Secret Key Constructions for Simple Multiterminal Source Models

Chunxuan Ye
InterDigital Communications Corporation
King of Prussia, PA 19406
E-mail: Chunxuan.Ye@InterDigital.com

Prakash Narayan
Department of Electrical and Computer Engineering
and Institute for Systems Research
University of Maryland
College Park, MD 20742, USA
E-mail: prakash@eng.umd.edu

***Abstract*— This work is motivated by the results of Csiszár and Narayan (*IEEE Trans. on Inform. Theory, Dec. 2004*), which highlight innate connections between secrecy generation by multiple terminals and multiterminal Slepian-Wolf near-lossless data compression (sans secrecy restrictions). We propose a new approach for constructing secret keys based on the long-known Slepian-Wolf code for sources connected by a virtual additive noise channel, due to Wyner (*IEEE Trans. on Inform. Theory, Jan. 1974*). Explicit procedures for such constructions, and their substantiation, are provided.**

I. Introduction

The problem of secret key generation by multiple terminals, based on their observations of distinct correlated signals followed by public communication among themselves, has been investigated by several authors ([9], [1], among others). It has been shown that these terminals can generate common randomness which is kept secret from an eavesdropper privy to the public interterminal communication. Of particular relevance to us are results in [4] for models with an arbitrary number of terminals, each of which observes a distinct component of a discrete memoryless multiple source (DMMS). Unrestricted public communication is allowed between these terminals. All the transmissions are observed by all the terminals and by the eavesdropper. A model considered in [4] which is directly relevant to our work is briefly described next.

Suppose that $d \geq 2$ terminals observe n i.i.d. repetitions of the (finite-valued) random variables (rvs) $X_1, \cdots X_d$, denoted by $\mathbf{X}_1, \cdots, \mathbf{X}_d$, respectively. A secret key (SK) generated by these terminals consists of "common randomness" – based on *public* interterminal communication – which is concealed from an eavesdropper with access to this communication. The largest (entropy) rate of such a SK is termed the SK-capacity, denoted by C_{SK}, and is shown in [4] to equal

$$C_{SK} = H(X_1, \cdots, X_d) - R_{min}, \tag{1}$$

where

$$R_{min} = \min_{(R_1, \cdots, R_d) \in \mathcal{R}} \sum_{i=1}^{d} R_i,$$

with

$$\begin{aligned} \mathcal{R} \quad = \quad & \{(R_1, \cdots, R_d) : \sum_{i \in B} R_i \geq \\ & H(\{X_j,\ j \in B\} | \{X_j,\ j \in B^c\}), B \subset \{1, \cdots, d\}\}, \end{aligned}$$

where $B^c = \{1, \cdots, d\} \backslash B$.

The result above affords the following interpretation. The SK-capacity C_{SK}, i.e., largest rate at which all the d terminals can generate a SK, is obtained by subtracting from the maximum rate of shared common randomness achievable by these terminals, viz. $H(X_1, \cdots, X_d)$, the smallest sum-rate R_{min} of the data-compressed interterminal communication which enables each of the terminals to acquire this maximal common randomness. It should be noted that R_{min} is obtained as a solution to a Slepian-Wolf (SW) multiterminal near-lossless data compression problem *not involving any secrecy constraints*. This characterization of the SK-capacity in terms of the decomposition above also mirrors the consecutive stages in the random coding argument for establishing the result. Loosely speaking, to generate a SK, the d terminals first generate common randomness (without any secrecy restrictions), say a rv L of entropy rate $\frac{1}{n}H(L) > 0$, through SW-compressed interterminal communication $\mathbf{F}$. This means that all the d terminals acquire the rv L with probability $\cong 1$. The next step entails an extraction from L of a SK $K = g(L)$ of entropy rate $\frac{1}{n}H(L|\mathbf{F})$, by means of a suitable operation performed *identically* at each terminal on the acquired common randomness L. When the common randomness first acquired by the d terminals is maximal, i.e., $L = (\mathbf{X}_1, \cdots, \mathbf{X}_d)$ with probability $\cong 1$, then the corresponding SK $K = g(L)$ has the best rate C_{SK} given by (1).

