# Fault-Tolerant Secret Key Generation

Himanshu Tyagi* Navin Kashyap† Yogesh Sankarasubramaniam‡ Kapali Viswanathan‡

***Abstract*—Mobile nodes observing correlated data communicate using an insecure bidirectional switch to generate a secret key, which must remain concealed from the switch. We are interested in fault-tolerant secret key rates, i.e., the rates of secret key generated even if a subset of nodes drop out before the completion of the communication protocol. We formulate a new notion of fault-tolerant secret key capacity, and present an upper bound on it. This upper bound is shown to be tight when the random variables corresponding to the observations of nodes are exchangeable. Further, it is shown that one round of interaction achieves the fault-tolerant secret key capacity in this case. The upper bound is also tight for the case of a pairwise independent network model consisting of a complete graph, and can be attained by a noninteractive protocol.**

## I. Introduction

A set of mobile nodes observing correlated data wish to generate a secret key (SK) by communicating interactively with each other via an honest-but-curious bidirectional central switch. The (honest) central switch makes the communication sent by each node available to all the other nodes. However, a subset of the nodes may drop out before the communication protocol is completed. The remaining nodes must agree upon an SK that is concealed from the (curious) central switch. Such fault-tolerant SK generation facilitates secure group communication for mobile nodes in a wireless environment.

We consider a multiterminal source model, and assume noiseless communication between the nodes and the central switch. Fixing the number of rounds of interaction, we formulate a notion of *fault-tolerant SK capacity*. This extends the concept of multiterminal SK capacity defined in [3]. We provide an upper bound on the fault-tolerant SK capacity.

Our upper bound is tight for two important source models of practical interest. For the first model involving exchangeable random variables (rvs) (see, for instance, [4, p. 365]), our results show that the fault-tolerant SK capacity does not improve with rounds of interaction. Furthermore, our achievability scheme shows the existence of an adaptive protocol that generates an SK of optimum rate for any remaining subset of nodes.

This work was supported by the U.S. National Science Foundation under Grants CCF0830697 and CCF1117546, and a research grant from Hewlett-Packard Labs India.

*Department of Electrical and Computer Engineering, and Institute for Systems Research, University of Maryland, College Park, MD 20742, USA. Email: tyagi@umd.edu

†Department of Electrical Communication Engineering, Indian Institute of Science, Bangalore. Email: nkashyap@ece.iisc.ernet.in

‡ Hewlett-Packard Labs India, Bangalore. Email: {yogesh,kapali}@hp.com

The second model we consider is a pairwise independent network (PIN) introduced in [5], [6]. This source model consists of independent bits shared by pairs of nodes, unknown to the central switch. These pairwise shared bits are represented as edges of a multigraph with nodes as the vertices. In [5], [6], an interactive protocol was provided to generate one bit of SK when this multigraph is a spanning tree. For a $(t+1)$-connected multigraph, we present a noninteractive and fault-tolerant generalization of this protocol that generates one bit of SK if up to $t$ nodes drop out. For the symmetric case of a complete graph, we use a modification of this protocol to achieve a fault-tolerant SK rate that matches the one given by the aforementioned upper bound, thus characterizing the fault-tolerant SK capacity in this case. In fact, we show that it is possible for the the nodes to agree with probability one on an SK of optimal rate that is statistically independent of the communication sent by the nodes; such an SK is termed a perfect SK. Furthermore, this SK can be generated using a noninteractive protocol. Moreover, our protocol generates a perfect SK of optimum rate for any remaining subset of nodes.

In the context of computational secrecy, a dynamic group extension of the Diffie-Hellman SK generation algorithm was presented in [7]. The information-theoretic formulation here, however, is new.

The rest of this paper is organized as follows. The basic concepts of SK and SK capacity are defined in Section II. The notions of fault-tolerant SK and fault-tolerant SK capacities, along with our main results, are given in Section III.

We establish some notation here. The set $\{1,\ldots,m\}$ is denoted by $\mathcal{M}$. Let $X_1,\ldots,X_m, m\geq 2$, be rvs taking values in finite sets $\mathcal{X}_1,\ldots,\mathcal{X}_m$, respectively, and with a known probability mass function. For $i\in\mathcal{M}$ and $n\geq 1$, let $X_i^n$ denote $n$ independent and identically distributed (i.i.d.) copies of $X_i$. For a subset $A\subseteq\mathcal{M}$, denote by $X_A$ the rvs $(X_i, i\in A)$, and by $X_A^n$ the rvs $(X_i^n, i\in A)$. Given $R_i\geq 0$, $1\leq i\leq m$, let $R_A$ denote the quantity $\sum_{i\in A} R_i$.

