entropy

MDPI

Article

Secrecy Capacity Region of the AWGN MAC with External Eavesdropper and Feedback

Haoheng Yuan [1,†], Guangfen Xie [1,†] and Bin Dai [1,2,*,†]

[1] School of Information Science and Technology, Southwest Jiaotong University, Chengdu 611756, China; yhhcd@my.swjtu.edu.cn (H.Y.); gfxie@my.swjtu.edu.cn (G.X.)
[2] Peng Cheng Laboratory, Shenzhen 518055, China
* Correspondence: daibin@home.swjtu.edu.cn; Tel.: +86-135-4805-3724
† These authors contributed equally to this work.

Abstract: For the point-to-point additive white Gaussian noise (AWGN) channel with an eavesdropper and feedback, it has already been shown that the secrecy capacity can be achieved by a secret key-based feedback scheme, where the channel feedback is used for secret sharing, and then encrypting the transmitted message by the shared key. By secret sharing, any capacity-achieving coding scheme for the AWGN channel without feedback can be secure by itself, which indicates that the capacity of the same model without the secrecy constraint also affords an achievable secrecy rate to the AWGN channel with an eavesdropper and feedback. Then it is natural to ask: is the secret key-based feedback scheme still the optimal scheme for the AWGN multiple-access channel (MAC) with an external eavesdropper and channel feedback (AWGN-MAC-E-CF), namely, achieving the secrecy capacity region of the AWGN-MAC-E-CF? In this paper, we show that the answer to the aforementioned question is no, and propose the optimal feedback coding scheme for the AWGN-MAC-E-CF, which combines an existing linear feedback scheme for the AWGN MAC with feedback and the secret key scheme in the literature. This paper provides a way to find optimal coding schemes for AWGN multi-user channels in the presence of an external eavesdropper and channel feedback.

Keywords: AWGN MAC; feedback; secrecy capacity; wiretap channel

Citation: Yuan, H.; Xie, G.; Dai, B. Secrecy Capacity Region of the AWGN MAC with External Eavesdropper and Feedback. *Entropy* **2023**, *25*, 1339. https://doi.org/10.3390/e25091339

Academic Editors: Pingyi Fan, Qi Chen, Suihua Cai and Gangtao Xin

Received: 14 August 2023
Revised: 13 September 2023
Accepted: 14 September 2023
Published: 15 September 2023

1. Introduction

The model of the wiretap channel lays the foundation of physical layer security (PLS). In references [1,2], it has been shown that the secrecy capacity of the additive white Gaussian noise (AWGN) wiretap channel model, which is the maximum transmission rate under the perfect weak secrecy (PWS) constraint, is equal to the difference between the channel capacities of the legal receiver and the eavesdropper, and this indicates that to achieve secrecy, the loss of transmission rate is inevitable.

Though channel feedback does not increase the capacity of a point-to-point memoryless channel [3], references [4,5] found that the feedback channel can be used to generate a secret key shared between the legal parties. Then, the transmitter encrypting via the transmitted message by this key, the secrecy capacity of the wiretap channel can be enhanced. Subsequently, references [6,7] further showed that for modulo-additive and AWGN cases, the secret key schemes in references [4,5] are optimal and achieve the capacities of the same models without feedback and the secrecy constraint. Then it is natural to ask: is the secret key-based feedback scheme still the optimal scheme for the AWGN multiple-access channel (MAC) with an external eavesdropper and channel feedback (AWGN-MAC-E-CF), namely, achieving the secrecy capacity region of the AWGN-MAC-E-CF? The answer to the aforementioned question is no, and this is due to the fact that feedback *increases* the capacity region of the AWGN MAC [8], and the secret key scheme only achieves the capacity region of the AWGN MAC without feedback. Then another question is: what is the optimal feedback scheme for the AWGN-MAC-E-CF, and is the secrecy capacity region of

the AWGN-MAC-E-CF equal to the capacity region of the AWGN MAC with feedback, which is in parallel to the fact that the secrecy capacity of the point-to-point AWGN channel with an eavesdropper and feedback equals the capacity of the same model without the secrecy constraint [6,7].

In [9], it has been shown that the classical Schalkwijk-Kailath (SK) scheme [10], which is a capacity-achieving scheme for the point-to-point AWGN channel with feedback, also achieves the secrecy capacity of the point-to-point AWGN channel with an eavesdropper and feedback. Motivated by [9], in this paper, we combine Ozarow's SK-type scheme for the AWGN MAC with feedback [8] and the secret key scheme in the literature to show that the secrecy capacity region of the AWGN-MAC-E-CF is equal to the capacity region of the AWGN MAC with feedback. The basic intuition behind this scheme is explained below. In [9], it has been shown that the SK scheme satisfies the PWS by itself and achieves the capacity of the point-to-point AWGN channel with feedback. In a similar way, we show that Ozarow's extended SK scheme [8] satisfies the PWS by itself, however, we find that this SK-type scheme does not achieve the entire capacity region of the AWGN MAC with feedback. To show that every point in the capacity region of the AWGN MAC with feedback satisfies PWS, we split the transmitted message of one transmitter into two parts, where one part together with the message of the other transmitter are encoded by Ozarow's SK-type scheme, and the other part is encrypted by a key which is generated by the channel noise at the first time instant and this key is only known by the legal parties. Following the security property of the SK-type scheme and the secret key, we show that every point in the capacity region of the AWGN MAC with feedback satisfies PWS, which indicates that the secrecy capacity region of the AWGN-MAC-E-CF is equal to the capacity region of the AWGN MAC with feedback.

2. Model Formulation and Main Result

2.1. Model Formulation

For the AWGN-MAC-E-CF (see Figure 1), the i-th ($i \in \{1, 2, \ldots, N\}$) channel inputs and outputs are given by

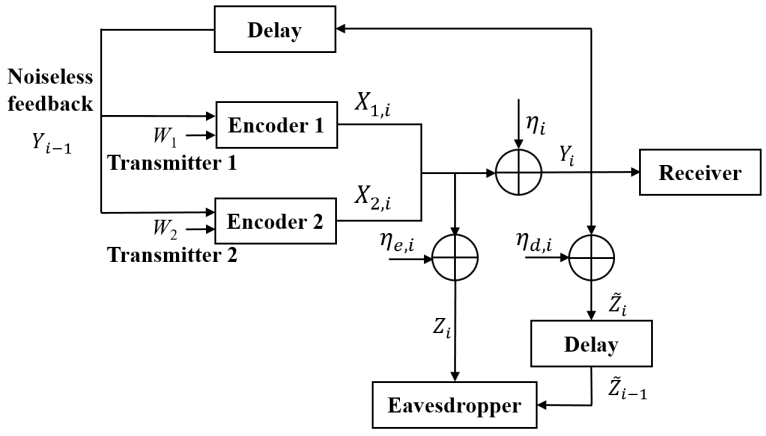

Figure 1. The AWGN MAC with an external eavesdropper and channel feedback.

$$\begin{aligned} &Y_i = X_{1,i} + X_{2,i} + \eta_i, \;\; Z_i = X_{1,i} + X_{2,i} + \eta_{e,i}, \;\; i \in \{1, 2, \ldots, N\} \\ &\widetilde{Z}_{i-1} = Y_{i-1} + \eta_{d,i-1}, \;\; i \in \{1, 2, \ldots, N-1\} \end{aligned} \tag{1}$$

where $X_{k,i}$ ($k \in \{1, 2\}$) is the channel codeword subject to an average power constraint P_k, namely, $\frac{1}{N}\sum_{i=1}^{N} E[X_{k,i}^2] \leq P_k$, Y_i is the legal receiver's channel output. Here, note that the eavesdropper eavesdrops the codewords $X_{1,i}$ and $X_{2,i}$ by an eavesdropping channel with output Z_i, and eavesdrops the feedback signal Y_{i-1} by another eavesdropping channel with output $\widetilde{Z}_{i-1}$. In addition, $\eta_i \sim \mathcal{N}(0, \sigma^2)$, $\eta_{e,i} \sim \mathcal{N}(0, \sigma_e^2)$, $\eta_{d,i} \sim \mathcal{N}(0, \sigma_d^2)$ are AWGNs, and they are independent of one another.

