Explicit Capacity-Achieving Coding Scheme For The Gaussian Wiretap Channel

Himanshu Tyagi
University of California, San Diego
La Jolla, CA 92093, USA
Email: htyagi@eng.ucsd.edu

Alexander Vardy
University of California, San Diego
La Jolla, CA 92093, USA
Email: avardy@ucsd.edu

***Abstract*—We extend the Bellare-Tessaro coding scheme for a discrete, degraded, symmetric wiretap channel to a Gaussian wiretap channel. Denoting by SNR the signal-to-noise ratio of the eavesdropper's channel, the proposed scheme converts a transmission code of rate R for the channel of the legitimate receiver into a code of rate $R-0.5\log(1+\mathtt{SNR})$ for the Gaussian wiretap channel. The conversion has a *polynomial complexity* in the codeword length and the proposed scheme achieves *strong security*. In particular, when the underlying transmission code is capacity achieving, this scheme achieves the secrecy capacity of the Gaussian wiretap channel.**

I. Introduction

Recently, Hayashi and Matsumoto [10] and Bellare and Tessaro [3] introduced a new coding scheme for a *discrete, degraded, symmetric wiretap channel*[1] (DSWC) that can be efficiently implemented and achieves the secrecy capacity of the wiretap channel. Specifically, they introduced a modular scheme that starts with a given transmission code of rate R for the channel of the legitimate receiver and converts it into a wiretap code of rate $R-I(W)$, where $I(W)$ is the capacity of the (symmetric) discrete memoryless channel W between the sender and the eavesdropper. The conversion is efficient – it is of polynomial complexity in the length of the code. In particular, the conversion in [3] uses an (efficiently) invertible extractor constructed from a 2-universal hash family (cf. [7], [11], [12]). When the transmission code achieves capacity of the legitimate channel T, i.e., $R=I(T)$, the proposed wiretap coding scheme achieves the capacity of a DSWC.

In this paper, we extend the aforementioned coding scheme to the *Gaussian wiretap channel* (GWC), which was studied first by Leung-Yan-Cheong and Hellman [15], following the pioneering work of Wyner [21]. They considered wiretap codes such that each codeword $\mathbf{x}$ has power $\|\mathbf{x}\|_2^2$ bounded above by nP and the *weak security* criterion is satisfied by the random message M and the eavesdropper's observation, i.e.,

$$\lim_{n\to\infty}\frac{1}{n}I(M\wedge Z^n)=0.$$

Denoting by $C_s(P)$ the maximum rate of such codes, the following result was shown in [15].

[1]The scheme in [10], [3] achieves capacities of symmetric channels for which uniform input yields a uniform output; it was extended to all symmetric channels by Tal and Vardy [19].

Theorem 1. *[15] The secrecy capacity $C_s(P)$ is given by*

$$C_s(P)=\frac{1}{2}\log\left(\frac{1+P/\sigma_T^2}{1+P/\sigma_W^2}\right),$$

where σ_T^2 and σ_W^2 are the variances of the zero mean additive Gaussian noise in the legitimate receiver's and the eavesdropper's channels, respectively.

Although the result above characterizes the optimum rate of wiretap codes, it does not give a constructive scheme for optimal codes. In [16], a lattice code based scheme was proposed for the GWC that achieves rates within $1/2$ nats of $C_s(P)$, while ensuring *strong security* with $I(M\wedge Z^n)\to 0$. However, even this scheme is not constructive and relies on random lattice codes. To the best of our knowledge, there is no explicit coding scheme known for the GWC. We fill this gap here and show that the wiretap coding scheme of [3] achieves the capacity of the GWC as well. Our proof of security relies on a simple extension of the well-known *leftover hash lemma* (cf. [17]) to mixed RVs. This is in contrast to the approach in [10] where the basic form of leftover hash lemma was deemed insufficient and the message equivocation $H(M|Z^n)$ was bounded in terms of the Gallager function.

A key feature of this scheme is that it is modular: while the underlying transmission code ensures *reliable recovery* of the transmitted message, a new *preprocessing layer* is added to ensure *security*. When the transmission code is capacity achieving for the channel T, this scheme achieves the secrecy capacity of the GWC. In effect, this approach allows us to reduce the problem of constructing efficient, secrecy capacity achieving codes for the GWC to that of constructing efficient, capacity achieving transmission codes for a Gaussian channel.

