Perfect Omniscience, Perfect Secrecy and Steiner Tree Packing

S. Nitinawarat and P. Narayan
Department of Electrical and Computer Engineering
and Institute for Systems Research
University of Maryland
College Park, MD 20742, USA
Email: {nitinawa, prakash}@umd.edu

***Abstract*—We consider perfect secret key generation for a "pairwise independent network" model in which every pair of terminals share a random binary string, with the strings shared by distinct terminal pairs being mutually independent. The terminals are then allowed to communicate interactively over a public noiseless channel of unlimited capacity. All the terminals as well as an eavesdropper observe this communication. The objective is to generate a perfect secret key shared by a given set of terminals at the largest rate possible, and concealed from the eavesdropper.**

First, we show how the notion of perfect omniscience plays a central role in characterizing perfect secret key capacity. Second, a multigraph representation of the underlying secrecy model leads us to an efficient algorithm for perfect secret key generation based on maximal Steiner tree packing. This algorithm attains capacity when all the terminals seek to share a key, and, in general, attains at least half the capacity. Third, when a single "helper" terminal assists the remaining "user" terminals in generating a perfect secret key, we give necessary and sufficient conditions for the optimality of the algorithm; also, a "weak" helper is shown to be sufficient for optimality.

I. Introduction

Given a collection of terminals $\mathcal{M} = \{1, \ldots, m\}$, suppose that every pair i, j of terminals, $1 \leq i < j \leq m$, share a random binary string of length e_{ij} (bits), with the strings shared by distinct pairs of terminals being mutually independent. Then all the terminals are allowed to communicate interactively in multiple rounds over a public noiseless channel of unlimited capacity, with all such communication being observed by all the terminals. The main goal is to generate, for a given subset A of the terminals in $\mathcal{M}$, a *perfect secret key* (SK) namely shared uniformly distributed random bits – of the largest size – such that these shared bits are exactly independent of an eavesdropper's observations of the interterminal communication. All the terminals in $\mathcal{M}$ cooperate in generating such a perfect SK for A.

This model for perfect SK generation, hereafter referred to as a "pairwise independent network" (PIN) model, is a specialized version of an earlier PIN model [15], [14], [12]. In the latter, every pair of terminals observe a pair of correlated signals (not necessarily identical as here) that are independent of pairs of signals observed by all other terminal pairs. In [12], we had studied Shannon theoretic SK generation (not in the perfect sense) in the asymptotic limit of large signal observation lengths, and its connection to the combinatorial problem of Steiner tree packing of a multigraph. Leading work on Shannon theoretic SK generation with public communication originated in [6], [7], [1]; see also [2] for related models.

In contrast with [12], the present work bears the essence of "zero-error information theory," and accordingly, we rely on mathematical techniques of a combinatorial nature. Specifically, our emphasis here is on *perfect* SK generation for fixed signal observation lengths as well as for their asymptotic limits. For convenience, we shall continue to refer to our present model as the PIN model. This model possesses the appropriate structure for investigating the concept of perfect SK in which the generated key is exactly recoverable by every terminal in the secrecy seeking set A; is exactly independent of the eavesdropper's observations; and is uniformly distributed. Also, its special structure makes for a new concept of perfect omniscience, which plays a central role. Furthermore, in the spirit of [12], the PIN model reveals points of contact between perfect SK generation and the combinatorial problem of maximal Steiner tree packing of a multigraph. We remark that tree packing has been used in the context of network coding (see, for instance, [13]).

Our three main contributions described below are motivated by a known general connection between (not necessarily perfect) SK generation at the maximum rate and the minimum communication for (not necessarily perfect) omniscience [3], [4], and by the mentioned connection between the former and the combinatorial problem of maximal Steiner tree packing of a multigraph [12].

First, the concept of perfect omniscience enables us to obtain a single-letter formula for the perfect SK capacity of the PIN model; moreover, this capacity is shown to be achieved by linear noninteractive communication, and coincides with the (standard) SK capacity derived in our previous work [12]. This result establishes a connection between perfect SK capacity and the minimum rate of communication for perfect omniscience, thereby particularizing to the PIN model a known general link between these notions *sans* the requirement of the omniscience or secrecy being perfect [3].

