal{X}}^n_{o''}) \end{aligned} \tag{59}$$

But $\nu(\omega, p_S(\cdot|\bar{\mathcal{X}}_{o'}), \bar{\mathcal{X}}_{o'}) \leq \omega(\mathcal{F})$, and $\nu(\omega, p_S(\cdot|\bar{\mathcal{X}}_{o''}), \bar{\mathcal{X}}_{o''}) \leq \omega(\mathcal{F})$. Hence (59) is smaller or equal than the following:

$$\begin{aligned} p_S(\mathcal{X}_{o'}|\mathcal{S}_o)\omega(\mathcal{F}) + p_S(\mathcal{X}_{o''}|\mathcal{S}_o)\omega(\mathcal{F}) + \\ + p_S(\bar{\mathcal{X}}^n_{o'}|\mathcal{S}_o)\omega(\mathcal{F}) + \\ + p_S(\bar{\mathcal{X}}_{o'} \backslash \bar{\mathcal{X}}^n_{o'}|\mathcal{S}_o)\nu(\omega, p_S(\cdot|\bar{\mathcal{X}}_{o'} \backslash \bar{\mathcal{X}}^n_{o'}), \bar{\mathcal{X}}_{o'} \backslash \bar{\mathcal{X}}^n_{o'}) + \\ + p_S(\bar{\mathcal{X}}^n_{o''}|\mathcal{S}_o)\omega(\mathcal{F}) + \\ + p_S(\bar{\mathcal{X}}_{o''} \backslash \bar{\mathcal{X}}^n_{o''}|\mathcal{S}_o)\nu(\omega, p_S(\cdot|\bar{\mathcal{X}}_{o''} \backslash \bar{\mathcal{X}}^n_{o''}), \bar{\mathcal{X}}_{o''} \backslash \bar{\mathcal{X}}^n_{o''}) \end{aligned} \tag{60}$$

Regrouping the summations, (60) can be rewritten as:

$$\begin{aligned} p_S(\mathcal{X}_{o'} \cup \bar{\mathcal{X}}^n_{o'}|\mathcal{S}_o)\omega(\mathcal{F}) + p_S(\mathcal{X}_{o''} \cup \bar{\mathcal{X}}^n_{o''}|\mathcal{S}_o)\omega(\mathcal{F}) + \\ + p_S(\bar{\mathcal{X}}_{o'} \backslash \bar{\mathcal{X}}^n_{o'}|\mathcal{S}_o)\nu(\omega, p_S(\cdot|\bar{\mathcal{X}}_{o'} \backslash \bar{\mathcal{X}}^n_{o'}), \bar{\mathcal{X}}_{o'} \backslash \bar{\mathcal{X}}^n_{o'}) + \\ + p_S(\bar{\mathcal{X}}_{o''} \backslash \bar{\mathcal{X}}^n_{o''}|\mathcal{S}_o)\nu(\omega, p_S(\cdot|\bar{\mathcal{X}}_{o''} \backslash \bar{\mathcal{X}}^n_{o''}), \bar{\mathcal{X}}_{o''} \backslash \bar{\mathcal{X}}^n_{o''}) \end{aligned} \tag{61}$$

Let us call $\mathcal{X}_{o'} \cup \bar{\mathcal{X}}^n_{o'} = \mathcal{Y}_1$ and $\mathcal{X}_{o''} \cup \bar{\mathcal{X}}^n_{o''} = \mathcal{Y}_2$. It follows that $\bar{\mathcal{X}}_{o'} \backslash \bar{\mathcal{X}}^n_{o'} = \bar{\mathcal{Y}}_1$, and that $\bar{\mathcal{X}}_{o''} \backslash \bar{\mathcal{X}}^n_{o''} = \bar{\mathcal{Y}}_2$. Hence (61) can be rewritten as:

$$\begin{aligned} p_S(\mathcal{Y}_1|\mathcal{S}_o)\omega(\mathcal{F}) + p_S(\bar{\mathcal{Y}}_1|\mathcal{S}_o)\nu(\omega, p_S(\cdot|\bar{\mathcal{Y}}_1), \bar{\mathcal{Y}}_1) + \\ + p_S(\mathcal{Y}_2|\mathcal{S}_o)\omega(\mathcal{F}) + p_S(\bar{\mathcal{Y}}_2|\mathcal{S}_o)\nu(\omega, p_S(\cdot|\bar{\mathcal{Y}}_2), \bar{\mathcal{Y}}_2) \end{aligned} \tag{62}$$

Manipulating the probabilities, (62) becomes:

$$
\begin{aligned}
&\frac{p_S(\mathcal{Y}_1)}{p_S(\mathcal{S}_o)} \cdot \frac{p_S(\mathcal{S}_{o'})}{p_S(\mathcal{S}_{o'})}\omega(\mathcal{F}) + \frac{p_S(\bar{\mathcal{Y}_1})}{p_S(\mathcal{S}_o)} \cdot \frac{p_S(\mathcal{S}_{o'})}{p_S(\mathcal{S}_{o'})}\nu(\omega, p_S(\cdot|\bar{\mathcal{Y}_1}), \bar{\mathcal{Y}_1})+ \\
+&\frac{p_S(\mathcal{Y}_2)}{p_S(\mathcal{S}_o)} \cdot \frac{p_S(\mathcal{S}_{o''})}{p_S(\mathcal{S}_{o''})}\omega(\mathcal{F}) + \frac{p_S(\bar{\mathcal{Y}_2})}{p_S(\mathcal{S}_o)} \cdot \frac{p_S(\mathcal{S}_{o''})}{p_S(\mathcal{S}_{o''})}\nu(\omega, p_S(\cdot|\bar{\mathcal{Y}_2}), \bar{\mathcal{Y}_2})
\end{aligned} \tag{63}
$$

From simple calculations, (63) becomes:

$$
\begin{aligned}
&\frac{p_S(\mathcal{S}_{o'})}{p_S(\mathcal{S}_o)}\left(p_S(\mathcal{Y}_1|\mathcal{S}_{o'})\omega(\mathcal{F}) + p_S(\bar{\mathcal{Y}_1}|\mathcal{S}_{o'})\nu(\omega, p_S(\cdot|\bar{\mathcal{Y}_1}), \bar{\mathcal{Y}_1})\right) + \\
+&\frac{p_S(\mathcal{S}_{o''})}{p_S(\mathcal{S}_o)}\left(p_S(\mathcal{Y}_2|\mathcal{S}_{o''})\omega(\mathcal{F}) + p_S(\bar{\mathcal{Y}_2}|\mathcal{S}_{o'})\nu(\omega, p_S(\cdot|\bar{\mathcal{Y}_2}), \bar{\mathcal{Y}_2})\right)
\end{aligned} \tag{64}
$$

Note that, by construction, $|\mathcal{Y}_1| \leq n^*$ and $|\mathcal{Y}_2| \leq n^*$. And since $n^* \leq n$, we can take the maximum over any set of size at most n and find that (64) is smaller or equal than the following:

$$
\begin{aligned}
&\frac{p_S(\mathcal{S}_{o'})}{p_S(\mathcal{S}_o)} \max_{\substack{\mathcal{Y}\in\mathcal{S}_{o'} \\ |\mathcal{Y}|\leq n}} \left(p_S(\mathcal{Y}|\mathcal{S}_{o'})\omega(\mathcal{F}) + p_S(\bar{\mathcal{Y}}|\mathcal{S}_{o'})\nu(\omega, p_S(\cdot|\bar{\mathcal{Y}}), \bar{\mathcal{Y}})\right) + \\
+&\frac{p_S(\mathcal{S}_{o''})}{p_S(\mathcal{S}_o)} \max_{\substack{\mathcal{Y}\in\mathcal{S}_{o''} \\ |\mathcal{Y}|\leq n}} \left(p_S(\mathcal{Y}|\mathcal{S}_{o''})\omega(\mathcal{F}) + p_S(\bar{\mathcal{Y}}|\mathcal{S}_{o''})\nu(\omega, p_S(\cdot|\bar{\mathcal{Y}}), \bar{\mathcal{Y}})\right)
\end{aligned} \tag{65}
$$

