On the Secret Key Capacity of the Harary Graph PIN Model

Navin Kashyap† Manuj Mukherjee† Yogesh Sankarasubramaniam‡

***Abstract*—A pairwise independent network (PIN) model consists of pairwise secret keys (SKs) distributed among m terminals. The goal is to generate, through public communication among the terminals, a group SK that is information-theoretically secure from an eavesdropper. In this paper, we study the Harary graph PIN model, which has useful fault-tolerant properties. We derive the exact SK capacity for a regular Harary graph PIN model. Lower and upper bounds on the fault-tolerant SK capacity of the Harary graph PIN model are also derived.**

I. Introduction

The problem of secret key (SK) generation in a multiterminal setting was put into an information-theoretic framework by Csiszár and Narayan [2]. A special case of their framework is the *pairwise independent network (PIN)* model [5], [6], specified by a graph G with vertex set $\mathcal{V}$, with $|\mathcal{V}|= m$, and edge set $\mathcal{E}$. The vertices of the graph are referred to as *terminals*. Each pair of terminals that is connected by an edge $e \in \mathcal{E}$ is assumed to share a *pairwise secret key*, which is a random variable B_e^n consisting of $n \geq 1$ iid copies of a random bit B_e uniformly distributed over $\{0,1\}$. For each $e \in \mathcal{E}$, the rv B_e^n is jointly independent of the rvs $(B_{e'}^n, e' \in \mathcal{E} \setminus \{e\})$ The terminals are allowed to communicate interactively in multiple rounds over a noiseless public communications channel of unlimited capacity, with all communications being observed by all terminals. The goal is for all terminals, or perhaps only some subset, to agree upon a *group secret key* of largest size, namely, b uniformly distributed random bits, with b as large as possible. Each terminal should be able to generate the group SK from its own observations, namely, the pairwise SKs it shares with its neighbours and the public communication. It is required that the group SK be independent of the public communication. This is, of course, to provide security against an eavesdropper who can listen in on the public communication.

Nitinawarat and Narayan [5] determined the *secret key capacity*, i.e., the largest group SK rate b/n, as $n \to \infty$, for the PIN model described above. They also gave an efficient algorithm, based on tree packings, for group SK generation. The algorithm was shown to achieve SK capacity in the case when all terminals are required to generate the group SK.

Tyagi *et al.* [8] studied group SK generation and SK capacity in a scenario where an arbitrary t-subset of the m terminals may drop out before the communication needed for SK generation is completed. They formulated various notions of *fault-tolerant secret key (FTSK) capacity*, which we elaborate upon in Section II, and showed that for a PIN model on the complete graph on m vertices, these notions of fault-tolerant capacity coincide. They also gave a simple noninteractive communication protocol, again based on tree packings, for FTSK generation, which achieved the FTSK capacity for the complete graph PIN model.

In the complete graph PIN model, every pair of terminals shares a pairwise SK, so that there are $\binom{m}{2}$ pairwise SKs in all. A natural question that arises is: if we only have a limited number of pairwise SKs available, what is the best way to distribute them among the m terminals so that the resulting PIN model has a large FTSK capacity?

The connectivity properties of a graph play a significant role in determining the fault-tolerant behaviour of the corresponding PIN model. Tyagi *et al.* [8] showed that if a graph has vertex connectivity[1] greater than t, then one bit of group SK can always be generated in the associated PIN model even when an arbitrary t-subset of the terminals drops out. Thus, a PIN model with good fault-tolerant properties can be obtained by distributing the pairwise SKs in such a way as to maximize the vertex connectivity of the underlying graph. Equivalently, for a target vertex connectivity, it is desirable to minimize the number of edges (pairwise SKs) required to obtain a graph with the required vertex connectivity. It is known that the *Harary graph* $\mathbf{H}_{k,m}$ [4] has the least number of edges among all graphs on m vertices with vertex connectivity equal to k. In this paper, we study the SK capacity and FTSK capacity of PIN models obtained from Harary graphs.

The rest of the paper is structured as follows. Section II contains definitions and relevant background material. Section III deals with the capacity of the Harary graph PIN model, while Section IV studies its fault-tolerant behaviour.

II. Definitions and Preliminaries

In this section, we introduce the definitions and notation used in the paper, and review some basic graph-theoretic results and prior work on the PIN model.

