Extractable Common Randomness From Gaussian Trees: Topological and Algebraic Perspectives

Ali Moharrer, Shuangqing Wei, George T. Amariucai, and Jing Deng, *Senior Member, IEEE*

***Abstract*— In this paper, we study both topological and algebraic properties of unrooted Gaussian trees in order to characterize their security performance. Such performance is measured by the corresponding potential in extracting common randomness from a given tree, which is further determined by max–min and min–max conditional mutual information (CMI) values, subject to the order of selecting variables from the tree by legitimate nodes Alice and Bob, and an eavesdropper Eve, respectively. A new operation is proposed to transform a Gaussian tree into another, and also to order different Gaussian trees. Through such operation we construct several equivalent classes of Gaussian trees. Each class includes multiple Gaussian trees that can be partially ordered based on the associated max–min or min–max CMI metric, and thus, we can find the most secure and the least secure trees in each partially ordered set (poset). The union of all posets generates all possible non-isomorphic trees of the given number of variables. Then, we assign a particular polynomial to each Gaussian tree, and show that such polynomial can determine the relative security performance of the Gaussian tree with respect to other trees within the same class. In the end, based on a generalized integer partition method, we propose a novel approach to efficiently enumerate the most secure structures of all posets.**

***Index Terms*— Gaussian trees, common randomness, conditional mutual information, partially ordered sets.**

I. Introduction

CONSIDER a problem of maximizing the number of established secret key bits through public discussions between two legitimate parties Alice and Bob in the presence of a passive adversary eavesdropper Eve [1]–[3]. In particular, assume three agents all have access to a set of n random variables whose joint probability density function (PDF) is featured in a graphical model, from which Alice and Bob choose two of the n variables, X_a and X_b, and Eve for another X_z, respectively. It has been shown in [1]–[3] that the conditional mutual information (CMI) is the achievable secrecy rate through public discussion. It quantifies the number of secret key bits per channel use established between Alice and Bob, in the presence of passive Eve, who not only overhears all publicly exchanged messages, but also has a full access to X_z. Under this framework, the primary problem we are tackling in this paper is twofold: (1) Given a graphical model for the joint PDF of n variables, what variables should Alice and Bob select to maximize the amount of achievable secret information under Eve's attack? (2) How should we compare the potential secrecy level of different graphical models under properly defined metrics? Does there exist a consistent ordering of graphical models under which we could select the most favorable or least favorable models in terms of some properly defined metrics?

Such problems can find applications where secrecy shall be established between legitimate parties who need to decide what correlated random variables are to be chosen among a set of dependent candidates. For example, in a sensor network with n sensor-nodes whose measurements on physical parameters, say, temperature or humidity, are to be taken as sources of common randomness. Alice and Bob thus need to determine which two variables should be taken considering the leakage to a third party who can only compromise one of the remaining nodes. In addition, if there are options as to the set of sensor deployments in multiple set-ups, which result in multiple joint distributions of random variables, which topology of the underlying graphical model is more favorable? Even more interesting is what if we could transform the joint distribution under certain constraints by some local changes of sensor deployment, what guidance we could provide to such changes to attain a more favorable topology and joint distribution in terms of a larger amount of extractable secret key bits? Our goal is to provide insights and answers to these interesting and security related questions on graphical models.

As a first step, we have adopted a game theoretic framework to study the proposed problems: (1) max-min perspective: Alice and Bob first pick two random variables out of n variables, based on the pessimistic assumption that Eve will later choose the best variable from the remaining $n-2$ variables, i.e. to find the solution to the max-min conditional mutual information $I(X_a; X_b|X_z)$; (2) min-max perspective: Eve selects its favorite random variable first, while Alice and Bob choose from $n-1$ remaining random variables in the second place to find the solution to the min-max of the conditional mutual information. It should be noted that such a modeling has been coined as the security game in several contexts [4]. In fact, [4] defines the secrecy capacity metric similar

Manuscript received August 4, 2015; revised December 14, 2015; accepted March 2, 2016. Date of publication March 17, 2016; date of current version July 29, 2016. This material is based upon works supported in part by the National Science Foundation under Grant 1320351. The associate editor coordinating the review of this manuscript and approving it for publication was Dr. Tansu Alpcan.

A. Moharrer and S. Wei are with the School of Electrical Engineering and Computer Science, Louisiana State University, Baton Rouge, LA 70803 USA (e-mail: amohar2@lsu.edu; swei@lsu.edu).

G. T. Amariucai is with the Department of Electrical and Computer Engineering, Iowa State University, Ames, IA 50011 USA (e-mail: gamari@iastate.edu).

J. Deng is with the Department of Computer Science, The University of North Carolina at Greensboro, Greensboro, NC 27412 USA (e-mail: jing.deng@uncg.edu).

Digital Object Identifier 10.1109/TIFS.2016.2543688

to the max-min value of conditional mutual information, which quantifies the maximum rate of reliable information transmitted from source to destination, in the presence of an eavesdropper. Due to the vast parameter space of graphical models, we restrict our attention to the cases where the joint PDF of n variables can be featured in unrooted Gaussian trees to address the aforementioned problems. Since in Gaussian trees there is a single path connecting any two variables, we found studying such models not only mathematically convenient, but also conducive to several fundamental insights. To solve the proposed problems, we have explored several results obtained in [5] regarding the conditional independence relationships in Gaussian trees.

As a constraint and also for the purpose of fair comparisons between Gaussian trees using either the max-min or min-max conditional mutual information, we require all weighted trees to share the same joint entropy, i.e., the same total amount of randomness. Consequently, we consider the secrecy levels of n random variables measured by either max-min or min-max CMI for cases where their joint distributions can be featured in un-rooted and weighted Gaussian trees under a constraint of a given total joint randomness, namely, the joint entropy.

The contributions of this paper can be categorized into two groups of topological and algebraic analysis:

- First, we show that in each scenario Alice, Bob, and Eve choose a triplet of nodes, where each node is in a special topological correspondence with others. As a result, our search space to find the max-min or min-max values is reduced significantly. Then, we formally define a pruning and grafting (PG) operation to transform one Gaussian tree into another. In particular, we introduce a special form of PG operation, namely, pruning and grafting of leaf with neighbor of degree 2 (PGLN-2). This operation has an important impact on Gaussian trees: the max-min (min-max) value of the resulting Gaussian tree is always less than or equal to the max-min (min-max) value of the original Gaussian tree, hence making the resulting tree less secure than the original one. As a result, we form partially ordered sets (posets) of Gaussian trees and analyze the structural properties of these posets, by introducing an equivalent graph for each of these sets.
- Second, we introduce some algebraic tools to study the Gaussian trees and our introduced operations. We use the notion of Tutte-like polynomials [6] to represent each Gaussian tree with a specific polynomial. We show the impact of PGLN-2 operation on the corresponding polynomial, and also show that although non-isomorphic trees may have identical polynomials, however, for each of the posets and in the most cases this problem does not happen. We also show that some useful information can be extracted from this polynomial: the relative security of each Gaussian tree in a poset can be determined by its corresponding polynomial. Finally, we show that in each poset there exists the most secure Gaussian tree, as the poset leader, and introduce a systematic approach based on integer partitions [7] to effectively and directly enumerate all such structures.

A. Related Work

Other than our preliminary results in [8] and [9] where partial findings were reported, to the best of our knowledge, there are no other previous works that fully capture the current problem.

The fundamental problem of secret key sharing between two users in the presence of an eavesdropper in a public discussion channel is considered in [1]–[3]. Manshaei et al. in [4] provide a game theoretic framework to introduce the secrecy capacity.

In [5] and [10]–[12], some fundamental properties of Gaussian graphical models have been tackled using algebraic methods.