The transmitted message W_k ($k \in \{1,2\}$) is uniformly drawn in $\mathcal{W}_k = \{1,2,\ldots,|\mathcal{W}_k|\}$), and at time $i \in \{1,2,\ldots,N\}$, the codeword $X_{k,i}$ ($k \in \{1,2\}$) is a (stochastic) function of the message W_k and the feedback $Y^{i-1} = (Y_1,\ldots,Y_{i-1})$. At time N, the legal receiver obtains $(\hat{W}_1,\hat{W}_2) = \psi(Y^N)$, where ψ is the decoding function and the average decoding error probability is denoted by

$$P_e = Pr[(\hat{W}_1,\hat{W}_2) \neq (W_1,W_2)] = \frac{\sum_{w_1,w_2 \in \mathcal{W}_1,\mathcal{W}_2} Pr\{\psi(Y^N) \neq (w_1,w_2) | (W_1,W_2) = (w_1,w_2)\}}{|\mathcal{W}_1||\mathcal{W}_2|}. \quad (2)$$

The eavesdropper's equivocation rate of W_1 and W_2 is denoted by

$$\Delta = \frac{1}{N} H(W_1,W_2|Z^N,\widetilde{Z}^{N-1}). \quad (3)$$

A rate pair (R_1,R_2) is achievable with PWS if for any $\epsilon > 0$ and sufficiently large N, there exist channel encoders-decoders such that

$$\frac{\log|\mathcal{W}_k|}{N} \geq R_k - \epsilon, \;\; \Delta \geq R_1 + R_2 - \epsilon, \;\; P_e \leq \epsilon. \quad (4)$$

The secrecy capacity region $\mathcal{C}_{s,mac}^f$ of the AWGN-MAC-E-CF is composed of all achievable secrecy rate pairs defined above.

2.2. Main Result

The following Theorem 1 shows that $\mathcal{C}_{s,mac}^f$ equals the capacity of AWGN MAC with feedback.

Theorem 1. *$\mathcal{C}_{s,mac}^f = \mathcal{C}_{mac}^f$, where $\mathcal{C}_{mac}^f$ is the capacity region of the AWGN MAC with feedback [8] (the model of Figure 1 without the secrecy constraint), and it is given by $\mathcal{C}_{mac}^f = \bigcup_{0\leq\rho\leq 1} R(\rho)$, and*

$$\begin{aligned} R(\rho) = \Bigg\{ (R_1,R_2) : R_1 &\leq \frac{1}{2}\log\left[1 + \frac{P_1}{\sigma^2}(1-\rho^2)\right], \\ R_2 &\leq \frac{1}{2}\log\left[1 + \frac{P_2}{\sigma^2}(1-\rho^2)\right], \\ R_1 + R_2 &\leq \frac{1}{2}\log\left(1 + \frac{P_1 + P_2 + 2\rho\sqrt{P_1P_2}}{\sigma^2}\right)\Bigg\}. \end{aligned} \quad (5)$$

Proof. See Section 3. □

Remark 1. *Applying the secret key feedback schemes in [6,7] to AWGN MAC with feedback, it is easy to see that any capacity-achieving coding scheme for the AWGN MAC without feedback is secure by itself, which indicates that the secret key inner bound $\mathcal{C}_{s,mac}^{f-in-1}$ on $\mathcal{C}_{s,mac}^f$ is in fact the capacity region $\mathcal{C}_{mac}$ of the AWGN MAC without feedback, i.e.,*

$$\begin{aligned} \mathcal{C}_{s,mac}^{f-in-1} = \mathcal{C}_{mac} = \Bigg\{ (R_1,R_2) : R_1 &\leq \frac{1}{2}\log\left(1 + \frac{P_1}{\sigma^2}\right), \\ R_2 \leq \frac{1}{2}\log\left(1 + \frac{P_2}{\sigma^2}\right), \;\; R_1 + R_2 &\leq \frac{1}{2}\log\left(1 + \frac{P_1+P_2}{\sigma^2}\right)\Bigg\}. \end{aligned} \quad (6)$$

Comparing (5) and (6), we conclude that the secret key scheme is not optimal for the AWGN-MAC-E-CF. In the next section, we propose a new feedback scheme that achieves $\mathcal{C}_{s,mac}^f$ in Theorem 1.

2.3. Numerical Example

The following Figure 2 plots $\mathcal{C}_{s,mac}^f$ and $\mathcal{C}_{s,mac}^{f-in-1}$ for $P_1 = 5$, $P_2 = 5$, $\sigma^2 = 5$, $\sigma_e^2 = 5$. It is easy to see that the gap is obvious and the secret key feedback scheme is not optimal for the AWGN-MAC-E-CF.

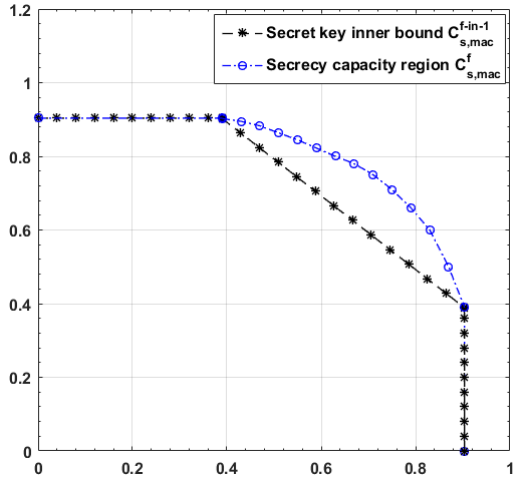

Figure 2. Capacity results on the AWGN-MAC-E-CF, where $P_1 = 5$, $P_2 = 5$, $\sigma^2 = 5$, $\sigma_e^2 = 5$.

3. Proof of the Theorem 1

First, note that $\mathcal{C}_{s,mac}^{f}$ cannot exceed the capacity region of the same model without the secrecy constraint, i.e., $\mathcal{C}_{s,mac}^{f} \subseteq \mathcal{C}_{mac}^{f}$. Then, it remains to be proven that any rate pair $(R_1, R_2) \in \mathcal{C}_{mac}^{f}$ is achievable with PWS defined in (4), which is equivalent to show that for any $0 \leq \rho \leq 1$, $R(\rho)$ in (5) is achievable with PWS. In Figure 3, we plot $R(\rho)$ for all $0 \leq \rho \leq 1$, where ρ^* is the ρ satisfying the sum of the right hand side (RHS) of the first two inequalities in (5), which equals the RHS of the third inequality, which is equivalent to ρ^* (the solution in $(0, 1)$), of

$$\sigma^2(\sigma^2 + P_1 + P_2 + 2\sqrt{P_1 P_2}\rho) = [\sigma^2 + P_1(1-\rho^2)][\sigma^2 + P_2(1-\rho^2)]. \tag{7}$$

From Figure 3, we see that when $\rho^* < \rho \leq 1$, $R(\rho)$ is included in $R(\rho^*)$, hence we only need to prove that for any $0 \leq \rho \leq \rho^*$, $R(\rho)$ is achievable with PWS. In the remainder of this section, the proof is given by two cases, i.e., $\rho = \rho^*$ and $0 \leq \rho < \rho^*$. The details are given below.

