Abstract. It is widely accepted by the information security community that a secrecy criterion based solely on minimizing the rate at which an eavesdropper extracts bits from a block of noisy channel outputs is too weak a concept to guarantee the confidentiality of the protected data. Even if this rate goes to zero asymptotically (i.e. for sufficiently large codeword length), vital information bits can easily be leaked to an illegitimate receiver. In contrast, many of the recent results in information-theoretic security for wireless channel models with continuous random variables rely on this weak notion of secrecy, even though previous work has shown that it is possible to determine the ultimate secrecy rates for discrete memoryless broadcast channels under a stronger secrecy criterion — namely one which bounds not the rate but the total number of bits obtained by the eavesdropper. Seeking to bridge the existing gap between fundamental cryptographic requirements and ongoing research in wireless security, we present a proof for the secrecy capacity of Gaussian broadcast channels under the strong secrecy criterion. As in the discrete memoryless case, the secrecy capacity is found to be the same as in the weaker formulation. The extension to fading channels is shown to be straightforward.

1 An Information-Theoretic Approach to Wireless Security

In contrast to their wireline counterparts, wireless links are exceptionally prone to eavesdropping attacks. As long as the eavesdropper (Eve, here with an antenna) is able to operate a suitable receiver at some location within the transmission range of the legitimate communication partners (Alice and Bob), information about the sent messages may be easily obtained from the transmitted signals and this eavesdropping activity is most likely to remain undetected. While the latter aspect is hard to prevent in wireless systems — in contrast to quantum systems which are known to have a no-cloning property — the former can be countered by (a) using strong end-to-end encryption to protect the confidential data (thus relying on computational security), (b) using secrecy attaining channel codes and signal processing at the physical-layer (exploiting the principles of
information-theoretic security), or (c) combining both solutions in an effective manner.

It is fair to state that cryptographic solutions based on the computational hardness of certain numerical problems have been the object of intense study for several decades, whereas information-theoretic security for wireless channels has only very recently caught the attention of the research community and is still very much at an infant stage. Building on Shannon’s notion of perfect secrecy [16], the information-theoretic foundations for a physical-layer approach to security were first laid by Wyner [19] and later by Csiszár and Körner [3], who proved in seminal papers that there exist channel codes guaranteeing both robustness to transmission errors and a prescribed degree of data confidentiality. An extension to the Gaussian instance of the wiretap channel was promptly provided by Leung-Yan-Cheong and Hellman in [8]. Owing to the basic circumstances that (a) the legitimate receiver must have less noise than the attacker for the secrecy capacity to be strictly positive, (b) secrecy capacity achieving codes were not yet available, and (c) a viable security solution based on public-key cryptography was made available at the same time by Diffie and Hellman [5], these basic results in information-theoretic security were viewed by many as not more than a theoretical curiosity. In [11], Maurer offered a breakthrough by observing that legitimate users can always generate a secret key through public communication over an insecure yet authenticated channel, even when they have a worse channel than the eavesdropper.

It was not until a decade later that information-theoretic concepts found their way into wireless security research. Hero [7] introduced space-time signal processing techniques for secure communication over wireless links, and Negi and Goel [12] investigated achievable secret communication rates taking advantage of multiple-input multiple output communications. Parada and Blahut [14] established the secrecy capacity of various degraded fading channels. Barros and Rodrigues [1] provided a detailed characterization of the outage secrecy capacity of slow fading channels, and they showed that fading alone guarantees that information-theoretic security is achievable, even when the eavesdropper has a better average Signal-to-Noise Ratio (SNR) than the legitimate receiver – without the need for public communication over a feedback channel or the introduction of artificial noise. Practical secret key agreement schemes for this scenario are described by Bloch et al. in [2]. The ergodic secrecy capacity of fading channels was derived independently by Liang et al. [9] and Gopala et al. in [6] and power and rate allocation schemes for secret communication over fading channels were presented. Other recent directions include secure relays and the secrecy capacity of systems with multiple antennas.

