Efficient One-Way Secret-Key Agreement and Private Channel Coding via Polarization

Joseph M. Renes, Renato Renner, and David Sutter

Institute for Theoretical Phyiscs,
ETH Zurich, Switzerland
{renes,renner,suttedav}@phys.ethz.ch

Abstract. We introduce explicit schemes based on the polarization phenomenon for the task of secret-key agreement from common information and one-way public communication as well as for the task of private channel coding. Our protocols are distinct from previously known schemes in that they combine two practically relevant properties: they achieve the ultimate rate—defined with respect to a strong secrecy condition—and their complexity is essentially linear in the blocklength. However, we are not able to give an efficient algorithm for code construction.

Keywords: One-way secret-key agreement, private channel coding, one-way secret-key rate, secrecy capacity, wiretap channel scenario, more capable, less noisy, degraded, polarization phenomenon, polar codes, practically efficient, strongly secure.

1 Introduction

Consider two parties, Alice and Bob, connected by an authentic but otherwise fully insecure communication channel. It has been shown that without having access to additional resources, it is impossible for them to communicate privately, with respect to an information-theoretic privacy condition [1,2]. In particular they are unable to generate an unconditionally secure key with which to encrypt messages transmitted over the public channel. However, if Alice and Bob have access to correlated randomness about which an adversary (Eve) has only partial knowledge, the situation changes completely: information-theoretically secure secret-key agreement and private communication become possible. Alternatively, if Alice and Bob are connected by a noisy discrete memoryless channel (DMC) to which Eve has only limited access—the so-called *wiretap channel scenario* of Wyner [3], Csiszár and Körner [4], and Maurer [2]—private communication is again possible.

In this paper, we present explicit schemes for efficient one-way secret-key agreement from common randomness and for private channel coding in the wiretap channel scenario. As discussed in Section 2.5, we improve previous work that requires extra assumptions about the structure of the wiretap channel or/and do not achieve strong secrecy. Our schemes are based on *polar codes*, a family of capacity-achieving linear codes, introduced by Arıkan [5], that can be encoded

K. Sako and P. Sarkar (Eds.) ASIACRYPT 2013 Part I, LNCS 8269, pp. 194–213, 2013.

and decoded efficiently. Previous work in a quantum setup [6] already implies that *practically efficient* one-way secret-key agreement and private channel coding in a classical setup is possible, where a practically efficient scheme is one whose computational complexity is essentially linear in the blocklength. The aim of this paper is to explain the schemes in detail and give a purely classical proof that the schemes are reliable, secure, practically efficient and achieve optimal rates.

This paper is structured as follows. Section 2 introduces the problems of performing *one-way secret-key agreement* and *private channel coding*. We summarize known and new results about the optimal rates for these two problems for different wiretap channel scenarios. In Section 3, we explain how to obtain one-way secret-key agreement that is practically efficient, strongly secure, reliable, and achieves the one-way secret-key rate. However, we are not able to give an efficient algorithm for code construction, as discussed in Section 3.3. Section 4 introduces a similar scheme that can be used for strongly secure private channel coding at the secrecy capacity. Finally we conclude in Section 5 and state an open problem that is of interest in the setup of this paper as well as in the quantum mechanical scenario introduced in [6].

2 Background and Contributions

2.1 Notation and Definitions

Let $[k] = \{1, \ldots, k\}$ for $k \in \mathbb{Z}^+$. For $x \in \mathbb{Z}_2^k$ and $\mathcal{I} \subseteq [k]$ we have $x[\mathcal{I}] = [x_i : i \in \mathcal{I}]$, $x^i = [x_1, \ldots, x_i]$ and $x_j^i = [x_j, \ldots, x_i]$ for $j \leqslant i$. The set $\mathcal{A}^{\mathsf{c}}$ denotes the complement of the set $\mathcal{A}$. The uniform distribution on an arbitrary random variable X is denoted by $\overline{P}_X$. For distributions P and Q over the same alphabet $\mathcal{X}$, the variational distance is defined by $\delta(P,Q) := \frac{1}{2}\sum_{x\in\mathcal{X}} |P(x) - Q(x)|$. Let X and Y be two (possibly correlated) random variables. We use standard information theoretic notation, such as $H(X)$ for the (Shannon) entropy of X, $H(X,Y)$ for the joint entropy of (X,Y), $H(X|Y)$ for the conditional entropy of X given Y, and $I(X;Y)$ for the mutual information between X and Y.[1] The notation $X - \circ - Y - \circ - Z$ means that the random variables X, Y, Z form a Markov chain in the given order.

In this setup we consider a discrete memoryless wiretap channel (DM-WTC) $\mathsf{W} : \mathcal{X} \to \mathcal{Y} \times \mathcal{Z}$, which is characterized by its transition probability distribution $P_{Y,Z|X}$.[2] We assume that the variable X belongs to Alice, Y to Bob and Z to Eve.

According to Körner and Marton [8], a DM-WTC $\mathsf{W} : \mathcal{X} \to \mathcal{Y} \times \mathcal{Z}$ is termed *more capable* if $I(X;Y) \geqslant I(X;Z)$ for every possible distribution on X. The

[1] These quantities are properly defined in [7].

[2] Recall that a *discrete channel* is defined as a system consisting of an input alphabet (here $\mathcal{X}$), an output alphabet (here $\mathcal{Y} \times \mathcal{Z}$) and a transition probability distribution (here $P_{Y,Z|X}$) between the input and the output. A channel is said to be *memoryless* if the probability distribution of the output depends only on the input at that time and is conditionally independent of previous channel inputs or outputs.

channel W is termed *less noisy* if $I(U;Y) \geqslant I(U;Z)$ for every possible distribution on (U,X) where U has finite support and $U \multimap X \multimap (Y,Z)$ form a Markov chain. If $X \multimap Y \multimap Z$ form a Markov chain, W is called *degraded*.[3] It has been shown [8] that being more capable is a strictly weaker condition than being less noisy, which is a strictly weaker condition than being degraded. Hence, having a DM-WTC W which is degraded implies that W is less noisy, which again implies that W is also more capable.

2.2 Polarization Phenomenon

Let X^N be a vector whose entries are i.i.d. Bernoulli(p) distributed for $p \in [0,1]$ and $N = 2^n$ where $n \in \mathbb{Z}^+$. Then define $U^N = G_N X^N$, where G_N denotes the polarization (or polar) transform which can be represented by the matrix

$$G_N := \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^{\otimes \log N}, \tag{1}$$

where $A^{\otimes k}$ denotes the kth Kronecker power of an arbitrary matrix A. Note that it turns out that G_N is its own inverse. Furthermore, let $Y^N = \mathsf{W}^N X^N$, where W^N denotes N independent uses of a DMC $\mathsf{W} : \mathcal{X} \to \mathcal{Y}$. For $\epsilon \in (0,1)$ we may define the two sets

$$\mathcal{R}_\epsilon^N(X|Y) := \left\{ i \in [N] : H\left(U_i \middle| U^{i-1}, Y^N\right) \geqslant 1-\epsilon \right\} \quad \text{and} \tag{2}$$

$$\mathcal{D}_\epsilon^N(X|Y) := \left\{ i \in [N] : H\left(U_i \middle| U^{i-1}, Y^N\right) \leqslant \epsilon \right\}. \tag{3}$$

The former consists of outputs U_j which are essentially uniformly random, even given all previous outputs U^{j-1} as well as Y^N, while the latter set consists of the essentially deterministic outputs. The polarization phenomenon is that essentially all outputs are in one of these two subsets, and their sizes are given by the conditional entropy of the input X given Y.