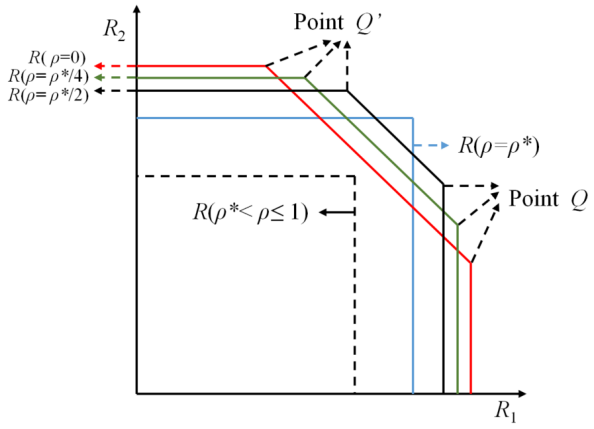

Figure 3. Illustration of $R(\rho)$ for $0 \leq \rho \leq 1$.

3.1. Case 1: $\rho = \rho^*$

In this case, we directly show that Ozarow's SK-type feedback scheme for AWGN MAC with feedback [8] is achievable with PWS. The basic intuition behind this scheme is described below. First, recall that for the classical point-to-point SK scheme, the receiver estimates the transmitted message by minimum mean square estimation (MMSE), and through a noiseless feedback channel, the estimation error of the receiver's estimation is known by the transmitter since he knows the real transmitted message, and hence in the

next time, the transmitter encodes this estimation error as a codeword and sends it to the receiver with the AWGN channel. By iteration, the receiver's estimation error vanishes as the coding blocklength tends to infinity. Then, for the two-user AWGN MAC with noiseless feedback, by viewing each other's transmitted codeword as part of the channel noise, this MAC model can be equivalent to two point-to-point AWGN channels with noiseless feedback. In addition to this, to further increase the sum rate of this MAC model, a modulation factor ρ is applied to the second user's encoder, which helps to enhance the mutual information between the transceiver. The detail of this scheme is given below.

For $k \in \{1, 2\}$, let $\mathcal{W}_k = \{1, 2, \ldots, 2^{NR_k}\}$ be the message set of W_k, divide the interval $[-0.5, 0.5]$ into 2^{NR_k} equally spaced sub-intervals, and each sub-interval center is mapped to a value in $\mathcal{W}_k$. The center of the sub-interval with respect to (w.r.t.) W_k is denoted by Θ_k, where its variance approximately equals $\frac{1}{12}$.

Coding procedure :

At time instant 1, Transmitter 2 sends nothing but zero, i.e., $X_{2,1} = 0$, and Transmitter 1 sends

$$X_{1,1} = \sqrt{12P_1}\Theta_1 + S, \tag{8}$$

where $S \sim \mathcal{N}(0, \sigma_0^2)$ is a Gaussian random variable and it is independent of the transmitted message and all signals in Figure 1. Here, S is used to obtain a steady ρ_i for $2 \leq i \leq N$, and this will be explained later.

Once the legal receiver obtains $Y_1 = \sqrt{12P_1}\Theta_1 + S + \eta_1$, his first estimation $\hat{\Theta}_{1,1}$ about Θ_1 is given by

$$\hat{\Theta}_{1,1} = \frac{Y_1}{\sqrt{12P_1}} = \Theta_1 + \frac{S + \eta_1}{\sqrt{12P_1}}. \tag{9}$$

For continuity, define the legal receiver's first estimation of Θ_2 as $\hat{\Theta}_{2,1} = 0$.

At the end of time instant 1, Transmitter 1 receives Y_1 via channel feedback, and he computes the error $\epsilon_{1,1}$ of the legal receiver's first estimation about Θ_1 by

$$\epsilon_{1,1} = \hat{\Theta}_{1,1} - \Theta_1 = \frac{S + \eta_1}{\sqrt{12P_1}}, \tag{10}$$

where the variance of $\epsilon_{1,1}$ is given by

$$\alpha_{1,1} = Var(\epsilon_{1,1}) = E\left[\left(\frac{S + \eta_1}{\sqrt{12P_1}}\right)^2\right] = \frac{\sigma_0^2 + \sigma^2}{12P_1}. \tag{11}$$

At time instant 2, Transmitter 1 sends nothing but zero, i.e., $X_{1,2} = 0$, and Transmitter 2 sends

$$X_{2,2} = \sqrt{12P_2}\Theta_2 + S. \tag{12}$$

Once the legal receiver obtains $Y_2 = \sqrt{12P_2}\Theta + S + \eta_2$, his second estimation $\hat{\Theta}_{2,2}$ about Θ_2 is given by

$$\hat{\Theta}_{2,2} = \frac{Y_2}{\sqrt{12P_2}} = \Theta_2 + \frac{S + \eta_2}{\sqrt{12P_2}}. \tag{13}$$

For continuity, define the legal receiver's second estimation of Θ_1 as $\hat{\Theta}_{1,2} = \hat{\Theta}_{1,1}$, which indicates that $\epsilon_{1,2} = \epsilon_{1,1}$, and $\alpha_{1,2} = \alpha_{1,1}$.

At the end of time instant 2, Transmitter 2 receives Y_2 via channel feedback, and computes the error $\epsilon_{2,2}$ of the legal receiver's second estimation about Θ_2 by

$$\epsilon_{2,2} = \hat{\Theta}_{2,2} - \Theta_2 = \frac{S + \eta_2}{\sqrt{12P_2}}, \tag{14}$$

where the variance of $\epsilon_{2,2}$ is given by

$$\alpha_{2,2} = Var(\epsilon_{2,2}) = E\left[\left(\frac{S+\eta_2}{\sqrt{12P_2}}\right)^2\right] = \frac{\sigma_0^2+\sigma^2}{12P_2}. \tag{15}$$

At time instant $3 \le i \le N$, first, define

$$\rho_{i-1} = \frac{E[\epsilon_{1,i-1}\epsilon_{2,i-1}]}{\sqrt{\alpha_{1,i-1}\alpha_{2,i-1}}} \tag{16}$$

as the correlation coefficient of $\epsilon_{1,i-1}$ and $\epsilon_{2,i-1}$, which are the legal receiver's estimation errors of Θ_1 and Θ_2 at the time instant $i-1$. Moreover, note that $\alpha_{k,i-1}$ ($k \in \{1,2\}$) is the variance of $\epsilon_{k,i-1}$. Next, define the symbolic function $\mathrm{sgn}(\rho_{i-1})$ of ρ_{i-1} as

$$\mathrm{sgn}(\rho_{i-1}) = \begin{cases} 1, & \rho_{i-1} \ge 0 \\ -1, & \rho_{i-1} < 0 \end{cases} \tag{17}$$

which is used as a modulation factor maximizing the mutual information between the transmitters and the legal receiver. Then, Transmitters 1 and 2 send

$$X_{1,i} = \sqrt{\frac{P_1}{\alpha_{1,i-1}}}\epsilon_{1,i-1}, \quad X_{2,i} = \sqrt{\frac{P_2}{\alpha_{2,i-1}}}\epsilon_{2,i-1}\cdot \mathrm{sgn}(\rho_{i-1}), \textit{respectively}. \tag{18}$$

