Secret Key and Private Key Constructions for Simple Multiterminal Source Models

Chunxuan Ye, *Senior Member, IEEE*, and Prakash Narayan, *Fellow, IEEE*

***Abstract*—We propose an approach for constructing secret and private keys based on the long-known Slepian–Wolf code, due to Wyner, for correlated sources connected by a virtual additive noise channel. Our work is motivated by results of Csiszár and Narayan which highlight innate connections between secrecy generation by multiple terminals that observe correlated source signals and Slepian–Wolf near-lossless data compression. Explicit procedures for such constructions and their substantiation are provided. The performance of low-density parity check channel codes in devising a new class of secret keys is examined.**

***Index Terms*—Binary symmetric channel, LDPC codes, maximum likelihood decoding, perfect secrecy, private key capacity, private key construction, secret key capacity, secret key construction, Slepian–Wolf data compression.**

I. Introduction

THE problem of secrecy generation by multiple terminals, based on their observations of separate but correlated signals followed by public communication among themselves, has been investigated by several authors ([31], [2], [6], [11], among others). It has been shown that these terminals can generate secrecy, namely "common randomness" which is kept secret from an eavesdropper that is privy to said public communication and perhaps also to additional "wiretapped" side information. For instance, in [31] and [6], this is accomplished in three phases termed advantage distillation, information reconciliation and privacy amplification.

Our work is motivated by [12] which studies secrecy generation for multiterminal "source models" with an arbitrary number of terminals, each of which observes a distinct component of a discrete memoryless multiple source (DMMS). Specifically, suppose that $d \geq 2$ terminals observe, respectively, n independent and identically distributed (i.i.d.) repetitions of finite-valued random variables (rvs) $X_1, \ldots, X_d$, denoted by $\mathbf{X}_1, \ldots, \mathbf{X}_d$, where $\mathbf{X}_i = (X_{i1}, \ldots, X_{in})$, $i = 1, \ldots, d$. Thereupon, unrestricted and noiseless public communication is allowed among the terminals. All such communication is observed by all the terminals and by the eavesdropper. The eavesdropper is assumed to be passive, i.e., unable to tamper with the public communication of the terminals. In this framework, two models considered in [12] dealing with a *secret key* (SK) and a *private key* (PK) are pertinent to our work.

(i) *Secret key*: Suppose that all the terminals in $\{1, \ldots, d\}$ wish to generate a SK, i.e., common randomness which is concealed from the eavesdropper with access to their public communication and which is nearly uniformly distributed.[1] The largest (entropy) rate of such a SK, termed the SK capacity and denoted by C_S, is shown in [12] to equal

$$C_S = H(X_1, \ldots, X_d) - R_{\min} \tag{1}$$

where

$$R_{\min} = \min_{(R_1, \ldots, R_d) \in \mathcal{R}} \sum_{i=1}^{d} R_i \tag{2}$$

with[2]

$$\mathcal{R} = \{(R_1, \ldots, R_d) \colon \sum_{i \in B} R_i \geq H(\{X_j,\, j \in B\} | \{X_j,\, j \in B^c\}), B \subset \{1, \ldots, d\}\} \tag{3}$$

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

(ii) *Private key*: For a given subset $A \subset \{1, \ldots, d\}$, a PK for the terminals in A, private from the terminals in A^c, is a SK generated by the terminals in A with the cooperation of the terminals in A^c, which is concealed from an eavesdropper with access to the public interterminal communication and also from the cooperating terminals in A^c (and, hence, private).[3] The largest (entropy) rate of such a PK, termed the PK capacity and denoted by $C_P(A)$, is shown in [12] to be

$$\begin{aligned} C_P(A) &= H(X_1, \ldots, X_d) - H(\{X_i,\, i \in A^c\}) - R_{\min}(A) \\ &= H(\{X_i,\, i \in A\} | \{X_i,\, i \in A^c\}) - R_{\min}(A) \end{aligned} \tag{4}$$

where

$$R_{\min}(A) = \min_{\{R_i,\, i \in A\} \in \mathcal{R}(A)} \sum_{i \in A} R_i \tag{5}$$

[1] In [12], a general situation is studied in which a subset of the terminals generate a SK with the cooperation of the remaining terminals.

[2] Here, $\subset$ denotes a proper subset.

[3] A general model is considered in [12] for privacy from a subset of A^c of the cooperating terminals.

Manuscript received August 11, 2010; revised June 16, 2011; accepted September 20, 2011. Date of current version February 08, 2012. The work of C. Ye and P. Narayan was supported by the National Science Foundation under Grants CCF0515124, CCF0635271, and CCF0830697. The material in this paper was presented in part at the 2005 IEEE International Symposium on Information Theory, and at the Information Theory and Applications Workshop, San Diego, CA, Feb. 2006.

C. Ye was with the Department of Electrical and Computer Engineering, and the Institute for Systems Research, University of Maryland, College Park, MD 20742 USA. He is now with InterDigital Communications, LLC, King of Prussia, PA 19406 USA (e-mail: chunxuan.ye@interdigital.com).

P. Narayan is with the Department of Electrical and Computer Engineering, and the Institute for Systems Research, University of Maryland, College Park, MD 20742 USA (e-mail: prakash@eng.umd.edu).

Communicated by E. Erkip, Associate Editor for Shannon Theory.

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TIT.2011.2173731

with

$$\mathcal{R}(A) = \{\{R_i,\ i \in A\} : \sum_{i \in B} R_i \geq H(\{X_j,\ j \in B\}|\{X_j,\ j \in B^c\}),\ B \subset A\}. \quad (6)$$

The expressions in (1)–(3) and (4)–(6) afford the following interpretation [12]. The joint entropy $H(X_1, \ldots, X_d)$ in (1) corresponds to the maximum rate of shared common randomness—sans secrecy constraints—that can ever be achieved by the terminals in $\{1, \ldots, d\}$ when each terminal becomes *omniscient*, i.e., reconstructs all the components of the DMMS with probability $\cong 1$ as the observation length n becomes large. Further, $R_{\min}$ in (2), (3) corresponds to the smallest aggregate rate of interterminal communication that enables every terminal to achieve omniscience [12]. Thus, from (1), the SK capacity C_S, i.e., the largest rate at which all the terminals in $\{1, \ldots, d\}$ can generate a SK, is obtained by subtracting from the maximum rate of shared common randomness achievable by these terminals, viz., $H(X_1, \ldots, X_d)$, the smallest overall rate $R_{\min}$ of the (data-compressed) interterminal communication that enables all the terminals to become omniscient. A similar interpretation holds for the PK capacity $C_P(A)$ in (4) as well, with the difference that the terminals in A^c, which cooperate in secrecy generation and yet must not be privy to the secrecy they help generate, can be assumed—without loss of generality—to simply "reveal" their observations [12]. Hence, the entropy terms in (1), (3) are now replaced in (4), (6) with additional conditioning on $\{X_i,\ i \in A^c\}$. It should be noted that $R_{\min}$ and $R_{\min}(A)$ are obtained as solutions to multiterminal Slepian–Wolf (SW) (near-lossless) data compression problems *not involving any secrecy constraints*.

The form of characterization of the SK and PK capacities in (1) and (4) also suggests successive steps for generating the corresponding keys. For instance, and loosely speaking, in order to generate a SK, the terminals in $\{1, \ldots, d\}$ first generate common randomness (without any secrecy restrictions) using SW-compressed interterminal communication denoted collectively by, say, $\mathbf{F}$. Thus, the terminals generate rvs $L_i = L_i(\mathbf{X}_i, \mathbf{F}),\ i \in \{1, \ldots, d\}$, with $\frac{1}{n}H(L_i) > 0$, which agree with probability $\cong 1$ for n suitably large; suppressing subscripts, let L denote the resulting "common" rv where $\frac{1}{n}H(L) > 0$. The second 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 g performed *identically* at each terminal on the acquired common randomness L. In particular, when the common randomness acquired by the terminals corresponds to omniscience, i.e., $L \cong (\mathbf{X}_1, \ldots, \mathbf{X}_d)$, and is achieved using interterminal communication $\mathbf{F}$ of the most parsimonious rate $\cong R_{\min}$ in (2), then the corresponding SK $K = g(L)$ has the best rate C_S given by (1). It is important to note, however, that as mentioned in [12, Sec. VI], and already known from [31] and [2], neither communication by every terminal nor omniscience is essential for generating secrecy (SK or PK) at the best rate; for instance, the rv L above need not correspond to omniscience for the SK $K = g(L)$ to have the best possible rate in (1).

A similar approach as above can be used to generate a PK of the largest rate in (4).

The discussion above suggests that techniques for SW data compression could be used to devise constructive schemes for obtaining SKs and PKs that achieve the corresponding capacities. Further, in SW data compression, the existence of linear encoders of rates arbitrarily close to the SW bound has been long known [9]. In the special situation when the i.i.d. sequences observed at the terminals are related to each other in probability law through virtual discrete memoryless channels (DMCs) characterized by independent additive noises, such linear SW encoders can be obtained in terms of cosets of linear error correction codes for such virtual channels, a fact first illustrated in [48] for the case of $d = 2$ terminals connected by a virtual binary symmetric channel (BSC), and later exploited in most known linear constructions of SW encoders (cf. e.g., [1], [8], [16], [17], [21], [23], [24], [26], [27], [32], [37], [43]). When the i.i.d. sequences observed by $d = 2$ terminals are connected by an arbitrary virtual DMC, the corresponding SW data compression can be viewed in terms of coding for a "semisymmetric" channel, i.e., a channel with independent additive noise that is defined over an enlarged alphabet [20]; the case of stationary ergodic observations at the terminals is also considered therein. These developments in SW data compression can translate into an emergence of new constructive schemes for secrecy generation.

Motivated by these considerations, we seek to devise new constructive schemes for secrecy generation in source models in which SW data compression plays a central role. The main technical contribution of this work is the following: Considering four simple models of secrecy generation, we show how a new class of SKs and PKs can be devised for them at rates arbitrarily close to the corresponding capacities, relying on the SW data compression code in [48]. In all these models, *the secrecy capacities are attained with perfect secrecy*, i.e., *with the corresponding SKs and PKs being exactly independent of the eavesdropper's knowledge and being exactly uniformly distributed*. Additionally, we examine the performance of low-density parity check (LDPC) codes in the SW data compression step of the procedure for secrecy generation. Preliminary results of this work have been reported in [49] and [50]. In independent work [33] for the case of $d = 2$ terminals which is akin to but different from ours, extraction of a SK from previously acquired common randomness by means of a linear transformation has been demonstrated. Also, in related work, SK generation for a source model with two terminals that observe continuous-amplitude signals, has been studied in [51], [47], [34], [35], [52].

We do not consider here the notion of a "wiretap" SK for a multiterminal source model [31], [2], [12]. This notion, more restrictive than that of a PK above, obtains when the wiretapped terminals in A^c *do not cooperate in secrecy generation*; specifically, they do not engage in public discussion. A single-letter characterization of the corresponding capacity of this practically relevant model remains unresolved in general but for partial results and bounds (cf. e.g., [31], [2], [38], [12], [13], [19]). However, it should be mentioned that the source model without a wiretapper, too, is of practical interest; see [51], [52].

In recent years, several secrecy generation schemes have been reported, relying on capacity-achieving channel codes, for "wiretap" secrecy models that differ from ours. For instance, it was shown in [45], [46] that such a channel code can attain the secrecy capacity for any wiretap channel. See also [7], [25].

Recently discovered polar channel codes [4], [5] have been considered for achieving wiretap secrecy capacity; see [29], [22], and [3]. The use of polar codes in SK and PK generation for our source models is not considered here.

The paper is organized as follows. Preliminaries are contained in Section II. In Section III, we consider four simple source models for which we provide elementary constructive schemes for SK or PK generation which rely on suitable SW data compression codes; the keys thereby generated are shown to satisfy the requisite secrecy and rate-optimality conditions in Section IV. Implementations of these constructions using LDPC codes are illustrated in Section V which also reports simulation results. Section VI contains closing remarks.

