编码器带有因果状态信息的任意变化窃听信道上的强保密通信

陈一齐[1]，董晨[2]，骆源[2]
（1.慕尼黑工业大学理论信息技术实验室，慕尼黑 80333；2.上海交通大学计算机学院，上海 200240）

摘　要：为了在存在干扰者和窃听者，且编码器在每个发送时刻可以检测到干扰信号的通信系统中进行可靠且保密的通信，提出一种编码方案并研究该通信系统的理论通信能力极限。该编码方案利用每个时刻检测到的干扰信号对信道输入进行针对性编码，首先构造出了用于组合信道上保密可靠通信的码。基于此码，利用一组对码字的随机置换构造出用于可以抵抗任意变化的干扰信号的强保密通信码，得到了所研究通信系统的强保密通信容量的下界。通过分析可得，当所构造的编码方案用于主信道比窃听信道严格低噪的情况时，达到了最优强保密容量，是该情况下的最优编码方案。

关键词：任意变化信道；窃听信道；强保密通信；可靠通信；因果状态信息
中图分类号：TN911
文献标志码：A
DOI：10.11959/j.issn.1000–436x.2026070

Strong secrecy of arbitrarily varying wiretap channels with causal side information at the encoder

Chen Yiqi[1], Dong Chen[2], Luo Yuan[2]
1. Chair of Theoretical Information Technology, Technical University of Munich, Munich 80333, Germany
2. School of Computer Science, Shanghai Jiao Tong University, Shanghai 200240, China

Abstract: To achieve reliable and secure communication over a channel in presence of a jammer and an eavesdropper, in which the encoder observes the jamming signal before transmitting each input symbol, a coding scheme was proposed, and the fundamental limit of the communication system was studied. The proposed coding scheme encoded each message using the observed jamming signal and was constructed as a code for reliable and secure communication over compound channels. Then, a set of random permutations over the codewords was used and the compound channel code was transformed into a code that could achieve reliable and secure communication over channels against arbitrarily varying jamming signals. A lower bound of the strong secrecy communication rate has been established. By analyzing the code over channels whose main channel is severely less noisy than the wiretap channel, the strong secrecy capacity of the channel is established and the proposed coding scheme is the optima scheme.

Keywords: arbitrarily varying channel, wiretap channel, strong secrecy communication, reliable communication, causal state information

0　引言

在点对点通信场景中，信道可以用一个条件分布$P_{Y|X}$来表示。香农开创性的研究[1]证明了能够可靠通信的最大码率为输入与输出之间的最大互信息$\max\limits_{P_X} I(X;Y)$，其中X为信道的输入随机变量，Y为信道的输出随机变量，P_X为X的分布。显然，要

收稿日期：2026–01–02；修回日期：2026–03–12
通信作者：骆源，yuanluo@sjtu.edu.cn
基金项目：国家自然科学基金资助项目（No.62571321）
Foundation Items：The National Natural Science Foundation of China (No.62571321)

达到最大可达码率，系统设计者需要知道条件分布$P_{Y|X}$，也就是信道的统计特性。从X到Y之间的随机性是由通信系统中的随机噪声带来。在实际通信中，通信状况往往会受环境的影响。为了对这一情况进行建模和理论分析，香农在文献[2]中引入了带信道状态的信道，并给出了在编码器以因果方式知晓信道状态信息情况下的信道容量。在文献[2]的模型中，尽管信道的状态会发生变化，但始终服从一个固定的分布以独立同分布的方式生成，并且该分布发送方和接收方都知道。文献[3]首次研究了一种更加复杂的信道模型：如果信道的状态分布未知，并且一直在发生变化，信道的容量表达式又是什么？在这种情况下，信道状态序列甚至可能以一种非独立的方式生成，并且收发双方都不知道具体的分布。这一模型被称为任意变化信道（arbitrarily varying channel, AVC）。这一模型可以从两方面来理解，一种是存在恶意干扰者的情况：假设在通信过程中，一个干扰者在不知道发送者所发送消息的情况下，不断地向信道发送干扰字符来破坏发送方与接收方之间的通信。由于干扰者的编码策略对发送方和接收方都是未知的，此时发送方无法完全得知信道的统计特性。另一种可能的情况则是在无协作的通信网络中，如在一个无人机网络中，如果无人机之间没有良好的协作，无人机A与B之间的通信信号就有可能成为无人机C与D之间通信的干扰信号。为了保证在存在干扰情况下可靠通信可以进行，通信系统设计者需要考虑最坏的情况：当干扰者以完全任意的方式变化其干扰信号，在任意可能的干扰信号下，可靠通信依然可以进行。本文仅讨论平均译码错误概率约束下的通信。