Finally, for $0\leq\epsilon<1$, we say an rv $U$ is $\epsilon$-recoverable from an rv $V$ if there exists a function $g$ of $V$ such that $\Pr(U=g(V))\geq 1-\epsilon$.

## II. Secret keys and perfect secret keys

We consider the multiterminal source model of [3]. Nodes $1,\ldots,m$ observe rvs $X_1^n,\ldots,X_m^n$, respectively. The communication between the nodes is enabled by a *bidirectional central switch*; any communication received by the switch is made available (exactly) to all the nodes. The communication transmitted by the $i$th node may be randomized using a locally available rv $U_i$. The rv $U_i$ is jointly independent of

978-1-4673-2579-0/12/$31.00 ©2012 IEEE

$(X_{\mathcal{M}}^n, U_j, j \in \mathcal{M} \setminus \{i\})$, and the rvs $U_{\mathcal{M}} := (U_1, \ldots, U_m)$ satisfy $H(U_{\mathcal{M}}) < \infty$. Throughout this paper, we assume that any communication originating from node $i$, $i \in \mathcal{M}$, is stamped with header information that identifies $i$.

**Definition 1.** An *$r$-rounds interactive communication protocol* consists of mappings $\{f_{ij} \mid j \in \mathcal{M}, 1 \le i \le r\}$, where $f_{ij}$ denotes the communication sent by the $j$th node in the $i$th round of the protocol; specifically, $f_{ij}$ is a function of $\left(U_j, X_j^n\right)$ and the communication sent in the previous rounds $\{f_{kl} \mid 1 \le k \le i-1, l \in \mathcal{M}\}$. Denote the rv corresponding to the communication by $\mathbf{F} = (F_{11}, \ldots, F_{1m}, \ldots, F_{r1}, \ldots, F_{rm})$. Note that $\mathbf{F} = \mathbf{F}^{(n)}(U_{\mathcal{M}}, X_{\mathcal{M}}^n)$. For $r = 1$, we call the protocol *noninteractive*.

The interactive protocol above is executed by the central switch, which upon relaying the communication $F_{1\mathcal{M}}, \ldots, F_{i\mathcal{M}}$ to all the nodes, receives the communication $F_{(i+1)j}$ from the $j$th node. Note that here all $m$ terminals are assumed to communicate in each round of interaction. In Section III, we will consider adaptive protocols in a scenario where some of the terminals may drop out, leaving only a subset $A_i \subseteq \mathcal{M}$ to communicate in round $i$.

**Definition 2.** Given $0 \le \epsilon < 1$, for some $n \ge 1$, an rv $K = K^{(n)}(U_{\mathcal{M}}, X_{\mathcal{M}}^n)$, taking values in a finite set $\mathcal{K}$, is an *$\epsilon$-secret key* ($\epsilon$-SK), achievable from observations of length $n$, using randomization $U_{\mathcal{M}}$, and $\epsilon$-recoverable from $r$-rounds interactive communication $\mathbf{F} = \mathbf{F}^{(n)}(U_{\mathcal{M}}, X_{\mathcal{M}}^n)$ if

(i) it satisfies the "strong" secrecy condition: $\log|\mathcal{K}| - H(K) + I(K \wedge \mathbf{F}) < \epsilon$; and

(ii) it is $\epsilon$-recoverable from $(\mathbf{F}, U_i, X_i^n)$, for all $i \in \mathcal{M}$.

The *rate* of this $\epsilon$-SK is given by $\frac{1}{n}\log|\mathcal{K}|$.

A rate $R \ge 0$ is an achievable SK rate if for every $0 < \epsilon < 1$, there exists an $\epsilon$-SK of rate greater than $R - \epsilon$. The *SK capacity* $C(\mathcal{M})$ is defined as the supremum of all achievable SK rates. A 0-SK $K$ is referred to as a *perfect SK*, and the supremum over the rates of a 0-SK is the *perfect SK capacity* $C_0(\mathcal{M})$.