Theorem 1 (Polarization Phenomenon [5,9]). *For any* $\epsilon \in (0,1)$

$$\left|\mathcal{R}_\epsilon^N(X|Y)\right| = NH(X|Y) - o(N) \quad \text{and} \tag{4}$$

$$\left|\mathcal{D}_\epsilon^N(X|Y)\right| = N\left(1 - H(X|Y)\right) - o(N). \tag{5}$$

Based on this theorem it is possible to construct a family of linear error correcting codes, called *polar codes*. The logical bits are encoded into the U_i for $i \in \mathcal{D}_\epsilon^N(X|Y)$, whereas the inputs to U_i for $i \in \mathcal{D}_\epsilon^N(X|Y)^{\mathsf{c}}$ are fixed.[4] It has been shown that polar codes have several desirable attributes [5,10,11,12]: they provably achieve the capacity of any DMC; they have an encoding and decoding

[3] To call a DM-WTC $\mathsf{W} : \mathcal{X} \to \mathcal{Y} \times \mathcal{Z}$ more capable is an abbreviation meaning that the main channel $\mathsf{W}_1 : \mathcal{X} \to \mathcal{Y}$ is more capable than the eavesdropping channel $\mathsf{W}_2 : \mathcal{X} \to \mathcal{Z}$. The same convention is used for less noisy and degraded DM-WTCs.

[4] These are the so-called *frozen bits*.

complexity that is essentially linear in the blocklength N; the error probability decays exponentially in the square root of the blocklength.

Non-binary random variables can be represented by a sequence of correlated binary random variables, which are then encoded separately. Correlated sequences of binary random variables may be polarized using a multilevel construction, as shown in [10].[5] Given M i.i.d. instances of a sequence $X = (X_{(1)}, X_{(2)}, \ldots, X_{(K)})$ and possibly a correlated random variable Y, the basic idea is to first polarize $X_{(1)}^M$ relative to Y^M, then treat $X_{(1)}^M Y^M$ as side information in polarizing $X_{(2)}^M$, and so on. More precisely, defining $U_{(j)}^M = G_M X_{(j)}^M$ for $j = 1, \ldots, K$, we may define the random and deterministic sets for each j as

$$\begin{aligned}
&\mathcal{R}_{\epsilon,(j)}^M(X_{(j)}|X_{(j-1)}, \cdots, X_{(1)}, Y) \\
&\quad = \{i \in [M] : H\Big(U_{(j),i}\Big|U_{(j)}^{i-1}, X_{(j-1)}^M, \cdots, X_{(1)}^M, Y^M\Big) \geqslant 1-\epsilon\}, \quad \text{and} \quad (6) \\
&\mathcal{D}_{\epsilon,(j)}^M(X_{(j)}|X_{(j-1)}, \cdots, X_{(1)}, Y) \\
&\quad = \{i \in [M] : H\Big(U_{(j),i}\Big|U_{(j)}^{i-1}, X_{(j-1)}^M, \cdots, X_{(1)}^M, Y^M\Big) \leqslant \epsilon\}. \quad (7)
\end{aligned}$$

In principle we could choose different ϵ parameters for each j, but this will not be necessary here. Now, Theorem 1 applies to the random and deterministic sets for every j. The sets $\mathcal{R}_\epsilon^M(X|Y) = \{\mathcal{R}_{\epsilon,(j)}^M(X_{(j)}|X_{(j-1)}, \ldots, X_{(1)}, Y)\}_{j=1}^K$ and $\mathcal{D}_\epsilon^M(X|Y) = \{\mathcal{D}_{\epsilon,(j)}^M(X_{(j)}|X_{(j-1)}, \ldots, X_{(1)}, Y)\}_{j=1}^K$ have sizes given by

$$\begin{aligned}
|\mathcal{R}_\epsilon^M(X|Y)| &= \sum_{j=1}^K \Big|\mathcal{R}_{\epsilon,(j)}^M(X_{(j)}|X_{(j-1)}, \ldots, X_{(1)}, Y)\Big| && (8) \\
&= \sum_{j=1}^K MH\big(X_{(j)}\big|X_{(1)}, \ldots, X_{(j-1)}, Y\big) - o(M) && (9) \\
&= MH(X|Y) - o(KM), && (10)
\end{aligned}$$

and

$$\begin{aligned}
|\mathcal{D}_\epsilon^M(X|Y)| &= \sum_{j=1}^K \Big|\mathcal{D}_{\epsilon,(j)}^M(X_{(j)}|X_{(j-1)}, \ldots, X_{(1)}, Y)\Big| && (11) \\
&= \sum_{j=1}^K M\left(1 - H\big(X_{(j)}\big|X_{(1)}, \ldots, X_{(j-1)}, Y\big)\right) - o(M) && (12) \\
&= M\left(K - H(X|Y)\right) - o(KM). && (13)
\end{aligned}$$

In the following we will make use of both the polarization phenomenon in its original form, Theorem 1, and the multilevel extension. To simplify the presentation, we denote by $\tilde{G}_M^K$ the K parallel applications of G_M to the K random variables $X_{(j)}^M$.

[5] An alternative approach is given in [13,14], where the polarization phenomenon has been generalized for arbitrary finite fields. We will however focus on the multilevel construction in this paper.

2.3 One-Way Secret-Key Agreement

At the start of the one-way secret-key agreement protocol, Alice, Bob, and Eve share $N = 2^n$, $n \in \mathbb{Z}^+$ i.i.d. copies (X^N, Y^N, Z^N) of a triple of correlated random variables (X, Y, Z) which take values in discrete but otherwise arbitrary alphabets $\mathcal{X}$, $\mathcal{Y}$, $\mathcal{Z}$.[6]

Alice starts the protocol by performing an operation $\tau_A : \mathcal{X}^N \to (\mathcal{S}^J, \mathcal{C})$ on X^N which outputs both her secret key $S_A^J \in \mathcal{S}^J$ and an additional random variable $C \in \mathcal{C}$ which she transmits to Bob over an public but noiseless public channel. Bob then performs an operation $\tau_B : (\mathcal{Y}^N, \mathcal{C}) \to \mathcal{S}^J$ on Y^N and the information C he received from Alice to obtain a vector $S_B^J \in \mathcal{S}^J$; his secret key. The secret-key thus produced should be reliable, i.e., satisfy the

$$\text{reliability condition:} \quad \lim_{N\to\infty} \Pr\left[S_A^J \neq S_B^J\right] = 0, \tag{14}$$

and secure, i.e., satisfy the

$$\text{(strong) secrecy condition:} \quad \lim_{N\to\infty} \left\| P_{S_A^J, Z^N, C} - \overline{P}_{S_A^J} \times P_{Z^N, C} \right\|_1 = 0, \tag{15}$$

where $\overline{P}_{S_A^J}$ denotes the uniform distribution on random variable S_A^J.

Historically, secrecy was first characterized by a (weak) secrecy condition of the form

$$\lim_{N\to\infty} \frac{1}{N} I\left(S_A^J; Z^N, C\right) = 0. \tag{16}$$

Maurer and Wolf showed that (16) is not a sufficient secrecy criterion [15,16] and introduced the strong secrecy condition

$$\lim_{N\to\infty} I\left(S_A^J; Z^N, C\right) = 0, \tag{17}$$

where in addition it is required that the key is uniformly distributed, i.e.,

$$\lim_{N\to\infty} \delta\left(P_{S_A^J}, \overline{P}_{S_A^J}\right) = 0. \tag{18}$$

In recent years, the strong secrecy condition (17), (18) has often been replaced by (15), since (half) the L_1 distance directly bounds the probability of distinguishing the actual key produced by the protocol with an ideal key. This operational interpretation is particularly helpful in the finite blocklength regime. In the limit $N \to \infty$, the two secrecy conditions (15) and (17) are equivalent, which can be shown using Pinskser's and Fano's inequalities.

Since having weak secrecy is not sufficient, we will only consider strong secrecy in this paper. It has been proven that each secret-key agreement protocol which achieves weak secrecy can be transformed into a strongly secure protocol [16]. However, it is not clear whether the resulting protocol is guaranteed to be practically efficient.

[6] The correlation of the random variables (X, Y, Z) is described by their joint probability distribution $P_{X,Y,Z}$.

For *one-way* communication, Csiszár and Körner [4] and later Ahlswede and Csiszár [17] showed that the optimal rate $R := \lim_{N\to\infty} \frac{J}{N}$ of generating a secret key satisfying (14) and (17), called the *secret-key rate* $S_{\rightarrow}(X;Y|Z)$, is characterized by a closed single-letter formula.

