Abstract—Practical implementations of secret-key generation are often based on sequential strategies, which successively deal with reliability and secrecy in two steps, called reconciliation and privacy amplification. In this paper, we propose an alternative scheme based on polar coding, that jointly deals with reliability and secrecy. We study a binary degraded symmetric discrete memoryless source model with uniform marginals, and assume one-way rate-limited public communication between two legitimate users. Specifically, we propose capacity-achieving polar coding schemes, when the legitimate users share beforehand a small secret, which we call a seed and which rate can be chosen arbitrarily small. For the model studied, we thus provide the first example of low-complexity capacity-achieving scheme that handles vector quantization, when the public communication is rate-limited. Furthermore, we show examples for which no seed is required.

I. INTRODUCTION

Secret-key generation

Secret-key generation plays a crucial role in information-theoretic security. Closed-form expressions for the secret-key capacity have been derived for numerous models [1]–[5]. However, few achievability schemes provide insight for practical implementations of secret-key generation, with the exception of sequential methods [6]–[8]. This paper presents a practical low-complexity capacity-achieving scheme based on polar codes [9] for some classes of sources. Note that polar codes have already been used to ensure weak secrecy [10]–[13], and strong secrecy [14] for the wire-tap channel.

Unlike sequential methods, which successively deal with reliability and secrecy in two steps, called reconciliation and privacy amplification [15], our scheme jointly deals with reliability and secrecy. Both the sequential reliability-secrecy approach, and the direct approach with polar codes have their advantages. On the one hand, sequential methods offer flexibility in design by separating reliability and secrecy, and remain optimal for two-way communication and continuous non degraded sources [8]. On the other hand, polar coding schemes may be easier to design in some scenarios, and appear to be very handy to deal with vector quantization when the public communication is rate-limited.

In this paper, we study secret-key generation for a binary degraded (symmetric) discrete memoryless source (BD(S)DMS) model, assuming one-way public communication. We assume that the legitimate users share beforehand a secret seed which.

I. PROBLEM STATEMENT

We define a BDMS $(X\rightarrow Y\rightarrow Z, p_{XYZ})$, as a DMS such that $X = \{0, 1\}$, $Y$, $Z$ are arbitrary finite discrete alphabets, and $X \rightarrow Y \rightarrow Z$ forms a Markov chain. A BDSDMS is similarly defined, but in addition, the test channels associated to $p_{Y|X}$ and $p_{Z|X}$ are symmetric. Moreover, we say that a BDSDMS has uniform marginals, if $X$ is $B(1/2)$, where $B(p)$ denotes the Bernoulli distribution with parameter $p \in [0, 1]$. As illustrated in Figure 1 we consider that two legitimate users, Alice and Bob, and an eavesdropper, Eve, observe the components, $X$, $Y$, and $Z$ of a BD(S)DMS, respectively. The source is assumed to be outside the control of all parties, but its statistics are known to all parties. One-way communication can be performed from Alice to Bob over an authenticated noiseless public channel with rate $R_p \in \mathbb{R} \cup \{+\infty\}$. A secret-key generation strategy is formally defined as follows.

Definition 1. Let $K$ be a key alphabet of size $2^{NR}$. The
protocol defined by the three following steps is called a \((2^{NR}, N, R_p)\) secret-key generation strategy, and is denoted by \(S_N\).

1) Alice observes \(X^N\) while Bob observes \(Y^N\).
2) Alice transmits \(A(X^N)\), such that \(H(A) \leq NR_p\).
3) Alice computes \(K(X^N) \in K\), while Bob computes \(\hat{K}(Y^N, A) \in K\).

The performance of a secret-key generation strategy \(S_N\) is measured in terms of the average probability of error between the key \(K\) generated by Alice and the key \(\hat{K}\) generated by Bob. \(P_e(S_N) \triangleq \mathbb{P}[K \neq \hat{K}]\), in terms of the information leakage to the eavesdropper \(L(S_N) \triangleq I(K; Z^N A)\), and in terms of the uniformity of the keys \(U(S_N) \triangleq \log[2^{NR}] - H(K)\).