**Theorem 1** (Csiszár-Narayan [3])**.** *The SK capacity is given by*

$$C(\mathcal{M}) = H(X_{\mathcal{M}}) - R_{CO}, \tag{1}$$

*where* $R_{CO} = \min_{(R_1,\ldots,R_m)\in\mathcal{R}_{CO}(\mathcal{M})} R_{\mathcal{M}}$, *with*

$$\mathcal{R}_{CO} = \{(R_1, \ldots, R_m) : R_B \ge H\left(X_B | X_{\mathcal{M}\setminus B}\right), B \subsetneq \mathcal{M}\}. \tag{2}$$

The quantity $R_{CO}$ above denotes the minimum rate of communication for "omniscience" [3], i.e., the minimum achievable rate of interactive communication $\mathbf{F}$ such that $X_{\mathcal{M}}^n$ is $\epsilon$-recoverable from $(\mathbf{F}, U_i, X_i^n)$, for all $i \in \mathcal{M}$. We further note from [3] that there exists a noninteractive communication of rate $R_{CO}$ that attains omniscience at $\mathcal{M}$ .

## III. Fault-tolerant SK generation

In this section, a new fault-tolerant version of the SK generation problem is formulated. We consider *adaptive protocols* that take into account the dropping out of nodes during the protocol. It is required that the nodes that remain at the end of a protocol agree upon an SK.

The adaptive protocol is executed by the central switch. Let $A_1$ denote the set of nodes that communicate in round 1, the rest of the nodes having dropped out without communicating. Knowing the set $A_1$, the central switch then provides the nodes in $A_1$ with all the round-1 communication, and anticipates the next round of communication from them. However, only the nodes in a subset $A_2$ of $A_1$ communicate in round 2. This process is repeated for $r$ rounds, with only the nodes in $A_r$ remaining in the $r$th round. Clearly we have $A_r \subseteq A_{r-1} \subseteq \ldots \subseteq A_1 \subseteq \mathcal{M}$. Note that in a given round of communication, each remaining node has access to the communication that was sent in the previous rounds. As in Definition 1, for $r = 1$, we call the protocol *noninteractive*.

In this paper, we assume that for $r \ge 2$, $A_r = A_{r-1}$, i.e., for adaptive protocols, the nodes remaining in the $(r-1)$th round are required to communicate in the $r$th round, or else the protocol fails. (The case of $r = 1$ is handled separately.) Thus, except when $r \ge 2$ and $i = r$, the set of nodes that will communicate in round $i$ is not known to the central switch at the end of the previous round. In the exceptional case, the assumption $A_r = A_{r-1}$ ensures that the set of nodes that will communicate in the $r$th round is known *a priori*. In practice, this could be implemented by having the central switch announce to all nodes at the beginning of the $r$th round that this is the final round of communication. If all nodes in $A_{r-1}$ respond, the protocol completes; otherwise it fails.

Using the adaptive protocol above, the nodes generate an SK for the remaining set, $A_r$, of nodes. We do not require that the SK be concealed from the nodes in $\mathcal{M} \setminus A_r$. Fixing the maximum number of nodes that may drop out during the protocol as $t$, the SK rate guaranteed by the protocol corresponds to the worst-case rate of an SK that is generated by the remaining nodes in $A_r$, for all choices of sets $A_r \subseteq \cdots \subseteq A_1$ with $|A_r| = |A_{r-1}| \ge m - t$.

Formally, we have the following two definitions.

**Definition 3.** For $r \ge 1$, and $n \ge 1$, an $r$-rounds adaptive protocol, for each $\mathcal{A} = \{A_l : 1 \le l \le r-1\}$, with $A_{r-1} \subseteq A_{r-2} \subseteq \ldots \subseteq A_1 \subseteq \mathcal{M}$, consists of mappings $\{f_{ij} \mid j \in A_{i-1}, 1 \le i \le r\}$, where $A_0 = \mathcal{M}$. For each $j \in A_{i-1}$, $f_{ij}$ is a function of $\left(U_j, X_j^n\right)$ and the communication from all the previous rounds, $\{f_{kl} \mid 1 \le k \le i-1, l \in A_k\}$.

Here $f_{ij}$ denotes the communication from the $j$th node in the $i$th round of communication, and so, is defined only for the nodes $j \in A_{i-1}$, where $A_{i-1}$ is the set of nodes that remain after the $(i-1)$th round. The function $f_{ij}$ depends on the sequence of sets $A_{i-1} \subseteq ... \subseteq A_1 \subseteq A_0 = \mathcal{M}$.

With a slight abuse of notation, let $\mathbf{F} = \mathbf{F}_{\mathcal{A}}$ denote the random value of the communication corresponding to the decreasing family of subsets $\mathcal{A}$.

It is perhaps worth clarifying that $f_{ij}$ in the definition above is what $j \in A_{i-1}$ prepares to communicate in the $i$th round; it may happen that $j$ drops out before actually sending this

communication. For $r \geq 2$, the nodes remaining at the end of $(r-1)$th round must communicate in the $r$th round, or else the protocol fails.