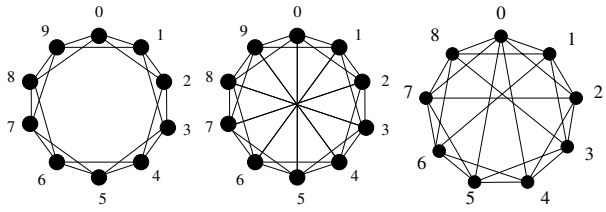
A. Graph-Theoretic Preliminaries

Given a graph $G = (\mathcal{V}, \mathcal{E})$ and an integer $n \geq 1$, we denote by $G^{(n)}$ the multigraph having the same vertex set $\mathcal{V}$ as G,

† N. Kashyap and M. Mukherjee are with the Department of Electrical Communication Engineering, Indian Institute of Science, Bangalore. Email: {nkashyap,manuj}@ece.iisc.ernet.in.

‡ Y. Sankarasubramaniam is with Hewlett-Packard Labs India, Bangalore. Email: yogesh@hp.com.

[1] See Section II for a definition.



(a) $m = 10$, $k = 4$ (b) $m = 10$, $k = 5$ (c) $m = 9$, $k = 5$

Fig. 1: Examples of the three types of Harary graphs $\mathbf{H}_{k,m}$.

but whose edge set $\mathcal{E}^{(n)}$ is the multiset consisting of n copies of each edge of G.

The *vertex (resp. edge) connectivity* of a connected graph G is the least number of vertices (resp. edges) that need to be removed from G so that the remaining graph is disconnected. We denote the vertex connectivity and edge connectivity of G by $\kappa(G)$ and $\lambda(G)$, respectively. By convention, $\kappa(K_m) = m-1$, where K_m is the complete graph on m vertices. It is well known that $\kappa(G) \leq \lambda(G)$ (see e.g., [3, Corollary 5.1.5]).

Theorem 1 ([3], Prop. 5.2.6, Thm. 5.2.7)**.** *An m-vertex graph with vertex or edge connectivity k has at least $\lceil \frac{km}{2} \rceil$ edges.*

We describe here a construction of graphs which achieve the lower bound of the above theorem. These graphs are called *Harary graphs*, in acknowledgement of their original construction by Harary [4]. The Harary graph $\mathbf{H}_{k,m}$ is a graph with m vertices, $\lceil \frac{km}{2} \rceil$ edges, and vertex and edge connectivity both equal to k. It is constructed on $\mathcal{V} = \{0, 1, \ldots, m-1\}$ as follows [3, Chapter 5, pp. 226–227]:

- m *even,* $k = 2r$: connect vertices i and j by an edge iff $(i-j) \bmod m \leq r$.
- m *even,* $k = 2r+1$: connect vertices i and j by an edge if $(i-j) \bmod m \leq r$; add the edges $(i, \frac{m}{2}+i)$ for $0 \leq i \leq \frac{m}{2} - 1$.
- m *odd,* $k = 2r+1$: connect vertices i and j by an edge if $(i-j) \bmod m \leq r$; add the edges $(0, \frac{m-1}{2})$, $(0, \frac{m+1}{2})$, and $(i, \frac{m+1}{2} + i)$ for $1 \leq i \leq \frac{m-3}{2}$.

Figure 1 shows typical examples of the Harary graphs $\mathbf{H}_{k,m}$.

The *spanning tree packing (STP) number*, $\sigma(G)$, of a graph G is the maximum number of edge-disjoint spanning trees that can be packed into the graph. The definition extends to the multigraphs $G^{(n)}$ as well. The following theorem shows that $\sigma(G)$ and $\lambda(G)$ are closely related.

Theorem 2 ([1])**.** $\left\lfloor \frac{\lambda(G)}{2} \right\rfloor \leq \sigma(G) \leq \lambda(G)$.

The next result, known as Menger's theorem, is one of the cornerstones of graph theory.

Theorem 3 ([3], Theorem 5.3.6)**.** *A graph G has $\kappa(G) \geq k$ iff any pair of vertices in G has k internally vertex-disjoint paths between them.*

B. PIN Model Preliminaries

The description here is largely based on [5]. Let $\mathcal{M} = \{0, 1, \ldots, m-1\}$, $m \geq 2$, denote the set of terminals. As described in Section I, a PIN model is specified by a graph $G = (\mathcal{V}, \mathcal{E})$ with $\mathcal{V} = \mathcal{M}$. The edges in $\mathcal{E}$ represent n-bit pairwise SKs shared by terminals. It is somewhat more convenient to use the multigraph $G^{(n)}$ to describe the PIN model, by associating one uniformly random bit B_e with each edge e of $G^{(n)}$. The random bits $(B_e, e \in \mathcal{E}^{(n)})$ are jointly independent. Terminal i observes the random variable (rv) X_i^n, which consists of the random bits B_e associated with the edges e incident on i. For $A \subseteq \mathcal{M}$, we set $X_A^n = (X_i^n, i \in A)$.

