Semantically-Secure Coding Scheme Achieving the Capacity of a Gaussian Wiretap Channel

Himanshu Tyagi and Alexander Vardy

Abstract

We extend a recently proposed wiretap coding scheme to the Gaussian wiretap channel and show that it is semantically-secure. Denoting by $\text{SNR}$ 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 $R - 0.5 \log(1 + \text{SNR})$ for the Gaussian wiretap channel. The conversion has a polynomial complexity in the codeword length and the proposed scheme achieves semantic security. In particular, when the underlying transmission code is capacity achieving, this scheme achieves the secrecy capacity of the Gaussian wiretap channel. Our security analysis relies on a single-shot bound on the mutual information between the message and the eavesdropper’s observation for the proposed scheme, which may be of independent interest.

I. INTRODUCTION

Consider a wiretap channel where for every input $x$ the legitimate receiver observes the output $y$ with probability $T(y|x)$ and the eavesdropper observes $z$ with probability $W(z|x)$ [26]. The goal is to reliably send a message to the legitimate receiver by using $n$ transmissions over the channel in such a manner that the message remains concealed from the eavesdropper. While the maximum rate of such a message, namely the wiretap capacity, was characterized almost four decades ago [26], [7], an efficient coding scheme that achieves the wiretap capacity for a degraded and symmetric wiretap channel with finite input and output alphabet has emerged only recently in the work of Hayashi-Matsumoto [11] and Bellare-Tessaro [3].

Specifically, they propose a modular scheme that starts with a given error correcting code (ECC) of rate $R$ for channel $T$ and converts it into a wiretap code of rate $R - I(W)$, where $I(W)$ is the
capacity of the symmetric discrete memoryless channel (DMC) $W$. 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 (UHF) (cf. [6], [13], [14]). For the case when $T$, too, is symmetric, the wiretap channel is degraded, and the ECC achieves the capacity of $T$, i.e., $R = I(T)$, the proposed wiretap coding scheme achieves the wiretap capacity under the strong secrecy criterion for uniformly distributed messages. Furthermore, if the underlying capacity achieving ECC is linear and separable, the scheme achieves the wiretap capacity under the semantic security criterion, namely it achieves the wiretap capacity while ensuring strong secrecy for arbitrarily distributed messages (see [4]).

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 [18]. They considered wiretap codes such that each codeword $x$ has $\|x\|_2^2$ bounded above by $nP$ and the weak security criterion is satisfied by the random message $M$ and the eavesdropper’s observation, i.e.,

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

Denote by $C(P)$ the wiretap capacity of the GWC with transmission noise variance $\sigma_T^2$ and eavesdropper’s noise variance $\sigma_W^2$, when the codewords satisfy the power constraint $P$ as above. The following result was shown in [18].

**Theorem 1.** [18] The wiretap capacity $C(P)$ is given by

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

where $\sigma_T^2$ and $\sigma_W^2$ 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 for a GWC, it does not give a explicit scheme for optimal codes. Motivated by the central role of wiretap channels in physical layer security, several explicit coding schemes for wiretap channels have been proposed over the past decade. However, to the best of our knowledge, no explicit coding scheme has been shown to achieve the wiretap capacity of a GWC. We begin by reviewing the known schemes.
A. Prior work

For the discrete case, LDPC based schemes were proposed in [24] and the role of capacity achieving ECCs in the design of wiretap capacity achieving codes (under weak secrecy) was highlighted. In [21], polar codes were shown to achieve the capacity of a binary-input, degraded, symmetric wiretap channel with discrete input and output, under the strong secrecy criterion and for a uniformly distributed message.

A remarkable general efficient coding scheme based on an invertible UHF for a discrete wiretap channel was proposed in [11] and was shown to achieve the capacity of a degraded, symmetric wiretap channel with discrete input and output, under strong secrecy for a uniformly distributed message. Subsequently, a construction with a specific choice of an efficiently invertible UHF was proposed in [3] which, for special choices of ECCs, was shown to be semantically secure (for all message distributions). In fact, the scheme in [11], [3] achieves capacities of discrete, degraded wiretap channels where the channels $T$ and $W$ are symmetric and have the property that a uniform input yields a uniform output for them; it was extended to all discrete, degraded, symmetric wiretap channels by Tal and Vardy [23]. A key feature of this scheme is that it is modular: An off-the-shelf transmission code is chosen to ensure reliable recovery of the transmitted message, and a new preprocessing layer is added to ensure security. In effect, this approach reduces the problem of constructing efficient, wiretap capacity achieving codes to that of constructing efficient, capacity achieving ECCs for $T$. An extension of this scheme to a substantially more general model has been proposed recently in [12].

For the GWC, a lattice code based scheme was proposed in [20] which achieves rates within $\frac{1}{2}$ nats of $C(P)$, while ensuring semantic security. A capacity achieving scheme for a GWC using lattice code has been proposed recently in [19], albeit under the weak secrecy criterion. Both these schemes rely on random lattices and are not explicit.