In [13], Patra and Lal propose an operation called *grafting* to order trees based on their *algebraic connectivity*, which is the second smallest eigenvalue (λ_2) of the Laplacian matrix. Moreover, in [14] the concept of *generalized tree shift* (GTS) is introduced to obtain certain posets for unlabeled and unweighted trees. It is further shown in [14] that the corresponding posets are also ordered based on the value of their algebraic connectivity.

In [8], we only considered the current problem for certain Gaussian trees with $n = \{4, 5\}$ nodes in the max-min scenario, where each random variable in a Gaussian tree has a unit variance. In [9], we extended the results of [8], to Gaussian trees with larger size. In this study, however, we generalize the scope into considering any Gaussian tree, with its random variables having arbitrary variance values. Moreover, we extend our study with the max-min metric to scenarios where min-max metric is adopted.

B. Paper Organization

The paper is organized as follows. Section II presents the system model. We define the notion of Gaussian trees, and introduce the squared partial correlation coefficient to be used in the max-min and min-max scenarios. We study topological properties of Gaussian trees in Section III. For both scenarios, we introduce the PG and PGLN-2 operations to partially order Gaussian trees. Furthermore, we formally define the equivalent classes of Gaussian trees, which are obtained by these operations. In Section IV certain types of polynomials are introduced to characterize the security performance of each Gaussian tree. Also, we propose an effective method to enumerate certain Gaussian structures with robust security performances. Section V gives the concluding remarks.

II. System Model

Here, for the simplicity of denotations, instead of X_a, X_b, and X_z we use a, b, and z as the random variables that represent the choice of Alice, Bob, and Eve, respectively. The capital letters A, B, and Z denote the corresponding subsets of random variables chosen by each group.

In this study, we consider the Gaussian joint distribution to capture the density of n variables, *i.e.*, $P_{\boldsymbol{x}}(x_1, x_2, \ldots, x_n) \sim N(\mu, \Sigma)$, where μ is the mean vector that without loss of generality we assume $\mu = 0$, and Σ is a symmetric positive-definite covariance matrix of n random variables with

$\sigma_{ij} \in \Sigma$ be the covariance between the random variables x_i and x_j. Furthermore, we assume that the joint density can be characterized by a weighted and unrooted tree $T = (V, E, W)$, where V is the set of nodes representing the random variables, E is the set of edges showing the dependency relations between variables [10]–[12], and W is the set of edge weights with elements $w_{ij} = \sigma_{ij}$ whenever there is an edge between the nodes x_i and x_j. For a fair comparison between any two Gaussian trees, we assume that the users in all models have the same total amount of randomness, i.e., the same entropy. In this case, it is well known that the entropy of $\boldsymbol{x} = (x_1, x_2, \ldots, x_n)$ can be obtained by $H = 1/2 \ln((2\pi e)^n |\Sigma|)$ [15]. Hence, in order to obtain a fixed entropy we have to fix the determinant of the covariance matrix, i.e., $|\Sigma| = C_E$, where $C_E \in \mathbb{R}$ is a finite and non-zero constant. Suppose x_i, x_j, x_k are three variables drawn from the Gaussian graphical model, where $x_i \perp x_j | x_k$, i.e., x_i is conditionally independent of x_j, given x_k. Then, one can show that $\sigma_{ij} = \sigma_{ik}\sigma_{jk}/\sigma_{kk}$ [5], where σ_{kk} is the variance for the node x_k. Now, suppose there is a path $p_{ij} = e_{i,i_1} e_{i_1,i_2} \ldots e_{i_{m-1},j}$ between i and j consisting of m edges. Since in Gaussian trees there is only one path between any two vertices, we can write

$$\sigma_{ij} = \sigma_{i,i_1}\sigma_{i_1,i_2} \ldots \sigma_{i_{m-1},j} \Big/ \prod_{l=i_1}^{i_{m-1}} \sigma_{ll} \tag{1}$$

Note that equation (1) is only valid for Gaussian tree models, hence makes studying these structures more convenient.

Next, we give a proper definition for the max-min problem, under the explained scenario.

Definition 1: Under the Gaussian tree model, legitimate entities Alice and Bob pick two nodes a and b on the tree under the attack by an eavesdropper Eve who selects the third and distinct node/variable z on the same tree. The objective of Alice and Bob is to select the pair (a, b) *to maximize the minimum conditional mutual information* $I(a; b|z)$. *In particular, we adopt* $\max_{\{a,b\}} \min_z I(a; b|z, T)$ *as the first metric to measure the privacy level of a given weighted Gaussian tree* $T = (V, E, W)$.

Similarly, we can define the min-max problem under the same circumstances. In this case we adopt $\min_z \max_{\{a,b\}} I(a; b|z, T)$ as another metric to measure the privacy level of a given weighted Gaussian tree $T = (V, E, W)$.

For Gaussian random variables the conditional mutual information $I(a; b|z)$ can be directly related to the *squared partial correlation coefficient*, which is defined as below [5],

$$\begin{aligned} \rho^2_{ab|z} &= \frac{(\sigma_{ab} - \sigma_{az}\sigma_{zz}^{-1}\sigma_{bz})^2}{(\sigma_{aa} - \sigma_{az}\sigma_{zz}^{-1}\sigma_{az})(\sigma_{bb} - \sigma_{bz}\sigma_{zz}^{-1}\sigma_{bz})} \\ &= 1 - e^{-2I(a;b|z)} \end{aligned} \tag{2}$$

where $\sigma_{ab} = E[(a - \mu_a)(b - \mu_b)]$, the (a, b)-th element of Σ, is the covariance value between variables a and b (with both of them having zero mean). From (2), we can see that the conditional mutual information is a monotone increasing function of the squared partial correlation coefficient. Hence, in the following, we use partial correlation coefficient instead of the conditional mutual information as the security and privacy metric. Hence, the corresponding max-min and min-max values for a given Gaussian tree $T = (V, E, W)$ can be restated as:

$$\begin{aligned} S_M(T, W) &= \max_{\{a,b\}} \min_z \rho^2_{(ab|z,T,W)} \\ S_m(T, W) &= \min_z \max_{\{a,b\}} \rho^2_{(ab|z,T,W)} \end{aligned} \tag{3}$$

which will be used to compare and order different trees.

III. Topological Properties of Gaussian Trees

A. Structural Properties of the Triplet (a, b, z) in Both Max-Min and Min-Max Problems

Generally, to determine the security performance of a given Gaussian graphical model, we should solve both min-max and max-min cases, over all possible triplets (a, b, z). For Gaussian trees, however, we show in Lemma 1 that this large search space shrinks to a very small space, in which the triplet (a, b, z) should have certain structural relationships.

Lemma 1: For any Gaussian tree $T = (V, E, W)$,

1) *The max-min value* $S_M(T, W)$ *is chosen from those set of triplets in which a and b are adjacent, and z is adjacent to either a or b [8].*
2) *The min-max value* $S_m(T, W)$ *is chosen from those set of triplets in which the node z is any internal (non-leaf) node, while a and b pick two adjacent nodes from the remaining vertices.*

Proof: See Appendix A. ∎

As expected, using Lemma 1 we can narrow down the large number of possible choices for both max-min and min-max cases to small subsets. Using Lemma 1 we can further simplify (2) and deduce the following formula for the squared partial correlation coefficient,

$$\rho^2_{ab|z} = \frac{\sigma^2_{ab}\sigma^2_{bz} - \sigma^2_{ab}\sigma_{bb}\sigma_{zz}}{\sigma^2_{ab}\sigma^2_{bz} - \sigma_{aa}\sigma^2_{bb}\sigma_{zz}} \tag{4}$$

Note that in (4) we implicitly assumed b is on the path from a to z, hence if in any case a lies in between b and z, then a and b should be switched in (4).