AVC有着与许多普通离散无记忆信道截然不同的性质。例如，对于许多离散无记忆信道，发送方与接收方之间的公共随机性并非必须的。也就是说，达到信道容量的编码方案并不需要公共随机性。对于AVC来说，其有公共随机性存在时的信道容量可以严格大于其没有公共随机性存在时的信道容量。事实上，如果将上述两种情况称为随机编码容量与确定性编码容量，Ahlswede[4]证明了AVC的确定性编码容量为0或者等于其随机编码容量，该性质被称为AVC的二分性。进一步，Csiszar[5]给出了确定性编码容量为0的充分必要条件，称为AVC的可对称性。在没有公共随机性的情况下，一个可对称化的AVC容量为0。文献[4]进一步证明了用于实现随机编码可靠通信所需要的公共随机性数量大小仅为关于码长的多项式级，这一结论被称为消除技术（elimination technique, ET）。这意味着当信道的确定性编码容量大于0时，发送方可以在本地进行一次随机试验，并用一个码率趋近于0的前缀码来向接收方描述随机试验的结果，以达到和拥有公共随机性相同的通信效果。ET的重要性在于它证明了当AVC的确定性编码容量为正时，公共随机性将不再被需要。在AVC的通信中，公共随机性需要使用额外的可靠且保密的方式在发送方与接收方之间共享，显然这会对通信系统带来额外的开销。公共随机性在通信系统中的其他应用包括随机种子模块化编码（seeded modular coding, SMC）[6-8]，关于在收发双方之间提取公共随机性的研究参考文献[9-12]。文献[13]给出了发送方以非因果方式知道整个干扰序列情况下任意变化信道的容量，进一步证明了在整个干扰序列都提前被发送方知道的情况下，信道的对称性不会对编码容量产生影响。文献[13]的另一个重要贡献是鲁棒性技术（robustification technique, RT）。该技术证明了给定一个用于组合信道（compound channel, CC）上可靠通信的码，总是可以通过随机置换的方式构造出一个用于AVC的随机编码，这里的公共随机性则是对码字置换方式的选择。

在现代无线通信网络中，保证通信的保密性同样非常重要。在考虑通信的保密性时，假设通信系统中存在一个除了合法接收方之外的窃听者。窃听者观测到一个不同于合法接收方的信道输出，并试图获取发送消息的信息。这一模型被称为窃听信道，由Wyner[14]提出。在文献[14]中，窃听信道输出是合法主信道输出的退化版本。文献[15]中将这一模型拓展到了一般窃听信道的情况，即窃听信道不是主信道的退化。近年来，关于窃听信道的研究包括多接入窃听信道[16-18]、组合信道[19-20]、中继信道[21-22]、带反馈的窃听信道[23-25]等。对于带信道状态的窃听信道，文献[26]给出了编码器带有非因果信道状态序列的窃听信道的保密容量下界和上界，其编码方案结合了Gel’fand-Pinsker编码和窃听编码。文献[26]考虑的是弱安全约束下的保密通信，文献[27]将通信场景拓展到了语义安全约束。文献[28]研究了编码器带有因果状态信息（causal

state information, CCSI）且接收方拥有信道状态信息的窃听信道，并给出了一种新颖的编码方案。编码器利用观测到的信道状态序列和信道输出是一对相关序列这一事实，构造出一个只能由合法接收方恢复的密钥，并利用这一密钥来加密消息。该文献给出了弱保密约束下可达容量的下界。文献[29]首先将模型拓展到了只有发送方以因果方式观测到信道状态序列的情形，并通过基于无损压缩的密钥协议给出了在强保密约束下的可达容量下界和特殊情况下的强保密容量。文献[30]将点对点信道模型拓展到了多接入信道，提出了一种新的基于有损压缩的密钥协议，并给出了一般情况下的强保密容量区域内界和特殊情况下的容量区域。本文研究的是AVC上的保密通信问题，即在前文所介绍的AVC通信系统中，存在第二个接收方作为窃听者，并将该模型称为任意变化窃听信道（arbitrarily varying wiretap channel, AVWC）。AVC上的保密通信最早在文献[31]中被提出，且该文献的主要结论是AVWC在弱保密约束下容量的下界。文献[32]将结论拓展到了强保密约束的情形。但是文献[31-32]都假设了在窃听信道所有可能的状态中存在一个“最坏”信道，只需要保证在这个最坏信道上的保密通信就可以实现整个AVWC的保密通信。一般化的AVWC、任意变化多接入窃听信道以及带状态约束的AVWC容量结论可参考文献[33-35]。

本文所研究的是编码器带因果状态信息的任意变化窃听信道（AVWC with causal channel state information, AVWC-CCSI）的强保密通信问题。带有CCSI的模型意味着编码器在发送信号前就知道了本次传输的信道状态，因此可以利用这一点对发送的符号进行编码。该模型常见于认知无线电系统（次级用户先检测主要用户对频谱的使用情况再进行编码和发送）或水印系统（发送方将代表水印的消息通过编码嵌入代表覆盖信号的信道状态中，并在接收方端恢复出水印）。在来自不同组织的多个无人机集群构成的复杂通信网络中，无人机试图与各自的地面基地进行通信。如果不同集群之间没有良好的协作，来自其他集群的通信信号就会成为随机变化的干扰信号。在每次发送信号前，无人机可以利用传感器检测当前周围的通信情况作为信道状态信息，同时为了保证发送的消息只能由对应的基站译码，对消息的编码必须确保能够达到保密性要求。本文首先通过研究CC上的强保密通信，再通过RT构造出用于AVWC的随机编码。最后，当主信道的确定性编码容量大于0时，通过ET将所需的随机性在发送方处用前缀码进行编码来构造出一个达到相同速率的确定性编码。尽管本文对RT和ET的使用与文献[32]类似，如在前文所提到的，文献[32]假设了一个“最坏情况”的窃听者，在进行安全分析时只需要对这一窃听者进行分析。这实际上将AVWC中窃听者的信道变成了一个单个状态的信道，大大简化了安全分析的复杂度。本文所研究的模型不对信道做任何的假设，因此研究的是最一般化AVWC的强保密通信。定理1给出了该模型强保密通信容量的下界。当主信道相比窃听信道严格低噪时，本文方案是最优的，相应的容量结论如推论1所示。