The basics of coding for a GWC are reviewed in the next section. The proposed scheme is described in Section III, followed by a proof of its security in Section IV. Our scheme in Section III assumes that all parties share a random seed. We get rid of this assumption in Section V. The final section contains a discussion on our notion of security.

Notation. All *random variables* (RVs) will be denoted by capital letters and their range sets by the corresponding calligraphic letters. P_U will denote the probability distribution of a RV U taking values in a set $\mathcal{U}$. Vectors $(u_1,...,u_n)$ will be denoted by either u^n or $\mathbf{u}$; a collection of RVs $U_1,...,U_n$

will be abbreviated as U^n. All logarithms are to the base 2.

II. Basics of coding for a GWC

A wiretap channel consists of two memoryless channels T and W, with a common input alphabet $\mathcal{X}$ and output alphabets $\mathcal{Y}$ and $\mathcal{Z}$, respectively. When the sender transmits an n-length sequence $x^n \in \mathcal{X}^n$, the (legitimate) receiver observes the $y^n \in \mathcal{Y}^n$ with probability $\prod_i T(y_i|x_i)$ and the eavesdropper observes the side information $z^n \in \mathcal{Z}^n$ with probability $\prod_i W(z_i|x_i)$. A code for this wiretap channel ensures reliable transmission of a message M from the sender to the receiver, while keeping it secret from the eavesdropper. Denote by Y^n and Z^n the n-length random vectors observed by the receiver and the eavesdropper, respectively. In this paper, we consider a GWC where the channels T and W are *additive white Gaussian noise* (AWGN) channels, with $\mathcal{X} = \mathcal{Y} = \mathcal{Z} = \mathbb{R}$. Specifically, for an input X selected by the sender, the receiver and the eavesdropper observe noisy versions of X given by $Y = X + N_T$ and $Z = X + N_W$, respectively, where N_T and N_W are zero mean Gaussian RVs with variances σ_T^2 and σ_W^2, respectively.

Definition 1. An (n, k, P)-code consists of a (stochastic) encoder $e : \{0,1\}^k \to \mathcal{X}^n$ and a decoder $d : \mathcal{Y}^n \to \{0,1\}^k$. The maximum probability of error $\epsilon(e, d)$ for the code (e, d) is given by

$$\epsilon(e,d) = \max_{m \in \{0,1\}^k} \mathbb{E} \sum_{\mathbf{y} \text{ s.t. } d(\mathbf{y}) \neq m} T^n(\mathbf{y} \mid e(m)),$$

where the expectation is over the random encoder. Furthermore, the encoder e satisfies the following *power constraint* with probability 1:

$$\|e(m)\|_2^2 \leq nP, \tag{1}$$

for every k-bit message $m \in \{0,1\}^k$, where $\|\mathbf{x}\|_2^2 = \sum_{i=1}^n x_i^2$.

Definition 2 (Secrecy capacity). A rate $R \geq 0$ is achievable with power constraint P if there exists a sequence of (n, k_n, P)-codes (e_n, d_n) such that

$$\liminf_{n\to\infty} \frac{k_n}{n} \geq R,$$

the maximum probability of error $\epsilon(e_n, d_n)$ vanishes to 0 asymptotically, and the random message M is "asymptotically independent" of Z^n, i.e.,

$$\lim_{n\to\infty} I(M \wedge Z^n) = 0. \tag{2}$$

The secrecy capacity $C_s(P)$ is defined as the supremum over all rates R that are achievable with power constraint P.

III. A polynomial-time coding scheme

In this section, we describe the coding scheme introduced in [10], [3], [5] for a discrete wiretap channel and extend it to the GWC. Following [3], [5], we shall assume first that the sender, the receiver, and the eavesdropper share a random seed S. In practice, however, the seed S must be shared via channel T since there is no other means of communication between the sender and the receiver. Indeed, as observed in [3], the scheme presented in this paper can be easily modified to share S over the channel T with a negligible loss in the code rate and while maintaining security. See Section V for further discussion.

The proposed scheme is modular and consists of two layers: an error-correcting layer and a security layer. The error-correcting layer consists of a transmission code (e_0, d_0) for the legitimate channel T. The security layer, consisting of an efficiently invertible extractor, converts *any* transmission code (e_0, d_0) for T into a code for the GWC. Formally, the two components are described below.