Second, the PIN model can be represented by a multigraph. Taking advantage of this representation, we put forth an efficient algorithm for perfect SK generation using a maximal packing of Steiner trees of the multigraph. This algorithm involves public communication that is linear as well as noninteractive, and produces a perfect SK of length equal to the maximum size of such Steiner tree packing. When all the

This manuscript has been submitted to ISIT 2010.

terminals in $\mathcal{M}$ seek to share a perfect SK, the algorithm is shown to achieve perfect SK capacity. However, when only a subset of terminals in $A \subset \mathcal{M}$ wish to share a key, the algorithm can fall short of achieving capacity; nonetheless, it is shown to achieve at least half of it. Additionally, we obtain nonasymptotic and asymptotic bounds on the size and rate of the best perfect SKs generated by the algorithm. *These bounds are of independent interest from a purely graph theoretic viewpoint as they constitute new estimates for the maximum size and rate of Steiner tree packing of a given multigraph.*

Third, a special configuration of the PIN model arises when a lone "helper" terminal m aids the "user" terminals in $A = \mathcal{M}\backslash\{m\}$ generate a perfect SK. This model has two special features: Firstly, (a single) terminal m possesses all the bit strings that are not in A; secondly, a Steiner tree for A is a spanning tree for either A or $\mathcal{M}$. These features enable us to obtain necessary and sufficient conditions for Steiner tree packing to achieve perfect SK capacity, as also a further sufficient condition that posits a "weak" role for the helper terminal m.

Preliminaries and the problem formulation are in Section II. Our results are described in Section III. Their proofs are contained in a recently submitted full-length manuscript [8], but are omitted here.

II. Preliminaries

Suppose that the terminals in $\mathcal{M} = \{1, \ldots, m\}$, $m \geq 2$, observe, respectively, n independent and identically distributed (i.i.d.) repetitions of the rvs $\tilde{X}_1, \ldots, \tilde{X}_m$, denoted by $\tilde{X}_1^n, \ldots, \tilde{X}_m^n$, where $\tilde{X}_i^n = \left(\tilde{X}_{i,1}, \ldots, \tilde{X}_{i,n}\right)$, $i \in \mathcal{M}$. We shall be concerned throughout with a PIN model $\tilde{X}_1, \ldots, \tilde{X}_m$ [14], defined by each rv $\tilde{X}_i$, $i \in \mathcal{M}$, being of the form $\tilde{X}_i = (X_{ij},\ j \in \mathcal{M}\backslash\{i\})$ with $m-1$ components, and the "reciprocal pairs" of rvs $\{(X_{ij}, X_{ji}),\ 1 \leq i < j \leq m\}$ being mutually independent. We assume further that $X_{ij} = X_{ji}$, $1 \leq i \neq j \leq m$, where X_{ij} is uniformly distributed over the set of all binary strings of length e_{ij} (bits). Thus, every pair of terminals is associated with a random binary string that is independent of all other random binary strings associated with all other pairs of terminals. The assumption is tantamount to every pair of terminals i, j sharing at the outset privileged and pairwise "perfect secrecy" of e_{ij} bits. Following their observation of the random sequences as above, the terminals in $\mathcal{M}$ are allowed to communicate among themselves over a public noiseless channel of unlimited capacity; all such public communication, which maybe interactive and conducted in multiple rounds, is observed by all the terminals. A communication from a terminal, in general, can be any function of its observed sequence as well as all previous public communication. The public communication of all the terminals will be denoted collectively by $\mathbf{F} = \mathbf{F}^{(n)}$.

Definition 1: The communication $\mathbf{F}$ is termed *linear noninteractive communication* (LC) if $\mathbf{F} = (F_1, \ldots, F_m)$ with[1] $F_i = L_i \tilde{X}_i^n$, where L_i is a $b_i \times \left(\sum_{j \neq i} n\, e_{ij}\right)$ matrix[2] with $\{0,1\}$-valued entries, $i = 1, \ldots, m$. The integer $b_i \geq 0$, $i = 1, \ldots, m$, represents the length (in bits) of the communication F_i from terminal i; the overall communication $\mathbf{F}$ has length $\sum_{i=1}^{m} b_i$ (bits).