Using the definition of worth of expectation under $=$, (65) can be rewritten as:

$$
\begin{aligned}
&\frac{p_S(\mathcal{S}_{o'})}{p_S(\mathcal{S}_o)} \mathit{WEXP}^{=}_{n,\nu}(\omega, p_S(\cdot|\mathcal{S}_{o'}), \mathcal{S}_{o'})+ \\
+&\frac{p_S(\mathcal{S}_{o''})}{p_S(\mathcal{S}_o)} \mathit{WEXP}^{=}_{n,\nu}(\omega, p_S(\cdot|\mathcal{S}_{o''}), \mathcal{S}_{o''})
\end{aligned} \tag{66}
$$

Comparing (55) and (66):

$$
\begin{aligned}
p_S(\mathcal{S}_o)\,\mathit{WEXP}^{=}_{n,\nu}(\omega, p_S(\cdot|\mathcal{S}_o), \mathcal{S}_o) \leq\ & p_S(\mathcal{S}_{o'})\,\mathit{WEXP}^{=}_{n,\nu}(\omega, p_S(\cdot|\mathcal{S}_{o'}), \mathcal{S}_{o'})+ \\
&+p_S(\mathcal{S}_{o''})\,\mathit{WEXP}^{=}_{n,\nu}(\omega, p_S(\cdot|\mathcal{S}_{o''}), \mathcal{S}_{o''})
\end{aligned} \tag{67}
$$

And since worth of expectation under $=$ is a composable measure, from (67) we conclude that by splitting blocks one can never decrease the worth of expectation under $=$ of the partition.

2. ($\Leftarrow$) We reason by counter-positive and show that if $\mathsf{P} \not\sqsubseteq \mathsf{P}'$, then there exists a probability distribution p_S on secrets and a W-measure ν that makes $\mathit{WEXP}^{=}_{n,\nu}(\omega, p_S, \mathsf{P}') < \mathit{WEXP}^{=}_{n,\nu}(\omega, p_S, \mathsf{P})$. By Proposition 12, $PG_n(p_S, \mathsf{P})$ is a special case of $\mathit{WEXP}^{=}_{\nu,n}(\omega, p_S, \mathsf{P})$ for some ν and ω, so we can use as our counter-example the same probability distribution used in Theorem 4 to prove that PG_n is consistent with respect to the `LoI`.

□

Proposition 12. *Let $\mathcal{S}$ be a set of secrets distributed according to p_S, and C_a be an attack. Then the following holds for all $n \geq 0$:*

$$PG_n(p_S, C_a) = WEXP^{=}_{n,\nu_{null}}(\omega_{bin}, p_S, C_a)$$

where ν_{null} is the null W-measure such that $\nu_{null}(\omega, p_S) = 0$ for every ω and p_S.

Proof. By definition, the value of $WEXP^{=}_{n,\nu_{null}}(\omega_{bin}, p_S)$ is given by:

$$\max_{\substack{\mathcal{S}' \subseteq \mathcal{S} \\ |\mathcal{S}'| \leq n}} \big(p_S(\mathcal{S}')\omega_{bin}(\mathcal{F}) + p_S(\bar{\mathcal{S}}')\nu_{null}(\omega, p_S(\cdot|\bar{\mathcal{S}}'))\big) \tag{68}$$

Using the definitions of ω_{bin} and ν_{null}, (68) reduces to:

$$\max_{\substack{\mathcal{S}' \subseteq \mathcal{S} \\ |\mathcal{S}'| \leq n}} \big(p_S(\mathcal{S}') \cdot 1 + p_S(\bar{\mathcal{S}}') \cdot 0\big) = \max_{\substack{\mathcal{S}' \subseteq \mathcal{S} \\ |\mathcal{S}'| \leq n}} (p_S(\mathcal{S}')) \tag{69}$$

But (69) is actually the definition of the probability of guessing $PG_n(p_S)$. From this, and from Definition 4, for every C_a it follows immediately that $PG_n(p_S, C_a) = WEXP^{=}_{n,\nu_{null}}(\omega_{bin}, p_S, C_a)$. □

A.VII Results regarding *W*-guessing entropy

Proposition 13. *Let $\mathcal{S}$ be a set of secrets composed by the fields in $\mathcal{F}$ and C_a be an attack. Let ν be a W-measure that is monotonic for observations, and $0 \leq \mathsf{w} \leq \omega(\mathcal{F})$. For every distribution p_S on $\mathcal{S}$ and every worth assignment ω the following holds.*

$$WNG_{\mathsf{w},\nu}(\omega, p_S, C_a) \leq WNG_{\mathsf{w},\nu}(\omega, p_S)$$

Proof. By definition of W-guessing entropy, $WNG_{\mathsf{w},\nu}(\omega, p_S, C_a)$ is given by:

$$\sum_{o \in \mathcal{O}} p_a(o) \min_{\substack{\mathcal{S}' \subseteq \mathcal{S} \\ \nu(\omega, p_S(\cdot|\bar{\mathcal{S}}', o)) \geq \mathsf{w}}} \big(p_S(\bar{\mathcal{S}}'|o) NG(p_S(\cdot|\bar{\mathcal{S}}', o)) + p_S(\mathcal{S}'|o)(|\bar{\mathcal{S}}'| + 1)\big) \tag{70}$$

Because ν is monotonic for observations, for every $o' \in \mathcal{O}$ we have $\nu(\omega, p_S(\cdot|\mathcal{S}', o)) \geq \nu(\omega, p_S(\cdot|\mathcal{S}'))$, so we can take the max out of the summation to deduce that (70) must be smaller or equal than:

$$\min_{\substack{\mathcal{S}'\subseteq\mathcal{S}\\ \nu(\omega,p_S(\cdot|\mathcal{S}'))\geq \mathsf{w}}} \sum_{o\in\mathcal{O}} p_a(o)\left(p_S(\bar{\mathcal{S}}'|o)NG(p_S(\cdot|\bar{\mathcal{S}}',o)) + p_S(\mathcal{S}'|o)(|\bar{\mathcal{S}}'|+1)\right) =$$

$$\min_{\substack{\mathcal{S}'\subseteq\mathcal{S}\\ \nu(\omega,p_S(\cdot|\mathcal{S}'))\geq \mathsf{w}}} \left(p_S(\bar{\mathcal{S}}')\left(\sum_{o\in\mathcal{O}} p_a(o|\bar{\mathcal{S}}')NG(p_S(\cdot|\bar{\mathcal{S}}',o))\right) + \right.$$

$$\left. + p_S(\mathcal{S}')(|\bar{\mathcal{S}}'|+1)\sum_{o\in\mathcal{O}} p_a(o|\mathcal{S}')\right) =$$

$$\min_{\substack{\mathcal{S}'\subseteq\mathcal{S}\\ \nu(\omega,p_S(\cdot|\mathcal{S}'))\geq \mathsf{w}}} \left(p_S(\bar{\mathcal{S}}')NG(p_S(\cdot|\bar{\mathcal{S}}',C_a)) + p_S(\mathcal{S}')(|\bar{\mathcal{S}}'|+1)\right) \quad (71)$$