(i) *Transmission code.* We start with an (n, l, P)-code (e_0, d_0) as in Definition 1; it holds by (1) that

$$\|e_0(m)\|_2^2 \leq nP, \quad \forall\, m \in \{0,1\}^l. \tag{3}$$

(ii) *Invertible extractor.* The second component is an invertible extractor. An extractor is a random mapping that takes as input a RV and outputs an "almost uniform" RV. It is well-known (see [6], [11], [12]) that such a mapping can be implemented by a 2-universal hash family [7], which is defined next.

Definition 3. A family $\{f_s : \mathcal{U} \to \{0,1\}^k, s \in \mathcal{S}\}$, is a 2-*universal hash family* if for every $u \neq u'$, we have

$$\frac{1}{|\mathcal{S}|} |\{s \mid f_s(u) = f_s(u')\}| \leq 2^{-k}.$$

Our coding scheme uses the following 2-*universal hash family*.

Let $\{0,1\}^l$ correspond to the elements of $GF(2^l)$ with multiplication operation $*$ and let $\mathcal{S} = \{0,1\}^l \setminus \{\mathbf{0}\}$. For $k \leq l$, define a mapping $f : \mathcal{S} \times \{0,1\}^l \to \{0,1\}^k$ and its inverse $\phi : S \times \{0,1\}^k \times \{0,1\}^{l-k} \to \{0,1\}^l$ as follows:

$$f : (s, v) \mapsto (s * v)_k,$$
$$\phi : (s, m, b) \mapsto s^{-1} * (m \| b),$$

where $(\cdot)_k$ selects the k most significant bits and $(\cdot\|\cdot)$ concatenates the two strings. It follows that

$$f(s, \phi(s, m, b)) = m, \tag{4}$$

for all s, b. The next result is well known and is easy to show.

Proposition 1. *The family of mappings* $\{f_s(v) := f(s, v), s \in \mathcal{S}\}$ *constitutes a* 2*-universal hash family.*

We are now in a position to describe our two-layered codes (e, d) for the GWC. See Figure 1 for an illustration.

Encoding. The sender draws a random seed S uniformly from the set $\mathcal{S}$ and shares it with the receiver and the eavesdropper. Next, the sender generates $l - k$ random bits B and encodes a message $m \in \{0,1\}^k$ as $e_0(\phi(S, m, B))$, i.e, the encoder mapping e can be described as follows:

$$e : (S, m, B) \mapsto e_0(\phi(S, m, B)) \in \mathcal{X}^n.$$

Decoding. Upon observing Y^n and S, the receiver decodes the message as $f(S, d_0(Y^n))$, i.e., the decoder d can be described

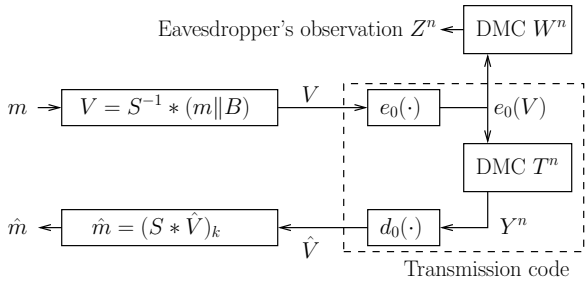

Fig. 1. Illustration of the new coding scheme

as follows:

$$d : (S, Y^n) \mapsto f(S, d_0(Y^n)) \in \{0,1\}^k.$$

Several polynomial-time implementations of the 2-universal hash family (f, ϕ) described above are known (cf. [14]). Therefore, the proposed scheme can be implemented efficiently as long as (e_0, d_0) can be implemented efficiently.

In view of (3), with a slight abuse of the notation, (e, d) constitutes an (n, k, P) wiretap code. Furthermore, it follows from (4) that

$$\epsilon(e, d) \le \epsilon(e_0, d_0). \tag{5}$$

Thus, (n, k, P)-code (e, d) ensures reliable transmission provided that the (n, l, P)-code (e_0, d_0) ensures reliable transmission over T. It remains to examine the security of the proposed scheme, which is done in the next section.

IV. Proof of security

We recast the proof of security in [3] in a form that will lend itself to the analysis for the Gaussian case; the proof is completed using a measure concentration result for chi-squared RVs. Instead of (2), we show first that for some $c > 0$,

$$\left\| \mathrm{P}_{MZ^nS} - \mathrm{P}_{\mathtt{unif}} \mathrm{P}_{Z^nS} \right\|_1 \le e^{-nc}, \tag{6}$$

where $M \sim \mathtt{unif}\{0,1\}^k$ and $\|\mathrm{P} - \mathrm{Q}\|_1$ is the total variation distance between the measures P and Q given by

$$\|P - Q\|_1 := \sup_{\mathcal{A}} |\mathrm{P}(\mathcal{A}) - \mathrm{Q}(\mathcal{A})|.$$

It will follow from [8, Lemma 1] (see, also, [4], [5]) that $I(M \wedge Z^n, S) \to 0$ as $n \to \infty$. The key technical tool for our proof is the leftover hash lemma. Below we present this result for the case of mixed RVs (U, Z), where U is discrete and the conditional probability distribution $\mathrm{P}_{Z|U}$ has a density $p(z|u)$; the proof is along the lines of [17, Corollary 5.6.1.] and is omitted. To state the result, we need the following definitions.