II. Preliminaries

A. Secret Key and Private Key Capacities

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

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

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

- secrecy condition

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

- uniformity condition

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

Let $A \subset \mathcal{D}$ be an arbitrary subset of the terminals. The rv $K_{\mathcal{P}}(A)$ represents an *ε-private key* (*ε -PK*) for the terminals in A, private from the terminals in $A^c = \mathcal{D} \backslash A$, achieved with communication $\mathbf{F}$, if there exist rvs $K_i = K_i(\mathbf{X}_i, \mathbf{F})$, $i \in A$, with K_i and $K_{\mathcal{P}}(A)$ taking values in the same finite set $\mathcal{K}_{\mathcal{P}}(A)$, such that $K_{\mathcal{P}}(A)$ satisfies the

- common randomness condition

$$\Pr\{K_i = K_{\mathcal{P}}(A),\ i \in A\} \geq 1 - \varepsilon$$

- secrecy condition

$$\frac{1}{n} I\left(K_{\mathcal{P}}(A) \wedge \{\mathbf{X}_i,\ i \in A^c\}, \mathbf{F}\right) \leq \varepsilon$$

- uniformity condition

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

Definition 1 [12]: A nonnegative number R is called an *achievable SK rate* if ε_n-SKs $K_S^{(n)}$ are achievable with suitable communication (with the number of rounds possibly depending on n), such that $\varepsilon_n \to 0$ and $\frac{1}{n} H\left(K_S^{(n)}\right) \to R$ as $n \to \infty$. The largest achievable SK rate is called the *SK capacity*, denoted by C_S. The PK capacity for the terminals in A, denoted by $C_P(A)$, is similarly defined. An achievable SK rate (respectively, PK rate) will be called *strongly achievable* if ε_n above can be taken to vanish exponentially in n. The corresponding capacities are termed *strong capacities*. A SK (respectively, PK) is *perfect* if it meets the corresponding secrecy and uniformity conditions with $\epsilon = 0$ for all n sufficiently large.

Single-letter characterizations have been obtained for C_S in the case of $d = 2$ terminals in [2], [31] and for $d \geq 2$ terminals in [12], given by (1); and for $C_P(A)$ in the case of $d = 3$ terminals in [2] and for $d \geq 3$ terminals in [12], given by (4). The proofs of the achievability parts exploit the close connection between secrecy generation and SW data compression. Loosely speaking, common randomness sans any secrecy restrictions is first generated through SW-compressed interterminal communication, whereby all the d terminals acquire a (common) rv with probability $\cong 1$. In the next step, secrecy is then extracted by means of a suitable *identical* operation performed at each terminal on the acquired common randomness. When the common randomness initially acquired by the d terminals is maximal, the corresponding SK has the best rate C_S given by (1).

In this work, we consider four simple models for which we illustrate the constructions of appropriate *perfect* SKs or PKs.

B. Linear Codes for the Binary Symmetric Channel

The SW codes of interest will rely on the following classic result concerning the existence of "good" linear channel codes for a BSC. A BSC with crossover probability p, $0 < p < \frac{1}{2}$, will be denoted by BSC(p). Let $h(p) = -p \log_2 p - (1-p) \log_2 (1-p)$ denote the binary entropy function.

Lemma 1 [14]: 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 a $\mathrm{BSC}(p)$, with $m < n[h(p) + \varepsilon]$, such that the average error probability of maximum likelihood decoding is less than $2^{-n\eta}$, for some $\eta > 0$.

Proof: See for instance [42, Th. 4.7]. ∎

C. Types and Typical Sequences

The following standard facts regarding "types" and "typical sequences" and their pertinent properties (cf. e.g., [10]) are compiled here in brief for ready reference.

Given finite sets $\mathcal{X}$, $\mathcal{Y}$, the *type* of a sequence $\mathbf{x} = (x_1, \ldots, x_n) \in \mathcal{X}^n$, $\mathcal{X}$ a finite set, is the probability mass function (pmf) $P_{\mathbf{x}}$ on $\mathcal{X}$ given by

$$P_{\mathbf{x}}(a) = \frac{1}{n}|\{i : x_i = a\}|,\ a \in \mathcal{X}$$

and the *joint type* of a pair of sequences $(\mathbf{x}, \mathbf{y}) \in \mathcal{X}^n \times \mathcal{Y}^n$ is the joint pmf $P_{\mathbf{xy}}$ on $\mathcal{X} \times \mathcal{Y}$ given by

$$P_{\mathbf{xy}}(a, b) = \frac{1}{n}|\{i : x_i = a, y_i = b\}|,\ a \in \mathcal{X},\ b \in \mathcal{Y}.$$

The numbers of different types of sequences in $\mathcal{X}^n$ (respectively, $\mathcal{X}^n \times \mathcal{Y}^n$) do not exceed $(n+1)^{|\mathcal{X}|}$ (respectively, $(n+1)^{|\mathcal{X}||\mathcal{Y}|}$).

Given rvs X, Y (taking values in $\mathcal{X}$, $\mathcal{Y}$, respectively), with joint pmf P_{XY} on $\mathcal{X} \times \mathcal{Y}$, the set of sequences in $\mathcal{X}^n$ which are *X–ξ -typical*, denoted by $T^n_{X,\xi}$, is defined as

$$T^n_{X,\xi} \triangleq \left\{\mathbf{x} \in \mathcal{X}^n : 2^{-n[H(X)+\xi]} \le P^n_X(\mathbf{x}) \le 2^{-n[H(X)-\xi]}\right\}$$

where $P^n_X(\mathbf{x}) \triangleq \Pr\{\mathbf{X} = \mathbf{x}\}$, $\mathbf{x} \in \mathcal{X}^n$; and the set of pairs of sequences in $\mathcal{X}^n \times \mathcal{Y}^n$ which are *XY–ξ-typical*, denoted by $T^n_{XY,\xi}$, is defined as

$$\begin{aligned}T^n_{XY,\xi} \triangleq \{(\mathbf{x}, \mathbf{y}) \in \mathcal{X}^n \times \mathcal{Y}^n : \mathbf{x} \in T^n_{X,\xi}, \mathbf{y} \in T^n_{Y,\xi},\\ 2^{-n[H(X,Y)+\xi]} \le P^n_{XY}(\mathbf{x}, \mathbf{y}) \le 2^{-n[H(X,Y)-\xi]}\}\end{aligned}$$

where $P^n_{XY}(\mathbf{x}, \mathbf{y}) \triangleq \Pr\{\mathbf{X} = \mathbf{x}, \mathbf{Y} = \mathbf{y}\}, \mathbf{x} \in \mathcal{X}^n, \mathbf{y} \in \mathcal{Y}^n$. It readily follows that for every $(\mathbf{x}, \mathbf{y}) \in T^n_{XY,\xi}$,

$$2^{-n[H(X|Y)+2\xi]} \le P^n_{X|Y}(\mathbf{x}|\mathbf{y}) \le 2^{-n[H(X|Y)-2\xi]}$$

where $P^n_{X|Y}(\mathbf{x}|\mathbf{y}) \triangleq \Pr\{\mathbf{X} = \mathbf{x}|\mathbf{Y} = \mathbf{y}\}, \mathbf{x} \in \mathcal{X}^n, \mathbf{y} \in \mathcal{Y}^n$.

For every $\mathbf{y} \in \mathcal{Y}^n$, the set of sequences in $\mathcal{X}^n$ which are *$X|Y$–ξ-typical with respect to* $\mathbf{y}$, denoted by $T^n_{X|Y,\xi}(\mathbf{y})$, is defined as

$$T^n_{X|Y,\xi}(\mathbf{y}) \triangleq \left\{\mathbf{x} \in \mathcal{X}^n : (\mathbf{x}, \mathbf{y}) \in T^n_{XY,\xi}\right\}$$

with $T^n_{X|Y,\xi}(\mathbf{y}) = \phi$ if $\mathbf{y} \notin T^n_{Y,\xi}$. The following is an independent and explicit statement of the well-known fact that the probability of a nontypical set decays to 0 exponentially rapidly in n (cf. e.g., [53, Th. 6.3]).

Proposition 1: Given a joint pmf P_{XY} on $\mathcal{X} \times \mathcal{Y}$ with $P_{XY}(x, y) > 0, x \in \mathcal{X}, y \in \mathcal{Y}$, for every $\xi > 0$,

$$\sum_{\mathbf{x} \in T^n_{X,\xi}} P^n_X(\mathbf{x}) \ge 1 - (n+1)^{|\mathcal{X}|} \cdot 2^{-n \frac{\xi^2}{2 \ln 2 \left[\sum_{a \in \mathcal{X}} \log \frac{1}{P_X(a)}\right]^2}} \quad (7)$$

and

$$\sum_{(\mathbf{x},\mathbf{y}) \in T^n_{XY,\xi}} P^n_{XY}(\mathbf{x}, \mathbf{y}) \ge 1 - (n+1)^{|\mathcal{X}||\mathcal{Y}|} \cdot 2^{-n \frac{\xi^2}{2 \ln 2 \left[\sum_{(a,b) \in \mathcal{X} \times \mathcal{Y}} \log \frac{1}{P_{XY}(a,b)}\right]^2}} \quad (8)$$

for all $n \ge 1$.

Proof: See Appendix A for a simple proof that is of independent interest. ∎

III. Main Results

We now present our main results on SK generation for three specific models, and PK generation for a fourth model. The proofs of the accompanying Theorems 1–4 are provided in Section IV.

A. Model 1

Let the terminals 1 and 2 observe, respectively, n i.i.d. repetitions of the $\{0,1\}$-valued rvs X_1 and X_2 with joint pmf

$$P_{X_1 X_2}(x_1, x_2) = \frac{1}{2}(1-p)\delta_{x_1 x_2} + \frac{1}{2}p\,(1 - \delta_{x_1 x_2}),\quad 0 < p < \frac{1}{2} \quad (9)$$

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

The (strong) SK capacity for this model [2], [12], [31], given by (1), is

$$C_S = I(X_1 \wedge X_2) = 1 - h(p).$$

We show a simple scheme for the terminals to generate a SK with rate close to $1 - h(p)$, which relies on Wyner's well-known method for SW data compression [48]. 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 $\mathbf{x}_2$.

Observe that under the given joint pmf (9), $\mathbf{X}_2$ can be considered as an input to a virtual $\mathrm{BSC}(p)$, with corresponding output $\mathbf{X}_1$, i.e., we can write

$$\mathbf{X}_1 = \mathbf{X}_2 \oplus \mathbf{V} \quad (10)$$

where $\mathbf{V} = (V_1, \ldots, V_n)$ is an i.i.d. sequence of $\{0,1\}$-valued rvs, independent of $\mathbf{X}_2$ and with $\Pr\{V_i = 1\} = p, 1 \le i \le n$.

(i) *SW data compression* [48]: Let $\mathcal{C}$ be a linear $(n, n-m)$ code as in Lemma 1 with parity check matrix $\mathbf{P}$. Both terminals know $\mathcal{C}$ (and $\mathbf{P}$). Terminal 1 communicates 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 sequence $\mathbf{v} \in \{0,1\}^n$ (under the pmf of $\mathbf{V}$ as above) 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. Note that in a standard array corresponding to the code $\mathcal{C}$ above, $f_{\mathbf{P}}(\mathbf{P}\mathbf{x}_1^t \oplus \mathbf{P}\mathbf{x}_2^t)$ is simply the coset leader of the coset with syndrome $\mathbf{P}\mathbf{x}_1^t \oplus \mathbf{P}\mathbf{x}_2^t$. Also, $\mathbf{x}_1$ and $\hat{\mathbf{x}}_2(1)$ lie in the same coset. We remark that owing to the complexity of generating a standard array for large n, the maximum likelihood estimate applying such an array may be replaced in practice by other efficient decoding algorithms (cf. Section V-B).