Theorem 2 (One-Way Secret-Key Rate [4,17]). *For triples (X,Y,Z) described by $P_{X,Y,Z}$ as explained above,*

$$S_{\rightarrow}(X;Y|Z) = \begin{cases} \max\limits_{P_{U,V}} H(U|Z,V) - H(U|Y,V) \\ \text{s.t. } V - \circ - U - \circ - X - \circ - (Y,Z), \\ \quad |\mathcal{V}| \leqslant |\mathcal{X}|,\ |\mathcal{U}| \leqslant |\mathcal{X}|^2. \end{cases} \tag{19}$$

The expression for the one-way secret-key rate given in Theorem 2 can be simplified if one makes additional assumptions about $P_{X,Y,Z}$.

Corollary 3. *For $P_{X,Y,Z}$ such that the induced DM-WTC W described by $P_{Y,Z|X}$ is more capable,*

$$S_{\rightarrow}(X;Y|Z) = \begin{cases} \max\limits_{P_V} H(X|Z,V) - H(X|Y,V) \\ \text{s.t. } V - \circ - X - \circ - (Y,Z), \\ \quad |\mathcal{V}| \leqslant |\mathcal{X}|. \end{cases} \tag{20}$$

Proof. In terms of the mutual information, we have

$$\begin{aligned} &H(U|Z,V) - H(U|Y,V) \\ &\quad = I(U;Y|V) - I(U;Z|V) && (21)\\ &\quad = I(X,U;Y|V) - I(X,U;Z|V) - (I(X;Y|U,V) - I(X;Z|U,V)) && (22)\\ &\quad \leqslant I(X,U;Y|V) - I(X,U;Z|V) && (23)\\ &\quad = I(X;Y|V) - I(X;Z|V), && (24) \end{aligned}$$

using the chain rule, the more capable condition, and the Markov chain properties, respectively. Thus, the maximum in $S_{\rightarrow}(X;Y|Z)$ can be achieved when omitting U. □

Corollary 4. *For $P_{X,Y,Z}$ such that the induced DM-WTC W described by $P_{Y,Z|X}$ is less noisy,*

$$S_{\rightarrow}(X;Y|Z) = H(X|Z) - H(X|Y). \tag{25}$$

Proof. Since W being less noisy implies W being more capable, we know that the one-way secret key rate is given by (20). Using the chain rule we obtain

$$\begin{aligned} &H(X|Z,V) - H(X|Y,V) \\ &\quad = I(X;Y|V) - I(X;Z|V) && (26)\\ &\quad = I(X,V;Y) - I(X,V;Z) - I(V;Y) + I(V;Z) && (27)\\ &\quad = I(X;Y) - I(X;Z) - (I(V;Y) - I(V;Z)) && (28)\\ &\quad \leqslant I(X;Y) - I(X;Z). && (29) \end{aligned}$$

Equation (28) follows from the chain rule and the Markov chain condition. The inequality uses the assumption of being less noisy. □

Note that (25) is also equal to the one-way secret-key rate for the case where W is degraded, as this implies W being less noisy. The proof of Theorem 2 does not imply that there exists an *efficient* one-way secret-key agreement protocol. A computationally efficient scheme was constructed in [18], but is not known to be practically efficient.[7]

For key agreement with two-way communication, no formula comparable to (19) for the optimal rate is known. However, it has been shown that the two-way secret-key rate is strictly larger than the one-way secret-key rate. It is also known that the *intrinsic information* $I(X;Y\downarrow Z) := \min_{P_{Z'|Z}} I(X;Y|Z')$ is an upper bound on $S(X;Y|Z)$, but is not tight [17,19,20].

2.4 Private Channel Coding

Private channel coding over a wiretap channel is closely related to the task of one-way secret-key agreement from common randomness (cf. Section 2.5). Here Alice would like to transmit a message $M^J \in \mathcal{M}^J$ privately to Bob. The messages can be distributed according to some arbitrary distribution P_{M^J}. To do so, she first encodes the message by computing $X^N = \mathrm{enc}(M^J)$ for some encoding function $\mathrm{enc} : \mathcal{M}^J \to \mathcal{X}^N$ and then sends X^N over the wiretap channel to Bob (and to Eve), which is represented by $(Y^N, Z^N) = \mathsf{W}^N X^N$. Bob next decodes the received message to obtain a guess for Alice's message $\hat{M}^J = \mathrm{dec}(Y^N)$ for some decoding function $\mathrm{dec} : \mathcal{Y}^N \to \mathcal{M}^J$. As in secret-key agreement, the private channel coding scheme should be reliable, i.e., satisfy the

$$\text{reliability condition:} \quad \lim_{J\to\infty} \Pr\left[M^J \neq \hat{M}^J\right] = 0, \quad \text{for all} \quad M^J \in \mathcal{M}^J \tag{30}$$

and (strongly) secure, i.e., satisfy the

$$\text{(strong) secrecy condition:} \quad \lim_{J\to\infty} \left\| P_{M^J,Z^N,C} - P_{M^J} \times P_{Z^N,C} \right\|_1 = 0. \tag{31}$$

The variable C denotes any additional information made public by the protocol.

As mentioned in Section 2.3, in the limit $J \to \infty$ this strong secrecy condition is equivalent to the historically older (strong) secrecy condition

$$\lim_{J\to\infty} I\big(M^J; Z^N, C\big) = 0. \tag{32}$$

The highest achievable rate $R := \lim_{N\to\infty} \frac{J}{N}$ fulfilling (30) and (31) is called the *secrecy capacity*.

Csiszár and Körner showed [4, Corollary 2] that there exists a single-letter formula for the secrecy capacity.[8]

[7] As defined in Section 1, we call a scheme practically efficient if its computational complexity is essentially linear in the blocklength.

[8] Maurer and Wolf showed that the single-letter formula remains valid considering strong secrecy [16].

Theorem 5 (Secrecy Capacity [4]). *For an arbitrary DM WTC* W *as introduced above,*

$$C_s = \begin{cases} \max\limits_{P_{V,X}} H(V|Z) - H(V|Y) \\ \text{s.t. } V \multimap X \multimap (Y,Z), \\ \quad |\mathcal{V}| \leqslant |\mathcal{X}|. \end{cases} \tag{33}$$

This expression can be simplified using additional assumptions about W.

Corollary 6 ([8]). *If* W *is more capable,*

$$C_s = \max_{P_X} H(X|Z) - H(X|Y)\,. \tag{34}$$

Proof. A proof can be found in [8] or [21, Section 22.1]. □

2.5 Previous Work and Our Contributions

In Section 3, we present a one-way secret-key agreement scheme based on polar codes that achieves the secret-key rate, is strongly secure, reliable and whose implementation is practically efficient, with complexity $O(N \log N)$ for blocklength N. Our protocol improves previous efficient secret-key constructions [22], where only weak secrecy could be proven and where the eavesdropper has no prior knowledge and/or degradability assumptions are required. Our protocol also improves a very recent efficient secret-key construction [23], which requires to have a small amount of shared key between Alice and Bob and only works for binary *degraded* (symmetric) discrete memoryless sources. However, we note that a possible drawback of our scheme compared to [23] is that its code construction may be more difficult.

In Section 4, we introduce a coding scheme based on polar codes that provably achieves the secrecy capacity for arbitrary discrete memoryless wiretap channels. We show that the complexity of the encoding and decoding operations is $O(N \log N)$ for blocklength N. Our scheme improves previous work on practically efficient private channel coding at the optimal rate [24], where only weak secrecy could be proven under the additional assumption that the channel W is degraded.[9] Recently, Bellare *et al.* introduced a polynomial-time coding scheme that is strongly secure and achieves the secrecy capacity for binary symmetric wiretap channels [25].[10] Several other constructions of private channel coding schemes have been reported [26,27,28], but all achieve only weak secrecy. Very recently, Şaşoğlu and Vardy introduced a new polar coding scheme that

[9] Note that Mahdavifar and Vardy showed that their scheme achieves strong secrecy if the channel to Eve (induced from W) is noiseless. Otherwise their scheme is not provably reliable [24].