1 模型与定义

本文使用大写字母X、小写字母x和花写字母$\mathcal{X}$分别表示随机变量、随机变量的样本值和随机变量的符号集。长度为n的随机序列，随机序列样本值分别表示为$X^n=(X_1,X_2,\cdots,X_n)$和$x^n=(x_1,x_2,\cdots,x_n)$。随机变量X的分布表示为P_X。一对随机变量(X,Y)的联合分布和条件分布分别表示为P_{XY}和$P_{Y|X}$。对于给定序列x^n，令$N(x|x^n)$为序列x^n中符号x出现的次数，$\mathcal{T}^n_{P_{X,\delta}}$为关于分布$P_X$的$\delta$－典型集使所有$x^n\in\mathcal{T}^n_{P_{X,\delta}}$满足

$$\left|N(x|x^n)-nP_X(x)\right|\leqslant n\delta,\ \forall x\in\mathcal{X} \tag{1}$$

类似的，定义联合典型集$\mathcal{T}^n_{P_{XY,\delta}}$为序列对$(x^n,y^n)$的集合满足

$$\left|N(x,y|x^n,y^n)-nP_{XY}(x,y)\right|\leqslant n\delta,\ \forall x\in\mathcal{X},y\in\mathcal{Y} \tag{2}$$

定义条件典型集$\mathcal{T}^n_{P_{XY,\delta}}[x^n]$为

$$\mathcal{T}^n_{P_{XY,\delta}}[x^n]=\{y^n\in\mathcal{Y}^n:(x^n,y^n)\in\mathcal{T}^n_{P_{XY,\delta}}\} \tag{3}$$

需要注意的是，对于给定联合分布P_{XY}，典型集、联合典型集以及条件典型集的差错系数δ可能不同。根据文献[36]中引理2.10，由P_X和P_{XY}分别定义的典型集其差错系数相差为一个与符号集$\mathcal{Y}$大小线性相关的系数。在本文的证明中，只需要保证δ随着码长$n\to\infty$而趋近于0。因此，为了简便起见，下文的证明不区分不同典型集的差错系数，统

一写作δ。更多关于典型集的性质参考文献[37]。

特别的，当$\delta=0$时，$P_X(x)=\dfrac{N(x|x^n)}{n}$。此时每个符号的概率等于其出现的频率。将满足这一性质的序列的集合写作$\mathcal{T}_{P_X}^n$，并称其为关于P_X的型集合。型集合$\mathcal{T}_{P_X}^n$中每个序列的型为P_X，本文的证明会大量使用信道状态的分布和型。为了简便起见，本文用q表示信道状态S的分布，用$\hat{q}$表示一个给定信道状态序列的型。关于型的性质参考文献[36]。

1.1　信道模型

本节给出本文所研究的信道模型的定义。

定义 1　任意变化窃听信道$\mathcal{W}=\{W_s:s\in\mathcal{S}\}$由输入字符集$\mathcal{X}$、信道状态字符集$\mathcal{S}$、信道输出字符集$\mathcal{Y},\mathcal{Z}$以及一组条件分布$W_s$定义。每一个$W_s$是从输入字符集$\mathcal{X}$到输出字符集$\mathcal{Y}\times\mathcal{Z}$的条件分布。因此，在需要表明随机变量之间的依赖关系时，也将W_s写作条件分布$W_{YZ|XS}$。给定信道状态序列s^n和输入序列x^n，信道输出y^n和z^n的概率为

$$W_{YZ|XS}^n(y^n,z^n|x^n,s^n)=\prod_{i=1}^n W_{YZ|XS}(y_i,z_i|x_i,s_i)=\prod_{i=1}^n W_{s_i}(y_i,z_i|x_i) \tag{4}$$

其中，Y^n是主信道的输出，Z^n是窃听信道的输出。

本文所考虑的AVWC-CCSI模型如图1所示。编码器要向译码器发送消息M。在每个时刻i，干扰者以系统其他参与者都未知且任意的方式生成一个干扰信号S_i，而编码器在每个发送时刻的开端可以检测到这一干扰信号，并生成一个信道输入信号X_i。每个时刻信道产生两个输出，分别为Y_i和Z_i。其中Y_i为译码器可以观测到的输出，Z_i为窃听者所观测到的信道输出。译码器需要在传输结束后进行译码并输出译码结果$\hat{M}$，窃听者则会根据所观测到的窃听信道输出，推测所发送的消息。

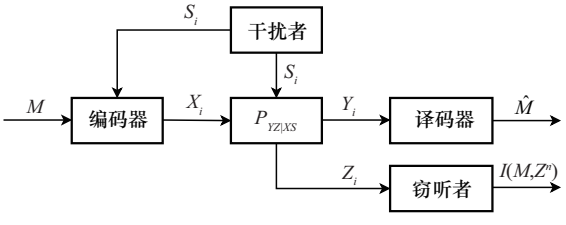

图1　编码器带因果状态信息的任意变化窃听信道模型

对于每个任意变化信道$\mathcal{W}=\{W_s:s\in\mathcal{S}\}$，可以定义一个等价平均信道$\bar{\mathcal{W}}=\{W_q:q\in\mathcal{Q}(\mathcal{S})\}$，其中$\mathcal{Q}(\mathcal{S})$是$\mathcal{S}$上所有概率分布的集合。