The probability of decoding error at terminal 2 is given by

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

and it readily follows from (10) that

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

By Lemma 1, $\Pr\{f_{\mathbf{P}}(\mathbf{P}\mathbf{V}^t) \neq \mathbf{V}\} < 2^{-n\eta}$ for some $\eta > 0$ and for all n sufficiently large, so that

$$\Pr\{\hat{\mathbf{X}}_2(1) = \mathbf{X}_1\} \geq 1 - 2^{-n\eta}.$$

(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 its coset i 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 coset i of the same standard array.

The following theorem asserts that K_1 constitutes a perfect SK with rate approaching SK capacity.

Theorem 1: Let $\varepsilon > 0$ be given. Then for some $\eta > 0$ and for all n sufficiently large, the pair of rvs (K_1, K_2) generated above, with (common) range $\mathcal{K}_1$ (say), satisfy

$$\Pr\{K_1 = K_2\} \geq 1 - 2^{-n\eta} \tag{11}$$

$$I(K_1 \wedge \mathbf{F}) = 0 \tag{12}$$

$$H(K_1) = \log|\mathcal{K}_1| \tag{13}$$

$$\frac{1}{n}H(K_1) > 1 - h(p) - \varepsilon. \tag{14}$$

Remark: The probability of K_1 differing from K_2 equals exactly the average error probability of maximum likelihood decoding when $\mathcal{C}$ is used on a $\mathrm{BSC}(p)$. Furthermore, the gap between the rate of the generated SK and SK capacity equals the gap between the rate of $\mathcal{C}$ and channel capacity.

B. Model 2

Let the terminals 1 and 2 observe, respectively, n i.i.d. repetitions of the $\{0,1\}$-valued rvs with joint pmf

$$\begin{aligned} P_{X_1X_2}(0,0) &= (1-p)(1-q) \\ P_{X_1X_2}(0,1) &= pq \\ P_{X_1X_2}(1,0) &= p(1-q) \\ P_{X_1X_2}(1,1) &= q(1-p) \end{aligned} \tag{15}$$

with $0 < p < \frac{1}{2}$ and $0 < q < 1$. These terminals wish to generate a strong SK of maximum rate.

Note that Model 1 is a formal special case of Model 2 for $q = \frac{1}{2}$. However, we choose to present them separately since the SK construction and proof of achievability of SK capacity for the former are elementary and do not involve typicality arguments unlike the latter.

We show below a scheme for the terminals to generate a SK with rate close to the (strong) SK capacity for this model [2], [12], [31], which is given by (1) as

$$C_S = I(X_1 \wedge X_2) = h(p + q - 2pq) - h(p).$$

(i) *SW data compression*: This step is identical to step (i) for Model 1. Note that under the given joint pmf (15), $\mathbf{X}_1$ and $\mathbf{X}_2$ can be written as in (10). It follows in the same manner as for Model 1 that for some $\eta > 0$ and for all n sufficiently large

$$\Pr\{\hat{\mathbf{X}}_2(1) = \mathbf{X}_1\} \geq 1 - 2^{-n\eta}.$$

(ii) *SK construction*: Both terminals know the linear $(n, n-m)$ code $\mathcal{C}$ as in Lemma 1, and a (common) standard array for $\mathcal{C}$. Let $\{\mathbf{e}_i : 1 \leq i \leq 2^m\}$ denote the set of coset leaders for all the cosets of $\mathcal{C}$.

Denote by A_i the set of sequences from $T^n_{X_1,\xi}$ in the coset of $\mathcal{C}$ with coset leader $\mathbf{e}_i$, $1 \leq i \leq 2^m$. If the number of sequences of the same type in A_i is more than $2^{n[I(X_1 \wedge X_2) - \varepsilon']}$, where $\varepsilon' > \xi + \varepsilon$ with ε satisfying $m < n[h(p) + \varepsilon]$ in Lemma 1, then collect arbitrarily $2^{n[I(X_1 \wedge X_2) - \varepsilon']}$ such sequences to compose a subset, which we term a *regular subset* (as it consists of sequences of the same type). Continue this procedure until the number of sequences of every type in A_i is less than $2^{n[I(X_1 \wedge X_2) - \varepsilon']}$. Let N_i denote the number of distinct regular subsets of A_i.

Enumerate (in any way) the sequences in each regular subset. Let $\mathbf{b}_{i,j,k}$, where $1 \leq i \leq 2^m$, $1 \leq j \leq N_i$, $1 \leq k \leq 2^{n[I(X_1 \wedge X_2) - \varepsilon']}$, denote the k-th sequence of the j-th regular subset in the i-th coset (with coset leader $\mathbf{e}_i$).

Terminal 1 sets $K_1 = k_1$ if $\mathbf{X}_1$ equals $\mathbf{b}_{i,j_1,k_1}$; else, K_1 is set to be uniformly distributed on $\left\{1, \ldots, 2^{n[I(X_1 \wedge X_2) - \varepsilon']}\right\}$, independent of $(\mathbf{X}_1, \mathbf{X}_2)$. Terminal 2 sets $K_2 = k_2$ if $\hat{\mathbf{X}}_2(1)$ equals $\mathbf{b}_{i,j_2,k_2}$; else, K_2 is set to be uniformly distributed on $\left\{1, \ldots, 2^{n[I(X_1 \wedge X_2) - \varepsilon']}\right\}$, independent of $(\mathbf{X}_1, \mathbf{X}_2, K_1)$.

The following theorem says that K_1 constitutes a perfect SK with rate approaching SK capacity.

Theorem 2: : Let $\varepsilon > 0$ be given. Then for some $\eta' = \eta'(\eta, \xi, \varepsilon, \varepsilon') > 0$ and for all n sufficiently large, the pair of rvs (K_1, K_2) generated above, with range $\mathcal{K}_1$ (say), satisfy

$$\Pr\{K_1 = K_2\} \geq 1 - 2^{-n\eta'} \tag{16}$$

$$I(K_1 \wedge \mathbf{F}) = 0 \tag{17}$$

$$H(K_1) = \log|\mathcal{K}_1| \tag{18}$$

$$\frac{1}{n}H(K_1) = h(p + q - 2pq) - h(p) - \varepsilon'. \tag{19}$$

C. Model 3

The following model is an instance of a *Markov chain on a tree* (cf. [18], [12]). Consider a tree $\mathcal{T}$ with vertex set $V(\mathcal{T}) = \{1, \ldots, d\}$ 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 $X_1, \ldots, X_d$ 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.

Let the terminals $1, \ldots, d$ *observe, respectively,* n i.i.d. *repetitions of* $\{0,1\}$ *-valued rvs* $X_1, \ldots, X_d$ *that form a Markov* *chain on the tree $\mathcal{T}$, with joint pmf $P_{X_1 \ldots X_d}$ specified as: for $(i,j) \in E(\mathcal{T})$*

$$P_{X_iX_j}(x_i,x_j) = \frac{1}{2}(1-p_{(i,j)})\delta_{x_ix_j} + \frac{1}{2}p_{(i,j)}(1-\delta_{x_ix_j}), \quad 0 < p_{(i,j)} < \frac{1}{2}$$

for $x_i, x_j \in \{0,1\}$. These d terminals wish to generate a strong SK of maximum rate.

Note that Model 1 is a special case of Model 3 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 (strong) SK capacity for this model [12] is given by (1) as

$$C_S = I(X_{i^*} \wedge X_{j^*}) = 1 - h(p_{\max}).$$

We show how to extract a SK with rate close to $1 - h(p_{\max})$ by using an extension of the SW data compression scheme of Model 1 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 a $\mathrm{BSC}(p_{\max})$, and with parity check matrix $\mathbf{P}$. Each terminal i communicates the syndrome $\mathbf{P}\mathbf{x}_i^t$, $1 \le i \le d$.

Let $\hat{\mathbf{x}}_i(j)$ denote the corresponding maximum likelihood estimate of $\mathbf{x}_j$ at terminal i, $1 \le i \ne j \le d$. For a terminal $i \ne i^*$, denote by $(i_0, i_1, \ldots, i_r)$ 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 $(\mathbf{x}_i, \mathbf{P}\mathbf{x}_{i_1}^t, \ldots, \mathbf{P}\mathbf{x}_{i_{r-1}}^t, \mathbf{P}\mathbf{x}_{i^*}^t)$, forms its estimate $\hat{\mathbf{x}}_i(i^*)$ of $\mathbf{x}_{i^*}$ through the following successive maximum likelihood estimates of $\mathbf{x}_{i_1}, \ldots, \mathbf{x}_{i_{r-1}}$:

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

and finally

$$\hat{\mathbf{x}}_i(i^*) = \hat{\mathbf{x}}_i(i_{r-1}) \oplus f_{\mathbf{P}}(\mathbf{P}\mathbf{x}_{i_{r-1}}^t \oplus \mathbf{P}\mathbf{x}_{i^*}^t). \tag{20}$$

Proposition 2: By the successive maximum likelihood estimation above, the estimate $\hat{\mathbf{X}}_i(i^*)$ at terminal $i \ne i^*$, satisfies

$$\Pr\{\hat{\mathbf{X}}_i(i^*) = \mathbf{X}_{i^*}\} \ge 1 - d \cdot 2^{-n\eta} \tag{21}$$

for some $\eta > 0$ and for all n sufficiently large.

Proof: See Appendix B. ■

It follows directly from (21) that for some $\eta' = \eta'(\eta, d) > 0$ and for all n sufficiently large

$$\Pr\{\hat{\mathbf{X}}_i(i^*) = \mathbf{X}_{i^*}, 1 \le i \ne i^* \le d\} \ge 1 - d^2 \cdot 2^{-n\eta} = 1 - 2^{-n\eta'}.$$

(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, $1 \le l \le 2^m$, $1 \le k \le 2^{n-m}$. Terminal i^* sets $K_{i^*} = k_{i^*}$ if $\mathbf{X}_{i^*}$ equals $\mathbf{a}_{l,k_{i^*}}$ in the standard array. Terminal i, $1 \le i \ne i^* \le d$, sets $K_i = k_i$ if $\hat{\mathbf{X}}_i(i^*)$ equals $\mathbf{a}_{l,k_i}$ in the same standard array.

The following theorem states that K_{i^*} constitutes a perfect SK with rate approaching SK capacity.

Theorem 3: Let $\varepsilon > 0$ be given. Then for some $\eta' = \eta'(\eta, d) > 0$ and for all n sufficiently large, the rvs $K_1, \ldots, K_d$ generated above, with range $\mathcal{K}_{i^*}$ (say), satisfy

$$\Pr\{K_1 = \ldots = K_d\} > 1 - 2^{-n\eta'} \tag{22}$$

$$I(K_{i^*} \wedge \mathbf{F}) = 0 \tag{23}$$

$$H(K_{i^*}) = \log|\mathcal{K}_{i^*}| \tag{24}$$

$$\frac{1}{n}H(K_{i^*}) > 1 - h(p_{\max}) - \varepsilon. \tag{25}$$

D. Model 4

Let the terminals 1, 2 and 3 observe, respectively n i.i.d. *repetitions of the $\{0,1\}$ -valued rvs X_1, X_2, X_3, with joint pmf $P_{X_1X_2X_3}$ given by:*

$$\begin{aligned}
P_{X_1X_2X_3}(0,0,0) = P_{X_1X_2X_3}(0,1,1) &= \frac{(1-p)(1-q)}{2}\\
P_{X_1X_2X_3}(0,0,1) = P_{X_1X_2X_3}(0,1,0) &= \frac{pq}{2}\\
P_{X_1X_2X_3}(1,0,0) = P_{X_1X_2X_3}(1,1,1) &= \frac{p(1-q)}{2}\\
P_{X_1X_2X_3}(1,0,1) = P_{X_1X_2X_3}(1,1,0) &= \frac{q(1-p)}{2}
\end{aligned} \tag{26}$$

with $0 < p < \frac{1}{2}$ and $0 < q < 1$. Terminals 1 and 2 wish to generate a strong PK of maximum rate, which is concealed from the helper terminal 3.

