Common Randomness, Multiuser Secrecy and Tree Packing

Sirin Nitinawarat*, Chunxuan Ye**, Alexander Barg*, Prakash Narayan* and Alex Reznik**
*Dept. of Electrical and Computer Engineering and
Institute for Systems Research
University of Maryland
College Park, MD 20742, USA
nitinawa@mail.umd.edu, abarg@umd.edu, prakash@umd.edu
**InterDigital
King of Prussia, PA 19406
Chunxuan.Ye@interdigital.com, AlexReznik@interdigital.com

Abstract—Inherent connections are known to exist between common randomness generated by multiterminal source coding and channel coding on the one hand, and information theoretic secrecy generation by means of public communication on the other hand. Based on these connections, points of contact have been found recently also between secrecy generation for a special model for the latter and the combinatorial problem of tree packing in a multigraph. This paper provides a brief (and partial) survey of these links, especially those between secrecy generation and combinatorial tree packing. Our objective is to highlight specific connections between common randomness, secrecy and tree packing.

I. INTRODUCTION

It is recognized now that close links exist between common randomness generated by multiterminal source coding and channel coding on the one hand, and information theoretic secrecy generation by means of public discussion on the other hand [12], [2], [6], [7]. Furthermore, points of contact have been found also between secrecy generation for a special model for the latter and the combinatorial problem of tree packing in a multigraph [16]. This paper provides a brief (and partial) survey of results from [6], [7] and [16], emphasizing the last. Our objective is to highlight specific connections that exist between common randomness, secrecy and tree packing.

Common randomness available at multiple terminals in different locations plays a central role in several aspects of communication and cryptography. A group of terminals possess common randomness if all of them agree on the outcome of a random experiment with probability $\geq 1$. For instance, common randomness available to a transmitter and a receiver enables the use of random codes which can strictly outperform deterministic codes for communication over an arbitrarily varying channel [1], [5]. Such common randomness also determines the maximum achievable identification rate in the theory of identification over noisy channels [3].

In secure communication, the theme of this paper, secret common randomness shared by legitimate transmitters and receivers but concealed from an eavesdropper, can be used as a “secret key” for encrypted communication between them [11], [12], [2], [6].

Multiple terminals can generate secrecy, i.e., secret common randomness, using resources at their disposal, e.g., prior and privileged access to correlated signals [12], [2], [6] or access to the inputs or outputs of noisy channels that connect them [12], [2], [7]. Remarkably, such secrecy generation can be enhanced greatly by additionally permitting public communication between the legitimate terminals in full view of the eavesdropper (and hence public), an important dimension introduced in [11], [12], [2]. This paper deals with the specific class of multiterminal source models for secrecy generation studied in [12], [2], [6] in which the legitimate terminals have the engineering means to acquire prior and privileged access to correlated signals and to engage in unfettered public discussion. For instance, suppose that terminals 1 and 2 observe correlated signals consisting of i.i.d. repetitions (finite-valued) random variables (rvs) $X_1$ and $X_2$, respectively, with a given joint probability distribution. The terminals then engage in public discussion based on their observed signals with the objective of generating a “secret key,” i.e., secret common randomness which is concealed from an eavesdropper which has access to the public discussion (but not to the prior correlated signals at the terminals). The maximum rate of such secrecy is $I(X_1;X_2)$ [12], [2]. This rate can be achieved by the public transmission by terminal 1 of a Slepian-Wolf codeword for its signal thereby enabling terminal 2 to recover it almost losslessly using its own signal as “receiver side-information.” Then the terminals extract, from their shared knowledge of terminal 1’s signal, a component which is “approximately” statistically independent of the publicly transmitted Slepian-
Wolfgang Wolf codeword; this component constitutes a secret key. This link between secrecy generation and Slepian-Wolf data compression has led to the discovery – for a general class of multiterminal source models – of an innate coupling between multiterminal secrecy generation with public communication on the one hand, and the multiterminal source coding of correlated signals without any secrecy constraints on the other hand [6], [15].