[10] They claim that their scheme works for a large class of wiretap channels. However, this class has not been characterized precisely so far. It is therefore not clear whether their scheme requires for example degradability assumptions. Note that to obtain strong secrecy for an arbitrarily distributed message, it is required that the wiretap channel is symmetric [25, Lemma 14].

can be used for private channel coding being strongly secure [29]. However, it still requires the assumption of having a degraded wiretap channel which we do not need for our scheme. In [30], an explicit construction that achieves the secrecy capacity for wiretap channel coding is introduced, but efficiency is not considered.

The tasks of one-way secret-key agreement and private channel coding explained in the previous two subsections are closely related. Maurer showed how a one-way secret-key agreement can be derived from a private channel coding scenario [2]. More precisely, he showed how to obtain the common randomness needed for one-way secret-key agreement by constructing a "virtual" degraded wiretap channel from Alice to Bob. This approach can be used to obtain the one-way secret-key rate from the secrecy capacity result in the wiretap channel scenario [21, Section 22.4.3]. One of the main advantages of the two schemes introduced in this paper is that they are both practically efficient. However, even given a practically efficient private coding scheme, it is not known that Maurer's construction will yield a practically efficient scheme for secret key agreement. For this reason, as well as simplicity of presentation, we treat the one-way secret-key agreement and the private channel coding problem separately in the two sections to follow.

3 One-Way Secret-Key Agreement Scheme

Our key agreement protocol is a concatenation of two subprotocols, an inner and an outer layer, as depicted in Figure 1. The protocol operates on blocks of N i.i.d. triples (X, Y, Z), which are divided into M sub-blocks of size L for input to the inner layer. At the outer layer, we use the multi-level construction introduced in Section 2.2. In the following we assume $\mathcal{X} = \{0, 1\}$, which however is only for convenience; the techniques of [10] and [31] can be used to generalize the schemes to arbitrary alphabets $\mathcal{X}$.

The task of the inner layer is to perform *information reconciliation* and that of the outer layer is to perform *privacy amplification*. Information reconciliation refers to the process of carrying out error correction to ensure that Alice and Bob obtain a shared bit string, and here we only allow communication from Alice to Bob for this purpose. On the other hand, privacy amplification refers to the process of distilling from Alice's and Bob's shared bit string a smaller set of bits whose correlation with the information available to Eve is below a desired threshold.

Each subprotocol in our scheme is based on the polarization phenomenon. For information reconciliation of Alice's random variable X^L relative to Bob's information Y^L, Alice applies a polar transformation to X^L and forwards the bits of the complement of the deterministic set $\mathcal{D}^L_{\epsilon_1}(X|Y)$ to Bob over a public channel, which enables him to recover X^L using the standard polar decoder [5]. Her remaining information is then fed into a multilevel polar transformation and the bits of the random set are kept as the secret key.

Let us now define the protocol more precisely. For $L = 2^\ell$, $\ell \in \mathbb{Z}^+$, let $V^L = G_L X^L$ where G_L is as defined in (1). For $\epsilon_1 > 0$, we define

$$\mathcal{E}_K := \mathcal{D}^L_{\epsilon_1}(X|Y), \tag{35}$$

with $K := |\mathcal{D}^L_{\epsilon_1}(X|Y)|$. Then, let $T_{(j)} = V^L[\mathcal{E}_K]_j$ for $j = 1, \ldots, K$ and $C_{(j)} = V^L[\mathcal{E}_K^c]_j$ for $j = 1, \ldots, L-K$ so that $T = (T_{(1)}, \ldots, T_{(K)})$ and $C = (C_{(1)}, \ldots, C_{(L-K)})$. For $\epsilon_2 > 0$ and $U^M_{(j)} = G_M T^M_{(j)}$ for $j = 1, \ldots K$ (or, more briefly, $U^M = \tilde{G}^K_M T^M$), we define

$$\mathcal{F}_J := \mathcal{R}^M_{\epsilon_2}(T|CZ^L), \tag{36}$$

with $J := |R^M_{\epsilon_2}(T|CZ^L)|$.

Protocol 1: One-way secret-key agreement

Given: Index sets $\mathcal{E}_K$ and $\mathcal{F}_J$ (code construction)
Notation: Alice's input: $x^N \in \mathbb{Z}_2^N$ (a realization of X^N)
Bob's / Eve's input: (y^N, z^N) (realizations of Y^N and Z^N)
Alice's output: s_A^J
Bob's output: s_B^J

Step 1: Alice computes $v_{i+1}^{i+L} = G_L x_{i+1}^{i+L}$ for all $i \in \{0, L, 2L, \ldots, (M-1)L\}$.
Step 2: Alice computes $t_i = v_{i+1}^{i+L}[\mathcal{E}_K]$ for all $i \in \{0, L, 2L, \ldots, (M-1)L\}$.
Step 3: Alice sends $c_i = v_{i+1}^{i+L}[\mathcal{E}_K^c]$ for all $i \in \{0, L, 2L, \ldots, (M-1)L\}$ over a public channel to Bob.
Step 4: Alice computes $u^M = \tilde{G}^K_M t^M$ and obtains $s_A^J = u^M[\mathcal{F}_J]$.[11]
Step 5: Bob applies the standard polar decoder [5,12] to (c_i, y_{i+1}^{i+L}) to obtain $\hat{v}_{i+1}^{i+L}$ and $\hat{t}_i = \hat{v}_{i+1}^{i+L}[\mathcal{E}_K]$, for $i \in \{0, L, 2L, \ldots, (M-1)L\}$.
Step 6: Bob computes $\hat{u}^M = \tilde{G}^K_M t^M$ and obtains $s_B^J = \hat{u}^M[\mathcal{F}_J]$.

3.1 Rate, Reliability, Secrecy, and Efficiency

Theorem 7. *Protocol 1 allows Alice and Bob to generate a secret key S_A^J respecitvely S_B^J using public one-way communication C^M such that for any $\beta < \frac{1}{2}$:*

$$\text{Reliability:} \quad \Pr\left[S_A^J \neq S_B^J\right] = O\left(M 2^{-L^\beta}\right) \tag{37}$$

$$\text{Secrecy:} \quad \left\| P_{S_A^J, Z^N, C} - \overline{P}_{S_A^J} \times P_{Z^N, C} \right\|_1 = O\left(\sqrt{N} 2^{-\frac{N^\beta}{2}}\right) \tag{38}$$

$$\text{Rate:} \quad R := \frac{J}{N} = H(X|Z) - \frac{1}{L} H\left(V^L[\mathcal{E}_K^c] \middle| Z^L\right) - \frac{o(N)}{N}. \tag{39}$$

All operations by both parties can be performed in $O(N \log N)$ steps.

[11] The expression $u^M[\mathcal{F}_J]$ is an abuse of notation, as $\mathcal{F}_J$ is not a subset of [M]. The expression should be understood to be the union of the random bits of $u^M_{(j)}$, for all $j = 1, \ldots, K$, as in the definition of $\mathcal{R}^M_{\epsilon_2}(T|CZ^L)$.

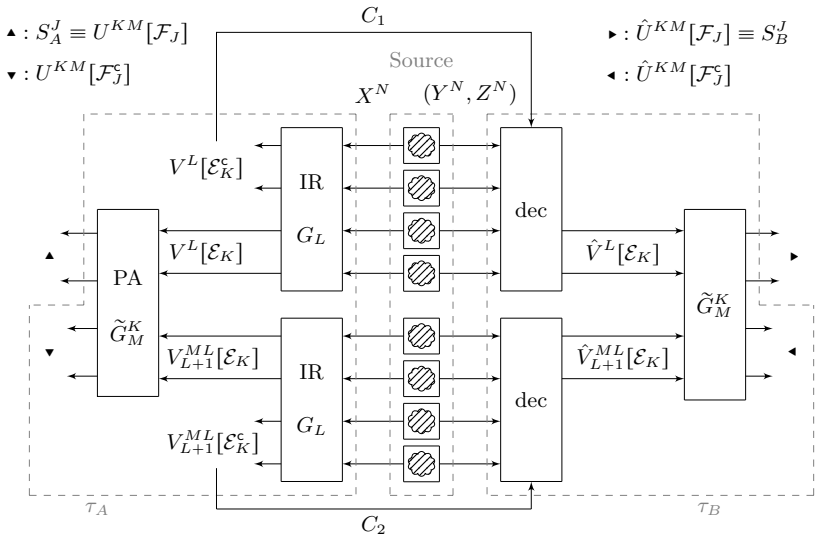

Fig. 1. The secret-key agreement scheme for the setup $N = 8$, $L = 4$, $M = 2$, $K = 2$, and $J = 2$. We consider a source that produces N i.i.d. copies (X^N, Y^N, Z^N) of a triple of correlated random variables (X, Y, Z). Alice performs the operation τ_A, sends $(V^L[\mathcal{E}_K^c])^M$ over a public channel to Bob and obtains S_A^J, her secret key. Bob then performs the operation τ_B which results in his secret key S_B^J.