**Definition 2.** A secret-key rate \(R\) is achievable for a source model if there exists a sequence of \((2^{NR}, N, R_p)\) secret-key generation strategies \(\{S_N\}_{N \geq 1}\) such that

\[
\lim_{N \to \infty} P_e(S_N) = 0 \quad \text{(reliability)},
\]

\[
\lim_{N \to \infty} L(S_N) = 0 \quad \text{(strong secrecy)},
\]

\[
\lim_{N \to \infty} U(S_N) = 0 \quad \text{(strong uniformity)}.
\]

Moreover, the supremum of such a rate \(R\) is called the secret-key capacity and is denoted \(C_{\text{WSK}}(R_p)\).

In the following sections, we propose capacity-achieving schemes based on polar coding.

**III. ACHIEVABILITY OF \(C_{\text{WSK}}(+\infty)\)**

In this section, we assume an unlimited public communication rate, i.e. \(R_p = +\infty\). We recall the expression of \(C_{\text{WSK}}(+\infty)\) in the following proposition.

**Proposition 1 (\([17]\)).** Let \((X^N, Y^N, Z)\) be a degraded DMS, that is \(X \rightarrow Y \rightarrow Z\) forms a Markov chain. The secret-key capacity \(C_{\text{WSK}}(+\infty)\) is

\[
C_{\text{WSK}}(+\infty) = I(X; Y) - I(X; Z) = I(X; Y | Z).
\]

In Theorem 1 we refine the early work started in \([17]\).

**Theorem 1.** Consider a BDDMS \((X^N, Y^N, Z)\). Assume that Alice and Bob share a secret seed with arbitrarily small rate. The secret-key capacity \(C_{\text{WSK}}(+\infty)\) is achievable by a polar coding scheme.

**Proof:** Let \(\delta > 0\), \(\beta \in [0, 1/2]\). Let \(n \in \mathbb{N}\) and \(N \triangleq 2^n\). Let \(G_N \triangleq \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \otimes B_N\) be the source polarization transform defined in \([18]\), and set \(U^N \triangleq X^NG_N\). For any set \(A \triangleq \{i_1, i_2, \ldots, i_{|A|}\} \subseteq [1, N]\), we define \(U^N[A] \triangleq [U_{i_1}, U_{i_2}, \ldots, U_{i_{|A|}}]\). In the following, we denote the complement set operation by the superscript \(c\). Define the following sets

\[
\mathcal{F}^c_E \triangleq \{i \in [1, N] \mid H(U_i | Z^N U^{i-1}) \geq 1 - 2^{-N^\beta}\},
\]

\[
\mathcal{F}_{E^c} \triangleq \{i \in [1, N] \mid H(U_i | Z^N U^{i-1}) \geq 1 - \delta\},
\]

\[
\mathcal{F}_E \triangleq \{i \in [1, N] \mid H(U_i | Y^N U^{i-1}) \geq 1 - \delta\}.
\]

**Lemma 1.** The sets \(\mathcal{F}_E^c\) and \(\mathcal{F}_E\) verify

1) \(\lim_{N \to +\infty} |\mathcal{F}_E^c|/N = H(X|Z)\),
2) \(\lim_{N \to +\infty} |\mathcal{F}_E \cap \mathcal{F}_{E^c}|/N = 0\),
3) \(\lim_{N \to +\infty} |\mathcal{F}_E^c \cap \mathcal{F}_E|/N = H(X|Y)\),
4) \(\lim_{N \to +\infty} |\mathcal{F}_E \cap |\mathcal{F}_E^c|/N = I(X; Y) - I(X; Z)\).

**Proof:** Observe that, for \(N\) large enough, \(\mathcal{F}_E \subset \mathcal{F}_E^c\); the data processing inequality also guarantees \(\mathcal{F}_E^c \subset \mathcal{F}_E\), since \(X \rightarrow Y \rightarrow Z\) forms a Markov chain. As in \([19]\), for a pair of random variables \((X, Y)\) distributed according to \(p_{XY}\) over \(X \times Y\), we define the Bhattacharyya parameter as

\[
Z(X|Y) = 2 \sum_y \sqrt{p_X(y) p_Y(y)}.
\]

Using the same technique as \([19]\) Lemma 20, we can show the following counterpart of \([18]\) Proposition 1.

**Lemma 2.** If \((X_1, Y_1)\) and \((X_2, Y_2)\) are two independent drawings from \((X, Y)\), then

\[
Z(X_1 \oplus X_2 | Y_1^2) \geq \sqrt{2Z(X|Y)^2 - Z(X|Y)^4}.
\]

1) \(\lim_{N \to +\infty} |\mathcal{F}_0|/N = H(X|Z)\).