The primary goal is to generate shared perfect secret common randomness for a given set $A \subseteq \mathcal{M}$ of terminals at the largest rate possible, with the remaining terminals (if any) cooperating in secrecy generation. The resulting perfect secret key must be accessible to every terminal in A; but it need not be accessible to the terminals not in A and nor does it need to be concealed from them. It must, of course, be kept perfectly secret from the eavesdropper that has access to the public interterminal communication $\mathbf{F}$, but is otherwise passive, i.e., unable to tamper with this communication.

The following basic concepts and definitions are adapted from [3], [4]. For rvs U, V, we say that U is *perfectly recoverable* from V if $Pr\{U = f(V)\} = 1$ for some function $f(V)$. With the rvs K and $\mathbf{F}$ representing a secret key and the eavesdropper's knowledge, respectively, information theoretic *perfect secrecy* entails that the security index[3]

$$\begin{aligned} s(K;\mathbf{F}) &= \log|\mathcal{K}| - H(K) + I(K \wedge \mathbf{F}) \\ &= \log|\mathcal{K}| - H(K|\mathbf{F}) \ = \ 0, \end{aligned} \qquad (1)$$

where $\mathcal{K}$ is the range of K and $|\ \boldsymbol{.}\ |$ denotes cardinality. This requirement simultaneously renders K to be uniformly distributed and independent of $\mathbf{F}$.

Definition 2: Given any set $A \subseteq \mathcal{M}$ of size $|A| \geq 2$, a rv K is a *perfect secret key* (SK) for the set of terminals A achievable with communication $\mathbf{F}$, if K is perfectly recoverable[4] from $\left(\tilde{X}_i^n, \mathbf{F}\right)$ for each $i \in A$ and, in addition, it satisfies the perfect secrecy condition (1).

Definition 3: A number R is an *achievable perfect SK rate* for a set of terminals $A \subseteq \mathcal{M}$ if there exist perfect SKs $K^{(n)}$ for A achievable with appropriate communication, such that

$$\frac{1}{n}\log|\mathcal{K}^{(n)}| \to R \quad \text{as} \quad n \to \infty,$$

where $\mathcal{K}^{(n)}$ is the range of $K^{(n)}$. The largest achievable perfect SK rate is the perfect SK capacity $C(A)$.

Thus, by definition, the perfect SK capacity for A is the largest rate of a rv that is perfectly recoverable at each terminal in A from the aggregate information available to it, and is uniformly distributed and concealed from an eavesdropper with access to the public interterminal communication; it need not be concealed from the terminals in $A^c = \mathcal{M}\backslash A$, which cooperate in secrecy generation. The notion of perfect SK capacity is more stringent than that of SK capacity under the requirements of the key being asymptotically recoverable for each $i \in A$ and the security index tending to 0, both as $n \to \infty$; in particular, now the security index must equal zero

[1] All additions and multiplications are modulo 2.

[2] It is assumed that $\sum_{j \neq i} e_{ij} \geq 1$, $\ i = 1, \ldots, m$.

[3] All logarithms are to the base 2.

[4] The extra requirement of perfectness in recoverability is not a limiting factor for the PIN model in contrast with other models of SK generation.

for all sufficiently large n. The latter SK capacity for the PIN model has been characterized in [9], [10], [12].

A central role is played by the notion of *perfect omniscience* which is a strict version of the concept of *omniscience* introduced in [3]. *This notion does not involve any secrecy requirements*.

Definition 4: The communication $\mathbf{F}$ is *communication for perfect omniscience* for A if $(\tilde{X}_1^n, \ldots, \tilde{X}_m^n)$ is perfectly recoverable from $(\tilde{X}_i^n, \mathbf{F})$ for every $i \in A$. Further, $\mathbf{F}$ is *linear noninteractive communication for perfect omniscience* (LCO$^{(n)}(A)$) if $\mathbf{F}$ is an LC and satisfies the previous perfect recoverability condition. The minimum length (in bits) of an LCO$^{(n)}(A)$, i.e., $\min_{\text{LCO}^{(n)}(A)} \sum_{i=1}^m b_i$, will be denoted by LCO$_m^{(n)}(A)$. The *minimum rate* of LCO$^{(n)}(A)$ is $OMN(A) \triangleq \limsup_n \frac{1}{n}\text{LCO}_m^{(n)}(A)$.