Proof. The reliability of Alice's and Bob's key follows from the standard polar decoder error probability and the union bound. Each instance of the decoding algorithm employed by Bob has an error probability which scales as $O(2^{-L^\beta})$ for any $\beta < \frac{1}{2}$ [9]; application of the union bound gives the prefactor M. Since G_L as defined in (1) is its own inverse, $\tilde{G}_M^K$ is its own inverse as well.

The rate of the scheme is

$$R = \frac{|\mathcal{F}_J|}{N} \tag{40}$$

$$= \frac{1}{L} H\big(V^L[\mathcal{E}_K] \big| V^L[\mathcal{E}_K^c], Z^L\big) - \frac{o(N)}{N} \tag{41}$$

$$= \frac{1}{L} \left(H\big(V^L \big| Z^L\big) - H\big(V^L[\mathcal{E}_K^c] \big| Z^L\big)\right) - \frac{o(N)}{N} \tag{42}$$

$$= H(X|Z) - \frac{1}{L} H\big(V^L[\mathcal{E}_K^c] \big| Z^L\big) - \frac{o(N)}{N}, \tag{43}$$

where (41) uses the polarization phenomenon stated in Theorem 1.

To prove the secrecy statement requires more effort. Using Pinsker's inequality we obtain

$$\delta\Big(P_{S_A^J,Z^N,C^M},\overline{P}_{S_A^J}\times P_{Z^N,C^M}\Big)\leqslant\sqrt{\tfrac{\ln 2}{2}D\Big(P_{S_A^J,Z^N,C^M}\Big\|\,\overline{P}_{S_A^J}\times P_{Z^N,C^M}\Big)} \tag{44}$$

$$=\sqrt{\tfrac{\ln 2}{2}\left(J-H\big(S_A^J|Z^N,C^M\big)\right)}, \tag{45}$$

where the last step uses the chain rule for relative entropies and that $\overline{P}_{S_A^J}$ denotes the uniform distribution. We can simplify the conditional entropy expression using the chain rule

$$\begin{aligned}
&H\big(S_A^J\big|Z^N,C^M\big)\\
&=H\big(U^M[\mathcal{F}_J]\big|Z^N,(V^L[\mathcal{E}_K^{\mathrm{c}}])^M\big) &(46)\\
&=\sum_{j=1}^{K}H\Big(U_{(j)}^M[\mathcal{F}_{(j)}]\Big|U_{(1)}^M[\mathcal{F}_{(1)}],\ldots,U_{(j-1)}^M[\mathcal{F}_{(j-1)}],Z^N,(V^L[\mathcal{E}_K^{\mathrm{c}}])^M\Big) &(47)\\
&=\sum_{j=1}^{K}\sum_{i=1}^{|\mathcal{F}_{(i)}|}H\left(U_{(j)}^M[\mathcal{F}_{(j)}]_i\middle|U_{(j)}^M[\mathcal{F}_{(j)}]^{i-1},\Big\{U_{(l)}^M[\mathcal{F}_{(l)}]\Big\}_{l=1}^{j-1},Z^N,(V^L[\mathcal{E}_K^{\mathrm{c}}])^M\right) &(48)\\
&\geqslant\sum_{j=1}^{K}\sum_{i\in\mathcal{F}_j}H\Big(U_{(j)i}\Big|U_{(j)}^{i-1},U_{(1)}^M[\mathcal{F}_{(1)}],\ldots,U_{(j-1)}^M[\mathcal{F}_{(j-1)}],Z^N,(V^L[\mathcal{E}_K^{\mathrm{c}}])^M\Big) &(49)\\
&\geqslant J\,(1-\epsilon_2)\,, &(50)
\end{aligned}$$

where the first inequality uses the fact that that conditioning cannot increase the entropy and the second inequality follows by the definition of $\mathcal{F}_J$. Recall that we are using the notation introduced in Section 2.2. For $\mathcal{F}_J$ as defined in (36), we have $\mathcal{F}_J=\big\{\mathcal{F}_{(j)}\big\}_{j=1}^{K}$ where $\mathcal{F}_{(j)}=\mathcal{R}_{\epsilon_2}^M\left(T_{(j)}\,|T_{(j-1)},\ldots,T_{(1)},C,Z^L\right)$. The polarization phenomenon, Theorem 1, implies $J=O(N)$, which together with (45) proves the secrecy statement of Theorem 7, since $\epsilon_2=O(2^{-N^\beta})$ for any $\beta<\frac{1}{2}$.

It remains to show that the computational complexity of the scheme is $O(N\log N)$. Alice performs the operation G_L in the first layer M times, each requiring $O(L\log L)$ steps [5]. In the second layer she performs $\tilde{G}_M^K$, or K parallel instances of G_M, requiring $O(KM\log M)$ total steps. From the polarization phenomenon, we have $K=O(L)$, and thus the complexity of Alice's operations is not worse than $O(N\log N)$. Bob runs M standard polar decoders which can be done in $O(ML\log L)$ complexity [5,12]. Bob next performs the polar transform $\tilde{G}_M^K$, whose complexity is not worse than $O(N\log N)$ as justified above. Thus, the complexity of Bob's operations is also not worse than $O(N\log N)$. □

In principle, the two parameters L and M can be chosen freely. However, to maintain the reliability of the scheme (cf.(37)), M may not grow exponentially fast in L. A reasonable choice would be to have both parameters scale comparably fast, i.e., $\frac{M}{L}=O(1)$.

Corollary 8. *The rate of Protocol 1 given in Theorem 7 can be bounded as*

$$R \geqslant \max\left\{0, H(X|Z) - H(X|Y) - \frac{o(N)}{N}\right\}. \tag{51}$$

Proof. According to (43) the rate of Protocol 1 is

$$R = H(X|Z) - \frac{1}{L}H\big(V^L[\mathcal{E}_K^{\mathsf{c}}]|Z^L\big) - \frac{o(N)}{N} \tag{52}$$

$$\geqslant \max\left\{0, H(X|Z) - \frac{|\mathcal{E}_K^{\mathsf{c}}|}{L} - \frac{o(N)}{N}\right\} \tag{53}$$

$$= \max\left\{0, H(X|Z) - H(X|Y) - \frac{o(N)}{N}\right\}, \tag{54}$$

where (54) uses the polarization phenomenon stated in Theorem 1. □

3.2 Achieving the Secret-Key Rate of a Given Distribution

Theorem 7 together with Corollaries 4 and 8 immediately imply that Protocol 1 achieves the secret-key rate $S_{\rightarrow}(X;Y|Z)$ if $P_{X,Y,Z}$ is such that the induced DM WTP W described by $P_{Y,Z|X}$ is less noisy. If we can solve the optimization problem (19), i.e., find the optimal auxiliary random variables V and U, our one-way secret-key agreement scheme can achieve $S_{\rightarrow}(X;Y|Z)$ for a general setup. We then make V public, replace X by U and run Protocol 1. Note that finding the optimal random variables V and U might be difficult. It has been shown that for certain distributions the optimal random variables V and U can be found analytically [18].

An open problem discussed in Section 5 addresses the question if Protocol 1 can achieve a rate that is strictly larger than $\max\{0, H(X|Z) - H(X|Y)\}$ if nothing about the optimal auxiliary random variables V and U is known, i.e., if we run the protocol directly for X without making V public.

