entropy

Article

# Stealthy Secret Key Generation

Pin-Hsun Lin [1,*], Carsten R. Janda [1], Eduard A. Jorswieck [1] and Rafael F. Schaefer [2]

[1] Information Theory and Communication Systems Department, Technische Universität Braunschweig, 38106 Braunschweig, Germany; Janda@ifn.ing.tu-bs.de (C.R.J.); Jorswieck@ifn.ing.tu-bs.de (E.A.J.)
[2] Information Theory and Applications Chair, Technische Universität Berlin, 10623 Berlin, Germany; rafael.schaefer@tu-berlin.de
* Correspondence: Lin@ifn.ing.tu-bs.de

Received: 1 June 2020; Accepted: 15 June 2020; Published: 18 June 2020

**Abstract:** In order to make a warden, Willie, unaware of the existence of meaningful communications, there have been different schemes proposed including covert and stealth communications. When legitimate users have no channel advantage over Willie, the legitimate users may need additional secret keys to confuse Willie, if the stealth or covert communication is still possible. However, secret key generation (SKG) may raise Willie's attention since it has a public discussion, which is observable by Willie. To prevent Willie's attention, we consider the source model for SKG under a strong secrecy constraint, which has further to fulfill a stealth constraint. Our first contribution is that, if the stochastic dependence between the observations at Alice and Bob fulfills the strict more capable criterion with respect to the stochastic dependence between the observations at Alice and Willie or between Bob and Willie, then a positive stealthy secret key rate is identical to the one without the stealth constraint. Our second contribution is that, if the random variables observed at Alice, Bob, and Willie induced by the common random source form a Markov chain, then the key capacity of the source model SKG with the strong secrecy constraint and the stealth constraint is equal to the key capacity with the strong secrecy constraint, but without the stealth constraint. For the case of fast fading models, a sufficient condition for the existence of an equivalent model, which is degraded, is provided, based on stochastic orders. Furthermore, we present an example to illustrate our results.

**Keywords:** secret key generation; source model; stealthy communications; covert communications; channel resolvability; conceptual wiretap channel; stochastically degraded; stochastic orders

## 1. Introduction

Consider the following motivating example. Two agents, Alice and Bob, want to establish a communication that does not raise the curiosity of a warden Willie, whose duty is to monitor if there is any suspicious activity and also decrypts the data. In order to realize a confidential transmission for such a scenario, we may adopt the following two steps. The first step is to make Willie unaware of the existence of the meaningful communication, which is embedded in the messages intended to be delivered to Bob. In contrast, in a meaningless communication, Bob does not care about the received signal, which is only used to confuse Willie. If Willie can successfully detect the existence of the meaningful transmission, then the second step is to use wiretap coding [1] to provide secrecy (or hidability [2]). There are two main concepts to attain the goal of the first step: (1) communications with a stealth constraint [2,3] and (2) communications with a covert constraint [2,4,5]. Both concepts make Willie unable to differentiate between the existence or nonexistence of the meaningful transmission, solely according to the probability distributions of his observations. More specifically, in the first concept, we transmit meaningful and meaningless signals non-overlapped in time. Note that the meaningful signal is the one Alice wants to communicate with Bob, while the meaningless signal is used to confuse Willie. If well designed, Willie cannot differentiate between those two signals, because the induced output distributions are close (the closeness can be defined in several different ways, e.g., by total variational distance, divergence, etc.) to each other. In the second concept, the meaningful signal can be superimposed on the meaningless one. Under the stealth constraint, we can have a positive capacity, while the covert transmission rate is zero, asymptotically. Even though the transmission rate of the second concept is in general zero, asymptotically, the second order rate is positive following the square root law [5,6].

For the aforementioned two concepts, if the channel between Alice and Bob (denoted by Bob's channel in the following) is no better than the channel between Alice and Willie (denoted by Willie's channel in the following), we need additional keys to conceal the meaningful signals, e.g., [4,5]. In particular, these additional keys are used to choose between codebooks to fool Willie. Our motivation is to design an achievable scheme for the source model secret key generation (SKG) for the above scenario, i.e., Bob has no channel advantage over Willie, while fulfilling both the security and stealth constraints, simultaneously. Note that the keys generated from the stealthy SKG can also be used to protect the data on top of concealing the behavior of transmission, e.g., encryption/one-time pad, etc. Note also that our design goal is violated if we directly apply common SKG schemes [7]. This is because common SKG schemes use public communications for several important operations including advantage distillation, information reconciliation, and privacy amplification ([7] Chapter 4.3).Without subtle modifications, these operations will raise Willie's curiosity. To attain our objective, we focus on stealthy SKG, which is from its counterpart, stealth communications [3]. The main reason not to consider covertness but stealth for the SKG is that, under the assumption of a noiseless public discussion channel, there is no ambient noise to hide the discussion signal. Instead, covert SKG may be feasible if there is a noisy public channel. In addition, in general, the covert SKG suffers a sub-linear rate, e.g., [8], which is inherited from the covert communications. Recall that a channel-model SKG with a rate-unlimited public channel was considered in [8]. The authors applied the scheme from covert communication to the key transmission, while a stealth-like public discussion was used.

The main contributions of this work are summarized in the following:

- We investigate a source-model SKG under strong secrecy with an additional stealth constraint.
- We derive an achievable secret key (SK) rate under the stealth constraint, if $I(X;Y) \geq I(X;Z)$, where $X$, $Y$, and $Z$ are the observations of the common randomness source at Alice, Bob, and Willie, respectively. Moreover, if $(X,Y,Z)$ form a Markov chain $X - Y - Z$, then the SK capacity with the additional stealth constraint can be achieved without extra cost, compared to the SKG without the stealth constraint.
- We prove that a sufficient condition to achieve the stealthy SK capacity can be relaxed from the physically degraded channel to a stochastically degraded one.
- A sufficient condition for the existence of an equivalent degraded model is derived by the usual stochastic order [9], which is for the fast fading Gaussian Maurer's (satellite) model [10].

Notation: Lower case bold letters denote deterministic vectors, and upper case normal/bold letters denote random variables/random vectors (or matrices), which will be defined when they are first mentioned. We denote the probability mass function (pmf) by $P$. The entropy of $X$ is denoted as $H(X)$. The mutual information between two random variables $X$ and $Y$ is denoted by $I(X;Y)$. The divergence between distributions $P_X$ and $P_Y$ is denoted by $\mathbb{D}(P_X||P_Y)$. $X \sim F$ denotes that the random variable $X$ follows the distribution $F$, while $\bar{F} \triangleq 1 - F$. The subscript $i$ in $X_i$ denotes the $i$th symbol, and $X^i \triangleq [X_1, X_2, \cdots, X_i]$. $X - Y - Z$ denotes the Markov chain. $\lceil \cdot \rceil$ denotes the ceiling operator. All logarithms are to base two. $(a)^+ \triangleq \max(a, 0)$.

The rest of the paper is organized as follows. In Section 2, we introduce the preliminaries and the considered system model. In Section 3, we derive our main results. Finally, Section 4 concludes this paper.

## 2. Preliminaries and System Model

### 2.1. Preliminaries

We first introduce some necessary definitions and results to develop our work.