B. Pruning and Grafting Edges in Gaussian Trees

One simple way to produce all trees of given order is to begin with any arbitrary structure and move one of its leaf edges to somewhere else, in order to obtain new structures. Note that this method may result in many *isomorphic* (redundant) tree structures, which should be eliminated from the list. In particular, consider the trees shown in Figure 1. Tree T_2 is obtained from T_1 by moving the edge e; we call this particular operation as *pruning and grafting* (PG) operation. In other words, we prune the edge e from the node n_1 and graft it to the node v', to obtain T_2. For Gaussian trees, we formally define the PG operation as follows:

Definition 2: Consider a Gaussian tree $T_1 = (V, E_1, W_1)$ *shown in Figure 1. The pruning and grafting (PG) operation refers to cutting the leaf edge e from* n_1 *and attaching it to some other node, namely,* v', *to obtain the Gaussian*

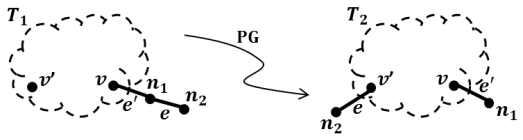


Fig. 1. Pruning and grafting operation performed on edge e in tree T_1.

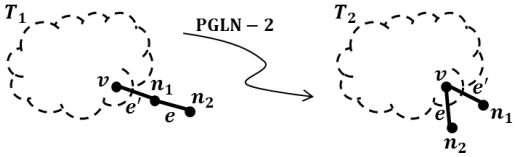


Fig. 2. T_2 is obtained from T_1 by PGLN-2 operation.

tree $T_2 = (V, E_2, W_2)$. Note that W_1 is any arbitrary set of edge-weights, and W_2 is obtained from W_1 by changing the covariance values associated with the altered edge. In particular, in PG operation we assume all the covariance values (including all the variances) in the covariance matrix remain unchanged, except those values that are related to the altered node, namely, n_2.

Note that since in PG operation we essentially only move the edge e to some other place, all other structures shown in Figure 1 (including everything in the clouds) remain unchanged. As a result, it is reasonable to assume that all the variances (including $\sigma_{n_2n_2}$) remain the same; also all the covariance elements except those values that are related to the altered edge remain unchanged. In particular, let us define $\sigma_{v_in_2}$ and $\sigma'_{v_in_2}$ as the covariance values between any node $v_i \in V\backslash n_2$ in T_1 and T_2, respectively. Then in general $\sigma_{v_in_2} \neq \sigma'_{v_in_2}$, for all $v_i \in V\backslash n_2$. The other elements in both covariance matrices corresponding to the Gaussian trees T_1 and T_2 are equal. In Lemma 2, whose proof can be found in [16], we show how to compute these altered covariances for a new tree.

Lemma 2: Consider any Gaussian tree $T = (V, E, W)$, with order $|V| = n$. We denote $|\Sigma_T|$ as the determinant of covariance matrix corresponding to T. Considering the PG operation shown in Figure 1, which transforms the Gaussian tree T_1 into T_2, with $|\Sigma_{T_1}| = |\Sigma_{T_2}|$. Let us denote $\sigma_{n_1n_2}$ and $\sigma'_{v'n_2}$ as the covariance values between the pairs (n_1, n_2) and (v', n_2) in trees T_1 and T_2, respectively; then we have $\sigma^2_{n_1n_2}/\sigma_{n_1n_1} = \sigma'^2_{v'n_2}/\sigma_{vv}$.

In the next sections, we discuss the importance of such results in determining the security performance of different Gaussian trees.

C. Pruning and Grafting Certain Leaf Edges in Gaussian Trees

In [13], Patra and Lal propose an operation called *grafting* to order trees based on their *algebraic connectivity*, which is the second smallest eigenvalue (λ_2) of the Laplacian matrix. Here, we introduce a new operation on Gaussian trees to obtain the ordering among different structures. We specify this operation as *pruning and grafting of leaf with neighbor of degree* 2 (PGLN-2). We show that by PGLN-2 one can change the security performance of Gaussian trees.

Definition 3: Consider a Gaussian tree $T_1 = (V, E_1, W_1)$ shown in Figure 2. The PGLN-2 operation refers to cutting the edge e and attaching it to the other end of its parent edge, i.e., e', to obtain the Gaussian tree $T_2 = (V, E_2, W_2)$. In fact, we can interpret PGLN-2, as a particular operation $\phi(.)$ acting on edge e in T_1, to produce the tree T_2, i.e., $\phi(T_1, e) = T_2$. Note that all the constraints regarding covariance values given in Definition 2 also hold in this case.

Note that $\phi(.)$ is not an *injective* mapping, since there might be two distinct edges (with their neighbors having degree of 2), say $e, e' \in E_1$ that $\phi(T_1, e)$ is isomorphic to $\phi(T_1, e')$. Also, by Lemma 2 we can conclude that $\sigma^2_{n_1n_2}/\sigma_{n_1n_1} = \sigma'^2_{vn_2}/\sigma_{vv}$. We have the following Lemma, whose proof can be found in Appendix B.

Lemma 3: Consider the Gaussian trees shown in Figure 2, where $T_2 = \phi(T_1, e)$. Note that W_1 is any arbitrary set of edge-weights, and W_2 is obtained from W_1 (by changing the covariance values associated with the altered edge). Suppose the max-min values for T_1, and T_2 are $S_M(T_1, W_1)$ and $S_M(T_2, W_2)$, respectively. Also, $S_m(T_1, W_1)$ and $S_m(T_2, W_2)$ are the corresponding min-max values for T_1 and T_2, respectively. We have $S_M(T_1, W_1) \geq S_M(T_2, W_2)$ and $S_m(T_1, W_1) \geq S_m(T_2, W_2)$.

Intuitively, for the max-min case using PGLN-2 operation on the edge e we are essentially adding another neighbor to the node n_2, hence giving more options to the eavesdropper to choose the best location to attack, resulting in smaller max-min values. On the other hand, although in the min-max case z cannot choose n_1 anymore (since it became a leaf), it can choose the node v (which has a higher degree now), thereby decreasing the number of possible choices for the pair (a, b). As we can see from Lemma 3, for any given Gaussian tree structure, the PGLN-2 operation always decreases both max-min and min-max values of the resulting Gaussian tree. As a result, this specific operation generates a certain ordering of Gaussian trees, in which the corresponding structures are ordered with regard to their respective max-min and min-max values. In the following, we formally define the tree ordering using the results obtained in Lemma 3,

Definition 4: Consider the trees $T_1 = (V, E_1, W_1)$ and $T_2 = (V, E_2, W_2)$, where $T_2 = \phi(T_1, e)$, for some leaf edge $e \in E_1$ that has a neighbor with degree two. We know from Lemma 3 that $S_M(T_1, W_1) \geq S_M(T_2, W_2)$ and $S_m(T_1, W_1) \geq S_m(T_2, W_2)$. In this setting, we write $T_1 \succeq T_2$, where the binary relation " $\succeq$ " shows the ordering of these trees, i.e., T_1 is more secure than T_2.

As we will see shortly, the ordering defined in Definition 4 leads to an interesting concept: we can define several *classes* for all Gaussian trees, and each class is a particular poset of distinct Gaussian trees.

While from Lemma 3 one may anticipate that any general PG operation results in less secure Gaussian trees, in the following proposition whose proof can be found in [16], we show that this is not the case.

Proposition 1: Consider the trees shown in Figure 1. Given a Gaussian tree $T_1 = (V, E_1, W_1)$, if we perform

PG operation on the edge e to obtain the Gaussian tree $T_2 = (V, E_2, W_2)$, where $v' \neq v$. Then, in general $T_1 \not\succeq T_2$, i.e., T_1 is not always more favorable than T_2.

From Proposition 1 we can see that if two trees are not related through one or more PGLN-2 operations, then in general they cannot be ordered using our defined binary relation. In fact, without assigning a specific covariance matrix to each Gaussian tree, these structures cannot be consistently compared. This motivates us to search for certain structures that cannot be compared with each other, and at the same time they cannot be improved further, using PGLN-2 operation. In particular, we form sets of Gaussian tree structures, where each set contains a unique leader that is the most favorable topology among all topologies in the same set. Other topologies in a poset might be comparable/incomparable with each other. By classifying the trees into certain sets we can further study both their topological and algebraic properties.