3.3 Code Construction

To construct the code the index sets $\mathcal{E}_K$ and $\mathcal{F}_J$ need to be determined. The set $\mathcal{E}_K$ can be computed approximately with a linear-time algorithm introduced in [32], given the distributions P_X and $P_{Y|X}$. Alternatively, Tal and Vardy's older algorithm [33] and its adaption to the asymmetric setup [12] can be used.

To approximately compute the outer index set $\mathcal{F}_J$ requires more effort. In principle, we can again use the above algorithms, which require a description of the "super-source" seen by the outer layer, i.e., the source which outputs the triple of random variables $(V^L[\mathcal{E}_K], (Y^L, V^L[\mathcal{E}_K^{\mathsf{c}}]), (Z^L, V^L[\mathcal{E}_K^{\mathsf{c}}]))$. However, its alphabet size is exponential in L, and thus such a direct approach will not be efficient in the overall blocklength N. Nonetheless, due to the structure of the inner layer, it is perhaps possible that the method of approximation by limiting the alphabet size [33,32] can be extended to this case. In particular, a recursive construction motivated by the decoding operation introduced in [6] could potentially lead to an efficient computation of the index set $\mathcal{F}_J$.

4 Private Channel Coding Scheme

Our private channel coding scheme is a simple modification of the secret key agreement protocol of the previous section. Again it consists of two layers, an inner layer which ensures transmitted messages can be reliably decoded by the intended receiver, and an outer layer which guarantees privacy from the unintended receiver. The basic idea is to simply run the key agreement scheme in reverse, *inputting* messages to the protocol where secret key bits would be *output* in key agreement. The immediate problem in doing so is that key agreement also produces outputs besides the secret key, so the procedure is not immediately reversible. To overcome this problem, the encoding operations here simulate the random variables output in the key agreement protocol, and then perform the polar transformations $\widetilde{G}_M^K$ and G_L in reverse.[12]

The scheme is visualized in Figure 2 and described in detail in Protocol 2. Not explicitly shown is the simulation of the bits $U^M[\mathcal{F}_J^c]$ at the outer layer and the bits $V^L[\mathcal{E}_K^c]$ at the inner layer. The outer layer, whose simulated bits are nearly deterministic, makes use of the method described in [34, Definition 1], while the inner layer, whose bits are nearly uniformly-distributed, follows [12, Section 4]. Both proceed by successively sampling from the individual bit distributions given all previous values in the particular block, i.e., constructing V_j by sampling from $P_{V_j|V^{j-1}}$. These distributions can be efficiently constructed, as described in Section 4.3.

Note that a public channel is used to communicate the information reconciliation information to Bob, enabling reliable decoding. However, it is possible to dispense with the public channel and still achieve the same rate and efficiency properties, as will be discussed in Section 4.3.

In the following we assume that the message M^J to be transmitted is uniformly distributed over the message set $\mathcal{M} = \{0,1\}^J$. As mentioned in Section 2.4, it may be desirable to have a private coding scheme that works for an arbitrarily distributed message. This can be achieved by assuming that the wiretap channel W is symmetric—more precisely, by assuming that the two channels $\mathsf{W}_1 : \mathcal{X} \to \mathcal{Y}$ and $\mathsf{W}_2 : \mathcal{X} \to \mathcal{Z}$ induced by W are symmetric. We can define a super-channel $\mathsf{W}' : \mathcal{T} \to \mathcal{Y}^L \times \mathcal{Z}^L \times \mathcal{C}$ which consists of an inner encoding block and L basic channels W. The super-channel W' again induces two channels $\mathsf{W}'_1 : \mathcal{T} \to \mathcal{Y}^L \times \mathcal{C}$ and $\mathsf{W}'_2 : \mathcal{T} \to \mathcal{Z}^L \times \mathcal{C}$. Arıkan showed that W_1 respectively W_2 being symmetric implies that W'_1 respectively W'_2 is symmetric [5, Proposition 13]. It has been shown in [24, Proposition 3] that for symmetric channels polar codes remain reliable for an arbitrary distribution of the message bits. We thus conclude that if W_1 is assumed to be symmetric, our coding scheme remains reliable for arbitrarily distributed messages. Assuming having a symmetric channel W_2 implies that W'_2 is symmetric which proves that our scheme is strongly secure for arbitrarily distributed messages.[13]

[12] As it happens, G_L is its own inverse.

[13] This can be seen easily by the strong secrecy condition given in (31) using that W'_2 is symmetric.

Protocol 2: Private channel coding

Given:	Index sets $\mathcal{E}_K$ and $\mathcal{F}_J$ (code construction)[14]
Notation:	Message to be transmitted: m^J
Outer enc.:	Let $u^M[\mathcal{F}_J] = m^J$[15] and $u^M[\mathcal{F}_J^{\mathsf{c}}] = r^{KM-J}$ where r^{KM-J} is (randomly) generated as explained in [34, Definition 1]. Let $t^M = \tilde{G}_M^K u^M$.
Inner enc.:	For all $i \in \{0, L, \ldots, L(M-1)\}$, Alice does the following: let $\bar{v}_{i+1}^{i+L}[\mathcal{E}_K] = t_{(i/L)+1}$ and $\bar{v}_{i+1}^{i+L}[\mathcal{E}_K^{\mathsf{c}}] = s_{i+1}^{i+L-K}$ where s_{i+1}^{i+L-K} is (randomly) generated as explained in [12, Section 4]. Send $C_{(i/K)+1} := s_{i+1}^{i+L-K}$ over a public channel to Bob. Finally, compute $x_{i+1}^{i+L} = G_L \bar{v}_{i+1}^{i+L}$.
Transmis.:	$(y^N, z^N) = \mathsf{W}^N x^N$
Inner dec.:	Bob uses the standard decoder [5,12] with inputs $C_{(i/L)+1}$ and y_{i+1}^{i+L} to obtain $\hat{v}_{i+1}^{i+L}$, and hence $\hat{t}_{(i/L)+1} = \hat{v}_{i+1}^{i+L}[\mathcal{E}_K]$, for each $i \in \{0, L, \ldots, L(M-1)\}$.
Outer dec.:	Bob computes $\hat{u}^M = \tilde{G}_M^K \hat{t}^M$ and outputs a guess for the sent message $\hat{m}^J = \hat{u}^M[\mathcal{F}_J]$.

4.1 Rate, Reliability, Secrecy, and Efficiency

Corollary 9. *For any $\beta < \frac{1}{2}$, Protocol 2 satisfies*

$$\text{Reliability:} \quad \Pr\left[M^J \neq \hat{M}^J\right] = O\left(M 2^{-L^\beta}\right) \tag{55}$$

$$\text{Secrecy:} \quad \left\| P_{M^J, Z^N, C} - \overline{P}_{M^J} \times P_{Z^N, C} \right\|_1 = O\left(\sqrt{N} 2^{-\frac{N^\beta}{2}}\right) \tag{56}$$

$$\text{Rate:} \quad R = H(X|Z) - \frac{1}{L} H\left(V^L[\mathcal{E}_K^{\mathsf{c}}] | Z^L\right) - \frac{o(N)}{N} \tag{57}$$

and its computational complexity is $O(N \log N)$.

Proof. Recall that the idea of the private channel coding scheme is to run Protocol 1 backwards. Since Protocol 2 simulates the nearly deterministic bits $U^M[\mathcal{F}_J]$ at the outer encoder as described in [34, Definition 1] and the almost random bits $V^L[\mathcal{E}_K^{\mathsf{c}}]$ at the inner encoder as explained in [12, Section 4], it follows that for large values of L and M the private channel coding scheme approximates the one-way secret-key scheme setup,[16] i.e., $\lim_{N\to\infty} \delta\left(P_{T^M}, P_{(V^L[\mathcal{E}_K])^M}\right) = 0$ and $\lim_{L\to\infty} \delta\left(P_{X^L}, P_{\hat{X}^L}\right) = 0$, where P_{X^L} denotes the distribution of the vector X^L which is sent over the wiretap channel W and $P_{\hat{X}^L}$ denotes the distribution of Alice's random variable $\hat{X}^L$ in the one-way secret-key agreement setup. We

[14] By the code construction the channel input distribution P_X is defined. P_X should be chosen such that it maximizes the scheme's rate.

[15] Again an abuse of notation. See the Footnote 11 of Protocol 1.