No doubt the recent surge in research on information-theoretic security for wireless channels has produced a considerable number of non-trivial results. However, in order to increase their potential cryptographic value it is useful to revisit the most common underlying assumptions. Beyond the fact that code constructions capable of bridging the gap between theory and practice are still elusive, many of the aforementioned contributions have a non-obvious drawback,
which is not necessarily related with the actual solutions but rather with subtle aspects of the problem formulation. Since they make use of the available secrecy results for Gaussian wiretap channels, a number of contributions in wireless information-theoretic security adopt the secrecy condition of the early work of Leung-Yan-Cheong and Helmann in [8] (and similarly [19,4]), which considers only the rate at which an eavesdropper is able to extract bits from a block of noisy channel outputs and not the total amount of information that he is able to obtain. As argued by Maurer and Wolf for discrete memoryless channels [10], the former is too weak a concept to guarantee the confidentiality of the protected data, because even if this rate goes to zero (in the limit of very large codeword length) vital information bits can easily be leaked to an illegitimate receiver. This motivates us to consider the secrecy capacity of wireless channels under the strong secrecy criterion.

1.1 A Case for Strong Secrecy

To underline the importance of a strong secrecy criterion, we now present two different examples. The first one shows a trivial (insecure) scheme that satisfies the weaker condition used in [8], whereas the second example highlights the fact that strong secrecy requires strong uniformity on what the eavesdropper sees.

Example 1. Suppose that Alice wants to send Bob a sequence of \( n \) bits, denoted \( u^n \), which she wants to keep secret from Eve. For simplicity, we assume that all channels are noiseless, which means that both Bob and Eve observe noiseless versions of the cryptogram \( x^n \) sent by Alice. We consider two different (asymptotic) secrecy conditions:

Weak Secrecy: \( \forall \epsilon > 0 \) we have that \( (1/n)H(U^n|X^n) \geq 1 - \epsilon \), for some \( n \) sufficiently large.

Strong Secrecy: \( \forall \epsilon > 0 \) we have that \( H(U^n|X^n) \geq n - \epsilon \), for some \( n \) sufficiently large.

Notice that the difference between these two measures of secrecy is that strong secrecy demands that the total uncertainty about \( u^n \) is arbitrarily close to \( n \) bits, whereas weak secrecy settles for the average uncertainty per bit to be arbitrarily close to 1. As we shall see this seemingly unimportant subtle issue can determine whether Eve is able to extract any information from the cryptogram \( x^n \).

Suppose now that Alice produces the cryptogram \( x^n \) by computing the XOR of the first \( k \) bits \( (u_1, u_2, \ldots, u_k) \), \( 0 < k < n \), with a secret sequence of random bits \( s^k \) and appending the remaining \( n - k \) bits \( (u_{k+1}, u_{k+2}, \ldots, u_n) \) to the cryptogram. The sequence of secret bits \( s^k \), which we assume to be shared via a private channel with Bob, is generated according to a uniform distribution and thus can be viewed as a one-time pad for the first \( k \) bits. Clearly, we have that \( H(U^n|X^n) = n - k \), which proves unequivocally that this trivial scheme does not satisfy the strong secrecy criterion. However, this is no longer true when we accept the weak secrecy criterion. In fact, since \( (1/n)H(U^n|X^n) = 1 - k/n \) Alice may actually disclose an extremely large number of bits, while satisfying the weak secrecy condition.
Example 2. Suppose once again that all channels are noiseless and Alice wants to send Bob a sequence of \( n \) bits, denoted \( u^n \), which she wants to keep secret from Eve. Alice now produces the cryptogram \( x^n \) by computing the XOR of each bit \( u_i \) with a secret random bit \( s_i \), such that \( x^n = u^n \oplus s^n \). The sequence of secret bits \( s^n \), which we assume to be shared via a private channel with Bob, is generated in a way such that the all-zero sequence has probability \( 1/n \) and all non-zero sequences are uniformly distributed. More formally, if \( S^n \) denotes the set of all binary sequences and \( 0^n \) denotes a \( n \)-bit sequence with \( n \) zeros, then the probability distribution of the secret sequence can be written as

\[
P(s^n) = \begin{cases} 
1/n & \text{if } s^n = 0 \\
\frac{(1-1/n)}{2^n} & \text{if } s^n \in S^n \setminus 0^n
\end{cases}
\]

Clearly, since \( s^n \) is not uniformly distributed according to \( P(S^n) = 1/2^{-n} \), Alice’s scheme cannot be classified as a one-time-pad and thus does not satisfy the perfect secrecy condition \( H(U^n | X^n) = n \) established by Shannon. To verify that the aforementioned asymptotic condition for weak secrecy is met by this scheme, we introduce an oracle \( J \) which returns the following values

\[
J = \begin{cases} 
0 & \text{if } s^n = 0 \\
1 & \text{otherwise}
\end{cases}
\]