B. Our contributions

We show that the explicit wiretap coding scheme of [3] achieves the wiretap capacity of the GWC as well. Furthermore, we show that the scheme is semantically-secure: For a message $M$ transmitted using the coding scheme with $n$ channel uses, the leakage $\max_{P_M} I(M \wedge Z^n)$ vanishes to zero exponentially rapidly in $n$. Our security analysis relies on a single-shot bound on the mutual information between the message and the eavesdropper’s observations for the proposed scheme. This basic result is, in effect, an inverse leftover hash lemma and plays the same role in secure message transmission as that of leftover hash lemma (cf. [22]) in randomness extraction. In particular, this result shows that for a given ECC and an eavesdropper’s channel $W$, the loss in message rate incurred due to the UHF layer is bounded above
by the *smooth max-information* of the combined channel obtained by precoding $W$ using the ECC.

Note that an alternative proof of security is possible by using a particularization of [12, Theorem 15] to the case of a wiretap channel. However, the results in [12] are stated for the discrete case and an extension to the continuous case will require a verification of the underlying technical conditions. Furthermore, the evaluation of bounds on mutual information in [12] relies on type arguments which do not apply to a GWC, and the bounds derived in Section V will be needed to complete the proof. Instead, we prefer the direct proof outlined above, which is tailored to the specific case of a wiretap channel and is self-contained.

C. Outline of the paper

The paper is organized as follows. In the next section, we review the basics of coding for a wiretap channel and notions of UHF. Furthermore, we introduce the notion of smooth max-information, which will play a pivotal role in the inverse leftover hash lemma. The proposed coding scheme for a GWC is described in Section III. In Section IV we prove the inverse leftover hash lemma and use it to re-derive the security of the scheme for a discrete wiretap channel. Section V contains our main result, namely the semantic security of the coding scheme for a GWC. We end with a discussion of our results in the final section.

D. Notation

All random variables 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 $u^n$ and a collection of RVs $U_1, ..., U_n$ will be abbreviated as $U^n$. All logarithms are to the base 2.

II. Preliminaries

A. Wiretap Codes

We consider a memoryless wiretap channel consisting of a transmission channel $T$ and an eavesdropper’s channel $W$, 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 $y^n \in \mathcal{Y}^n$ with probability $\prod_i T(y_i|x_i)$ and the eavesdropper observes the side information $z^n \in \mathcal{Z}^n$ with probability $\prod_i W(z_i|x_i)$. Denote by $Y^n$ and $Z^n$ the $n$-length random vectors observed by the receiver and the eavesdropper, respectively.

\[1\]

1We assume without any loss of generality that $Y^n$ and $Z^n$ are independent given $X^n$. 

December 19, 2014 DRAFT
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. That is, in addition to the usual error correcting property for transmissions over $T$, a wiretap code also ensures the secrecy of the message $M$ from the output of $W$. In this work, we require the message to satisfy \textit{semantic security} which was introduced for the wiretap channel in \cite{4}. Specifically, we require that for every message distribution the eavesdropper cannot infer any more about any function $f(M)$ of the message than a random guess, which is the same as requiring the mutual information $I(M \land Z^n)$ to be small for every message distribution $P_M$ (see \cite{4}).

We mainly focus on a GWC where the channels $T$ and $W$ are \textit{additive white Gaussian noise} (AWGN) channels with $X = Y = Z = \mathbb{R}$. For an input $X$ selected by the sender, the receiver and the eavesdropper, respectively, observe noisy versions of $X$ given by $Y = X + N_T$ and $Z = X + N_W$, where $N_T$ and $N_W$ are zero mean Gaussian RVs with variances $\sigma^2_T$ and $\sigma^2_W$. As is the norm, we consider codes satisfying a power constraint $P$.

\textbf{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

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

where the expectation is over the random encoder. Furthermore, the encoder $e$ satisfies the following \textit{power constraint} with probability 1:

$$
\frac{1}{n} \| e(m) \|^2 \leq P,
$$

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

The largest possible rate of a code that is asymptotically reliable and secure is called the \textit{wiretap capacity}.

\textbf{Definition 2.} 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 \textit{maximum probability of error} $\epsilon(e_n, d_n) \to 0$ as $n \to \infty$, and $M$ is semantically-secure of $Z^n$, i.e.,

$$
\lim_{n \to \infty} \max_{P_M} I(M \land Z^n) = 0.
$$
The wiretap capacity $C(P)$ is defined as the supremum of rates $R$ that are achievable with power constraint $P$.

### B. 2-Universal hash families and smooth max-information

A UHF is a key primitive in information theoretic secrecy and appears in applications such as secret key agreement [5], quantum key distribution [22], and biometric and hardware security [9]. In this section, we describe a UHF construction which is efficiently invertible and underlies the code construction in [4]. Furthermore, we describe a basic information theoretic quantity that will be pivotal in our security analysis.