The public communication sent by any terminal i is a function of X_i^n and all the previous communication that has already taken place. The public communications channel is assumed to be noiseless. The rv $F_{i,j}$ is associated with the communication sent by terminal i in the jth round of communication. We denote by $\mathbf{F}$ or $\mathbf{F}^{(l)}$ the rv $(F_{1,1}, F_{2,1}, \ldots, F_{m,1}, \ldots, F_{1,l}, \ldots, F_{m,l})$ associated with l rounds of public communication. For $A \subseteq \mathcal{M}$, we set $\mathbf{F}_A^{(l)} = (F_{i,j} : i \in A, 1 \leq j \leq l)$.

An rv U is said to be *perfectly recoverable* from an rv V if there exists a function g such that $Pr[U = g(V)] = 1$. Let $K^{(n)}$ be an rv computed from $X_{\mathcal{M}}^n$. We define the *security index* of $K^{(n)}$ by

$$s(K^{(n)}; \mathbf{F}) = I(K^{(n)}; \mathbf{F}) + \log|\mathcal{K}^{(n)}| - H(K^{(n)}),$$

where $\mathcal{K}^{(n)}$ is the range of $K^{(n)}$, and all logs are base-2.

Definition 1. *For $n \geq 1$, an rv $K^{(n)}$ is said to be a* (perfect) group SK *for $\mathcal{M}$, achievable with communication $\mathbf{F}$, if $K^{(n)}$ is perfectly recoverable from $(X_i^n, \mathbf{F})$ for each $i \in \mathcal{M}$, and $s(K^{(n)}; \mathbf{F}) = 0$.*

Tyagi *et al.* [8] showed that if the underlying graph G is connected, then for $n = 1$, a group SK $K^{(1)}$ consisting of one uniformly random bit is always achievable through a 1-round communication protocol, termed "Protocol 1" in [8]. The following lemma is a compact statement of this fact.

Lemma 4. *Any connected graph yields one bit of group SK.*

Definition 2. *A real number $R > 0$ is said to be an* achievable SK rate *if there exists a sequence of group SKs $(K^{(n)})$ for $\mathcal{M}$, achievable with appropriate communication, such that $\frac{1}{n} H(K^{(n)}) \to R$ as $n \to \infty$. The supremum of all achievable SK rates is called the* SK capacity *for $\mathcal{M}$, denoted by $\mathcal{C}(\mathcal{M})$.*

For notational convenience, given a graph G, we will denote by $\mathcal{C}(G)$ the SK capacity of the PIN model specified by G.

Theorem 5 ([5], Prop. 4 and Theorem 5)**.** *For a graph G, the limit $\lim_{n\to\infty} \frac{\sigma(G^{(n)})}{n}$ exists, and equals $\mathcal{C}(G)$.*

We now introduce fault-tolerance into our definitions of SK rate and capacity. The definitions here are simplified versions, sufficient for the purpose of this paper, of those in [8]. The motivation for these definitions is the event that an arbitrary subset of the m terminals drops out before the group SK generation protocol is completed. Let B denote the set of terminals (the *communicating terminals*) that actually send some communication during the course of the protocol. The

subset $A \subseteq B$ of terminals that ultimately remain (the *residual terminals*) must agree upon a group SK, K, of largest size. There is no requirement that the group SK generated by A be kept secret from the terminals in $\mathcal{M} \setminus A$. We assume that at most $t < m$ terminals may drop out, so that $|A| \geq m - t$.

We are interested in communication protocols that guarantee a certain group SK size (and this guaranteed group SK size must be made as large as possible) *irrespective* of which subset of terminals drops out and when. In this paper, we will consider protocols involving at most two rounds of communication. The terminals that communicate in the first round form the set $B \subseteq \mathcal{M}$. In a 1-round protocol, after the single round of communication, the residual terminals in $A \subseteq B$ must generate an SK. Here, note that the residual terminals would only be aware of the identities of the members of B, and would not know which of these form the subset A. In a 2-rounds protocol, we assume that no terminals drop out after the first round of communication, so that $A = B$. The residual terminals can identify the set A from the communication in the first round, use this knowledge to generate the second round of communication, and finally compute an SK.