**Definition 4.** For $1 \leq t \leq m$ and $r \geq 2$, a rate $R \geq 0$ is said to be an achievable $(r,t)$-fault-tolerant SK rate, if for every $0 < \epsilon < 1$, there exists $n \geq 1$, and an $r$-rounds adaptive protocol as above, such that for every decreasing family $\mathcal{A}$, with $|A_{r-1}| \geq m-t$, there exists an $\epsilon$-SK $K = K^{(n)}\left(U_{A_{r-1}}, X^n_{A_{r-1}}\right)$, of rate greater than $R-\epsilon$, that

(i) satisfies the "strong" secrecy condition: $\log|\mathcal{K}| - H(K) + I(K \wedge \mathbf{F}) < \epsilon$; and

(ii) is $\epsilon$-recoverable from $(\mathbf{F}, U_i, X_i^n)$, for all $i \in A_{r-1}$; we say that $K$ is an $\epsilon$-SK for $A_{r-1}$ recoverable from the protocol.

Note that a rate $R$ is achievable if every remaining subset $A_{r-1}$ of size $m-t$ or more can form an SK of rate $R$, *irrespective* of $\mathcal{A}$. The actual SK $K$, however, may depend on $\mathcal{A}$.

Similarly, $R \geq 0$ is an achievable $(1,t)$-fault-tolerant SK rate if for every $0 < \epsilon < 1$, there exists $n \geq 1$, and a noninteractive (1-round adaptive) protocol, such that for every $A \subset \mathcal{M}$, with $|A| \geq m-t$, there exists an $\epsilon$-SK $K = K^{(n)}(U_A, X_A^n)$, of rate greater than $R-\epsilon$, that satisfies (i) and (ii) above. The $(r,t)$-fault-tolerant SK capacity $C^{r,t}(\mathcal{M})$ is defined as the supremum of all $(r,t)$-fault-tolerant SK rates.

The $(r,t)$-fault-tolerant perfect SK capacity $C_0^{r,t}(\mathcal{M})$ is defined analogously.

Since any $r$-rounds adaptive protocol can be implemented in $r+1$ rounds by choosing $f_{1j} = \emptyset$, and defining the last $r$ rounds of communication $f_{ij}$, $2 \leq i \leq r+1$ as in the $r$-rounds protocol, we have from their definitions that various notions of fault-tolerant capacity are related as below:

For $r \geq 2$,

$$C_0^{1,t}(\mathcal{M}) \leq C^{1,t}(\mathcal{M}) \leq C^{r,t}(\mathcal{M}) \leq C^{r+1,t}(\mathcal{M}).$$

Next, given $A \subseteq \mathcal{M}$, consider the family $A_1 = ... = A_{r-1} = A_r = A$. This family corresponds to the case where the nodes $j$ that communicate during the protocol never drop-out. Therefore, the rate $R$ of an SK that a fault-tolerant protocol generates for this family can not exceed the SK capacity for $A$, $C(A)$ (see Definition 2). Here $C(A)$ is defined as in (1), with constraints in (2) now applied for all $B \subsetneq A$[1]. Thus, if $R$ is an achievable $(r,t)$-fault-tolerant SK rate, then for any subset $A$ of $\mathcal{M}$, with $|A| \geq m-t$, it holds that

$$R \leq C(A).$$

Consequently,

$$C^{r,t}(\mathcal{M}) \leq \min_{\substack{A \subseteq \mathcal{M} \\ |A| \geq m-t}} C(A), \quad r \geq 1.$$

In fact, the following lemma allows us to restrict to the sets with $|A| = m-t$ in the upper bound above.

**Lemma 2** (Monotonicity of SK capacity)**.**

$$C(\mathcal{M}) \geq \min_{\substack{A \subseteq \mathcal{M} \\ |A| = m-1}} C(A).$$

The proof is based on an alternative expression for $C(\mathcal{M})$ derived in [1], and is omitted due to space constraints. We summarize the observations above in the following Lemma.

**Lemma 3.** *For $r \geq 1$, the $(r,t)$-fault-tolerant SK capacity satisfies the following:*

$$C_0^{1,t}(\mathcal{M}) \leq C^{r,t}(\mathcal{M}) \leq C^{r+1,t}(\mathcal{M}) \leq \min_{\substack{A \subseteq \mathcal{M} \\ |A| = m-t}} C(A).$$

The fault-tolerant SK capacity represents the optimal *worst-case rate* of an SK. A much stronger optimality criterion given below requires the protocol to generate an optimum rate SK for each remaining subset of nodes.