III. Results

Before stating our results, we mention that Theorem 1 (with proof outline) and a preliminary version of Theorem 2 (and Corollary) appeared in [11]. Yet we present Theorem 1 here to place in context our subsequent new results. Also, Theorem 2 is now stated in its new and complete form.

A. Perfect SK Capacity for the PIN Model

Our first main contribution is a (single-letter) characterization of the perfect SK capacity for the PIN model, which brings forth a connection with the minimum rate of communication for perfect omniscience.

Theorem 1 [11]: *The perfect SK capacity for a set of terminals $A \subseteq \mathcal{M}$ is*

$$C(A) \ = \ \sum_{i,j} e_{ij} \ - \ OMN(A) \tag{2}$$

where

$$OMN(A) \ = \ \min_{(R_1,\ldots,R_m) \ \in \ \mathcal{R}(A)} \ \sum_{i=1}^{m} R_i, \tag{3}$$

with

$$\mathcal{R}(A) = \left\{ \begin{array}{c} (R_1, \ldots, R_m) \in \mathbb{R}^m : \ R_i \geq 0, \ i = 1, \ldots, m, \\ \sum_{i \in B} R_i \ \geq \ \sum_{1 \leq i < j \leq m, \ i \in B, \ j \in B} e_{ij}, \\ \forall B \not\supseteq A, \ \emptyset \neq B \subset \mathcal{M} \end{array} \right\}. \tag{4}$$

Furthermore, this perfect SK capacity can be achieved with linear noninteractive communication.

Remarks: (i) Clearly, the perfect SK capacity, by definition, cannot exceed the (standard) SK capacity studied in [9], [12]. Indeed, Theorem 1 implies that the latter is attained by a perfect SK.

(ii) In the same vein, the minimum rate of communication for (asymptotic) omniscience [3] can be attained for the PIN model with perfect recoverability at A of $(\tilde{X}_1^n, \ldots, \tilde{X}_m^n)$ for all n sufficiently large, and with linear noninteractive communication. We mention that noninteractive communication, without a claim of linearity, was shown to suffice for (asymptotic) omniscience in [3].

B. Maximal Steiner Tree Packing and Perfect SK Generation

Theorem 1 serves to establish the sufficiency of an LC in achieving perfect SK capacity through the intermediate attainment of perfect omniscience for A. However, decoding is by exhaustive search of prohibitive complexity.

The PIN model can be represented by a multigraph. This representation leads us to an efficient algorithm for perfect SK generation, not necessarily through perfect omniscience, by a maximal packing of Steiner trees of the multigraph. In particular, this algorithm entails public communication in the form of an LC. On the other hand, such an algorithm based on maximal Steiner tree packing need not attain perfect SK capacity. The size of the largest perfect SK that is thus generated can be estimated in terms of the minimum length of an LCO$^{(n)}(A)$.

Definition 5: A *multigraph* $G = (V, E)$ with vertex set V and edge set E is a connected undirected graph with no selfloops and with multiple edges possible between any pair of vertices. Given $G = (V, E)$ and a positive integer n, let $G^{(n)} = \big(V, E^{(n)}\big)$ denote the multigraph with vertex set V and edge set $E^{(n)}$ wherein every vertex pair is connected by n times as many edges as in E; in particular, $G^{(1)} = G$. Furthermore, $|E^{(n)}|$ will denote the total number of edges in $E^{(n)}$.

To the PIN model $\tilde{X}_1, \ldots, \tilde{X}_m$ (cf. section II), we can associate a multigraph $G = (\mathcal{M}, E)$ with $\mathcal{M} = \{1, \ldots, m\}$ and the number of edges connecting a vertex pair (i, j) in E equal to e_{ij}; in particular, the edge connecting (i, j) will be associated with the random binary string X_{ij}.