Once receiving $Y_i = X_{1,i} + X_{2,i} + \eta_i$, the legal receiver updates his estimation of Θ_k by

$$\hat{\Theta}_{k,i} = \hat{\Theta}_{k,i-1} - \beta_{k,i}Y_i, \tag{19}$$

where

$$\beta_{k,i} = \frac{E[\epsilon_{k,i-1}Y_i]}{E[Y_i^2]}. \tag{20}$$

Since $\epsilon_{k,i} = \hat{\Theta}_{k,i} - \Theta_k$, (19) can be rewritten as

$$\epsilon_{k,i} = \epsilon_{k,i-1} - \beta_{k,i}Y_i. \tag{21}$$

For $3 \le i \le N$, the variance $\alpha_{k,i}$ ($k \in \{1,2\}$) of $\epsilon_{k,i}$ can be calculated as

$$\alpha_{k,i} = \alpha_{k,i-1}\frac{\sigma^2 + P_k(1-\rho_{i-1}^2)}{P_1+P_2+2\sqrt{P_1P_2}|\rho_{i-1}|+\sigma^2}. \tag{22}$$

Now, substituting (21) and (22) into (16), we have

$$\rho_i = \frac{\rho_{i-1}\sigma^2 - \mathrm{sgn}(\rho_{k-1})\sqrt{P_1P_2}(1-\rho_{i-1}^2)}{\sqrt{[P_1(1-\rho_{i-1}^2)+\sigma^2][P_2(1-\rho_{i-1}^2)+\sigma^2]}}, \tag{23}$$

where

$$\rho_2 = \frac{\sigma_0^2}{\sigma_0^2+\sigma^2}. \tag{24}$$

In general, $|\rho_i| \ne |\rho_{i-1}|$, to find a steady point in $|\rho_i|$, i.e., $|\rho_i| = |\rho_{i-1}|$, we substitute (23) into $1-\rho_i^2 = 1-\rho_{i-1}^2$, which is equivalent to

$$\sigma^2\left(\sigma^2+P_1+P_2+2\sqrt{P_1P_2}\rho_{i-1}\right) = \left[\sigma^2+P_1(1-\rho_{i-1}^2)\right]\left[\sigma^2+P_2(1-\rho_{i-1}^2)\right]. \tag{25}$$

Here, note that the equation in (25) is exactly the same as that in (7), and ρ^* is the solution to this equation. Hence, choosing an appropriate variance σ_0^2 of S such that ρ_2 in (24) satisfies $\rho_2 = \rho^*$, we conclude that $|\rho_i| = \rho^*$ for all $2 \le i \le N$.

Next, following the error probability analysis in [8], we conclude that if $(R_1, R_2) \in R(\rho^*)$, $P_e \to 0$, as $N \to \infty$. Now it remains to show that any rate pair $(R_1, R_2) \in R(\rho^*)$ satisfies PWS; see the details below.

Equivocation analysis: first, note that for $3 \le i \le N$, the codewords $X_{1,i}$ and $X_{2,i}$ are linear combinations of $\eta_1, \ldots, \eta_{i-1}$, and S, which is in parallel to that of the classical SK scheme [9] for the point-to-point AWGN channel. Then the eavesdropper's equivocation rate is bounded by

$$
\begin{aligned}
\Delta &= \frac{1}{N} H(W_1, W_2 | Z^N, \widetilde{Z}^{N-1}) \overset{(a)}{=} \frac{1}{N} H(\Theta_1, \Theta_2 | Z^N, \widetilde{Z}^{N-1}) \\
&\ge \frac{1}{N} H(\Theta_1, \Theta_2 | Z^N, \widetilde{Z}^{N-1}, \eta_1, \ldots, \eta_N, S) \\
&= \frac{1}{N} H(\Theta_1, \Theta_2 | \underbrace{\sqrt{12P_1}\Theta_1 + S + \eta_{e,1}}_{Z_1}, \underbrace{\sqrt{12P_2}\Theta_2 + S + \eta_{e,2}}_{Z_2}, \underbrace{X_{1,3} + X_{2,3} + \eta_{e,3}, \ldots, X_{1,N} + X_{2,N} + \eta_{e,N}}_{Z_3, \ldots, Z_N}, \eta_1, \ldots, \eta_N, S, \\
&\underbrace{\sqrt{12P_1}\Theta_1 + S + \eta_1 + \eta_{d,1}}_{\widetilde{Z}_1}, \underbrace{\sqrt{12P_2}\Theta_2 + S + \eta_2 + \eta_{d,2}}_{\widetilde{Z}_2}, \underbrace{X_{1,3} + X_{2,3} + \eta_3 + \eta_{d,3}, \ldots, X_{1,N-1} + X_{2,N-1} + \eta_{N-1} + \eta_{d,N-1}}_{\widetilde{Z}_3, \ldots, \widetilde{Z}_{N-1}}) \\
&\overset{(b)}{=} \frac{1}{N} H(\Theta_1, \Theta_2 | \sqrt{12P_1}\Theta_1 + \eta_{e,1}, \sqrt{12P_2}\Theta_2 + \eta_{e,2}, \sqrt{12P_1}\Theta_1 + \eta_{d,1}, \sqrt{12P_2}\Theta_2 + \eta_{d,2}, \\
&\eta_{e,3}, \ldots, \eta_{e,N}, \eta_{d,3}, \ldots, \eta_{d,N-1}, \eta_1, \ldots, \eta_N, S) \\
&\overset{(c)}{=} \frac{1}{N} H(\Theta_1, \Theta_2 | \sqrt{12P_1}\Theta_1 + \eta_{e,1}, \sqrt{12P_2}\Theta_2 + \eta_{e,2}, \sqrt{12P_1}\Theta_1 + \eta_{d,1}, \sqrt{12P_2}\Theta_2 + \eta_{d,2}) \\
&\overset{(d)}{\ge} \frac{H(\Theta_1) + H(\Theta_2) + h(\eta_{d,1}) + h(\eta_{d,2}) + h(\eta_{e,1}) + h(\eta_{e,2})}{N} - \frac{h(\sqrt{12P_1}\Theta_1 + \eta_{e,1}) + h(\sqrt{12P_2}\Theta_2 + \eta_{e,2})}{N} \\
&- \frac{h(\sqrt{12P_1}\Theta_1 + \eta_{d,1}) + h(\sqrt{12P_2}\Theta_2 + \eta_{d,2})}{N} \\
&\overset{(e)}{\ge} R_1 + R_2 - \underbrace{\frac{1}{N}\left[\frac{1}{2}\log\left(1 + \frac{P_1}{\sigma_e^2}\right) + \frac{1}{2}\log\left(1 + \frac{P_2}{\sigma_e^2}\right)\right]}_{\text{information leakage on the forward channel}} - \underbrace{\frac{1}{N}\left[\frac{1}{2}\log\left(1 + \frac{P_1}{\sigma_d^2}\right) + \frac{1}{2}\log\left(1 + \frac{P_2}{\sigma_d^2}\right)\right]}_{\text{information leakage on the feedback channel}},
\end{aligned}
\tag{26}
$$

where (a) follows from the fact that Θ_k $(k = 1, 2)$ is a deterministic function of W_k, (b) follows from the fact that $X_{1,i}$ and $X_{2,i}$ are linear combinations of $\eta_1, \ldots, \eta_{i-1}$, and S, (c) follows from the fact that Θ_1, Θ_2, $\eta_{e,1}$, $\eta_{e,2}$, $\eta_{d,1}$, $\eta_{d,2}$ are independent of $\eta_{e,3}, \ldots, \eta_{e,N}$, $\eta_1, \ldots, \eta_N$, $\eta_{d,3}, \ldots, \eta_{d,N}$, and S, (d) follows from the fact that Θ_1, Θ_2, $\eta_{e,1}$, $\eta_{e,2}$, $\eta_{d,1}$, $\eta_{d,2}$ are independent of one another, (e) follows from $H(\Theta_1) = NR_1$, $H(\Theta_2) = NR_2$, and the variance of Θ_k $(k = 1, 2)$ equals $\frac{1}{12}$ as N tends to infinity.