**Definition 1.** *The strong secrecy and the stealth constraints are respectively defined as:*

$$\mathbb{D}(P_{MZ^n}||P_M P_{Z^n}) \leq \epsilon,$$
$$\mathbb{D}(P_{Z^n}||Q_{Z^n}) \leq \epsilon,$$

*for arbitrarily small $\epsilon > 0$, where $M$, $Z^n$, $P_{Z^n}$, and $Q_{Z^n}$ are transmitted messages, the observed signal at Willie, and the output distributions at Willie induced by meaningful and meaningless signals, respectively.*

The second constraint in the above definition can be explained by hypothesis testing as discussed in [3]. By this viewpoint, if the second constraint is fulfilled, the adversary's best strategy is to blindly guess whether the current transmitted signal is meaningful or meaningless.

**Definition 2.** *Denote a common random source as $(\mathcal{X}, \mathcal{Y}, \mathcal{Z}, P_{XYZ})$, where $\mathcal{X}$, $\mathcal{Y}$, and $\mathcal{Z}$ are the alphabets of the observations at Alice, Bob, and Willie. The random source is stochastically degraded, if the marginal distributions $P_{Y|X}$ and $P_{Z|X}$ are identical to those of another source of common randomness $(\mathcal{X}, \mathcal{Y}, \mathcal{Z}, P_{X\tilde{Y}\tilde{Z}})$ following the physical degradedness, i.e., $X - \tilde{Y} - \tilde{Z}$.*

**Corollary 1.** *The same marginal property for one transmitter ([11] Theorem 13.9) Consider a discrete memoryless multiuser channel including one transmitter and two non-cooperative receivers with input and output alphabets $\mathcal{X}$ and $\mathcal{Y} \times \mathcal{Z}$, respectively. The capacity region of such a channel depends only on the conditional marginal distributions $P_{Y|X}$ and $P_{Z|X}$ and not on the joint conditional distribution $P_{Y,Z|X}$, where $X \in \mathcal{X}$ and $Y \in \mathcal{Y}$ and $Z \in \mathcal{Z}$ are the transmit signal and the two receive signals, respectively.*

**Definition 3.** *$\delta$-robust typicality ([12] Appendix)*
*The sequence $x^n \in \mathcal{X}^n$ is $\delta$-robust typical for $\delta > 0$:*

$$T_{\delta}^{(n)}(P_X) = \left\{ x^n \in \mathcal{X}^n : \left| \frac{N(a|x^n)}{n} - P_X(a) \right| \leq \delta P_X(a), \forall a \in \mathcal{X} \right\}, \tag{1}$$

*where $N(a|x^n)$ is the number of occurrences of $a$ in $x^n$.*

**Definition 4.** *([9] (1.A.3) For random variables $A$ and $B$, $A \leq_{st} B$ if and only if $\bar{F}_A(a) \leq \bar{F}_B(a)$ for all $a$.*

Let $A =_{st} A'$ denote that $A$ and $A'$ have the same distribution.

**Lemma 1.** *Coupling [13]: $A \leq_{st} B$ if and only if there exists random variables $\hat{A} =_{st} A$ and $\hat{B} =_{st} B$ such that $\hat{A} \leq \hat{B}$ almost surely.*

### 2.2. System Model

The considered system model is shown in Figure 1. We denote the $n$-time source observations at Alice, Bob, and Willie by $X^n$, $Y^n$, and $Z^n$, respectively, which follow the independent and identically distributed (i.i.d.) joint distribution $P_{X^nY^nZ^n} = \prod_{i=1}^{n} P_{X_iY_iZ_i} = \prod_{i=1}^{n} P_{XYZ}$ with alphabets $\mathcal{X}$, $\mathcal{Y}$, $\mathcal{Z}$, respectively. The public discussion between Alice and Bob through a noiseless channel is denoted by a random vector $F^n \in \mathcal{F}^n$. We consider the case without rate limitation on the public discussion channel. Willie can perfectly observe $F^n$. The joint distributions of the signals that Willie can observe when the SKG is meaningful and meaningless are denoted by $P_{F^nZ^n}$ and $Q_{F^nZ^n}$, respectively. Alice and Bob aim at sharing keys $K \in \mathcal{K}$ satisfying the constraints as follows:

$$\mathbb{P}_e \triangleq \Pr(K \neq \hat{K}) \leq \epsilon, \tag{2}$$
$$\log|\mathcal{K}| - H(K) \leq \epsilon, \tag{3}$$
$$\mathbb{D}(P_{KZ^nF^n}||P_K P_{Z^nF^n}) \leq \epsilon, \tag{4}$$
$$\mathbb{D}(P_{F^nZ^n}||Q_{F^nZ^n}) \leq \epsilon \tag{5}$$

for arbitrarily small $\epsilon > 0$, where (2) is the error probability having different keys at Bob from Alice, (3) is the keys' uniformity constraint, while $|\mathcal{K}|$ is the number of keys and (4) is the constraint for the strong secret key, which is an adaptation from the stealth communication in Definition 1. In particular, $K$ is dual to $M$, and $Z^nF^n$ is dual to $Z^n$. The stealth constraint is considered in (5), which is again an adaptation from Definition 1, i.e., here, $F^nZ^n$ is what Willie can observe, instead of solely $Z^n$ in stealth communications.

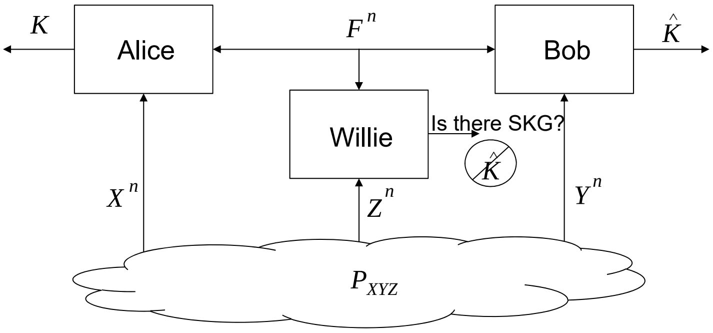

**Figure 1.** The system model of the considered stealthy secret key generation (SKG).

**Definition 5.** *The rate of the keys generated fulfilling* (2)–(5) *is called the achievable stealthy strong SK rate.*

**Definition 6.** *The maximum achievable stealthy strong SK rate is called the stealthy strong SK capacity.*

## 3. Main Results

We show two main result in this section: (1) the stealthy strong SK rate and a condition to attain the capacity; (2) a scheme to identify the fast fading Gaussian Maurer's model as a degraded one, so that the stealth SK capacity can be determined explicitly.

### 3.1. Stealthy Strong Secret Key Rate and Capacity

Our main result is described by the following theorem followed by discussions.

**Theorem 1.** *If $(X, Y, Z)$ drawn from the common random source $(\mathcal{X}, \mathcal{Y}, \mathcal{Z}, P_{XYZ})$, then the stealthy strong SK capacity $C_{SK}$ of source model SKG with the stealth constraint can be bounded by:*

$$\max\{I(X;Y) - I(X;Z),\ I(Y;X) - I(Y;Z)\} \leq C_{SK} \leq \min\{I(X;Y|Z),\ I(X;Y)\}. \tag{6}$$

*Furthermore, if $(X, Y, Z)$ forms a Markov chain $X - Y - Z$, the stealthy strong SK capacity is:*

$$C_{SK} = I(X;Y) - I(X;Z). \tag{7}$$

### *3.2. Sufficient Conditions for a Degraded Common Randomness*

In this section, we derive a sufficient condition to obtain $C_{SK} = I(X;Y) - I(X;Z)$. In particular, we show that this sufficient condition, i.e., the common randomness forming a Markov chain $X - Y - Z$, can be relaxed to be stochastically degraded. After that, we show that this relaxed condition can be satisfied under a quite common setting by, e.g., the fast fading Gaussian Maurer's (satellite) model [10]. In particular, a central random source $S_0$ emits signals passing through fast fading additive white Gaussian noise (AWGN) channels, which are observed as $X$, $Y$, and $Z$ at Alice, Bob, and Willie, respectively.