By this association, it will be convenient to represent (3) and (4) as

$$OMN_G(A) \ = \ \min_{(R_1,\ldots,R_m) \ \in \ \mathcal{R}_G(A)} \ \sum_{i=1}^{m} R_i, \tag{5}$$

with

$$\mathcal{R}_G(A) = \left\{ \begin{array}{c} (R_1, \ldots, R_m) \in \mathbb{R}^m : \ R_i \geq 0, \ i = 1, \ldots, m, \\ \sum_{i \in B} R_i \geq \ \sum_{1 \leq i < j \leq m, \ i \in B, \ j \in B} \ e_{ij}, \\ \forall B \not\supseteq A, \ \emptyset \neq B \subset \mathcal{M} \end{array} \right\}, \tag{6}$$

whereupon (2) can be restated as

$$C(A) \ = \ |E| - OMN_G(A). \tag{7}$$

Furthermore, it is easy and useful to note that for every $n \geq 1$,

$$OMN_{G^{(n)}}(A) \ = \ nOMN_G(A). \tag{8}$$

Definition 6: For $A \subseteq V$, a *Steiner tree* (for A) of $G = (V, E)$ is a subgraph of G that is a tree, i.e., containing no cycle, and whose vertex set contains A; such a Steiner tree is said to *cover* A. A *Steiner tree packing* of G is any collection of edge-disjoint Steiner trees of G. Let $\mu(A, G)$ denote the *maximum* size of such a packing (cf. [5]). The *maximum* *rate* of Steiner tree packing of G is $\lim_{n\to\infty}\frac{1}{n}\mu(A,G^{(n)})$. When $A=V$, a Steiner tree becomes a *spanning tree*, with corresponding notions of *spanning tree packing*, maximum size and rate.

Given a PIN model, the notion of Steiner tree packing of the associated multigraph leads to an efficient algorithm for constructing an LCO$^{(n)}(A)$ and thereby generating a perfect SK. The next Theorem 2 indicates that the largest size of a perfect SK that the algorithm generates is the maximum size of the Steiner tree packing. Furthermore, Theorem 2 and its corollary, and Theorem 5 provide nonasymptotic and asymptotic bounds on the size and rate, respectively, of the best perfect SKs generated by the algorithm. *Of independent interest from a purely graph theoretic viewpoint, these results also constitute new bounds for the maximum size and rate of Steiner tree packing of a given multigraph.*

Theorem 2: *For the multigraph $G=(\mathcal{M},E)$ associated with a PIN model and for $A\subseteq\mathcal{M}$, it holds for every $n\geq 1$ that*

(i) *the terminals in $\mathcal{M}$ can devise an LCO$^{(n)}(A)$ of total length $n|E^{(1)}|-\mu(A,G^{(n)})$ and subsequently generate a perfect SK $K^{(n)}$ with $\log|\mathcal{K}^{(n)}|=\mu(A,G^{(n)})$;*

(ii) $$\mu(A,G^{(n)}) \;\leq\; n|E^{(1)}|-LCO_m^{(n)}(A); \tag{9}$$

(iii) *furthermore, $LCO_m^{(n)}(A)$ is bounded below by the value of an integer linear program according to*

$$LCO_m^{(n)}(A) \;\geq\; INT_{G^{(n)}}(A)$$

where

$$INT_{G^{(n)}}(A) \;=\; \min_{(I_1,\ldots,I_m)\,\in\,\mathcal{I}_{G^{(n)}}(A)} \;\sum_{i\,=\,1}^{m} I_i, \tag{10}$$

with

$$\mathcal{I}_{G^{(n)}}(A) \;= \left\{\begin{array}{c} (I_1,\ldots,I_m)\,\in\,\mathbb{Z}^m:\; I_i\geq 0,\; i=1,\ldots,m, \\ \sum_{i\,\in\,B} I_i \;\geq\; n\,\sum_{1\leq i<j\leq m,\; i\in B,\; j\in B}\; e_{ij}, \\ \forall B\not\supseteq A,\; \emptyset\neq B\subset\mathcal{M} \end{array}\right\}. \tag{11}$$

Corollary 3: *For every $n\geq 1$, the maximum size of Steiner tree packing of a multigraph $G^{(n)}$ satisfies*

$$\mu(A,G^{(n)}) \;\leq\; n\;|E^{(1)}|-INT_{G^{(n)}}(A), \tag{12}$$

with equality when $A=\mathcal{M}$.