Note that under the joint pmf of X_1, X_2, X_3 above, we can write

$$\mathbf{X}_1 = \mathbf{X}_2 \oplus \mathbf{X}_3 \oplus \mathbf{V} \tag{27}$$

where $\mathbf{V} = (V_1, \ldots, V_n)$ is an i.i.d. sequence of $\{0,1\}$-valued rvs, independent of $(\mathbf{X}_2, \mathbf{X}_3)$, with $\Pr\{V_i = 1\} = p$, $1 \le i \le n$. Further, (X_2, X_3) plays the role of (X_1, X_2) in Model 1 with q in lieu of p in the latter.

We show below a scheme for terminals 1 and 2 to generate a PK with rate close to (strong) PK capacity for this model [2], [11], [12], given by (4) as

$$C_P(\{1,2\}) = I(X_1 \wedge X_2 | X_3) = h(p + q - 2pq) - h(p).$$

The first step of this scheme entails terminal 3 simply revealing its observations $\mathbf{x}_3$ to both terminals 1 and 2. Then, Wyner's SW data compression scheme is used for reconstructing $\mathbf{x}_1$ at terminal 2 from the SW codeword for $\mathbf{x}_1$ and its own knowledge of $\mathbf{x}_2 \oplus \mathbf{x}_3$.

(i) *SW data compression*: This step is identical to step (i) for Model 1, as seen with the help of (27). Obviously,

$$\Pr\{\hat{\mathbf{X}}_2(1) = \mathbf{X}_1\} \ge 1 - 2^{-n\eta}$$

for some $\eta > 0$ and for all n sufficiently large.

(ii) *PK construction*: Suppose that terminals 1 and 2 know a linear $(n, n-m)$ code $\mathcal{C}$ as in Lemma 1, and a (common) standard array for $\mathcal{C}$. Let $\{\mathbf{e}_i : 1 \le i \le 2^m\}$ denote the set of coset leaders for all the cosets of $\mathcal{C}$.

For a sequence $\mathbf{x}_3 \in \{0,1\}^n$, denote by $A_i(\mathbf{x}_3)$ the set of sequences from $T^n_{X_1|X_3,\xi}(\mathbf{x}_3)$ in the coset of $\mathcal{C}$ with coset leader $\mathbf{e}_i$, $1 \le i \le 2^m$. If the number of sequences of the same joint type with $\mathbf{x}_3$ in $A_i(\mathbf{x}_3)$ is more than $2^{n[I(X_1 \wedge X_2|X_3)-\varepsilon']}$, where $\varepsilon' > 2\xi + \varepsilon$ and ε satisfies $m < n[h(p)+\varepsilon]$ (as in Lemma 1), then collect arbitrarily $2^{n[I(X_1 \wedge X_2|X_3)-\varepsilon']}$ such sequences to compose a regular subset. Continue this procedure until the number of sequences of every joint type with $\mathbf{x}_3$ in $A_i(\mathbf{x}_3)$ is less than $2^{n[I(X_1 \wedge X_2|X_3)-\varepsilon']}$. Let $N_i(\mathbf{x}_3)$ denote the number of distinct regular subsets of $A_i(\mathbf{x}_3)$.

For a given sequence $\mathbf{x}_3$, enumerate (in any way) the sequences in each regular subset. Let $\mathbf{b}_{i,j,k}(\mathbf{x}_3)$, where $1 \le i \le 2^m$, $1 \le j \le N_i(\mathbf{x}_3)$, $1 \le k \le 2^{n[I(X_1 \wedge X_2|X_3)-\varepsilon']}$, denote the k-th sequence of the j-th regular subset in the i-th coset.

Terminal 1 sets $K_1 = k_1$ if $\mathbf{X}_1$ equals $\mathbf{b}_{i,j_1,k_1}(\mathbf{x}_3)$; else, K_1 is set to be uniformly distributed on $\left\{1, \ldots, 2^{n[I(X_1 \wedge X_2|X_3)-\varepsilon']}\right\}$, independent of $(\mathbf{X}_1, \mathbf{X}_2, \mathbf{X}_3)$. Terminal 2 sets $K_2 = k_2$ if $\hat{\mathbf{X}}_2(1)$ equals $\mathbf{b}_{i,j_2,k_2}(\mathbf{x}_3)$; else, K_2 is set to be uniformly distributed on $\left\{1, \ldots, 2^{n[I(X_1 \wedge X_2|X_3)-\varepsilon']}\right\}$, independent of $(\mathbf{X}_1, \mathbf{X}_2, \mathbf{X}_3, K_1)$.

The following theorem establishes that K_1 constitutes a perfect PK with rate approaching PK capacity.

Theorem 4: Let $\varepsilon > 0$ be given. Then for some $\eta' = \eta'(\eta, \xi, \varepsilon, \varepsilon') > 0$ and for all n sufficiently large, the pair of rvs (K_1, K_2) generated above, with range $\mathcal{K}_1$ (say), satisfy

$$\Pr\{K_1 \ne K_2\} < 2^{-n\eta'} \tag{28}$$

$$I(K_1 \wedge \mathbf{X}_3, \mathbf{F}) = 0 \tag{29}$$

$$H(K_1) = \log |\mathcal{K}_1| \tag{30}$$

$$\frac{1}{n} H(K_1) = I(X_1 \wedge X_2 | X_3) - \varepsilon'. \tag{31}$$

Remark: The PK construction scheme above applies for any joint pmf $P_{X_1X_2X_3}$ satisfying (27) and is not restricted to the given joint pmf in (26).

IV. Proofs of Theorems 1–4

Proof of Theorem 1: It follows from the SK construction scheme for Model 1 that

$$\Pr\{K_1 \ne K_2\} = \Pr\{\hat{\mathbf{X}}_2(1) \ne \mathbf{X}_1\} < 2^{-n\eta}$$

which is (11). Since X_1 is uniformly distributed on $\{0,1\}$, we have for $1 \le i \le 2^m$, $1 \le j \le 2^{n-m}$, that

$$\Pr\{\mathbf{X}_1 = \mathbf{a}_{i,j}\} = 2^{-n}.$$

Hence

$$\begin{aligned}\Pr\{K_1 = j\} &= \sum_{i=1}^{2^m} \Pr\{\mathbf{X}_1 = \mathbf{a}_{i,j}\} \\ &= 2^{-(n-m)}, \ 1 \le j \le 2^{n-m}\end{aligned}$$

i.e., K_1 is uniformly distributed on $\mathcal{K}_1 = \{1, \ldots, 2^{n-m}\}$, and so

$$H(K_1) = \log 2^{n-m} = n - m = \log |\mathcal{K}_1|$$

which is (13). Therefore, (14) holds since $m < n[h(p)+\varepsilon]$.

It remains to show that K_1 satisfies (12) with $\mathbf{F} = \mathbf{P}\mathbf{X}_1^t$. Let $\{\mathbf{e}_i, 1 \le i \le 2^m\}$ be the set of coset leaders for the cosets of $\mathcal{C}$. For $1 \le i \le 2^m$, $1 \le j \le 2^{n-m}$

$$\begin{aligned}\Pr\{K_1 = j | \mathbf{P}\mathbf{X}_1^t = \mathbf{P}\mathbf{e}_i^t\} &= \frac{\Pr\{K_1 = j, \mathbf{P}\mathbf{X}_1^t = \mathbf{P}\mathbf{e}_i^t\}}{\Pr\{\mathbf{P}\mathbf{X}_1^t = \mathbf{P}\mathbf{e}_i^t\}} \\ &= \frac{\Pr\{\mathbf{X}_1 = \mathbf{a}_{i,j}\}}{\sum_{j'=1}^{2^{n-m}} \Pr\{\mathbf{X}_1 = \mathbf{a}_{i,j'}\}} \\ &= 2^{-(n-m)} \\ &= \Pr\{K_1 = j\}\end{aligned}$$

i.e., K_1 is independent of $\mathbf{F}$ and so $I(K_1 \wedge \mathbf{F}) = 0$, establishing (12). ∎

Proof of Theorem 2: Let $\mathcal{F}$ denote the union of all regular subsets in $\bigcup_{i=1}^{2^m} A_i$. Clearly $\mathcal{F} \subseteq T^n_{X_1,\xi}$, so that

$$\begin{aligned}\Pr\{\mathbf{X}_1 \in \mathcal{F}\} &= \Pr\{\mathbf{X}_1 \in T^n_{X_1,\xi}, \mathbf{X}_1 \in \mathcal{F}\} \\ &= \Pr\{\mathbf{X}_1 \in T^n_{X_1,\xi}\} - \Pr\{\mathbf{X}_1 \in T^n_{X_1,\xi} \backslash \mathcal{F}\}. \end{aligned}\tag{32}$$

By Proposition 1, $\Pr\{\mathbf{X}_1 \in T^n_{X_1,\xi}\}$ goes to 1 exponentially rapidly in n. We show below that $\Pr\{\mathbf{X}_1 \in T^n_{X_1,\xi} \backslash \mathcal{F}\}$ decays to 0 exponentially rapidly in n.

Since the number of different types of sequences in $\{0,1\}^n$ does not exceed $(n+1)^2$, we have that

$$\begin{aligned}\left|\{\mathbf{x}_1 : \mathbf{x}_1 \in T^n_{X_1,\xi} \backslash \mathcal{F}\}\right| &\le 2^m \cdot (n+1)^2 \cdot 2^{n[I(X_1 \wedge X_2)-\varepsilon']} \\ &< (n+1)^2 \cdot 2^{n[H(X_1)+\varepsilon-\varepsilon']}\end{aligned}$$

where the first inequality follows from the specifics of the SK construction for Model 2 in Section III-B, and the second inequality is from $m < n[h(p)+\varepsilon] = n[H(X_1|X_2)+\varepsilon]$.

Since $P^n_{X_1}(\mathbf{x}_1) \le 2^{-n[H(X_1)-\xi]}$, $\mathbf{x}_1 \in T^n_{X_1,\xi}$, we get

$$\Pr\{\mathbf{X}_1 \in T^n_{X_1,\xi} \backslash \mathcal{F}\} < (n+1)^2 \cdot 2^{-n(\varepsilon'-\xi-\varepsilon)}.$$

Choosing $\varepsilon' > \xi + \varepsilon$, $\Pr\{\mathbf{X}_1 \in T^n_{X_1,\xi} \backslash \mathcal{F}\}$ goes to 0 exponentially rapidly. Therefore, it follows from (32) that $\Pr\{\mathbf{X}_1 \in \mathcal{F}\}$ goes to 1 exponentially rapidly in n, with exponent depending on $(\xi, \varepsilon, \varepsilon')$.

By the SK construction scheme for Model 2

$$\begin{aligned}\Pr\{K_1 \ne K_2\} &= \Pr\{K_1 \ne K_2, \mathbf{X}_1 \in \mathcal{F}\} \\ &\quad + \Pr\{K_1 \ne K_2, \mathbf{X}_1 \notin \mathcal{F}\} \\ &\le \Pr\{\hat{\mathbf{X}}_2(1) \ne \mathbf{X}_1, \mathbf{X}_1 \in \mathcal{F}\} + \Pr\{\mathbf{X}_1 \notin \mathcal{F}\} \\ &\le \Pr\{\hat{\mathbf{X}}_2(1) \ne \mathbf{X}_1\} + \Pr\{\mathbf{X}_1 \notin \mathcal{F}\}.\end{aligned}$$

Since $\Pr\{\hat{\mathbf{X}}_2(1) \ne \mathbf{X}_1\} < 2^{-n\eta}$, by the observation in the previous paragraph, we have

$$\Pr\{K_1 \ne K_2\} < 2^{-n\eta'}$$

for some $\eta' = \eta'(\eta, \xi, \varepsilon, \varepsilon') > 0$ and for all n sufficiently large, which is (16).