**Definition 3.** A family $\{f_s : \{0, 1\}^l \rightarrow \{0, 1\}^k, s \in S\}$ is a UHF if

$$\frac{1}{|S|} \left| \{ s \mid f_s(v) = f_s(v') \} \right| \leq 2^{-k}, \quad \text{for all } v \neq v'.$$

The importance of a UHF lies in the role it plays in randomness extraction. In particular, the *leftover hash lemma* (cf. [22]) shows that for a UHF $\{f_s, s \in S\}$ with (range size in bits) $k$ less than the smooth min-entropy $H_{\epsilon}(P_X)$ of $X$ and a seed $S$ distributed uniformly over $S$, the variation distance $\|P_{f_s(X)S} - P_{\text{unif}} \times P_S\|_1$ is small$^2$. That is, a UHF extracts $H_{\epsilon}(P_X)$ approximately uniform, random bits from $X$.

In Section IV we show that for semantically-secure message transmission over a wiretap channel, the balanced invertible UHF defined below plays a similar role as that of a UHF in randomness extraction. Specifically, we show that a balanced invertible UHF can be used to convert an ECC to a code for the wiretap channel, with a rate loss less than the *smooth-max information* of eavesdropper’s channel $W$. Here we define the basic concepts needed to state this result.

**Definition 4.** For $M \subset \{0, 1\}^k$ and $\delta \geq 0$, an $(M, b, \delta)$-balanced UHF $\{f_s : \{0, 1\}^l \rightarrow \{0, 1\}^k, s \in S\}$ is a UHF that additionally has the following three properties:

1) For every seed $s \in S$ and $m \in \{0, 1\}^k$,

$$|\{v \mid f_s(v) = m\}| = 2^b;$$

2) there exists a constant $b'$ such that one of the following holds for every $v \in \{0, 1\}^l$:

$$|\{s \in S \mid f_s(v) = m\}| = 2^{b'}, \quad m \in M,$$

$^2$ For a statement in terms of the Kullback-Leibler divergence in place of the variation distance, see [10].
or

\[ |\{ s \in S \mid f_s(v) = m \}| = 0, \quad m \in \mathcal{M}; \]

3) the parameters \( b', k \) satisfy

\[ (1 + \delta)^{-1} \leq |S|2^{-(k+b')} \leq 1. \]

The wiretap coding scheme described in Section III relies on the efficiently invertible balanced UHF described below. Let \( \{0, 1\}^l \) correspond to the elements of \( GF(2^l) \) and let \( S = \{0, 1\}^l \setminus \{0\} \). For \( k \leq l \), define a mapping \( f : S \times \{0, 1\} \to \{0, 1\}^k \) as follows:

\[ f(s,u) = (s \cdot v)_k, \]

where \((v)_k\) selects the \( k \) most significant bits of \( v \). The inverse of \( f \) can be efficiently computed using the mapping \( \phi(s,m,b) = s^{-1} \cdot (m|b) \), where \((m|b)\) denotes the concatenation of \( m \) and \( b \). Note that \( \phi \) is indeed the inverse of \( f \) since \( f(s, \phi(s,m,b)) = m \) for every \( s,m,b \).

**Lemma 2.** For \( \mathcal{M} = \{0, 1\}^k / \{0\} \), the family of mappings \( \{f_s(v) := f(s,v), s \in S\} \) constitutes an \( (\mathcal{M}, l-k, 1) \)-balanced UHF.

**Proof:** For \( v, v' \neq 0, v \neq v' \),

\[
|\{ s \in S : (s \cdot v)_k = (s \cdot v')_k \}| + 1
= |\{ s \in \{0, 1\}^k : (s \cdot v)_k = (s \cdot v')_k \}|
= \sum_{s,b,b'} I\left((s \cdot v) = (m|b), (s \cdot v') = (m|b'), m \in \{0, 1\}^k\right)
= \sum_{b,b'} I\left(v^{-1} \cdot (m|b) = v'^{-1} \cdot (m|b'), m \in \{0, 1\}^k\right)
\leq \sum_{b,b'} I\left(v' \cdot v^{-1} \cdot (0|b) = (u|b'), u \in \{0, 1\}^{l-k}\right)
\leq 2^{l-k}.
\]

Also, the bound above holds if one of \( v \) or \( v' \) is 0. Thus,

\[
\frac{1}{|S|} |\{ s \in S : f(s,v) = f(s,v')\}| \leq \frac{2^{l-k} - 1}{2^l - 1} = \frac{2^{l-k} - 1}{2^l - 1} \leq 2^{-k}.
\]

Note that

\[
|\{ v \mid (s \cdot v)_k = m \}| = |\{ v \mid v = s^{-1}(m|b), b \in \{0, 1\}^{l-k}\}| = 2^{l-k},
\]
which proves the first property. Similarly, the second property holds since $|\{s \in S \mid (s \cdot v)_k = m\}| = 2^{l-k}$ for $v \neq 0$ and $|\{s \in S \mid (s \cdot 0)_k = m\}| = 0$ for $m \neq 0$. Finally, the third property holds since

$$|S|2^{-(k+b')} = 1 - 2^{-l} \geq 1/2.$$ 

Next, we define smooth max-information of a channel $W$. For technical reasons we define max-information for the more general, subnormalized channels $W$, i.e., channels $W : \mathcal{X} \to \mathcal{Z}$ with