2) \(\lim_{N \to +\infty} |\mathcal{F}_0|/N = H(X|Z)\).

3) \(\lim_{N \to +\infty} |\mathcal{F}_0|/N = H(X|Z)\).

4) \(\lim_{N \to +\infty} |\mathcal{F}_0|/N = H(X|Z)\).

**Lemma 3.** The bits \(U^N[\mathcal{F}_E]\) verify the following property

\[
H(U^N[\mathcal{F}_E] | Z^N) \geq |\mathcal{F}_E| \left(1 - 2^{-N^\beta}\right).
\]

We define a secret-key generation strategy \(S_N\) as follows. Define the key as \(K \triangleq U^N[\mathcal{F}_E \cap \mathcal{F}_B]\), the public message as \(A \triangleq U^N[\mathcal{F}_E \cap \mathcal{F}_B]\), and assume there is also a secret communication \(A'\) between Alice and Bob, where \(A' \triangleq U^N[\mathcal{F}_E \cap \mathcal{F}_B]\). The secret communication is performed by a one-time pad with the seed shared by Alice and Bob. By \([18]\) Theorem 3, Bob can reconstruct \(K\) from \(A\) and \(A'\) with an error probability satisfying \(P_e(S_N) = O\left(2^{-N^\beta}\right)\). Moreover, by Lemma 1 and Proposition 1 the key rate clearly achieves the secret-key capacity. We now establish the strong secrecy. We need the following lemma.

**Lemma 3.** The bits \(U^N[\mathcal{F}_E]\) verify the following property

\[
H(U^N[\mathcal{F}_E] | Z^N) \geq |\mathcal{F}_E| \left(1 - 2^{-N^\beta}\right).
\]
Proof: We have
\[ H(U^N|F_k^E|Z^N) = \sum_{i \in F_k^E} H(U_i|U_i^{-1}|F_k^E|Z^N), \]
\[ \geq \sum_{i \in F_k^E} H(U_i|U_i^{-1}|Z^N), \]
\[ \geq |F_k|^\left(1 - 2^{-N^a}\right), \]
where the last inequality follows from the definition of \( F_k^E \).

We now write the information leakage as follows,
\[ I(K; AZ^N) = I(U^N|F_k^E \cap F_B; U^N|F_k^E \cap F_B|Z^N) = H(U^N|F_k^E \cap F_B) - H(U^N|F_k^E \cap F_B|Z^N). \]

We first bound the second term in (1) as,
\[ H(U^N|F_k^E \cap F_B) = H(U^N|F_k^E \cap F_B) - H(U^N|F_k^E \cap F_B|Z^N) \]
\[ = H(U^N|F_k^E|Z^N) - H(U^N|F_k^E \cap F_B|Z^N), \]
and holds because conditioning reduces entropy and (b) holds by Lemma 3. We then bound the first term in (1) as,
\[ H(U^N|F_k^E \cap F_B) \leq |F_k^E| - |F_k^E \cap F_B|. \]
Hence, combining (1), (2) and (3), we obtain
\[ L(S_N) \leq N2^{-N^a}. \]

We now show the uniformity of the key. We have,
\[ H(K) = \sum_{i \in F_k^B} H(U_i|K) \]
\[ = H(U^N|F_k^E \cap F_B) - H(U^N|F_k^E \cap F_B|Z^N), \]
where (c) holds because conditioning reduces entropy, (d) holds by (2); we also have
\[ U(S_N) = \log|K| - H(K) \]
\[ = |F_k^E| - |F_k^E \cap F_B| - H(K), \]
Hence, combining (4) and (5),
\[ U(S_N) \leq N2^{-N^a}. \]

Finally, we show that the seed rate can be made arbitrarily small by performing block encoding [14]. Assume we repeat the previous secret-key generation strategy over \( k \) blocks of length \( N \). For \( i \in [1, k] \), we note \( A_i' \) the secret seed needed to obtain \( K_i \), the secret key generated over the block \( i \). First, we need \( |A_i'| \) bits to perform the secret-key generation over the first block, then for \( i \in [2, k] \), we can use \( |A_i'| \) bits of the secret key generated with block \( i-1 \), to privately transmit \( A_i' \) and generate \( K_i \). This operation does not affect the key rate per block for large \( N \), since for all \( i \in [1, k] \), \( |A_i'| = o(N) \) by Lemma 4. Consequently, we only need to secretly transmit \( |A_0'| \) bits, which translates to an overall seed rate \( |A_0'|/(kN) \), which decreases to zero independently of \( N \) as the number \( k \) of blocks goes to infinity.