From (26), we conclude that choosing sufficiently large N, the secrecy constraint $\Delta = \frac{H(W_1, W_2 | Z^N, \widetilde{Z}^{N-1})}{N} \ge R_1 + R_2 - \epsilon$ in (4) is guaranteed, which indicates that any pair (R_1, R_2) in $R(\rho^*)$ is achievable with PWS.

3.2. Case 2: $0 \le \rho < \rho^*$

In this case, we show that the pentagon rate region $R(0 \le \rho < \rho^*)$ in Figure 3 is achievable with PWS. We only need to show that the corner point Q is achievable with PWS, then by symmetry, Q' is also achievable with PWS, finally, using time sharing between Q and Q', the line QQ' is achievable with PWS, which indicates that the entire region $R(0 \le \rho < \rho^*)$ is achievable with PWS. The secure coding scheme that achieves Q is briefly explained below. Divide the message W_1 of Transmitter 1 into two parts, where one part together with the message W_2 of Transmitter 2 are encoded by the SK-type scheme shown in case 1, and the other part of W_1 is encrypted by a key which is generated by the channel

noise at the first time instant and this key is only known by the legal parties. In case 1 we have shown that Ozarow's SK-type scheme is achievable with PWS, and note that the other part of W_1 is also achievable with PWS since it is protected by a secret key, which indicates that the whole scheme satisfies PWS. The details of our proposed scheme are given below.

Message splitting: the message W_1 is divided into two independent parts (W_a, W_b), where W_a takes values in $\mathcal{W}_a = \{1, 2, \ldots, 2^{NR_a}\}$, W_b takes values in $\mathcal{W}_b = \{1, 2, \ldots, 2^{NR_b}\}$, and $R_a + R_b = R_1$. W_2 takes values in $\mathcal{W}_2 = \{1, 2, \ldots, 2^{NR_2}\}$. Divide the interval $[-0.5, 0.5]$ into $2^{NR_l}(l \in \{b, 2\})$ equally spaced sub-intervals, and each sub-interval center corresponds to a value in W_l. The center of the sub-interval w.r.t. W_b (W_2) is denoted by Θ_1 (Θ_2), where the variance of Θ_k ($k \in \{1, 2\}$) approximately equals $\frac{1}{12}$.

Secret key generation: at time instant 1, Transmitters 1 and 2 send $X_{1,1} = X_{2,1} = 0$. The legal receiver receives $Y_1 = X_{1,1} + X_{2,1} + \eta_1 = \eta_1$, and transmits Y_1 back to the transmitters. Since Y_1 is continuous, we can generate a secret key K with arbitrary rate from Y_1 and this key is uniformly distributed in $\mathcal{W}_a = \{1, 2, \ldots, 2^{N\tilde{R}_a}\}$.

Encoding-decoding procedure: at time instants 2 and 3, the transmission codewords are exactly the same as those in case 1 at time instants 1 and 2, namely, $X_{1,2} = \sqrt{12P_1}\Theta_1 + S$, $X_{2,2} = 0$, $X_{1,3} = 0$ and $X_{2,3} = \sqrt{12P_2}\Theta_2 + S$.

At time instant $4 \le i \le N$, Transmitters 1 and 2 send

$$X_{1,i} = U_i + V_i = U_i + \sqrt{\frac{(1-\gamma)P_1}{\alpha_{1,i-1}}}\epsilon_{1,i-1}, X_{2,i} = \sqrt{\frac{P_2}{\alpha_{2,i-1}}}\epsilon_{2,i-1}\mathrm{sgn}(\rho_{i-1}), \tag{27}$$

respectively, where U_i is the codeword of the encrypted sub-message $W_a \oplus K$ with transmission power γP_1 $(0 \le \gamma \le 1)$, V_i is the codeword of the sub-message W_b with transmission power $(1-\gamma)P_1$. Here, note that the codeword $U_4^N = (U_4, \ldots, U_N)$ is generated by Shannon's random coding scheme [3], namely, each component of U_4^N is i.i.d. generated according to the Gaussian distribution with zero mean and variance γP_1, and U_4^N is one-to-one mapped to a value of $W_a \oplus K$. In addition, for $4 \le i \le N$, V_i and $X_{2,i}$ (codewords for W_b and W_2) are generated in the same way as the SK-type scheme of case 1, where $U_i + \eta_i$ is viewed as the "channel noise" for the codewords V_i and $X_{2,i}$. Note that $\epsilon_{1,i}$, $\epsilon_{2,i}$, $\alpha_{1,i}$, $\alpha_{2,i}$, ρ_i, and $\mathrm{sgn}(\rho_i)$ are defined in the same way as those in Section 3.1 by replacing η_i by $U_i + \eta_i$.

Decoding procedure: successive cancellation decoding is employed, specifically, first, viewing $U_i + \eta_i$ as the equivalent channel noise and using the SK-type decoding scheme in case 1, for sufficiently large N, W_b and W_2 can be decoded by the legal receiver with arbitrary small decoding error probability if

$$\begin{aligned} R_b &\le \frac{1}{2}\log\left[1 + \frac{(1-\gamma)P_1}{\sigma^2 + \gamma P_1}(1 - \rho^{**2})\right], \\ R_2 &\le \frac{1}{2}\log\left[1 + \frac{P_2}{\sigma^2 + \gamma P_1}(1 - \rho^{**2})\right], \end{aligned} \tag{28}$$

where ρ^{**} is the solution in $(0, 1)$ of

$$\begin{aligned} &(\sigma^2 + \gamma P_1)[\sigma^2 + \gamma P_1 + (1-\gamma)P_1 + P_2 + 2\sqrt{(1-\gamma)P_1 P_2}\rho^{**}] \\ &= \left[\sigma^2 + \gamma P_1 + (1-\gamma)P_1(1 - \rho^{**2})\right]\left[\sigma^2 + \gamma P_1 + P_2(1 - \rho^{**2})\right]. \end{aligned} \tag{29}$$

Here, note that $\frac{N}{N-1}R_b$ and $\frac{N}{N-1}R_2$ are actual transmission rates of W_b and W_2, respectively. For sufficiently large N, $\frac{N}{N-1}R_b$ and $\frac{N}{N-1}R_2$ tend to R_b and R_2, respectively.

After decoding W_b and W_2, the legal receiver subtracts V_i and $X_{2,i}$ from his received signal Y_i, which indicates that the channel noise of the equivalent channel for the transmission of U_i is η_i, then based on the channel coding theorem [3], we conclude that for

sufficiently large N, W_a can be decoded by the legal receiver with arbitrary small decoding error probability if

$$R_a \leq \frac{1}{2}\log\left(1+\frac{\gamma P_1}{\sigma^2}\right). \tag{30}$$

Here, note that $\frac{N}{N-3}R_b$ is the actual transmission rate of W_a, and for sufficiently large N, $\frac{N}{N-3}R_b$ tends to R_a.