$$W(\mathcal{Z} \mid x) \leq 1 \text{ for all } x \in \mathcal{X}.$$ 

**Definition 5.** Consider a subnormalized channel $W : \mathcal{X} \to \mathcal{Z}$ with a finite input alphabet $\mathcal{X}$ and such that for each $x \in \mathcal{X}$ the measure $W(\cdot \mid x)$ on $\mathcal{Z}$ has a density $\omega(z|x)$ with respect to a measure $\mu$ on $\mathcal{Z}$. The **max-information** of $W$ is given by

$$I_{\text{max}}(W) = \log \int \max_{x \in \mathcal{X}} \omega(z|x) \, d\mu.$$ 

For a subset $T$ of $\mathcal{X} \times \mathcal{Z}$, denote by $W_T$ the subnormalized channel corresponding to the density

$$\omega_T(z \mid x) = \begin{cases} \omega(z|x), & (x,z) \in T, \\ 0, & \text{otherwise}. \end{cases}$$

The $\epsilon$-smooth max-information of $W$, $I_{\text{max}}^\epsilon(W)$, is given by the infimum of $I_{\text{max}}(W_T)$ over all sets $T \subset \mathcal{X} \times \mathcal{Z}$ such that

$$W(\{z : (x,z) \in T\} \mid x) \geq 1 - \epsilon, \quad \text{for all } x \in \mathcal{X}. \quad (1)$$

**III. CODING SCHEME**

We describe the coding scheme introduced in [11], [3], [4] for a discrete wiretap channel and extend it to the GWC. Following [3], [4], 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 a further clarification.

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

1) **ECC**. We start with an $(n, l, P)$-code $(e_0, d_0)$ as in Definition I that satisfies the average power constraint

$$\frac{1}{n} \|e_0(m)\|_2^2 \leq P, \quad \forall m \in \{0, 1\}^l. \quad (2)$$

2) **Efficiently invertible balanced UHF**. With $\mathcal{M} = \{0, 1\}^k/\{0\}$, the second component of our scheme is the $(\mathcal{M}, l - k, 1)$-balanced UHF of Lemma II. The key feature of this UHF is that the hash mappings $f_s$ are easy to compute and invert (using $\phi(s, m, b) = s^{-1} \cdot (m|b)$).

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

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

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

**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 as follows:

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

Several polynomial-time implementations of the balanced UHF $(f, \phi)$ described above are known (cf. [16]). Therefore, the proposed scheme can be implemented efficiently as long as $(e_0, d_0)$ can be implemented efficiently.

In view of (2), $(e, d)$ constitutes an $(n, k, P)$-code for the wiretap channel. Furthermore, it follows from $f(s, \phi(s, m, b)) = m$ that

$$\epsilon(e, d) \leq \epsilon(e_0, d_0),$$

i.e., the maximum probability of error for $(e, d)$ is no more than that for $(e_0, d_0)$. 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 $T$.

In the next two sections, we establish the security of this scheme, starting with a general result applicable to any balanced UHF and wiretap channel in the next section, followed by a specific analysis for the GWC in the subsequent section.

IV. INVERSE LEFTOVER HASH

We establish a general result on the security of wiretap coding schemes based on balanced UHFs of Definition 4. Our result is single-shot and applies to any (eavesdropper’s) channel $W$. Similar bounds have been derived in [12] in terms of the Gallager exponent of $W$.

Consider a channel $W : X \rightarrow Z$ with input alphabet $X = \{0, 1\}^l$ and density $\omega(z | x)$ with respect to a measure $\mu$ on $Z$.

Theorem 3 (Inverse leftover hash). Let $\{f_s : \{0, 1\}^l \rightarrow \{0, 1\}^k, s \in S\}$ be an $(M, b, \delta)$-balanced UHF. For each message $M \in M$ and seed $S \in S$, let channel input $X$ be uniformly distributed over $f^{-1}_S(M) := \{v \mid f_S(v) = M\}$. Then, for a uniformly distributed seed $S$ and every $0 \leq \epsilon \leq 1$,

$$\max_{P_M} I(M \wedge Z, S) \leq \frac{(1 + \delta)}{\ln 2} 2^{-(b-I_{\max}(W))} + \epsilon(k + 1).$$

Corollary 4. For the balanced UHF of Lemma 2 and $M, S, X$ as above,

$$\max_{P_M} I(M \wedge Z, S) \leq \frac{2}{\ln 2} 2^{k-(l-I_{\max}(W))} + \epsilon(k + 1).$$

We momentarily allow shared public randomness $S$. 

December 19, 2014 DRAFT
Remark. In the coding scheme of Section III based on a \((\mathcal{M}, b, \delta)\)-balanced UHF, the set \(\mathcal{M}\) plays the role of the set of messages. Therefore, while the size of the code is \(\log |\mathcal{M}| \leq k\), security requires \(k < l - I^\epsilon_{\text{max}}(W)\). In particular, the balanced UHF of Lemma 2 leads a code of size \(|\mathcal{M}| = 2^k - 1\), while the security of this code requires that \(k \ll l - I^\epsilon_{\text{max}}(W)\).