Next, points of contact have been found recently between secrecy generation with public communication for a specialized multiterminal source model and the combinatorial problem of the maximal packing of Steiner trees in a multigraph [16]. Specifically, the maximum number of tree packings in a given multigraph is always a lower bound for the maximum rate of secrecy generation in an associated multiterminal source model, and can sometimes be tight. This preliminary finding raises two interesting possibilities. First, information theoretic tools could play a role in examining an open problem in theoretical computer science of characterizing exactly the maximum number of Steiner trees that can be packed in a given multigraph [10], [4]. Reciprocally, polynomial-time tree packing algorithms for multigraphs can play a role in the formation of rate-optimal secret common randomness for a group of terminals through the dissemination of secret keys devised locally between pairs of terminals [16].

In this paper, we first consider a multiterminal source model for which we restate from [6] results pertaining to a precise connection between a problem of “omniscience” - attainment (a special form of common randomness generation) by a given set of the terminals and a problem of secrecy generation by the same set, both with the cooperation of the remaining terminals. In light of these results, we then turn to the problem of secrecy generation for a “pairwise independent network” model introduced in [18] (see also [17]). This model, hereafter abbreviated as the PIN model, is a special case of the multiterminal source model in [6], and is motivated by practical aspects of a wireless communication network in which terminals communicate on the same frequency [17], [16]. Each pair of terminals is assumed to observe correlated sources which are independent of sources observed by all other pairs of terminals. For the PIN model, we outline points of contact between secret key generation and a combinatorial problem of tree packing, described earlier in [16].

II. PRELIMINARIES: THE MULTITERMINAL SOURCE MODEL

In a multiterminal source model, introduced in [6], terminals 1, . . . , m observe, respectively, the correlated signals

\[ X_i^n = (X_{i1}, \ldots, X_{in}), \ldots, X_m^n = (X_{m1}, \ldots, X_{mn}) \]

representing different noisy versions of a (common) broadcast signal or of a (common) parameter of the environment. Suppose that for each terminal \( i \in \mathcal{M} = \{1, \ldots, m\} \), the observed signal \( X_i^n \) consists of \( n \) i.i.d. repetitions of the rv \( X_i \) taking values in a finite set, and that the joint probability distribution of the rvs \( X_1, \ldots, X_m \) is known. The goal is for all the terminals in a given set \( A \subseteq \mathcal{M} \), \( |A| > 2 \), to generate shared secret common randomness, i.e., a shared secret key, with the remaining terminals (if any) cooperating in secrecy generation. To this end, following their observations of the random sequences as above, all the terminals in \( \mathcal{M} \) are allowed to communicate among themselves in the form of public broadcasts over a noiseless channel of unlimited capacity, interactively and in several rounds if necessary. A public message from a terminal, in general, can be any function of its observed signal as well as of all previous public communication. All such public communication, denoted collectively by \( F \), is observed by all the terminals as well as by an eavesdropper.

The resulting 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 secret from the eavesdropper which has access to the public interterminal communication \( F \), but is otherwise passive, i.e., unable to tamper with this communication. Specifically, the rvs \( K_i \), \( i \in A \), will yield a secret key \( K \) for the terminals in \( A \) if

- \( K_i \) is a function only of the data available at terminal \( i \), i.e.,

\[ K_i = K_i(X_i^n, F), \quad i \in A, \]  

with \( K_i, i \in A \), taking values in the same (finite) key space \( K \);

- the rvs \( K_i, i \in A \), represent common randomness, i.e.,

\[ \Pr\{K = K_i, i \in A\} \approx 1; \]  

- the key \( K \) satisfies the secrecy condition

\[ s(K; F) = \log |K| - H(K|F) \approx 0; \]  

where \( |\cdot| \) denotes cardinality; smallness of the security index \( s(K; F) \) [6] is tantamount to a nearly uniform distribution for \( K \) (i.e., \( \log |K| - H(K) \) is small) and the near independence of \( K \) and \( F \) (i.e., the mutual information \( I(K; F) \) is close to 0). In fact, we adopt the concept of strong secrecy by demanding that the security index decay to 0 exponentially rapidly in \( n \) [6], [7], [13], [14]. Note that no limitations are assumed on the computing power of the eavesdropper.