**Definition 5.** For $r \geq 2$ and $n \geq 1$, we say that an $r$-rounds adaptive protocol is *strongly optimal* for fault-tolerant SK generation if for every decreasing family $\mathcal{A}$, consisting of $A_{r-1} \subseteq \ldots \subseteq A_1$, and for every $0 < \epsilon < 1$, there exists an $\epsilon$-SK $K$ for $A_{r-1}$, recoverable from the protocol, of rate greater than $C(A_{r-1}) - \epsilon$. A similar definition holds for adaptive protocols with $r = 1$.

In applications like mobile communication, it is required that all the nodes have a symmetric role in the SK generation protocol. In fact, it is often the case that the underlying source model is also symmetric. In the remainder of this paper, we will focus on such symmetric models for fault-tolerant SK generation. We are now in a position to state our main results.

### A. Exchangeable source model

We first consider a symmetric source model consisting of exchangeable rvs $X_1, \ldots, X_m$, i.e., $\mathtt{P}_{X_1,\ldots,X_m} = \mathtt{P}_{X_{\sigma(1)},\ldots,X_{\sigma(m)}}$, for all permutations $\sigma$ of $\{1,\ldots,m\}$. Then, for $A \subseteq \mathcal{M}$, $H\left(X_A | X_{\mathcal{M}\setminus A}\right)$ depends only on the size of $A$; for $1 \leq i,j < m$ and $i+j \leq m$, denote by $g(i|j)$ the conditional entropy $H(X_1,\ldots,X_i|X_{i+1},\ldots,X_{i+j})$, with the convention $g(m|0) = H(X_{\mathcal{M}})$ and $g(0|m) = 0$. We characterize next the minimum rate of communication for omniscience $R_{CO}$ for exchangeable rvs.

**Lemma 4.** *Given exchangeable rvs $X_1, \ldots, X_m$, for*

$$\alpha_m = \frac{g(m-1|1)}{m-1},$$

*$(\alpha_m, \ldots, \alpha_m)$ is in $\mathcal{R}_{CO}$ and $R_{CO} = m\alpha_m$ (see Theorem 1).*

As noted in the discussion following Theorem 1, the optimum rate communication for omniscience can be noninteractive. The lemma above implies that it is possible to attain omniscience using noninteractive communication of equal rates from each node. The next lemma shows that this equal rate of transmission decreases with the number of nodes.

**Lemma 5.** *The $\alpha_m$ defined above is decreasing in $m$.*

[1]This is different from the notation in [3] where $C(A)$ corresponds to the maximum rate of a SK that can be generated by the nodes in $A$ when nodes $\mathcal{M} \setminus A$ act as helpers.

The proofs of Lemmas 4 and 5 are based on elementary properties of the conditional entropies $g(i|j)$ and are omitted due to space constraints.

Using these observations, the following theorem characterizes the $(r,t)$-fault-tolerant SK capacity for exchangeable rvs, when $r \geq 2$.

**Theorem 6.** *For $1 \leq t \leq m$ and $r \geq 2$, the $(r,t)$-fault-tolerant SK capacity is given by*

$$C^{2,t}(\mathcal{M}) = C^{r,t}(\mathcal{M}) = g(m-t|0) - (m-t)\alpha_{m-t}.$$

*Furthermore, there exists a 2-rounds adaptive protocol that is strongly optimal.*

*Proof*. We first note from Lemma 3, Theorem 1, and Lemma 4 that $C^{r,t}(\mathcal{M}) \leq g(m-t|0) - (m-t)\alpha_{m-t}$.

We next show that $C^{2,t}(\mathcal{M}) \geq g(m-t|0) - (m-t)\alpha_{m-t}$. Fix $0 < \epsilon < 1$. Assume, for now (we will prove this later), that for sufficiently large $n$, there exists a 2-rounds adaptive protocol with the following properties:

(i) For $j \in \mathcal{M}$, $f_{1j} : \mathcal{X}_j^n \to \{1, \ldots, \lceil 2^{n\alpha_m} \rceil\}$,
(ii) for $A \subseteq \mathcal{M}$, with $k = |A|$, let $f_{2j} = f_{2j}^k$, where $f_{2j}^k : \mathcal{X}_j^n \to \left\{1, \ldots, \lceil 2^{n(\alpha_k - \alpha_m)} \rceil\right\}$, for all $j \in A$; denote its random value by $F_{2j}^k$,
(iii) for each $A \subseteq \mathcal{M}$, $X_A^n$ is $\epsilon$-recoverable from $\left(X_l^n, F_{1j}, F_{2j}^k, j \in A\right)$, for all $l \in A$.