$$W_q(y,z|x)=\sum_{s\in\mathcal{S}}q(s)W_s(y,z|x),\forall x,y,z \tag{5}$$

$\bar{\mathcal{W}}$同样是一个AVC。此时，该信道的信道状态为原始信道状态的概率分布。从输入到输出的转移概率为

$$W_{q^n}^n(y^n,z^n|x^n)=\prod_{i=1}^n W_{q_i}(y_i,z_i|x_i) \tag{6}$$

文献[1]证明了AVC的容量与其等价平均信道的容量相同。本文进一步定义一个组合信道$\mathcal{W}_{\mathrm{COM}}=\{W_q:q\in\mathcal{Q}(\mathcal{S})\}$，其信道条件分布和信道状态的联合分布满足

$$W_q(y^n,z^n|x^n,s^n)q^n(s^n)=\prod_{i=1}^n W_q(y_i,z_i|x_i)q(s_i) \tag{7}$$

可以看出，$\mathcal{W}_{\mathrm{COM}}$和$\mathcal{W}$的区别在于，组合信道的信道状态分布在整个输入序列的传输过程中保持不变。

AVC相比普通离散无记忆信道最大的不同点在于发送方与接收方之间的公共随机性有时能严格提高其可靠通信速率，而对于普通的离散无记忆信道，达到信道容量不需要公共随机性。为了更好地理解模型，可以将AVC看作是存在一个干扰者的通信模型。干扰者控制着信道状态并试图破坏发送方与接收方之间的通信。当一个AVC是可对称化的信道时（定义2），干扰者可以任意从码本中选择一个码字并基于该码字生成信道状态序列。在这种情况下译码器将无法分辨被发送方选择的码字和被干扰者选择的码字。

定义 2　对于给定的任意变化信道$\mathcal{W}=\{W_s:s\in\mathcal{S}\}$，如果存在一个条件分布$T:\mathcal{X}\to\mathcal{S}$满足

$$\sum_s W(y|x,s)T(s|x')=\sum_s W(y|x',s)T(s|x) \tag{8}$$

则对所有的$x,x'\in\mathcal{X},y\in\mathcal{Y}$都成立，则该任意变化信道是可对称化的。

前文讨论了任意变化信道$\mathcal{W}$的等价平均信道$\bar{\mathcal{W}}$。对于一个码本中的码字x^n，可以定义n个分布$T_{S|x_i}$以及等价平均信道$W_{T_{S|x_i}},i=1,\cdots,n$。显然，由对称性的定义，对于可对称化的AVC，发送方选择码字x^n、干扰者选择码字$x^{n\prime}$以及分布$T_{S^n|x^{n\prime}}$产生的平均信道的输出统计特性与发送方选择码字$x^{n\prime}$和干扰者选择码字x^n产生的平均信道的输出统计特性是相同的。因此，接收方无法分辨这两个码字。此时，任何确定性编码方案都无法达到一个正的通信

速率，因此该信道的确定性编码容量为0。这里的确定性描述的是编码方案和码本。与之对应的是随机编码和随机编码容量。这里本文简单叙述随机编码和确定性编码的区别。在可达性证明中，通过随机生成一个码本并证明在对码本取期望后可以达到足够小的译码错误概率，可以说明至少存在一个码本的具体实现可以达到足够小的译码错误概率。一旦该码本被确定，消息到码本的映射是确定的，这就是确定性编码。随机编码是分布在一组确定性编码上的随机变量。为此，需要额外假设发送方与接收方之间存在一个公共随机变量。每次传输消息前，该公共随机变量进行一次随机试验并将结果通过额外的可靠且保密的途径告知发送方与接收方。随机试验的结果决定了随机编码的具体实现方式。接下来给出具体定义。首先，给出确定性编码的定义。

定义3 用于AVWC-CCSI的确定性编码(n,R,f,g)包括：1) 一个消息集$\mathcal{M}=[1:2^{nR}]$；2) 一系列随机编码器$f_i:\mathcal{M}\times\mathcal{S}^i\to\mathcal{X},i=1,2,\cdots,n$；3) 一个译码器$g:\mathcal{Y}^n\to\mathcal{M}$。

注意该定义允许f_i为一个随机编码器，这意味着$f_i(M,S^{i-1})$是分布在$\mathcal{X}$上的随机变量。

定义4 用于AVWC-CCSI的随机编码(n,R,F,G,Γ)为分布在一组确定性编码$\left(n,R,f^\gamma,g^\gamma\right)_{\gamma\in\Gamma}$上的随机变量。其中$\Gamma$为服从分布$\mu$的公共随机变量。每一个具体实现$(n,R,f^\gamma,g^\gamma)$由定义3所定义。

本文使用消息M与窃听信道输出Z^n之间的互信息来衡量信息泄露程度。接下来，给出可达码率和强保密容量的定义。

定义5 如果对于任意的正数ϵ，存在一个足够大的正整数N满足对于任意的$n>N$，存在一个(n,R,F,G,Γ)码满足

$$\Pr\left\{M\neq\hat{M}|s^n\right\}\leqslant\epsilon,I\left(M;Z^n|s^n\right)\leqslant\epsilon \tag{9}$$

对任意$s^n\in\mathcal{S}^n$都成立，则码率R在随机编码下可达，其中$\hat{M}$为译码结果，即译码器对所发送消息的估计。该模型的随机编码强保密通信容量C_R为随机编码可达码率的上确界，下标R表示随机编码。对应的，若存在确定性编码方案(n,R,F,G,Γ)满足译码错误概率和强保密约束，则称对应的码率R在确定性编码下可达。该模型的确定性编码强保密通信容量C_D为确定性编码可达码率的上确界，下标D表示确定性编码。

