ABSTRACT
The globalization of collaboration in engineering design has raised several new concerns regarding information sharing. In particular, data shared during collaboration has the potential to leak private information through inferences that may be made by another collaborator. Enterprises that must keep certain information confidential, fearing loss of intellectual property, may turn down potential collaborations that would otherwise be mutually beneficial. Thus, there is need for a method to study this tradeoff between confidentiality and value in engineering collaboration. In this paper, a framework for analyzing this tradeoff is proposed, along with an illustrative example of a possible implementation and its effects on the collaborative design process. This framework estimates and quantifies the confidentiality loss and value gain associated with information revelation during design iterations. We believe that such analysis would aid designers in making better decisions about sharing information with their collaborators. Studying this tradeoff may incentivize designers to engage in more frequent, and more secure, collaboration.

1 INTRODUCTION
Information age technologies have provided enormous opportunity to transform designs into digital data, and have also enabled various ways of sharing that data with other designers, especially within a single enterprise. The transparency about the data shared allow every participant to provide their best possible solutions towards achieving mutually agreed-upon objectives. Such approaches provide the best possible utility of every participant’s information. This traditional method of open sharing has been very effective among collaborators within a single enterprise.

Modern products, such as cars and aircrafts, have become complex in nature. Designing such products requires domain knowledge experts to collaborate with each other. It is unlikely that all the required experts will be within a single organization. Hence, original equipment manufacturers (OEMs) designing these products must rely on design collaborations crossing national and enterprise boundaries.

With globalization, companies face increasingly stiff competition, and many companies have adopted outsourcing in order to reduce the time taken to develop a product. These outsourcing collaborations demand information flow across national and/or enterprise boundaries. In such collaborations, designer(s) typically face barriers to sharing information due to several reasons, such as government regulations and the need for intellectual property protection. There is a growing concern among enterprises: how secure is my confidential data in a collaboration? Companies are hesitant to utilize open sharing of information with collaborators for various reasons. A few of them are listed below:

1. Confidential information can reach competitor(s) through a
common collaborator. For example, Bosch is a common supplier to both Audi and BMW, and may pass information from one OEM to another.

2. Collaborators can become competitors. For example, Samsung became a competitor to Apple in many markets.

In the early stages of forming a collaborative design team, collaborators need to share critical and confidential information with each other even though they are not sure about whether they will be part of the collaboration. Sometimes, this information sharing is necessary in order to determine the abilities/expectations of a prospective participant or lead collaborator. This is a catch-22 situation for a collaborator; any information revealed at this stage may be leaked to competitors (say by a rejected participant), but may be necessary to determine if the collaboration will be successful. Thus, confidentiality plays a major role in collaboration. This has created a need to address such barriers, so that designers can still engage in meaningful collaboration and make better designs.

One approach to secure information is to use masking techniques, such as generalization and suppression, on confidential information before sharing. These techniques help collaborators to protect their confidential information while sharing by increasing the uncertainty associated with the information shared. This helps in maintaining confidentiality, but this uncertainty can lead to inferior design solutions as compared to open sharing. Other techniques involve legal agreements, such as non-disclosure agreements (NDA’s), but these methods do not prevent collaborators from attaining the information, and provide very limited purpose control to the original data owner once the agreement is signed.

Sharing of information may have both positive and negative impacts. While these impacts have been studied in supply-chains, there is a lack of understanding of this trade-off in the context of collaborative engineering design. The objectives of this paper are two-fold. First, we discuss the implication of information security in collaborative design. Second, we propose a framework to help designers in determining value gained versus confidentiality lost given potential information to be shared in a collaborative design process, and demonstrate its use with an example.

The rest of the paper is structured as follows. Section 2 provides an overview of state-of-the-art information sharing techniques and highlights the need to help designers in making decisions about revealing information during the design process. Section 3 introduces the proposed framework for studying the value/confidentiality trade-off in collaborative design. We describe the application of this framework in Section 4 and demonstrate its use with an example in Section 5. Section 6 discusses the potential future extensions of this work.

1There can be applications where confidentiality is not valued in design. For example, collaborations exist in open source environments. We acknowledge this and we agree that our paper is addressed to applications where confidentiality is valued.

2 LITERATURE REVIEW

In this section, current approaches to addressing the confidentiality/value trade-off in design are presented, with their motivations, virtues, and drawbacks. The goal of this section is to present a targeted survey of work relevant to confidentiality and value in engineering design, which motivates the work presented in following sections. In particular, methods including cryptography, access and inference control, and generalization are discussed, as well as the concept of entropy as an information security measure in collaboration. This measure will be explored throughout the paper.

2.1 Computer Science and Information Security

The concept of information security is well understood in the field of computer science. The domain of security in computer science encompasses topics such as confidentiality, integrity, availability and accountability. Confidentiality implies that information is accessible to authorized participant(s) among the participants in a collaboration. Integrity guarantees that design information is immune to intentional or accidental modifications by a non-data owner. Availability implies uninterrupted access to information for an authorized participant. Accountability enables keeping track of the modifications done on a particular parameter. In this paper, we consider only the exchange of information between collaborating designers, and do not consider attacks on a collaborator’s information or loss of availability. Thus, we focus on confidentiality of information only, and how this may be related to the value of revealing information.

Multi-party computations are very common in collaborations. In the field of cryptography, this form of computation is well studied. Techniques such as fully homomorphic evaluation, and circuit evaluation protocols maintain complete confidentiality, but are complex and time-intensive. Thus, further study into such computations, especially in early design stages which are inherently iterative in nature and involve uncertainty in the selection of design parameters, is needed. In this paper, we focus on the trade-off between value of information to a design process and the loss of confidentiality through revelation, and not these existing protocols.