Note that if only the nodes in a subset $A$ with $|A| = k$ remain after the first round, the overall rate of communication for the protocol is $k\alpha_k$. Using a version of the Balanced Coloring Lemma [3, Lemma B.3], for sufficiently large $n$, there exists an rv $K = K(X_A^n)$ of rate greater than $H(X_A) - k\alpha_k - \epsilon$ with $I\left(K \wedge F_{1j}, F_{2j}^k, j \in A\right) \leq \epsilon$. The nodes first use the protocol above to recover $X_A^n$, and then compute the SK $K = K(X_A^n)$. It follows from Lemma 4 and Theorem 1 that $C(A) = H(X_A) - k\alpha_k$, which establishes the strong optimality of the protocol above. Furthermore, from Lemma 2, if $k \geq m-t$, then $C(A) \geq g(m-t|0) - (m-t)\alpha_{m-t}$. Thus, the proof of the theorem would be complete once we show the existence of the protocol above.

To that end, from Lemma 4 and [2, Lemma 13.13], for sufficiently large $n$, random mappings $F_j$, $j \in A$, of rate $\alpha_k$ result in omniscience at the terminals in $A$. In fact, the same result holds if $F_j$ is replaced by two independent random mappings of rates that sum to $\alpha_k$. Specifically, consider random mappings $F_{1j}$ of $X_j^n$ of rate $\alpha_m$ for $j \in \mathcal{M}$. For $k \leq m$, for $1 \leq j \leq k$, let $F_{2j}^k$ be random mappings of rate $\alpha_k - \alpha_m$. Note that from Lemma 5 we have $\alpha_k - \alpha_m \geq 0$. Therefore, from the discussion above, the random mappings $F_{1j}$, $j \in \mathcal{M}$, and $F_{2j}^k$, $1 \leq j \leq k$, constitute a protocol with the required properties, with probability close to 1 for $n$ sufficiently large. □

*Remark.* It remains unresolved whether the inequality $C^{1,t}(\mathcal{M}) \leq C^{2,t}(\mathcal{M})$ is strict or not for the exchangeable source model studied here.

### *B. PIN model*

In this section, we consider fault-tolerant SK generation for a special case of the multiterminal source model, namely, the PIN model (see [5], [6]). The PIN model is specified by a graph $G = (\mathcal{V}, \mathcal{E})$, with vertex set $\mathcal{V} = \mathcal{M}$ and edge set $\mathcal{E}$. For $n \geq 1$, let $G^{(n)}$ be the multigraph with vertex set $\mathcal{V} = \mathcal{M}$ and edge set $\mathcal{E}^{(n)}$ containing $n$ copies of each edge of $G$. The $n$ copies of an edge $e = \{i,j\} \in \mathcal{E}$ represent $n$ i.i.d. copies of an unbiased random bit $B_e$ available to the nodes $i$ and $j$. For each $e \in \mathcal{E}$, the rv $B_e^n$ is jointly independent of the rvs $(B_{e'}^n, e' \in \mathcal{E} \setminus \{e\})$. Consequently, for each $i \in \mathcal{M}$, the observations of the $i$th node are given by the rv

$$X_i^n = \left(B_{\{i,j\}}^n, j \in \mathcal{M}, \{i,j\} \in \mathcal{E}\right).$$

As before, $X_{\mathcal{M}} = (X_1, \ldots, X_m)$ and $X_{\mathcal{M}}^n = (X_1^n, \ldots, X_m^n)$.

For this PIN model, an interactive communication protocol was given in [5], [6] to generate a 1-bit perfect SK from $X_{\mathcal{M}}$, when $G$ is a spanning tree for the vertices in $\mathcal{M}$. Here, we present a new fault-tolerant variant of that protocol. In particular, our protocol below yields a 1-bit $(1,t)$-fault-tolerant perfect SK for a PIN model consisting of a $(t+1)$-connected spanning graph $G$ (we say that a graph $G$ is $(t+1)$-connected if the subgraph $G(A)$ induced by $G$ on the vertices in $A \subseteq \mathcal{M}$ is connected whenever $|A| \geq m-t$).

*Protocol 1:*
For each $i \in \mathcal{M}$, the $i$th node communicates

$$f_i(X_i) = \left(B_{\{i,j\}} \oplus B_{\{i,j'\}} : \{i,j\}, \{i,j'\} \in \mathcal{E}, j \neq j'\right).$$

For $A \subseteq \mathcal{M}$, $|A| \geq m-t$, let $e_A$ be an edge in $G(A)$; such an edge exists as $G$ is $(t+1)$-connected.