1.2 主要结论

本文的主要结论为AVWC-CCSI的强保密容量下界。下文通过在互信息和熵的符号中使用下标q来表示该互信息所涉及随机变量的联合分布中S的分布为q。例如，$I_q(X;Y)$表示该互信息中随机变量(X,Y)的联合分布满足$\sum_s P_X q\sum_z W_{YZ|XS}$。

定理1 AVWC-CCSI的随机编码强保密容量C_R满足

$$\min_{q,q'}\max_{P_{U\mathrm{V}}P_{X|\mathrm{US}}}\left(I\left(U;Y_q|V\right)-I\left(U;Z|V,S\right)\right)\geqslant C_R\geqslant \max_{P_UP_{X|\mathrm{US}}}\left(\min_q I_q(U;Y)-\max_{q'}I_{q'}(U;Z)\right) \tag{10}$$

其中，随机变量的联合分布满足$q,P_UP_{X|US}P_{Y|XS}$和q' $P_UP_{X|US}P_{Z|XS}$，$P_{Y|XS}$和$P_{Z|XS}$分别是$W_{YZ|XS}$关于Y和Z的边缘分布。如果该信道的主信道$P_{Y|XS}$是不可对称化的，则其确定性编码容量C_D同样满足式(10)。

证明见第2节。

注1 对于带因果状态信息的信道，在没有安全约束的情况下，由于互信息是关于信道转移概率$P_{Y|US}$的凸函数，函数的最大值总是在端点处取到，即可以将条件概率$P_{X|US}$替换成一个关于U和S的确定性函数$x(u,s)$。基于同样的理由，由于$I_{q'}(U;Z)$是关于$P_{Z|U}$的凸函数，而$P_{Z|U}$是关于q'的线性函数，因此$I_{q'}(U;Z)$同样是关于q'的凸函数，其最大值由端点取到。因此

$$\max_{q'}I_{q'}(U;Z)=\max_s I\left(U;Z|S=s\right) \tag{11}$$

此外，将$P_{X|US}$替换为$P_{X|U}$并令$U=X$恢复了文献[32]中任意变化窃听信道的强保密容量下界。此时的发送方没有关于信道状态的信息。尽管下界表达式相同，本文所使用的证明不需要假设存在一个最坏窃听者。

注2 定理1中的容量下界是两个互信息的差。其中第一项$\min_q I_q(U;Y)$是在主信道中进行可靠通信的可达速率，第二项$\max_{q'}I_{q'}(U;Z)$则是为了达到强保密通信的额外开销。简单地说，本文方案是基于经典的窃听信道编码，在编码器端引入了额外的局部随机性。在常规的无安全约束的信道中，每个消息对应码本中的一个码字。当有窃听者存在时，这样的一一对应关系会泄露更多关于消息的信息。

因此，本文为每个消息生成一个子码本。当需要发送某个消息时，编码器从消息对应的子码本中随机挑选一个码字。当每个子码本的大小大于$\max\limits_{q'} I_{q'}(U;Z)$时，窃听者在任何可能的状态序列$s^n$下获取的关于消息的信息都会非常小。注意到该下界对第一项互信息关于信道的状态分布取了最小，而对于第二项窃听信道的开销又关于信道状态分布取了最大，这是因为信道状态在以一种未知的方式任意变化。为了确保在任何可能的信道状态序列下可靠通信和强保密通信可以同时满足，必须考虑最坏的情况。

注3　定理1中上下界之间的差距来自两方面。第一，外界的互信息条件上有一个额外的随机变量V，这意味着在对上下界表达式进行最优化时，上界有着更多的优化自由度。第二，由于上下界的互信息表达式是两个互信息的差，它们不再是关于信道状态分布q的凸函数。根据Minimax定理，通常有$\min\limits_{x}\max\limits_{y} f(x,y) \geqslant \max\limits_{y}\min\limits_{x} f(x,y)$。下文将给出一个上下界重合的特殊情况。

注4　当编码器观测到的是不完美的信道状态信息（channel state information, CSI）时，可以用一个条件概率$P_{V|S}$来表示从信道状态到编码器端的随机转移概率分布。显然利用对组合窃听信道（compound wiretap channel, CWC）构造编码方案再转换成用于任意变化窃听信道的码，不完美的CSI并不影响可达性证明，只需要将生成码字的条件概率从$P_{X|US}$改写成$P_{X|VS}$即可。

接下来，定义一类特殊的任意变化窃听信道。如果对于任意的分布$P_U P_{X|US}$，总有

$$\min_{q} I_q(U;Y) \geqslant \max_{s} I(U;Z|S) \tag{12}$$

则该任意变化窃听信道是严格低噪的。对于严格低噪的任意变化窃听信道，有如下容量结论。

推论1　严格低噪的AVWC-CCSI随机编码容量为

$$C_R = \max_{P_{X|S}} \min_{q\in\mathcal{P}(\mathcal{S})} I_q(X;Y) - \max_{s\in\mathcal{S}} I(X;Z|S) \tag{13}$$

若该AVWC的主信道$P_{Y|XS}$不可对称化，则其确定性编码容量为

$$C_D = C_R \tag{14}$$

证明见第3节。该最优容量结论的证明依赖于严格低噪的假设。该假设可以在逆定理的证明中消去辅助随机变量U。而在正定理的可达性证明中，总是可以令$U=X$，以此来证明容量的上界是可达的。