Definition 3. *For $l = 1$ and $1 \leq t < m$, a real number $R > 0$ is said to be an achievable (l, t) fault-tolerant secret key (FTSK) rate if $\forall\, \epsilon > 0$, $\exists\, n \geq 1$ s.t. for all (A, B) satisfying $A \subseteq B \subseteq \mathcal{M}$ and $|A| \geq m - t$, we can find an rv $K^{(n)}$ (i.e., an (l, t)-FTSK) with the following properties:*

- *$K^{(n)}$ is perfectly recoverable from $(X_i^n, \boldsymbol{F}_B^{(l)})$ for all $i \in A$;*
- *$s(K^{(n)}; \mathbf{F}_B^{(l)}) = 0$; and*
- *$\frac{1}{n} H(K^{(n)}) > R - \epsilon$.*

The supremum of all achievable (l, t) FTSK rates is called the (l, t) FTSK capacity for $\mathcal{M}$, denoted by $\mathcal{C}^{l,t}(\mathcal{M})$.

For $l = 2$, the same definitions apply, except that B is restricted to be equal to A.

Given a graph G on vertex set $\mathcal{M}$, we will denote by $\mathcal{C}^{l,t}(G)$ the (l, t) FTSK capacity of the PIN model specified by G.

Theorem 6. *For a PIN model specified by a graph G,*

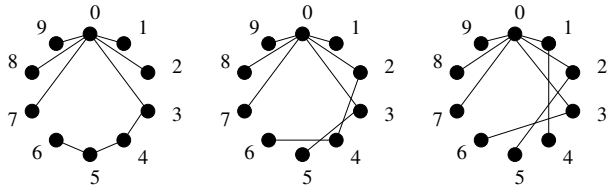
$$\mathcal{C}^{1,t}(G) \leq \mathcal{C}^{2,t}(G) = \min_{A \subseteq \mathcal{M}: |A| \geq m-t} \mathcal{C}(G_A),$$

where G_A is the subgraph of G induced by the vertices in A.

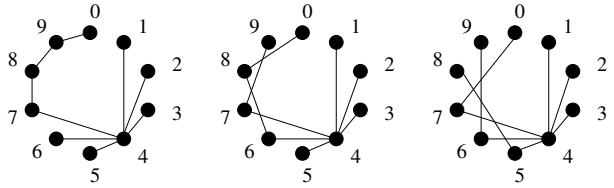
Proof: The first inequality is a straightforward consequence of the definitions, noting that an SK rate of at least $C^{1,t}$ has to be achievable with a 1-round protocol even in the case when $B = A$.

$\mathcal{C}^{2,t}(G) \leq \min_{A:|A| \geq m-t} \mathcal{C}(G_A)$: From the definitions, we have that for any residual set A, $C^{2,t}(G) \leq C'(A)$, where $C'(A)$ denotes the maximum SK rate asymptotically achievable using X_A^n. Now, X_A^n includes pairwise SKs shared between terminals in A and terminals in $\mathcal{M} \setminus A$. Theorem 3 of [2] can be used to show that these pairwise SKs play no role in achieving $C'(A)$, so that $C'(A) = C(G_A)$. Hence, $C^{2,t}(G) \leq C(G_A)$ for any residual set A.

$\mathcal{C}^{2,t}(G) \geq \min_{A:|A| \geq m-t} \mathcal{C}(G_A)$: Let A be a residual set achieving the minimum $\mathcal{C}(G_A)$. Consider a maximal STP of $G_A^{(n)}$. In the second round of communication, we can use Protocol 1 of [8] on each tree comprising the maximal STP to generate 1 bit of group SK (Lemma 4). The $\sigma(G_A^{(n)})$ bits so obtained are all independent as the trees in the packing are edge-disjoint. It follows that an SK rate of $\lim_{n \to \infty} \frac{1}{n} \sigma(G_A^{(n)}) = C(G_A)$ (Theorem 5) is achievable. ■



(a) T_{01}, T_{02}, T_{03}



(b) T_{41}, T_{42}, T_{43}

Fig. 2: Some of the spanning trees in the STP of $\mathbf{H}_{6,10}^{(9)}$ constructed in the proof of Proposition 7.

III. SK Capacity of Regular Harary Graphs

In this section, we derive the SK capacity of a PIN model specified by a regular Harary graph. From the construction of the graphs $\mathbf{H}_{k,m}$ described in Section II-A, it can be seen that $\mathbf{H}_{k,m}$ is regular iff km is even. Throughout this section, we assume that $k < m - 1$. When $k = m - 1$, $\mathbf{H}_{k,m}$ is the complete graph K_m, and it is known that $\mathcal{C}(K_m) = \frac{m}{2}$ [8].