It is well known that posterior guessing entropy is always smaller than prior guessing entropy, so for every C_a, $NG(p_S(\cdot|\bar{\mathcal{S}}',C_a)) \leq NG(p_S(\cdot|\bar{\mathcal{S}}'))$ and (71) must be smaller or equal than:

$$\min_{\substack{\mathcal{S}'\subseteq\mathcal{S}\\ \nu(\omega,p_S(\cdot|\mathcal{S}'))\geq \mathsf{w}}} \left(p_S(\bar{\mathcal{S}}')NG(p_S(\cdot|\bar{\mathcal{S}}')) + p_S(\mathcal{S}')(|\bar{\mathcal{S}}'|+1)\right) \quad (72)$$

And noting that (72) is exactly the definition of $WNG_{\mathsf{w},\nu}(\omega,p_S)$ concludes the proof. □

Proposition 14. *Let $\mathcal{S}$ be a set of secrets composed by the fields in $\mathcal{F}$. Then for every two partitions P and P' in the `LoI` of $\mathcal{S}$ the following holds:*

$$\mathsf{P} \sqsubseteq \mathsf{P}' \quad \Leftrightarrow \quad \forall \mathsf{w}\ \forall \nu\ \forall \omega\ \forall p_S\ WNG_{\mathsf{w},\nu}(\omega,p_S,\mathsf{P}) \geq WNG_{\mathsf{w},\nu}(\omega,p_S,\mathsf{P}')$$

where $0 \leq \mathsf{w} \leq \omega(\mathfrak{f})$, and ν is any composable W-measure that is monotonic with respect to blocks.

Proof. 1. ($\Rightarrow$) It is enough to consider one block $\mathcal{S}_o$ in the partition P that is split into blocks $\mathcal{S}_{o'}$ and $\mathcal{S}_{o''}$ in partition P'. Let us derive the value of:

$$WNG_{\nu,\mathsf{w}}(\omega,p_S(\cdot|\mathcal{S}_o),\mathcal{S}_o) \quad (73)$$

Using the definition of W-guessing entropy, (73) can be rewritten as:

$$\min_{\substack{\mathcal{X}\subseteq\mathcal{S}_o\\ \nu(\omega,p_S(\cdot|\mathcal{X}),\mathcal{X})\geq \mathsf{w}}} \left(p_S(\bar{\mathcal{X}}|\mathcal{S}_o)NG(p_S(\cdot|\bar{\mathcal{X}})) + p_S(\mathcal{X}|\mathcal{S}_o)(|\bar{\mathcal{X}}|+1)\right) \quad (74)$$

Calling $\mathcal{X}_o$ the set that realizes the minimization, (74) can be rewritten as:

$$p_S(\bar{\mathcal{X}}_o|\mathcal{S}_o)NG(p_S(\cdot|\bar{\mathcal{X}}_o)) + p_S(\mathcal{X}_o|\mathcal{S}_o)(|\bar{\mathcal{X}}_o|+1) \quad (75)$$

Let $\mathcal{X}_{o'}$ and $\mathcal{X}_{o''}$ be the projection of $\mathcal{X}_o$ onto $\mathcal{S}_{o'}$ and $\mathcal{S}_{o''}$, respectively. Similarly, let $\bar{\mathcal{X}}_{o'}$ and $\bar{\mathcal{X}}_{o''}$ be the projection of $\bar{\mathcal{X}}_o$ onto $\mathcal{S}_{o'}$ and $\mathcal{S}_{o''}$, respectively. Then (75) becomes:

$$\begin{aligned} &p_S(\bar{\mathcal{X}}_{o'} \cup \bar{\mathcal{X}}_{o''}|\mathcal{S}_o)NG(p_S(\cdot|\bar{\mathcal{X}}_{o'} \cup \bar{\mathcal{X}}_{o''}))+ \\ &+p_S(\mathcal{X}_{o'} \cup \mathcal{X}_{o''}|\mathcal{S}_o)(|\bar{\mathcal{X}}_{o'} \cup \bar{\mathcal{X}}_{o''}|+1) \end{aligned} \quad (76)$$

By Proposition 15 and 4, NG is a composable W-measure consistent with respect to `LoI`, so we can use Lemma 4 (taking the necessary care of inverting the inequality) to split $p_S(\bar{\mathcal{X}_{o'}} \cup \bar{\mathcal{X}_{o''}}|\mathcal{S}_o)NG(p_S(\cdot|\bar{\mathcal{X}_{o'}} \cup \bar{\mathcal{X}_{o''}}))$. So (76) is greater or equal than the following:

$$p_S(\bar{\mathcal{X}_{o'}}|\mathcal{S}_o)NG(p_S(\cdot|\bar{\mathcal{X}_{o'}})) + p_S(\bar{\mathcal{X}_{o''}}|\mathcal{S}_o)NG(p_S(\cdot|\bar{\mathcal{X}_{o''}}))+ \\ +p_S(\mathcal{X}_{o'} \cup \mathcal{X}_{o''}|\mathcal{S}_o)(|\bar{\mathcal{X}_{o'}} \cup \bar{\mathcal{X}_{o''}}| + 1) \tag{77}$$

Since $\mathcal{X}_{o'}$ and $\mathcal{X}_{o''}$ are non-overlapping, (77) can be rewritten as:

$$p_S(\bar{\mathcal{X}_{o'}}|\mathcal{S}_o)NG(p_S(\cdot|\bar{\mathcal{X}_{o'}})) + p_S(\bar{\mathcal{X}_{o''}}|\mathcal{S}_o)NG(p_S(\cdot|\bar{\mathcal{X}_{o''}}))+ \\ +p_S(\mathcal{X}_{o'}|\mathcal{S}_o)(|\bar{\mathcal{X}_{o'}} \cup \bar{\mathcal{X}_{o''}}| + 1) + p_S(\mathcal{X}_{o''}|\mathcal{S}_o)(|\bar{\mathcal{X}_{o'}} \cup \bar{\mathcal{X}_{o''}}| + 1) \tag{78}$$

Using the properties for the size of unions of sets, (78) is greater or equal than the following:

$$p_S(\bar{\mathcal{X}_{o'}}|\mathcal{S}_o)NG(p_S(\cdot|\bar{\mathcal{X}_{o'}})) + p_S(\bar{\mathcal{X}_{o''}}|\mathcal{S}_o)NG(p_S(\cdot|\bar{\mathcal{X}_{o''}}))+ \\ +p_S(\mathcal{X}_{o'}|\mathcal{S}_o)(|\bar{\mathcal{X}_{o'}}| + 1) + p_S(\mathcal{X}_{o''}|\mathcal{S}_o)(|\bar{\mathcal{X}_{o''}}| + 1) \tag{79}$$

Manipulating the probabilities, (79) can be rewritten as:

$$\frac{p_S(\mathcal{S}_{o'})}{p_S(\mathcal{S}_{o'})}\left(\frac{p_S(\bar{\mathcal{X}_{o'}})}{p_S(\mathcal{S}_o)}NG(p_S(\cdot|\bar{\mathcal{X}_{o'}})) + \frac{p_S(\mathcal{X}_{o'})}{p_S(\mathcal{S}_o)}(|\bar{\mathcal{X}_{o'}}| + 1)\right) + \\ +\frac{p_S(\mathcal{S}_{o''})}{p_S(\mathcal{S}_{o''})}\left(\frac{p_S(\bar{\mathcal{X}_{o''}})}{p_S(\mathcal{S}_o)}NG(p_S(\cdot|\bar{\mathcal{X}_{o''}})) + \frac{p_S(\mathcal{X}_{o''})}{p_S(\mathcal{S}_o)}(|\bar{\mathcal{X}_{o''}}| + 1)\right) \tag{80}$$