Using this definition, we may write

\[
(1/n)H(U^n | X^n) \geq (1/n)H(U^n | X^n, J)
\]

\[
= -\sum_{x^n,u^n} p(x^n, u^n, J = 0) \log p(x^n | u^n, J = 0)
- \sum_{x^n,u^n} p(x^n, u^n, J = 1) \log p(x^n | u^n, J = 1).
\]

Since the first term is equal to zero, we can restrict our attention to the second term. Notice that

\[
p(x^n, u^n, J = 1) = p(x^n | u^n, J = 1)p(u^n | J = 1)p(J = 1)
\]

with

\[
p(x^n | u^n, J = 1) = \begin{cases} 
0 & \text{if } x^n = u^n \\
\frac{1}{2^n} & \text{otherwise}
\end{cases}
\]

whereas \( p(u^n | J = 1) = 1/2^n \) and \( p(J = 1) = 1 - 1/n \). It follows that

\[
(1/n)H(U^n | X^n) \geq -\sum_{x^n \neq u^n} \frac{1}{2^n-1} \frac{1}{2^n} (1 - \frac{1}{n}) \log \frac{1}{2^n - 1}
\]

\[
= -(1 - \frac{1}{n}) \log \frac{2^n - 1}{2^n - 1}
\]

\[
= \log 2^n - 1 - \log(2^n - 1)
\]

\[
\geq \log(2^n - 1) - 1.
\]
Thus, we conclude that for any $\epsilon > 0$ there exists an $n_0$ such that $(1/n)H(U^n|X^n) \geq 1 - \epsilon$, and weak secrecy holds.

However, this does not at all imply that strong secrecy can be achieved by this scheme, in fact the following argument proves its failure:

$$\forall \epsilon > 0 \quad H(U^n|X^n) = H(X^n \oplus S^n|X^n)$$
$$= H(S^n|X^n)$$
$$\leq H_b(\alpha)$$
$$= -\frac{1}{n} \log \frac{1}{n} - (2^n - 1) \cdot \left(1 - \frac{1}{n}\right) \log \left(1 - \frac{1}{n}\right)$$
$$= H_b(1/n) + (1 - 1/n) \log(2^n - 1)$$
$$\leq H_b(1/n) + n - 1$$
$$\leq n - 1 + \epsilon, \quad \text{for } n \text{ sufficiently large},$$

where $H_b(\alpha) = -\alpha \log \alpha - (1/\alpha) \log(1/\alpha)$ is the binary entropy function. Although the weak secrecy condition would suggest that this scheme is secure, it follows from our analysis that the eavesdropper can acquire on average at least one bit of information from the cryptogram. A closer inspection reveals that there is actually a non-negligible probability that the eavesdropper is able to obtain the entire information sequence. For example, if $n = 100$ bits, then the per letter entropy of the key becomes $(1/n)H(S^n) = 0.99$, which is very close to 1. However, the all-zero sequence occurs with probability $P(S^n = 0) = 0.01$, which implies that, because of the slight non-uniformity of the key, the eavesdropper has a one in one hundred chance of succeeding — even when the weak secrecy condition is met.

1.2 Contribution

Our contribution is a proof for the secrecy capacity of the Gaussian wiretap channel of [8] under the strong secrecy condition defined in [10]. As in the discrete memoryless case and using similar arguments as in [10], we are able to show that substituting the weak secrecy criterion by the stronger version does not alter the secrecy capacity. Based on this result, it is possible to re-evaluate the cryptographic validity of previous results on information-theoretic security for wireless channels. We believe that both this contribution and the work of Nitinawarat [13] on strong secret key agreement with Gaussian random variables and public discussion are important steps towards adding credibility to physical-layer security schemes based on information-theoretic reasoning (e.g. [18] and [3]).

The remainder of the paper is organized as follows. Section 2 provides a set of basic definitions and states the problem in a formal way. This is followed by a strong secrecy result for the Gaussian channel in Section 3. The paper concludes in Section 4 with a discussion of the implications of this result for the secrecy capacity of wireless fading channels.
2 Problem Statement

We assume that a legitimate user (Alice) wants to send messages to another user (Bob). Alice encodes the message $W \in \{1, \ldots, 2^nR\}$ into the codeword $X^n$. When Alice transmits her codeword, Bob observes the output of a discrete-time Gaussian channel (the main channel) given by

$$Y(i) = X(i) + Z_m(i),$$

where $Z_m(i)$ is a zero-mean Gaussian random variable that models the noise introduced by the channel at time $i$.