Proof: Consider a random message \(M\) taking values in \(\mathcal{M}\) and with a distribution \(P_M\). We first prove the result without any smoothing, i.e., for \(\epsilon = 0\). Denote by \(X_+\) the set of \(x \in \{0, 1\}^l\) such that for all \(m \in \mathcal{M}\), \(|\{s|f_s(x) = m\}| \neq 0\); therefore, by property 2 of a balanced UHF \(|\{s|f_s(x) = m\}| = 2^k\) for all \(m \in \mathcal{M}, x \in X_+\). We have

\[
I(M \land Z, S) = \mathbb{E}\log \frac{\sum_{x' \in X_+} \omega(Z | x') \mathbb{1} (f_S(x') = M) / |\{v | f_S(v) = M\}|}{\sum_{x \in X_+} \omega(z | x) \mathbb{1} (f_S(x) = m) / |\{v | f_S(v) = m\}|} 
\]

\[
= \sum_{s \in S} 2^{-b} \int_{x \in X_+} \sum_{m \in \mathcal{M}} P_M(m) \omega(z | x) \mathbb{1} (f_s(x) = m) \times \log \frac{\sum_{x' \in X_+} \omega(z | x') \mathbb{1} (f_s(x') = m)}{\sum_{x \in X_+} \omega(z | x) \mathbb{1} (f_s(x) = m)} \mu(dz) 
\]

\[
= \sum_{s \in S} 2^{-b} \int_{x \in X_+} \sum_{m \in \mathcal{M}} P_M(m) \omega(z | x) \mathbb{1} (f_s(x) = m) \times \log \frac{\sum_{x' \in X_+} \omega(z | x') \mathbb{1} (f_s(x') = f_s(x))}{\sum_{x \in X_+} \omega(z | x) \mathbb{1} (f_s(x) = m)} \mu(dz) 
\]

\[
\leq \frac{2^{-b}}{|S|} \int_{x \in X_+} \sum_{m \in \mathcal{M}} P_M(m) \omega(z | x) \mathbb{1} (f_s(x) = m) \times \log \frac{\sum_{s \in S, x' \in X_+} \omega(z | x') \mathbb{1} (f_s(x') = f_s(x))}{\sum_{s \in S, x \in X_+} \omega(z | x) \mathbb{1} (f_s(x) = m)} \mu(dz), 
\]

where the last inequality is by log-sum inequality (cf. Lemma 3.1). Using the balanced UHF properties

\[
\sum_s \mathbb{1} (f_s(x) = m) = 2^k, 
\]

\[
\frac{1}{|S|} \sum_s \mathbb{1} (f_s(x') = f_s(x)) \leq 2^{-k}, \quad x \neq x'. 
\]
Thus,

\[ I(M \wedge Z, S) \leq \frac{2^{-b+b'}}{|S|} \int_Z \sum_{x \in X} \omega(z \mid x) \log \left( \frac{|S|2^{-k} \sum_{x' \neq x} \omega(z \mid x') + |S|\omega(z \mid x)}{2^b \sum_x \omega(z \mid x) + \omega(z \mid x)} \right) \mu(dz) \]

\[ = \frac{2^{-b+b'}}{|S|} \int_Z \sum_{x \in X} \omega(z \mid x) \log \left( \frac{|S| + |S|2^b \sum_x \omega(z \mid x)}{2^b \sum_x \omega(z \mid x)} \right) \mu(dz) \]

\[ \leq \frac{2^{-b+b'}+k}{|S|} \int_Z \sum_{x \in X} \omega(z \mid x) \right) \mu(dz) \]

\[ \leq (1 + \delta)2^{-b+I_{\max}(W)}, \]

where the last three inequalities use \( \log(1 + x) \leq x \) and property 3 of a balanced UHF.

Moving to the case \( \epsilon > 0 \), denote by \( g(W) \) the expression on the right-side of (3). Consider a set \( T \) as in Definition 5. Proceeding as in the proof for the case \( \epsilon = 0 \) we get

\[ g(W_T) \leq (1 + \delta)2^{-b+I_{\max}(W)} \]

and also,

\[ g(W_{T^c}) \leq P((X, Z) \in T^c) \log(1 + 2^k) \leq \epsilon(k + 1). \]

These two inequalities, together with log-sum inequality, yield

\[ I(M \wedge Z, S) = g(W) \]

\[ \leq g(W_T) + g(W_{T^c}) \]

\[ \leq (1 + \delta)2^{-b+I_{\max}(W_T)} + \epsilon(k + 1). \]

The proof is completed upon optimizing \( I_{\max}(W_T) \) over sets \( T \) that satisfy (1). \( \square \)

By Lemma 2 and Corollary 4 we can securely send \( 2^k - 1 \) messages provided \( k \ll l - I_{\max}(W) \). In the coding scheme of the previous section, the channel \( W \) corresponds to \( n \) uses of a memoryless channel with inputs corresponding to the codewords of an ECC. Specifically, denoting by \( e_{0n} : \{0, 1\}^l \rightarrow X^n \) the encoder of an ECC and by \( W_{e_{0n}} : \{0, 1\}^n \rightarrow Z^n \) the combined channel \( W_{e_{0n}}(\cdot \mid v) = W^n(\cdot | e_{0n}(v)) \), the rate loss incurred by the scheme of the previous section is given by \( I_{\max}(W_{e_{0n}}) \) for \( \epsilon = o(1/n) \).