Remarks: (i) Note that the bounds in Theorem 2 are nonasymptotic, i.e., valid for every n. Also, note in the bound in Theorem 2 (ii) for $\mu(A,G^{(n)})$ that LCO$_m^{(n)}(A)$ is defined in terms of its *operational significance.*

(ii) Further, Theorem 2 provides a nonasymptotic *computable* lower bound for LCO$_m^{(n)}(A)$ in terms of an integer linear program. The optimum value of its linear programming relaxation constitutes a further lower bound which equals $OMN_{G^{(n)}}(A)=nOMN_G(A)$, by (8).

Next, we turn to connections between perfect SK capacity $C(A)$ and the maximum rate of Steiner tree packing of $G=(\mathcal{M},E)$.

Theorem 4: *For the multigraph $G=(\mathcal{M},E)$ associated with the PIN model and for $A\subseteq\mathcal{M}$, it holds that*

$$\frac{1}{2}C(A) \;\leq\; \lim_{n\to\infty}\frac{1}{n}\mu(A,G^{(n)}) \;\leq\; C(A). \tag{13}$$

Furthermore, when $A=\mathcal{M}$,

$$\lim_{n\to\infty}\frac{1}{n}\mu(\mathcal{M},G^{(n)}) \;=\; C(\mathcal{M}). \tag{14}$$

Remarks: (i) For the PIN model with m terminals, every Steiner tree has at most $m-1$ edges. Also, from (13), $\mu(A,G^{(n)}) \lesssim nC(A)$ for all large n. Hence, the overall complexity of the perfect SK generation algorithm based on Steiner tree packing is linear (in n).

(ii) The upper bound on $\lim_{n\to\infty}\frac{1}{n}\mu(A,G^{(n)})$ in Theorem 5 is not tight, in general, as seen by an example in [8].

C. The Single Helper Case

As observed in the previous Remark (ii), the maximum rate of Steiner tree packing can fail to achieve perfect SK capacity. A natural question that remains open is whether the maximum rate of Steiner tree packing equals perfect SK capacity for the special case of the PIN model in which a lone "helper" terminal m assists the "user" terminals in $A=\{1,\ldots,m-1\}$ generate a perfect SK. In this section, we provide partial answers.

First, we derive necessary and sufficient conditions for the maximum rate of Steiner tree packing to equal perfect SK capacity in (13) and, analogously, the (nonasymptotic) maximum size of Steiner tree packing to meet its upper bound in (12). These conditions entail the notion of a *fractional* multigraph. Throughout this section, we shall assume that $A=\{1,\ldots,m-1\}\subset\mathcal{M}=\{1,\ldots,m\}$.

Definition 7: Given a multigraph $G=(\mathcal{M},E)$ as in Definition 5, a *fractional multigraph* $\tilde{G}=(A,\tilde{E})$ in A (with vertex set A) has edge set $\tilde{E}=\{\tilde{e}_{ij}\in\mathbb{R},\ 0\leq\tilde{e}_{ij}\leq e_{ij},\ 1\leq i<j\leq m-1\}$. For any such $\tilde{G}$, the *complementary fractional multigraph* $G\backslash\tilde{G}=(\mathcal{M},E\backslash\tilde{E})$ has vertex set $\mathcal{M}$ and edge set $E\backslash\tilde{E}\triangleq\{e_{ij}-\tilde{e}_{ij},\ 1\leq i<j\leq m-1;\ e_{im},\ 1\leq i\leq m-1\}$. The definitions of $\mathcal{R}_G(A)$ in (6) and $OMN_G(A)$ in (5) have obvious extensions to $\tilde{G}$ and $G\backslash\tilde{G}$ as well. Further, (8) also holds for $\tilde{G}$ and $G\backslash\tilde{G}$.