Any spanning tree of a connected graph $G = (\mathcal{V}, \mathcal{E})$ has $|\mathcal{V}| - 1$ edges, from which it easily follows that $\sigma(G) \leq \frac{|\mathcal{E}|}{|\mathcal{V}|-1}$. By extension, $\sigma(G^{(n)}) \leq \frac{n\,|\mathcal{E}|}{|\mathcal{V}|-1}$. Thus, for regular Harary graphs $\mathbf{H}_{k,m}$, we have $\sigma(\mathbf{H}_{k,m}^{(n)}) \leq \frac{nkm}{2(m-1)}$, which is achieved for certain values of n.

Proposition 7. *Let α be a positive integer.*
(a) For k even and $n = \alpha(m-1)$: $\sigma(\mathbf{H}_{k,m}^{(n)}) = \frac{\alpha k m}{2}$.
(b) For k odd, m even, and $n = 2\alpha(m-1)$: $\sigma(\mathbf{H}_{k,m}^{(n)}) = \alpha k m$.

Proof: The proof is by construction of spanning tree packings (STPs) of the required size. It is enough to consider $\alpha = 1$, as for larger integers α, we can simply use α copies of each spanning tree used in the basic construction. Due to space constraints, we only provide the specifics of the construction for the case when k is even. The k odd and m even case requires a different construction.

Let $G = \mathbf{H}_{k,m}$, with k even, and let $n = m - 1$. We wish to construct a STP of $G^{(n)}$ of size $km/2$. The spanning trees in our construction are denoted by $T_{i,j}$, $0 \leq i \leq m-1$ and $1 \leq j \leq k/2$.

For $j \in \{1, \ldots, k/2\}$, the tree $T_{0,j}$ is constructed as follows:

Step 0: Draw the edges $(0, v)$ and $(0, m - v)$ for $v = 1, 2, \ldots, k/2$. Set $p = \frac{k}{2} + 1$.

Step 1: Draw the edges $(m-p, m-p-j), (m-p-j, m-p-2j), \ldots$, till a path from $m-p$ to 0 is formed.
Step 2: Increment p by 1. If there exists a path from $m-p$ to 0, then STOP. Else, go to Step 1.

It is easy to check that the $T_{0,j}$s are spanning trees of G. Figure 2(a) depicts these trees for $\mathbf{H}_{6,10}$.

For $i > 0$, the trees $T_{i,j}$ are "i-step rotations" of $T_{0,j}$. The *i-step rotation* of a graph H with vertex set $\{0, 1, \ldots, m-1\}$ and edge set $\mathcal{E}$ is the graph $\pi^i(H)$ on the same vertex set, but with edge set $\{(\pi^i(u), \pi^i(v)) : (u, v) \in \mathcal{E}\}$, where $\pi^i(z) = z + i \mod m$ for $z \in \{0, 1, \ldots, m-1\}$. Figure 2(b) depicts the 4-step rotations of the trees in Figure 2(a).

It can be verified that the trees $T_{i,j}$ form an STP of $G^{(n)}$; we omit the details. ∎

We can now easily obtain the SK capacity of a regular Harary graph.

Theorem 8. *For a regular Harary graph $\mathbf{H}_{k,m}$, we have*

$$\mathcal{C}(\mathbf{H}_{k,m}) = \frac{km}{2(m-1)}.$$

Proof: By virtue of Theorem 5, we need to determine $\lim_{n\to\infty} \frac{1}{n}\sigma(\mathbf{H}_{k,m}^{(n)})$. By Proposition 7, this limit equals $\frac{km}{2(m-1)}$ for a regular Harary graph $\mathbf{H}_{k,m}$. ∎

We expect that the result of Theorem 8 extends to irregular Harary graphs ($\mathbf{H}_{k,m}$ with both k and m odd), but we do not yet have a result analogous to Proposition 7 for this case.

IV. FTSK Capacity of Harary Graphs

We now turn our attention to the fault-tolerant behaviour of the Harary graph PIN model.

A. Lower bounds

We first derive lower bounds on $\mathcal{C}^{1,t}$ and $\mathcal{C}^{2,t}$ for the Harary graph PIN model.