**Remark 1.** In the special case of a BDSDMS, Theorem 7 can indirectly be obtained from wiretap codes and the recent paper [14], following [1]. [7] Section 4.2.1. However, this indirect proof might not be suitable to practical implementations.

**Remark 2.** Recall that, for lossless source coding, there is a fundamental trade-off between error probability and uniformity of the encoder output with respect to the variational distance [20]. Section VI. However, as shown in [21], [22], this impossibility can be overcome if the encoder and the decoder share a small seed beforehand. In our coding scheme, it translates to the impossibility of ensuring strong secrecy and strong uniformity simultaneously, unless the legitimate users share a small seed.

IV. Achievability of \( C_{WSK}(R_p) \), \( \mathbb{R}^+ \in \mathbb{R}^+ \)

In this section, as depicted in Figure 2 we consider a rate-limited public communication rate \( R_p \in \mathbb{R}^+ \), between the legitimate users, and a BDSDMS \( (X \cup Y \cup Z) \) with uniform marginals, where \( X \triangleq Y \triangleq Z \), and such that \( Y \triangleq X \triangleq B_1 \) and \( Z \triangleq Y \triangleq B_2 \), with \( B_1 \sim B(p), B_2 \sim B(q) \). We recall in the following proposition the closed-form expression of the secret-key capacity for this setup.

**Proposition 2 (\textbf{I}).** Let \( R_p \in \mathbb{R}^+ \). Define the following associative and commutative operation \( a * b \triangleq (1 - b)a + b(1 - a) \), for any \( a, b \in [0, 1] \). The secret-key capacity \( C_{WSK}(R_p) \) is
\[ \begin{align*}
H_b(p \ast \beta_0 \ast q) - H_b(p \ast \beta_0), & \quad \text{if } R_p \leq H(X|Y), \\
H_b(p \ast q) - H_b(p), & \quad \text{if } R_p > H(X|Y),
\end{align*} \]
with \( H_b(\cdot) \) the binary entropy, and \( \beta_0 \), any of the two symmetric solutions of the equation
\[ H_b(p \ast \beta_0) - H_b(\beta_0) = R_p. \]

**Theorem 2.** Consider a BDSDMS \( (X \cup Y \cup Z, p_{XYZ}) \) with uniform marginals. Assume that Alice and Bob share a secret seed with arbitrarily small rate and let \( R_p \in \mathbb{R}^+ \). The secret-key capacity \( C_{WSK}(R_p) \) is achievable by a polar coding scheme.

Observe that by Proposition 2 for any \( R_p \in [H(X|Y), +\infty[ \), \( C_{WSK}(R_p) = C_{WSK}(+\infty) \). Hence, by
Theorem 1, the assumption of uniform distribution can be removed in Theorem 2 as long as $R_p \geq H(X|Y)$.

**Proof:** Our proof is inspired by polar coding for the Wyner-Ziv problem [19]. We assume $R_p \leq H(X|Y)$, since the case $R_p \geq H(X|Y)$ is deduced from Theorem 1 and Proposition 2. Let $\epsilon > 0$, $\beta \in [0, 1/2]$. Let $n \in \mathbb{N}$ and $N = 2^n$. For any set $A$ of indices in $[1, N]$, we define $U_n[A]$ as in the proof of Theorem 1. For $i \in [1, N]$, we denote $Z_N(i)$, the Bhattacharyya parameter of $W_N(i)$, the $i$-th bit channel, as defined in [9], corresponding to a binary symmetric channel with parameter $\alpha \in [0, 1]$. Define the following sets

$$F_S \triangleq \left\{ i : Z_N(i) > 1 - 2\delta_N \right\},$$

$$F_B \triangleq \left\{ i : Z_N(i) > 1 - \delta_N \right\},$$

$$F_{B'} \triangleq \left\{ i : Z_N(i) > \delta_N \right\},$$

$$F_E \triangleq \left\{ i : Z_N(i) > 2\delta_N \right\},$$

where $\beta_0$ is defined in [6].