2　定理1的证明

本节给出定理1的证明。证明分成三部分：首先，通过构造一套编码方案来证明对于一个给定信道状态分布，发送方拥有CCSI的情况下该信道的强保密可达速率；其次，在第一步所提出编码方案的基础上，对于CWC构造出一个不依赖于具体信道状态分布的编码方案；最后，通过第二步中用于组合信道的编码方案构造出一个可以用于任意变化窃听信道的方案。

2.1　信道状态分布固定时的强保密可达速率

本节的目标是对一个固定的信道状态分布q，构造一个可以实现强保密可靠通信的编码方案。为了确保该方案可以进一步扩展到组合信道和任意变化信道，本节所提出的编码方案需满足$I(M;Z^n|S^n)\leqslant\epsilon$。这是一个比普通强保密约束更强的要求。由于消息的分布和信道状态独立，它等价于$I(M;Z^n,S^n)$。这意味着即便窃听者知道信道状态序列，强保密约束依然成立。首先引入如下引理。

引理1　文献[36]中引理17.3。对于一个定义在有限集合$\mathcal{U}$上的概率分布P和正数$\epsilon>0$，令$\mathcal{F}=\left\{u:P(u)\leqslant\frac{1}{d}\right\}$，如果$P(\mathcal{F})\geqslant 1-\eta$，那么一个随机映射$\kappa:\mathcal{U}\to\{1,\cdots,k\}$满足

$$\sum_{i=1}^{n}\left|P\left(\kappa^{-1}(i)\right)-\frac{1}{k}\right|\leqslant\epsilon+2\eta \tag{15}$$

该随机映射满足式(15)的概率为

$$1-2k\mathrm{e}^{-\frac{\epsilon^2(1-\eta)d}{2k(1+\epsilon)}} \tag{16}$$

特别的，如果P是$\mathcal{U}$上满足假设条件的概率分布集合$\mathcal{P}$中的一个元素，那么上述随机映射对集合中所有分布均满足(15)的概率为

$$1-2|\mathcal{P}|k\mathrm{e}^{-\frac{\epsilon^2(1-\eta)d}{2k(1+\epsilon)}} \tag{17}$$

注5　通过简单的代数运算可以得出$1-2|\mathcal{P}|k\mathrm{e}^{-\frac{\epsilon^2(1-\eta)d}{2k(1+\epsilon)}}>0$的一个充分条件为

$$\mathrm{lb}\,k < \frac{\epsilon^2(1-\epsilon)d\,\mathrm{lb}\,e}{2(1+\epsilon)\mathrm{lb}\,2|\mathcal{P}|} \tag{18}$$

事实上，通过引理1，本节所构造的编码方案可以用于更加复杂的通信系统，即主信道为组合信道，窃听信道为任意变化信道的通信模型。首先，固定信道状态分布q，输入分布$P_U P_{X|US}$并给定消息集的大小$\mathcal{M}=\left[1:2^{nR}\right]$。定义非负实数

$$\tilde{R} \leqslant I_q(U;Y), \tag{19}$$

$$\tilde{R}-R \geqslant \max_{q\in\mathcal{P}(\mathcal{S})} I_q(U;Z) \tag{20}$$

接下来，为信道状态分布q构造一套编码方案$\left(n,R,f_q,g_q\right)$，其中f_q为编码器，g_q为译码器。

码本构造：对每个消息$m\in\mathcal{M}$，生成一个大小为$2^{n\left(\tilde{R}-R\right)}$的子码本$\left\{u^n(m,l)\right\},l\in\left[1:2^{n\left(\tilde{R}-R\right)}\right]$。每个码字根据分布$P_U$独立同分布生成。

编码方案：为了发送消息m，编码器在子码本$\left\{u^n(m,l)\right\}$中随机选择一个码字$u^n(m,l)$。然后，编码器根据条件分布生成信道输入。

$$P^n_{X|US}\left(x^n|u^n(m,l),s^n\right)=\prod\nolimits_{i=1}^{n}P_{X|US\left(x_i|u_i,s_i\right)} \tag{21}$$

译码方案：合法接收者观测到信道输出Y^n。译码器从全体码本中寻找唯一一对$\left(\hat{m},\hat{l}\right)$使$U^n\left(\hat{m},\hat{l}\right)$满足$\left(U^n\left(\hat{m},\hat{l}\right),Y^n\right)\in\mathcal{T}^n_{P_{UY},\delta}$。如果不存在这样的$U^n$或者存在不止一个这样的$U^n$，译码器报告一个错误。译码器输出译码结果为$\hat{m}$。该方案的可靠性证明与普通带有因果状态信息的离散无记忆信道编码问题完全一致，参考文献[37]。当非负实数$\tilde{R}$满足式(22)时，译码错误概率趋近于0，即$\Pr\left\{M\neq\hat{M}\right\}\leqslant 2^{-nv},v>0$。

$$\tilde{R}\leqslant I_q(U;Y) \tag{22}$$

本节剩余内容主要证明当$\tilde{R}-R$进一步满足式(23)时，构造的编码方案对于任意的s^n都能使信息泄露随着码长$n\to\infty$趋近于0。

$$\tilde{R}-R\geqslant\max_{q\in\mathcal{P}(\mathcal{S})} I_q(U;Z) \tag{23}$$

证明所使用的主要工具为引理1。令U^n为被编码器选中的码字。根据大数定律以及本节的编码方案，总有

$$\Pr\left\{\left(U^n,Z^n,s^n\right)\in\mathcal{T}^n_{P_{USZ},\delta}\right\}\to 1 \tag{24}$$