The discussion above suggests that techniques for multiterminal SW data compression could be used for the *construction* of SKs. Next, in SW coding, the existence of linear data compression codes with rates arbitrarily close to the SW bound has been long known [3]. In particular, when the i.i.d. sequences observed at the terminals are related to each other through virtual communication channels characterized by independent additive noises, such linear data compression codes can be obtained in terms of the cosets of linear error-correction codes for these virtual channels, a fact first illustrated in [13] for the special case of $d = 2$ terminals connected by a virtual binary symmetric channel (BSC). This fact, exploited by most known linear constructions of SW codes (cf. e.g. [2], [6], [8], [11]), can enable us to translate these constructions and other significant recent developments in capacity-achieving linear codes into new SK constructions. (See also recent independent

work [10] for related existence results, as also [12].)

Motivated by these considerations, we seek to devise new *constructive schemes* for secrecy generation. The main technical contribution of this work is the following: we consider two simple models of secrecy generation and show how a new class of secret keys can be constructed, based on the SW data compression code from [13]. While we do not specify exactly the linear capacity-achieving channel codes used in the SW step of the procedure, these can be chosen – for instance – from the class of LDPC [8] and turbo codes [6] that have attracted wide attention.

II. Preliminaries

Consider a DMMS with $d \geq 2$ components, with corresponding generic rvs $X_1, \cdots, X_d$ taking values in finite alphabets $\mathcal{X}_1, \cdots, \mathcal{X}_d$, respectively. Let $\mathbf{X}_i = (X_{i,1}, \cdots, X_{i,n})$, $i \in \mathcal{D} = \{1, \cdots, d\}$, be n i.i.d. repetitions of rv X_i. Terminals $1, \cdots, d$, with respective observations $\mathbf{X}_1, \cdots, \mathbf{X}_d$, represent the d users that wish to generate a SK by public communication. These terminals can communicate with each other through broadcasts over a noiseless public channel, possibly interactively in many rounds. In general, a transmission from a terminal is allowed to be any function of its observations, and of all previous transmissions. Let $\mathbf{F}$ denote collectively all the public transmissions.

Given $\varepsilon > 0$, the rv $K_{\mathcal{S}}$ represents an *ε-secret key* (ε-*SK*) for the terminals in $\mathcal{D}$, achieved with communication $\mathbf{F}$, if there exist rvs $K_i = K_i(\mathbf{X}_i, \mathbf{F})$, $i \in \mathcal{D}$, with K_i and $K_{\mathcal{S}}$ taking values in the same finite set $\mathcal{K}_{\mathcal{S}}$ such that $K_{\mathcal{S}}$ satisfies

- the common randomness condition

$$\Pr(K_i = K_{\mathcal{S}},\ i \in \mathcal{D}) \geq 1 - \varepsilon;$$

- the secrecy condition

$$\frac{1}{n} I(K_{\mathcal{S}} \wedge \mathbf{F}) \leq \varepsilon;$$

- the uniformity condition

$$\frac{1}{n} H(K_{\mathcal{S}}) \geq \frac{1}{n} \log |\mathcal{K}_{\mathcal{S}}| - \varepsilon.$$

Definition 1 [4]: A nonnegative number R is called an *achievable SK rate* if an ε_n-SK $K_{\mathcal{S}}^{(n)}$ is achievable with suitable communication (with the number of rounds possibly depending on n), such that $\varepsilon_n \to 0$ and $\frac{1}{n} H\left(K_{\mathcal{S}}^{(n)}\right) \to R$. The largest achievable SK rate is called the *SK-capacity*, denoted by C_{SK}. An achievable SK rate will be called strongly achievable if ε_n above can be taken to vanish exponentially in n. The corresponding capacity is termed strong capacity.