We seek a secret key of the largest rate \( \frac{1}{n} \log |K| \) with a vanishingly small value of security index, ideally zero in which case the key will afford perfect secrecy. The solution to this secrecy generation problem is intertwined with that of the multiterminal lossless data compression problem (not involving any secrecy constraints) in which each terminal in \( A \) wishes to reconstruct with probability \( \approx 1 \) all the signals observed by all the other terminals in \( \mathcal{M} \) using optimally compressed interterminal communication, say \( F \), for the purpose. This is accomplished using data-compressed communication \( F \) of minimal rate \( R_{min}(A) \) given by [6], [7]

\[ R_{min}(A) = \max_{\lambda \in \Lambda(A)} \sum_{B \in \mathcal{B}(A)} \lambda_B H(X_B|X_{B^-}), \]  

and, as a consequence, each terminal in \( A \) achieves a
common random subset of $H(X_1, \ldots, X_m)$. In (4), for $A \subseteq \mathcal{M}$, $B(A) = \{B \subseteq \mathcal{M} : B \neq \emptyset, A \not\subseteq B\}$, and $B_i(A)$, $i \in \mathcal{M}$, is its subset consisting of those $B \in B(A)$ that contain $i$; and $\Lambda(A)$ is the set of all collections $\lambda = \{\lambda_B : B \in B(A)\}$ of weights $0 \leq \lambda_B \leq 1$, satisfying $\sum_{B \in B(A)} \lambda_B = 1$ for all $i \in \mathcal{M}$.

The secret key capacity $C_S(A)$, i.e., the largest achievable secret key rate for the terminals in $A$ is shown in [6] to be

$$C_S(A) = H(X_1, \ldots, X_m) - R_{\min}(A),$$

and can be achieved by a single autonomous public communication sent by each terminal in $\mathcal{M}$, i.e., interactive communication, though permitted, is not needed.

Thus, the largest rate at which the terminals in $A$ can generate a secret key is obtained by subtracting from the maximum rate of shared common randomness achievable by these terminals, viz. $H(X_1, \ldots, X_m)$ (corresponding to a lossless reconstruction of all the signals observed by all the terminals in $\mathcal{M}$), the smallest rate $R_{\min}(A)$ of data-compressed interterminal public communication needed for the reconstruction. This coupling of secrecy generation and data compression can be interpreted in terms of the following heuristic idea: If the rv $L = L(X_1^n, \ldots, X_m^n)$ represents common randomness for all the terminals in $A$, achievable through multidata compression using publicly sent codewords $F$, then a Slepian-Wolf codeword for $L$ with $F$ as “decoder side information” – of rate $\frac{1}{n}H(L|F)$ and which each terminal in $A$ now can construct from $L$ upon purging the effect of $F$ – constitutes a secret key (as $L$ must be nearly independent of $F$, else $L$ could be compressed further). In particular, when $L \equiv (X_1^n, \ldots, X_m^n)$,

$$\frac{1}{n}H(L|F) \cong \frac{1}{n}H(X_1^n, \ldots, X_m^n|F) = H(X_1, \ldots, X_m) - \frac{1}{n}H(F),$$

which, with $F$ devised to be of the minimal rate in (4), leads to the capacity formula in (5).

III. RESULTS: THE PIN SOURCE MODEL

The “pairwise independent network” (PIN) source model introduced in [17], [18] reveals an intriguing point of contact between secrecy generation with public communication and a combinatorial problem of the maximal packing of Steiner trees in a multigraph [16].

The PIN model is a special case of the multiterminal source model of section II above, with every pair of terminals observing correlated signals which are independent of the signals observed by all other pairs of terminals. Specifically, each terminal $i \in \mathcal{M} = \{1, \ldots, m\}$ observes a signal $X_i^n$ consisting of $n$ i.i.d. repetitions of the rv $X_i$, with $X_i$ being of the special form $X_i = (Y_{ij}, j \in \mathcal{M}\{\{i\}\})$ with $m-1$ components, and the “reciprocal pairs” of rvs $(Y_{ij}, Y_{ji}), 1 \leq i \neq j \leq m$ are mutually independent. Thus, every pair of terminals $i, j$ in $\mathcal{M}$ is associated with a corresponding pair of rvs $(Y_{ij}, Y_{ji})$, which are independent of all other pairs of rvs $(Y_{ij'}, Y_{ji'})$ associated with the terminals $i', j'$ with $i' \neq i$ or $j' \neq j$ (or both). All the rvs are assumed to take their values in finite sets.