As an illustration, we present in the next result a simple upper bound on \( I_{\max}(W_{e_{0n}}) \) for a DMC \( W \) with finite input and output alphabets.
**Lemma 5.** For any encoder $e_{0n}$ and a DMC $W : \mathcal{X} \to \mathcal{Z}$ with finite input and output alphabets $\mathcal{X}$ and $\mathcal{Y}$, respectively, there exists a constant $c > 0$ such that for $\epsilon_n = e^{-nc}$

$$\limsup_n \frac{1}{n} I_{\max}^{\epsilon_n}(W_{e_{0n}}) \leq \max_{P_{X}} I(X \land Z).$$

**Remark.** In view of the foregoing discussion, using an ECC of rate $l_n/n = R$ in the scheme of the previous section leads to a wiretap code of rate

$$\frac{k_n}{n} = R - \max_{P_{X}} I(X \land Z) - \delta,$$

with semantic security, since for this choice of $k_n$ and $l_n$ the scheme satisfies

$$\max_{P_{M}} I(M \land Z^n, S) \leq 2^{-n\delta + 1} \ln 2 + nR2^{-nc} = o(1).$$

For the particular case of a degraded, symmetric wiretap channel with discrete input and output alphabets, it was shown in [17] that the wiretap capacity is given by $I(X \land Y) - I(X \land Z)$ where $X$ is a uniform distribution. Therefore, if the underlying ECC is any capacity achieving code for the transmission channel $T$, the UHF based scheme constitutes a semantically-secure capacity achieving wiretap code. This extends the results of [3], [4], [23] where the same result was obtained for a restricted choice of ECC.

**Proof:** We first prove the result for a constant composition code where each codeword $e_{0n}(v)$ is of a fixed type $P$, i.e., for $e_{0n}$ such that each element $x \in \mathcal{X}$ appears $nP(x)$ times in every codeword $x^n = e_{0n}(v)$.

Denote by $\mathcal{T}$ the set of sequences $(x^n, z^n)$ such that $z^n$ is $W$-conditionally typical given $x^n$, by $\mathcal{T}_P$ the set of sequences $(x^n, z^n) \in \mathcal{T}$ such that $x^n$ has type $P$, and by $\mathcal{T}_{P,W}$ the projection of $\mathcal{T}_P$ on $\mathcal{Z}^n$ (see [8] for basic notions of type and typical sets). Then, for each $(x^n, z^n) \in \mathcal{T}_P$

$$\log W^n(z^n \mid x^n) \leq -nH(W \mid P) + o(n)$$

and

$$\log |\mathcal{T}_{P,W}| \leq nH(P \circ W) + o(n),$$

where $P \circ W$ denotes the output distribution for channel $W$ when the input distribution is $P$. Since there exists a $c > 0$ such that for all $v$

$$\sum_{z^n,(e_{0n}(v),z^n)\notin \mathcal{T}} W^n(z^n \mid e_{0n}(v)) \leq 2^{-nc},$$
we have

\[ I_{\mathrm{max}}^e(W_{e_0}) \leq I_{\mathrm{max}}(W_{e_0}, \mathcal{T}) \]
\[ = \log \sum z \max_v W^n(z^n | e_0(v)) \mathbb{1} ((e_0(v), z^n) \in \mathcal{T}) \]
\[ \leq -nH(W | P) + \log \sum z \max_v \mathbb{1} ((e_0(v), z^n) \in \mathcal{T}) + o(n) \]
\[ \leq -nH(W | P) + \log |\mathcal{T}_{P,W}| + o(n) \]
\[ \leq nI(P; W) + o(n) \]

which completes the proof for a constant composition code.

Proceeding to the case of a general code, denote by \( C_P \) the set of codewords \( e_0(v) \) of type \( P \). As before, we have

\[ I^e_{\mathrm{max}}(W_{e_0}) \leq I_{\mathrm{max}}(W_{e_0}, \mathcal{T}) \]
\[ = \log \sum z \max_v W^n(z^n | e_0(v)) \mathbb{1} ((e_0(v), z^n) \in \mathcal{T}) \]
\[ \leq \log \sum P \max_z \sum_{x^n \in C_P} W^n(z^n | x^n) \mathbb{1} ((x^n, z^n) \in \mathcal{T}) \]
\[ \leq n \max_{P_X} I(P_X; W) + o(n), \]

where the final inequality is obtained in the manner of (4) upon using the fact that the number of types is polynomial in \( n \) (cf. [8]).

V. Security of the Coding Scheme for a GWC

We now analyze the security of the coding scheme of Section III for a GWC. In view of the previous section, it suffices to bound the smooth max-information \( I^e_{\mathrm{max}}(W_{e_0}) \) for an AWGN \( W \) and ECC \((e_0, d_{0n})\) that satisfies the average power constraint (2).