2.2 Security in Collaborative Design

Recent work on collaborative engineering design focuses on two key areas: (i) enabling collaboration between geographically distant designers, often through the ‘cloud’ or on some other problem-specific platform, and (ii) securing the information passed between collaborators. For the second area in particular, research in computer science, information theory and cybersecurity has made tremendous progress in protecting collaborators’ information from outside attackers.

When sharing data or other information, designers often wish to protect some data from their collaborators. When sharing/protecting information on, say, parameters in a model, the common approaches used: (i) access control and (ii) inference control. In access control, one designer simply denies ac-
cess to certain information for one or more collaborators. Typically, this option is built into collaboration platforms, such as CAD platforms allowing sharing in neutral file formats such as .IGES [6]. Designers can also refuse to share certain information, requiring collaborators to rely on prior information and experience to form estimations, unless their role in the design process requires that information [17]. In inference control, designers actively seek ‘safe’ information to reveal to collaborators; such information limits what can be learned about his or her sensitive information when made public. In engineering design, models are typically physics-based and often provide clear mathematical dependencies that may be exploited to gain more information on a hidden parameter [2,6]. When one parameter is revealed, these dependencies may be used to learn more about another parameter; these inferences are actively sought out and prevented using inference controlling security measures. These issues have been studied in an engineering context primarily with supply chains.

2.3 Information Sharing in Supply Chains

The issue of confidentiality preservation has been a recent topic of investigation in supply chain management. As examples, recent focus areas include protection of intellectual property in supply chains [18] and research into secure supply chain collaboration and risks inherent in sharing product information [19,20]. Zhang and coauthors quantify the risk of leaking design parameters during supply chain collaboration using Bayesian statistics [6], providing a conceptual framework for modeling the security risk associated with sharing design parameters. In Zhang’s work, it is assumed that the manufacturer has control over all parameters in the design, and that the design is already finalized or close to being finalized. The manufacturer must consider the effects of revealing information on one parameter to a supplier on the supplier’s knowledge of other parameters. Wang and coauthors have developed protocols allowing for convergence to an optimal solution when there are relatively few design parameters and mathematical system models are of high fidelity and commonly known [13].

In design, and especially in early collaborative design, confidentiality preservation is also crucial. In particular, design information leakage [6,13,18] during design iterations, where information may be exchanged frequently with varying confidentiality risk and value gain, is of interest. When information is exchanged, some confidentiality may be preserved using methods such as suppression and generalization.

2.4 Suppression and Generalization

Suppression and generalization primarily relate to database publishing, rather than releases of individual parameter values. Suppression involves removing some elements of the database completely, while generalization involves replacing values in the database with corresponding ranges (\(x = 20\) becomes \(x \in [0, 30]\), for example) [11]. The goal is to prevent a user from identifying particular entries in a database (such as a particular person with some disease in a medical database) while still being able to perform meaningful statistical calculations.

As an example, suppression and generalization are common practice when releasing sensitive census or medical data. Consider for instance that regulations require individual entries in a health database to be obscured [11,21]. Thus, the publisher must ensure that any user accessing the database cannot identify a particular member of the dataset by studying the relationships between data values. In engineering, a designer sharing a parameter-free .STEP file, and not the fully parametrized version containing fine dimension data, is an example of suppression, while sharing datasets with common ranges instead of the exact values being used is an example of generalization.

Suppression and generalization have widespread applications in database sharing, and has motivated a large body of research. In particular, \(k\)-anonymity forms the basis of most practical database sharing methods [11]. The \(k\)-anonymity approach involves using suppression and/or generalization to statistically ensure that the modified database may, at most, allow a user to identify a group of size \(k\) by studying the data. Thus, any member of the database is assured that there are at least \((k - 1)\) other members that would look identical to an attacker.

This method quickly becomes less useful, and eventually useless, as datasets increase in dimension (this is described as the ‘curse of dimensionality’ in literature [21]), or as the attacker’s prior information over members of the dataset increases. \(L\)-diversity, which involves ensuring anonymity between groups in the dataset, addresses some of this concern but also fails with high-dimensional datasets or well-informed attackers [21]. In the context of collaborative design, such an attacker may be a collaborator interested in learning more about a competitor’s design or business model by studying such a dataset. Still, generalization and suppression are valuable to designers trying to communicate broad information for low-dimensional problems.

2.5 Research Gaps

We wish to analyze confidentiality and value of private information during a collaboration, especially in early design. Hence, the work discussed in this section is relevant but cannot be directly deployed.

Existing work in computer science does not focus on the study of inference during collaboration, and current methods may be difficult to implement and may be too time-intensive to be used during design iterations. Existing literature in supply chain management does not address the quantification of confidentiality lost in iterative collaborative design as information is shared during the early design process, nor does it address the quantification of value gained by sharing certain information as a balance to security lost. This trade-off, especially applied to early design where parameters may change rapidly, has not been studied, nor has the effect of sequential revelations throughout multiple design stages.

This trade-off may also be considered from the perspective of a non-cooperative game between collaborators involved in decentralized design scenarios. There is an established interest in
investigating the applications of game theory and related fields in collaborative design, going back to Vincent [22]. Interactions between such collaborators have been investigated from the perspective of game theory [23], as well as the evolution of collaborative decisions [24][25]. Evaluation from the perspective of the value/confidentiality trade-off, however, has not been addressed.