A particularization of (5) (using (4)) to the PIN model yields that its secret key capacity $C_S(A)$ is given by [16]

**Proposition 3.1:** For a PIN model, the SK capacity for a set of terminals $A \subseteq \mathcal{M}$, with $|A| \geq 2$, is

$$C_S(A) = \min_{\lambda \in \Lambda(A)} \left[ \sum_{1 \leq i < j \leq m} \left( \sum_{B \in B(A) : i \in B, j \in B^c} \lambda_B \right) I(Y_{ij} \wedge Y_{ji}) \right].$$

We remark that $I(Y_{ij} \wedge Y_{ji})$ is the optimum rate of a secret key that can be generated by the terminals $i, j$ acting in isolation of all the other terminals [12], [2] (and also follows as a special case of (5)). The dependence of the secret key capacity for the PIN model in (6) on the joint distribution of the underlying rvs only through the pairwise reciprocal mutual information terms, is noteworthy for two reasons: (i) it suggests the possibility that a secret key for the terminals in $A$ can be built from pairwise keys; and, as such, (ii) it hints at the possibility of a connection to algorithms for tree packing in order to propagate pairwise keys among the terminals in $A$. Both are validated through the following natural connection between secrecy generation for the PIN model and the combinatorial problem of tree packing in an associated multigraph, found in recent preliminary work [16].

Let $G = (V, E)$ be a multigraph, i.e., a connected undirected graph with no self-loops and with possibly multiple edges between any vertex pair, whose vertex set $V = \mathcal{M} = \{1, \ldots, m\}$ and edge set is $E$. For $A \subseteq \mathcal{M}$, a Steiner tree of $G$ is a subgraph of $G$ which is a tree and whose vertex set contains $A$. A Steiner 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. [9]). An exact formula for $\mu(A, G)$ constitutes an open problem [10], [4].

We can assume without any loss of generality that in the PIN model, all pairwise reciprocal mutual information values $I(Y_{ij} \wedge Y_{ji}), 1 \leq i \neq j \leq m$, are rational numbers, and hereafter restrict ourselves to those positive integers $n$ such that $nI(Y_{ij} \wedge Y_{ji})$ is integer-valued for all $1 \leq i \neq j \leq m$. For a PIN model, consider a sequence of associated multigraphs $\{G^{(n)} = (\mathcal{M}, E^{(n)})\}$, where $E^{(n)}$ is such that the number of edges between any pair of vertices $i, j$ is equal to $nI(Y_{ij} \wedge Y_{ji})$. As remarked above following Proposition 3.1, every pair of vertices $(i, j)$ in $G$ can generate a pairwise secret key of size $nI(Y_{ij} \wedge Y_{ji})$. By the definition of the PIN model, all such pairwise secret keys are mutually independent. Further, every Steiner tree serves to generate one bit of secret key for the terminals in $A$ [16]. Therefore, the secret key capacity $C_S(A)$ is always bounded below by the rate of the maximal Steiner tree packing. Precisely [16]

\[ \text{WeB1.2} \]
Theorem 3.2: For a PIN model, the SK capacity satisfies
\[ C_S(A) \geq \sup_{n \in \mathbb{N}} \frac{1}{n} \mu(A, G(n)). \] (7)
for every \( A \subseteq M \).

This connection between secrecy generation for the PIN model and Steiner tree packing has the following implications. First, from a theoretical standpoint, for a combinatorial problem of Steiner tree packing of a given multigraph, we can always find an associated PIN model whose secret key capacity affords a new upper bound for the rate of the maximal packing. Second, from an engineering standpoint, tree packing algorithms could play an important role in a PIN model for generating a group-wide secret key out of pairwise keys.

The latter implication is already felt in the situation when all the terminals in \( M \) wish to share a secret key, i.e., \( A = M \). Then, a Steiner tree is a spanning tree of \( G(n) \), and the bound in (7) is tight [16].

Theorem 3.3: (i) For a PIN model, the SK capacity \( C_S(M) \) is
\[ C_S(M) = \sup_{n \in \mathbb{N}} \frac{1}{n} \mu(M, G(n)). \] (8)
(ii) Furthermore, a polynomial-time algorithm exists for SK generation at the optimum rate in (8).

We remark that the previous algorithm (relying on [8]) generates a capacity-achieving secret key for the terminals in \( M \) out of optimum and mutually independent pairwise secret keys. However, there is no polynomial-time algorithm that exists for maximal Steiner tree packing [10], [4], [9].

IV. ACKNOWLEDGEMENT

P.N. thanks Samir Khuller for the very helpful pointer to [8].

REFERENCES