**Claim:** For each $i \in A$, $B_{e_A}$ is a function of $(F_A, X_i)$, and $I(B_{e_A} \wedge F_A) = 0$. Thus, $B_{e_A}$ is a 1-bit perfect SK achievable from $X_A$.

*Proof.* Since $G$ is $(t+1)$-connected, and $|A| \geq m-t$, for each $i \in A$ and for some edge $e_l$ incident on $i$, there exists a path $\{e_A, e_1, \ldots, e_l\}$ in $G(A)$. Since $e_l$ is incident on $i$, $B_{e_l}$ is a function of $X_i$. Further, note that the communication $F_A$ includes the rvs $B_{e_A} \oplus B_{e_1}, B_{e_1} \oplus B_{e_2}, \ldots, B_{e_{l-1}} \oplus B_{e_l}$. Therefore, $B_{e_A} = (B_{e_A} \oplus B_{e_1}) \oplus (B_{e_1} \oplus B_{e_2}) \oplus \ldots \oplus (B_{e_{l-1}} \oplus B_{e_l}) \oplus B_{e_l}$ is a function of $(F_A, X_i)$.

Labelling the rest of the edges so that $\mathcal{E} = \{e_0 = e_A, e_1, \ldots, e_k\}$, we have

$$H\left(B_{e_i} \oplus B_{e_j}, 0 \leq i,j \leq k\right) = H\left(B_{e_0} \oplus B_{e_j}, 1 \leq j \leq k\right) \leq k. \quad (3)$$

The equality above follows from the fact that for all $i,j$, we have $B_{e_i} \oplus B_{e_j} = (B_{e_0} \oplus B_{e_i}) \oplus (B_{e_0} \oplus B_{e_j})$. Similarly,

$$H\left(B_{e_i} \oplus B_{e_j}, 0 \leq i,j \leq k \mid B_{e_A}\right) = H\left(B_{e_1}, \ldots, B_{e_k} \mid B_{e_0}\right) = k, \quad (4)$$

where the last equality follows from the pairwise independence assumption. Hence,

$$0 \leq I(B_{e_A} \wedge F_A) \leq I\left(B_{e_A} \wedge B_{e_i} \oplus B_{e_j}, 0 \leq i,j \leq k\right) \leq 0,$$

the last inequality following from (3) and (4). □

For the remainder of this section we take $G$ to be $K_m$, i.e., the complete graph on $m$ vertices. This is the unique choice of $G$ for which the rvs $X_1, \ldots, X_m$ are exchangeable. For this symmetric model, the theorem below shows the strong optimality (see Definition 5) of Protocol 1, when it is applied to a certain packing of spanning trees.

**Theorem 7.** *For the PIN model specified by the complete graph $K_m$, we have*

$$C^{r,t}(\mathcal{M}) = C_0^{1,t}(\mathcal{M}) = \frac{m-t}{2}, \quad 0 \le t \le m, r \ge 1.$$

*Furthermore, there exists a strongly optimal protocol for fault-tolerant SK generation.*

*Proof.* For $i \in \mathcal{M}$, denote by $Y_i$ the "star-shaped" spanning tree with edge set given by $\mathcal{E}_i = \{\{i,j\} : j \in \mathcal{M}, j \neq i\}$. Then, for any subset $A \subseteq \mathcal{M}$, the union of $\bigcup_{i \in A} Y_i(A)$ is precisely the multigraph, $K_A^{(2)}$, on the vertex set $A$ with two edges between each pair of distinct vertices. Therefore, if the nodes in a subset $A$ of $\mathcal{M}$ remain, we can use Protocol 1 to generate a 1-bit perfect SK bit for each $Y_i(A)$, $i \in A$. This yields a perfect SK of size $|A|$ bits achievable from the observations $X_A^2 = (X_i^2, i \in A)$. The rate of this SK is $|A|/2$. Thus, for $0 \le t \le m$, $(m-t)/2$ is an achievable $(1,t)$-fault-tolerant perfect SK rate.