Single-letter characterizations have been provided for C_{SK} in the case of $d = 2$ terminals in [9], [1] and for $d \geq 2$ in [4]. The proofs of the achievability parts exploit the close connection between secrecy generation and SW data compression. For instance, "common randomness," without any secrecy restrictions, is first generated through SW-compressed interterminal communication. This means that all the d terminals acquire a rv with probability $\cong 1$. In the next step, secrecy is then extracted from this common randomness by means of a suitable *identical* operation performed at each terminal on the acquired common randomness. When the common randomness first acquired by the d terminals is maximal, then the corresponding secret key has the best rate C_{SK} given by (1).

In this work, we consider two simple models for which we illustrate the *construction* of appropriate *strong* secret keys, exploiting suitable SW codes. The SW codes of interest will rely on the following result concerning the existence of "good" linear channel codes for a BSC.

Hereafter, a BSC with crossover probability p, $0 < p < \frac{1}{2}$, will be denoted by BSC(p). Let h_b denote binary entropy.

Lemma 1 [5]: For every $\varepsilon > 0$, $0 < p < \frac{1}{2}$, and for all n sufficiently large, there exists a binary linear $(n, n-m)$ code for the BSC(p), with $m < n[h_b(p) + \varepsilon]$, such that the average error probability of maximum likelihood decoding is less than $2^{-n\eta}$, for some $\eta > 0$.

III. Main Results

MODEL 1: *Let the terminals* 1 *and* 2 *observe, respectively,* n *i.i.d. repetitions of the correlated rvs* X_1 *and* X_2*, where* X_1*,* X_2 *are* $\{0,1\}$*-valued rvs with joint probability mass function (pmf)*

$$P_{X_1X_2}(x_1, x_2) = \frac{1}{2}(1-p)\delta_{x_1x_2} + \frac{1}{2}p\ (1 - \delta_{x_1x_2}), \quad p < \frac{1}{2}, \tag{2}$$

with δ *being the Kronecker delta function. These two terminals wish to generate a strong SK of maximal rate.*

The SK-capacity for this model is [9], [1], [4]

$$C_{SK} = I(X_1 \wedge X_2) = 1 - h_b(p)\ bit/symbol.$$

We show a simple scheme for both terminals to generate a SK with rate close to $1 - h_b(p)$ bit/symbol, which relies on Wyner's well-known method for SW data compression [13]. The SW problem of interest entails terminal 2 reconstructing the observed sequence $\mathbf{x}_1$ at terminal 1 from the SW codeword for $\mathbf{x}_1$ and its own observed sequence $\mathbf{x}_2$.

(i) SW data compression [13]: Let $\mathcal{C}$ be the linear $(n, n-m)$ code specified in Lemma 1 with parity check matrix $\mathbf{P}$. Both terminals know $\mathcal{C}$ (and $\mathbf{P}$).

Terminal 1 transmits the syndrome $\mathbf{P}\mathbf{x}_1^t$ to terminal 2. The maximum likelihood estimate of $\mathbf{x}_1$ at terminal 2 is:

$$\hat{\mathbf{x}}_2(1) = \mathbf{x}_2 \oplus f_{\mathbf{P}}(\mathbf{P}\mathbf{x}_1^t \oplus \mathbf{P}\mathbf{x}_2^t),$$

where $f_{\mathbf{P}}(\mathbf{P}\mathbf{x}_1^t \oplus \mathbf{P}\mathbf{x}_2^t)$ is the most likely n-sequence $\mathbf{v}$ with syndrome $\mathbf{P}\mathbf{v}^t = \mathbf{P}\mathbf{x}_1^t \oplus \mathbf{P}\mathbf{x}_2^t$, with $\oplus$ denoting addition modulo 2 and t denoting transposition.