[16] This approximation can be made arbitrarily precise for sufficiently large values of L and M.

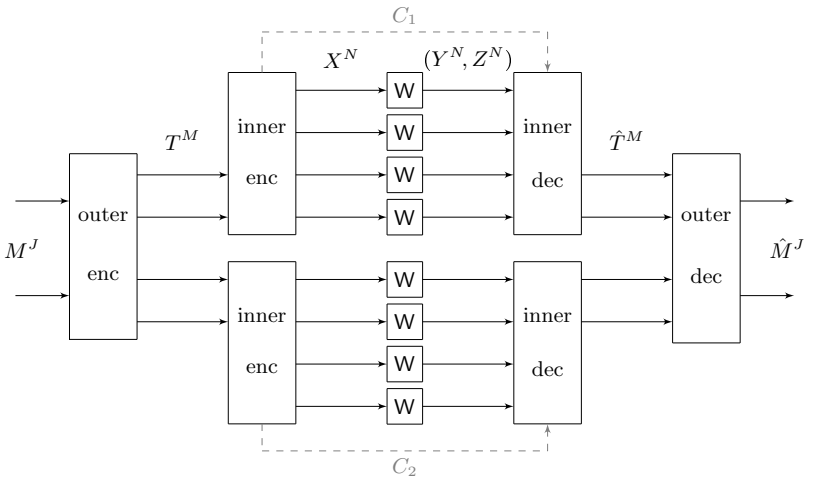

Fig. 2. The private channel coding scheme for the setup $N = 8$, $L = 4$, $M = 2$, $K = 2$, and $J = 2$. The message M^J is first sent through an outer encoder which adds some bits (simulated as explained in [12, Section 4]) and applies the polarization transform $\widetilde{G}_M^K$. The output $T^M = (T_{(1)}, \ldots, T_{(K)})^M$ is then encoded a second time by M independent identical blocks. Note that each block again adds redundancy (as explained in [34, Definition 1]) before applying the polarization transform G_L. Each inner encoding block sends the frozen bits over a public channel to Bob. Note that this extra public communication can be avoided as justified in Section 4.3. The output X^N is then sent over N copies of the wiretap channel W to Bob. Bob then applies a decoding operation as in the key agreement scheme, Section 3.

thus can use the decoder introduced in [9] to decode the inner layer. Since we are using M identical independent inner decoding blocks, by the union bound we obtain the desired reliability condition. The secrecy and rate statement are immediate consequences from Theorem 7. □

As mentioned after Theorem 7, to ensure reliability of the protocol, M may not grow exponentially fast in L.

Corollary 10. *The rate of Protocol 2 given in Corollary 9 can be bounded as*

$$R \geqslant \max\left\{0, H(X|Z) - H(X|Y) - \frac{o(N)}{N}\right\}. \tag{58}$$

Proof. The proof is identical to the proof of Corollary 8. □

4.2 Achieving the Secrecy Capacity of a Wiretap Channel

Corollaries 6 and 10 immediately imply that our private channel coding scheme achieves the secrecy capacity for the setup where W is more capable. If we can find the optimal auxiliary random variable V in (33), Protocol 2 can achieve

the secrecy capacity for a general wiretap channel scenario. We define a super-channel $\overline{\mathsf{W}} : \mathcal{V} \to \mathcal{Y} \times \mathcal{Z}$ which includes the random variable X and the wiretap channel W. The super-channel $\overline{\mathsf{W}}$ is characterized by its transition probability distribution $P_{Y,Z|V}$ where V is the optimal random variable solving (33). The private channel coding scheme is then applied to the super-channel, achieving the secrecy capacity. Note that finding the optimal random variable V might be difficult.

In Section 5, we discuss the question if it is possible that Protocol 2 achieves a rate that is strictly larger than $\max\{0, \max_{P_X} H(X|Z) - H(X|Y)\}$, if nothing about the optimal auxiliary random variable V is known.

4.3 Code Construction and Public Channel Communication

To construct the code the index sets $\mathcal{E}_K$ and $\mathcal{F}_J$ as defined in (35) and (36) need to be computed. This can be done as explained in Section 3.3. One first chooses a distribution P_X that maximizes the scheme's rate given in (57), before looking for a code that defines this distribution P_X.

We next explain how the communication $C^M \in \mathcal{C}^M$ from Alice to Bob can be reduced such that it does not affect the rate, i.e., we show that we can choose $|\mathcal{C}| = o(L)$. Recall that we defined the index set $\mathcal{E}_K := \mathcal{D}^L_{\epsilon_1}(X|Y)$ in (35). Let $\mathcal{G} := \mathcal{R}^L_{\epsilon_1}(X|Y)$ using the noation introduced in (2) and $\mathcal{I} := [L] \backslash (\mathcal{E}_K \cup \mathcal{G}) = \mathcal{E}_K^{\mathrm{c}} \backslash \mathcal{G}$. As explained in Section 2.2, $\mathcal{G}$ consists of the outputs V_j which are essentially uniformly random, even given all previous outputs V^{j-1} as well as Y^L, where $V^L = G_L X^L$. The index set $\mathcal{I}$ consists of the outputs V_j which are neither essentially uniformly random nor essentially deterministic given V^{j-1} and Y^L. The polarization phenomenon stated in Theorem 1 ensures that this set is small, i.e., that $|\mathcal{I}| = o(L)$. Since the bits of $\mathcal{G}$ are almost uniformly distributed, we can fix these bits independently of the message—as part of the code construction—without affecting the reliability of the scheme for large blocklengths.[17] We thus only need to communicate the bits belonging to the index set $\mathcal{I}$.

We can send the bits belonging to $\mathcal{I}$ over a seperate public noiseless channel. Alternatively, we could send them over the wiretap channel W that we are using for private channel coding. However since W is assumed to be noisy and it is essential that the bits in $\mathcal{I}$ are recieved by Bob without any errors, we need to protect them using an error correcting code. To not destroy the essentially linear computational complexity of our scheme, the code needs to have an encoder and decoder that are practically efficient. Since $|\mathcal{I}| = o(L)$, we can use any error correcting code that has a non-vanishing rate. For symmetric binary DMCs, polar coding can be used to transmit reliably an arbitrarily distributed message [24, Proposition 3]. We can therefore symmetrize our wiretap channel W and use polar codes to transmit the bits in $\mathcal{I}$.[18]

[17] Recall that we choose $\epsilon_1 = O\left(2^{-L^\beta}\right)$ for any $\beta < \frac{1}{2}$, such that for $L \to \infty$ the index set $\mathcal{G}$ contains only uniformly distributed bits.

[18] Note that the symmetrization of the channel will reduce its rate which however does not matter as we need a non-vanishing rate only.

As the reliability of the scheme is the average over the possible assignments of the random bits belonging to $\mathcal{I}$ (or even $\mathcal{E}_K^{\mathsf{c}}$), at least one choice must be as good as the average, meaning a reliable, efficient, and deterministic scheme must exist. However, it might be computationally hard to find this choice. This means that there exists a scheme for private channel coding (having the properties given in Corollary 9) that does not require any extra communication from Alice to Bob, i.e., $\mathcal{C} = \varnothing$, however its code construction might be computationally inefficient.

5 Conclusion and Open Problems

We have constructed practically efficient protocols (with complexity essentially linear in the blocklength) for one-way secret-key agreement from correlated randomness and for private channel coding over discrete memoryless wiretap channels. Each protocol achieves the corresponding optimal rate. Compared to previous methods, we do not require any degradability assumptions and achieve strong (rather than weak) secrecy. Our scheme is formulated for arbitrary discrete memoryless wiretap channels. Using ideas of Şaşoğlu *et al.* [10] the two protocols presented in this paper can also be used for wiretap channels with continuous input alphabets.

Finally, we want to describe an open problem which addresses the question of whether rates beyond $\max\{0, H(X|Z) - H(X|Y)\}$ can be achieved by our key agreement scheme, even if the optimal auxiliary random variables V and U are not given, i.e., if we run Protocol 1 directly for X (instead of U) without making V public. The question could also be formulated in the private coding scenario, whether rates beyond $\max\{0, \max_{P_X} H(X|Z) - H(X|Y)\}$ are possible, but as a positive answer in the former context implies a positive answer in the latter, we shall restrict attention to the key agreement scenario for simplicity.