The *conditional min-entropy* $H_{min}(\mathrm{P}_{UZ} \mid \mathrm{P}_Z)$ of U given Z is defined as

$$H_{min}(\mathrm{P}_{UZ} \mid \mathrm{P}_Z) = -\log \int_{\mathbb{R}^n} \max_u \mathrm{P}_U(u)\, p(z|u) dz.$$

The definitions above remains valid even when the conditional probability densities $p(z|u)$ are replaced by nonnegative, subnormalized functions $p(z|u)$, i.e., $p(z|u) \ge 0$ such that

$$\int_{\mathbb{R}^n} p(z|u) dz \le 1.$$

The *ϵ-smooth* conditional min-entropy $H^\epsilon_{min}(\mathrm{P}_{UZ} \mid \mathrm{P}_Z)$ is defined as [18]

$$H^\epsilon_{min}(\mathrm{P}_{UZ} \mid \mathrm{P}_Z) = \sup_{\substack{\mathrm{Q}_{UZ}: \\ \|\mathrm{Q}_{UZ} - \mathrm{P}_{UZ}\|_1 \le \epsilon}} H_{min}(\mathrm{Q}_{UZ} \mid \mathrm{Q}_Z),$$

where the supremum is over all Q_{UZ} with Q_U discrete and $\mathrm{Q}_{Z|U}$ described by a nonnegative, subnormalized density $q(z|u)$. Note that for mixed measures P_{UZ} and Q_{UZ} as above,

$$\begin{aligned} &\|\mathrm{P}_{UZ} - \mathrm{Q}_{UZ}\|_1 \\ &= \frac{1}{2} \sum_u \int_{\mathbb{R}^n} \left| \mathrm{P}_U(u)\, p(z|u) - \mathrm{Q}_U(u) q(z|u) \right| dz. \end{aligned}$$

Lemma 2 (Leftover Hash). *Let P_{UZ} be a mixed measure as above, and let $\{f_s : \mathcal{U} \to \{1, ..., 2^k\} | s \in \mathcal{S}\}$ be a 2-universal hash family. Then, with $S \sim \mathtt{unif}(\mathcal{S})$, we have*

$$\begin{aligned} &\mathbb{E}_S \left\| \mathrm{P}_{f_S(U)Z} - \mathrm{P}_{\mathtt{unif}} \mathrm{P}_Z \right\|_1 \\ &\le 2\epsilon + \frac{1}{2} \sqrt{2^{k - H^\epsilon_{min}(\mathrm{P}_{UZ} | \mathrm{P}_Z)}}. \end{aligned}$$

Our goal is to bound $\|\mathrm{P}_{MZ^nS} - \mathrm{P}_{\mathtt{unif}} \mathrm{P}_{Z^nS}\|_1$. Unfortunately, Lemma 2 does not directly apply to RVs $U = M$, $Z = Z^n$. However, the following result allows us to replace RVs M, Z^n, S with RVs $\tilde{M}, \tilde{Z}^n, \tilde{S}$, to which Lemma 2 applies. Denote by V the RV $\phi(S, M, B)$, where B is as in the description of the scheme. Note that S, M, B are mutually independent and (S, M)—V—Z^n form a Markov chain.

Lemma 3. *For RVs S, M, V, Z^n as above, we have*

$$\mathrm{P}_{MVZ^nS} \equiv \mathrm{P}_{\tilde{M}\tilde{V}\tilde{Z}^n\tilde{S}},$$

where $\tilde{S}$ and $\tilde{V}$ are independent, $(\tilde{S}, \tilde{M})$—$\tilde{V}$—$\tilde{Z}^n$ form a Markov chain, and

$$\begin{aligned} &\tilde{S} \sim \mathtt{unif}\, \mathcal{S}, \quad \tilde{V} \sim \mathtt{unif}\{0,1\}^l, \\ &\tilde{M} = f(\tilde{S}, \tilde{V}) \text{ and } \mathrm{P}_{\tilde{Z}^n|\tilde{V}} \equiv \mathrm{P}_{Z^n|V}. \end{aligned}$$

We also need the following fact.