In this paper, the primary interest is in protecting information held by one collaborator from the other collaborators, while at the same time studying the value some information revelation may have in the collaboration effort. In many design scenarios, and especially in early design, collaborators may wish to protect some of their information or knowledge from each other, knowing that today’s collaborator is tomorrow’s competitor. In some cases, one party may not even be confident in the feasibility of a collaboration, and wishes to protect sensitive information until that feasibility is established. The challenge addressed here is revealing just enough information to ensure usefulness without too large a compromise in confidentiality.

If uncertainty regarding parameters or other design information is modeled using random variables with probability density functions representing the current state of knowledge possessed by a collaborator, the risk of sharing some information due to inferencing may be quantified using methods like Kullback-Leibler Divergence or differential entropy, discussed later. This form of analysis has been the focus of some study [6][19] and is explored later in the following sections. In Section 3, we establish the general framework followed for the remainder of this paper.

3 FRAMEWORK FOR ANALYZING THE IMPACT OF INFORMATION SHARING IN COLLABORATIVE DESIGN

Collaborative design processes may have more than one objective to be met. A common approach is to partition the design process into stages. Stages can be targeted towards different "Design for X" (DFX) activities, where X may be manufacturing, feasibility, environment, etc. Each stage involves designers working towards a design goal. At each stage, the responsible designers are assigned a specific task towards meeting the objective in that stage.

These design processes involve exchanges of information, and most of the existing processes encourage open sharing among collaborators to get the best possible solutions from the collaboration. However, some of these information exchanges may involve confidential information. Moreover, these information exchanges may be iterative in nature, with compounding effects. Thus, there is a need to analyze information leakage associated with these exchanges. In this section, we establish a generalized framework for examining such information exchanges during a design process.

![FIGURE 1. Participant’s state of knowledge ($K_{(p,i)}$) vs information exchanges](image-url)

3.1 A Model for Collaborative Design

Collaborative design involves participants working with parameters and the relationships between parameters. While designing, parameters/relationships may vary or remain constant throughout the design process. Parameters are numerical in nature, whereas relationships can be numerical, logical, relational, or arithmetic. Every participant in a collaboration works with a certain set of parameters and relationships. These sets can be mutually exclusive, mutually inclusive, or both. For performing a certain task assigned at a given design stage, participants may choose to exchange information on these parameters and relationships.

Through these information exchanges, every participant develops knowledge on the parameters and relationships involved. We define this as the participant’s state of knowledge after those information exchanges. As the design evolves, this state of knowledge might increase or stay constant. One such possible scenario is illustrated conceptually in Figure 1. This figure denotes the state of knowledge of a particular participant across information exchanges that occur during an entire design process. Before the start of information exchanges, it is possible that a participant has some initial knowledge. This state is referred as the participant’s initial state of knowledge. Within a collaboration, usually, this state of knowledge has an upper bound defined by the owner of that parameter/relationship. Consider the following example: OEM and supplier are collaborating with each other. Assume that supplier is supplying tires to OEM. In our framework, we assume that supplier has better knowledge (such as performance characteristics) about its tire than OEM.

3.1.1 Product model Let $n$ denote the number of participants in a collaboration. Let $P_i$ denote an $i^{th}$ participant and

---

2The entities (e.g., designers or teams) involved in a collaboration will be referred to as participants.
\( P_{-i} \) denote all the participants except \( P_i \). Also, let \( K_{p,i} \) denote the state of knowledge of \( i^{th} \) participant on parameter or relationship \( p \). As the collaboration proceeds, participants exchange information about the parameters and relationships involved. In other words, other participants \( (P_{-i}) \) learn and their state of knowledge, say on parameter \( p \), increases. Let \( K_{p,-i} \) denote the states of knowledge achieved by all except \( P_i \) on parameter \( p \). Please note that \( K_{p,-i} \) and \( K_{p,i} \) are sets of length \( (n - 1) \) whereas, \( K_{p,i} \) and \( P_i \) are singleton sets. Further, these parameters and relationships can be classified into the following categories:

**Private Parameter/Relationship:** A parameter/relationship owned by a single participant \( P_i \). For example, only the OEM will be aware of the emission strategy while designing a car.

**Shared Parameter/Relationship:** A parameter/relationship owned by a single participant \( P_i \) whose value is known to a set of participants, \( S \). Please note the size of set \( S: |S| \leq n \). For example, some (but perhaps not all) collaborating manufacturers will know the number of cylinders in an engine.

A scenario of the product model is illustrated in Figure 2. The boxes in gray represent participants, and the circles within the box denote the ownership of parameters/relationships by that participant. The white circles (and dotted lines) represent shared parameters (and shared relationships) and the black circles (and solid lines) represent private parameters (and private relationships). This model attempts to describe the relationships, the parameters, and their interactions in a way relevant to all participants, similar to the concept of Logical Dependency Graph introduced by Zhang [6] but with emphasis on knowledge ownership and evolution of knowledge throughout a collaboration.

### 3.1.2 Process model

Design processes involve various stages. At a design stage \( k \), there is a goal \( (g_k) \) to be met. Please note that \( g_k \) is a function of parameters and relationships involved in the design. For example, while designing a car, an initial goal may be to pass emission standards. At later stages, performance could be considered. In this process, the car design will be updated if the expected improvement at a given stage meets the stage goal. The process model illustrated in Figure 2 describes two design stages, \( k \) and \( k + 1 \). In these design stages, we use the product model along with a decision gate. This decision gate is used to decide whether to iterate the design by sharing more information and recalculating, or to commit the design and move to the next stage.

With these definitions in place, we shall now state the assumptions upon which this framework is built.

### 3.2 Key Assumptions in this Framework

There are several general assumptions implicit in this framework. These include:

1. Every participant works towards mutually agreed objective(s) subject to his/her internal constraint(s).
2. Every participant is honest but curious; i.e., he/she will not deliberately try to deceive other participants and will work towards the goals of the collaboration, but is also interested in gaining knowledge of his/her participants’ private information.
3. Every participant tries to minimize sensitive information leakage while sharing and maximize the benefits of the collaboration.