**Lemma 4.** The sets $F_S$, $F_B$, $F_{B'}$, and $F_E$ verify

1. $F_S \subset F_B \subset F_E$.
2. $\lim_{N \to +\infty} |F_S|/N = H_b(\beta_0)$.
3. $\lim_{N \to +\infty} |F_B|/N = H_b(\beta_0 * p)$.
4. $\lim_{N \to +\infty} |F_{B'}|/F_B|/N = 0$.
5. $\lim_{N \to +\infty} |F_E|/N = H_b(\beta_0 * p * q)$.

**Proof:** We first show 1). Assume $i \in F_S$, then, by [19] Lemma 21), we have $Z_N(i)(\beta_0) > 2\delta_N \geq 1 - \delta_N$. Assume now $i \in F_B$, then by [19] Lemma 21), we have $Z_N(i)(\beta_0 * p) > 2\delta_N > 1 - \delta_N > 1 - 2\delta_N$, i.e. $i \in F_{B'}$. Finally, 4) holds by [19] Theorem 18 and 1).

Assume we encode Alice's observations $x_N$ as in [19] Theorem 3, using the successive-cancellation encoder for the polar code defined by the frozen set $F_S$, i.e. we perform lossy source coding with distortion $\beta_0$. We note the output of this encoding process $\hat{U}$. The following lemma states that the encoder output $\hat{U}$ is asymptotically uniform in divergence.

**Lemma 5.** Consider the lossy source coding problem, and assume the same encoding as in [19] Theorem 3 using the polar code defined by the frozen set $F_S$. If $\hat{U}$ is the encoder output, then

$$H(\hat{U}|F_S) \geq |F_S|-\delta_N,$$

with $\lim_{N \to +\infty} \delta_N = 0$.

**Proof:** By [23] Lemmas 4, 5.

We define a secret-key generation strategy $\mathcal{S}_N$ as follows. Define the key as $K \triangleq \hat{U}[F_E|F_B]$, the public communication as $A \triangleq \hat{U}[F_B|F_S]$, and assume there is also a secret communication $A' \triangleq \hat{U}[F_B'\setminus F_B]$ between Alice and Bob. Since $|F_B| - |F_B'| = o(N)$ by Lemma 4, as in the proof of Theorem 1, we treat the secret communication by block encoding [14] to obtain an arbitrarily small seed rate.

By [19] Theorem 14, Bob can reconstruct $K$ from $A$ and $A'$ with an error probability satisfying $P_e(S_N) = O(2^{-N^\epsilon})$. Moreover, by the expression $C_{\text{WSSK}}(R_p)$ in Proposition 2 and Lemma 3 the key rate is capacity-achieving. We also satisfy the public communication constraint between Alice and Bob, since by Lemma 4, we have for $N$ large enough

$$H(A) \leq |F_B| - |F_S| \leq N(H_b(\beta_0 * p) - H_b(\beta_0) + \epsilon).$$

We now show the strong secrecy. We first write

$$I(K; AZ^N) = I(\hat{U}[F_E|F_B]; \hat{U}|F_B'|F_S)Z^n) = H(\hat{U}[F_E|F_B]) - H(\hat{U}[F_E|F_B]|\hat{U}[F_B'|F_S|Z^n).$$

We bound the first term in (7) as,

$$H(\hat{U}[F_E|F_B]) \leq |F_E| - |F_B'| = |F_B| - |F_E|.$$ (8)

We bound the second term in (7) as,

$$H(\hat{U}[F_E|F_B]|\hat{U}[F_B'|F_S|Z^n)$$

$$= H(\hat{U}[F_E|F_B]|\hat{U}[F_B'|F_S|Z^n) - H(\hat{U}[F_B'|F_S|Z^n)$$

$$= H(\hat{U}[F_E|F_B]|\hat{U}[F_B'|F_S|Z^n)$$

$$= I(\hat{U}[F_E|F_B]; Z^n) - H(\hat{U}[F_B'|F_S|Z^n).$$

Finally, 4) holds by [19] Theorem 18 and 1).