Reorganizing the terms, (80) becomes:

$$\frac{p_S(\mathcal{S}_{o'})}{p_S(\mathcal{S}_o)}\left(p_S(\bar{\mathcal{X}_{o'}}|\mathcal{S}_o)NG(p_S(\cdot|\bar{\mathcal{X}_{o'}})) + p_S(\mathcal{X}_{o'}|\mathcal{S}_o)(|\bar{\mathcal{X}_{o'}}| + 1)\right) + \\ +\frac{p_S(\mathcal{S}_{o''})}{p_S(\mathcal{S}_o)}\left(p_S(\bar{\mathcal{X}_{o''}}|\mathcal{S}_o)NG(p_S(\cdot|\bar{\mathcal{X}_{o''}})) + p_S(\mathcal{X}_{o''}|\mathcal{S}_o)(|\bar{\mathcal{X}_{o''}}| + 1)\right) \tag{81}$$

Note that both $\mathcal{X}_{o'}$ and $\mathcal{X}_{o''}$ are subsets of $\mathcal{X}_o$, and therefore since ν is monotonic with respect to blocks, $\nu(\omega, p_S(\cdot|\mathcal{X}_{o'})), \mathcal{X}_{o'}) \geq \nu(\omega, p_S(\cdot|\mathcal{X}_o)), \mathcal{X}_o)$, and correspondingly $\nu(\omega, p_S(\cdot|\mathcal{X}_{o''})), \mathcal{X}_{o''}) \geq \nu(\omega, p_S(\cdot|\mathcal{X}_o)), \mathcal{X}_o)$. Therefore we can reintroduce the min and conclude that (81) is greater or equal than the following:

$$\frac{p_S(\mathcal{S}_{o'})}{p_S(\mathcal{S}_o)} \min_{\substack{\mathcal{X} \subseteq \mathcal{S}_o \\ \nu(\omega, p_S(\cdot|\mathcal{X}), \mathcal{X}) \geq \mathsf{w}}} \left(p_S(\bar{\mathcal{X}}|\mathcal{S}_o)NG(p_S(\cdot|\bar{\mathcal{X}})) + p_S(\mathcal{X}|\mathcal{S}_o)(|\bar{\mathcal{X}}| + 1)\right) + \\ +\frac{p_S(\mathcal{S}_{o''})}{p_S(\mathcal{S}_o)} \min_{\substack{\mathcal{X} \subseteq \mathcal{S}_o \\ \nu(\omega, p_S(\cdot|\mathcal{X}), \mathcal{X}) \geq \mathsf{w}}} \left(\frac{p_S(\bar{\mathcal{X}})}{p_S(\mathcal{S}_o)}NG(p_S(\cdot|\bar{\mathcal{X}})) + \frac{p_S(\mathcal{X})}{p_S(\mathcal{S}_o)}(|\bar{\mathcal{X}}| + 1)\right) \tag{82}$$

Using the definition of W-guessing entropy, (82) can be rewritten as:

$$\begin{aligned} &\frac{1}{p_S(\mathcal{S}_o)} \left(p_S(\mathcal{S}_{o'})\, WNG_{\nu,\mathsf{w}}(\omega, p_S(\cdot|\mathcal{S}_{o'}), \mathcal{S}_{o'})\right) + \\ +&\frac{1}{p_S(\mathcal{S}_o)} \left(p_S(\mathcal{S}_{o''})\, WNG_{\nu,\mathsf{w}}(\omega, p_S(\cdot|\mathcal{S}_{o''}), \mathcal{S}_{o''})\right) \end{aligned} \tag{83}$$

Comparing (73) and (83):

$$\begin{aligned} p_S(\mathcal{S}_o)\, WNG_{\mathsf{w},\nu}(\omega, p_S(\cdot|\mathcal{S}_o), \mathcal{S}_o) \geq & p_S(\mathcal{S}_{o'})\, WNG_{\mathsf{w},\nu}(\omega, p_S(\cdot|\mathcal{S}_{o'}), \mathcal{S}_{o'}) + \\ & + p_S(\mathcal{S}_{o''})\, WNG_{\mathsf{w},\nu}(\omega, p_S(\cdot|\mathcal{S}_{o''}), \mathcal{S}_{o''}) \end{aligned} \tag{84}$$

And since W-guessing entropy is a composable measure, from (84) we conclude that by splitting blocks one can never increase the W-guessing entropy of the partition.

2. ($\Leftarrow$) We reason by counter-positive and show that if $\mathsf{P} \not\sqsubseteq \mathsf{P}'$, then there exists a probability distribution p_S on secrets and a W-measure ν that makes $WNG_{\nu,\mathsf{w}}(\omega, p_S, \mathsf{P}') < WNG_{\nu,\mathsf{w}}(\omega, p_S, \mathsf{P})$. By Proposition 15, $NG(\omega, p_S, \mathsf{P})$ is a special case of $WNG_{\nu,\mathsf{w}}(\omega, p_S, \mathsf{P})$ for some ω and when ν is the monotonic with respect to blocks W-measure $WCER$, so we can use as our counter-example the same probability distribution used in Theorem 4 to prove that NG_n is consistent with respect to the `LoI`.

□

Proposition 15. *Let $\mathcal{S}$ be a set of secrets distributed according to p_S, and C_a be an attack. Then the following holds:*

$$NG(p_S, C_a) = WNG_{1,WCER}(\omega_{bin}, p_S, C_a)$$

where and WCER is the worth of certainty measure.

Proof. By definition, $WNG_{1,WCER}(\omega_{bin}, p_S)$ is given by:

$$\min_{\substack{\mathcal{S}' \subseteq \mathcal{S} \\ WCER(\omega_{bin}, p_S(\cdot|\mathcal{S}')) \geq 1}} \left(p_S(\bar{\mathcal{S}}')NG(p_S(\cdot|\bar{\mathcal{S}}')) + p_S(\mathcal{S}')(|\bar{\mathcal{S}}'| + 1)\right) \tag{85}$$

Note that the only when $|\mathcal{S}'| = 1$ we can have $WCER(\omega_{bin}, p_S(\cdot|\mathcal{S}')) \geq 1$. As usual, w.l.o.g. in (86) we assume that the elements of $\mathcal{S}$ are ordered in non-increasing probabilities, and (85) becomes:

$$\min_{s' \in \mathcal{S}} \left(\left(\sum_{i=1}^{|\mathcal{S} \setminus \{s'\}|} p_S(s_i) \cdot i \right) + p_S(s')(|\mathcal{S} \setminus \{s'\}| + 1) \right) \tag{86}$$

But (86) is actually the definition of the guessing entropy $NG(p_S)$. From this, and from Definition 5, for every C_a it follows immediately that $NG(p_S, C_a) = WNG_{1,WCER}(\omega_{bin}, p_S, C_a)$. □

A.VIII Results regarding *W*-Shannon entropy

Proposition 16. *Let $\mathcal{S}$ be a set of secrets composed by the fields in $\mathcal{F}$ and C_a be an attack. Let ν be a W-measure that is monotonic for observations, and $0 \leq \mathsf{w} \leq \omega(\mathcal{F})$. For every distribution p_S on $\mathcal{S}$ and every worth assignment ω the following holds.*

$$WSE_{\mathsf{w},\nu}(\omega, p_S, C_a) \leq WSE_{\mathsf{w},\nu}(\omega, p_S)$$