### 3.3 Need for Quantifying the State of Knowledge

Every participant is curious, and wants to learn about private information belonging to other participants. So, participants develop a fear of \( P_{-i} \) making inferences about their private information during collaboration. Hence, participants adopt techniques discussed in Section 2 such as suppression and generalization, to overcome this fear. However, these techniques may not inhibit \( P_{-i} \) from making reasonably good estimates on the private information of \( P_i \). Although these estimates may draw on several factors, such as market information or reverse engineering, in our framework we restrict these inferences such that they are entirely due to the information shared by \( P_i \) during design iterations.

Given that these inferences are possible, \( P_i \) desires an approach to predict increases in the state of knowledge \( K_{p,-i} \) while sharing information on parameter \( j \). In other words, \( P_i \) wishes to estimate \( P_{-i} \)'s understanding of parameter \( j \), parameter \( p \), and the relationships between them in order to estimate \( K_{p,-i} \) given the potential information on \( j \). Based on this estimation, \( P_i \) may develop a strategy for parameter \( j \) that best controls the states of knowledge of the other participants on parameter \( p \). Without loss of generality, we consider that an increase in \( K_{p,-i} \) would result in information leakage on parameter \( p \) from \( P_i \)'s point of view.

### 3.4 Confidentiality and Value in Collaborative Design

In collaboration, typically, information exchanged is used in certain forms of computations, or (in the case of relationship information) to define computations. In Section 2 we saw different information exchange methods that enable us to perform multi-party computations (SMCs). These methods provide different levels of protection against information leakages. We consider such information leakages leading to loss of confidentiality.
Now, we shall briefly discuss the different ways of maintaining confidentiality within a collaboration.

In **Zero Confidentiality**, all parameters and relationships involved are made available to all the participants throughout the collaboration. In other words, there is no confidentiality associated with the parameters. In **Semi-Confidentiality**, confidentiality is compromised strategically to improve the solution obtained through the collaboration. In this scenario, one or more participants would share his/her private information with a set of collaborators as the collaboration proceeds, or share a generalized or suppressed version of the information to preserve some confidentiality [11,21], as discussed in Section 2. In **Full Confidentiality**, the extreme case of Semi-Confidentiality, neither the parameters nor their relationships are revealed throughout the collaboration. So, a particular participant is only aware of the exact values of his own model parameters and the associated relationships.

In these information exchanges, however, it is apparent that transparency helps in achieving the best possible solutions from a collaboration. As discussed Sections 1 and 3.3, information sharing in a collaboration can have adverse effects as well. Thus, all participants must consider the value and confidentiality associated with every parameter and relationship involved in a collaboration, both during collaboration and before agreeing to a potentially collaborative project. We define these two indicators as follows:

**Value**: At a given design stage $k$, information is exchanged in order to meet the goal $g_k$. Each participant has their own understanding of design goals; in this paper we consider goals $g_k$ to be common knowledge. Here, the value $V_i$ is defined as the confidence of $P_i$ towards achieving the goal $g_k$ given the information shared by $P_i$.

**Confidentiality**: In Section 1 we stated that confidentiality involves a set of rules through which authorized personnel can access sensitive information. In the collaborative design context, this translates to the access of parameters or relationships of $P_i$ by $P_{-i}$. The rule we adhere to is as follows: $P_i$ is willing to share information if $\max(K_{p_{-i}})$ below his/her acceptable threshold. That is, any member of $P_{-i}$ should not learn more than what is acceptable to $P_i$ about the parameters and relationships owned by $P_i$.

In Section 4 we explain the techniques to determine the confidence of $P_i$, $\max(K_{p_{-i}})$. Please note the thresholds mentioned here are subjective in nature; these can be determined by psychometric models or derived from economic or other models. Since the scope of this paper is only to build the framework and demonstrate its use, such models are not discussed here.

In the following section, we develop a specific collaborative design scenario, which will be explored for the remainder of this paper as an example of how this framework can be applied.

### 4 APPLICATION OF THE PROPOSED FRAMEWORK

In this section, the state of knowledge on parameters and relationships is modeled using probability distributions from a Bayesian point of view. At the start of collaboration, each participant $P_i$ has priors on other participants’ private parameters and relationships. A random variable, say $X$, with probability density function $P(X = x) = p(x)$, may be used to model the current state of knowledge ($K_{p,i}$) the participant has on a given parameter $p$. For instance, a parameter generalized to some range could be modeled as a uniformly distributed random variable with the corresponding upper and lower bounds. As design iterations occur, the state of knowledge ($K_{p,i}$) changes and these distributions will be adjusted through direct (shared) or inferred information.

We use the framework presented in Section 3 to quantify both value and confidentiality based on these priors. This quantification is based upon the notions of divergence and differential entropy, which are described later in this section. For this section, we consider the following specific design scenario:

The participants’ $P_i$ goal is to minimize an objective function, with feasible solutions being those that drive the objective function below some goal $g_{k,i}$.
4.1 Value Analysis

When information is revealed during an exchange at design stage $k$, the participant(s) owning the information wish to add some value to the design, with respect to achieving the design goal ($g_k$). To gain a better understanding of the information’s impact in the collaboration, the participant $P_i$ is interested in quantifying the value of his/her information. The value of the information revelation is quantified using probability theory.

As an example, consider an aircraft design problem where there is a constraint on the maximum weight of the engine. At the current design stage, meeting this constraint is the goal $g_k$. The value of some revelation by participant $P_i$ corresponds to the probability of achieving a design below the maximum weight, given the information being revealed and the current state of knowledge of participant $P_i$.