接下来，定义$\mathcal{Z}^n$的两个子集分别为

$$\mathcal{B}_0\left(s^n\right)=\left\{z^n\in\mathcal{T}^{\mathrm{n}}_{P_{SZ},\delta}\left[s^n\right]:\Psi\left(z^n,s^n\right)\leqslant 2^{-\frac{nv}{2}}\right\} \tag{25}$$

$$\mathcal{B}_1\left(s^n\right)=\left\{z^n:\Pr\left\{Z^n=z^n|s^n\right\}<2^{-\frac{nv}{2}}\prod\nolimits_{i=1}^{n}P_{Z|S_i}\left(z_i|s_i\right)\right\} \tag{26}$$

其中，$\Psi\left(z^n,s^n\right)=\Pr\left\{X^n\notin\mathcal{T}^n_{P_{X|SZ},2\delta}\left[z^n,s^n\right]|z^n,s^n\right\}$。

根据式(24)，可得

$$\begin{aligned}1-2^{-nv}\leqslant&\sum_{z^n\in\mathcal{B}\left(s^n\right)}\Pr\left\{Z^n=z^n|s^n\right\}\Pr\left\{X^n\in\mathcal{T}^n_{P_{X|SZ},\delta}\left[z^n,s^n\right]|z^n,s^n\right\}+\\&\sum_{z^n\in\mathcal{T}^n_{P_{SZ},\delta}\left[s^n\right]\backslash\mathcal{B}_0\left(s^n\right)}\Pr\left\{Z^n=z^n|s^n\right\}\Pr\left\{X^n\in\mathcal{T}^n_{P_{X|SZ},\delta}\left[z^n,s^n\right]|z^n,s^n\right\}\leqslant\\&\Pr\left\{Z^n\in\mathcal{B}_0\left(s^n\right)|s^n\right\}+\left(1-\Pr\left\{Z^n\in\mathcal{B}_0\left(s^n\right)|s^n\right\}\right)\left(1-2^{-\frac{nv}{2}}\right)\end{aligned} \tag{27}$$

其中，最后一个不等式由$\mathcal{B}_0\left(s^n\right)$和$\Psi\left(z^n,s^n\right)$的定义得到，整理不等式可得

$$\Pr\left\{Z^n\in\mathcal{B}_0\left(s^n\right)|s^n\right\}>1-2^{-\frac{nv}{2}} \tag{28}$$

对于$\mathcal{B}_1\left(s^n\right)$，有

$$\begin{aligned}&\Pr\left\{Z^n\in\mathcal{B}_1\left(s^n\right)\right\}=\sum_{z^n\in\mathcal{B}_1\left(s^n\right)}\Pr\left\{Z^n|s^n\right\}<\\&\sum\nolimits_{z^n\in\mathcal{B}_1\left(s^n\right)}2^{-\frac{nv}{2}}\prod\nolimits_{i=1}^{n}P_{Z|S_i}\left(z_i|s_i\right)\leqslant 2^{-\frac{nv}{2}}\end{aligned} \tag{29}$$

定义$\mathcal{B}\left(s^n\right)=\mathcal{B}_0\left(s^n\right)\backslash\mathcal{B}_1\left(s^n\right)$，可以得到

$$\Pr\left\{Z^n\in\mathcal{B}\left(s^n\right)\right\}>1-2\cdot 2^{-\frac{nv}{2}} \tag{30}$$

接下来，设置引理1中的参数如下：$\epsilon=2^{-\frac{nv}{2}},d=2^{n\left(R-\frac{\tau}{2}\right)},k=2^{n(R-\tau)},\mathcal{P}=\left\{P^n_{U^n}\right\}\cup\left(P^n_{U^n|z^n s^n}:z^n\in\mathcal{B}\left(s^n\right),s^n\in\mathcal{S}^n\right)$。其中，$P^n_{U^n}$和$P^n_{U^n|z^n s^n}$都是码本上码字的分布。根据引理1，存在一个映射$h$满足

$$\sum_{m=1}^{k}\left|\Pr\left\{M_\kappa\left(U^n\right)=m\right\}-\frac{1}{k}\right|<3\epsilon \tag{31}$$

$$\sum_{m=1}^{k}\left|\Pr\left\{M_\kappa\left(U^n\right)=m|z^n,s^n\right\}-\frac{1}{k}\right|<3\epsilon \tag{32}$$

其中，$M_\kappa\left(X^n\right)=\kappa\left(X^n\right)$。此处的$M_\kappa$是一个分布在消息集上的随机变量，依赖于映射$\kappa$。从式(31)可以看出这个随机变量已经非常接近于均匀分布，但并非完全均匀分布。根据熵函数的连续性[1]，进一步有

$$\left|H\left(M_\kappa\left(U^n\right)|z^n,s^n\right)-H(M)\right|\leqslant -3\epsilon\,\mathrm{lb}\,\frac{3\epsilon}{k} \tag{33}$$

根据式(33)和式(30)可得

$$H\left(M_\kappa\left(U^n\right)|z^n,s^n\right)\geqslant(1-2\epsilon)\left(\mathrm{lb}\,k+3\epsilon\,\mathrm{lb}\,\frac{3\epsilon}{k}\right) \tag{34}$$

$$I\left(M_\kappa\left(U^n\right);Z^n|S^n\right)\leqslant 5\epsilon\,\mathrm{lb}\,k-3\epsilon\,\mathrm{lb}\,3\epsilon \tag{35}$$