Next, we shall show that K_1 satisfies (18). For $1 \le k \le 2^{n[I(X_1 \wedge X_2)-\varepsilon']}$, it is clear by choice that

$$\Pr\{K_1 = k|\mathbf{X}_1 \notin \mathcal{F}\} = 2^{-n[I(X_1 \wedge X_2)-\varepsilon']} \tag{33}$$

and that

$$\begin{aligned}\Pr\{K_1 =k|\mathbf{X}_1 \in \mathcal{F}\} &= \frac{\Pr\{K_1 = k, \mathbf{X}_1 \in \mathcal{F}\}}{\Pr\{\mathbf{X}_1 \in \mathcal{F}\}} \\ &= \frac{\sum_{i=1}^{2^m} \sum_{j=1}^{N_i} \Pr\{\mathbf{X}_1 = \mathbf{b}_{i,j,k}\}}{\sum_{i=1}^{2^m} \sum_{j=1}^{N_i} 2^{n[I(X_1 \wedge X_2)-\varepsilon']} \Pr\{\mathbf{X}_1 = \mathbf{b}_{i,j,k}\}} \qquad (34) \\ &= 2^{-n[I(X_1 \wedge X_2)-\varepsilon']} \qquad (35)\end{aligned}$$

where (34) is due to every regular subset consisting of sequences of the same type. From (33) and (35)

$$\Pr\{K_1 = k\} = 2^{-n[I(X_1 \wedge X_2)-\varepsilon']} \tag{36}$$

i.e., K_1 is uniformly distributed on $\mathcal{K}_1 = \left\{1, \dots, 2^{n[I(X_1 \wedge X_2)-\varepsilon']}\right\}$, with

$$\frac{1}{n} H(K_1) = I(X_1 \wedge X_2) - \varepsilon'$$

which is (19).

It remains to show that K_1 satisfies (17) with $\mathbf{F} = \mathbf{P}\mathbf{X}_1^t$. For $1 \le i \le 2^m$, $1 \le k \le 2^{n[I(X_1 \wedge X_2)-\varepsilon']}$, we have

$$\Pr\{K_1 = k|\mathbf{P}\mathbf{X}_1^t = \mathbf{P}\mathbf{e}_i^t, \mathbf{X}_1 \notin \mathcal{F}\} = 2^{-n[I(X_1 \wedge X_2)-\varepsilon']}$$

by choice, and

$$\begin{aligned}\Pr\{K_1 = k&|\mathbf{P}\mathbf{X}_1^t = \mathbf{P}\mathbf{e}_i^t, \mathbf{X}_1 \in \mathcal{F}\} \\ &= \frac{\Pr\{K_1 = k, \mathbf{P}\mathbf{X}_1^t = \mathbf{P}\mathbf{e}_i^t, \mathbf{X}_1 \in \mathcal{F}\}}{\Pr\{\mathbf{P}\mathbf{X}_1^t = \mathbf{P}\mathbf{e}_i^t, \mathbf{X}_1 \in \mathcal{F}\}} \\ &= \frac{\sum_{j=1}^{N_i} \Pr\{\mathbf{X}_1 = \mathbf{b}_{i,j,k}\}}{\sum_{j=1}^{N_i} 2^{n[I(X_1 \wedge X_2)-\varepsilon']} \Pr\{\mathbf{X}_1 = \mathbf{b}_{i,j,k}\}} \\ &= 2^{-n[I(X_1 \wedge X_2)-\varepsilon']}.\end{aligned}$$

Hence

$$\begin{aligned}\Pr\{K_1 = k&|\mathbf{P}\mathbf{X}_1^t = \mathbf{P}\mathbf{e}_i^t\} \\ &= \Pr\{K_1 = k|\mathbf{P}\mathbf{X}_1^t = \mathbf{P}\mathbf{e}_i^t, \mathbf{X}_1 \in \mathcal{F}\} \\ &\quad \times \Pr\{\mathbf{X}_1 \in \mathcal{F}|\mathbf{P}\mathbf{X}_1^t = \mathbf{P}\mathbf{e}_i^t\} \\ &\quad + \Pr\{K_1 = k|\mathbf{P}\mathbf{X}_1^t = \mathbf{P}\mathbf{e}_i^t, \mathbf{X}_1 \notin \mathcal{F}\} \\ &\quad \times \Pr\{\mathbf{X}_1 \notin \mathcal{F}|\mathbf{P}\mathbf{X}_1^t = \mathbf{P}\mathbf{e}_i^t\} \\ &= 2^{-n[I(X_1 \wedge X_2)-\varepsilon']} \\ &= \Pr\{K_1 = k\}\end{aligned}$$

where the previous equality follows from (36). Thus, K_1 is independent of $\mathbf{F}$, establishing (17). ■

Proof of Theorem 3: Applying the same arguments used in Theorem 1, we see that the rvs $K_1, \dots, K_m$ satisfy (22), (24), and (25). It then remains to show that K_{i^*} satisfies (23) with $\mathbf{F} = (\mathbf{P}\mathbf{X}_1^t, \dots, \mathbf{P}\mathbf{X}_d^t)$.

Under the given joint pmf $P_{X_1 \cdots X_d}$, for each $i \ne i^*$, we can write

$$\mathbf{X}_i = \mathbf{X}_{i^*} \oplus \mathbf{V}_i$$

where $\mathbf{V}_i = (V_{i,1}, \dots, V_{i,n})$ is an i.i.d. sequence of $\{0,1\}$-valued rvs. Further, $\mathbf{V}_i$, $1 \le i \ne i^* \le d$, and $\mathbf{X}_{i^*}$ are mutually independent. Then

$$\begin{aligned}I(K_{i^*} \wedge \mathbf{F}) &= I(K_{i^*} \wedge \{\mathbf{P}\mathbf{X}_i^t,\, 1 \le i \le d\}) \\ &\le I(K_{i^*} \wedge \mathbf{P}\mathbf{X}_{i^*}^t, \{\mathbf{P}\mathbf{V}_i^t,\, 1 \le i \ne i^* \le d\}) \\ &\le I(K_{i^*} \wedge \mathbf{P}\mathbf{X}_{i^*}^t) \\ &\quad + I(K_{i^*}, \mathbf{P}\mathbf{X}_{i^*}^t \wedge \{\mathbf{P}\mathbf{V}_i^t,\, 1 \le i \ne i^* \le d\}).\end{aligned} \tag{37}$$

Clearly, the first term on the right side of (37) is zero. Since for a fixed $\mathbf{P}$, $(K_{i^*}, \mathbf{P}\mathbf{X}_{i^*}^t)$ is a function of $\mathbf{X}_{i^*}$

$$\begin{aligned}I(K_{i^*}, \mathbf{P}\mathbf{X}_{i^*}^t &\wedge \{\mathbf{P}\mathbf{V}_i^t,\, 1 \le i \ne i^* \le d\}) \\ &\le I(\mathbf{X}_{i^*} \wedge \{\mathbf{V}_i,\, 1 \le i \ne i^* \le d\}) = 0\end{aligned}$$

i.e., K_{i^*} is independent of $\mathbf{F}$, establishing (23). ■

Proof of Theorem 4: For every $\mathbf{x}_3 \in \{0,1\}^n$, let $\mathcal{F}(\mathbf{x}_3)$ denote the union of all regular subsets in $\bigcup_{i=1}^{2^m} A_i(\mathbf{x}_3)$. Since $\mathcal{F}(\mathbf{x}_3) \subseteq T^n_{X_1|X_3,\xi}(\mathbf{x}_3)$,

$$\begin{aligned}\Pr\{\mathbf{X}_1 \in \mathcal{F}(\mathbf{X}_3)\} &= \Pr\{\mathbf{X}_1 \in T^n_{X_1|X_3,\xi}(\mathbf{X}_3)\} \\ &\quad - \Pr\{\mathbf{X}_1 \in T^n_{X_1|X_3,\xi}(\mathbf{X}_3) \backslash \mathcal{F}(\mathbf{X}_3)\}.\end{aligned} \tag{38}$$

It follows from Proposition 1 that $\Pr\{\mathbf{X}_1 \in T^n_{X_1|X_3,\xi}(\mathbf{X}_3)\}$ goes to 1 exponentially rapidly in n. We show below that $\Pr\{\mathbf{X}_1 \in T^n_{X_1|X_3,\xi}(\mathbf{X}_3) \backslash \mathcal{F}(\mathbf{X}_3)\}$ goes to 0 exponentially rapidly in n.

Recall that the number of different joint types of pairs in $\{0,1\}^n \times \{0,1\}^n$ does not exceed $(n+1)^4$. Thus

$$\begin{aligned}\Big|\{\mathbf{x}_1 : \mathbf{x}_1 \in T^n_{X_1|X_3,\xi}&(\mathbf{x}_3) \backslash \mathcal{F}(\mathbf{x}_3)\}\Big| \\ &\le 2^m \cdot (n+1)^4 \cdot 2^{n[I(X_1 \wedge X_2|X_3)-\varepsilon']} \\ &< (n+1)^4 \cdot 2^{n[H(X_1|X_3)+\varepsilon-\varepsilon']}\end{aligned}$$

where the previous inequality is from $m < n[h(p) + \varepsilon] = n[H(X_1|X_2, X_3) + \varepsilon]$.

Since $P^n_{X_1|X_3}(\mathbf{x}_1|\mathbf{x}_3) \le 2^{-n[H(X_1|X_3)-2\xi]}$, $(\mathbf{x}_1, \mathbf{x}_3) \in T^n_{X_1 X_3,\xi}$, we get

$$\Pr\{\mathbf{X}_1 \in T^n_{X_1|X_3,\xi}(\mathbf{X}_3) \backslash \mathcal{F}(\mathbf{X}_3)\} < (n+1)^4 \cdot 2^{-n(\varepsilon'-2\xi-\varepsilon)}.$$

Choosing $\varepsilon' > 2\xi + \varepsilon$, $\Pr\{\mathbf{X}_1 \in T^n_{X_1|X_3,\xi}(\mathbf{X}_3) \backslash \mathcal{F}(\mathbf{X}_3)\}$ goes to 0 exponentially rapidly. Therefore, it follows from (38) that $\Pr\{\mathbf{X}_1 \in \mathcal{F}(\mathbf{X}_3)\}$ goes to 1 exponentially rapidly in n, with an exponent depending on $(\xi, \varepsilon, \varepsilon')$.

By the PK construction scheme for Model 4, we have

$$\begin{aligned}\Pr\{K_1 \neq K_2\} &= \Pr\{K_1 \neq K_2, \mathbf{X}_1 \in \mathcal{F}(\mathbf{x}_3)\}\\ &\quad + \Pr\{K_1 \neq K_2, \mathbf{X}_1 \notin \mathcal{F}(\mathbf{x}_3)\}\\ &\leq \Pr\{\hat{\mathbf{X}}_2(1) \neq \mathbf{X}_1, \mathbf{X}_1 \in \mathcal{F}(\mathbf{x}_3)\}\\ &\quad + \Pr\{\mathbf{X}_1 \notin \mathcal{F}(\mathbf{x}_3)\}\\ &\leq \Pr\{\hat{\mathbf{X}}_2(1) \neq \mathbf{X}_1\} + \Pr\{\mathbf{X}_1 \notin \mathcal{F}(\mathbf{X}_3)\}.\end{aligned}$$

Since $\Pr\{\hat{\mathbf{X}}_2(1) \neq \mathbf{X}_1\} < 2^{-n\eta}$ by the observation in the previous paragraph, we have

$$\Pr\{K_1 \neq K_2\} < 2^{-n\eta'}$$

for some $\eta' = \eta'(\eta, \xi, \varepsilon, \varepsilon') > 0$ and for all n sufficiently large, which is (28).