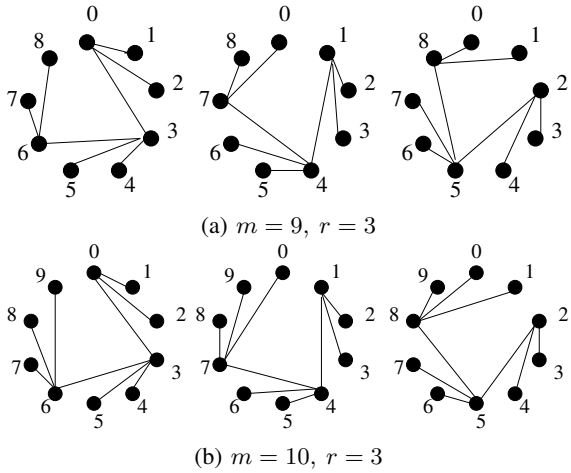
Theorem 9. *Let G be the Harary graph $\mathbf{H}_{k,m}$. For $t < k$,*

$$\mathcal{C}^{2,t}(G) \geq \max\left\{1, \left\lfloor \frac{k-t}{2} \right\rfloor\right\}.$$

Proof: We use the expression for $C^{2,t}(G)$ in Theorem 6. Note that, by Theorem 5, $\mathcal{C}(G_A) = \lim_{n\to\infty} \frac{1}{n}\sigma(G_A^{(n)})$, which is at least $\sigma(G_A)$, since $\sigma(G_A^{(n)}) \geq n\sigma(G_A)$ for all n. Therefore, it is enough to show that for each $A \subset \mathcal{M}$, with $|A| \geq m - t$, we have $\sigma(G_A) \geq \max\left\{1, \lfloor \frac{k-t}{2} \rfloor\right\}$.

Suppose that some subset of at most $t < k$ vertices are removed from G to obtain G_A. Since $\kappa(G) = k$, G_A is still connected, so $\sigma(G_A) \geq 1$. Now, consider any two distinct vertices u and v of G_A. By Theorem 3, in G, there were at least k vertex-disjoint paths between u and v. At least $k - t$ of these paths would have survived in G_A. Thus, again by Theorem 3, $\kappa(G_A) \geq k - t$. Now, use the facts that $\lambda(G_A) \geq \kappa(G_A)$ and $\sigma(G_A) \geq \lfloor \frac{\lambda(G_A)}{2} \rfloor$ (Theorem 2). ∎

Next we turn our attention to $\mathcal{C}^{1,t}$. Lower bounds on $\mathcal{C}^{1,t}(G)$ can be obtained by the following device. Suppose that we can construct an STP, $\{T_1, \ldots, T_r\}$, of G with the property that the removal of any t vertices from G results in at most t of the trees T_j getting disconnected. Then, the remaining (still connected) trees form an STP of size at least $r - t$, of the residual graph G_A. As we explain next, this would imply a 1-round communication protocol that yields an achievable $(1, t)$ FTSK rate $R \geq r - t$, and hence, $C^{1,t}(G) \geq r - t$.



(a) $m = 9,\ r = 3$

(b) $m = 10,\ r = 3$

Fig. 3: The STP construction in the proof of Proposition 10 applied to (a) $\mathbf{H}_{6,9}$ and (b) $\mathbf{H}_{6,10}$.

Let $\{T_1, \ldots, T_r\}$ be an STP of G as above. The terminals in $\mathcal{M}$ prepare to communicate as per Protocol 1 of [8] applied to each of the trees T_j. (If there are no drop-outs, this would generate an r-bit SK for $\mathcal{M}$). Let $B \subseteq \mathcal{M}$ be the subset of terminals that are able to fulfill their obligations under Protocol 1 by sending their communication, and let $A \subseteq B$, $|A| \geq m - t$, be the residual set. Each terminal in A can reconstruct the graph G_B, and determine which of the graphs $T_j(B)$ (subgraph of T_j induced by the vertices in B) remain connected. The connected graphs $T_j(B)$ form an STP of G_B of size at least $r - t$, and so the terminals in A can generate at least $r - t$ bits of group SK. Note that these $r - t$ bits are generated from pairwise SKs of size $n = 1$. Scaling this protocol to an arbitrary $n \geq 1$, we see that an $(1, t)$ FTSK rate $R \geq r - t$ is achievable.

Proposition 10. *Let G be a Harary graph $\mathbf{H}_{k,m}$ with $k = 2r$ or $k = 2r + 1$. Suppose that one of the following holds: (i) $m \mod r \in \{0, 1\}$, or (ii) $r = 3$. Then, $C^{1,t}(G) \geq \max\{1, r-t\}$.*

Proof: Any Harary graph has a Hamiltonian cycle (i.e., a cycle containing all m vertices). So even if one terminal drops out, the remaining part of the Hamiltonian cycle is still connected. Therefore, the protocol implicit in Lemma 4 ensures that an $(1, 1)$ FTSK rate equal to 1 is achievable, and hence $\mathcal{C}^{1,t}(G) \geq 1$.