**Theorem 2.** *If a common random source* $(\mathcal{X}, \mathcal{Y}, \mathcal{Z}, P_{X\tilde{Y}\tilde{Z}})$ *is stochastically degraded such that* $P_{\tilde{Y}|X} = P_{Y|X}$ *and* $P_{\tilde{Z}|X} = P_{Z|X}$, *where* $X - Y - Z$, *then:*

$$C_{SK} = I(X;Y) - I(X;Z). \tag{8}$$

The proof is delegated to Appendix C.

Example: Consider the fast fading Gaussian Maurer's (satellite) model [10] as a special case of Theorem 2:

$$X = A_X S_0 + N_X, \tag{9a}$$
$$Y = A_Y S_0 + N_Y, \tag{9b}$$
$$Z = A_Z S_0 + N_Z, \tag{9c}$$

where $N_X$, $N_Y$, and $N_Z$ are independent AWGNs at Bob and Willie, respectively, while both are with zero mean and unit variance; $A_X$, $A_Y$, and $A_Z$ follow CDFs $F_X$, $F_Y$, and $F_Z$, respectively, and are the i.i.d. fast fading channel gains from the source $S_0$ to Alice and Willie, respectively. Note that intuitively, $X$, $Y$, and $Z$ have no degradedness relation in general due to the random fading. This is because, by the definition of degradedness, the trichotomy order of all realizations between the two fading channels within a codeword length should be the same. We can invoke the same marginal property [14] to construct an equivalent channel, wherein by imposing the usual stochastic order constraint, we can identify those fading channels that can be re-ordered in the equivalent channel to keep the trichotomy order fixed.

If the random channels $A_X$ and $A_Z$ fulfill $\bar{F}_{A_X^2}(x) \geq \bar{F}_{A_Z^2}(x)$ for all $x$, where the subscripts denote the absolute square of the channel magnitudes, then from Lemma 1, we have equivalent (in the sense of having the same stealthy SK capacity) observations at Bob and Willie as $\hat{Y} = \hat{A}_X S_0 + N_Y$ and $\hat{Z} = \hat{A}_Z S_0 + N_Z$, respectively, where $\hat{A}_X^2 \geq \hat{A}_Z^2$ almost surely. Therefore, it is clear that $\bar{F}_{A_X^2}(x) \geq \bar{F}_{A_Z^2}(x)$ is a relaxed sufficient condition to guarantee that $Z$ is an equivalently stochastically degraded version of $Y$.

Assume that $A_X$ and $A_Z$ in Equations (9a)–(9c) are fast fading magnitudes following the Nakagami-$m$ distribution with shape parameters $m_x$ and $m_z$ and spread parameters $w_x$ and $w_z$ [15], respectively. From Theorem 2, we know that $Z$ is a degraded version of $X$ if:

$$\gamma\left(m_x, \frac{m_x}{w_x}x\right)\Gamma(m_z) \geq \gamma\left(m_z, \frac{m_z}{w_z}x\right)\Gamma(m_x), \forall x,$$

where $\gamma(s,x) = \int_0^x t^{s-1}e^{-t}dt$ is the incomplete gamma function and $\Gamma(s) = \int_0^\infty t^{s-1}e^{-t}dt$ is the ordinary gamma function. An example satisfying the above inequality is $(m_x, w_x) = (1,3)$ and $(m_z, w_z) = (1,2)$.

## 4. Conclusions

In this work, we analyzed the performance of the secret key generation from a common random source, which satisfied the additional constraint that the generation of keys should not invoke the warden Willie's attention. Our results showed that compared to the normal SKG, the additional stealth constraint could be fulfilled without extra cost. In particular, the stealthy SK capacity with strong secrecy constraint is $I(X;Y) - I(X;Z)$, if the common random source satisfies $I(X;Y) \geq I(X;Z)$. To emphasize the practical relevance, a sufficient condition was derived to attain the degradedness by the usual stochastic order for the Gaussian Maurer's (satellite) model for the source of common randomness under fast fading. As a final note, we can also use Slepian–Wolf coding with a proper use of the binning code book to derive the same result.

**Author Contributions:** Formal analysis, P.-H.L.; investigation, P.-H.L., C.R.J., and E.A.J.; supervision, E.A.J.; validation, C.R.J. and R.F.S.; writing, review and editing, C.R.J., E.A.J., and R.F.S. All authors have read and agreed to the published version of the manuscript.

**Funding:** The work of Pin-Hsun Lin was supported in part by German Research Foundation (DFG) LI 2886/2-1. The work of Eduard A. Jorswieck was supported in part by DFG, C. Janda was supported by DFG within the project Play Scate (DFG JO 801/21-1). We acknowledge support by the German Research Foundation and the Open Access Publication Funds of the Technische Universität Braunschweig. This work of R. F. Schaefer was supported by the German Federal Ministry of Education and Research (BMBF) within the national initiative for "Post Shannon Communication (NewCom)" under Grant 16KIS1004.

**Acknowledgments:** The authors would like to thank Matthieu Bloch for fruitful discussions and the anonymous reviewers' efforts on Remark 1 and also on improving the quality of the presentation of this paper.

**Conflicts of Interest:** The authors declare no conflict of interest.

## Appendix A. Proof of Theorem 1

Our main idea for deriving the lower bound of the SK capacity in the second scheme is by constructing a conceptual WTC (CWTC) as in [16]. An equivalent wiretap codebook $\{U^n(m,w)\}$ is constructed, where $m = 1, \cdots, L_0$, $w = 1, \cdots, L_1$, $L_0 \triangleq 2^{nR}$ is the number of secure messages, and $L_1 \triangleq 2^{nR_1}$ is the number of confusion messages; $m$ and $w$ are uniformly and independently selected; $U^n(m,w) \in \mathcal{X}^n$, $\forall(m,w)$. In addition, $(Z^n, F^n, U^n)$ are generated according to $P_{Z^nF^nU^n} = \prod_{i=1}^n P_{Z_iF_iU_i} = \prod_{i=1}^n P_{Z_iF_i|U_i}P_{U_i}$, where we consider the equivalent channel from Alice to Willie as:

$$P_{Z^nF^n|U^n} = \prod_{i=1}^{n} P_{Z_iF_i|U_i}, \tag{A1}$$

where $(Z^n,\ F^n)$ is the equivalent channel output at Willie. Similarly, $(Y^n,\ F^n)$ is the equivalent channel output at Bob. We choose $U^n$ mutually independent of $X^n$, $Y^n$, and $Z^n$.