Lemma 4. *For RVs $\tilde{M}, \tilde{V}, \tilde{Z}^n, \tilde{S}$ as in Lemma 3, it holds that*

$$\mathrm{P}_{\tilde{M}\tilde{Z}^n|\tilde{S}}(m, z \mid s) = \mathrm{P}_{f(s,\tilde{V})\tilde{Z}^n}(m, z), \qquad \forall\, m, z, s.$$

The proofs of Lemmas 3 and 4 are straightforward and are omitted due to lack of space. Upon combining these observations, we get the following result.

Lemma 5. *For RVs $M, Z^n, S, \tilde{V}, \tilde{Z}^n$ as above, we have*

$$\|\mathrm{P}_{MZ^nS} - \mathrm{P}_{\mathtt{unif}} \mathrm{P}_{Z^nS}\|_1 \le 2\epsilon + \frac{1}{2} \sqrt{2^{k - H^\epsilon_{\min}(\mathrm{P}_{\tilde{V}\tilde{Z}^n} | \mathrm{P}_{\tilde{Z}^n})}}.$$

Proof. Lemmas 3 and 4, along with the independence of RVs $\tilde{S}$ and $\tilde{Z}^n$, imply

$$\begin{aligned}
&\|\mathrm{P}_{MZ^nS} - \mathrm{P}_{\mathtt{unif}}\mathrm{P}_{Z^nS}\|_1 \\
&= \|\mathrm{P}_{\tilde{M}\tilde{Z}^n\tilde{S}} - \mathrm{P}_{\mathtt{unif}}\mathrm{P}_{\tilde{Z}^n\tilde{S}}\|_1 \\
&= \left\|\mathrm{P}_{f(\tilde{S},\tilde{V})\tilde{Z}^n}\mathrm{P}_{\tilde{S}} - \mathrm{P}_{\mathtt{unif}}\mathrm{P}_{\tilde{Z}^n}\mathrm{P}_{\tilde{S}}\right\|_1 \\
&= \mathbb{E}_{\tilde{S}}\left\|\mathrm{P}_{f(\tilde{S},\tilde{V})\tilde{Z}^n} - \mathrm{P}_{\mathtt{unif}}\mathrm{P}_{\tilde{Z}^n}\right\|_1 \\
&\leq 2\epsilon + \frac{1}{2}\sqrt{2^{k-H^{\epsilon}_{\min}\left(\mathrm{P}_{\tilde{V}\tilde{Z}^n}|\mathrm{P}_{\tilde{Z}^n}\right)}},
\end{aligned}$$

where the last inequality follows by Lemma 2, along with Proposition 1, upon choosing $U = \tilde{V}$, $Z = \tilde{Z}^n$. □

Thus, a lower bound for $H^{\epsilon}_{min}(\mathrm{P}_{\tilde{V}\tilde{Z}^n}|\mathrm{P}_{\tilde{Z}^n})$ will result in an upper bounds for $\|\mathrm{P}_{MZ^nS} - \mathrm{P}_{\mathtt{unif}}\mathrm{P}_{Z^nS}\|_1$; the next lemma establishes such a lower bound.

Lemma 6. *Fix $0 < \delta < 1/2$ and let $\epsilon = e^{-n\delta^2/8}$. Then,*

$$H^{\epsilon}_{min}(\mathrm{P}_{\tilde{V}\tilde{Z}^n}|\mathrm{P}_{\tilde{Z}^n}) \geq l - \frac{n}{2}\log\left(1+\delta+\frac{P}{\sigma_W^2}\right) - \frac{n\delta}{2} + o(n).$$

Proof. Consider $\mathrm{Q}_{\tilde{V}\tilde{Z}^n}$ with $\mathrm{Q}_{\tilde{V}} = \mathrm{P}_{\tilde{V}}$ and $\mathrm{Q}_{\tilde{Z}^n|\tilde{V}}$ described by a nonnegative, subnormalized density $q(z|v)$. Then,

$$H^{\epsilon}_{min}(Q_{\tilde{V}\tilde{Z}^n}|Q_{\tilde{Z}^n}) = l - \log\int_{\mathbb{R}^n}\max_v q(z|v)dz.$$