Question 1 *Does for some distributions $P_{X,Y,Z}$ the rate of Protocol 1 satisfy*

$$R > \max\{0, H(X|Z) - H(X|Y)\}, \quad \text{for} \quad N \to \infty? \tag{59}$$

An equivalent formulation of this question is whether inequality (53) is always tight for large enough N, i.e.,

Question 1' *Is it possible that*

$$\lim_{L\to\infty} \frac{1}{L} H\big(V^L[\mathcal{E}_K^{\mathsf{c}}] \big| Z^L\big) < \lim_{L\to\infty} \frac{1}{L} |\mathcal{E}_K^{\mathsf{c}}|, \quad \text{for} \quad R > 0? \tag{60}$$

From the polarization phenomenon stated in Theorem 1 we obtain $\lim_{L\to\infty} \frac{1}{L} |\mathcal{E}_K^{\mathsf{c}}| = H(X|Y)$, which together with (60) would imply that $R > \max\{0, H(X|Z) - H(X|Y)\}$ for $N \to \infty$ is possible. Relation (60) can only be satisfied if the high-entropy set with respect to Bob's side information, i.e., the set $\mathcal{E}_K^{\mathsf{c}}$, is not always a high-entropy set with respect to Eve's side information. Thus, the question of rates in the key agreement protocol is closely related to fundamental structural properties of the polarization phenomenon.

A positive answer to Question 1 implies that we can send quantum information reliable over a quantum channel at a rate that is beyond the *coherent information* using the scheme introduced in [6].

Acknowledgments. The authors would like to thank Alexander Vardy for useful discussions. This work was supported by the Swiss National Science Foundation (through the National Centre of Competence in Research 'Quantum Science and Technology' and grant No. 200020-135048) and by the European Research Council (grant No. 258932).

References

1. Shannon, C.E.: Communication theory of secrecy systems. Bell System Technical Journal 28, 656–715 (1949)
2. Maurer, U.: Secret key agreement by public discussion from common information. IEEE Trans. on Information Theory 39, 733–742 (1993)
3. Wyner, A.D.: The wire-tap channel. Bell System Technical Journal 54, 1355–1387 (1975)
4. Csiszár, I., Körner, J.: Broadcast channels with confidential messages. IEEE Trans. on Information Theory 24, 339–348 (1978)
5. Arıkan, E.: Channel polarization: A method for constructing capacity-achieving codes for symmetric binary-input memoryless channels. IEEE Trans. on Information Theory 55, 3051–3073 (2009)
6. Sutter, D., Renes, J.M., Dupuis, F., Renner, R.: Efficient quantum channel coding scheme requiring no preshared entanglement. In: Proc. IEEE Int. Symposium on Information Theory (to appear, 2013)
7. Cover, T.M., Thomas, J.A.: Elements of Information Theory. Wiley Interscience (2006)
8. Körner, J., Marton, K.: Comparison of two noisy channels. In: Bolyai, J. (ed.) Topics in Information Theory. Colloquia Mathematica Societatis, pp. 411–424. North-Holland, The Netherlands (1977)
9. Arıkan, E.: Source polarization. In: Proc. IEEE Int. Symposium on Information Theory, pp. 899–903 (2010)
10. Şaşoğlu, E., Telatar, E., Arıkan, E.: Polarization for arbitrary discrete memoryless channels. In: Proc. Information Theory Workshop, pp. 144–148 (2009)
11. Arıkan, E., Telatar, E.: On the rate of channel polarization. In: Proc. IEEE Int. Symposium on Information Theory (2009)
12. Honda, J., Yamamoto, H.: Polar coding without alphabet extension for asymmetric channels. In: Proc. IEEE Int. Symposium on Information Theory, pp. 2147–2151 (2012)
13. Abbe, E.: Randomness and dependencies extraction via polarization. In: Information Theory and Applications Workshop (ITA), pp. 1–7 (2011)
14. Sahebi, A.G., Pradhan, S.S.: Multilevel polarization of polar codes over arbitrary discrete memoryless channels. In: 49th Annual Allerton Conference on Communication, Control, and Computing (Allerton), pp. 1718–1725 (2011)
15. Maurer, U.: The strong secret key rate of discrete random triples. In: Blahut, R.E. (ed.) Communication and Cryptography, pp. 271–285. Kluwer Academic, Boston (1994)
16. Maurer, U., Wolf, S.: Information-theoretic key agreement: From weak to strong secrecy for free. In: Preneel, B. (ed.) EUROCRYPT 2000. LNCS, vol. 1807, pp. 351–368. Springer, Heidelberg (2000)
17. Ahlswede, R., Csiszár, I.: Common randomness in information theory and cryptography. i. secret sharing. IEEE Trans. on Information Theory 39, 1121–1132 (1993)

18. Holenstein, T., Renner, R.: One-way secret-key agreement and applications to circuit polarization and immunization of public-key encryption. In: Shoup, V. (ed.) CRYPTO 2005. LNCS, vol. 3621, pp. 478–493. Springer, Heidelberg (2005)
19. Maurer, U., Wolf, S.: Unconditionally secure key agreement and the intrinsic conditional information. IEEE Trans. on Information Theory 45, 499–514 (1999)
20. Renner, R., Wolf, S.: New bounds in secret-key agreement: The gap between formation and secrecy extraction. In: Biham, E. (ed.) EUROCRYPT 2003. LNCS, vol. 2656, pp. 562–577. Springer, Heidelberg (2003)
21. El Gamal, A., Kim, Y.H.: Network Information Theory. Cambridge University Press (2012)
22. Abbe, E.: Low complexity constructions of secret keys using polar coding. In: Proc. Information Theory Workshop (2012)
23. Chou, R.A., Bloch, M.R., Abbe, E.: Polar coding for secret-key generation (2013), http://arxiv.org/abs/1305.4746
24. Mahdavifar, H., Vardy, A.: Achieving the secrecy capacity of wiretap channels using polar codes. IEEE Trans. on Information Theory 57, 6428–6443 (2011)
25. Bellare, M., Tessaro, S., Vardy, A.: Semantic security for the wiretap channel. In: Safavi-Naini, R., Canetti, R. (eds.) CRYPTO 2012. LNCS, vol. 7417, pp. 294–311. Springer, Heidelberg (2012)
26. Andersson, M., Rathi, V., Thobaben, R., Kliewer, J., Skoglund, M.: Nested polar codes for wiretap and relay channels. IEEE Communications Letters 14, 752–754 (2010)
27. Hof, E., Shamai, S.: Secrecy-achieving polar-coding. In: Proc. Information Theory Workshop, pp. 1–5 (2010)
28. Koyluoglu, O.O., El Gamal, H.: Polar coding for secure transmission and key agreement. In: IEEE 21st International Symposium on Personal Indoor and Mobile Radio Communications (PIMRC), pp. 2698–2703 (2010)
29. Şaşoğlu, E., Vardy, A.: A new polar coding scheme for strong security on wiretap channels. In: Proc. IEEE Int. Symposium on Information Theory (to appear, 2013)
30. Hayashi, M., Matsumoto, R.: Construction of wiretap codes from ordinary channel codes. In: Proc. IEEE Int. Symposium on Information Theory, pp. 2538–2542 (2010)
31. Karzand, M., Telatar, E.: Polar codes for q-ary source coding. In: Proc. IEEE Int. Symposium on Information Theory, pp. 909–912 (2010)
32. Tal, I., Sharov, A., Vardy, A.: Constructing polar codes for non-binary alphabets and macs. In: Proc. IEEE Int. Symposium on Information Theory, pp. 2132–2136 (2012)
33. Tal, I., Vardy, A.: How to construct polar codes. Submitted to IEEE Transactions on Information Theory (2011), arXiv:1105.6164
34. Sutter, D., Renes, J.M., Dupuis, F., Renner, R.: Achieving the capacity of any DMC using only polar codes. In: Proc. Information Theory Workshop, pp. 114–118 (2012); extended version available at arXiv:1205.3756