In order to analyze the stealth, the respective distributions of the meaningful and meaningless signals at the equivalent channel output at Willie are:

$$P_{Z^nF^n} = \frac{1}{L_0L_1}\sum_{m=1}^{L_0}\sum_{w=1}^{L_1} P_{Z^n,F^n|U^n}(z^n, f^n|u^n(m,w)), \tag{A2}$$

$$Q_{Z^nF^n} = \sum_{u^n} P_{Z^n,F^n|U^n}(z^n, f^n|u^n)P_{U^n}(u^n). \tag{A3}$$

We first decompose the stealth secrecy constraint as follows:

$$\begin{aligned}
&\mathbb{D}(P_{KZ^nF^n}||P_K P_{Z^nF^n}) + \mathbb{D}(P_{Z^nF^n}||Q_{Z^nF^n})\\
&= \sum_{K,Z^n,F^n} P_{KZ^nF^n}\left(\log\frac{P_{KZ^nF^n}}{P_K P_{Z^nF^n}} + \log\frac{P_{Z^nF^n}}{Q_{Z^nF^n}}\right)\\
&= \sum_{K,Z^n,F^n} P_{KZ^nF^n}\left(\log\frac{P_{KZ^nF^n}}{P_K Q_{Z^nF^n}}\right)\\
&\triangleq \mathbb{D}(P_{KZ^nF^n}||P_K Q_{Z^nF^n}) \qquad \text{(A4)}\\
&\overset{(a)}{=} \mathbb{D}(P_K||P_K) + \mathbb{D}(P_{Z^nF^n|K}||Q_{Z^nF^n}|P_K)\\
&= \mathbb{D}(P_{Z^nF^n|K}||Q_{Z^nF^n}|P_K), \qquad \text{(A5)}
\end{aligned}$$

where (a) follows the chain rule of divergence ([17] Th.2.2.2).

We then apply the channel resolvability analysis [18] to the CWTC, in order to find the rate constraint on the confusion messages, in order to guarantee the validity of the stealth secrecy constraint (A4).

From the analysis conducted in Appendix B, we know:

$$\mathbb{E}_{\mathcal{C}}[\mathbb{D}(P_{Z^nF^n|K}||Q_{Z^nF^n}|P_K)] \le \mathbb{E}_{Z^nF^nU^n}\left[\log\left(\frac{P_{Z^nF^n|U^n}}{L_1 Q_{Z^nF^n}} + 1\right)\right]. \qquad \text{(A6)}$$

Recall that $L_1 = 2^{\lceil nR_1 \rceil}$ is the number of confusion messages inside each bin, and we need to design it such that (A6) is vanishing. The main difference between our proof and that in [3] is that we introduce an additional channel output at both Bob and Willie by constructing a CWTC for the considered SKG model, which makes the results from [3] not able to be directly applied.

Now, we reexpress the ratio in the logarithm on the right-hand side (RHS) of (A6) as follows:

$$\frac{P_{Z^nF^n|U^n}}{Q_{Z^nF^n}} \overset{(a)}{=} \frac{P_{Z^nF^nU^n}}{P_{U^n}}\frac{1}{P_{Z^n}Q_{F^n}} \overset{(b)}{=} \frac{P_{Z^nF^nU^n}}{P_{Z^nU^n}}\frac{1}{Q_{F^n}} = \frac{P_{F^n|Z^nU^n}}{Q_{F^n}}, \qquad \text{(A7)}$$

where (a) is due to the fact that $F^n$ and $Z^n$ are independent when a meaningless discussion is transmitted, which has a pmf denoted by $Q_{F^n}$; (b) comes the fact that $U^n$ is independent of $Z^n$ by selection, i.e., $P_{Z^nU^n} = P_{Z^n}P_{U^n}$.

Note that even though $Z^n$ and $F^n$ are independent and $Z^n$ and $U^n$ are independent by assumption, that does not mean $Z^n$, $F^n$, and $U^n$ are necessarily generated according to $P_{Z^n,F^n,U^n} = P_{Z^n}P_{F^n,U^n}$ or $P_{Z^n,F^n,U^n} = P_{Z^n}P_{F^n}P_{U^n}$. In fact, since pairwise independence does not imply mutual independence ([19] Chapter 7.1, 7.2), there exists joint distribution $P_{Z^n,F^n,U^n}$ such that we can invoke tools from the joint asymptotic equipartition property [20].

Then, we can rewrite (A6) as follows:

$$\mathbb{E}_{\mathcal{C}}[\mathbb{D}(P_{Z^nF^n|K}||Q_{Z^nF^n}|P_K)] \le \mathbb{E}_{Z^nF^nU^n}\left[\log\left(\frac{P_{F^n|Z^nU^n}}{L_1 Q_{F^n}} + 1\right)\right]. \qquad \text{(A8)}$$

The RHS of (A8) can be discussed in two cases as follows similar to [3], according to whether $(z^n, f^n, u^n)$ are jointly typical or not:

$$d_1 = \sum_{\substack{(z^n,f^n,u^n)\in\\ T_\delta^n(P_{Z^n,F^n,U^n})}} P_{Z^nF^nU^n}(z^n,f^n,u^n)\log\left(\frac{P_{F^n|U^nZ^n}(f^n|u^nz^n)}{L_1Q_{F^n}(f^n)}+1\right),$$

$$d_2 = \sum_{\substack{(z^n,f^n,u^n)\notin\\ T_\delta^n(P_{Z^n,F^n,U^n})}} P_{Z^nF^nU^n}(z^n,f^n,u^n)\log\left(\frac{P_{F^n|U^nZ^n}(f^n|u^nz^n)}{L_1Q_{F^n}(f^n)}+1\right),$$

where $T_\delta^n$ follows the $\delta$-robust typicality [12] definition for the subsequent derivation.

The Chernoff bound and an important upper bound, which will be used later, are restated in the following.

**Lemma A1.** *(Chernoff bound ([12] Lemma 16) For every $a \in \mathcal{X}$, $x^n \in \mathcal{X}^n$, and $\delta > 0$,*

$$P\left(\frac{N(a|x^n)}{n} \le (1+\delta)P_X(a)\right) \le e^{-\delta^2 P_X(a)n/3}. \tag{A9}$$

**Lemma A2.** *(Upper bound of the probability of a non-typical set ([12] Lemma 17)*

$$P(x^n \notin T_\delta^{(n)}) \le 2|S_X|e^{-\delta^2\mu_X n/3}, \tag{A10}$$

*where $S_X \triangleq \{x \in \mathcal{X} : P(x) > 0\}$ and $\mu_x \triangleq \min_{x\in S_X} P(x)$.*

Next, we derive the constraint (The constraint that Bob should successfully decode both the secret and confusion messages is a point-to-point transmission without secrecy, which can be seen from [12]. Therefore, we omit the proof here.) on $R_1$ as follows:

$$\begin{aligned} d_1 &\overset{(a)}{\le} \left(\sum_{\substack{(z^n,f^n,u^n)\in\\ T_\delta^n(P_{Z^nF^nU^n})}} P_{Z^nF^nU^n}(z^n,f^n,u^n)\right)\log\left(1+\frac{2^{-n[H(F|UZ)-\delta]}}{L_1 2^{-n(1+\epsilon)H(F)}}\right)\\ &\overset{(b)}{\le} \log\left(1+\frac{2^{-n[H(F|UZ)-\delta]}}{L_1 2^{-n(1+\epsilon)H(F)}}\right)\\ &\overset{(c)}{=} \log\left(1+2^{-n(R_1-I(F;UZ)-\epsilon')}\right), \end{aligned} \tag{A11}$$

where (a) comes from ([12] Lemma 18, Lemma 20); (b) comes from the fact that the total probability of the jointly typical set is smaller than one; (c) is from definition of $L_1$ and $\epsilon' \triangleq \epsilon[1+H(F)] = \epsilon[1+H(U)]$. After that, we have $d_1 \to 0$ if $n \to \infty$ when the following constraint is fulfilled:

$$R_1 > I(UZ;F)+\epsilon' \overset{(a)}{=} I(UZ;U\oplus X)+\epsilon' \overset{(b)}{=} H(U)-H(X|Z)+\epsilon', \tag{A12}$$