To prove $C^{1,t}(G) \geq r-t$, we construct an STP of G, of size r, such that each vertex of G is internal to (i.e., is of degree 2 in) at most one tree in the STP. Then, removal of any t vertices from G would result in at most t of the r spanning trees being disconnected.

It is enough to give the construction for $k = 2r$ only. This is because $\mathbf{H}_{2r,m}$ is a subgraph of $\mathbf{H}_{2r+1,m}$, and so, any STP of the former is also an STP of the latter.

Case 1: $m \bmod r = 1$. Write $m = pr + 1$. The first spanning tree ST_1 is obtained by taking the edges $(qr, qr + j)$ for $0 \le q \le p - 1$ and $1 \le j \le r$. For $2 \le i \le r$, the spanning tree ST_i is the $(i-1)$-step rotation of ST_1. Figure 3(b) shows this construction for $m = 10$ and $r = 3$.

Case 2: $m \bmod r = 0$. Write $m = pr$. The first spanning tree ST_1 is obtained by taking the edges described in Case 1 above, *except* for the edge $((p-1)r, pr)$. For $2 \le i \le r$, the spanning tree ST_i is the $(i-1)$-step rotation of ST_1. Figure 3(a) shows this construction for $m = 9$ and $r = 3$.

We omit the somewhat more complicated construction in the remaining case when $r = 3$ (and $m \bmod r = 2$).

It can be verified that in each of the cases above, the trees ST_i, $1 \le i \le r$, form an STP with the required property. ∎

B. Upper bounds

From Theorem 6, we see that for $l = 1, 2$, $\mathcal{C}^{l,t}(G)$ can be bounded above by $\mathcal{C}(G_A)$ for any $A \subseteq \mathcal{M}$ with $|A| \ge m - t$. A careful choice of the subset A can yield good upper bounds.

The upper bounds in this section are obtained for regular Harary graphs, i.e., $\mathbf{H}_{k,m}$ with k even or m even. As before, we call the subgraph of the original graph induced by the terminals in A as G_A. We also use the following notation: let $b = \lfloor \frac{k}{2} \rfloor + 1$, and let $m = pb + d$, $0 \le d < b$. Further, let $t = ap + c$, where $0 \le c < p$ if $0 \le a < b$, and $0 \le c < d$ if $a = b$. Our results can now be stated as follows.

Proposition 11. *(a) For the regular Harary graph $\mathbf{H}_{k,m}$, k even, we have for $t < k$, and $l = 1$ or 2,*

$$\mathcal{C}^{l,t}(\mathbf{H}_{k,m}) \le \min\left\{ k - t, \frac{\frac{km}{2} - |\mathcal{E}_{\mathcal{M}\setminus A}(k)|}{m - t - 1} \right\},$$

where $|\mathcal{E}_{\mathcal{M}\setminus A}(k)|$ is specified in Table I.
(b) For the regular Harary graph $\mathbf{H}_{k,m}$, k odd, we have for $t < k$, and $l = 1$ or 2,

$$\mathcal{C}^{l,t}(\mathbf{H}_{k,m}) \le \min\left\{ k - t, \frac{\frac{km}{2} - |\mathcal{E}_{\mathcal{M}\setminus A}(k-1)| - |\mathcal{E}_\delta|}{m - t - 1} \right\}$$

where $|\mathcal{E}_{\mathcal{M}\setminus A}(k-1)|$ is obtained from Table I, and $|\mathcal{E}_\delta|$ is specified in Table II.

TABLE I: $|\mathcal{E}_{\mathcal{M}\setminus A}(k)|$ for k even.

$\lvert\mathcal{E}_{\mathcal{M}\setminus A}(k)\rvert$	**applicable when**
$kt - a(c + t - p)$	$d = 0$
$kt - a(c + t - p) + \frac{a(a-1)}{2}$	$d \ge 1, t \le (d+1)p$
$kt - a(c + t - p) + \frac{d(2a-d-1)}{2}$	$d \ge 1, (d+1)p < t \le bp$
$\frac{km - d(d-1) + c(2d-c-1)}{2}$	$d \ge 1, t > bp$

TABLE II: $|\mathcal{E}_\delta|$ for k odd.