For sets $\mathcal{Z}_v \subseteq \mathbb{R}^n$ (to be specified later) such that

$$\int_{\mathcal{Z}_v} p(z|v) \geq 1 - 2\epsilon, \tag{7}$$

on choosing $q(z|v) = \mathbf{1}(z \in \mathcal{Z}_v)p(z|v)$, we get

$$\|\mathrm{Q}_{\tilde{V}\tilde{Z}^n} - \mathrm{P}_{\tilde{V}\tilde{Z}^n}\|_1 \leq \epsilon.$$

Therefore,

$$H^{\epsilon}_{min}(\mathrm{P}_{\tilde{V}\tilde{Z}^n}|\mathrm{P}_{\tilde{Z}^n}) \geq l - \log\int_{\mathbb{R}^n}\max_v \mathbf{1}(z \in \mathcal{Z}_v)p(z|v)dz. \tag{8}$$

We now select sets $\mathcal{Z}_v$ satisfying (7). Denote by $g(z)$ the standard normal density on $\mathbb{R}^n$; then, $p(z|v) = g\left(\sigma_W^{-1}(z - e_0(v))\right)$. On defining

$$\mathcal{Z}_0 = \left\{z \in \mathbb{R}^n \middle| \left|\frac{1}{n}\|z\|_2^2 - 1\right| \leq \delta\right\},$$

and

$$\mathcal{Z}_v = \sigma_W\mathcal{Z}_0 + e_0(v),$$

standard measure concentration results for chi-squared RVs (cf. [2, Exercise 2.1.30]) yield

$$\int_{\mathcal{Z}_v} p(z|v)dz = \int_{\mathcal{Z}_0} g(z)dz \geq 1 - 2e^{-n\delta^2/8}.$$

It follows from (8) and the definition of $\mathcal{Z}_v$ that

$$\begin{aligned}
&H^{\epsilon}_{min}(\mathrm{P}_{\tilde{V}\tilde{Z}^n}|\mathrm{P}_{\tilde{Z}^n}) \\
&\geq l - \log\int_{\mathbb{R}^n}\max_v \mathbf{1}(z \in \mathcal{Z}_v)g\left(\frac{z - e_0(v)}{\sigma_W}\right)dz \\
&\geq l - \log\frac{e^{-\frac{n(1-\delta)}{2}}}{(2\pi\sigma_W^2)^{\frac{n}{2}}}\int_{\mathbb{R}^n}\max_v \mathbf{1}(z \in \mathcal{Z}_v)dz \\
&\geq l - \log\frac{e^{-\frac{n(1-\delta)}{2}}}{(2\pi\sigma_W^2)^{\frac{n}{2}}}\mathrm{vol}\left(\bigcup_v \mathcal{Z}_v\right).
\end{aligned}$$

Denote by $\mathcal{B}_n(\rho)$ the sphere of radius ρ in $\mathbb{R}^n$ and by $\nu_n(\rho)$ its volume, which can be approximated as (cf. [20])

$$\nu_n(\rho) = \frac{1}{\sqrt{n\pi}}\left(\frac{2\pi e}{n}\right)^{\frac{n}{2}}\rho^n\left(1 + O(n^{-1})\right) \tag{9}$$

By (3), we have

$$\bigcup_v \mathcal{Z}_v \subseteq \mathcal{B}_n\left(\rho_n\right),$$

where $\rho_n = \sqrt{n\left(\sigma_W^2(1+\delta) + P\right)}$. Therefore,

$$H^{\epsilon}_{min}(\mathrm{P}_{\tilde{V}\tilde{Z}^n}|\mathrm{P}_{\tilde{Z}^n}) \geq l - \log\frac{e^{-\frac{n(1-\delta)}{2}}}{(2\pi\sigma_W^2)^{\frac{n}{2}}}\nu_n(\rho_n),$$

which yields the claimed inequality in view of (9). □

On combining Lemmas 5 and 6, we get the following theorem.