D. Forming the Posets of Gaussian Trees

Based on the obtained results in Proposition 1 and Lemma 3 we can form posets [17] of Gaussian trees. Each poset is formed from its most favorable (MF) structure, $T_M = (V, E_M, W_M)$. In other words, T_M is the poset leader acting as the *ancestor* to all other Gaussian trees in the same poset, i.e., all other Gaussian trees can be obtained from T_M using one or more PGLN-2 operations (composition of several $\phi(.)$ functions). Also, in each poset given two trees T and T', they are adjacent if $T' = \phi(T, e)$, for the leaf edge $e \in E(T)$ that is connected to the a node having degree of two. Note that by Definitions 2 and 3, via the PGLN-2 operation only the covariance values regarding to the altered node will be changed, while the determinant of the covariance matrix corresponding to the trees remain the same. Hence, all trees in the same poset have a fixed determinant for their corresponding covariance matrices. Moreover, in Lemma 4, whose proof can be found in [16] we show the uniqueness of LF structures in each poset.

Lemma 4: In any poset with a given $T_M = (V, E_M, W_M)$ acting as a poset leader, we can find a unique least favorable (LF) structure, $T_L = (V, E_L, W_L)$, which acts as a descendant to all other trees.

Hence, we observe that our defined posets are certain classes of posets, which have a unique MF and LF structures. Also, from the results in Lemma 3 we know that T_M has the most secure structure, while T_L has the least secure structure in each poset. As an example, Figure 3 shows all six posets of Gaussian trees on 8 nodes. The posets consist of several unlabeled trees. Each poset consists of several Gaussian trees, and while such trees are weighted and consequently labeled, we consider them as being unlabeled. This is because by considering labeled trees, we are producing Gaussian trees (with isomorphic unlabeled structures) capturing different joint densities but with exactly the same security performance, making the obtained trees redundant. In Figure 3, the MF and LF structures are placed at the top and bottom of each poset, respectively. Note that in this figure, posets 1, 2, 3 and 6 are the special cases where posets are basically formed as

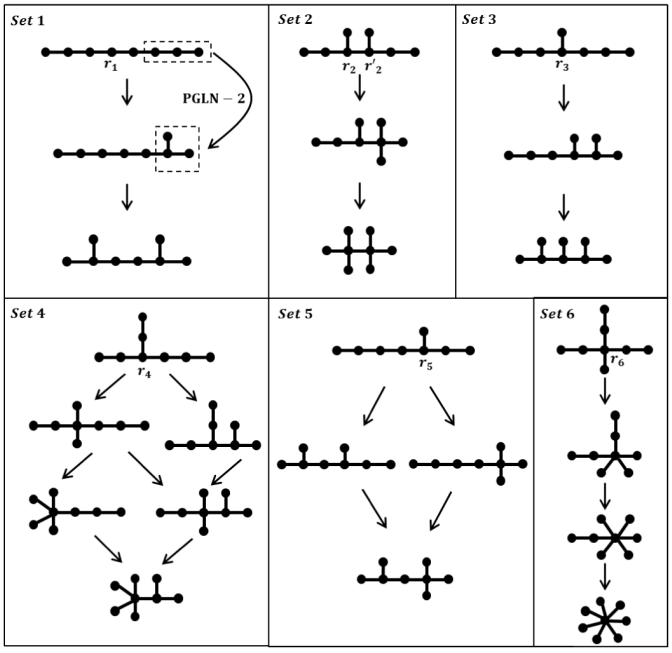


Fig. 3. All the possible posets for Gaussian trees with $n = 8$ nodes.

fully ordered sets, hence any tree structure in each of these posets can be compared to other trees in the same poset, through one or more PGLN-2 operations. On the other hand, in each of the posets 4 and 5 there are some structures that cannot be compared using the rules given in Lemma 3. Note that beginning from any tree and performing several PGLN-2 (or performing reverse PGLN-2) we can obtain all other trees in the same poset. However, if we begin from MF structure, then by performing only PGLN-2 (and not its reverse) we can produce all other structures in the poset. In other words, the MF structures, acting as the poset leaders, can fully describe the poset structure. On the other hand, we also know that the MF topologies are the most secure trees in each poset. Hence, finding such structures is of huge importance, and there should be a method to systematically obtain these topologies. Thus, in section IV, we propose an efficient algebraic approach to enumerate all these structures systematically.

E. Directed Super-Graph Corresponding to Each Poset

From now on, for the simplicity of notations we call the leaf edges that are connected to a node with degree two as *special leaf edges*. Figure 3 gives us an intuition in order to construct a directed super-graph containing Gaussian trees. In particular, each poset can be converted into a directed super-graph $G = (V_s, E_s)$, where V_s is the set of trees in a poset acting as vertices, and E_s is the set of directed edges between the two nodes that can be related using PGLN-2. Using this super-graph, we can easily identify the comparable tree structures: If there is a directed path between two structures, then they are comparable. Hence, we can conclude that both MF and LF structures can be compared with any other tree in a poset. For example, in Figure 3, in posets 1, 2, 3, and 6 there is a directed path between any tree structure so all the trees are comparable with each other, making each poset a fully

ordered set. On the other hand, in posets 4 and 5 there are certain trees with no directed path between them, making such structures incomparable with each other under Lemma 3 conditions. In each poset, the MF structure has the maximum number of special leaf edges, while the LF structure has none of such edges. Also, observe that the poset leader fully characterizes the structure of its super-graph. In particular, the number of those special leaf edges in MF structure specifies the *length* (number of consecutive grafting operations plus 1) of the super-graph. Moreover, the structure of those special leaf edges specifies the *width* of the super-graph. For example, in Figure 3 we can see that the poset 2 has two special leaf edges, hence the super-graph has length 3. Also, since these special leaf edges are fully *symmetric* with respect to each other (performing PGLN-2 operation on either of those edges, results in an isomorphic tree structure), the poset 2 becomes fully ordered. On the other hand, in poset 5 because of the two *asymmetric* special leaf edges we obtain two different topologies in the next level. Roughly speaking, if those special edges become more symmetric, the poset tends to become fully ordered.

Although converting each poset to its corresponding super-graph simplifies the comparison between tree topologies in a set, as it can be observed, for larger trees identifying these special branches and ordering trees by grafting operation becomes more challenging. Hence, in the following, we aim to study the tree structures and their associated posets in a more abstract and general way.

IV. Algebraic Properties of Gaussian Trees

A. Tutte-Like Polynomials for Gaussian Trees in Posets

In this section, in order to model the Gaussian trees and the corresponding posets more systematically, we study the algebraic properties of these models. As we may see in the following, these properties will further help us characterize the special leaf edges, and thus allow us to evaluate the security robustness of any tree structure within a poset. To achieve this goal, for each tree, we associate a two-variable *Tutte-like* polynomial defined in [6], where Chaudhary and Gordon modify the definition of the Tutte polynomial to obtain a new invariant for both rooted and unrooted trees. Also, they proved that this polynomial uniquely determines rooted trees. For unrooted trees however, it is shown in [18] that certain classes of caterpillars have the same polynomials assigned to them. However, interestingly, we prove that in each poset, in many cases the trees have unique polynomials.

Let $R(T)$ denote the collection of all subtrees of T, and $L_E(S)$ denote the leaf edges in the subtree S, i.e., the edges that are connected to leaf nodes, then we have [6],

$$f_E(T;t,z)=\sum_{S\subseteq R(T)} t^{|E(S)|}(z+1)^{|E(S)|-|L_E(S)|} \tag{5}$$

where $|E(S)|$ is the total number of edges in the subtree S. Note that z used in (5), is completely irrelevant to the random variable z used in the previous sections. Basically, this polynomial is a generating function that encodes the number of subtrees with a given internal and leaf edges [18]. We next show that such polynomials can help us systematically generate trees in a poset from the poset leader. The proof can be found in [16].