Theorem 5: *For the multigraph $G=(\mathcal{M},E)$ associated with the PIN model,*

(i)

$$\lim_{n\to\infty}\frac{1}{n}\mu(A,G^{(n)}) \;=\; C(A) \tag{15}$$

iff

$$OMN_G(A)=\min_{\tilde{G}}\; OMN_{\tilde{G}}(A)+OMN_{G\backslash\tilde{G}}(\mathcal{M}), \tag{16}$$

where the minimum is over all fractional multigraphs $\tilde{G} = (A, \tilde{E})$ in A;

(ii)

$$\mu(A, G^{(n)}) = |E| - INT_G(A)$$

iff

$$INT_G(A) = \min_{\tilde{G}_I} \; INT_{\tilde{G}_I}(A) + INT_{G \backslash \tilde{G}_I}(\mathcal{M}), \qquad (17)$$

where the minimum is over all multigraphs $\tilde{G}_I = (A, \tilde{E})$ for which $\tilde{E}$ consists of only integer-valued $\tilde{e}_{ij}$s.

The proof of Theorem 5 relies on the fact that for the PIN model with a single helper terminal m, a Steiner tree for A is a spanning tree for either A or $\mathcal{M}$. We decompose the multigraph $G = (\mathcal{M}, E)$ into fractional multigraphs $\tilde{G} = (A, \tilde{E})$ and $G \backslash \tilde{G} = (\mathcal{M}, E \backslash \tilde{E})$ in such a manner that maximal spanning tree packings of them, taken together, constitute a maximal Steiner tree packing for A of G. Recall from (14) in Theorem 4 that maximal spanning tree achieves, in effect, the prefect SK capacity of the corresponding secrecy model.

Our final result provides another sufficient condition for the maximum rate of Steiner tree packing to equal perfect SK capacity. Recall from Theorem 1 that, in general, perfect SK capacity for A can be attained with public communication that corresponds to the minimum communication for perfect omniscience. If the latter can be accomplished with the sole helper terminal m communicating "sparingly," then it transpires that maximal Steiner tree packing attains the best perfect SK rate. An analogous nonasymptotic version of this claim also holds. Heuristically, a sufficient "weak" role of the helper terminal m turns the Steiner tree packing of A, in effect, into a spanning tree packing of A.

Let $d_i \triangleq \sum_{j \neq i} e_{ij}$ denote the degree of vertex $i, \; i \in \mathcal{M}$. Clearly, any $(R_1^*, \ldots, R_m^*)$ (resp. $(I_1^*, \ldots, I_m^*)$) that attains the minimum corresponding to $OMN_G(A)$ (cf. (5)) (resp. $INT_G(A)$ (cf. (10))) must satisfy $R_i^* \leq d_i$ (resp. $I_i^* \leq d_i$), $i = 1, \ldots, m$.

Theorem 6: *For the multigraph $G = (\mathcal{M}, E)$ associated with the PIN model,*

(i) *if there exists $(R_1^*, \ldots, R_m^*)$ that attains $OMN_G(A)$ (cf. (5)) with $R_m^* \leq d_m/2$, then*

$$\lim_{n \to \infty} \frac{1}{n} \mu(A, G^{(n)}) \; = \; C(A) \; = \; |E| - OMN_G(A).$$

(ii) *if there exists $(I_1^*, \ldots, I_m^*)$ that attains $INT_G(A)$ (cf. (10)) with $I_m^* \leq \lfloor d_m/2 \rfloor$, then*

$$\mu(A, G) \; = \; |E| - INT_G(A).$$

The idea of the proof of Theorem 6 is as follows. If G has more than one vertex in A connecting to m, say $u, v \in A$, we "split off" the edges (u, m) and (v, m) by communicating publicly the modulo two sum of two bits, one corresponding to each edge. This creates a shared secure bit between u, v. The associated "reduced" multigraph $G^{uv} = (\mathcal{M}, E^{uv})$ is obtained by reducing e_{um} and e_{vm} each by unity and increasing e_{uv} by unity, all in G. It then follows that the maximum number of perfect SK bits attainable in G is always bounded below by that in G^{uv}. Furthermore, a Steiner tree packing of G^{uv} is always a similar packing of G. The condition (ii) guarantees that such a reduced multigraph always retains the maximum number of achievable SK bits, and that such a reduction can be performed repeatedly until the role of the helper terminal m becomes redundant at which point spanning tree packing is optimal. The proof of (i) follows by applying (ii) to $G^{(n)} = (\mathcal{M}, E^{(n)})$ and taking appropriate limits.