Next, we shall show that K_1 satisfies (30). For $\mathbf{x}_3 \in \{0,1\}^n$ and $1 \leq k \leq 2^{n[I(X_1 \wedge X_2|X_3)-\varepsilon']}$, it is clear by choice that

$$\Pr\{K_1 = k|\mathbf{X}_1 \notin \mathcal{F}(\mathbf{x}_3), \mathbf{X}_3 = \mathbf{x}_3\} = 2^{-n[I(X_1 \wedge X_2|X_3)-\varepsilon']}$$

and that

$$\begin{aligned}&\Pr\{K_1 = k|\mathbf{X}_1 \in \mathcal{F}(\mathbf{x}_3), \mathbf{X}_3 = \mathbf{x}_3\}\\ &= \frac{\Pr\{K_1 = k, \mathbf{X}_1 \in \mathcal{F}(\mathbf{x}_3)|\mathbf{X}_3 = \mathbf{x}_3\}}{\Pr\{\mathbf{X}_1 \in \mathcal{F}(\mathbf{x}_3)|\mathbf{X}_3 = \mathbf{x}_3\}}\\ &= \frac{\sum_{i=1}^{2^m}\sum_{j=1}^{N_i(\mathbf{x}_3)} \Pr\{\mathbf{X}_1 = \mathbf{b}_{i,j,k}(\mathbf{x}_3)|\mathbf{X}_3 = \mathbf{x}_3\}}{\sum_{i=1}^{2^m}\sum_{j=1}^{N_i(\mathbf{x}_3)} 2^{n[I(X_1 \wedge X_2|X_3)-\varepsilon']}\Pr\{\mathbf{X}_1 = \mathbf{b}_{i,j,k}(\mathbf{x}_3)|\mathbf{X}_3 = \mathbf{x}_3\}}\\ &= 2^{-n[I(X_1 \wedge X_2|X_3)-\varepsilon']}\end{aligned}$$

where the second equality is due to every regular subset consisting of sequences of the same joint type with $\mathbf{x}_3$. Therefore

$$\begin{aligned}\Pr\{K_1 = k\} &= \sum_{\mathbf{x}_3 \in \{0,1\}^n} \Pr\{K_1 = k, \mathbf{X}_3 = \mathbf{x}_3\}\\ &= \sum_{\mathbf{x}_3 \in \{0,1\}^n} [\Pr\{\mathbf{X}_1 \in \mathcal{F}(\mathbf{x}_3), \mathbf{X}_3 = \mathbf{x}_3\}\\ &\quad \times \Pr\{K_1 = k|\mathbf{X}_1 \in \mathcal{F}(\mathbf{x}_3), \mathbf{X}_3 = \mathbf{x}_3\}\\ &\quad + \Pr\{\mathbf{X}_1 \notin \mathcal{F}(\mathbf{x}_3), \mathbf{X}_3 = \mathbf{x}_3\}\\ &\quad \times \Pr\{K_1 = k|\mathbf{X}_1 \notin \mathcal{F}(\mathbf{x}_3), \mathbf{X}_3 = \mathbf{x}_3\}]\\ &= 2^{-n[I(X_1 \wedge X_2|X_3)-\varepsilon']} \qquad (39)\end{aligned}$$

i.e., K_1 is uniformly distributed on $\mathcal{K}_1 = \left\{1, \ldots, 2^{n[I(X_1 \wedge X_2|X_3)-\varepsilon']}\right\}$, with

$$\frac{1}{n}H(K_1) = I(X_1 \wedge X_2|X_3) - \varepsilon'$$

which is (31).

It remains to show that K_1 satisfies (29) with $(\mathbf{X}_3, \mathbf{F}) = (\mathbf{X}_3, \mathbf{P}\mathbf{X}_1^t)$. For $\mathbf{x}_3 \in \{0,1\}^n$, $1 \leq i \leq 2^m$ and $1 \leq k \leq 2^{n[I(X_1 \wedge X_2|X_3)-\varepsilon']}$, we have

$$\begin{aligned}&\Pr\{K_1 = k|\mathbf{P}\mathbf{X}_1^t = \mathbf{P}\mathbf{e}_i^t, \mathbf{X}_1 \notin \mathcal{F}(\mathbf{x}_3), \mathbf{X}_3 = \mathbf{x}_3\}\\ &\qquad = 2^{-n[I(X_1 \wedge X_2|X_3)-\varepsilon']}\end{aligned}$$

by choice, and

$$\begin{aligned}&\Pr\{K_1 = k|\mathbf{P}\mathbf{X}_1^t = \mathbf{P}\mathbf{e}_i^t, \mathbf{X}_1 \in \mathcal{F}(\mathbf{x}_3), \mathbf{X}_3 = \mathbf{x}_3\}\\ &= \frac{\Pr\{K_1 = k, \mathbf{P}\mathbf{X}_1^t = \mathbf{P}\mathbf{e}_i^t, \mathbf{X}_1 \in \mathcal{F}(\mathbf{x}_3)|\mathbf{X}_3 = \mathbf{x}_3\}}{\Pr\{\mathbf{P}\mathbf{X}_1^t = \mathbf{P}\mathbf{e}_i^t, \mathbf{X}_1 \in \mathcal{F}(\mathbf{x}_3)|\mathbf{X}_3 = \mathbf{x}_3\}}\\ &= \frac{\sum_{j=1}^{N_i(\mathbf{x}_3)} \Pr\{\mathbf{X}_1 = \mathbf{b}_{i,j,k}(\mathbf{x}_3)|\mathbf{X}_3 = \mathbf{x}_3\}}{\sum_{j=1}^{N_i(\mathbf{x}_3)} 2^{n[I(X_1 \wedge X_2|X_3)-\varepsilon']}\Pr\{\mathbf{X}_1 = \mathbf{b}_{i,j,k}(\mathbf{x}_3)|\mathbf{X}_3 = \mathbf{x}_3\}}\\ &= 2^{-n[I(X_1 \wedge X_2|X_3)-\varepsilon']}.\end{aligned}$$

Hence

$$\begin{aligned}\Pr\{K_1 = k|\mathbf{P}\mathbf{X}_1^t = \mathbf{P}\mathbf{e}_i^t, \mathbf{X}_3 = \mathbf{x}_3\} &= 2^{-n[I(X_1 \wedge X_2|X_3)-\varepsilon']}\\ &= \Pr\{K_1 = k\}\end{aligned}$$

where the previous equality follows from (39). Thus, K_1 is independent of $(\mathbf{X}_3, \mathbf{F})$, establishing (29). ■

V. Implementation With LDPC Codes

We outline an implementation using LDPC codes (cf. e.g., [44], [28], [39], [40]) of the scheme for the construction of a SK for Model 1 in Section III. As will be indicated below, similar implementations can be applied to Models 2–4 as well.

A. SK Construction

Without any loss of generality, we consider a systematic $(n, n-m)$ linear code $\mathcal{C}$ with generator matrix $\mathbf{G} = [\mathbf{I}_{n-m}\ \mathbf{A}]$, where $\mathbf{I}_{n-m}$ is an $(n-m) \times (n-m)$-identity matrix and $\mathbf{A}$ is an $(n-m) \times m$-matrix. Then, the parity check matrix for $\mathcal{C}$ is $\mathbf{P} = [\mathbf{A}^t\ \mathbf{I}_m]$, where $\mathbf{I}_m$ is an $m \times m$-identity matrix. The first $n-m$ bits of every codeword in $\mathcal{C}$, namely the *information bits*, are pairwise distinct. Further, since the coset with coset leader $\mathbf{e}_i$, $1 \leq i \leq 2^m$, must contain the sequence $\mathbf{b}_i = [\mathbf{0}_{n-m}\ \mathbf{e}_i\mathbf{P}^t]$, with $\mathbf{0}_{n-m}$ denoting a sequence of $n-m$ zeros, the first $(n-m)$-bit-segments of the sequences in the coset $\{\mathbf{b}_i \oplus \mathbf{c},\ \mathbf{c} \in \mathcal{C}\}$ are pairwise distinct.

Terminal 1 transmits the syndrome $\mathbf{P}\mathbf{x}_1^t$, whereupon terminal 2, knowing $(\mathbf{x}_2, \mathbf{P}\mathbf{x}_1^t)$, estimates $\hat{\mathbf{x}}_2(1)$. Since the first $n-m$ bits of the sequences in each coset are pairwise distinct, these bits can serve as the index of a sequence in its coset. Then, terminal 1 (respectively, 2) sets K_1 (respectively, K_2) as the first $n-m$ bits of $\mathbf{x}_1$ (respectively, $\hat{\mathbf{x}}_2(1)$).

The same implementation of the SW data compression scheme above holds for Models 2 and 4, too. It can be applied repeatedly also for the successive estimates (20) in Model 3. In Model 3, K_{i^*} (respectively, K_i, $i \neq i^*$) is set as the first $n-m$ bits of $\mathbf{x}_{i^*}$ (respectively, $\hat{\mathbf{x}}_i(i^*)$). It should be noted that *the current complexity of generating regular subsets in Models 2 and 4 poses a hurdle for explicit efficient constructions of a SK and a PK, respectively, for these models.*

B. Simulation Results

We provide simulation results for the tradeoff between the relative secret key rate (i.e., the difference between the SK capacity and the rate of the generated SK) and the rate of generating unequal SKs at different terminals (corresponding to the bit error

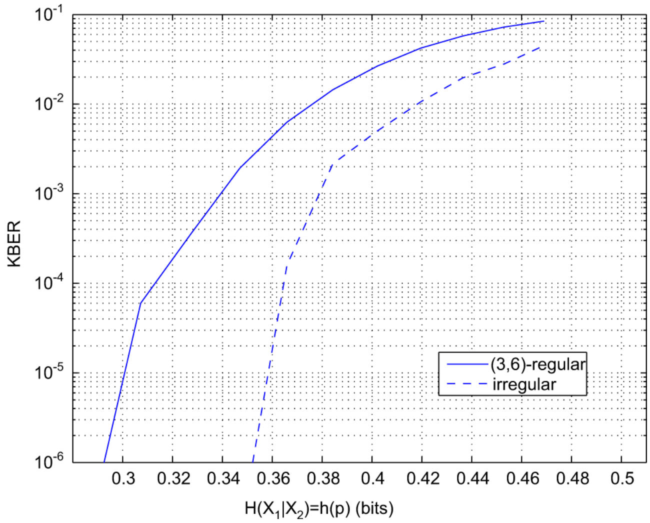

Fig. 1. Simulation results for the (3,6)-regular and the irregular LDPC codes.

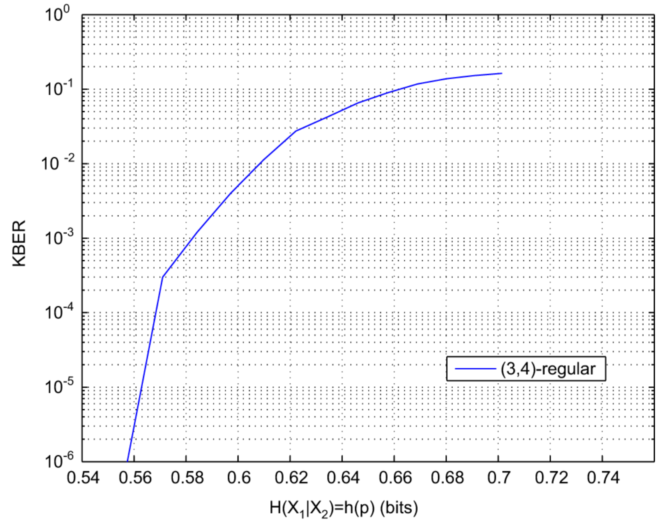

Fig. 2. Simulation results for the (3,4)-regular LDPC code.

rate in SK-matching), when LDPC codes are used for SK construction in Model 1.

For the purpose of comparison, three different LDPC codes were used: i) a $(3,4)$-regular LDPC code; ii) a $(3,6)$-regular LDPC code; and iii) an irregular LDPC code with degree distribution pair (cf. [26])

$$\begin{aligned}\lambda(x) =& 0.234029x + 0.212425x^2 + 0.146898x^5 \\ &+ 0.102840x^6 + 0.303808x^{19} \\ \rho(x) =& 0.71875x^7 + 0.28125x^8\end{aligned}$$

with a common codeword length of 10^3 bits, and up to 60 iterations of the belief-propagation algorithm (cf. [26]) were allowed. Over 10^3 blocks were transmitted from terminal 1. Since every linear code is equivalent to a systematic code (cf. e.g., [36]), the arguments of Section V-A facilitate SK generation.