The design goals may be formulated in terms of relevant parameters and their relationships ($g_k = f(p)$), and can be determined by every participant. Here, $p$ denotes the parameters and $f$ denotes the relationships involved. However, the values differ since $K_{p,i}$ are different among the participants. Assume that for a particular participant $P_i$, a probability distribution function (pdf) $f_{P_i}(p)$ can be constructed based on $K_{p,i}$ for the design goal $g_k$ perhaps through some uncertainty propagation analysis such as a Monte Carlo simulation (as done for the example presented in Section 5). For this participant and his/her objective function(s), given some goal $g_{k,i}$ denoting the maximum feasible value of that objective, the value index $VI_{est}$ is given by a ratio of cumulative distribution function (cdf) evaluations:

$$VI_{est} = \int_{-\infty}^{g_{k,i}} f_{P_i}(p) dp$$

which quantifies the probability of achieving a feasible solution given $g_{k,i}$. As an example, consider an early stage design goal of keeping an artifact under some target weight, $g_{k,i} = Weight < Target$. A visualization of this index for a given distribution for a parameter $p$ is given in Figure 4. This index has a minimum of 0 (no probability of feasible solution) and tends to 1 as the probability of feasibility increases. Note that if the participant has a minimum value target, then the numerator integral has ranges $[g_{k,i}, +\infty]$ instead.

Next, we discuss our approach to confidentiality analysis, and introduce the concepts of divergence and differential entropy.

4.2 Confidentiality Analysis

Let $Q(X = x)$ represent the knowledge prior to an information exchange, and $M(X = x)$ represent the knowledge following an information exchange. We use the following two quantification methods to analyze these priors: (i) Kullback-Leibler (KL) divergence [6], [26] and (ii) differential entropy and the corresponding privacy measure [26], which may be used to construct a confidentiality index (CI).

KL divergence quantifies the difference in two pdf’s. The higher the KL divergence, the greater the change from prior to posterior knowledge. It should be noted that this does not necessarily correspond to a “more correct” view of the parameter, but only that knowledge has changed. The KL divergence $D_{KL}(M||Q)$ of any distribution $Q(X = x) = q(x)$ from $M(X = x) = m(x)$ is given by [6]:

$$D_{KL}(M||Q) = \int_{-\infty}^{+\infty} m(x)\log \left(\frac{m(x)}{q(x)}\right) dx$$

Differential entropy may be derived from KL divergence, and is a measure of the ‘randomness’ of a pdf. When the pdf models uncertainty in a parameter, it is also commonly extended to quantify that uncertainty. In the case of a confidential parameter that is intentionally obscured, it may be used to quantify confidentiality as well [26]. For a random variable $X$ with pdf $m(x)$, the differential entropy $H(X)$ is defined as [26]:

$$H(X) = -\int_{-\infty}^{+\infty} m(x)\log(m(x))dx$$

If parameter $p$ modeled using random variable $X$, where $M(X = x) = m(x)$, is intentionally being hidden, the corresponding privacy measure $\Pi(p)$ may be defined as [26]:

$$\Pi(p) = e^{H(X)}$$

As information exchanges take place, the plausible ranges of parameter $p$ may decrease. This corresponds to narrower distributions of $X$, and thus a smaller $\Pi(p)$. This is of interest to participants who do not own data on parameter $p$.

Entropy’s advantage to KL divergence as a security measure in collaboration is that decreasing entropy directly corresponds to increased confidence in a parameter value, which relates directly to loss of security on that parameter given feasible prior
knowledge. Note that this measure is not suited for unbounded distributions. However, such distributions are unlikely to occur in an engineering context.

The Confidentiality Index (CI), corresponding to a given parameter and a given participant, is given by,

\[ CI_{est} = \frac{\Pi_{est}}{\Pi_0} \]  \hspace{1cm} (5)

where, \( CI_{est} \) is the current estimated confidentiality index of the given parameter with respect to the current state of shared information, \( \Pi_0 \) is the security measure corresponding to the initial state of knowledge, and \( \Pi_{est} \) is the estimated security measure based on \( \max(K_{p-i}) \) (defined in Equations 3 and 4), given the potentially revealed information. Note that our focus in this paper is quantifying the confidence of the participant in a given confidential parameter estimation. Our metric for confidentiality focuses solely on the entropy of the posterior distribution, and differs from other metrics, such as the conditional probability proposed by Zhang [6], which consider confidentiality lost when \( W \) from this collaboration is to minimize the weight \( W \) of the truss.

The configuration of the truss is illustrated in Figure 5. Two tubular bars of thickness \( t \) are pinned to the surface on one end and welded with each other on the other end. These members are subjected to a vertical load of \( 2P \). The outer diameter of the tubes is \( d \), and the welded joint is at a height \( H \).

Alice can have private parameters associated with her objective function, \( F_{des} \). For example,

\[ F_{des} = k_1W + k_2\frac{W}{V} \]  \hspace{1cm} (6)

where, \( W, V \) denote weight and volume, respectively, of the truss configuration, and \( k_1, k_2 \) are weightages in the objective function. Alice can have such weightages as private parameters. However, in the current example, we assume \( F_{des} \) to be just the weight (\( W \)) of the truss. The weight is given by [27]:

\[ F_{des} = W = 2\pi dt\sigma \left(\frac{B^2 + H^2}{\gamma}\right) \]  \hspace{1cm} (7)

where, \( W_0 \) is the maximum allowable weight of the truss from Alice’s point of view. So, \( W_0 \) would be a private parameter of Alice and \( W \leq W_0 \) is a private relationship. Bob would like to know the possible diameter of the rod for a combination of load and geometry. The constraint on diameter (\( d \)) is given by [27]:

\[ \frac{P\sqrt{\left(B^2 + H^2\right)}}{\pi\sigma_f H} \leq d \]  \hspace{1cm} (8)

where, \( \sigma_f \) is the factor of safety.