A third party (Eve) is also capable of eavesdropping Alice’s transmissions. Eve observes the output of an independent Gaussian channel (the eavesdropper channel) given by

$$Z(i) = X(i) + Z_w(i),$$

where the random variable $Z_w(i)$ represents zero-mean Gaussian noise.

It is assumed that the channel input and the channel noise are independent. The codewords transmitted by Alice are subject to the average power constraint

$$\frac{1}{n} \sum_{i=1}^{n} E[|X(i)|^2] \leq P,$$

and the average noise power in the main and the eavesdropper channels are denoted by $N_m$ and $N_w$, respectively.

Let the transmission rate between Alice and Bob be $R$ and the average error probability $P_{ne} = P(W \neq \hat{W})$, where $W$ denotes the sent message chosen uniformly at random and $\hat{W}$ denotes Bob’s estimate of the sent message. We are interested in the following two notions of secrecy with respect to Eve.

**Definition 1 (Weak Secrecy [19,4]).** We say that the rate $R'$ is achievable with weak secrecy if $\forall \epsilon > 0$ for some $n$ sufficiently large there exists an encoder-decoder pair satisfying $R \geq R' - \epsilon$, $P_{ne} \leq \epsilon$ and

$$(1/n) H[W|Z^n] \geq 1 - \epsilon. \quad (1)$$

**Definition 2 (Strong Secrecy [10]).** We say that the rate $R'$ is achievable with strong secrecy if $\forall \epsilon > 0$ for some $n_0$ such that $n > n_0$ there exists an encoder-decoder pair satisfying $R \geq R' - \epsilon$, $P_{ne} \leq \epsilon$ and

$$H[W|Z^n] \geq n - \epsilon. \quad (2)$$

The weak secrecy capacity $C_{ws}$ of the Gaussian channel corresponds to the maximum rate $R$ that is achievable with weak secrecy. Its value was determined in [8] and can be computed according to

$$C_{ws} = \begin{cases} C_m - C_w & \text{for } N_w > N_m \\ 0 & \text{otherwise.} \end{cases} \quad (3)$$
where
\[ C_m = \frac{1}{2} \log \left( 1 + \frac{P}{N_m} \right) \quad \text{and} \quad C_w = \frac{1}{2} \log \left( 1 + \frac{P}{N_w} \right) \]
denote the capacity of the main and of the eavesdropper’s channel, respectively.

Our goal is to determine the strong secrecy capacity \( C_s \) of the Gaussian channel, defined as the maximum transmission rate at which Bob and Alice can communicate with strong secrecy with respect to Eve.

3 Strong Secrecy Capacity for the Gaussian Channel

3.1 Proof Idea

The main results in information-theoretic security thus far can be roughly divided into two classes: (i) secrecy capacity (or rate-equivocation region) for channel models (e.g. [19]) and (ii) secret key capacity for source models (e.g. [11]).

In the latter case, it is assumed that the legitimate partners may use the noisy channel to generate common randomness and communicate freely over a noiseless authenticated channel in order to agree on a common secret key. Although they are conceptually different, it is useful for our purposes to establish a clear connection between these two classes of problems. Specifically, we shall now show at an intuitive level that secure communication over a wiretap channel can be viewed as a special case of secret key agreement. These notions shall be made precise in the next Section, where we present the proof of our main theorem.

According to Shannon, “the fundamental problem of communication is that of reproducing at one point either exactly or approximately a message selected at another point” [16]. Suppose that communication in the source model occurs only in one direction, namely from Alice to Bob. In this case, Alice will know beforehand which secret key Bob will generate from the noisy channel outputs, because, knowing the side information sent by Alice, Bob is going to recover with overwhelming probability the exact same random sequence that is available to Alice at the start of the secret key agreement scheme. Thus, simply by carrying out the key generation process on her random sequence, Alice can construct the actual secret key before transmitting any data to Bob.