Simulation results are shown in Figs. 1 and 2, where conditional entropy (i.e., $H(X_1|X_2) = h(p)$) is plotted against key bit error rate (KBER). We note that in this simulation SKs are generated at fixed rates that are equal to the rates of the LDPC codes used. Since for Model 1, SK capacity equals $1 - h(p)$, the conditional entropy $h(p)$ serves as an indicator of the gap between SK capacity and the rate of the generated SK.

Fig. 1 shows the performance of the (3, 6)-regular and the irregular LDPC codes; Fig. 2 shows the performance of the (3,4)-regular LDPC code. It is seen in both figures that KBER increases with $h(p)$. Since SK capacity decreases with increasing $h(p)$, an increase of $h(p)$ narrows the gap between SK capacity and the rate of the generated SK, but raises the likelihood of generating unequal SKs at the two terminals.

It is seen from Fig. 1 that the irregular LDPC code outperforms the (3,6)-regular LDPC code. For instance, for a fixed crossover probability $p = 0.068$, say, and $h(p) \approx 0.3584$, the KBER for the irregular LDPC code is as low as 10^{-5}, while the KBER for the (3,6)-regular LDPC code is only about 4×10^{-3}.

VI. Discussion

We have considered four simple secrecy generation models involving multiple terminals, and propose a new approach for constructing SKs and PKs. This approach is based on Wyner's well-known SW data compression code for sources connected by virtual channels with additive independent noise.

In all the models considered in this paper, the i.i.d. sequences observed at the different terminals possess the following structure: They can be described in terms of sequences at *pairs of terminals* where each terminal in a pair is connected to the other terminal by a virtual communication channel with additive independent noise. While the correlated sources in all our models have binary alphabets, the approach extends to alphabets that are finite groups.

There are two steps in the SK construction schemes. The first step constitutes SW data compression for the purpose of common randomness generation at the terminals. Although the existence of linear data compression codes with rate arbitrarily close to the SW bound has been long known for *arbitrarily correlated* sources [9], constructions of such linear data compression codes are understood in terms of the cosets of linear error-correction codes for the virtual channel, say $P_{X_1|X_2}$, only when this virtual channel is characterized by (independent) additive noise [48]. For instance, when two terminals are connected by a virtual BSC $P_{X_1|X_2}$, a linear data compression code, which attains the SW rate $H(X_1|X_2)$ for terminal 2 to reconstruct the signal at terminal 1, is then provided by a linear channel code which achieves the capacity of the BSC $P_{X_1|X_2}$.

When the i.i.d. sequences observed at terminals 1 and 2 are *arbitrarily correlated*, the associated virtual communication channel $P_{X_1|X_2}$ connecting them is no longer symmetric and corresponds to a virtual channel with input-dependent noise. In this case, while linear codes are no longer rate-optimal for the given channel [15], linear code constructions for a suitably enlarged "semisymmetric" channel that are used for SW data compression [20] could pave the way for devising schemes for SK construction.

The second step in the SK construction schemes involves SK extraction from the previously acquired CR. It has been shown [33] that for the special case of a two-terminal source model, this extraction can be accomplished by means of a linear transformation. However, it is unknown yet whether this holds also for a general source model with more than two terminals.

Appendix A
Proof of Proposition 1

We shall prove (7) here. The proof of (8), which is similar, is omitted. Fix $\delta > 0$ and consider the set $T^n_{[P_X]_\delta}$ of sequences in $\mathcal{X}^n$ which are *P_X-typical with constant δ* (cf. [10, p. 33]), i.e.,

$$T^n_{[P_X]_\delta} = \{\mathbf{x} \in \mathcal{X}^n : \max_{a\in\mathcal{X}} |P_{\mathbf{x}}(a) - P_X(a)| \le \delta\}.$$

Since $T^n_{[P]_\delta}$ is the union of the sets of those types $\tilde{P}$ of sequences in $\mathcal{X}^n$ that satisfy

$$\max_{a\in\mathcal{X}} |\tilde{P}(a) - P_X(a)| \le \delta \tag{40}$$

we have

$$\begin{aligned}\sum_{\mathbf{x}\in\left(T^n_{[P_X]_\delta}\right)^c} & P^n_X(\mathbf{x}) \\ &= \sum_{\tilde{P}:\max_{a\in\mathcal{X}} |\tilde{P}(a)-P_X(a)|>\delta} P^n_X\left(\{\mathbf{x} : P_{\mathbf{x}} = \tilde{P}\}\right) \\ &\le (n+1)^{|\mathcal{X}|} \cdot 2^{-n \min_{\tilde{P}:\min_{a\in\mathcal{X}} |\tilde{P}(a)-P_X(a)|>\delta} D(\tilde{P}\|P_X)}\end{aligned} \tag{41}$$

using the fact that $P^n_X(\{\mathbf{x} : P_{\mathbf{x}} = \tilde{P}\}) \le 2^{-nD(\tilde{P}\|P)}$ (cf. [10, Lem. 2.6]).

Next, by Pinsker's inequality (cf. e.g., [10, p. 58])

$$\begin{aligned}D(\tilde{P}\|P) &\ge \frac{1}{2ln2}\left(\min_{a\in\mathcal{X}} |\tilde{P}(a) - P_X(a)|\right)^2 \\ &\ge \frac{\delta^2}{2ln2}\end{aligned} \tag{42}$$

with the previous inequality holding for every $\tilde{P}$ in (40). It follows from (41) and (42) that

$$\sum_{\mathbf{x}\in T^n_{[P]_\delta}} P^n_X(\mathbf{x}) \ge 1 - (n+1)^{|\mathcal{X}|} \cdot 2^{-n\frac{\delta^2}{2ln2}} \tag{43}$$

for all $n \ge 1$.

Finally, observe that

$$T^n_{[P_X]_\delta} \subseteq T^n_{X,\xi}, \text{ if } \xi = \delta\left[\sum_{a\in\mathcal{X}} \log\frac{1}{P_X(a)}\right] \tag{44}$$

which is readily seen from the fact that for each $\mathbf{x} \in \mathcal{X}^n$

$$\begin{aligned}-\frac{1}{n}\log P^n_X(\mathbf{x}) - H(P_X) &= -\frac{1}{n}\log\left(2^{-n[H(P_{\mathbf{x}})+D(P_{\mathbf{x}}\|P_X)]}\right) \\ &\quad - H(P_X) \\ &= H(P_{\mathbf{x}}) + D(P_{\mathbf{x}}\|P_X) - H(P_X) \\ &= H(P_{\mathbf{x}}) - H(P_{\mathbf{x}}) \\ &\quad + \sum_{a\in\mathcal{X}} P_{\mathbf{x}}(a)\log\frac{1}{P_X(a)} - H(P_X) \\ &= \sum_{a\in\mathcal{X}} [P_{\mathbf{x}}(a) - P_X(a)]\log\frac{1}{P_X(a)}.\end{aligned}$$

Clearly, (43) and (44) imply (7). ■

Appendix B
Proof of Proposition 2

The proof of Proposition 2 relies on the following lemma concerning the average error probability of maximum likelihood decoding.

A sequence $\mathbf{u} \in \{0,1\}^n$ is called a *descendent* of a sequence $\mathbf{v} \in \{0,1\}^n$ if $u_i = 1$ implies that $v_i = 1, 1 \le i \le n$. A subset $\Omega \subset \{0,1\}^n$ is called *quasiadmissible* if the conditions that $\mathbf{u} \in \Omega$ and $\mathbf{u}$ is a descendent of $\mathbf{v}$ together imply that $\mathbf{v} \in \Omega$.

Lemma 2 [30]: If Ω is a quasiadmissible subset of $\{0,1\}^n$, then for $0 \le p \le 1$

$$\frac{d\mu_p(\Omega)}{dp} > 0$$

where

$$\mu_p(\Omega) = \sum_{\mathbf{x}\in\Omega} p^{w_H(\mathbf{x})}(1-p)^{n-w_H(\mathbf{x})}$$

with $w_H(\mathbf{x})$ denoting the Hamming weight of $\mathbf{x}$. ■

For a binary linear code, let $\mathbf{E}$ denote the set of coset leaders. It is known (cf. [36, Th. 3.11]) that $\Omega' = \{0,1\}^n\backslash\mathbf{E}$ is a quasiadmissible subset of $\{0,1\}^n$. If a binary linear code is used on BSC(p), the average error probability of maximum likelihood decoding is given by (cf. [41, Th. 5.3.3])

$$\mu_p(\Omega') = \sum_{\mathbf{x}\in\Omega'} p^{w_H(\mathbf{x})}(1-p)^{n-w_H(\mathbf{x})}.$$

Lemma 2 implies that if the same binary linear code is used on two binary symmetric channels with different crossover probabilities, say, $0 < p_1 < p_2 < \frac{1}{2}$, then the average error probability of maximum likelihood decoding for a $\mathrm{BSC}(p_1)$ is strictly less than that for a $\mathrm{BSC}(p_2)$; note that a $\mathrm{BSC}(p_2)$ is a degraded version of a $\mathrm{BSC}(p_1)$, being a cascade of the latter and a BSC $\left(\frac{p_2-p_1}{1-2p_1}\right)$.

Returning to the proof of Proposition 2, it follows from Lemma 1 that for some $\eta > 0$ and for all n sufficiently large

$$\Pr\{\hat{\mathbf{X}}_{j^*}(i^*) \ne \mathbf{X}_{i^*}\} < 2^{-n\eta}.$$

Recall that $p_{(i^*,j^*)} = \max_{(i,j)\in E(\mathcal{T})} p_{(i,j)}$ and $(i = i_0, i_1, \ldots, i_r = i^*)$ is the path from i to i^*. It follows by Lemma 2 that

$$\Pr\{\hat{\mathbf{X}}_i(i_1) \neq \mathbf{X}_{i_1}\} < \Pr\{\hat{\mathbf{X}}_{j^*}(i^*) \neq \mathbf{X}_{i^*}\} < 2^{-n\eta}.$$

Consequently

$$\begin{aligned}\Pr\{\hat{\mathbf{X}}_i(i_2) \neq \mathbf{X}_{i_2}\} =& \Pr\{\hat{\mathbf{X}}_i(i_2) \neq \mathbf{X}_{i_2}, \hat{\mathbf{X}}_i(i_1) \neq \mathbf{X}_{i_1}\} \\ &+ \Pr\{\hat{\mathbf{X}}_i(i_2) \neq \mathbf{X}_{i_2}, \hat{\mathbf{X}}_i(i_1) = \mathbf{X}_{i_1}\} \\ \leq& \Pr\{\hat{\mathbf{X}}_i(i_1) \neq \mathbf{X}_{i_1}\} \\ &+ \Pr\{\hat{\mathbf{X}}_i(i_2) \neq \mathbf{X}_{i_2}, \hat{\mathbf{X}}_i(i_1) = \mathbf{X}_{i_1}\} \\ \leq& \Pr\{\hat{\mathbf{X}}_i(i_1) \neq \mathbf{X}_{i_1}\} \\ &+ \Pr\{\hat{\mathbf{X}}_{i_1}(i_2) \neq \mathbf{X}_{i_2}, \hat{\mathbf{X}}_i(i_1) = \mathbf{X}_{i_1}\} \\ \leq& \Pr\{\hat{\mathbf{X}}_i(i_1) \neq \mathbf{X}_{i_1}\} + \Pr\{\hat{\mathbf{X}}_{i_1}(i_2) \neq \mathbf{X}_{i_2}\} \\ <& 2 \cdot 2^{-n\eta}\end{aligned}$$

where the second inequality is due to $\mathbf{X}_i, \mathbf{X}_{i_1}, \mathbf{X}_{i_2}$ forming a Markov chain. Continuing this procedure, we have finally that

$$\Pr\{\hat{\mathbf{X}}_i(i^*) \neq \mathbf{X}_{i^*}\} < r \cdot 2^{-n\eta} < d \cdot 2^{-n\eta}.$$

■

References

[1] A. Aaron and B. Girod, "Compression with side information using turbo codes," in *Proc. IEEE Data Compression Conf.*, Snowbird, UT, Apr. 2002, pp. 252–261.