Both Alice and Bob are ignorant of the exact values of their collaborator’s parameters. The ownership of these parameters is
listed in Table[1] However, Bob has prior knowledge on Alice’s private parameters \((P,t)\). These priors may be informed by prior experience, initial contact with Alice, or a combination of these and other factors, and serve as a model of Bob’s initial state of knowledge. With these priors, Bob determines his first proposal for the diameter, \(d\). Based on acceptance/rejection of Bob’s design proposals, Alice would offer more information on her parameters, and Bob would refine his own priors and his solution for \(d\). The information exchanges that occur between Alice and Bob are briefly described as follows:

1. Bob shares a value of diameter \(d\) with Alice based on the current understanding of \(P,t\).
2. Alice determines the weight \(W\) using the diameter \(d\) proposed by Bob and her priors on Bob’s values for \(γ\) and \(σ_0\), and informs Bob if the proposed diameter is acceptable (see next section).
3. If the proposed diameter is rejected, Bob needs more clarity on Alice’s private information to re-design. So, he performs a value analysis on one of the Alice’s private parameters and arrives at a value of \(VI\). He shares this with Alice and asks her to reveal private information.
4. Alice concurrently performs confidentiality analysis and determines the confidentiality index, and estimates the value index stemming from revealing the requested information. If both value and confidentiality indexes are above her threshold, she reveals further information. Else, Alice stops information sharing and the design is accepted as-is or the collaboration is terminated.

These information exchanges are summarized in Figure 6. Now, we illustrate our approach with this example. The following are assumptions made for this analysis:

1. Alice’s revealing strategy is as follows: information only about a particular private parameter (parameter or relationship) is revealed in all the design iterations involved. If Alice’s confidentiality index is above her threshold, she chooses to reveal information either on \(P\) or \(t\), but not both.
2. The limits for Alice’s and Bob’s confidentiality index are 0 and 1. Hence, design iterations continue until \(VI\) approaches 1 or \(CI\) approaches 0.
3. Relationships are universally shared throughout the collaboration. Alice is concerned only with the confidentiality of her parameters.

Using this example, we determine which parameter revelations might be beneficial for Alice, given some subjective criteria for value and confidentiality. The following sections are meant as an illustration of Alice’s and Bob’s communication throughout several design iterations of this initial design stage. As Alice is the leader of this collaboration, we work from her perspective, focusing on her concepts of value and confidentiality.

### 5.1 Revealing information on load, \(P\)

We first assume that Alice and Bob meet and establish an initial knowledge state. That is, they agree on the mathematical models governing the co-designed system, the shared parameters, and the private parameters. In this example, we assume that Alice and Bob decide to reveal their values of \(H\) and \(s_f\), respectively (note that in this scenario \(H = B\)). We also assume the actual values of the private parameters and the priors held by the opposite collaborator are as stated in Table 2. Bob’s priors on \((P,t)\) are derived from Alice’s description of the design problem, while Alice’s priors on \((σ_0, γ)\) stem from Alice’s implicit knowledge on Bob’s likely material (steel).

Thus, Alice may reveal information on \(P\) or on \(t\) in order to drive Bob to provide more satisfying values of \(d\) (that is, \(d\) values that drive the weight down while still being safe under the load). In this example, we assume this revelation comes from Alice narrowing Bob’s priors on these parameters (telling Bob that \(P ∈ [100,300]\)kN instead of \(P ∈ [100,500]\)kN, for instance). Alice first considers revealing information on \(P\) to Bob by narrowing the revealed range of possible \(P\) values until the value is completely revealed.

In this section, we restrict ourselves to analysis of Alice providing information to Bob. The converse analysis may be carried out in a similar fashion. The initial state of knowledge on the private and design parameters was generated through Monte Carlo simulation in Python with respect to the initial priors given above and in Table 2 and are plotted as sampled distributions in Figure 7.

#### 5.1.1 Value Analysis

Alice (and Bob) first consider the value of such a revelation. Both Alice and Bob perform this analysis by assigning a Value Index (\(VI\)) describing the desired outcome. In this analysis, Alice wishes to minimize the weight \(W\) of the truss. Thus, Alice decides on an estimated Value Index, defined as follows:

\[
VI_{est} = \frac{P(W < W_0)_{est}}{P(W < W_0)_{des}} = \frac{\int_{W_0}^\infty p(w)dw}{\int_{-\infty}^W p(w)dw}
\]

(9)

where \(P(W < W_0)_{des}\) is the desired probability that the final truss weight will satisfy the requirements; in this case, \(P(W < W_0)_{des} = 1\). \(P(W < W_0)_{est}\) is the estimated probability of the same event given the considered information on \(P\) is revealed. \(VI_{est} = 1\) corresponds to an estimated 1.0 probability of a successful value of \(W\), given the information. These probabilities are arrived at by constructing a probability distribution for the final value of \(W\) considering Alice’s priors on the material density \(γ\) and Alice’s expectation on the change in \(d\) given the considered revelation and her comprehension of Bob’s prior on \(t\), using Equations 7 and 8. The probabilities in Equation 9 are given by the CDF of the distribution of \(W\) in the range \([0,W_0]\). These and subsequent calculations were carried out using Alice’s and Bob’s current knowledge states.
Alice asks Bob to submit his design proposal

Bob estimates priors on Alice’s private information

Bob submits design proposal to Alice

Alice’s objective is met?