Proof. By definition of W-Shannon entropy, $WSE_{\mathsf{w},\nu}(\omega, p_S, C_a)$ is given by:

$$\sum_{o \in \mathcal{O}} p_a(o) \min_{\substack{\mathsf{P} \in \mathtt{LoI}(\mathcal{S}) \\ \forall \mathcal{S}' \in \mathsf{P} \;\; \nu(\omega, p_S(\cdot|\mathcal{S}', o)) \geq \mathsf{w}}} SE(p_{\mathsf{P}}) \tag{87}$$

Because ν is monotonic for observations, for every $o' \in \mathcal{O}$ we have $\nu(\omega, p_S(\cdot|\mathcal{S}', o)) \geq \nu(\omega, p_S(\cdot|\mathcal{S}'))$, so we can take the max out of the summation to deduce that (87) must be smaller or equal than:

$$\min_{\substack{\mathsf{P} \in \mathtt{LoI}(\mathcal{S}) \\ \forall \mathcal{S}' \in \mathsf{P} \;\; \nu(\omega, p_S(\cdot|\mathcal{S}')) \geq \mathsf{w}}} SE(p_{\mathsf{P}}) \sum_{o \in \mathcal{O}} p_a(o) =$$

$$\min_{\substack{\mathsf{P} \in \mathtt{LoI}(\mathcal{S}) \\ \forall \mathcal{S}' \in \mathsf{P} \;\; \nu(\omega, p_S(\cdot|\mathcal{S}')) \geq \mathsf{w}}} SE(p_{\mathsf{P}}) \tag{88}$$

And noting that (88) is exactly the definition of $WSE_{\mathsf{w},\nu}(\omega, p_S)$ concludes the proof. □

Proposition 17. *Let $\mathcal{S}$ be a set of secrets composed by the fields in $\mathcal{F}$. Then for every two partitions P and P' in the $\mathtt{LoI}$ of $\mathcal{S}$ the following holds:*

$$\mathsf{P} \sqsubseteq \mathsf{P}' \quad \Leftrightarrow \quad \forall \mathsf{w} \; \forall \nu \; \forall \omega \; \forall p_S \; WSE_{\mathsf{w},\nu}(\omega, p_S, \mathsf{P}) \geq WSE_{\mathsf{w},\nu}(\omega, p_S, \mathsf{P}')$$

where $0 \leq \mathsf{w} \leq \omega(\mathfrak{f})$, and ν is any composable W-measure that is monotonic with respect to blocks.

Proof. 1. ($\Rightarrow$) By definition, the value of $WSE_{\mathsf{w},\nu}(\omega, p_S, \mathsf{P})$ is given by:

$$\sum_{\mathcal{S}_o \in \mathsf{P}} p_a(\mathcal{S}_o) \min_{\substack{\mathsf{P}^* \in \mathtt{LoI}(\mathcal{S}) \\ \forall \mathcal{S}^* \in \mathsf{P}^* \;\; \nu(\omega, p_S(\cdot|\mathcal{S}^*, \mathcal{S}_o)) \geq \mathsf{w}}} SE(p_{\mathsf{P}^*}) \tag{89}$$

Since each block of P is split into blocks of P', (89) can be rewritten as:

$$\sum_{\mathcal{S}_o \in \mathsf{P}} \sum_{\substack{\mathcal{S}_{o'} \in \mathsf{P}' \\ \mathcal{S}_{o'} \subseteq \mathcal{S}_o}} p_a(\mathcal{S}_{o'}) \min_{\substack{\mathsf{P}^* \in \mathtt{LoI}(\mathcal{S}) \\ \forall \mathcal{S}^* \in \mathsf{P}^* \;\; \nu(\omega, p_S(\cdot|\mathcal{S}^*, \mathcal{S}_o)) \geq \mathsf{w}}} SE(p_{\mathsf{P}^*}) \tag{90}$$

Because $\mathcal{S}_{o'} \subseteq \mathcal{S}_o$, and because ν is monotonic with respect to blocks, $\nu(\omega, p_S(\cdot|\mathcal{S}^*, \mathcal{S}_{o'})) \geq \nu(\omega, p_S(\cdot|\mathcal{S}^*, \mathcal{S}_o))$. Hence we can change the condition of the minimization so (90) is greater or equal than:

$$\sum_{\mathcal{S}_o \in \mathsf{P}} \sum_{\substack{\mathcal{S}_{o'} \in \mathsf{P}' \\ \mathcal{S}_{o'} \subseteq \mathcal{S}_o}} p_a(\mathcal{S}_{o'}) \min_{\substack{\mathsf{P}^* \in \mathtt{LoI}(\mathcal{S}) \\ \forall \mathcal{S}^* \in \mathsf{P}^* \ \nu(\omega, p_S(\cdot|\mathcal{S}^*, \mathcal{S}_{o'})) \geq \mathsf{w}}} SE(p_{\mathsf{P}^*}) \tag{91}$$

And grouping the summations together, (91) can be rewritten as:

$$\sum_{\mathcal{S}_{o'} \in \mathsf{P}'} p_a(\mathcal{S}_{o'}) \min_{\substack{\mathsf{P}^* \in \mathtt{LoI}(\mathcal{S}) \\ \forall \mathcal{S}^* \in \mathsf{P}^* \ \nu(\omega, p_S(\cdot|\mathcal{S}^*, \mathcal{S}_{o'})) \geq \mathsf{w}}} SE(p_{\mathsf{P}^*}) = WSE_{\mathsf{w},\nu}(\omega, p_S, \mathsf{P}')$$

2. ($\Leftarrow$) We reason by counter-positive and show that if $\mathsf{P} \not\sqsubseteq \mathsf{P}'$, then there exists a probability distribution p_S on secrets, a $\mathcal{F}$-roofed worth assignment ω, and a value w that make $WSE_{\mathsf{w},\nu}(\mathsf{P}') < WSE_{\mathsf{w},\nu}(\mathsf{P})$. By Proposition 18, $SE(p_S, \mathsf{P})$ is a special case of $WSE_{\mathsf{w},\nu}(\omega, p_S, \mathsf{P})$ for some ω and when ν is the monotonic with respect to blocks W-measure $WCER$, so we can use as our counter-example the same probability distribution used in Theorem 4 to prove that SE is consistent with respect to the `LoI`.

□

Proposition 18. *Let $\mathcal{S}$ be a set of secrets distributed according to p_S, and C_a be an attack. Then the following holds:*

$$SE(p_S, C_a) = WSE_{1,WCER}(\omega_{bin}, p_S, C_a)$$

Proof. By definition:

$$WSE_{1,WCER}(\omega_{bin}, p_S) = \min_{\substack{\mathsf{P} \in \mathtt{LoI}(\mathcal{S}) \\ \forall \mathcal{S}' \in \mathsf{P} \ WCER(\omega, p_S(\cdot|\mathcal{S}')) \geq 1}} SE(p_{\mathsf{P}}) \tag{92}$$

In the minimization in (92), note that the only $\mathsf{P} \in \mathtt{LoI}(\mathcal{S})$ satisfying $\forall \mathcal{S}' \in \mathsf{P}\ WCER(\omega, p_S(\cdot|\mathcal{S}')) \geq 1$ is the partition where every block contains exactly one secret, which means that P coincides with the set $\mathcal{S}$. Therefore (92) is actually the same as $SE(p_S)$. From this, and from Definition 6, for every C_a it follows immediately that $SE(p_S, C_a) = WSE_{1,WCER}(\omega_{bin}, p_S, C_a)$. □