[2] R. Ahlswede and I. Csiszár, "Common randomness in information theory and cryptography, Part I: Secret sharing," *IEEE Trans. Inf. Theory*, vol. 39, no. 4, pp. 1121–1132, Jul. 1993.

[3] M. Andersson, V. Rathi, R. Thobaben, J. Kliewer, and M. Skoglund, Nested polar codes for wireless and relay channels 2010 [Online]. Available: http://arxiv.org/pdf/1006.3573

[4] E. Arikan, "Channel polarization: A method for constructing capacity-achieving codes for symmetric binary-input memoryless channel," *IEEE Trans. Inf. Theory*, vol. 55, no. 7, pp. 3051–3073, Jul. 2009.

[5] E. Arikan and E. Telatar, "On the rate of channel polarization," in *Proc. Int. Symp. Inf. Theory*, Seoul, Korea, Jun. 2009.

[6] C. H. Bennett, G. Brassard, C. Crépeau, and U. M. Maurer, "Generalized privacy amplification," *IEEE Trans. Inf. Theory*, vol. 41, no. 6, pp. 1915–1923, Nov. 1995.

[7] M. Bloch, J. Barros, M. Rodrigues, and S. W. M. McLaughlin, "Wireless information theoretic security," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2515–2534, Jun. 2008.

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

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

[10] I. Csiszár and J. Körner, *Information Theory: Coding Theorems for Discrete Memoryless Systems*. New York: Academic, 1982.

[11] I. Csiszár and P. Narayan, "Common randomness and secret key generation with a helper," *IEEE Trans. Inf. Theory*, vol. 46, no. 2, pp. 344–366, Mar. 2000.

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

[13] I. Csiszár and P. Narayan, "Secrecy capacities for multiterminal channel models," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2437–2452, Jun. 2008.

[14] P. Elias, "Coding for noisy channels," *IRE Convention Rec.*, pt. 4, pp. 37–46, 1955.

[15] E. M. Gabidulin, "Bounds for the probability of decoding error when using linear codes over memoryless channels," *Prob. Pered. Inf.*, vol. 3, pp. 55–62, 1967.

[16] J. Garcia-Frias and Y. Zhao, "Compression of correlated binary sources using turbo codes," *IEEE Commun. Lett.*, vol. 5, no. 11, pp. 417–419, Oct. 2001.

[17] J. Garcia-Frias and W. Zhong, "LDPC codes for compression of multi-terminal sources with hidden Markov correlation," *IEEE Commun. Lett.*, vol. 7, no. 3, pp. 115–117, Mar. 2003.

[18] H. O. Georgii, *Gobbs Measures and Phase Transitions*. Berlin, Germany: De Gruyter, 1988.

[19] A. A. Gohari and V. Anantharam, "Information-theoretic key agreement of multiple terminals—part I," *IEEE Trans. Inf. Theory*, vol. 56, no. 8, pp. 3973–3996, Aug. 2010.

[20] D.-K. He and E.-H. Yang, "On the duality between Slepian–Wolf coding and channel coding," in *Proc. Int. Symp. Inf. Theory*, Seattle, WA, Jul. 2006, pp. 2546–2550.

[21] R. Hu, R. Viswanathan, and J. Li, "A new coding scheme for the noisy-channel Slepian–Wolf problem: Separate design and joint decoding," in *Proc. Global Commun. Conf.*, Dallas, TX, 2004.

[22] O. O. Koyluoglu and H. E. Gamal, Polar coding for secure transmission and key agreement 2010 [Online]. Available: http://arxiv.org/pdf/1003.1422

[23] C. Lan, A. Liveris, K. Narayanan, Z. Xiong, and C. N. Georghiades, "Slepian–Wolf coding of multiple M-ary sources using LDPC code," in *Proc. IEEE Data Compression Conf.*, Snowbird, UT, Mar. 2004, p. 549.

[24] J. Li, Z. Tu, and R. Blum, "Slepian–Wolf coding for nonuniform sources using turbo codes," in *Proc. IEEE Data Compression Conf.*, Snowbird, UT, Mar. 2004, pp. 312–321.

[25] Y. Liang, H. V. Poor, and S. Shamai, "Information theoretic security," *Found. rends Commun. Inf. Theory*, vol. 5, no. 4–5, pp. 355–580, 2008.

[26] A. D. Liveris, Z. Xiong, and C. N. Georghiades, "Compression of binary sources with side information at the decoding using LDPC codes," *IEEE Commun. Lett.*, vol. 6, no. 10, pp. 440–442, Oct. 2002.

[27] A. D. Liveris, C. Lan, K. R. Narayanan, Z. Xiong, and C. N. Georghiades, "Slepian–Wolf coding of three binary sources using LDPC codes," in *Proc. Int. Symp. Turbo Codes and Related Topics*, Brest, France, Sep. 2003.

[28] D. J. C. Mackay, "Good error correcting codes based on very sparse matrices," *IEEE Trans. Inf. Theory*, vol. 45, no. 2, pp. 399–431, Mar. 1999.

[29] H. Mahdavifar and A. Vardy, Achieving the secrecy capacity of wiretap channels using polar codes 2010 [Online]. Available: http://arxiv.org/abs/1001.0210

[30] G. A. Margulis, "Probabilistic characteristics of graphs with large connectivity," *Probl. Inf. Trans.*, vol. 10, pp. 174–179, Apr. 1974.

[31] U. M. Maurer, "Secret key agreement by public discussion from common information," *IEEE Trans. Inf. Theory*, vol. 39, no. 3, pp. 733–742, May 1993.

[32] P. Mitran and J. Bajcsy, "Turbo source coding: A noise-robust approach to data compression," in *IEEE Data Compression Conf.*, Snowbird, UT, Apr. 2002, p. 465.

[33] J. Muramatsu, "Secret key agreement from correlated source outputs using LDPC matrices," *IEICE Trans. Fundamentals*, vol. E89-A, pp. 2036–2046, Jul. 2006.

[34] S. Nitinawarat, "Secret key generation for correlated Gaussian sources," in *Proc. Allerton Conf. Commun., Control, and Computing*, Monticello, IL, Sep. 2007, pp. 1054–1058.

[35] S. Nitinawarat and P. Narayan, "Secret key generation for correlated Gaussian sources," *IEEE Trans. Inf. Theory*, 2011, to be published.

[36] W. W. Peterson and E. J. Weldon, *Error-Correcting Codes*, 2nd ed. Cambridge, MA: MIT Press, 1972.

[37] S. S. Pradhan and K. Ramchandran, "Distributed source coding using syndromes (DISCUS): Design and construction," *IEEE Trans. Inf. Theory*, vol. 49, no. 3, pp. 626–643, Mar. 2003.

[38] R. Renner and S. Wolf, "New bounds in secret-key agreement: The gap between formation and secrecy extraction," in *Proc. EUROCRYPT*, 2003, vol. 2656, Lecture Notes in Computer Science, pp. 562–577.

[39] T. J. Richardson and R. L. Urbanke, "The capacity of low-density parity-check codes under message-passing decoding," *IEEE Trans. Inf. Theory*, vol. 47, no. 2, pp. 599–618, Feb. 2001.

[40] T. Richardson and R. Urbanke, *Modern Coding Theory*. Cambridge, U.K.: Cambridge Univ. Press, 2008.
[41] S. Roman, *Introduction to Coding and Information Theory*. New York: Springer, 1996.
[42] R. M. Roth, *Introduction to Coding Theory*. Cambridge, U.K.: Cambridge Univ. Press, 2006.
[43] D. Schonberg, K. Ramchandran, and S. S. Pradhan, "Distributed code constructions for the entire Slepian–Wolf rate region for arbitrarily correlated sources," in *Proc. IEEE Data Compression Conf.*, Snowbird, UT, Mar. 2004, pp. 292–301.
[44] R. M. Tanner, "A recursive approach to low complexity codes," *IEEE Trans. Inf. Theory*, vol. 27, no. 5, pp. 533–547, Sep. 1981.
[45] 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.
[46] A. Thangaraj, S. Dihidar, A. R. Calderbank, S. McLaughlin, and J. M. Merolla, "Applications of LDPC codes to the wiretap channel," *IEEE Trans. Inf. Theory*, vol. 53, no. 8, pp. 2933–2945, Aug. 2007.
[47] R. Wilson, D. Tse, and R. Scholtz, "Channel identification: Secret sharing using reciprocity in ultrawideband channels," *IEEE Trans. Inf. Foren. Secur.*, vol. 2, no. 3, pp. 364–375, Sep. 2007.
[48] A. D. Wyner, "Recent results in the Shannon theory," *IEEE Trans. Inf. Theory*, vol. 20, no. 1, pp. 2–10, Jan. 1974.
[49] C. Ye and P. Narayan, "Secret key and private key constructions for simple multiterminal source models," in *Proc. IEEE Int. Symp. Inf. Theory*, Adelaide, Australia, Sep. 2005, pp. 2133–2137.
[50] C. Ye and P. Narayan, "Secret key constructions for simple multiterminal source models," in *Proc. Inf. Theory and Applications Workshop*, San Diego, CA, Feb. 2006.
[51] C. Ye, A. Reznik, and Y. Shah, "Extracting secrecy from jointly Gaussian random variables," in *Proc. Int. Symp. Inf. Theory*, Jul. 2006, pp. 2593–2597.
[52] C. Ye, S. Mathur, A. Reznik, Y. Shah, W. Trappe, and N. Mandayam, "Information-theoretically secret key generation for fading wireless channels," *IEEE Trans. Inf. Foren. Secur.*, vol. 5, no. 2, pp. 240–254, Jun. 2010.
[53] R. W. Yeung, *Information Theory and Network Coding*. New York: Springer, 2008.

Chunxuan Ye (S'01–M'06–SM'10) received the B.Eng. (Hons) degree in electrical engineering from Shanghai Jiao Tong University, Shanghai, China, the M.Phil. degree in information engineering from the Chinese University of Hong Kong, Hong Kong, and the Ph.D. degree in electrical and computer engineering from the University of Maryland, College Park, in 1997, 2000, and 2005, respectively.

He has been working at InterDigital Communications, King of Prussia, PA, since 2005. His research interests are in the areas of information theory, communication theory, and wireless communication systems. These include information theoretic security, cooperative and relayed networks, network coding and source coding, wireless system prototyping platform, cognitive radio, and wireless communications networks. He has published more than 25 papers and book chapters. He has more than 20 pending U.S. patents.

Prakash Narayan (S'80–M'81–SM'94–F'01) received the B.Tech. degree in electrical engineering from the Indian Institute of Technology, Madras, India, in 1976, and the M.S. degree in systems science and mathematics in 1978 and the D.Sc. degree in electrical engineering, both from Washington University, St. Louis, MO, in 1981.

He is currently a Professor of electrical and computer engineering at the University of Maryland, College Park, with a joint appointment at the Institute for Systems Research. He has held visiting appointments at ETH, Zurich; the Technion, Haifa; the Renyi Institute of the Hungarian Academy of Sciences, Budapest; the University of Bielefeld; the Institute of Biomedical Engineering (formerly LADSEB), Padova; and the Indian Institute of Science, Bangalore. His research interests are in multiuser information theory, communication theory, communication networks, cryptography, and information theory and statistics.

Dr. Narayan has served as Associate Editor for Shannon Theory for the IEEE TRANSACTIONS ON INFORMATION THEORY. He was Co-Organizer of the IEEE Workshop on Multi-User Information Theory and Systems, VA (1983), Technical Program Chair of the IEEE/IMS Workshop on Information Theory and Statistics, VA (1994), General Co-Chair of the IEEE International Symposium on Information Theory, Washington, D.C. (2001), and Technical Program Co-Chair of the IEEE Information Theory Workshop, Bangalore (2002). He currently serves as a member of the Board of Governors of the IEEE Information Theory Society.