From (28) and (30), $R_1 = R_a + R_b$, and letting $\rho = \sqrt{(1-\gamma)}\rho^{**}$, we conclude that any pair (R_1, R_2) in $R(0 \leq \rho < \rho^*)$ is achievable. Now it remains to be shown that any rate pair $(R_1, R_2) \in R(0 \leq \rho < \rho^*)$ satisfies PWS; see the details below.

Equivocation analysis: the eavesdropper's equivocation rate is bounded by

$$\begin{aligned}\frac{H(W_1, W_2|Z^N, \widetilde{Z}^{N-1})}{N} &= \frac{H(W_a, W_b, W_2|Z^N, \widetilde{Z}^{N-1})}{N}\\ &= \frac{H(W_a|Z^N, \widetilde{Z}^{N-1})}{N} + \frac{H(W_b, W_2|W_a, Z^N, \widetilde{Z}^{N-1})}{N}.\end{aligned} \tag{31}$$

The first term in (31) can be calculated by

$$\begin{aligned}\frac{H(W_a|Z^N, \widetilde{Z}^{N-1})}{N} &\geq \frac{H(W_a|Z^N, \widetilde{Z}^{N-1}, U_4^N)}{N} \overset{(a)}{=} \frac{H(W_a|U_4^N)}{N} \overset{(b)}{=} \frac{H(W_a|U_4^N, W_a \oplus K)}{N}\\ &= \frac{H(K|U_4^N, W_a \oplus K)}{N} \overset{(c)}{=} \frac{H(K)}{N} = R_a,\end{aligned} \tag{32}$$

where (a) follows from the Markov chain $W_a \to U_4^N \to (Z^N, \widetilde{Z}^{N-1})$, (b) follows from U_4^N is a deterministic function of $(W_a \oplus K)$, and (c) follows from K is independent of $(W_a \oplus K)$ and U_4^N, and K is uniformly drawn from $\{1, 2, \ldots, 2^{NR_a}\}$.

For the second term in (31), along the lines of the equivocation analysis in case 1, we conclude that

$$\begin{aligned}&\frac{1}{N}H(W_b, W_2|Z^N, \widetilde{Z}^{N-1}, W_a) = \frac{1}{N}H(W_b, W_2|Z^N, \widetilde{Z}^{N-1}, W_a, U_4^N)\\ &\geq R_b + R_2 - \frac{1}{2N}\log\left(1+\frac{P_1}{\sigma_e^2}\right) - \frac{1}{2N}\log\left(1+\frac{P_2}{\sigma_e^2}\right) - \frac{1}{2N}\log\left(1+\frac{P_1}{\sigma_d^2}\right) - \frac{1}{2N}\log\left(1+\frac{P_2}{\sigma_d^2}\right).\end{aligned} \tag{33}$$

Substituting (32) and (33) into (31), choosing sufficiently large N, $\Delta = \frac{H(W_1, W_2|Z^N, \widetilde{Z}^{N-1})}{N} \geq R_1 + R_2 - \epsilon$ is guaranteed, which completes the proof.

4. Discussion

In this section, we show that Ozarow's scheme is in fact a secure finite blocklength (FBL) coding scheme, and characterize its sum rate under fixed coding blocklength, decoding error probability and the eavesdropper's uncertainty about the transmitted messages. Then, we further explain the results via numerical examples.

4.1. The Definition of the Secure FBL Scheme for the AWGN-MAC-E-CF

For the AWGN-MAC-E-CF, the channel's input and output relationship is given in Section 2.1.

A $(N, |\mathcal{W}_1|, |\mathcal{W}_2|, P_1, P_2)$-code under average power constraints consists of:

- Message $W_k (k \in \{1, 2\})$, uniformly drawn in $\mathcal{W}_k = \{1, 2, \ldots, |\mathcal{W}_k|\}$.
- Encoder k with outputs $X_{k,i} = f_{k,i}(W_k, Y_{k,1}^{i-1})$ satisfies the average power constraints

$$\frac{1}{N}\sum_{i=1}^{N} E[X_{k,i}^2] \leq P_k, \tag{34}$$

where $f_{k,i}(\cdot)$ is a (stochastic) function.

- The decoder with outputs
$$(\hat{W}_1, \hat{W}_2) = \psi(Y^N), \tag{35}$$
where ψ is the decoding function of the Receiver.

The average decoding error probability P_{ek} is defined as

$$P_e = Pr[(\hat{W}_1, \hat{W}_2) \neq (W_1, W_2)] = \frac{\sum_{w_1, w_2 \in \mathcal{W}_1, \mathcal{W}_2} Pr\{\psi(Y^N) \neq (w_1, w_2) | (W_1, W_2) = (w_1, w_2)\}}{|\mathcal{W}_1||\mathcal{W}_2|}. \tag{36}$$

In addition, define the eavesdropper's normalized equivocation (also called the secrecy level) as

$$\Delta_f = \frac{H(W_1, W_2 | Z^N, \widetilde{Z}^{N-1})}{H(W_1, W_2)}, \tag{37}$$

where $0 \leq \Delta \leq 1$. The (N, ϵ, δ)-rate pair $(R_1(N, \epsilon, \delta), R_2(N, \epsilon, \delta))$ is achievable with a secrecy level of $\delta (0 \leq \delta \leq 1)$ if for given blocklength N, error probability ϵ and secrecy level δ, there exists a $(N, |\mathcal{W}_1|, |\mathcal{W}_2|, P_1, P_2)$-code described above such that

$$\frac{\log |\mathcal{W}_1|}{N} = R_1(N, \epsilon, \delta), \ \ \frac{\log |\mathcal{W}_2|}{N} = R_2(N, \epsilon, \delta), \ \ P_e \leq \epsilon, \ \ \Delta_f \geq \delta. \tag{38}$$

For the AWGN-MAC-E-CF, the achievable sum-rate is denoted by

$$R_{sum}(N, \epsilon, \delta) = R_1(N, \epsilon, \delta) + R_2(N, \epsilon, \delta), \tag{39}$$

and the maximal sum-rate $R^*_{sum}(N, \epsilon, \delta)$ is the maximum sum-rate $R_{sum}(N, \epsilon, \delta)$ defined in (39).

4.2. Main Result

Theorem 2. *For given decoding error probability ϵ and boding blocklength N, let $R_{sum}(N, \epsilon)$ be the achievable sum-rate of the SK-type scheme for the AWGN-MAC-E-CF without the consideration of secrecy. Then for a given secrecy level δ, if the coding blocklength N in $R_{sum}(N, \epsilon)$ satisfies*

$$NR_{sum}(N, \epsilon) \geq \frac{1}{2(1-\delta)} \log \left[\left(1 + \frac{P_1}{\sigma_e^2}\right) \left(1 + \frac{P_2}{\sigma_e^2}\right) \left(1 + \frac{P_1}{\sigma_d^2}\right) \left(1 + \frac{P_2}{\sigma_d^2}\right) \right], \tag{40}$$

the rate $R_{sum}(N, \epsilon)$ also serves as a lower bound on the maximal sum-rate $R^*_{sum}(N, \epsilon, \delta)$, i.e.,

$$R^*_{sum}(N, \epsilon, \delta) \geq R_{sum}(N, \epsilon), \tag{41}$$

where

$$\begin{aligned} R_{sum}(N, \epsilon) = & \frac{1}{2} \log \left(1 + \frac{P_1 + P_2 + 2\rho^* \sqrt{P_1 P_2}}{\sigma^2}\right) \\ & - \frac{1}{N} \log \left(\left(1 + \frac{P_1 + P_2 + 2\rho^* \sqrt{P_1 P_2}}{\sigma^2}\right) \frac{\sigma_0^2 + \sigma^2}{12\sqrt{P_1 P_2}} \left[Q^{-1}\left(\frac{\epsilon}{2}\right)\right]^2 \right), \end{aligned} \tag{42}$$