Yes

End of design iterations

No

Alice computes VI for a particular information

VI_{curr} < VI_{next}

Yes

Alice computes CI for the same particular information

CI_{curr} < CI_{next}

Yes

Alice will share information with Bob

No

Alice computes VI for a particular information

FIGURE 6. Exchange information protocol during design iterations, Alice providing information to Bob.

FIGURE 7. Initial information represented by samples of probability distributions of parameters $P$ (a), $t$ (b), $W$ (c), and $d$ (d).
Alice (and Bob) arrive at values for $V_{I_{est}}$ conditional on the revealed range of $P$. These are then compared against each other and the confidentiality indexes calculated as described in the following section to arrive at a revelation strategy.

### 5.1.2 Confidentiality Analysis

Alice now considers the confidentiality compromised on her other private parameter, $t$. As Alice reveals information on $P$, Bob gains insight into the design problem and may update his prior on $t$ as he also works to refine his value of $d$. Alice attempts to estimate and quantify this effect by constructing an estimated Confidentiality Index $CI_{est}$ on $t$ given Bob’s initial state of knowledge and the new state after the potential revelation. $CI_{est}$ is the confidentiality (see Section 4.2) of revealing various posteriors for $t$ conditional on the potential revelation. $\Pi(t|\text{initial})$ is the confidentiality (see Section 4.2) on $t$ given the initial information, while $\Pi(t|\text{reveal})$ is the confidentiality given the potential revelation. $CI_{est} = 1$ corresponds to no loss of confidentiality on $t$, while $CI_{est} = 0$ corresponds to complete confidence in Bob’s value of $t$ given the current $d$. Note that Bob could still deviate from the true value of $t$, due to his lack of knowledge on the optimal value of $d$. These confidentialities are found by constructing the expected distributions of $t$ given Bob’s assumed information on $P$, $d$, and his private information at the given iteration and state of knowledge, and then following the entropy calculation outlined in Section 4.2. Again, this is achieved using Equation 4.

After the value and confidentiality analysis is carried out, Alice may compare the Value and Confidentiality Indexes provided for various possible revelations of the parameter $P$. If some of the possible revelations are expected to fall within acceptable ranges for the indexes (subjectively defined by Alice), she may choose to make that revelation to Bob. For example, Alice may insist that $V_{I_{est}} > 0.5$ and $CI_{est} > 0.6$ must hold for any revelation during the given iteration. Bob may have similar expectations before sharing any information on $\sigma_0$ or $\gamma$.

### 5.2 Revealing information on thickness, $t$

A similar analysis may be carried out by Alice as she considers revealing information on $t$. In this case, the relevant distributions are constructed using the relationships between $t$, $P$, $W$, and $d$ given in Equations 7 and 8.

During this analysis, Alice considers instead narrowing Bob’s information on $t$, and studying how that may affect his proposed value of $d$ and therefore the expected result for $W$. The Value Index and the method is identical to that in Section 5.1.1, but instead the range of $P$ is held constant while $t$ is explored. Similarly, the confidentiality analysis and index are the same as those described in Section 5.1.2. As Alice estimates the effects of revealing various posteriors for $t$, the values for $CI_{est}$ may be compared with the previous $V_{I_{est}}$ to arrive at worthwhile revelations for $t$, if they exist.

In the following section, we present results for a study carried out as described above, from Alice’s perspective, as well as a possible revelation strategy Alice may follow based on the results and her (personal) requirements for $V_{I_{est}}$ and $CI_{est}$ for a given design iteration. Eleven possible revelation strategies are analyzed for both revealing $P$ and revealing $t$; these strategies and corresponding indexes used in Section 5.3 are reported in Table 3.
5.3 Alice’s Potential Revelation Strategy

Alice first considers revealing information according to the posterior ranges for $P$ and $t$ by providing Bob with successively smaller ranges of possible values for each parameter. As this information is revealed, Alice wishes to anticipate the change in the acceptability of the weight objective (Value Index) as well as the loss of confidentiality on the parameter she is not sharing (Confidentiality Index). Following the analysis procedure outlined earlier, Alice performs value and confidentiality analyses on various revelation scenarios for both parameters and studies the resulting values for $V_{\text{est}}$ and $C_{\text{est}}$. Bob performs value analysis to prioritize requests for information from Alice. The results for these analyses are described in reference to the plots in Figures 8 and 9.

Consider first revealing information on $P$. The given initial range of $P$, with interval size $400kN$, initially yields a $V_{\text{est}}$ value of 0 (that is, Alice predicts no feasible solution for $W$ given Bob’s prior knowledge) (Figure 8, Table 3). According to this analysis, the index is expected to rise dramatically for revelations narrowing this range to $[200, 300]kN$, where a feasible (not necessarily optimal) design solution is expected to be inevitable. Compare this to the expected $V_{\text{est}}$ values for revealing $t$ alone (Figure 9), which suggest that a feasible design will not be produced for any revelation of $t$ by Alice. This analysis reveals that, if information on $t$ is not accompanied by information on $P$, the values of $V_{\text{est}}$ are not expected to increase. In both possible revelation paths, values of $C_{\text{est}}$ (Figures 8, 9) decrease steadily as information is revealed, as is expected for this relatively simple formulation. If Alice is to choose between revealing $P$ and revealing $t$, these estimates suggest revealing information on $P$ would yield more value for a given compromise on security. Bob’s expected values for $P$ and $t$, given the proposed knowledge of the other, are plotted in Figure 10.