where (a) comes from a specific use of the public discussion following ([16] Theorem 3) and $\oplus$ is the modulo addition in $\mathcal{X}$. We can follow the argument in ([21] Appendix B) in order to apply the crypto lemma in (A12) or (A14) to unbounded $X$ like the Gaussian case. (b) comes from the fact that $U$ is uniformly distributed with the crypto lemma. In addition, we can derive that $d_2 \to 0$ as $n \to \infty$ as follows:

$$\begin{aligned} d_2 &\overset{(a)}{\leq} \sum_{(z^n,u^n,f^n)\notin T_\delta^n(P_{Z^n,U^n,F^n})} P_{Z^nF^nU^n}(z^n,f^n,u^n)\log\left(\frac{1}{Q^n_{F^n}(f^n)}+1\right) \\ &\overset{(b)}{\leq} \sum_{(z^n,u^n,f^n)\notin T_\delta^n(P_{Z^n,U^n,F^n})} P_{Z^nF^nU^n}(z^n,f^n,u^n)\log\left(\frac{1}{\mu^n_{f^n}}+1\right) \\ &\overset{(c)}{\leq} \sum_{(z^n,u^n,f^n)\notin T_\delta^n(P_{Z^n,U^n,F^n})} P_{Z^nF^nU^n}(z^n,f^n,u^n) n\log\left(\frac{1}{\mu_f}+1\right) \\ &\overset{(d)}{=} n\mathrm{Pr}\left((z^n,u^n,f^n)\notin T_\delta^n(P_{Z^n,U^n,F^n})\right)\log\left(\frac{1}{\mu_f}+1\right) \\ &\overset{(e)}{\leq} 2n|S_{ZUF}|e^{-\delta^2\mu_{ZUF}n/3}\log\left(\frac{1}{\mu_f}+1\right), \end{aligned} \tag{A13}$$

where (a) is due to the fact that $P_{F^n|U^nZ^n}(f^n|u^nz^n) \leq 1$, and therefore, $P_{F^n|U^nZ^n}(f^n|u^nz^n)/L_1 \leq 1$; (b) is by lower bounding $Q^n_{F^n}(f^n)$ with $\mu_f = \min_{f^n \in S_{F^n}} Q_{F^n}(f^n)$, where $S_{F^n} \triangleq \{f^n \in \mathcal{X}^n : P(f^n) > 0\}$; (c) by simple algebra; (d) is by definition of probability; (e) is by Lemma A2. Note that $\mu_f$ in (A13) is a constant, but not a function of $n$. Therefore, the RHS of (A13) can be easily seen to vanish exponentially fast, if $n \to \infty$. Then, from (A11) and (A13), it is clear that (4) and (5) are fulfilled.

By constructing the CWTC, the following rate between Alice and Bob is achievable:

$$\begin{aligned} n(R+R_1) &\leq I(U^n \oplus X^n, Y^n; U^n) \\ &= H(Y^n, U^n \oplus X^n) - H(Y^n, U^n \oplus X^n|U^n) \\ &\overset{(a)}{=} H(Y^n) + H(U^n) - H(X^n, Y^n) \\ &= H(U^n) - H(X^n|Y^n), \end{aligned} \tag{A14}$$

where (a) again comes from the crypto lemma with the selection of $U^n$ being independent of $Y^n$. Then, from (A12) and (A14), the achievable stealthy strong SK rate can be derived as follows:

$$\begin{aligned} nR &\leq H(U^n) - H(X^n|Y^n) - nR_1 \\ &\overset{(a)}{<} n[H(X|Z) - H(X|Y)] \\ &= n[I(X;Y) - I(X;Z)], \end{aligned} \tag{A15}$$

where (a) is by plugging (A12) with the assumption of a memoryless common randomness, which is independent and identically distributed (i.i.d.). We can interchange the roles of $X$ and $Y$ to get $I(Y;X) - I(Y;Z)$, which completes the proof.

**Remark A1.** *In addition to the channel resolvability scheme, we can also attain the proof by a modified SWC scheme, which is sketched as follows. We can first construct a binary auxiliary random variable $S$, which selects the meaningful or meaningless discussion when $S = 1$ and $S = 0$, respectively. The stealth constraint is to avoid Willie successfully guessing the realization of $S$ and can be formulated as $I(S; Z^nF^n) \leq \epsilon$. By the data processing inequality for divergence [17], we can have the inequality $I(S; Z^nF^n) \leq \mathbb{D}(P_{KZ^nF^n}||P_KQ_{Z^n}Q_{F^n})$, which is an effective secrecy constraint of the considered SKG model. It is the counterpart to the one of the wiretap channel with stealth constraint [3]. We can then construct two binning codebooks for $S = 0$ and $S = 1$, where in each case, there is one corresponding binning codebook, in order to fulfill the secrecy constraint. In the error analysis, there are two cases: (1) when $S = 1$, the probability of Alice and Bob having different keys; (2) when $S = 0$,* *the probability of Bob generating a key that is not null. By vanishing enforcing the average error probability, we can attain the result in Theorem 1.*

**Remark A2.** *In the analysis by the WTC scheme in Appendix A, we derive the stealthy strong SK rate by combining a tool based one channel resolvability developed in [3] with the CWTC. In particular, we first derive an upper bound of the averaged stealth secrecy constraint (A5) by the random coding analysis. By enforcing the upper bound to vanish, we can derive the constraints on the stealthy strong SK rate and the confusion rate in the codebook design. By this scheme, we can proceed with the derivation based on the result of the wiretap channel.*

## Appendix B. Proof of (A6)

In the following, we show the tedious derivation for (A6) from channel resolvability [3]:

$$
\begin{aligned}
&\mathbb{E}_{\mathcal{C}}[\mathbb{D}(P_{Z^nF^n|K}||Q_{Z^nF^n}|P_K)]\\
&\overset{(a)}{=} \mathbb{E}_{\mathcal{C}}[\mathbb{D}(P_{Z^nF^n|M}||Q_{Z^nF^n}|P_M)]\\
&\overset{(b)}{=} \mathbb{E}_{\mathcal{C},M}\left[\sum_{z^n,F^n} P_{Z^n,F^n|M}(z^n,f^n|M=m)\log\left(\frac{P_{Z^n,F^n|M}(z^n,f^n|M=m)}{Q_{Z^n,F^n}(z^n,f^n)}\right)\right]\\
&\overset{(c)}{=} \mathbb{E}_{\mathcal{C},M}\left[\sum_{z^n,F^n}\sum_{w=1}^{L_1}\frac{1}{L_1}P_{Z^n,F^n|U^n}(z^n,f^n|u^n(m,w))\log\left(\frac{\sum_{l=1}^{L_1}\frac{1}{L_1}P_{Z^n,F^n|U^n}(z^n,f^n|u^n(m,l))}{Q_{Z^n,F^n}(z^n,f^n)}\right)\right]\\
&\overset{(d)}{=} \frac{1}{LL_1}\mathbb{E}_{\mathcal{C}}\left[\sum_{z^n,F^n}\sum_{m=1}^{L}\sum_{w=1}^{L_1}P_{Z^n,F^n|U^n}(z^n,f^n|u^n(m,w))\log\left(\frac{\sum_{l=1}^{L_1}Q_{Z^n,F^n|U^n}(z^n,f^n|u^n(m,l))}{L_1P_{Z^n,F^n}(z^n,f^n)}\right)\right]\\
&\overset{(e)}{=} \frac{1}{LL_1}\mathbb{E}_{\mathcal{C}}\left[\sum_{z^n,F^n}\sum_{m=1}^{L}\sum_{w=1}^{L_1}P_{Z^n,F^n|U^n}(z^n,f^n|u^n(m,w))\log\left(\frac{A_m(z^n,f^n|u^n)}{B(z^n,f^n)}\right)\right]\\
&\overset{(f)}{=} \frac{1}{LL_1}\sum_{u^n(1,1)}\cdots\sum_{u^n(L,L_1)}\prod_{m=1,w=1}^{L,L_1}P_U^n(u^n(m,w))\left[\sum_{z^n,F^n}\sum_{m=1}^{L}\sum_{w=1}^{L_1}P_{Z^n,F^n|U^n}(z^n,f^n|u^n)\log\left(\frac{A_m(z^n,f^n|u^n)}{B(z^n,f^n)}\right)\right]\\
&\overset{(g)}{=} \frac{1}{LL_1}\sum_{u^n(1,1)}\cdots\sum_{u^n(L,L_1)}\prod_{m=1,w=1}^{L,L_1}P_U^n(u^n(m,w))\\
&\sum_{z^n,F^n}\begin{bmatrix}
(P_{Z^n,F^n|U^n}(\cdot|u^n(1,1))+ & \cdots & +P_{Z^n,F^n|U^n}(\cdot|u^n(1,L_1)))\cdot\log\left(\frac{A_1(z^n,f^n|u^n)}{B(z^n,f^n)}\right)+\\
\vdots & \ddots & \vdots\\
(P_{Z^n,F^n|U^n}(\cdot|u^n(L,1)) & \cdots & +P_{Z^n,F^n|U^n}(\cdot|u^n(L,L_1)))\cdot\log\left(\frac{A_L(z^n,f^n|u^n)}{B(z^n,f^n)}\right)
\end{bmatrix}\\
&\overset{(h)}{=} \frac{1}{LL_1}\sum_{u^n(1,1)}\cdots\sum_{u^n(L,L_1)}\\
&\sum_{z^n,F^n}\begin{bmatrix}
\Big(P_{Z^n,F^n,U^n}(\cdot,u^n(1,1))\prod_{m\neq 1,w\neq 1}^{L,L_1}P_U^n(u^n(m,w))+\cdots+P_{Z^n,F^n,U^n}(\cdot,u^n(1,L_1))\prod_{m\neq 1,w\neq L_1}^{L,L_1}P_U^n(u^n(m,w))\Big)\cdot\\
\log\left(\frac{A_1(z^n,f^n|u^n)}{B(z^n,f^n)}\right)+\cdots\\
\Big(P_{Z^n,F^n,U^n}(\cdot,u^n(L,1))\prod_{m\neq L,w\neq 1}^{L,L_1}P_U^n(u^n(m,w))+\cdots+P_{Z^n,F^n,U^n}(\cdot,u^n(L,L_1))\prod_{m\neq L,w\neq L_1}^{L,L_1}P_U^n(u^n(m,w))\Big)\cdot\\
\log\left(\frac{A_L(z^n,f^n|u^n)}{B(z^n,f^n)}\right)
\end{bmatrix}
\end{aligned}
$$

$$
\begin{aligned}
&\overset{(i)}{=} \frac{1}{LL_1}\sum_{z^n,F^n}\left[\begin{array}{l}
\sum\limits_{u^n(1,1)} P_{Z^n,F^n,U^n}(\cdot,u^n(1,1))\mathbb{E}_{\underline{U}^n\setminus\underline{U}^n(1,1)}\left[\log\left(\frac{A_1(z^n,f^n|u^n)}{B(z^n,f^n)}\right)\right]+\cdots+\\
\sum\limits_{u^n(k,l)} P_{Z^n,F^n,U^n}(\cdot,u^n(k,l))\mathbb{E}_{\underline{U}^n\setminus\underline{U}^n(k,l)}\left[\log\left(\frac{\triangle_k(z^n,f^n|u^n)}{B(z^n,f^n)}\right)\right]+\cdots+\\
\sum\limits_{u^n(L,L_1)} P_{Z^n,F^n,U^n}(\cdot,u^n(L,L_1))\mathbb{E}_{\underline{U}^n\setminus\underline{U}^n(L,L_1)}\left[\log\left(\frac{A_L(z^n,f^n|u^n)}{B(z^n,f^n)}\right)\right]
\end{array}\right]\\
&\overset{(j)}{=} \frac{1}{LL_1}\sum_{z^n,F^n}\sum_{(a,b)=(1,1)}^{(L,L_1)}\sum_{u^n(a,b)} P_{Z^n,F^n,U^n}(\cdot,u^n(a,b))\mathbb{E}_{\underline{U}^n\setminus\underline{U}^n(a,b)}\left[\log\left(\frac{A_a(z^n,f^n|u^n)}{B(z^n,f^n)}\right)\right]\\
&\overset{(k)}{\leq} \frac{1}{LL_1}\sum_{z^n,F^n}\sum_{(a,b)=(1,1)}^{(L,L_1)}\sum_{u^n(a,b)} P_{Z^n,F^n,U^n}(\cdot,u^n(a,b))\log\left(\mathbb{E}_{\underline{U}^n\setminus\underline{U}^n(a,b)}\left[\left(\frac{A_a(z^n,f^n|u^n)}{B(z^n,f^n)}\right)\right]\right)\\
&\overset{(l)}{=} \frac{1}{LL_1}\sum_{z^n,F^n}\sum_{(a,b)=(1,1)}^{(L,L_1)}\sum_{u^n(a,b)} P_{Z^n,F^n,U^n}(\cdot,u^n(a,b))\log\left(\frac{P_{Z^n,F^n|U^n}(\cdot|u^n(a,b))+\sum\limits_{s\neq b}\sum\limits_{u^n(a,s)}P_{Z^n,F^n,U^n}(\cdot,u^n(a,s))}{B(z^n,f^n)}\right)\\
&\overset{(m)}{\leq} \frac{1}{LL_1}\sum_{z^n,F^n}\sum_{(a,b)=(1,1)}^{(L,L_1)}\sum_{u^n(a,b)} P_{Z^n,F^n,U^n}(\cdot,u^n(a,b))\log\left(\frac{P_{Z^n,F^n|U^n}(\cdot|u^n(a,b))+\sum\limits_{(r,s)=(1,1)}^{(L,L_1)}\sum\limits_{u^n(r,s)}P_{Z^n,F^n,U^n}(\cdot,u^n(r,s))}{B(z^n,f^n)}\right)\\
&\overset{(n)}{\leq} \frac{1}{LL_1}\sum_{z^n,F^n}\sum_{(a,b)=(1,1)}^{(L,L_1)}\sum_{u^n(a,b)} P_{Z^n,F^n,U^n}(\cdot,u^n(a,b))\log\left(\frac{P_{Z^n,F^n|U^n}(\cdot|u^n(a,b))}{B(z^n,f^n)}+1\right)\\
&\overset{(o)}{=} \mathbb{E}_{Z^nF^nU^n}\left[\log\left(\frac{P_{Z^nF^n|U^n}}{L_1Q_{Z^nF^n}}+1\right)\right],
\end{aligned}
\tag{A16}
$$