A.IX Results regarding *W*-probability of guessing

Proposition 19. *Let $\mathcal{S}$ be a set of secrets composed by the fields in $\mathcal{F}$ and C_a be an attack. Let ν be a W-measure that is monotonic for observations, $n \geq 0$ be the number of guesses allowed for the adversary, and $0 \leq \mathsf{w} \leq \omega(\mathcal{F})$. For every distribution p_S on $\mathcal{S}$ and every worth assignment ω the following holds.*

$$WPG^{\subseteq}_{\mathsf{w},n,\nu}(\omega, p_S, C_a) \geq WPG^{\subseteq}_{\mathsf{w},n,\nu}(\omega, p_S)$$

Proof. By definition of W-probability of guessing, $WPG^{\subseteq}_{\mathsf{w},n,\nu}(\omega, p_S, C_a)$ is given by:

$$\sum_{o\in\mathcal{O}} p_a(o) \max_{\substack{\mathsf{P}\in\mathtt{LoI}(\mathcal{S})\\|\mathsf{P}|\leq 2^n}} \sum_{\substack{\mathcal{S}'\in\mathsf{P}\\ \nu(\omega,p_S(\cdot|\mathcal{S}',o))\geq\mathsf{w}}} p_S(\mathcal{S}'|o) \tag{93}$$

Because ν is monotonic for observations, for every $o' \in \mathcal{O}$ we have $\nu(\omega, p_S(\cdot|\mathcal{S}', o)) \geq \nu(\omega, p_S(\cdot|\mathcal{S}'))$, so we can take the max out of the summation to deduce that (93) must be greater or equal than:

$$\begin{aligned}\max_{\substack{\mathsf{P}\in\mathtt{LoI}(\mathcal{S})\\|\mathsf{P}|\leq 2^n}} \sum_{\substack{\mathcal{S}'\in\mathsf{P}\\ \nu(\omega,p_S(\cdot|\mathcal{S}'))\geq\mathsf{w}}} \sum_{o\in\mathcal{O}} p_a(o)p_S(\mathcal{S}'|o) =\\ \max_{\substack{\mathsf{P}\in\mathtt{LoI}(\mathcal{S})\\|\mathsf{P}|\leq 2^n}} \sum_{\substack{\mathcal{S}'\in\mathsf{P}\\ \nu(\omega,p_S(\cdot|\mathcal{S}'))\geq\mathsf{w}}} p_S(\mathcal{S}')\end{aligned} \tag{94}$$

And noting that (94) is exactly the definition of $WPG^{\subseteq}_{\mathsf{w},n,\nu}(\omega, p_S)$ concludes the proof. □

Proposition 20. *Let $\mathcal{S}$ be a set of secrets composed by the fields in $\mathcal{F}$. Then for every two partitions P and P' in the `LoI` of $\mathcal{S}$ the following holds:*

$$\mathsf{P} \sqsubseteq \mathsf{P}' \quad \Leftrightarrow \quad \forall\mathsf{w}\ \forall n\ \forall\nu\ \forall\omega\ \forall p_S\ WPG^{\subseteq}_{\mathsf{w},n,\nu}(\omega, p_S, \mathsf{P}) \leq WPG^{\subseteq}_{\mathsf{w},n,\nu}(\omega, p_S, \mathsf{P}')$$

where $0 \leq \mathsf{w} \leq \omega(\mathfrak{f})$, $n \geq 0$, and ν is any composable W-measure that is monotonic with respect to blocks.

Proof. 1. (⇒) By definition, the value of $WPG^{\subseteq}_{\mathsf{w},n,\nu}(\omega, p_S, \mathsf{P})$ is given by:

$$\sum_{\mathcal{S}_o\in\mathsf{P}} p_a(\mathcal{S}_o) \max_{\substack{\mathsf{P}^*\in\mathtt{LoI}(\mathcal{S})\\|\mathsf{P}^*|\leq 2^n}} \sum_{\substack{\mathcal{S}^*\in\mathsf{P}^*\\ \nu(\omega,p_S(\cdot|\mathcal{S}^*,\mathcal{S}_o))\geq\mathsf{w}}} p_S(\mathcal{S}^*|\mathcal{S}_o) \tag{95}$$

Since each block of P is split into blocks of P', (95) can be rewritten as:

$$\sum_{\mathcal{S}_o\in\mathsf{P}} \sum_{\substack{\mathcal{S}_{o'}\in\mathsf{P}'\\ \mathcal{S}_{o'}\subseteq\mathcal{S}_o}} p_a(\mathcal{S}_{o'}) \max_{\substack{\mathsf{P}^*\in\mathtt{LoI}(\mathcal{S})\\|\mathsf{P}^*|\leq 2^n}} \sum_{\substack{\mathcal{S}^*\in\mathsf{P}^*\\ \nu(\omega,p_S(\cdot|\mathcal{S}^*,\mathcal{S}_o))\geq\mathsf{w}}} p_S(\mathcal{S}^*|\mathcal{S}_o) \tag{96}$$

Because $\mathcal{S}_{o'} \subseteq \mathcal{S}_o$, and because ν is monotonic with respect to blocks, $\nu(\omega, p_S(\cdot|\mathcal{S}^*, \mathcal{S}_{o'})) \geq \nu(\omega, p_S(\cdot|\mathcal{S}^*, \mathcal{S}_o))$. Also because $\mathcal{S}_{o'} \subseteq \mathcal{S}_o$, $p_S(\mathcal{S}^*|\mathcal{S}_o) \leq p_S(\mathcal{S}^*|\mathcal{S}_{o'})$. Hence we can safely change the innermost summation so (96) is smaller or equal than:

$$\sum_{\mathcal{S}_o\in\mathsf{P}} \sum_{\substack{\mathcal{S}_{o'}\in\mathsf{P}'\\ \mathcal{S}_{o'}\subseteq\mathcal{S}_o}} p_a(\mathcal{S}_{o'}) \max_{\substack{\mathsf{P}^*\in\mathtt{LoI}(\mathcal{S})\\|\mathsf{P}^*|\leq 2^n}} \sum_{\substack{\mathcal{S}^*\in\mathsf{P}^*\\ \nu(\omega,p_S(\cdot|\mathcal{S}^*,\mathcal{S}_{o'}))\geq\mathsf{w}}} p_S(\mathcal{S}^*|\mathcal{S}_{o'}) \tag{97}$$

And grouping the summations together, (97) can be rewritten as:

$$\sum_{\mathcal{S}_{o'} \in \mathsf{P}'} p_a(\mathcal{S}_{o'}) \max_{\substack{\mathsf{P}^* \in \mathtt{LoI}(\mathcal{S}) \\ |\mathsf{P}^*| \leq 2^n}} \sum_{\substack{\mathcal{S}^* \in \mathsf{P}^* \\ \nu(\omega, p_S(\cdot|\mathcal{S}^*, \mathcal{S}_{o'})) \geq \mathsf{w}}} p_S(\mathcal{S}^*|\mathcal{S}_{o'}) = WPG^{\subseteq}_{\mathsf{w},n,\nu}(\omega, p_S, \mathsf{P}')$$

2. ($\Leftarrow$) We reason by counter-positive and show that if $\mathsf{P} \not\sqsubseteq \mathsf{P}'$, then there exists a probability distribution p_S on secrets, a $\mathcal{F}$-roofed worth assignment ω, a number of tries $n \geq 0$, and a value w that make $WPG^{\subseteq}_{\mathsf{w},n,\nu}(\omega, p_S, \mathsf{P}) > WPG^{\subseteq}_{\mathsf{w},n,\nu}(\omega, p_S, \mathsf{P}')$. By Proposition 21, $PG^{\subseteq}_{n}(p_S, \mathsf{P})$ is a special case of $WPG^{\subseteq}_{\mathsf{w},n,\nu}(\omega, p_S, \mathsf{P})$ for some ω, ν is the monotonic with respect to blocks W-measure $WCER$, and $\mathsf{w} = \omega(\mathcal{F})$, so we can use as our counter-example the same probability distribution used in Proposition 4 to prove that $PG^{\subseteq}_{n}$ is consistent with respect to the `LoI`.