Acknowledgements

The authors thank Chunxuan Ye, Alexander Barg and Alex Reznik for very helpful discussions. The work of S. Nitinawarat and P. Narayan was supported by the National Science Foundation under Grants CCF0515124, CCF0635271, CCF0830697 and InterDigital.

References

[1] R. Ahlswede and I. Csiszár, "Common randomness in information theory and cryptography, Part I: Secret sharing," *IEEE Trans. Inform. Theory*, vol. 39, pp. 1121-1132, July 1993.

[2] I. Csiszár and P. Narayan, "Common randomness and secret key generation with a helper," *IEEE Trans. Inform. Theory*, vol. 46, pp. 344-366, March 2000.

[3] I. Csiszár and P. Narayan, "Secrecy capacities for multiple terminals," *IEEE Trans. Inform. Theory*, vol. 50, pp. 3047-3061, December 2004.

[4] I. Csiszár and P. Narayan, "Secrecy capacities for multiterminal channel models," *Special Issue of the IEEE Trans. Inform. Theory on Information Theoretic Security*, vol. 54, pp. 2437-2452, June 2008.

[5] M. Grötschel, A. Martin and R. Weismantel, "Packing Steiner trees: A cutting plane algorithm and computational results," *Mathematical Programming*, vol. 72, pp. 125-145, February 1996.

[6] U. M. Maurer, "Provably secure key distribution based on independent channels," presented at the *IEEE Workshop Inform. Theory*, Eindhoven, The Netherlands, June 1990.

[7] U. M. Maurer, "Secret key agreement by public discussion from common information," *IEEE Trans. Inform. Theory*, vol. 39, pp. 733-742, May 1993.

[8] S. Nitinawarat and P. Narayan, "Perfect Omniscience, Perfect Secrecy and Steiner Tree Packing," *IEEE Trans. Inform. Theory*, submitted.

[9] S. Nitinawarat, C. Ye, A. Barg, P. Narayan and A. Reznik, "Secret key generation for a pairwise independent network model," *Proceedings of the IEEE International Symposium on Information Theory*, pp. 1015-1019, Toronto, Ontario, Canada, July 2008.

[10] S. Nitinawarat, C. Ye, A. Barg, P. Narayan and A. Reznik, "Common randomness, multiuser secrecy and tree packing," *Proceedings of the 46th Annual Allerton Conference on Communication, Control, and Computing*, Monticello, IL, September 2008.

[11] S. Nitinawarat, C. Ye, A. Barg, P. Narayan and A. Reznik, "Perfect Secrecy, Perfect Omniscience and Steiner Tree Packing," *Proceedings of the IEEE International Symposium on Information Theory*, pp. 1288-1292, Seoul, Korea, June-July, 2009.

[12] S. Nitinawarat, C. Ye, A. Barg, P. Narayan and A. Reznik, "Secret key generation for a pairwise independent network model," *IEEE Trans. Inform. Theory*, submitted.

[13] Y. Wu, K. Jain and S.-Y. Kung, "A unification of network coding and tree-packing (routing) theorems," *IEEE Trans. Inform. Theory*, vol. 52, pp. 2398-2409, June 2006.

[14] C. Ye and A. Reznik, "Group secret key generation algorithms," *Proceedings of the IEEE International Symposium on Information Theory*, pp. 2596-2600, Nice, France, June 2007.

[15] C. Ye, A. Reznik and Y. Shah, "Extracting secrecy from jointly Gaussian random variables," *Proceedings of the IEEE International Symposium on Information Theory*, pp. 2593-2597, Seattle, USA, July 2006.