where (a) is by constructing a CWTC, such that the key $K$ is interchangeable with the message $M$; (b) is by definition of the conditional K-L distance ([17] Definition 2.2); (c) is due to the fact that $P_{Z^n,F|M}$ is the marginalization of $P_{Z^n,F^n|U^n}$ with respect to $w$, which is the index of the confusion message; in (d), we expand the expectation with respect to $M$; (e) is by defining $\sum_{l=1}^{L_1} P_{Z^n,F^n|U^n}(z^n,f^n|u^n(m,l))$ and $L_1Q_{Z^n,F^n}(z^n,f^n)$ by $A_m(z^n,f^n|u^n)$ and $B(z^n,f^n)$, respectively, to simplify the expression, where $m=1,\cdots,L$; (f) is by definition of the expectation over $\{U^n(m,w)\}_{m=1,w=1}^{L,L_1}$. Since $\{U^n(m,w)\}$ are generated independently and identically according to $P_U^n$, the joint distribution of codewords in a codebook is the product of marginal distributions; in (g), we expand the summation with respect to $m$ and $w$; in (h), we expand the product according to the form in step (g); in (i), we collect terms to form the expectation $\mathbb{E}_{\underline{U}^n\setminus\underline{U}^n(k,l)}$; in (j), we collect the terms by introducing additional indices $(a,b)$; in (k), we apply Jensen's inequality to the logarithm; (l) is by expanding the expectation $\mathbb{E}_{\underline{U}^n\setminus\underline{U}^n(k,l)}$; (m) is by adding the term $P_{Z^nF^nU^n}(z^n,f^n,u^n(a,b))$; (n) is by the definition of marginalization over $P_{Z^nF^nU^n}$ with respect to $U^n$. In particular, the second term on the RHS of the numerator in (m) becomes $\mathbb{E}_{U^n}[P_{Z^n,F^n|U^n}]=Q_{Z^nF^n}$ from (A3); (o) is by definition of the expectation.

## Appendix C. Proof of Theorem 2

We sketch the proof as follows in three steps, while the main idea is summarized in Figure A1. The key is to show that the stochastically degraded source $(X,\tilde{Y},\tilde{Z})$ implies that the corresponding CWTC [16] is also stochastically degraded, then the secret key capacity $C_{SK}$ of the source is the same as the secrecy capacity of a CWTC constructed from a physically degraded source $(X,Y,Z)$. The first step is to construct the CWTC of the source $(X,Y,Z)$ and prove that, if $X-Y-Z$, then $U-Y'-Z'$, i.e., the corresponding CWTC is also physically degraded, where $U$ is the conceptual code symbol, uniformly distributed in $\mathcal{X}$ and independent of $(X,Y,Z)$. The equivalently received signals at Bob and Willie in the CWTC are $Y'\triangleq(Y,U\oplus X)$ and $Z'\triangleq(Z,U\oplus X)$, respectively, while $U\oplus X$ is the signal transmitted through the public channel. The second step is to construct a stochastically degraded source $(X,\tilde{Y},\tilde{Z})$ from $(X,Y,Z)$. After that, we construct the corresponding CWTC of $(X,\tilde{Y},\tilde{Z})$ as $(U,Y'',Z'')$, where $Y''\triangleq(\tilde{Y},U\oplus X)$ and $Z''\triangleq(\tilde{Z},U\oplus X)$. The third step is to show that the CWTC described by $(U,Y'',Z'')$ has the same marginals as the CWTC described by $(U,Y',Z')$, i.e., the two CWTC's have the same secrecy capacity. In addition to the fact that stochastic degradedness is no stronger than the physical degradedness, this results in that the former one should not have a higher secret key capacity than the latter one. We then know that the sources $(X, Y, Z)$ and $(X, \tilde{Y}, \tilde{Z})$ have the same secret key capacity, which completes the proof.

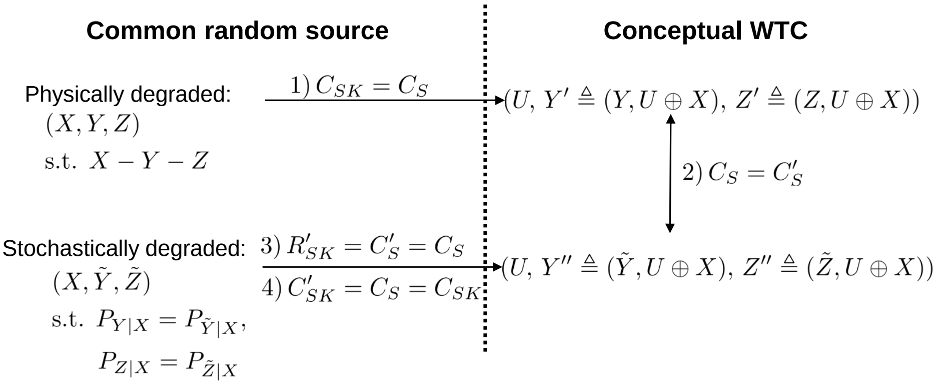
Common random source
Conceptual WTC
Physically degraded:
$(X, Y, Z)$
s.t. $X - Y - Z$
1) $C_{SK} = C_S$
$(U,\ Y' \triangleq (Y, U \oplus X),\ Z' \triangleq (Z, U \oplus X))$
2) $C_S = C'_S$
Stochastically degraded:
$(X, \tilde{Y}, \tilde{Z})$
s.t. $P_{Y|X} = P_{\tilde{Y}|X}$,
$P_{Z|X} = P_{\tilde{Z}|X}$
3) $R'_{SK} = C'_S = C_S$
4) $C'_{SK} = C_S = C_{SK}$
$(U,\ Y'' \triangleq (\tilde{Y}, U \oplus X),\ Z'' \triangleq (\tilde{Z}, U \oplus X))$

**Figure A1.** Key steps in the proof of Theorem 2. First is to show that the CWTCalso physically degraded if the source is physically degraded. Then, we show that the CWTC constructed from a stochastically degraded source corresponding to the physically degraded source is a stochastically degraded CWTC with the same marginal as that physically degraded CWTC. Finally, we show that the secrecy capacity of the second CWTC is indeed the secret key capacity of the stochastically degraded source. The key and secrecy capacities of the physically degraded source and the corresponding CWTC are denoted by $C_{SK}$ and $C_S$, respectively, while the key (rate) and secrecy capacities of the stochastic source and the corresponding CWTC are denoted by $C'_{SK}$ ($R'_{SK}$) and $C'_S$, respectively.

In the following, we will prove that the stochastically degraded random source $(X, \tilde{Y}, \tilde{Z})$ implies that the corresponding CWTC [16] is also stochastically degraded, which is constructed by the corresponding physically degraded source $(X, Y, Z)$. We start from constructing the CWTC of the random source $(X, Y, Z)$, where the equivalently received signals at Bob and Willie are $Y' \triangleq (Y, U \oplus X)$ and $Z' \triangleq (Z, U \oplus X)$, respectively. If $X - Y - Z$, then $U - Y' - Z'$, i.e., the CWTC is also a physically degraded one, which can be shown as follows:

$$\begin{aligned} I(U; Z'|Y') &\overset{(a)}{=} H(Z, U \oplus X|Y, U \oplus X) - H(Z, U \oplus X|Y, U \oplus X, U) \\ &\overset{(b)}{=} H(Z|Y) - H(Z|Y, U \oplus X, U) \\ &\overset{(c)}{=} H(Z|Y) - H(Z|Y, X, U) \\ &\overset{(d)}{=} H(Z|Y) - H(Z|Y, X) \\ &\overset{(e)}{=} 0, \end{aligned} \tag{A17}$$

where (a) is by the definition of $Y'$ and $Z'$; (b) is by the crypto lemma [22], and $U$ is selected to be independent of $Y$ and $Z$; (c) is from the fact that given $U$, we can know $X$ from $U \oplus X$; (d) is by the same reason as (b); (e) is due to $X - Y - Z$ and by the definition of conditional mutual information.