To prove the converse, first note from Lemma 2 that

$$C_0^{1,t}(\mathcal{M}) \le C^{r,t}(\mathcal{M}) \le C(A),$$

for $A \subseteq \mathcal{M}$, $|A| = m - t$. Thus the converse will follow upon showing that $C(A) = (m-t)/2$, when $|A| = m - t$. In fact, if $C(A) = (m-t)/2$ holds, then the protocol is strongly optimal. To that end, since the rvs $X_1, \ldots, X_m$ are exchangeable, a straightforward computation using Theorem 1 and Lemma 4 yields $C(A) = \frac{m-t}{2}$. □

The rate-optimal protocol above is noninteractive and does not require local randomness. However, it does need observations of length $n = 2$. We next propose a fault-tolerant perfect SK generation protocol that works with observations of length $n = 1$, is noninteractive, and generates $\lfloor m/2 \rfloor - t$ bits of SK when upto $t$ nodes leave. Specifically, for $K_m$, our result below gives a spanning tree packing of size $\lfloor m/2 \rfloor$, i.e., a collection of $\lfloor m/2 \rfloor$ disjoint[2] spanning trees of $K_m$, such that every vertex is a leaf for all but one of the spanning trees in the packing. The SK generation protocol then involves using Protocol 1 on each of these disjoint spanning trees. Removing a vertex only disconnects those spanning trees for which the vertex is not a leaf. Consequently, upon removing $t$ vertices, the remaining graph still contains $\lfloor m/2 \rfloor - t$ disjoint spanning trees. Hence, when up to $t$ nodes leave, the remaining nodes generate $\lfloor m/2 \rfloor - t$ bits of SK.

**Lemma 8.** *$K_m$ contains a spanning tree packing of size $\lfloor m/2 \rfloor$, such that every vertex is a leaf for all but one of the disjoint spanning trees in the packing.*

[2]Here, "disjoint" means that distinct spanning trees share no edges.

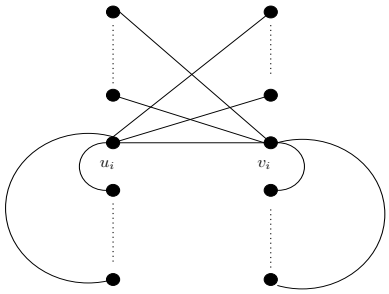


Fig. 1. Spanning tree $T_i$ corresponding to the edge $\{u_i, v_i\}$

*Proof.* We give a construction for even $m$. For odd $m$, the proof can be completed by introducing a dummy node, carrying out the construction for $K_{m+1}$, and finally deleting the dummy node.

For $m = 2k$, consider a perfect matching in $K_m$. It partitions the vertices into two disjoint sets $\{u_1, \ldots, u_k\}$ and $\{v_1, \ldots, v_k\}$, and consists of edges $\{u_i, v_i\}$ for $1 \le i \le k$. For each edge $\{u_i, v_i\}$ of the matching, consider the spanning tree $T_i$, whose edge set is the union of $\{\{u_i, u_j\}, i < j \le k\}$, $\{\{u_i, v_j\}, 1 \le j \le i\}$, $\{\{v_i, v_j\}, i < j \le k\}$, and $\{\{v_i, u_j\}, 1 \le j < i\}$, as depicted in Fig. 1. It is clear that the edge-disjoint spanning trees $T_i$, $i = 1, \ldots, k$, satisfy the properties claimed above. □

## IV. Concluding Remarks

The adaptive protocols considered in this paper are admittedly a first step towards the larger goal of information-theoretic SK agreement for dynamic groups. The next step is to allow rejoining of terminals that drop out, and more generally, to handle arbitrary dropping in-and-out of the $m$ terminals. We also intend to consider stronger adversarial models.


## Acknowledgement

The authors thank Amitabh Saxena and Andrew Thangaraj for useful discussions leading up to this work. The first author would also like to thank Prakash Narayan for helpful comments.


## References


[1] C. Chan and L. Zheng, "Mutual dependence for secret key agreement," *in Proceedings of 44th Annual Conference on Information Sciences and Systems (CISS)*, 2010.

[2] I. Csiszár and J. Körner, *Information theory: Coding Theorems for Discrete Memoryless Channels*. 2nd Edition. Cambridge University Press, 2011.

[3] I. Csiszár and P. Narayan, "Secrecy capacities for multiple terminals," *IEEE Trans. Inform. Theory*, vol. 50, no. 12, pp. 3047–3061, 2004.

[4] M. Loéve, *Probability Theory*. D. Van Nostrand Company, Inc, 1960.

[5] S. Nitinawarat and P. Narayan, "Perfect omniscience, perfect secrecy, and Steiner tree packing," *IEEE Trans. Inform. Theory*, vol. 56, no. 12, pp. 6490 – 6500, December 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, no. 12, pp. 6482 – 6489, December 2010.

[7] M. Steiner, G. Tsudik, and M. Waidner, "Key agreement in dynamic peer groups," *IEEE Trans. on Parallel and Distributed Systems*, vol. 11, no. 8, pp. 769–780, 2000.