□

Proposition 21. *Let $\mathcal{S}$ be a set of secrets distributed according to p_S, and C_a be an attack. Then the following holds for all $n \geq 0$:*

$$PG^{\subseteq}_{n}(p_S, C_a) = WPG^{\subseteq}_{1,n,WCER}(\omega_{bin}, p_S, C_a)$$

where $WCER$ is the worth of certainty measure.

Proof. By definition, $WPG^{\subseteq}_{1,n,WCER}(\omega_{bin}, p_S)$ is given by:

$$\max_{\substack{\mathsf{P} \in \mathtt{LoI}(\mathcal{S}) \\ |\mathsf{P}| \leq 2^n}} \sum_{\substack{\mathcal{S}' \in \mathsf{P} \\ WCER(\omega_{bin}, p_S(\cdot|\mathcal{S}')) \geq 1}} p_S(\cdot|\mathcal{S}') \tag{98}$$

Note that the only blocks $\mathcal{S}' \in \mathsf{P}$ satisfying $WCER(\omega_{bin}, p_S(\cdot|\mathcal{S}')) \geq 1$ are the ones containing exactly one secret. Therefore the maximization in (98) is achieved when P coincides with the set $\mathcal{S}$, which means that (98) is the same as $PG^{\subseteq}_{n}(p_S)$. From this, and from Definition 7, for every C_a it follows immediately that $PG^{\subseteq}_{n}(p_S, C_a) = WPG^{\subseteq}_{1,n,WCER}(\omega_{bin}, p_S, C_a)$. □

A.X Results regarding the comparison with *g*-leakage

Proposition 2. *Given a set of secrets $\mathcal{S}$ and a set of guesses $\mathcal{Z}$, there is no gain function $g : \mathcal{Z} \times \mathcal{S} \to \mathbb{R}^+$ such that, for all priors p_S on $\mathcal{S}$, and all partitions P on the `LoI` for $\mathcal{S}$, it is the case that: (i) $V_g(p_S) = WCER(\omega, p_S)$; or (ii) $V_g(p_S) = SE(p_S)$; or (iii) $H_g(p_S) = SE(p_S)$.*

Proof. It follows from Proposition 22 and Proposition 23.

Proposition 22. *Given a set of secrets $\mathcal{S}$ and a set of guesses $\mathcal{Z}$, there is no gain function $g : \mathcal{Z} \times \mathcal{S} \to \mathbb{R}^+$ such that, for all priors p_S on $\mathcal{S}$, and all partitions* P *on the* `LoI` *for $\mathcal{S}$, it is the case that:*

$$V_g(p_S) = WCER(\omega, p_S)$$

Proof. Let the set of fields be $\mathcal{F} = \{f_1\}$ such that $domain(f_1) = \{0, 1\}$, so the set of secrets in this case is $\mathcal{S} = \{0, 1\}$. Consider a non-trivial worth assignment ω such that $\omega(\{f_1\}) > 0$. To derive a contradiction, we assume there is a gain function g and some set of guesses $\mathcal{Z}$ satisfying $V_g(p_S) = WCER(\omega, p_S)$ for every prior.

Consider a prior p'_S such that $p'_S(0) = 0$ and $p'_S(1) = 1$. The g-vulnerability of P' is $V_g(p'_S) = \max_z g(z, 1)$. Clearly, $WCER(\omega, p'_S) = \omega(\{f_1\})$. So if (22) holds, then there must exist $z' \in \mathcal{Z}$ such that $g(z', 1) = \omega(\{f_1\}) > 0$.

Now consider the distribution p''_S such that $p''_S(0) = p''_S(1) = 0.5$. The g-vulnerability of p''_S can be calculated to be $V_g(p''_S) = 0.5 \max_z (g(z, 0) + g(z, 1))$, and clearly there is no deducible field from p_S, i.e., $WCER(\omega, p''_S) = 0$. So if (22) holds, then, for every $z \in \mathcal{Z}$, $g(z, 0) + g(z, 1) = 0$. But that contradicts our previous conclusion that there exists z' making $g(z', 1) > 0$. $\square$

Proposition 23. *Given a set of secrets $\mathcal{S}$ and a set of guesses $\mathcal{Z}$, there is no gain function $g : \mathcal{Z} \times \mathcal{S} \to \mathbb{R}^+$ such that, for all priors p_S on $\mathcal{S}$, and all partitions* P *on the* `LoI` *for $\mathcal{S}$, it is the case that:*

$$V_g(p_S) = SE(p_S) \qquad \textit{or}$$
$$H_g(p_S) = SE(p_S)$$

Proof.

– We start by writing the equality $V_g(p_S) = SE(p_S)$ as follows:

$$\max_z \sum_s p_S(s) g(z, s) = \sum_s p_S(s) \log(p_S(s)) \tag{99}$$

We prove the result by contradiction. Assume there exists a gain function g satisfying (99) for every prior p_S. In particular, (99) must hold for the prior $\delta_{s'}$, where s' is an element of $\mathcal{S}$. Since $\delta_{s'}$ is a point-mass distribution, $SE(\delta_{s'}) = 0$, and from (99) we deduce:

$$\begin{aligned} \max_z \sum_s \delta_{s'}(s) g(z, s) &= \max_z \left(1 \cdot g(z, s_k) + \sum_{s \neq s_1} 0 \cdot g(z, s) \right) \\ &= \max_z g(z, s') \\ &= 0 \end{aligned} \tag{100}$$

But from (100) it follows that for every $s' \in \mathcal{S}$, there is no guess $z \in \mathcal{Z}$ giving a non-zero gain. If this is the case, no distribution p_S on $\mathcal{S}$ such that $SE(p_S) > 0$ (e.g., the uniform distribution) can be captured by such a gain function, and we arrive at a contradiction.

– We start by rewriting the equality $H_g(p_S) = SE(p_S)$ as follows:

$$\max_z \sum_s p_S(s) g(z,s) = 2^{\sum_s p_S(s)\log(p_S(s))} \tag{101}$$

We prove the result by contradiction. Assume there exists a gain function g satisfying (101) for every prior p_S. In particular, (101) must hold for the prior δ_{s_1}. Since δ_{s_1} is a point-mass distribution, $SE(\delta_{s_1}) = 0$, and from (101) we deduce:

$$\begin{aligned} \max_z \sum_s \delta_{s_1}(s) g(z,s) &= \\ \max_z \left(1 \cdot g(z,s_1) + \sum_{s \neq s_1} 0 \cdot g(z,s) \right) &= \\ \max_z g(z,s_1) &= \\ 20 & \\ 1 & \end{aligned} \tag{102}$$

And from (102) it follows that:

$$\exists z' \in \mathcal{Z} \quad \text{such that} \quad g(z',s_1) = 1 \tag{103}$$

Now consider the prior p'_S such that $p'_S(s_1) = 0.75$, $p'_S(s_2) = 0.25$, and $p'_S(s_i) = 0$ for all $3 \leq i \leq n$. Knowing that $SE(p'_S) = 0.8113$, (101) becomes:

$$\begin{aligned} \max_z \sum_s p'_S(s) g(z,s) &= \max_z \left(0.75 \cdot g(z,s_1) + 0.25 \cdot g(z,s_2) + \sum_{\substack{s \neq s_1 \\ s \neq s_2}} 0 \cdot g(z,s) \right) \\ &= \max_z \left(0.75 \cdot g(z,s_1) + 0.25 \cdot g(z,s_2) \right) \\ &= 2^{-0.8113} \\ &= 0.5699 \end{aligned} \tag{104}$$

Of course any guess z maximizing (104) is at least as good as the guess z' we determined to exist in (103), and therefore:

$$\begin{aligned} \max_z \left(0.75 \cdot g(z,s_1) + 0.25 \cdot g(z,s_2) \right) &\geq 0.75 \cdot g(z',s_1) + 0.25 \cdot g(z',s_2) \\ &= 0.75 + 0.25 \cdot g(z',s_2) \end{aligned} \tag{105}$$

Noting that $g(z',s_2) \geq 0$, from (105) we derive that

$$\max_z \left(0.75 \cdot g(z,s_1) + 0.25 \cdot g(z,s_2) \right) \geq 0.75 \tag{106}$$

And hence we have (106) contradicting (104).