Lemma 5: Suppose there is a directed path from the tree T_n to T_{n-m} in a poset, i.e., T_{n-m} can be obtained from T_n through m PGLN-2 operations. Then, their associated polynomials have the following recursive relationship,

$$f(T_n;t,z)=f(T_{n-m};t,z)+t(1-tz)[m-\sum_{k=1}^{m} g_{n-k}(t,z)] \tag{6}$$

where, $g_{n-k}(t,z)$ is the polynomial associated with the rooted tree obtained from the tree T_{n-k}, after deleting the special leaf edge e and its neighbor edge e' (e.g., see e and e' shown in Figure 2 for the tree T_1), in a given step k, and putting their common node as a root (e.g., the node v in Figure 2). Note that in (6)*, $T_{n-(n-1)}=T_1$ becomes the LF topology.*

Using the recursive equation derived in (6), we then have the following corollary, whose proof is in Appendix C.

Corollary 1: In a poset, if one of the following cases happens then two polynomials corresponding to the trees are distinct: (1) If there exists a directed path between two trees; (2) If both trees have the same parent tree; (3) If the two structures lie at different levels (stages) in the super-graph.

Hence, by Corollary 1, we see that although Tutte-like polynomial is not graph invariant in general, in many cases the polynomials associated with trees in a same poset are distinct. As an example, consider the poset 5 shown in Figure 3. Since all trees satisfy at least one of the conditions in Corollary 1, all of their associated polynomials are thus distinct. Following (5), we have

$$\begin{aligned}
f(T_M;t,y)&=t^7y^4+t^6(y^4+2y^3)+t^5(3y^3+2y^2)\\
&\quad+t^4(4y^2+2y)+t^3(6y+1)+7t^2+7t+1\\
f(T_l;t,y)&=t^7y^3+t^6(3y^3+y^2)+t^5(2y^3+4y^2)\\
&\quad+t^4(5y^2+3y)+t^3(6y+2)+8t^2+7t+1\\
f(T_r;t,y)&=t^7y^3+t^6(3y^3+y^2)+t^5(3y^3+3y^2+y)\\
&\quad+t^4(4y^2+3y+1)+t^3(5y+4)+9t^2+7t+1\\
f(T_L;t,y)&=t^7y^2+5t^6y^2+t^5(8y^2+y)+t^4(6y^2+4y+1)\\
&\quad+t^3(5y+5)+10t^2+7t+1
\end{aligned} \tag{7}$$

where T_M and T_L are the MF and LF structures in poset 5, respectively. Also, T_l and T_r are the left and right structures, respectively that located in the middle of poset 5. For the simplicity of polynomials we replaced $z+1$ with y. As we expected, all the computed polynomials in (7) are distinct.

The Tutte-like polynomial can be used to evaluate certain topological properties of trees. In the following lemma, whose proof is in [16], we propose an interesting result: the Tutte-like polynomial can enable us to obtain the exact number of special leaf edges in the corresponding tree. Hence, using this result we estimate the security robustness of a tree structure by computing its distance from LF structure.

Lemma 6: Given the polynomial $f(T;t,z)$ associated with a tree T having $|I|$ internal edges, the second highest degree term has the form $t^{|E|-1}(\alpha(1+z)^{|I|-1}+\beta(1+z)^{|I|})$.

The coefficient α shows the number of leaf edges, which are connected to a node with degree two.

Corollary 2: The coefficient α defined in Lemma 6 shows the distance between the tree T and LF structure. Also, if $\alpha = 0$ then T is the LF structure.

Example 1: Consider the tree topologies in poset 5 of Figure 3, and their associated polynomials that are computed in (7). The MF tree T_M has two special leaf edges, hence in its corresponding polynomial, the second highest degree term has the form $t^6(y^4 + 2y^3)$. Hence, $\alpha = 2$. The two middle trees in the same poset, each have one special leaf edge, and in this case we have $t^6(3y^3 + y^2)$ for both second highest degree terms, in which $\alpha = 1$. On the other hand, the LF tree T_L has no such leaf edges. From (7) we can see the second highest degree term for $f(T_L; t, y)$ is $5t^6y^2$, hence $\alpha = 0$.

The results obtained in Lemma 6 and Corollary 2 show a strong correlation between the Tutte-like polynomial and security robustness of a Gaussian tree. In particular, being closer to LF structure, hence having smaller values for α (comparing to others in the same poset), makes the Gaussian tree less favorable comparing to other structures in the same poset.

B. Enumerating Poset Leaders: Restricted Integer Partition Approach

In the previous sections, we studied certain properties of tree topologies in the same poset. In this section, we find a systematic method to generate different poset leaders, which is further related to *restricted* integer partition problems. The following example will demonstrate new ways to quickly enumerate these MF structures. First consider the following example:

Example 2: Consider the MF structure in poset 5 shown in Figure 3. For a moment, picture the node r_5 as a junction to three *branches*. In particular, these branches are chain structures each having 1, 2, and 4 nodes (excluding r_5), hence we assign the string $(1 + 2 + 4)$ to this topology. Note that, each summand in a partition is also called a *part*, e.g., here the parts are 1, 2, and 4. Here, we name r_5 as the *anchor* node to this MF structure. Similarly, in poset 3 and 4 having anchor nodes r_3 and r_4, respectively; we can assign the strings $(1 + 3 + 3)$ and $(2 + 2 + 3)$ to these structures. The MF structure in the poset 6 has four branches that come out of the anchor node r_6. Therefore, we can assign $(1+2+2+2)$ to this structure. Next, consider the MF topology in poset 1. This is a special case (i.e., an integer partition having two parts), where any internal node can be an anchor node. Here, we arbitrarily choose r_1 as the anchor node, hence obtaining $(3 + 4)$ for this structure. However, one can choose other internal nodes to obtain equivalent partitions such as $(2 + 5)$ or $(1 + 6)$. Note that in all MF structures above we have only one anchor node, hence all the parts in each string sums up to $|V| - 1 = 8 - 1 = 7$. Lastly, consider the MF structure in poset 2. Here, there are two anchor nodes r_2 and r_2', each having two branches with lengths 1 and 2. Therefore, the integer partition is separated into two sections, i.e., $(1 + 2) + (1 + 2)$, where each section corresponds to one anchor node. In this case since we have two anchor nodes, the parts sum up to $|V| - 2 = 6$.

Algorithm 1 Enumerating Poset Leaders

```
Input: n, as the order of Gaussian trees
Output: P, as the list of all poset leaders
P ← ∅
for A := 1 to A_max do
    Given n − A, find the subset of all AIPs
    P_A = {p_1, p_2, ..., p_{m_A}} each having A parts;
    for i := 1 to m_A do
        Find those parts in p_i that can be further
        partitioned to obtain new and AIPs and add them
        to P_A;
    end
    Check for any permutation of parts that gives a new
    AIP and add them to P_A;
    Check for redundant AIPs in P_A and eliminate them
    from the list;
    P ← P ∪ P_A;
end
```

Based on this example, we propose an effective algorithm to enumerate all poset leaders of a given order. As we anticipate, integer partition methods [7] can be very helpful in order to quickly reach this goal. However, this method should be systematically implemented. In particular, we use *restricted* integer partitions to find all poset leaders. Each integer partition should satisfy the following constraints: (1) Each section should have at most a single 1; (2) The parts in the leftmost (first) and rightmost (last) sections should each sum up to values larger than or equal to 3. Essentially, the first constraint is to ignore the non-poset leader cases, while the second constraint is to ignore the cases where two or more sections can be merged and form already produced sections, hence, making this method more effective. In this case, the partitions that satisfy the above constraints are defined to be *acceptable integer partitions* (AIP). Algorithm 1, effectively finds the list of all AIPs corresponding to poset leaders of given order n:

Here A shows the number of anchor nodes; and $A_{\max}$ can be determined by combining the two aforementioned constraints. In particular, given $|V| = n$ as the order of trees, then $A_{\max} = n - (3 + 3) = n - 6$. For example, each of the MF structures shown in Figure 3 have only one anchor node, except the MF structure in poset 2 that has two anchor nodes, and we know in this case $A_{\max} = 2$. Also, note that unlike normal integer partitions the position of parts matters, so we should count some of permutations of different parts. In particular, two non-isomorphic poset leader topologies may have identical integer partitions, but with different ordering of parts.