If we disregard complexity issues (which are of no importance in information-theoretic reasoning), then there is nothing preventing Alice from generating all possible secret keys beforehand. In other words, she can take all random sequences and run the key generation process. The set of secret keys that she can generate in this manner can be viewed as the set of messages that she can convey to Bob reliably and securely (in the Shannon sense on both counts).

3.2 Main Result

Our main result, whose proof follows [10] closely with the necessary adaptations for the Gaussian channel, is summarized in the following theorem.
Theorem 1. For the Gaussian channel with power constraint \( P \), we have that \( C_s = C_w \).

We will prove this result using a succession of lemmas.

Lemma 1 (adapted from [10]). Let \( Q \) be a scalar quantizer, and let us assume that the eavesdropper observes \( Z_\Delta = Q(Z) \) instead of \( Z \). Let \( X_\Delta \) be a random variable with \( E[X_\Delta^2] \leq P \) taking only a finite number of (real) values, and let \( p_{X_\Delta} \) denote its probability distribution. All rates \( R_s \) satisfying

\[
R_s \leq \max_{p_{X_\Delta}} [I(X_\Delta; Y) - I(X_\Delta; Z_\Delta)]
\]

are achievable strong secrecy rates.

Proof. The key idea of this lemma is to analyze a simpler channel than the initial Gaussian wiretap channel illustrated in Fig. 1. The assumption that the eavesdropper observes a quantized version of the channel output is merely a mathematical convenience and shall be removed later.

We consider the conceptual channel illustrated in Fig. 2, where, in addition to the Gaussian wiretap channel, Alice has the option of sending messages to Bob over a public authenticated channel with infinite capacity. Furthermore, Alice’s inputs \( X_n \) to the conceptual channel are restricted to discrete random variables, that is random variables whose support is a finite set of \( \mathbb{R} \), and we assume that Eve observes a scalar quantized version \( Z_n \) of the continuous output \( Z^n \) of the channel.

Let \( \epsilon > 0 \) and let \( p_{X_\Delta}(x) \) be a probability mass function on \( \mathbb{R} \). We also define \( R_s = I(X_\Delta; Y) - I(X_\Delta; Z_\Delta) \).

\[ \Box \]

Encoding and decoding procedures.

The coding scheme that we will use to communicate over the channel of Fig. 2 consists of three key ingredients.

1. a wiretap code \( \mathcal{C} \) of blocklength \( n \) and rate \( R_s \) achieving an average probability error \( P_e \leq \epsilon' \) over the main channel and ensuring an equivocation rate \((1/n)H(W|Z^n_\Delta) \geq R_s - \epsilon'\); for \( n \) sufficiently large; the existence of such a code for any \( \epsilon' > 0 \) follows from [19]; we let \( \mathcal{C}^\otimes m \) denote the code obtained by the \( m \)-fold concatenation of \( \mathcal{C} \);

![Fig. 1. Gaussian wiretap channel](image-url)
Fig. 2. Conceptual channel used in proof. Alice’s inputs $X^n_A$ to the Gaussian channels are restricted to discrete random variables and Eve observes a scalar quantized version $Z^n$ of the continuous output $Z^n$ of the channel.

2. a Slepian-Wolf encoder $f : \{0, 1\}^{km} \rightarrow \{0, 1\}^t$ (and its associated decoder $g : \{0, 1\}^t \times \{0, 1\}^{km} \rightarrow \{0, 1\}^{km}$), whose parameters are to be determined later; the existence of such a code follows from [17];

3. an extractor $E : \{0, 1\}^{km} \times \{0, 1\}^d \rightarrow \{0, 1\}^r$ whose parameters are to be determined later (extractors appear also in [10]); by enumerating all the values of $E$ over $\{0, 1\}^{km} \times \{0, 1\}^d$, it is possible to associate to each sequence $w^r \in \{0, 1\}^r$ a set $S(w^r) \subset \{0, 1\}^{km} \times \{0, 1\}^d$, such that

$$\forall w^{km}, w^d \in \{0, 1\}^{km} \times \{0, 1\}^d \quad E(w^{kr}, w^d) = w^r;$$

In order to transmit a sequence $w^r$, Alice performs the following encoding procedure.

1. select a pair $(w^{km}, w^d)$ uniformly at random in $S(w^r)$;
2. transmit $w^d$ over the public authenticated channel;
3. send $f(w^{km})$ obtained with the Slepian-Wolf encoder over the public authenticated channel;
4. encode $w^{km}$ according to the code $C^{\otimes m}$ and transmit the resulting codeword over the wiretap channel.