Theorem 7 (Security bound for the scheme)**.** *For a message $M \sim \mathtt{unif}\{0,1\}^k$ and a seed $S \sim \mathtt{unif}\{0,1\}^l/\{\mathbf{0}\}$, let Z^n be the output of the eavesdropper's channel W when the coding scheme above is applied. Then,*

$$\begin{aligned}
&\|\mathrm{P}_{MZ^nS} - \mathrm{P}_{\mathtt{unif}}\mathrm{P}_{Z^nS}\|_1 \\
&\leq 2e^{-n\delta^2/8} + \frac{1}{2}\sqrt{2^{k-l+\frac{n}{2}\log\left(1+\delta+\frac{P}{\sigma_W^2}\right)+\frac{n\delta}{2}+o(n)}}.
\end{aligned}$$

Corollary 8 (Rate of the code). *Let (e_{0n}, d_{0n}) be a sequence of transmission codes of rate R for the channel T that satisfy (3) and have the maximum probability of error $\epsilon(e_{0n}, d_{0n})$ vanishing to 0 as n goes to ∞. Then, for every $0 < \delta < 1/2$, the proposed coding scheme achieves the rate*

$$R - \frac{1}{2}\log\left(1+\delta+\frac{P}{\sigma_W^2}\right) - \delta$$

for the GWC and, for a uniformly distributed message M, satisfies

$$\lim_{n\to\infty} I\left(M \wedge Z^n, S\right) = 0.$$

Proof. The bound (5) and an application of Theorem 7 with $l = \lfloor nR \rfloor$ and

$$k = \left\lfloor nR - \frac{n}{2}\log\left(1+\delta+\frac{P}{\sigma_W^2}\right) - n\delta\right\rfloor$$

implies that the proposed scheme achieves the claimed rate and satisfies

$$\|\mathrm{P}_{MZ^nS} - \mathrm{P}_{\mathtt{unif}}\mathrm{P}_{Z^nS}\|_1 \leq 2^{-n\delta/4+o(n)}.$$

It follows from [8, Lemma 1] (see, also, [4], [5]) that the Kullback-Leibler divergence $D(\mathrm{P}_{MZ^nS}\|\mathrm{P}_{\mathtt{unif}}\mathrm{P}_{Z^nS})$ goes to 0, and so,

$$\begin{aligned} I(M \wedge Z^n, S) &\leq k - H(M \mid Z^n, S) \\ &= D(\mathrm{P}_{MZ^nS}\|\mathrm{P}_{\mathtt{unif}}\mathrm{P}_{Z^nS}) \to 0, \end{aligned}$$

which completes the proof. □

Remarks. (i) Note that the proposed scheme depends on the eavesdropper's channel W only through the rate k_n/n of the extractor. In particular, the scheme yields an (n, k_n, P)-wiretap code for all AWGN channels W such that the following holds for n sufficiently large:

$$\frac{1}{2}\log\left(1 + \frac{P}{\sigma_W^2}\right) < R - \frac{k_n}{n},$$

where R is the rate of the transmission code (e_0, d_0), i.e., for all Ws with a sufficiently small signal-to-noise ratio.

(ii) To achieve the secrecy capacity of the GWC using the scheme above, one needs to start with a transmission code (e_0, d_0) that achieves the capacity of the AWGN channel T; several such schemes have been proposed (cf. [1], [13]).

V. Sharing the random seed

In the wiretap codes described in this paper, it is assumed that all parties share a random seed S. However, there is no other means of communication between the legitimate parties except the channel T. Therefore, $S \in \mathcal{S}_l$ must be communicated via T; the security proof remains unchanged since it is already assumed that the eavesdropper knows S. Such a modification of the original scheme was given in [3] and is reviewed below for completeness.

Denoting by (e_n, d_n) the sequence of wiretap codes above, consider the wiretap coding scheme obtained by first generating the random seed $S \in \{0,1\}^{nR}$, next sending S over T using the rate R transmission code (e_{0n}, d_{0n}), and finally, using the code (e_n, d_n) t_n-times with the same seed S. Let M_i, $1 \leq i \leq t_n$, denote the uniformly distributed message sent in the ith use and let $Z^n(i)$ denote the corresponding observations of the eavesdropper. Also, with $N = (t_n + 1)n$, let (e_N, d_N) denote the new scheme. Then, as observed in [3, Lemma 4.1], we have

$$\epsilon(e_N, d_N) \leq (t_n + 1)\epsilon(e_n, d_n). \tag{10}$$

Note that $(M_i, Z^n(i))$—S—$(M_j, Z^n(j))_{j\neq i}$ form a Markov chain. Therefore,

$$\begin{aligned} I(M_1, ..., M_{t_n} \wedge Z^N) &\leq \sum_{i=1}^{t_n} I(M_i \wedge Z^n(i), S) \\ &= t_n I(M \wedge Z^n, S), \end{aligned} \tag{11}$$

where M, Z^n, S are as in Corollary 8. On choosing $t_n \to \infty$ such that the right-sides of (10) and (11) go to 0, we get the required code (e_N, d_N) of rate

$$\lim_{n\to\infty} \frac{t_n k_n}{(t_n + 1)n} = \lim_{n\to\infty} \frac{k_n}{n},$$

i.e., the new code (e_N, d_N) has the same rate as (e_n, d_n).