Figure 4 shows two different permutations of integer partitions for $n = 12$. As we can see from the figure, these two structures are non-isomorphic, but they have the same parts and sections. Also, observe that both integer partitions sum up to $(1+2)+(0)+(1)+(1+3) = (1+2)+(1)+(0)+(1+3) = 8$,

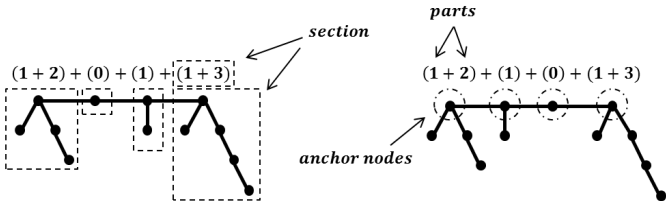


Fig. 4. Two different structures of poset leaders on $n = 12$ nodes.

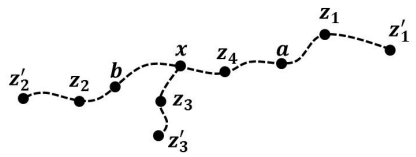


Fig. 5. All the possible locations for the eavesdropper given the fixed correlates.

since based on the algorithm we do not count the anchor nodes (here there are 4 of them) in the partitions.

V. Conclusion

In this paper, we studied the problem of comparing security performance of Gaussian trees in both max-min and min-max scenarios. First, we introduced the PGLN-2 operation to obtain a partial ordering among such trees. The poset of Gaussian trees is defined as equivalence classes containing certain Gaussian trees that can be transformed into each other using one or more PGLN-2 operations. Also, each poset consists of unique MF and LF structures with the best and worst security performances, respectively. Second, we assigned a polynomial to each Gaussian tree, and showed that using such polynomials one can estimate the relative security performance of a Gaussian tree with respect to other structures within the same poset. We also obtained an effective approach, based on restricted integer partitions, to enumerate the MF structures.

Appendix A
Proof of Lemma 1

First, consider the max-min case, in which Alice and Bob choose a pair of nodes, under the pessimistic assumption that Eve chooses the best possible node to minimize the conditional mutual information $I(a; b|z)$. Figure 5 shows all the possible cases that a particular eavesdropper can take, in a fixed path between the nodes a and b. In other words, Eve may pick any node z_1, z_1', z_2, z_2', z_3, z_3' or z_4. Note that there might be several edges on a path between any pair of nodes.

We use the results provided in Theorem 1 and Theorem 2, which are proposed in [5, pp. 348–349]. Essentially, Theorem 1 is a conditional version of the well-known information inequality and holds in general for mutual information of any distribution [15]. Intuitively, for the Gaussian trees the condition in Theorem 1 is satisfied when b lies on the path between a and b', where b' is the alternative choice for Bob. In other words, the longer path implies weaker dependence. On the other hand, Theorem 2 holds in general for the Gaussian joint density. The first part of Theorem 2 shows that if a, b, and z are pairwise separated given x, then conditioning always reduces the mutual information between a and b. In Gaussian trees, the second part of the Theorem 2 shows that for the fixed correlates a and b, the eavesdropper z wants to be closer to the path between them.

From Figure 5 we can see that there are totally four possible choices for Eve: When z is connected to the path p_{ab} through one of the nodes a or b; when z is connected to p_{ab} through the node x; and when z lies on the path between a and b.

Recall that the objective is to find the value for z that minimizes the mutual information between a and b: $\min_z I(a; b|z)$.

Cases 1 and 2: When z is along the path p_{ab}, i.e., the case z_1 or z_2: First, consider the case z_1, the analysis for z_2 is exactly the same. From Theorem 1 we know that because $a \perp z_1'|z_1$ we have: $I(b; z_1) \geq I(b; z_1')$. Now we want to compare two values for the mutual information. First, observe that $b \perp z_1|a$. So we can conclude that $I(b; a, z_1) = I(b; a)$. The same condition holds for z_1': $I(b; a, z_1') = I(b; a)$.

$$\begin{aligned} & I(b; z_1) > I(b; z_1') \\ & \quad \rightarrow I(b; a) - I(b; z_1) < I(b; a) - I(b; z_1') \\ & \quad \rightarrow I(b; a, z_1) - I(b; z_1) < I(b; a, z_1') - I(b; z_1') \\ & \quad \rightarrow I(b; a|z_1) < I(b; a|z_1') \end{aligned} \tag{8}$$

Eq. (8) shows that $I(a; b|z_1) \leq I(a; b|z_1')$. In other words, the eavesdropper wants to be as close as possible to the path p_{ab}.

Case 3: Now consider the case when z is a branch node, i.e., it is connected to p_{ab} through the node x: It is obvious that by replacing z_3 with z and z_3' with z' in the Theorem 2's conditions, we can satisfy all the constraints in this theorem. Hence, we can conclude that $I(a; b|z_3) \leq I(a; b|z_3')$. Again, we conclude that z wants to be closer to the path p_{ab}.

Case 4: When z lies on the path p_{ab}: In this case it is obvious that $a \perp b|z_4$. As a result we have $I(a; b|z_4) = 0$, which is not desirable choice for a and b.

Next, we find possible cases that maximize the mutual information between a and b, given the fixed node for z. We show that to maximize the conditional mutual information, a and b should be close to each other. Consider the case where Bob has two choices b or b', where b is on the path between b' and Alice's choice a. Then for any given subset of choices Z for Eve, by data processing inequality [15] we have $I(a; b|Z) \geq I(a; b'|Z)$ Hence, we can immediately see that Alice and Bob pick the pair of nodes that are adjacent. Also, it can be argued that if a and b are not adjacent, then the eavesdropper wants to pick the best node: z picks any node on the path p_{ab}. As a result $I(a; b|z)$ becomes zero. This validates the first result in Lemma 1.

Next, consider the min-max case, in which Eve chooses a particular node, assuming that Alice and Bob choose the best pair of nodes to maximize the conditional mutual information $I(a; b|z)$. Similar to the max-min case, observe that regardless of Eve's choice, Alice and Bob choose adjacent nodes, since otherwise based on Theorem 1, $I(a; b|z)$ becomes either zero, or it can be improved further. Furthermore, let us assume that Eve picks a leaf node, say z, which is adjacent to z'. Now, the min-max value for this particular case is computed by $\rho^2_{ab|z} = max_{(a,b)\in E\setminus(z',z)}$. On the other hand, if the eavesdropper picks z', the min-max value becomes $\rho'^2_{ab|z'} = max_{(a,b)\in E\setminus(z',adj(z'))}$, where $adj(z')$ is the set of adjacent

nodes to z', which contains z as well as some other nodes. Hence, using Theorem 2 clearly $\rho'^2_{ab|z'} \leq \rho^2_{ab|z}$ and since Eve chooses the minimum between all possible cases, so it rules out all the leaf nodes. This completes the proof.