ρ^* is the largest solution in $(0, 1)$ of

$$\sigma^2 \left(\sigma^2 + P_1 + P_2 + 2\sqrt{P_1 P_2}\rho\right) = \left[\sigma^2 + P_1(1 - \rho^2)\right] \left[\sigma^2 + P_2(1 - \rho^2)\right], \tag{43}$$

and σ_0^2 satisfies

$$\frac{\sigma_0^2}{\sigma_0^2 + \sigma^2} = \rho^*. \tag{44}$$

Proof. See Section 4.4. □

4.3. Numerical Results

Define the minimum blocklength N satisfying (40) as the PLS requirement blocklength threshold. Figure 4 plots the relationship between secrecy level, decoding error probability, and PLS requirement blocklength threshold for the AWGN MAC with an external eavesdropper and feedback ($P_1 = P_2 = 2, \sigma^2 = 1$). From Figure 4, we conclude that for a fixed decoding error probability, the PLS requirement threshold is increasing while the secrecy level is increasing. Moreover, when the decoding error probability $\epsilon = 10^{-7}$ and the secrecy level $\delta = 0.99$, the PLS requirement blocklength threshold is about 115.

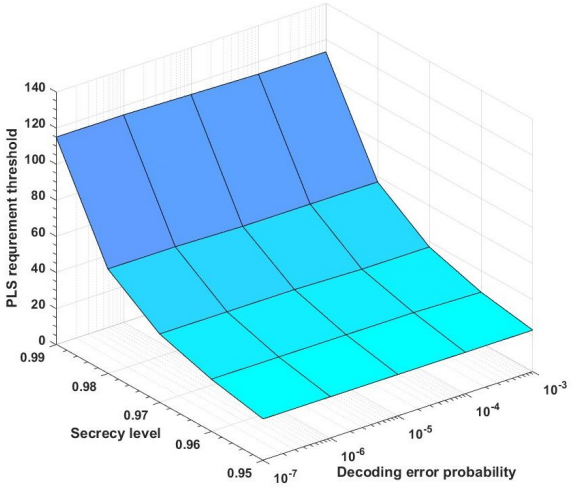

Figure 4. The relationship between secrecy level, decoding error probability, and PLS requirement blocklength threshold for the AWGN MAC with an external eavesdropper and feedback ($P_1 = P_2 = 2$, $\sigma^2 = 1$).

Figure 5 plots the decoding error probability P_e of Ozarow's SK scheme [8] and LDPC code [11] for $P_1 = P_2 = 2$, and the length of transmission bits is 80. From Figure 5, we conclude that compared with LDPC scheme, the average error probability P_e of Ozarow's SK scheme decays much faster with the increasing coding blocklength N.

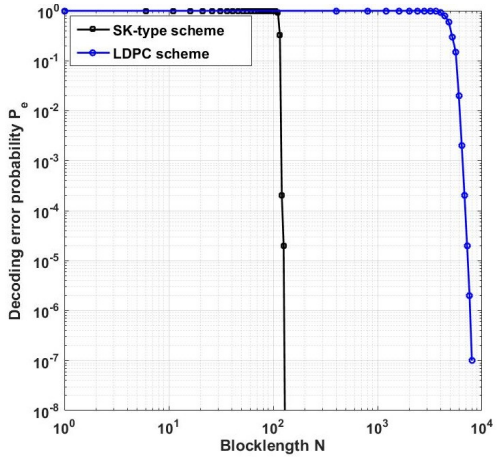

Figure 5. Comparison of the decoding error probability P_e for $P_1 = P_2 = 2$, $\sigma^2 = 1$ and N taking values in $[0, 8000]$.

4.4. Proof of the Theorem 2

Encoding-decoding procudure: in fact, Ozarow's scheme [8] is inherently a secure FBL coding scheme. The encoding and decoding processes are exactly the same as those described in Section 3.1, so we omit the detailed explanation here.

Decoding error probability analysis: the target error probability of the whole scheme is chosen to be ϵ. Then, we let the error probability of transmitting W_k be $P_{e,k}$ which at most $\epsilon/2$, i.e.,

$$P_{e,k} \leq \frac{\epsilon}{2}. \tag{45}$$

From (45) and the error probability analysis in [10], we have

$$R_k(N,\epsilon) = \frac{1}{2}\log\left[1+P_k(1-\rho^{*2})\right] - \frac{1}{2N}\log\left(\left[1+P_k(1-\rho^{*2})\right]^2 \frac{\sigma_0^2+\sigma_k^2}{12P_k}\left[Q^{-1}\left(\frac{\epsilon}{2}\right)\right]^2\right). \tag{46}$$

Let $R_k(N,\epsilon)$ be message W_k's achievable rate of the SK-type scheme for the AWGN-MAC-E-CF without the consideration of secrecy. From (39) and (46), we have $R_{sum}(N,\epsilon)$ which is given in (42).

Equivocation analysis: now we show the above scheme satisfies the PLS requirement when the coding blocklength is larger than a threshold.

$$\begin{aligned}
\Delta_f &= \frac{H(W_1,W_2|Z^N,\widetilde{Z}^{N-1})}{H(W_1,W_2)} \geq \frac{H(W_1,W_2|Z^N,\widetilde{Z}^{N-1},\eta_1,\ldots,\eta_N,S)}{H(W_1,W_2)} \\
&\geq \frac{1}{H(W_1,W_2)} H(W_1,W_2|Z^N,\widetilde{Z}^{N-1},\eta_1,\ldots,\eta_N,S) \\
&= \frac{1}{H(W_1,W_2)} H(W_1,W_2|\underbrace{\sqrt{12P_1}\Theta_1+S+\eta_{e,1}}_{Z_1},\underbrace{\sqrt{12P_2}\Theta_2+S+\eta_{e,2}}_{Z_2},\underbrace{X_{1,3}+X_{2,3}+\eta_{e,3},\ldots,X_{1,N}+X_{2,N}+\eta_{e,N}}_{Z_3,\ldots,Z_N}, \\
&\underbrace{\sqrt{12P_1}\Theta_1+S+\eta_1+\eta_{d,1}}_{\widetilde{Z}_1},\underbrace{\sqrt{12P_2}\Theta_2+S+\eta_2+\eta_{d,2}}_{\widetilde{Z}_2},\underbrace{X_{1,3}+X_{2,3}+\eta_3+\eta_{d,3},\ldots,X_{1,N-1}+X_{2,N-1}+\eta_{N-1}+\eta_{d,N-1}}_{\widetilde{Z}_3,\ldots,\widetilde{Z}_{N-1}}, \\
&\eta_1,\ldots,\eta_N,S) \\
&\overset{(d)}{=} \frac{1}{H(W_1,W_2)} H(W_1,W_2|\sqrt{12P_1}\Theta_1+\eta_{e,1},\sqrt{12P_2}\Theta_2+\eta_{e,2},\sqrt{12P_1}\Theta_1+\eta_{d,1},\sqrt{12P_2}\Theta_2+\eta_{d,2}, \\
&\eta_{e,3},\ldots,\eta_{e,N},\eta_{d,3},\ldots,\eta_{d,N-1},\eta_1,\ldots,\eta_N,S) \\
&\overset{(e)}{=} \frac{1}{H(W_1,W_2)} H(W_1,W_2|\sqrt{12P_1}\Theta_1+\eta_{e,1},\sqrt{12P_2}\Theta_2+\eta_{e,2},\sqrt{12P_1}\Theta_1+\eta_{d,1},\sqrt{12P_2}\Theta_2+\eta_{d,2}) \\
&\overset{(f)}{\geq} \frac{H(W_1,W_2)+h(\eta_{d,1})+h(\eta_{d,2})+h(\eta_{e,1})+h(\eta_{e,2})}{H(W_1,W_2)} - \frac{h(\sqrt{12P_1}\Theta_1+\eta_{e,1})+h(\sqrt{12P_2}\Theta_2+\eta_{e,2})}{H(W_1,W_2)} \\
&- \frac{h(\sqrt{12P_1}\Theta_1+\eta_{d,1})+h(\sqrt{12P_2}\Theta_2+\eta_{d,2})}{H(W_1,W_2)} \\
&\overset{(g)}{\geq} 1 - \frac{\log\left(1+\frac{P_1}{\sigma_e^2}\right)+\log\left(1+\frac{P_2}{\sigma_e^2}\right)+\log\left(1+\frac{P_1}{\sigma_d^2}\right)+\log\left(1+\frac{P_2}{\sigma_d^2}\right)}{2NR_{sum}(N,\epsilon)},
\end{aligned} \tag{47}$$