**Lemma 6.** Let \( W : \mathbb{R} \to \mathbb{R} \) be an AWGN channel with noise variance \( \sigma^2_W \), and let \( e_0 : \{0, 1\}^l \to \mathbb{R}^n \) be an encoder satisfying (2). Then, denoting \( \epsilon_n = e^{-n\delta^2/8} \), it holds for the combined channel \( W_{e_0} \) for every \( 0 < \delta < 1/2 \) that

\[ I_{\mathrm{max}}^e(W_{e_0}) \leq \frac{n}{2} \log \left( 1 + \delta + \frac{P}{\sigma^2_W} \right) - \frac{n\delta}{2} + o(n). \]
Proof: Denote by \( g(z) \) the standard normal density on \( \mathbb{R}^n \). For the set
\[
Z_0 := \left\{ z \in \mathbb{R}^n \left| \frac{1}{n} \|z\|_2^2 - 1 \leq \delta \right. \right\},
\]
the standard measure concentration results for chi-squared RVs (cf. [2, Exercise 2.1.30]) yield
\[
\int_{Z_0} g(z)dz \geq 1 - 2e^{-n\delta^2/8}.
\]
Define \( T \) as the set of sequences \( (x^n, z^n) \) such that the sequence \( z^n - x^n \) belongs to \( Z_0 \). Thus, for each \( x^n \in \mathbb{R}^n \),
\[
W^n(\{z^n | (x^n, z^n) \in T\} | x^n) = \int_{Z_0} g(z)dz \geq 1 - 2e^{-n\delta^2/8}.
\]
Further, let \( T_{P,Z_0} \) denote the set \( \bigcup_{x^n: \|x^n\|_2 \leq nP} \{Z_0 + x^n\} \). We get the following inequalities:
\[
I_{\text{max}}^n(W_{e_0n}) \leq I_{\text{max}}(W_{e_0n,T}) \leq \log \int_{\mathbb{R}^n} \max_v g \left( \frac{z - e_0n(v)}{\sigma_W} \right) \mathbb{1}((e_0n(v), z^n) \in T)dz
\]
\[
\leq \log \frac{e^{-n(1-\delta)^2/2}}{(2\pi \sigma_W^2)^{n/2}} \int_{\mathbb{R}^n} \max_v \mathbb{1}((e_0n(v), z^n) \in T)dz
\]
\[
\leq \log \frac{e^{-n(1-\delta)^2/2}}{(2\pi \sigma_W^2)^{n/2}} \text{vol}(T_{P,Z_0}),
\]
where the second inequality holds since \( z - e_0n(v) \in Z_0 \) and the last since \( e_0n(v) \) satisfy (2) for all \( v \).
Denote by \( B_n(\rho) \) the sphere of radius \( \rho \) in \( \mathbb{R}^n \) and by \( \nu_n(\rho) \) its volume, which can be approximated as (cf. [25])
\[
\nu_n(\rho) = \frac{1}{\sqrt{n\pi}} \left( \frac{2\pi e}{n} \right)^{\frac{n}{2}} \rho^n (1 + O(n^{-1}))
\]
(5)
Note that for \( \rho_n = \sqrt{n \left( \sigma_W^2(1+\delta) + P \right)} \),
\[
T_{P,Z_0} \subseteq B_n(\rho_n).
\]
Therefore, by the inequalities above we get
\[
I_{\text{max}}^n(W_{e_0n}) \leq \log \frac{e^{-n(1-\delta)^2/2}}{(2\pi \sigma_W^2)^{n/2}} \nu_n(\rho_n),
\]
which yields the claimed inequality in view of (5). 

Now, we state our main result.
Theorem 7. Let \((e_{0n}, d_{0n})\) be a sequence of transmission codes of rate \(R\) for the channel \(T\) that satisfy (2) and have the maximum probability of error \(\epsilon(e_{0n}, d_{0n})\) vanishing to 0 as \(n\) goes to \(\infty\). 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 satisfies

\[
\lim_{n \to \infty} \max_{M} I(M \wedge Z^n, S) = 0.
\]

Proof: Consider the balanced UHF of Lemma 2 with \(l = \lfloor nR \rfloor\) and

\[
k_n = \left\lfloor n \left( R - \frac{1}{2} \log \left( 1 + \delta + \frac{P}{\sigma_W^2} \right) - \delta \right) \right\rfloor.
\]

The claim then follows by Corollary 4 and Lemma 6.

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 \(W_s\) 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. [11, 15]).