Appendix B
Proof of Lemma 3

First, note that since PGLN-2 changes the local structure, most of the parts in both trees T_1 and T_2 shown in Figure 2 remains the same. This in turn results in both max-min values to be equal in many cases. Let us denote the squared partial correlation coefficients for trees T_1 and T_2 as $\rho^2_{ab|z}$ and $\rho'^2_{a'b'|z'}$, respectively, then we have the following cases for the max-min scenario:

1. Suppose in tree T_1, Alice and Bob choose a pair $(a, b) \in E_C(T_1)$, where $E_C(T_1)$ is the set of all edges inside the cloud other than v. Then, according to Lemma 1, Eve chooses z from appropriate nodes in $V_C(T_1)$, i.e., the set of nodes inside the cloud (including v). Now, if $(a', b') \in E_C(T_2)$ then since $E_C(T_2) = E_C(T_1)$ and $V_C(T_2) = V_C(T_1)$, so the max-min values for this case are equal.

2. Suppose in tree T_1, Alice and Bob choose the pair $(a, b) = (x_i, v)$, where $x_i \in adj(v)$ is adjacent to v. Then $z \in \{adj(x_i), n_1\}$. Now, if in T_2 the pair $(a', b') \in (x_i, v)$, then $z' \in \{adj(x_i), n_1, n_2\}$. In T_2, Eve has one more option (i.e., n_2) to choose from, comparing to its choices in T_1, hence we can immediately conclude that for this case $\rho^2_{ab|z} \geq \rho'^2_{a'b'|z'}$.

3. Suppose in T_1, Alice and Bob choose the pair $(a, b) = (v, n_1)$. In this case $z \in \{adj(v), n_2\}$. Now, if in T_2 the pair $(a', b') = (v, n_1)$, then $z' \in \{adj(v), n_2\}$. Now we know $\sigma^2_{n_1n_2}/\sigma_{n_1n_1} = \sigma'^2_{vn_2}/\sigma_{vv}$, then if we replace $\sigma'^2_{vn_2}$ with $\sigma^2_{n_1n_2}\sigma_{vv}/\sigma_{n_1n_1}$ in the equation regarding to $\rho'^2_{vn_1|n_2}$ we can conclude that $\rho^2_{vn_1|n_2} = \rho'^2_{vn_1|n_2}$. As a result, the max-min values for both trees in this case are equal.

4. Suppose in T_1, Alice and Bob choose the pair $(a, b) = (n_1, n_2)$. Then Eve has only one option, which is choosing v. Now, if in T_2, $(a', b') = (v, n_2)$, then $z' \in adj(v)$, where $adj(v)$ consists of the set of vertices inside the cloud, as well as n_1. Now, using similar arguments as in case 3, and by $\sigma^2_{n_1n_2}/\sigma_{n_1n_1} = \sigma'^2_{vn_2}/\sigma_{vv}$, we can show that $\rho^2_{n_1n_2|v} = \rho'^2_{vn_2|n_1}$. Since, in T_2, Eve can choose any z' other than n_2, hence in this case $\rho^2_{ab|z} \geq \rho'^2_{a'b'|z'}$.

Following discussed cases, showing that $T_1 \succeq T_2$ is straightforward: for example, suppose $S_M(T_1, W)$ is chosen from case 1, then if $S_M(T_2, W)$ is chosen from the same case, we know $S_M(T_1, W) = S_M(T_2, W)$. Otherwise, if $S_M(T_2, W)$ is chosen from any other case (let's name this value as $S'_M(T_2, W)$), then since Eve chooses the minimum among the four cases, so $S'_M(T_2, W) \leq S_M(T_2, W) = S_M(T_1, W)$. As another example, suppose $S_M(T_1, W)$ is chosen from case 2, then if $S_M(T_2, W)$ is chosen from the same case, we know $S_M(T_1, W) \geq S_M(T_2, W)$. Otherwise, if the max-min value, say $S'_M(T_2, W)$ is chosen from any other case, using the same arguments $S'_M(T_2, W) \leq S_M(T_2, W) \leq S_M(T_1, W)$. Similar arguments can be used for the remaining cases.

Next, similar to the max-min problem, we can conclude the following cases for the min-max problem:

1. Suppose in T_1, the eavesdropper picks a (non-leaf) node v_c from inside the cloud, where $v_c \in V_C(T_1)$. Then, the possible choices for the pair Alice and Bob are $(a, b) \in \{E_C(T_1), (v, n_1), (n_1, n_2)\}$. If we also assume $z' = v_c$, then $(a', b') \in \{E_C(T_2), (v, n_1), (v, n_2)\}$. We know since $E_C(T_1) = E_C(T_2)$, hence the only difference is the pair $(n_1, n_2) \in E(T_1)$ versus $(v, n_2) \in E(T_2)$. Using the fact that $\sigma^2_{n_1n_2}/\sigma_{n_1n_1} = \sigma'^2_{vn_2}/\sigma_{vv}$ and using (4) it is not hard to show that $\rho^2_{n_1n_2|v_c} \geq \rho'^2_{vn_2|v_c}$ for all $v_c \in V_C(T_1)$. As a result, for this case we have $\rho^2_{ab|z} \geq \rho'^2_{a'b'|z'}$.

2. Suppose in T_1, the eavesdropper picks the node v. Then, for the pair of legitimate nodes we have $(a, b) \in \{E_C(T_1), (n_1, n_2)\}$. If we also assume that $z' = v$, then $(a', b') \in E_C(T_2)$. Now, we know the Alice and Bob want to maximize their security; since in T_1 they have one more option (i.e., (n_1, n_2)) to choose from, therefore for this case again we have $\rho^2_{ab|z} \geq \rho'^2_{a'b'|z'}$.

3. Suppose in T_1, Eve picks the node n_1. Then, $(a, b) \in E_C(T_1)$. Note that in the tree T_2 the node $z' \neq n_1$, since it is a leaf. Hence, again suppose $z' = v$. So, similar to case 2 we know $(a', b') \in E_C(T_2)$. Note that the node z' lies on the path from the pairs (a', b') (inside the cloud in T_2) to n_1. Therefore, using Theorem 2 in [5, p. 349] we conclude that $\rho^2_{ab|z=n_1} \geq \rho'^2_{a'b'|z'=v}$.

Now, we show $T_1 \succeq T_2$: for example, suppose $S_M(T_1, W)$ is chosen from case 1, then if $S_M(T_2, W)$ is chosen from the same case, we know $S_M(T_1, W) \geq S_M(T_2, W)$. Otherwise, if the max-min value, say $S'_M(T_2, W)$ is chosen from the other case (i.e., case 2), since (a, b) in T_1 have chosen the case with maximum value $S_M(T_1, W) \geq \rho^2_{ab|z=n_1}$, where $\rho^2_{ab|z=n_1}$ corresponds to case 3 in T_1. But we know from above that $\rho^2_{ab|z=n_1} \geq \rho'^2_{a'b'|z'=v} = S'_M(T_2, W)$, hence $S_M(T_1, W) \geq S'_M(T_2, W)$. We can use similar arguments for the other cases as well. This completes the proof.

Appendix C
Proof of Corollary 1

First, suppose $f(T_n; t, z) = f(T_{n-m}; t, z)$ then using (6) we should have $t(1 - tz)[m - \sum_{k=1}^{m} g_{n-k}(t, z)] = 0$, or $\sum_{k=1}^{m} g_{n-k}(t, z) = m$. Recall that all $g_{n-k}(t, z)$ are polynomials associated with rooted trees, so the only possibility is $g_{n-k}(t, z) = 1$, for all $1 \leq k \leq m$, a contradiction.