Assume we encode Alice’s observations $x_N$ as in [19] Theorem 3, using the successive-cancellation encoder for the polar code defined by the frozen set $F_S$, i.e. we perform lossy source coding with distortion $\beta_0$. We note the output of this encoding process $\hat{U}$. The following lemma states that the encoder output $\hat{U}$ is asymptotically uniform in divergence.
hence, combining (11) and (12), we obtain
\begin{align*}
I \left( \hat{U} \mid F_E \cup F_S ; Z^N \right) \\
= \sum_{i \in F_E \cup F_S} I \left( Z^N ; \hat{U}_i [\hat{U}^{i-1} | F_E \cup F_S] \right) \\
\leq \sum_{i \in F_E \cup F_S} I \left( \hat{U}^{i-1} | F_E \cup F_S ; Z^N ; \hat{U}_i \right) \\
\leq \sum_{i \in F_E \cup F_S} I \left( \hat{U}^{i-1} Z^N ; \hat{U}_i \right) \\
\leq \sum_{i \in F_E \cup F_S} \sqrt{1 - \left( Z^{(i)} N \beta_0 \ast p \ast q \right)^2} \\
\leq |F_E \cup F_S| 2 \sqrt{\delta N (1 - \delta N)} \\
\leq 2N \sqrt{\delta N}.
\end{align*}

where (c) holds by [9, Proposition1], and (d) holds by definition of $F_E$. Hence, combining (7), (8), (9), and (10), we obtain $L(S_N) \leq \delta N + 2N \sqrt{\delta N}$. We now show the uniformity of the key. We start with
\begin{align*}
H(K) &= H \left( \hat{U} \mid F_E \cup F_E^c \right) \\
&= H \left( \hat{U} \mid F_E \cup F_B \right) \\
&\geq H \left( \hat{U} \mid F_E \cup F_B \mid \hat{U} \mid F_E \cup F_S \right) \\
&\geq |F_E \cup F_B| - |F_E^c| - \delta N,
\end{align*}

where (e) holds because conditioning reduces entropy, (f) holds by Equation (7) (where $Z^N$ is replaced by $\delta_0$); also
\begin{align*}
U(S_N) = \log |\mathcal{K}| - H(K) &= |F_E^c| - |F_E^c| - H(K),
\end{align*}

hence, combining (11) and (12), we obtain $U(S_N) \leq \delta N$. □

V. SCENARIOS FOR WHICH NO SEED IS REQUIRED

Although the seed rate that the legitimate users need to share in Sections II-IV can be made arbitrarily small, it is interesting to identify examples for which no seed is required.

Example 1. Consider a DMS $(X \cup Y, Z, p_{XYZ})$ with $X = \{0, 1\}$. Assume that Alice and Bob have the same observations, i.e. $X = Y$, then the secret-key capacity $C_{WSK} = H(X | Z)$ is achievable by a polar coding scheme.

Note that Example 1 corresponds to the setting of privacy amplification [15].

Example 2. Consider a BDSM $(X \cup Y, p_{XY})$ with uniform marginals, and the same setting as in Section IV with $Z = \emptyset$. The secret-key capacity is denoted $C_{SK}$ and given by
\begin{align*}
\begin{cases}
1 - H_b(p \ast \beta_0), & \text{if } R_p \leq H(X | Y), \\
1 - H_b(p), & \text{if } R_p \geq H(X | Y).
\end{cases}
\end{align*}

Moreover, $C_{SK}$ is achievable by a polar coding scheme.

The proofs for Example 1 and Example 2 are similar to the ones for Theorem 1 and Theorem 2 respectively, and are thus omitted.

ACKNOWLEDGEMENTS

The authors would like to thank Eren Şaşoğlu and Alexander Vardy for sharing their preprint [14].

REMARK ABOUT [24]

During the preparation of the current paper, a related article [24] was posted to arXiv. In [24], the authors provide another solution to the problem studied in Section III. The major difference between their approach and ours is that their construction is sequential, i.e. it successively deals with reliability and secrecy by means of reconciliation and privacy amplification, whereas our approach jointly deals with reliability and secrecy. Consequently, the construction in [24] Theorem 7] has the advantage of not requiring a seed, and to generalize to non-degraded sources, within the limits described in [24] Section III.B]. On the other hand, our protocol requires only one “polarization layer” which code construction is efficient, whereas the sequential approach of [24] requires an inner and an outer layer, the latter having no efficient code construction at the moment, see [24, Section III.C].