It is worth mentioning not only the effects of revealing information, but also the direction of revelation. For Bob’s $P$ and $t$ priors (Table 2), the true value of $t$ is much closer to the expected value of $t$ Bob would calculate via his prior, compared to the true value of $P$. Therefore, revelation of $t$ from one direction only (such as lowering the upper bound on the revealed range and leaving the lower bound alone, as was considered in these trials) may skew Bob’s understanding of the problem in a more undesirable direction than similar revelations for $P$. Thus, in this scenario and for these revelations, $P$ appears to be the more useful parameter to share.

Note that any participant’s revelation strategy may rely on the indexes calculated in this method, but will ultimately be decided by subjective criteria determined by the participants in a given scenario. Alice, based on the previous analysis, chooses only to reveal information about the value of $P$, successively narrowing the range provided to Bob. In this scenario, we assume Alice would first prioritize obtaining feasible solutions (driving $V_{\text{est}}$ above, say, 0.5) while also preserving reasonable security (ensuring $C_{\text{est}}$ does not drop by more than, say, 0.25 per revelation). Based on these assumptions, Alice may follow a four-iteration revelation strategy outlined in Table 4, arriving at a 100% expected probability of obtaining a feasible solution after the final revelation, with a final $C_{\text{est}}$ greater than 0.5.

In this scenario, as $P$ is gradually revealed, Bob’s submissions for $d$ become progressively less conservative, as expected. This results from Bob’s better understanding of $P$, and the decrease in the expected value of $P$ as the range is narrowed from the upper bound. Note that, if the range was instead narrowed from the lower bound, the solution may actually suffer if not also supplemented with information on $t$. This lower-bound incrementation causes the slight dip in the $VI$ plot in Figure 8. This highlights the fact that participants must be cognizant of the implications of their revelations, and in particular whether they are driving a prior’s expected value in a helpful direction.

6 CLOSING COMMENTS

As globalization has encouraged unprecedented cooperation and collaboration in engineering design, it has also brought new concerns to light. One of them is the confidentiality of designer’s private information. Designers must be aware that the information they share could be used against their interests through leakage of sensitive information as much as it could help them reach a better solution. In this paper, we proposed one possible approach for quantifying such trade-offs. We also demonstrate our approach using a simple collaborative design problem where the tradeoff between confidentiality and value must be considered. However, our method of application to this framework has the following limitations:

1. Our method uses metrics that are suited for bounded pdf’s.
2. This method only addresses scenarios where all participants know the relations between parameters involved in the design problem.

Here, our focus is to introduce the notion of tradeoff between confidentiality and value in collaborative design. The proposed method using the same framework can be further extended to the following scenarios:

1. Addressing design scenarios with more than two collaborators, with more complex information sharing and confidentiality scenarios including those with ambiguous relationships between various parameters in the model.
2. Addressing the recursive properties of inferring various parameters during information exchange, which were not addressed in this paper. In particular, as more parameters are introduced, the nature of inferences become more complex, and the tradeoff between computational time spent on inference and the value of the inferences may need further analysis.
3. Addressing objective functions with more than one term. In particular, the weights associated with each term may differ between collaborators, and may be modeled as private parameters.
4. Addressing competitive scenarios, where (in early design) Alice may consider several material designers and use this
FIGURE 8. VI results (a) and CI results (b) for sharing $P$

FIGURE 9. VI results (a) and CI results (b) for sharing $t$ (no VI benefit if information on $P$ is not shared)

FIGURE 10. Bob's expected values for $t$ (a) and $P$ (b) due to revelations of the opposite parameter
approach to determine the most suitable collaborator while revealing minimal information.

We believe that this trade-off analysis is important to enable collaborations across enterprise and national boundaries. As this line of study develops, results will empower designers to better control the flow of information during collaborative design and ensure shared information does quantitatively more good than harm.

ACKNOWLEDGMENT

Portions of this work were supported by National Science Foundation Grants CPS-1329979, CNS-0915436, CMMI-1265622, Science and Technology Center CCF-093970; and by sponsors of the Center for Education and Research in Information Assurance and Security. The statements made herein are solely the responsibility of the authors.

REFERENCES


---

| TABLE 3 | Revelation strategies considered by Alice for parameters P and t |
|---|---|---|---|---|---|---|---|---|
| Strategy | 1, 2 | 3, 4 | 5, 6 | 7, 8 | 9, 10 | 11 |
| P(kN) [low:high] | [100, 470] | [100, 400] | [100, 330] | [100, 270] | [120, 200] | [148, 152] |
| [100, 430] | [100, 370] | [100, 300] | [120, 250] | [120, 170] |
| t(mm) [low:high] | [1.0, 5.5] | [1.0, 4.5] | [1.0, 3.5] | [1.0, 3.0] | [1.5, 2.7] | [2.52, 2.56] |
| [1.0, 5.0] | [1.0, 4.0] | [1.0, 3.2] | [1.5, 3.0] | [2.0, 2.7] |

| TABLE 4 | Results for Alice’s Revelation Strategy (Revealing P only, comparison to initial information) |
|---|---|---|---|---|---|---|
| P Revealed | VI predicted | CI expected on t | d_submitted | VI realized | Bob’s t estimate (deviation) |
| [100, 500]kN | 0.00 | 1.00 | 81.0mm | 0.00 | 3.43mm (+35.4%) |
| [100, 370]kN | 0.21 | 0.76 | 72.8mm | 0.23 | 2.69mm (+5.7%) |
| [100, 330]kN | 0.54 | 0.67 | 69.5mm | 0.72 | 2.48mm (−2.6%) |
| [100, 300]kN | 0.79 | 0.53 | 67.2mm | 1.00 | 2.29mm (−9.7%) |