At the receiver, Bob decodes its information by performing the following operations.

1. retrieve $w^d$ and $f(w^{km})$ from the public channel;
2. estimate $\hat{w}^{km}$ from the output of the wiretap channel according to the wiretap code $C^{\otimes m}$;
3. decode $\hat{w}^{km} = g(\hat{w}^{km}, f(w^{km}))$;
4. estimate $\hat{w}^r = E(\hat{w}^{km}, w^r)$;

In the remainder of this section, the random variables corresponding to the sequences $w^{km}, \hat{w}^{km}, w^r, \hat{w}^r, and w^d$ are denoted by $W^{km}, \hat{W}^{km}, W^r, \hat{W}^r,$ and $W^d$, respectively.
\[\min-\text{entropy} H = \text{the sequences}\]

Letting \( P_{\epsilon|m} = P \left[ W_{km} \neq \hat{W}_{km} \right] \) denote the average probability of error of achieved by the code \( C_{\epsilon|m} \), we immediately have by the union bound:

\[ P_{\epsilon|m} \leq mP_e \leq me'. \]

From [17] (see also [10] Lemma 1), for \( m \) large enough, there exist an encoding function \( f : \{0,1\}^{km} \rightarrow \{0,1\}^t \) and a decoding function \( g : \{0,1\}^{km} \times \{0,1\}^t \rightarrow \{0,1\}^{km} \) such that

\[ t \leq H(W_{km}|W_{km}) (1 + \epsilon') \]

and

\[ P \left[ W' \neq W^r \right] = P \left[ W_{km} \neq g \left( f (W_{km}) , \hat{W}_{km} \right) \right] < \epsilon. \]

Note that by Fano’s inequality we have

\[ t \leq (kP_{\epsilon|m} + 1) (1 + \epsilon') = (mke' + 1) (1 + \epsilon'). \]

\[ \square \] Analysis of probability of error.

By definition of the wiretap code \( C \), we have that \( H(W^k|Z^n_\Delta) > n \left( R_s - \epsilon' \right) \). The following results states that if \( m \) is large enough, the inequality also holds for the min-entropy \( H_\infty \).

Formally, let \( \delta > 0 \) and let \( \mathcal{F}(\delta) \) denote the event that the sequences \( w_{km} \) and \( (w_{km}, z_{\Delta}^{nm}) \) are \( \delta \)-typical, and that \( z_{\Delta}^{nm} \) is such that the probability taken over \( w_{km} \) according to the distribution \( p(w_{km}|Z_\Delta^n = z_{\Delta}^{nm}) \) that \( (w_{km}, z_{\Delta}^{nm}) \) is \( \delta \)-typical is at least \( 1 - \delta \). Then, from [10] Lemma 6 we have

\[ m \left( 1 - P(\mathcal{F}(\delta)) \right) \rightarrow 0 \quad \text{as} \quad m \rightarrow \infty, \]

\[ H_\infty(W_{km}|Z_\Delta^{nm}, \mathcal{F}(\delta)) \geq m \left( H(W^k|Z^n_\Delta) - 2\delta \right) + \log(1 - \delta), \]

\[ \geq mn \left( R_s - \epsilon' - \frac{2\delta}{m} \right) + \log(1 - \delta). \]

Taking into account the messages disclosed over the public channel we have by [10] Lemma 10 that with probability at least \( 1 - 2^{-\log mn} \)

\[ H_\infty(W_{km}|Z_\Delta^{nm}, f(W_{km}), \mathcal{F}(\delta)), \]

\[ \geq mn \left( R_s - \epsilon' - \frac{2\delta}{m} \right) + \log(1 - \delta) - (mke' + 1) (1 + \epsilon') - \log m, \]

\[ \geq \frac{3}{4} mnR_s(1 - \eta) \quad \text{where} \quad \eta \rightarrow 0 \quad \text{as} \quad n \rightarrow \infty. \]

From [10] Lemma 9, for any \( \alpha, \eta' > 0 \) and sufficiently large \( m \), we can choose \( E : \{0,1\}^{km} \rightarrow \{0,1\}^t \) with \( d \leq \alpha km \) and \( r \geq (R_s(1 - \eta) - \eta') mn \) such that

\[ H(E(W_{km},W^d)|W^d, f(W^km), \mathcal{F}(\delta)) \geq r - 2^{-\left( mn \right)^{1/2 - \alpha(1)}}. \]