$\lvert\mathcal{E}_\delta\rvert$	**applicable when**
$\frac{ap}{2} + \min(c, \frac{p}{2})$	$d = 0$, p even
$\min(t, \frac{m}{2})$	$d = 0$, p odd
t	$d \ge 1$, p even, $t \le \frac{dp}{2}$
$\frac{ap}{2} + \frac{dp}{4} + \min(c, \frac{p}{2})$	$d \ge 1$, p even, $\frac{dp}{2} < t \le (b - \frac{d}{2})p$
$\frac{m}{2} - (b - a) + \mathbb{I}(c \ge \frac{p}{2})$	$d \ge 1$, p even, $(b - \frac{d}{2})p < t \le bp$
$\frac{m}{2}$	$d \ge 1$, p even, $t > bp$
t	$d \ge 1$, p odd, $t \le \frac{(b-d)p}{2}$
$\frac{a(p+1)}{2} + \frac{(b-d)(p-1)}{4} + \max(0, c - \lfloor \frac{p}{2} \rfloor)$	$d \ge 1$, p odd, $\frac{(b-d)p}{2} < t \le \frac{(b+d)p}{2}$
$\frac{m}{2}$	$d \ge 1$, p odd, $t > \frac{(b+d)p}{2}$

Proof sketch for Prop. 11: Let $\xi(G_A)$ denote the limit $\lim_{n\to\infty} \frac{1}{n}\sigma(G_A^{(n)})$, so that $C(G_A) = \xi(G_A)$ by Theorem 5.

We first display a subgraph G_A for which $\xi(G_A) \le k - t$, which will show that $C^{l,t}(\mathbf{H}_{k,m}) \le k - t$. We use the fact that $\xi(G_A) \le \lambda(G_A)$ — this easily follows from Theorem 2.

To construct the desired G_A, remove t vertices from $\mathbf{H}_{k,m}$ as follows:

- if $t \le \lfloor k/2 \rfloor$: remove the vertices labeled $1, 2, \ldots, t$;
- if k is even, and $k/2 < t \le k$: remove the $k/2$ vertices labeled $1, 2, \ldots, \frac{k}{2}$, and the $(t - k/2)$ vertices labeled $m - 1, m - 2, \ldots, m - t + \frac{k}{2}$;
- if k is odd, and $\lfloor k/2 \rfloor < t \le k$: remove the vertex labeled $\frac{m}{2}$, then the $\lfloor k/2 \rfloor$ vertices labeled $1, 2, \ldots, \lfloor \frac{k}{2} \rfloor$, and the $(t - \lfloor k/2 \rfloor - 1)$ vertices labeled $m - 1, m - 2, \ldots, m - t + \lfloor \frac{k}{2} + 1 \rfloor$.

For $t < k$, it is sufficient to remove $k - t$ edges from G_A to disconnect vertex 0 from the rest of G_A. Thus, $\lambda(G_A) \le k - t$. In fact, equality holds, since $\lambda(G_A) \ge \kappa(G_A) = k - t$. Hence, $\xi(G_A) \le \lambda(G_A) = k - t$.

The bound $C^{l,t} \le k - t$ may be quite loose for small t. For example, for $\mathbf{H}_{6,10}$ with $t = 2$, we find that $k - t = 4$ is greater than even the SK capacity $\mathcal{C}(\mathcal{M}) = \frac{10}{3}$. This prompts us to derive an alternate upper bound based on the fact that $\xi(G_A)$ cannot exceed $\frac{|\mathcal{E}_A|}{m-t-1}$, where $\mathcal{E}_A$ is the edge set of G_A — see the paragraph preceding the statement of Proposition 7. The choice of G_A here is not as simple, and requires a break-up into several cases. We omit the details. ∎

REFERENCES

[1] P.A. Catlin, "Supereulerian graphs: a survey," *J. Graph Theory*, vol. 16, pp. 177–196, 1992.

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

[3] J. L. Gross and J. Yellen, *Graph Theory and its Applications*, 2nd ed., Chapman and Hall, 2006.

[4] F. Harary, "Maximum connectivity of a graph," *Proc. Nat. Acad. Sci.*, vol. 48, pp. 1142–1145, 1962.

[5] S. Nitinawarat and P. Narayan, "Perfect omniscience, perfect secrecy and Steiner tree packing," *IEEE Trans. Inform. Theory*, vol. 56, pp. 6490–6500, Dec. 2010.

[6] S. Nitinawarat, C. Ye, A. Barg, P. Narayan, and A. Reznik, "Secret key generation for a pairwise independent network model," *IEEE Trans. Inform. Theory*, vol. 56, pp. 6482–6489, Dec. 2010.

[7] E. M. Palmer, "On the spanning tree packing number of a graph: a survey," *Discrete Math.*, vol. 230, pp. 13–21, 2001.

[8] H. Tyagi, N. Kashyap, Y. Sankarasubramaniam, and K. Viswanathan, "Fault tolerant secret key generation," *Proc. 2012 IEEE Int. Symp. Inform. Theory (ISIT 2012)*, pp. 1787–1791.