REFERENCES

[1] U. Maurer, “Secret Key Agreement by Public Discussion from Common Information,” IEEE Trans. Inf. Theory, vol. 39, pp. 733–742, 1993.
[2] R. Ahlswede and I. Csiszár, “Common Randomness in Information Theory and Cryptography Part I: Secret Sharing,” IEEE Trans. Inf. Theory, vol. 39, pp. 1121–1132, 1993.
[3] 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, 2000.
[4] ——, “Secrecy Capacities for Multiple Terminals.” IEEE Trans. Inf. Theory, vol. 50, no. 12, pp. 3047–3061, 2004.
[5] ——, “Secrecy Capacities for Multiterminal Channel Models,” IEEE Trans. Inf. Theory, vol. 54, no. 6, pp. 2437–2452, 2008.
[6] U. Maurer and S. Wolf, “Information-Theoretic Key Agreement: From Weak to Strong Secrecy for Free,” in Lecture Notes in Computer Science. Springer-Verlag, 2000, pp. 351–368.
[7] M. Bloch and J. Barros, Physical-Layer Security: from Information Theory to Security Engineering. Cambridge University Press, 2011.
[8] R. Chou and M. Bloch, “Separation of Reliability and Secrecy in Rate-Limited Secret Key-Distillation,” arXiv preprint arXiv:1210.4482, 2012.
[9] E. Arikan, “Channel Polarization: A Method for Constructing Capacity-Achieving Codes for Symmetric Binary-Input Memoryless Channels,” IEEE Trans. Inf. Theory, vol. 55, no. 7, pp. 3051–3073, 2009.
[10] E. Hof and S. Shamai, “Secrecy-Achieving Polar-Coding,” in IEEE Trans. Inf. Theory Workshop, 2010, pp. 1–5.
[11] O. Koyluoglu and H. El Gamal, “Polar Coding for Secure Transmission and Key Agreement,” in IEEE Int. Symp. on Personal Indoor and Mobile Radio Communications, 2010, pp. 2698–2703.
[12] M. Andersson, V. Rathi, R. Thobaben, J. Kliewer, and M. Skoglund, “Nested Polar Codes for Wiretap and Relay Channels,” IEEE Communications Letters, vol. 14, no. 8, pp. 752–754, 2010.
[13] H. Mahdavifar and A. Vardy, “Achieving the Secrecy Capacity of Wiretap Channels using Polar Codes,” IEEE Trans. Inf. Theory, vol. 57, no. 10, pp. 6428–6443, 2011.
[14] E. Şaşoğlu and A. Vardy, “A New Polar Coding Scheme for Strong Security on Wiretap Channels,” submitted to IEEE Int. Symp. Inf. Theory, 2013.
[15] C. Bennett, G. Brassard, and U. Maurer, “Generalized Privacy Amplification,” IEEE Trans. Inf. Theory, vol. 41, pp. 1915–1923, 1995.

[16] M. N. Wegman and J. Carter, “New Hash Functions and their Use in Authentication and Set Equality,” Journal of Computer and System Sciences, vol. 22, no. 3, pp. 265 – 279, 1981.

[17] E. Abbe, “Low Complexity Constructions of Secret Keys Using Polar Coding,” presented at IEEE Inf. Theory Workshop, 2012.

[18] E. Arikan, “Source polarization,” in IEEE Int. Symp. Inf. Theory, 2010, pp. 899–903.

[19] S. B. Korada and R. L. Urbanke, “Polar Codes are Optimal for Lossy SourceCoding,” IEEE Trans. Inf. Theory, vol. 56, no. 4, pp. 1751–1768, 2010.

[20] M. Hayashi, “Second-Order Asymptotics in Fixed-Length Source Coding and Intrinsic Randomness,” IEEE Trans. Inf. Theory, vol. 54, no. 10, pp. 4619–4637, 2008.

[21] Y. Dodis, “On Extractors, Error-Correction and Hiding All Partial Information,” in IEEE Inf. Theory Workshop, 2005.

[22] R. Chou and M. Bloch, “Data Compression with Nearly Uniform Output,” accepted to IEEE Int. Symp. Inf. Theory, 2013.

[23] M. Bloch, L. Luzzi, and J. Kliewer, “Strong Coordination with Polar Codes,” in Proc. of the Annual Allerton Conf. on Communication Control and Computing, 2012.

[24] D. Sutter, J. M. Renes, and R. Renner, “Efficient One-Way Secret-Key Agreement and Private Channel Coding via Polarization,” ArXiv e-prints, Apr. 2013.