The probability of decoding error at terminal 2 is given by

$$\Pr(\hat{\mathbf{X}}_2(1) \neq \mathbf{X}_1) = \Pr(\mathbf{X}_2 \oplus f_{\mathbf{P}}(\mathbf{P}\mathbf{X}_1^t \oplus \mathbf{P}\mathbf{X}_2^t) \neq \mathbf{X}_1).$$

Under the given joint pmf (2), $\mathbf{X}_2$ can be considered as an input to a virtual BSC(p), while $\mathbf{X}_1$ is the corresponding output, i.e., we can write

$$\mathbf{X}_1 = \mathbf{X}_2 \oplus \mathbf{V},$$

where $\mathbf{V} = (V_1, \cdots, V_n)$ is an i.i.d. sequence of $\{0,1\}$-valued rvs, independent of $\mathbf{X}_2$, with $\Pr(V_i = 1) = p$, $1 \leq i \leq n$. It readily follows that

$$\Pr(\hat{\mathbf{X}}_2(1) \neq \mathbf{X}_1) = \Pr(f_{\mathbf{P}}(\mathbf{P}\mathbf{V}^t) \neq \mathbf{V}).$$

Therefore, we obtain from Lemma 1 that for some $\eta > 0$,

$$\Pr(\hat{\mathbf{X}}_2(1) \neq \mathbf{X}_1) < 2^{-n\eta},$$

for all n sufficiently large.

(ii) SK construction: Consider a (common) standard array for $\mathcal{C}$ known to both terminals. Denote by $\mathbf{a}_{i,j}$ the element of the i^{th} row and the j^{th} column in the standard array, $1 \leq i \leq 2^m$, $1 \leq j \leq 2^{n-m}$.

Terminal 1 sets $K_1 = j_1$ if $\mathbf{X}_1$ equals $\mathbf{a}_{i,j_1}$ in the standard array. Terminal 2 sets $K_2 = j_2$ if $\hat{\mathbf{X}}_2(1)$ equals $\mathbf{a}_{i,j_2}$ in the same standard array.

(iii) SK criteria: The following theorem shows that K_1 constitutes a strongly achievable SK with rate approaching the SK-capacity.

Theorem 1: The pair of rvs (K_1, K_2) generated above, with (common) range $\mathcal{K}_1$ (say), satisfy

$$\Pr(K_1 = K_2) \geq 1 - 2^{-n\eta};$$

$$I(K_1 \wedge \mathbf{F}) = 0;$$

$$H(K_1) = \log|\mathcal{K}_1|.$$

Further,

$$\frac{1}{n}H(K_1) > 1 - h_b(p) - \varepsilon.$$

Remark: The probability of K_1 being different from K_2 exactly equals the average error probability of maximum likelihood decoding when $\mathcal{C}$ is used on a BSC(p). Furthermore, the gap between the rate of the generated SK and the SK-capacity is as wide as the gap between the rate of $\mathcal{C}$ and the channel capacity. Therefore, if a "better" channel code for a BSC(p), in the sense that the rate of this code is closer to the channel capacity and the average error probability of maximum likelihood decoding is smaller, is applied, then a "better" SK can be generated at both terminals, in the sense that the rate of this SK is closer to the SK-capacity and the probability is smaller that the keys generated at different terminals do not agree with each other.

The next model is an instance of a *Markov chain on a tree* (cf. [7], [4]), which considers a tree $\mathcal{T}$ with vertex set $V(\mathcal{T}) = \{1, \cdots, d\}$ and edge set $E(\mathcal{T})$. For $(i,j) \in E(\mathcal{T})$, let $B(i \leftarrow j)$ denote the set of all vertices connected with j by a path containing the edge (i,j). The rvs $X_1, \cdots, X_d$ form a *Markov chain on the tree* $\mathcal{T}$ if for each $(i,j) \in E(\mathcal{T})$, the conditional pmf of X_j given $\{X_l, l \in B(i \leftarrow j)\}$ depends only on X_i (i.e., is conditionally independent of $\{X_l, l \in B(i \leftarrow j)\}\backslash\{X_i\}$, conditioned on X_i). Note that when $\mathcal{T}$ is a chain, this concept reduces to that of a standard Markov chain.