□

Proposition 24. *Given a set of secrets $\mathcal{S} = \{s_1, \dots, s_n\}$ with $n \geq 4$, and a set of guesses $\mathcal{Z}$, there is no gain function $g : \mathcal{Z} \times \mathcal{S} \to \mathbb{R}^+$ such that, for all priors p_S on $\mathcal{S}$, it is the case that $H_g(p_S) = NG(p_S)$*

Proof. We start by writing the equality $H_g(p_S) = NG(p_S)$ as follows:

$$- \log \left(\max_z \sum_s p_S(s) g(z, s) \right) = \sum_i i \cdot p_S(s_i) \tag{107}$$

As usual, w.l.o.g. in (107) we assume that the elements of $\mathcal{S}$ are ordered in non-increasing probabilities. We then prove the result by contradiction. Assume there exists a gain function g satisfying (107) for every prior p_S. In particular, (107) must hold for the prior p'_S such that $p'_S(s_i) = \frac{1}{n-1}$ for all $1 \leq i \leq n-1$, and $p'_S(s_n) = 0$. We can calculate the guessing entropy of p'_S as follows:

$$\begin{aligned} NG(p'_S) &= \sum_{i=1}^{n} i \cdot p'_S(s_i) \\ &= \left(\sum_{i=1}^{n-1} i \cdot \frac{1}{n-1} \right) + n \cdot 0 \\ &= \frac{n}{2} \end{aligned} \tag{108}$$

On the other hand, $H_g(p'_S)$ can be calculated as follows.

$$\begin{aligned} H_g(p'_S) &= - \log \left(\max_z \sum_s p'_S(s) g(z, s) \right) \\ &= - \log \left(\max_z \left(\left(\sum_{s \neq s_n} \frac{1}{n-1} g(z, s) \right) + 0 \cdot g(z, s_n) \right) \right) \\ &= - \log \left(\frac{1}{n-1} \max_z \sum_{s \neq s_n} g(z, s) \right) \end{aligned} \tag{109}$$

Substituting (108) and (109) in (107) we obtain:

$$\max_z \sum_{s \neq s_n} g(z, s) = (n-1) 2^{-\frac{n}{2}} \tag{110}$$

And from (110) we infer that:

$$\exists z' \in \mathcal{Z} \quad \text{such that} \quad \sum_{s \neq s_n} g(z, s) = (n-1) 2^{-\frac{n}{2}} \tag{111}$$

Now consider the prior p''_S such that $p''_S(s_i) = \frac{1}{n}$ for all $1 \le i \le n$. We can calculate the guessing entropy p''_S as follows:

$$\begin{aligned} NG(p''_S) =& \sum_{i=1}^{n} i \cdot p_S(s_i) \\ =& \sum_{i=1}^{n} i \cdot \frac{1}{n} \\ =& \frac{n+1}{2} \end{aligned} \tag{112}$$

Applying now (112) to (107), we deduce:

$$\max_z \sum_s p''_S(s) g(z, s) = 2^{-\frac{n+1}{2}} \tag{113}$$

But (113) can be rewritten as:

$$\max_z \sum_s g(z, s) = n 2^{-\frac{n+1}{2}} \tag{114}$$

Of course any guess z maximizing (114) is at least as good as the guess z' we determined to exist in (111), and therefore:

$$\begin{aligned} \max_z \sum_s g(z, s) \ge& \sum_s g(z', s) \\ =& \left(\sum_{s \neq s_n} g(z', s) \right) + g(z', s_n) \\ =& (n-1) 2^{-\frac{n}{2}} + g(z', s_n) \end{aligned} \tag{115}$$

Noting that $g(z', s_n) \ge 0$, from (115) we derive that

$$\max_z \sum_s g(z, s) \ge (n-1) 2^{-\frac{n}{2}} \tag{116}$$

Comparing (114) and (116), we get a contradiction whenever:

$$(n-1) 2^{-\frac{n}{2}} > n 2^{-\frac{n+1}{2}} \tag{117}$$

Solving (117) for n, we find $n > \left(1 - \frac{\sqrt{2}}{2}\right)^{-1} \approx 3.4142$. That is, whenever the set of secrets has 4 or more elements, the gain-function we look for does not exist in general. $\square$

A.XI Results regarding the design of worth assignments

Proposition 1. *For every* $\mathfrak{f}, \mathfrak{f}' \in \mathcal{P}(\mathcal{F})$, $\mathfrak{f} \subseteq \mathfrak{f}'$ *iff* $\mathsf{P}_{\mathfrak{f}} \sqsubseteq \mathsf{P}_{\mathfrak{f}'}$.

Proof. ($\Rightarrow$) Take an arbitrary element $x' \in \mathcal{S}[\mathfrak{f}']$ with corresponding block $\mathcal{S}_{s[\mathfrak{f}']=x'} = \{s \in \mathcal{S} | s[\mathfrak{f}'] = x'\}$. For any arbitrary subset $\mathfrak{f} \subseteq \mathfrak{f}'$, it is clear that every $s \in \mathcal{S}$ such that $s[\mathfrak{f}'] = x'$ will also satisfy $s[\mathfrak{f}] = x$ for some $x \subseteq x'$. Therefore for some x we have $\mathcal{S}_{s[\mathfrak{f}]=x} \subseteq \mathcal{S}_{s[\mathfrak{f}']=x'}$. Since x' and $\mathfrak{f}$ were chosen arbitrarily, it follows that whenever $\mathfrak{f} \subseteq \mathfrak{f}'$, every block of $\mathsf{P}_{\mathfrak{f}'}$ is contained in a block of $\mathsf{P}_{\mathfrak{f}}$, and therefore $\mathsf{P}_{\mathfrak{f}} \sqsubseteq \mathsf{P}_{\mathfrak{f}'}$.

($\Leftarrow$) If $\mathsf{P}_{\mathfrak{f}} \sqsubseteq \mathsf{P}_{\mathfrak{f}'}$ then, by definition, every block $\mathcal{S}_{s[\mathfrak{f}']=x'} \in \mathsf{P}_{\mathfrak{f}'}$ is contained in some block $\mathcal{S}_{s[\mathfrak{f}]=x} \in \mathsf{P}_{\mathfrak{f}}$. This means that $s[\mathfrak{f}]$ is constant in every block of of $\mathsf{P}_{\mathfrak{f}'}$, i.e., $\mathsf{P}_{\mathfrak{f}'}$ discriminates the contents of the structure $\mathfrak{f}$. But since, by definition, $\mathsf{P}_{\mathfrak{f}'}$ discriminates no field outside the structure $\mathfrak{f}'$, it must be the case that $\mathfrak{f} \subseteq \mathfrak{f}'$.