Now, we consider the stochastically degraded source of common randomness $(X, \tilde{Y}, \tilde{Z})$ fulfilling $P_{\tilde{Y}|X} = P_{Y|X}$ and $P_{\tilde{Z}|X} = P_{Z|X}$. Similar to the first step, we construct the CWTC from $(X, \tilde{Y}, \tilde{Z})$, namely $\{(U, Y'', Z''),\ P_{U,Y'',Z''} = P_U P_{Y'',Z''|U}\}$, where $Y'' \triangleq (\tilde{Y}, U \oplus X)$ and $Z'' \triangleq (\tilde{Z}, U \oplus X)$ are the equivalent channel outputs at Bob and Willie, respectively. To prove that the two CWTC's $P_{Y',Z'|U}$ and $P_{Y'',Z''|U}$ are equivalent, we can invoke the same marginal property in ([11] Theorem 16.6) to prove that $P_{Y''|U} = P_{Y'|U}$ and $P_{Z''|U} = P_{Z'|U}$, which is shown in the following. By the definitions of $Y''$ and $Y'$, we know that $P_{Y''|U=u} = P_{\tilde{Y},u \oplus X} \triangleq P_{\tilde{Y},X_u}$ and $P_{Y'|U=u} = P_{Y,u \oplus X} \triangleq P_{Y,X_u}$, respectively, where we define $X_u$ as $u \oplus X$. Note that due to the closed operation $\oplus$ in $\mathcal{X}$, the distribution of $X_u$ is a left circular shift of that of $X$ by $u$. Instead of directly proving $P_{\tilde{Y},X_u} = P_{Y,X_u}$, we can equivalently prove $P_{\tilde{Y}|X_u} = P_{Y|X_u}$, $\forall u$, as follows:

$$P_{\tilde{Y}|X_u=x} = P_{\tilde{Y}|X=x'} = P_{Y|X=x'} = P_{Y|X_u=x'}, \tag{A18}$$

where the second equality is due to the assumption of $(X, \tilde{Y}, \tilde{Z})$ forming a stochastically degraded source from the physically degraded one $(X, Y, Z)$. Therefore, $P_{Y''|U} = P_{Y'|U}$. Similarly, we can derive $P_{Z''|U} = P_{Z'|U}$. Hence, we prove that the CWTC of a stochastic degraded source is also a degraded CWTC and the two CWTC's have the same secrecy capacity.

Note that due to $X - Y - Z$, we can derive the key capacity $C_{SK}$ from the corresponding CWTC, not just an achievable key rate. For the source $(X, \tilde{Y}, \tilde{Z})$, till now, we may only claim the achievable secret key rate, but not the secret key capacity, namely $C'_{SK}$, is the same as $C_{SK}$. That is because the CWTC is in general only an achievable scheme to derive the secret key rate. However, due to the fact that the stochastic degradedness is more general than the physical degradedness, i.e., less stringent on characterizing the order between $X$, $\tilde{Y}$ and $\tilde{Z}$, the stochastic degradedness cannot result in a larger secret key capacity than the physically degraded one. Therefore, we attain that $C'_{SK} = C_{SK} = I(X;Y) - I(X;Z)$, which completes the proof.

## References

1. Wyner, A.D. The wiretap channel. *Bell Syst. Tech. J.* **1975**, *54*, 1355–1387. [CrossRef]
2. Che, P.H.; Bakshi, M.; Jaggi, S. Reliable deniable communication: Hiding messages in noise. In Proceedings of the 2013 IEEE International Symposium on Information Theory, Istanbul, Turkey, 7–12 July 2013; pp. 2945–2949.
3. Hou, J.; Kramer, G. Effective secrecy: Reliability, confusion and stealth. In Proceedings of the 2014 IEEE International Symposium on Information Theory, Honolulu, HI, USA, 29 June–4 July 2014; pp. 601–605.
4. Wang, L.; Wornell, G.W.; Zheng, L. Fundamental limits of communication with low probability of detection. *IEEE Trans. Inf. Theory* **2016**, *62*, 3493–3503. [CrossRef]
5. Bloch, M.R. Covert Communication Over Noisy Channels: A Resolvability Perspective. *IEEE Trans. Inf. Theory* **2016**, *62*, 2334–2353. [CrossRef]
6. Bash, B.A.; Goeckel, D.; Towsley, D. Limits of reliable communication with low probability of detection on AWGN channels. *IEEE J. Sel. Areas Commun.* **2013**, *31*, 1921–1930. [CrossRef]
7. Bloch, M.; Barros, J. *Physical-Layer Security From Information Theory to Security Engineering*; Cambridge University Press: Cambridge, UK, 2011.
8. Tahmasbi, M.; Bloch, M.R. Covert Secret Key Generation. In Proceedings of the 2017 IEEE Conference on Communications and Network Security (CNS), Las Vegas, NV, USA, 9–11 October 2017; pp. 540–544.
9. Shaked, M.; Shanthikumar, J.G. *Stochastic Orders*; Springer: Berlin/Heidelberger, Germany,2007.
10. Naito, M.; Watanabe, S.; Matsumoto, R.; Uyematsu, T. Secret key agreement by soft-decision of signals in Gaussian Maurer's model. *IEICE Trans. Fundam.* **2009**, *E92-A*, 525–534. [CrossRef]
11. Moser, S.M. Advanced Topics in Information Theory-Lecture Notes. 2013. Available online: http://moser-isi.ethz.ch/docs/it_script_v46.pdf (accessed on 10 June 2020).
12. Orlitsky, A.; Roche, J. Coding for computing. *IEEE Trans. Inf. Theory* **2001**, *47*, 903–917. [CrossRef]
13. Thorisson, H. *Coupling, Stationarity, and Regeneration*; Springer: New York, NY, USA, 2000.
14. Gamal, A.E.; Kim, Y.H. *Network Information Theory*; Cambridge University Press: Cambridge, UK, 2012.
15. Simon, M.K.; Alouini, M.S. *Digital Communication over Fading Channels*; John Wiley & Sons: Chichester, UK, 2000.
16. Maurer, U.M. Secret Key Agreement by Public Discussion from Common Information. *IEEE Trans. Inf. Theory* **1993**, *39*, 733–742. [CrossRef]
17. Polyanskiy, Y.; Wu, Y. Lecture Notes on Information Theory 2019. Available online: http://www.stat.yale.edu/~yw562/teaching/itlectures.pdf (accessed on 10 June 2020).
18. Hou, J.; Kramer, G. Informational divergence approximations to product distributions. In Proceedings of the 2013 13th Canadian Workshop on Information Theory, Toronto, ON, Canada, 18–21 June 2013.

19. Stoyanov, J.M. *Counterexamples in Probability*, 3rd ed.; Dover: New York, NY, USA, 2013.
20. Cover, T.M. Broadcast Channels. *IEEE Trans. Inf. Theory* **1972**, *18*, 2–14. [CrossRef]
21. Bennatan, A.; Burshtein, D.; Caire, G.; Shamai, S. Superposition coding for side-information channels. *IEEE Trans. Inf. Theory* **2006**, *52*, 1872–1889. [CrossRef]
22. Forney, G.D., Jr. On the Role of MMSE Estimation in Approaching the Information-Theoretic Limits of Linear Gaussian Channels: Shannon meets Wiener. 2004. Available online: https://arxiv.org/pdf/cs/0409053.pdf (accessed on 10 June 2020).