MODEL 2: *Let the terminals $1, \cdots, d$ observe, respectively, n i.i.d. repetitions of $\{0,1\}$-valued rvs $X_1, \cdots, X_d$ which form a Markov chain on the tree $\mathcal{T}$, and have a joint pmf $P_{X_1 \cdots X_d}$ described in the following manner: for $(i,j) \in E(\mathcal{T})$,*

$$P_{X_i X_j}(x_i, x_j) = \frac{1}{2}(1 - p_{(i,j)})\delta_{x_i x_j} + \frac{1}{2}p_{(i,j)}\ (1 - \delta_{x_i x_j}),$$

where $p_{(i,j)} < \frac{1}{2}$ and $x_i, x_j \in \{0,1\}$. These d terminals wish to generate a strong SK of maximal rate.

Note that Model 1 is a special case of Model 2 for $d = 2$. Without any loss of generality, let

$$p_{max} = p_{(i^*,j^*)} = \max_{(i,j)\in E(\mathcal{T})} p_{(i,j)}.$$

Then, the SK-capacity for this model is [4]

$$C_{SK} = I(X_{i^*} \wedge X_{j^*}) = 1 - h_b(p_{max})\ bit/symbol.$$

We show below how to extract a SK with rate close to $1 - h_b(p_{max})$ by using a SW data compression scheme for reconstructing $\mathbf{x}_{i^*}$ at all the terminals.

(i) SW data compression: Let $\mathcal{C}$ be the linear $(n, n-m)$ code as in Lemma 1 for the BSC(p_{max}), with parity check matrix $\mathbf{P}$. Each terminal i transmits the syndrome $\mathbf{P}\mathbf{x}_i^t$, $1 \leq i \leq d$.

Let $\hat{\mathbf{x}}_i(j)$ denote the maximum likelihood estimate at terminal i of $\mathbf{x}_j$, $i \neq j$. For a terminal i, $i \neq i^*$, denote by $(i_0, i_1, \cdots, i_r)$ the (only) path in the tree $\mathcal{T}$ from i to i^*, where $i_0 = i$ and $i_r = i^*$; this terminal i, with the knowledge of $(\mathbf{x}_i,\ \mathbf{P}\mathbf{x}_{i_1}^t, \cdots, \mathbf{P}\mathbf{x}_{i_{r-1}}^t, \mathbf{P}\mathbf{x}_{i^*}^t)$, forms its estimate $\hat{\mathbf{x}}_i(i^*)$ of $\mathbf{x}_{i^*}$ through the following successive maximum likelihood estimates of $\mathbf{x}_{i_1}, \cdots, \mathbf{x}_{i_{r-1}}$:

$$\begin{aligned}
\hat{\mathbf{x}}_i(i_1) &= \mathbf{x}_i \oplus f_{\mathbf{P}}(\mathbf{P}\mathbf{x}_i^t \oplus \mathbf{P}\mathbf{x}_{i_1}^t),\\
\hat{\mathbf{x}}_i(i_2) &= \hat{\mathbf{x}}_i(i_1) \oplus f_{\mathbf{P}}(\mathbf{P}\mathbf{x}_{i_1}^t \oplus \mathbf{P}\mathbf{x}_{i_2}^t),\\
&\vdots\ \ \vdots\ \ \vdots\\
\hat{\mathbf{x}}_i(i_{r-1}) &= \hat{\mathbf{x}}_i(i_{r-2}) \oplus f_{\mathbf{P}}(\mathbf{P}\mathbf{x}_{i_{r-2}}^t \oplus \mathbf{P}\mathbf{x}_{i_{r-1}}^t)
\end{aligned}$$

and finally,

$$\hat{\mathbf{x}}_i(i^*) = \hat{\mathbf{x}}_i(i_{r-1}) \oplus f_{\mathbf{P}}(\mathbf{P}\mathbf{x}_{i_{r-1}}^t \oplus \mathbf{P}\mathbf{x}_{i^*}^t).$$