where (d) follows from the fact that $X_{1,i}$ and $X_{2,i}$ are linear combinations of $\eta_1,\ldots,\eta_{i-1}$, and S, (e) follows from the fact that Θ_1, Θ_2, $\eta_{e,1}$, $\eta_{e,2}$, $\eta_{d,1}$, $\eta_{d,2}$ are independent of $\eta_{e,3},\ldots,\eta_{e,N}$, $\eta_1,\ldots,\eta_N$, $\eta_{d,3},\ldots,\eta_{d,N}$, and S, (f) follows from the fact that W_1, W_2, $\eta_{e,1}$, $\eta_{e,2}$, $\eta_{d,1}$, $\eta_{d,2}$ are independent of one another and the fact that Θ_k $(k=1,2)$ is a deterministic function of W_k, (g) follows from the fact that $H(W_1,W_2) = NR_{sum}(N,\epsilon)$($R_{sum}(N,\epsilon)$ is defined in Theorem 2) , and the maximum differential entropy lemma [3]. Substituting (47) into (38), the secrecy constraint

$$\Delta \geq 1 - \frac{\log\left(1+\frac{P_1}{\sigma_e^2}\right)+\log\left(1+\frac{P_2}{\sigma_e^2}\right)+\log\left(1+\frac{P_1}{\sigma_d^2}\right)+\log\left(1+\frac{P_2}{\sigma_d^2}\right)}{2NR_{sum}(N,\epsilon)} \geq \delta \tag{48}$$

is guaranteed by choosing blocklength N such that

$$NR_{sum}(N,\epsilon) \geq \frac{1}{2(1-\delta)} \log\left[\left(1+\frac{P_1}{\sigma_e^2}\right)\left(1+\frac{P_2}{\sigma_e^2}\right)\left(1+\frac{P_1}{\sigma_d^2}\right)\left(1+\frac{P_2}{\sigma_d^2}\right)\right]. \quad (49)$$

The proof of Theorem 2 is completed.

5. Conclusions and Future Work

In this paper, we show that for the AWGN-MAC-E-CF, the traditional secret key feedback scheme is not optimal, and propose an optimal scheme that achieves the secrecy capacity region of the AWGN-MAC-E-CF, which combines the linear feedback coding scheme for the same model without the secrecy constraint and the secret key scheme. Possible future work could consist of checking whether this kind of hybrid scheme is still optimal for other multi-user AWGN channel models in the presence of an external eavesdropper and channel feedback.

Author Contributions: Formal analysis, H.Y. and G.X.; Writing—original draft, H.Y.; Writing—review & editing, B.D.; Supervision, B.D. All authors have read and agreed to the published version of the manuscript.

Funding: This paper was supported by the National Key Research and Development Program of China under Grant 2022YFA1005000, the National Natural Science Foundation of China under Grants 62071392, U21A20454; in part by the Natural Science Foundation of Sichuan under Grant 2022NSFSC0484; in part by the central government to guide local scientific and technological development under Grant No. 2021ZYD0001; and in part by the 111 Project No. 111-2-14.

Institutional Review Board Statement: Not applicable.

Data Availability Statement: Not applicable.

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

Abbreviations

The following abbreviations are used in this manuscript:

PLS	Physical layer security
AWGN	Additive white Gaussian noise
PWS	Perfect weak secrecy
MAC	Multiple-access channel
AWGN-MAC-E-CF	Multiple-access channel with an external eavesdropper and channel feedback
SK	Schalkwijk-Kailath
FBL	Finite blocklength

References

1. Wyner, A.D. The wire-tap channel. *Bell Syst. Tech. J.* **1975**, *54*, 1355–1387. [CrossRef]
2. Leung-Yan-Cheong, S.K.; Hellman, M.E. The Gaussian wire-tap channel. *IEEE Trans. Inf. Theory* **1978**, *24*, 451–456. [CrossRef]
3. Gamal, A.E.; Kim, Y.-H. *Network Information Theory*; Cambridge University Press: New York, NY, USA, 2012.
4. Ahlswede, R.; Cai, N. Transmission, identification and common randomness capacities for wire-tap channels with secure feedback from the decoder. In *Identification and Other Probabilistic Models: Rudolf Ahlswede's Lectures on Information Theory*; Springer: Berlin, Germany, 2006; pp. 258–275.
5. Ardestanizadeh, E.; Franceschetti, M.; Javidi, T.; Kim, Y. Wiretap channel with secure rate-limited feedback. *IEEE Trans. Inf. Theory* **2009**, *55*, 5353–5361. [CrossRef]
6. Lai, L.; Gamal, H.E.; Poor, H.V. The Wiretap Channel with Feedback: Encryption Over the Channel. *IEEE Trans. Inf. Theory* **2008**, *54*, 5059–5067. [CrossRef]
7. Wei, C.; Lin, M.; Dai, B. Some new results on the Gaussian wiretap feedback channel. *Entropy* **2019**, *21*, 817. [CrossRef]
8. Ozarow, L. The capacity of the white Gaussian multiple access channel with feedback. *IEEE Trans. Inf. Theory* **1984**, *30*, 623–629. [CrossRef]
9. Gunduz, D.; Brown, D.R.; Poor, H.V. Secret communication with feedback. In Proceedings of the International Symposium on Information Theory and Its Applications, (ISITA), Auckland, New Zealan, 7–10 December 2008; pp. 1–6.

10. Schalkwijk, J.; Kailath, T. A coding scheme for additive noise channels with feedback–I: No bandwidth constraint. *IEEE Trans. Inf. Theory* **1966**, *12*, 172–182. [CrossRef]
11. Sharifi, S.; Tanc, A.K.; Duman, T.M. LDPC code design for the two-user Gaussian multiple access channel. *IEEE Trans. Wireless Commun.* **2016**, *15*, 2833–2844. [CrossRef]