VI. Discussion on the notion of security

The notion of security in (2) and (6) assumes a uniform distribution on M. This suffices as long as the eavesdropper has no prior knowledge of the likelihood of different messages. In general, it is desirable to guarantee security irrespective of what likelihood the eavesdropper assigns, *a priori*, to different messages. One such guarantee of security is the cryptographic notion of semantic security (cf, [9], [4], [5]). Establishing semantic security of our scheme for all message distributions, with additional assumptions on the structure of (e_0, d_0), is work in progress.

References

[1] E. Abbe and A. Barron, "Polar coding schemes for the AWGN channel," *IEEE International Symposium on Information Theory*, pp. 194–198, 2011.

[2] G. W. Anderson, A. Guionnet, and O. Zeitouni, *An introduction to random matrices*. Cambridge University Press, 2010.

[3] M. Bellare and S. Tessaro, "Polynomial-time, semantically-secure encryption achieving the secrecy capacity," Cryptology ePrint Archive, Report 2012/022, 2012, http://eprint.iacr.org/.

[4] M. Bellare, S. Tessaro, and A. Vardy, "A cryptographic treatment of the wiretap channel," Cryptology ePrint Archive, Report 2012/015, 2012, http://eprint.iacr.org/.

[5] ——, "Semantic security for the wiretap channel," *CRYPTO, LNCS*, vol. 7417, pp. 294–311, 2012.

[6] C. H. Bennett, G. Brassard, and J.-M. Robert, "Privacy amplification by public discussion," *SIAM J. Comput.*, vol. 17, no. 2, pp. 210–229, 1988.

[7] J. L. Carter and M. N. Wegman, "Universal classes of hash functions," *Journal of Computer and System Sciences*, vol. 18, no. 2, pp. 143 – 154, 1979.

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

[9] S. Goldwasser and S. Micali, "Probabilistic encryption," *Journal of Computer and System Sciences*, vol. 28, no. 2, pp. 270 – 299, 1984.

[10] M. Hayashi and R. Matsumoto, "Construction of wiretap codes from ordinary channel codes," *Proc. IEEE International Symposium on Information Theory*, pp. 2538–2542, 2010.

[11] R. Impagliazzo, L. A. Levin, and M. Luby, "Pseudo-random generation from one-way functions," in *Proc. ACM Symposium on Theory of Computing (STOC)*, 1989, pp. 12–24.

[12] R. Impagliazzo and D. Zuckerman, "How to recycle random bits," in *Proc. Annual Symposium on Foundations of Computer Science (FOCS)*, 1989, pp. 248–253.

[13] A. Joseph and A. R. Barron, "Least squares superposition codes of moderate dictionary size are reliable at rates up to capacity," *IEEE Trans. Inf. Theory*, vol. 58, no. 5, pp. 2541–2557, 2012.

[14] H. Krawczyk, "LFSR-based hashing and authentication," *CRYPTO, LNCS*, vol. 839, pp. 129–139, 1994.

[15] S. Leung-Yan-Cheong and M. Hellman, "The Gaussian wiretap channel," *IEEE Trans. Inf. Theory*, vol. 24, no. 4, pp. 451–456, 1978.

[16] C. Ling, L. Luzzi, J.-C. Belfiore, and D. Stehlé, "Semantically secure lattice codes for the gaussian wiretap channel," *CoRR*, vol. abs/1210.6673v3, 2013.

[17] R. Renner, "Security of quantum key distribution," *Ph. D. Dissertation, ETH Zurich*, 2005.

[18] R. Renner and S. Wolf, "Simple and tight bounds for information reconciliation and privacy amplification," in *Proc. ASIACRYPT*, 2005, pp. 199–216.

[19] I. Tal and A. Vardy, "Channel upgrading for semantically-secure encryption on wiretap channels," *Proc. IEEE International Symposium on Information Theory*, pp. 1561–1565, 2013.

[20] X. Wang, "Volumes of generalized unit balls," *Mathematics Magazine*, vol. 78, no. 5, 2005.

[21] A. D. Wyner, "The wiretap channel," *Bell System Technical Journal*, vol. 54, no. 8, pp. 1355–1367, October 1975.