Hence, for \( m \) sufficiently large, the overall code achieves an equivocation

\[ H (W^r|W^d, f(W^km)) \geq H(E(W_{km},W^d)|W^d, f(W^km), \mathcal{F}(\delta))(1 - \delta) \geq r - \epsilon, \]

\[ \square \] Analysis of equivocation.
with a communication rate $R = r/(mn) \geq R_s - \epsilon$ over the wiretap channel, and the transmission of
\[
\alpha kn + (mk\epsilon' + 1)(1 + \epsilon') + \log m \overset{\mathcal{A}}{=} \eta_3 mn
\]
bits over the public channel, where $\eta_3 \to 0$ as $n \to \infty$. Notice that the public messages could be transmitted error-free over the wiretap channel itself (using for instance a capacity-approaching code) at a negligible cost in terms of overall transmission rate.

Therefore, $R_s = I(X_\Delta; Y) - I(X_\Delta; Z_\Delta)$ is an achievable strong secrecy rate.

The following lemma shows that restricting the eavesdropper’s observations to quantized values is merely a mathematical convenience.

**Lemma 2.** If the eavesdropper does not quantize his observations, all rates $R_s$ satisfying
\[
R_s \leq \max_{P_X} \left[ I(X_\Delta; Y) - I(X_\Delta; Z_\Delta) \right]
\]
are achievable strong secrecy rates.

**Proof.** The proof relies heavily on the measure-theoretic definition of entropy, as described in [15]. We refer the reader to the above reference for a precise definition of entropy and information in this case.

Let us first introduce a family of scalar quantizers as follows. If $I$ is an interval of $\mathbb{R}$, we denote its indicator function by $1_I$. For any $j \geq 1$, let $\{I_j^k : k \in \{1, \ldots, 2^j\}\}$ be the unique set of disjoint intervals of $\mathbb{R}$, symmetric around 0, such that for all $k$, $P_Z(I_j^k) = \frac{1}{2^j}$. For each $I_j^k$, define as $x_j^k$ the middle point of $I_j^k$. The quantizer $Q_j$ is defined as follows.

\[
Q_j : \mathbb{R} \rightarrow \mathbb{R} : z \mapsto \sum_{k \in \{1, \ldots, 2^j\}} x_j^k 1_{I_j^k}.
\]

By construction, the knowledge of $Q_j(z)$ allows to reconstruct the values of $Q_j(z)$ for all $j \in \{0, \ldots, n\}$.

Let us now consider a suboptimal eavesdropper who would quantize the continuous output of the channel $Z$ using the family of quantizers $\{Q_j\}_{j \geq 0}$. The random variables $Q_j(Z)$ resulting from the quantizations are denoted by $\tilde{Z}_j$. By construction, the sequence $Z_\Delta$ converges almost surely to the random variable $Z$ as $j \rightarrow \infty$. Therefore, we have:

\[
H(W|Z^n) \overset{(a)}{=} H(W|\{Z_\Delta^n\}_{j \geq 0}),
\]

\[
\overset{(b)}{=} H(W|\{Z_\Delta^n\}_{j \geq 0}),
\]

\[
\overset{(c)}{=} \lim_{k \rightarrow \infty} H(W|\{Z_\Delta^n\}_{0 \leq j \leq k}),
\]

\[
\overset{(d)}{=} \lim_{k \rightarrow \infty} H(W|Z_\Delta^n),
\]

where
where (a) follows from \cite[Corollary (b) p. 48]{15}, (b) follows from the almost sure convergence of $\{Z^n_{\Delta}\}$, (c) follows from \cite[Theorem 3.10.1]{15} and the fact that $W$ takes only a finite number of values, and (d) follows from \cite[Corollary (b) p. 48]{15}.

For any $k$, since $I(X_\Delta; Z_{\Delta_k}) \leq I(X_\Delta; Z)$, Lemma 1 guarantees that, for any $p_{X_\Delta}$, there exists a code achieving a rate $R_s = I(X_\Delta; Y) - I(X_\Delta; Z)$ and ensuring an equivocation $H(W|Z_{\Delta_k})$ arbitrarily close to $nR_s$. As a consequence of the above equalities, for any $\epsilon > 0$, there exists $k_0$ sufficiently large and a code designed assuming that the eavesdropper quantizes his observations with $Q_{k_0}$ such that

$$H(W|Z^n) \geq H(W|Z^n_{\Delta_k}) - \epsilon,$$

which concludes the proof.