Theorem 7 shows that in the presence of shared public randomness \(S\), our coding scheme achieves the capacity of a GWC. In the absence of shared public randomness, \(S\) must be communicated via \(T\). In fact, it is possible to send the seed \(S\) over \(T\) with a negligible rate loss. Note that 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 message sent in the \(i\)th 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

$$\epsilon(e_N, d_N) \leq (t_n + 1)\epsilon(e_n, d_n). \quad (6)$$

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

$$I(M_1, \ldots, M_{t_n} \wedge Z^N) \leq \sum_{i=1}^{t_n} I(M_i \wedge Z^n(i), S) \leq \sum_{i=1}^{t_n} I(M_1 \wedge Z^n(1), S). \quad (7)$$

On choosing $t_n \rightarrow \infty$ such that the right-sides of (6) and (7) go to 0, we get the required code $(e_N, d_N)$ of rate

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

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

VI. DISCUSSION

We have shown that the modular coding scheme of [11], [3], [4] achieves the wiretap capacity of a GWC under the semantic-security criterion. Underlying our security analysis is a single-shot bound on the mutual information between the message and the eavesdropper’s observation, when the message is passed through the inverse of a balanced UHF before transmission. This basic result given in Theorem 3 essentially says that the rate-loss incurred due to the presence of a balanced UHF can be bounded above by the rate of the smooth max-information between the message and the eavesdropper’s observation. We saw in Lemma 6 that, for an appropriately chosen smoothing parameter, the smooth max-information rate for an AWGN with codewords satisfying the power constraint (2) is bounded above by the capacity of the AWGN, which in turn shows that the modular scheme achieves the wiretap capacity of a GWC if the underlying ECC is capacity achieving for the AWGN. Similarly, when eavesdropper’s channel $W$ is a DMC, Lemma 5 shows that the smooth max-information rate is bounded above by the capacity of $W$. Therefore, the scheme achieves the wiretap capacity of a discrete, degraded, symmetric wiretap channel if the underlying ECC is capacity achieving for $T$. In [3], [4], [23], the proposed modular scheme was shown to achieve the wiretap capacity of such a wiretap channel with semantic security only when the underlying capacity achieving ECC satisfies the linearity and the separability conditions described in [4]. Our results show that these extra conditions are not needed, and the scheme remains wiretap capacity achieving as long as the underlying ECC is capacity achieving.
ACKNOWLEDGMENTS

The authors would like to thank Shun Watanabe and Masahito Hayashi for discussions that were helpful in clarifying the relation of this work to [12].

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, “Semantic security for the wiretap channel,” CRYPTO, LNCS, vol. 7417, pp. 294–311, 2012.
[5] C. H. Bennett, G. Brassard, C. Crépeau, and U. M. Maurer, “Generalized privacy amplification,” IEEE Trans. Inf. Theory, vol. 41, no. 6, pp. 1915–1923, November 1995.
[6] 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.
[7] I. Csiszar and J. Korner, “Broadcast channels with confidential messages,” IEEE Trans. Inf. Theory, vol. 24, no. 3, pp. 339–348, May 1978.
[8] I. Csizár and J. Körner, Information theory: Coding theorems for discrete memoryless channels. 2nd edition. Cambridge University Press, 2011.
[9] Y. Dodis, R. Ostrovsky, L. Reyzin, and A. Smith, “Fuzzy extractors: How to generate strong keys from biometrics and other noisy data,” SIAM Journal on Computing, vol. 38, no. 1, pp. 97–139, 2008.
[10] M. Hayashi, “General nonasymptotic and asymptotic formulas in channel resolvability and identification capacity and their application to the wiretap channel,” IEEE Trans. Inf. Theory, vol. 52, no. 4, pp. 1562–1575, April 2006.
[11] M. Hayashi and R. Matsumoto, “Construction of wiretap codes from ordinary channel codes,” Proc. IEEE International Symposium on Information Theory, pp. 2538–2542, 2010.
[12] ——, “Secure multiplex coding with dependent and non-uniform multiple messages,” CoRR, vol. abs/1202.1332v3, 2013.
[13] 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.
[14] R. Impagliazzo and D. Zuckerman, “How to recycle random bits,” in Proc. Annual Symposium on Foundations of Computer Science (FOCS), 1989, pp. 248–253.
[15] 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.
[16] H. Krawczyk, “LFSR-based hashing and authentication,” CRYPTO, LNCS, vol. 839, pp. 129–139, 1994.
[17] S. Leung-Yan-Cheong, “On a special class of wiretap channels,” IEEE Trans. Inf. Theory, vol. 23, no. 5, pp. 625–627, 1977.
[18] S. Leung-Yan-Cheong and M. Hellman, “The Gaussian wiretap channel,” IEEE Trans. Inf. Theory, vol. 24, no. 4, pp. 451–456, 1978.
[19] C. Ling and J.-C. Belfiore, “Achieving AWGN channel capacity with lattice gaussian coding,” CoRR, vol. abs/1302.5906, 2014.
[20] C. Ling, L. Luzzi, J.-C. Belfiore, and D. Stehlé, “Semantically secure lattice codes for the gaussian wiretap channel,” *IEEE Trans. Inf. Theory*, vol. 60, no. 10, pp. 6399–6416, Oct 2014.

[21] 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, Oct 2011.

[22] R. Renner, “Security of quantum key distribution,” *Ph.D. Dissertation, ETH Zurich*, 2005.

[23] 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.

[24] A. Thangaraj, S. Dihidar, A. Calderbank, S. McLaughlin, and J. M. Merolla, “Applications of LDPC codes to the wiretap channel,” *IEEE Trans. Inf. Theory*, vol. 53, no. 8, pp. 2933–2945, Aug 2007.

[25] X. Wang, “Volumes of generalized unit balls,” *Mathematics Magazine*, vol. 78, no. 5, 2005.

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