It can be shown that for some $\eta' = \eta'(\eta, d) > 0$,

$$\Pr(\hat{\mathbf{X}}_i(i^*) = \mathbf{X}_{i^*}, 1 \leq i \neq i^* \leq d) > 1 - 2^{-n\eta'}.$$

(ii) SK construction: Consider a (common) standard array for $\mathcal{C}$ known to all the terminals. Denote by $\mathbf{a}_{l,k}$ the element of the l^{th} row and the k^{th} column in the standard array, $1 \leq l \leq 2^m$, $1 \leq k \leq 2^{n-m}$.

Terminal i^* sets $K_{i^*} = k_{i^*}$ if $\mathbf{X}_{i^*}$ equals $\mathbf{a}_{l,k_{i^*}}$ in the standard array. Terminal i, $1 \leq i \neq i^* \leq d$, sets $K_i = k_i$ if $\hat{\mathbf{X}}_i(i^*)$ equals $\mathbf{a}_{l,k_i}$ in the same standard array.

(iii) SK criteria: The following theorem shows that K_{i^*} constitutes a strongly achievable SK with rate approaching the SK-capacity.

Theorem 2: The set of rvs $(K_1, \cdots, K_d)$ generated above, with range $\mathcal{K}_{i^*}$ (say), satisfy

$$\Pr(K_1 = \cdots = K_d) \geq 1 - 2^{-n\eta'};$$

$$I(K_{i^*} \wedge \mathbf{F}) = 0;$$

$$H(K_{i^*}) = \log |\mathcal{K}_{i^*}|.$$

Further,

$$\frac{1}{n} H(K_{i^*}) > 1 - h_b(p_{max}) - \varepsilon.$$

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] T. P. Coleman, A. H. Lee, M. Médard, and M. Effros, "On some new approaches to practical Slepian-Wolf compression inspired by channel coding," *Proc. IEEE Data Compression Conference*, pp. 282–291, Snowbird, UT, March 2004.

[3] I. Csiszár, "Linear codes for sources and source networks: Error exponents, universal coding," *IEEE Trans. Inform. Theory*, vol. 28, no. 4, pp. 585–592, July, 1982.

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

[5] P. Elias, "Coding for noisy channels," *IRE Convention Record*, Part 4, pp. 37–46, 1955.

[6] J. Garcia-Frias and Y Zhao, "Compression of correlated binary sources using turbo codes," *IEEE Commun. Lett.*, vol. 5, pp. 417–419, Oct. 2001.

[7] H. O. Georgii, *Gibbs Measures and Phase Transitions.* de Gruyter, Berlin – New York, 1988.

[8] A. D. Liveris, Z. Xiong, C. N. Georghiades, "Compression of binary sources with side information at the decoding using LDPC codes," *IEEE Commun. Lett.*, vol. 6, pp. 440–442, Oct. 2002.

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

[10] J. Muramatsu, "Secret key agreement from correlated source outputs using LDPC matrices," *IEICE Trans. Fundamentals*, vol. E87-A, 2004.

[11] S. S. Pradhan and K. Ramchandran, "Distributed source coding using syndromes (DISCUS): Design and construction," *IEEE Trans. Inform. Theory*, vol. 49, pp. 626–643, March 2003.

[12] A. Thangaraj, S. Dihidar, A. R. Calderbank, S. McLaughlin and J. M. Merolla, "Capacity achieving codes for the wiretap channel with applications to quantum key distribution," e-print cs. IT/0411003, 2004.

[13] A. D. Wyner, "Recent results in the Shannon theory," *IEEE Trans. Inform. Theory*, vol. 20, pp. 2–10, Jan. 1974.