**Lemma 3.** The weak secrecy capacity is an achievable strong secrecy rate.

**Proof.** Let $G$ be a Gaussian random variable with zero mean and variance $P$. Let $Q_j$ be the quantizer defined as in Lemma 2 (by replacing $Z$ by $G$). Notice that we can always choose the quantized values in such a way that the random variable $G_{\Delta_j} = Q_j(\Delta)$ satisfies the power constraint; hence, $I(G_{\Delta_j}; Y) - I(G_{\Delta_j}; Z)$ is an achievable strong secret key rate. Following the same approach as in the proof of Lemma 2, one can show that for any $\epsilon > 0$, there exists $k_0$ sufficiently large such that

$$I(G_{\Delta_{k_0}}; Y) \geq \frac{1}{2} \log(1 + \frac{P}{N_m}) - \epsilon$$

and

$$I(G_{\Delta_{k_0}}; Z) \leq \frac{1}{2} \log(1 + \frac{P}{N_w}).$$

Consequently, for any $\epsilon > 0$

$$R_s = \frac{1}{2} \log(1 + \frac{P}{N_m}) - \frac{1}{2} \log(1 + \frac{P}{N_w}) - \epsilon$$

is an achievable strong secrecy rate.

**Lemma 4.** For the Gaussian wiretap channel, the strong secrecy capacity is equal to the weak secrecy capacity.

**Proof.** By definition, the strong secrecy capacity cannot exceed the weak secrecy capacity; therefore all achievable strong secrecy rates are upper bounded by the weak secrecy capacity.

### 4 Implications for Fading Channels

Having established the strong secrecy capacity of the Gaussian Wiretap Channel, the next natural question is how this affects the fundamental security limits of wireless channels. More specifically, we consider the scenario in which Bob and Eve observe the outputs of a discrete-time Rayleigh fading channel (the main channel) given by

$$Y_m(i) = H_m(i)X(i) + Z_m(i),$$
and (the eavesdropper’s channel) given by

\[ Y_w(i) = H_w(i)X(i) + Z_w(i), \]

respectively. Here, \( H_m(i) \) and \( H_w(i) \) are circularly symmetric complex Gaussian random variables with zero-mean and unit-variance representing the main channel and eavesdropper’s channel fading coefficient, respectively. \( Z_m(i) \) and \( Z_w(i) \) denote zero-mean circularly symmetric complex Gaussian noise random variables. We further assume that the codewords transmitted by Alice are subject to the average power constraint

\[ \frac{1}{n} \sum_{i=1}^{n} \mathbb{E} \left[ |X(i)|^2 \right] \leq P, \]

and the average noise powers in the main channel and the eavesdropper’s channel are denoted by \( N_m \) and \( N_w \), respectively. The channel input, the channel fading coefficients, and the channel noises are all independent.

There are two cases of interest:

1. The main channel and the eavesdropper’s channel are quasi-static fading channels, that is the fading coefficients, albeit random, are constant during the transmission of an entire codeword (\( \forall i = 1, \ldots, n \) \( H_m(i) = H_m \) and \( H_w(i) = H_w \)) and, moreover, independent from codeword to codeword. This corresponds to a situation where the coherence time of the channel is large \([2]\);

2. The main channel and the eavesdropper’s channel are ergodic fading channels, that is the fading coefficients are drawn randomly in an independent and identically distributed fashion for each transmitted symbol, which corresponds to a situation where the coherence time of the channel is short \([9]\).

In both cases, the secrecy capacity is generically computed by assuming in the first case that every particular fading realization corresponds to one instance of the Gaussian wiretap channel, and in the second case that delay plays no role and so the encoder can wait as long as necessary to have enough identical fading realizations to be able to encode as if it was transmitting over the corresponding instance of the Gaussian wiretap channel.

Close inspection of the proofs shows that in both cases we can safely substitute the weak secrecy capacity achieving random code construction by the strong secrecy construction we presented in the previous section and obtain the strong secrecy capacity for both slow fading (as in \([12]\)) and ergodic fading channels (as in \([9]\)).

References