Second, consider two trees T_{n-m} and T_{n-l}, at different levels having nearest common ancestor T_n. Then using (6) we have the following:

$$f(T_n; t, z) = \begin{cases} f^L(T_{n-m}; t, z) + t(1 - tz)[m - \sum_{k=1}^{m} g^L_{n-k}] \\ f^R(T_{n-l}; t, z) + t(1 - tz)[l - \sum_{k=1}^{l} g^R_{n-k}] \end{cases}$$

suppose, $f^L(T_{n-m}; t, z) = f^R(T_{n-l}; t, z)$ then we obtain,

$$\sum_{k=1}^{m} g^L_{n-k} - \sum_{k=1}^{l} g^R_{n-k} = m - l \tag{9}$$

If $m = l = 1$, i.e., both trees T_{n-m} and T_{n-l} are obtained from T_n by a single grafting operation. But, since they have two different structures, the corresponding polynomials for the rooted trees g^L_{n-1} and g^R_{n-1} are distinct, because in [6]

it is shown that Tutte-like polynomial for rooted trees is graph invariant. Hence, $f^L(T_{n-1};t,z)$ and $f^R(T_{n-1};t,z)$ are distinct. So, the trees at the same level that are obtained from their parent through one grafting operation are distinct.

Finally, suppose we have $m \neq l$. Let's define $y_i = g_i - 1$ for all polynomials $g_i(t,z)$. Now, using (9) we have,

$$\sum_{k=1}^{m} y_{n-k}^{L} - \sum_{k=1}^{l} y_{n-k}^{R} = 0 \tag{10}$$

The highest degree term corresponds to the rooted trees resulted by eliminating the edges e and e' and putting the common node between these two edges as a root. Also, the highest degree terms are resulted from the subtrees associated to y_i^L and y_i^R and no other proper subsets of these trees. Hence, from (10) and assuming that original tree T_n has the size $|E|$, then we can conclude,

$$t^{|E|-2}\sum_{k=1}^{m}(1+z)^{L_{n-k}} = t^{|E|-2}\sum_{k=1}^{l}(1+z)^{R_{n-k}} \tag{11}$$

where L_{n-k} and R_{n-k} are non-negative integer powers, which show the largest number of internal edges for each tree associated to polynomials y_{n-k}^L and y_{n-k}^R.

Equation (11) should hold for all values of t and z. Let's set $t = 1$ and $z = 0$, we obtain $m = l$, a contradiction.

REFERENCES

[1] U. M. Maurer, "Secret key agreement by public discussion from common information," *IEEE Trans. Inf. Theory*, vol. 39, no. 3, pp. 733–742, May 1993.

[2] R. Ahlswede and I. Csiszàr, "Common randomness in information theory and cryptography—Part I: Secret sharing," *IEEE Trans. Inf. Theory*, vol. 39, no. 4, pp. 1121–1132, Jul. 1993.

[3] R. Ahlswede and I. Csiszár, "Common randomness in information theory and cryptography—Part II: CR capacity," *IEEE Trans. Inf. Theory*, vol. 44, no. 1, pp. 225–240, Jan. 1998.

[4] M. H. Manshaei, Q. Zhu, T. Alpcan, T. Bacşar, and J.-P. Hubaux, "Game theory meets network security and privacy," *ACM Comput. Surv.*, vol. 45, no. 3, p. 25, Jun. 2013.

[5] S. Chaudhuri, "Qualitative inequalities for squared partial correlations of a Gaussian random vector," *Ann. Inst. Statist. Math.*, vol. 66, no. 2, pp. 345–367, Apr. 2014.

[6] S. Chaudhary and G. Gordon, "Tutte polynomials for trees," *J. Graph Theory*, vol. 15, no. 3, pp. 317–331, Jul. 1991.

[7] G. E. Andrews, *The Theory of Partitions*, vol. 2. Cambridge, U.K.: Cambridge Univ. Press, 1998.

[8] A. Moharrer, S. Wei, G. T. Amariucai, and J. Deng, "Evaluation of security robustness against information leakage in Gaussian polytree graphical models," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, Mar. 2015, pp. 1404–1409.

[9] A. Moharrer, S. Wei, G. T. Amariucai, and J. Deng, "Topological and algebraic properties for classifying unrooted Gaussian trees under privacy constraints," in *Proc. IEEE Global Commun. Conf. (GlobeCom)*, Dec. 2015, pp. 1–6.

[10] S. Sullivant, "Algebraic geometry of Gaussian Bayesian networks," *Adv. Appl. Math.*, vol. 40, no. 4, pp. 482–513, May 2008.

[11] H. Roozbehani and Y. Polyanskiy. (Jan. 2014). "Algebraic methods of classifying directed graphical models." [Online]. Available: http://arxiv.org/abs/1401.5551

[12] P. Šimecek, "Gaussian representation of independence models over four random variables," in *Proc. COMPSTAT Conf.*, 2006, pp. 1–8.

[13] K. L. Patra and A. K. Lal, "The effect on the algebraic connectivity of a tree by grafting or collapsing of edges," *Linear Algebra Appl.*, vol. 428, no. 4, pp. 855–864, Feb. 2008.

[14] P. Csikvári, "On a poset of trees II," *J. Graph Theory*, vol. 74, no. 1, pp. 81–103, Sep. 2013.

[15] T. M. Cover and J. A. Thomas, *Elements of Information*. Hoboken, NJ, USA: Wiley, 2012.

[16] A. Moharrer, S. Wei, G. T. Amariucai, and J. Deng. (2016). "Classifying unrooted Gaussian trees under privacy constraints." [Online]. Available: http://arxiv.org/abs/1504.02530

[17] W. T. Trotter, *Combinatorics and Partially Ordered Sets: Dimension Theory*, vol. 6. Baltimore, MD, USA: The Johns Hopkins Univ. Press, 2001.

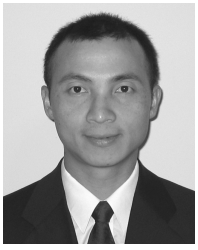
[18] D. Eisenstat and G. Gordon, "Non-isomorphic caterpillars with identical subtree data," *Discrete Math.*, vol. 306, nos. 8–9, pp. 827–830, May 2006.

Ali Moharrer is currently pursuing the Ph.D. degree with the Department of Electrical and Computer Engineering, Louisiana State University, Baton Rouge.

He is also with the Information Sensing, Learning, and Security Laboratory, Louisiana State University. His research interests include information theory and its applications in graphical models and deep learning systems.

Shuangqing Wei received the B.E. and M.E. degrees in electrical engineering from Tsing-hua University, in 1995 and 1998, respectively, and the Ph.D. degree from the University of Massachusetts, Amherst, in 2003. He started his academic career at Louisiana State University (LSU). He is currently a Tenured Associate Professor with the Division of ECE, School of EECS, LSU, and holds the Michael B. Voorhies Distinguished Professorship of Electrical Engineering. His research interests include information theory, statistical inference, communication theory, and their applications in the areas of telecommunication networks and complex systems.

George T. Amariucai received the Ph.D. degree from Louisiana State University, Baton Rouge, in 2009. He is currently an Adjunct Assistant Professor with the Department of Electrical and Computer Engineering, Iowa State University, Ames, IA. His research interests are focused on cyber security and its intersections with information theory, cryptography, wireless networks, social networks, and machine learning.



Jing Deng (S'98–M'02–SM'13) received the B.E. and M.E. degrees in electronics engineering from Tsinghua University, Beijing, China, in 1994 and 1997, respectively, and the Ph.D. degree from the School of Electrical and Computer Engineering, Cornell University, Ithaca, NY, USA, in 2002. He served as a Research Assistant Professor with the Department of Electrical Engineering and Computer Science, Syracuse University, from 2002 to 2004. He visited the Department of Electrical Engineering, Princeton University, and the Department of Electrical and Computer Engineering, WINLAB, Rutgers University, in Fall 2005. He was with the Department of Computer Science, University of New Orleans, from 2004 to 2008. He is an Associate Professor with the Department of Computer Science, The University of North Carolina at Greensboro, Greensboro, NC, USA.

Dr. Deng is an Editor of the IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY. He was a co-recipient of the 2013 Test of Time Award by the ACM Special Interest Group on Security, Audit, and Control. His research interests include wireless network and security, information assurance, mobile ad hoc networks, and social networks.