本节至此已经构造出了一个几乎均匀的划分，得到的信息泄露$I\left(M_\kappa\left(U^n\right);Z^n|S^n\right)$已经满足强安全约束。但是，由于原始的消息是均匀分布，需要进一步微调所得到的划分方式来得到一个完全均匀的划分。为此引入引理2。

引理2　文献[38]中引理4。对于任意给定码本$\mathcal{C}$，如果映射$\kappa:\mathcal{C}\to[1:k]$满足

$$\sum_{m=1}^{k}\left|\Pr\left\{M_\kappa\left(U^n\right)=m\right\}-\frac{1}{k}\right|<3\epsilon \tag{36}$$

则存在一个映射κ'满足：1) $|\mathcal{C}_m|=\dfrac{2^{n\tilde{R}}}{k}$对所有$m$都成立，其中$\mathcal{C}_m=\{u^n\in\mathcal{C}:\kappa\left(u^n\right)=m\}$；2) $H\left(M_{\kappa'}(U^n)|M_\kappa\left(U^n\right)\right)<4\sqrt{\epsilon}\,\mathrm{lb}\,k$。

根据引理2，可以进一步构造映射κ'（即码本上的一种子码本划分的方式）使每个子码本的大小相同且$H\left(M|M_\kappa\right)\to 0$。进一步的可得

$$I\left(M;Z^n|S^n\right)\leqslant I\left(M,M_\kappa;Z^n|S^n\right)\leqslant I\left(M_\kappa;Z^n|S^n\right)+H\left(M|M_\kappa\right)\leqslant\epsilon' \tag{37}$$

其中，ϵ'随着ϵ趋近于0而趋近于0。

2　2组合信道上的强保密通信速率

2.1节中证明了对于信道状态分布固定为q时的强保密通信。需要注意的是$I\left(M;Z^n|S^n\right)\leqslant\epsilon$是比$I\left(M;Z^n\right)\leqslant\epsilon$更强的安全约束。接下来，本节将讨论如何在编码器带因果状态信息的组合窃听信道（CWC-CCSI）上进行强保密通信。为此，需要构造一个与信道状态分布q无关的编码方案。关键在于编码器需要通过观测到的信道状态信息来学习信道的状态分布，这需要发送端收集足够多的信道状态信息以根据大数定理来估计其统计特性。

为此，设计如下编码策略。首先，定义正整数n,n_0,n_1满足$n=n_0+n_1$。对于n_0长序列s^{n_0}的每一个型$\hat{q}$，编码器设计一套在2.1节中证明的强保密编码方案。由于n_0长序列S^{n_0}最多只有$\left(n_0+1\right)^{|\mathcal{S}|}$种型，其数量是关于码长多项式级大小。在通信开始后，编码器使用前n_0次信道来传输与译码器提前约定好的无意义空字符x_0。这n_0次传输的目的是让编码器观测到信道的前n_0个信道状态s^{n_0}。由于本文定义的组合信道在一次完整的码字传输过程中分布保持不变，只要n_0足够大，根据大数定理发送端可以通过s^{n_0}来估计本次传输中的信道状态分布。同时，为了保证这一学习的过程不会造成过大的码率损失，相比实际消息码字的长度n_1，n_0需要足够小（如$\sqrt{n_1}$）。在观测到前n_0个信道状态并计算其型$\hat{q}$后，编码器使用$\hat{q}$所对应的码$\left(f_{\hat{q}},g_{\hat{q}}\right)$。用$\mathcal{D}_m$表示消息$m$的译码集。根据2.1节中的证明，如果信道状态服从分布$\hat{q}$，则有

$$\frac{1}{|\mathcal{M}|}\sum_{m=1}^{|\mathcal{M}|}\sum_{s^n}P^n_{Y|XS}\left(\mathcal{D}_m^c|f_{\hat{q}}(m),s^n\right)\hat{q}^n\left(s^n\right)\leqslant\epsilon \tag{38}$$

$$I_{\hat{q}}\left(M;Z^n|S^n\right)\leqslant\epsilon \tag{39}$$

同时，根据大数定理，对于任意的$s\in\mathcal{S}$,总有$\left|\hat{q}(s)-q(s)\right|\leqslant\delta$，其中$\delta$随着$n$趋近于0而趋近于0。由于互信息是关于概率分布的连续函数，有

$$\frac{1}{|\mathcal{M}|}\sum_{m=1}^{|\mathcal{M}|}\sum_{s^n}P^n_{Y|XS}\left(\mathcal{D}_m^c|f_{\hat{q}}(m),s^n\right)q^n\left(s^n\right)\leqslant\epsilon' \tag{40}$$

$$I_q\left(M;Z^n|S^n\right)\leqslant\epsilon' \tag{41}$$

至此组合信道上的强保密通信证明完毕。

2.3　任意变化信道上的强保密通信

最后，本节将通过上述用于CWC强保密通信的编码方案来构造用于AVWC的随机编码方案，以证明AVWC-CCSI上的强保密通信。定义Π_n为对集合$\{1,2,\cdots,n\}$上置换的集合。对于任意的$\pi\in\Pi_n$，

$\pi s^n=(s_{\pi(1)},s_{\pi(2)},\cdots,s_{\pi(n)})$。为了完成证明，需要引入引理3。

引理 3[13] 如果 $h:\mathcal{S}^n\to[0,1]$ 满足存在一个 $\alpha\in(0,1)$，则式(42)对所有 $q^n=\prod_{i=1}^n q$ 都成立。

$$\sum_{s^n\in\mathcal{S}^n}h(s^n)q^n(s^n)>1-\alpha \tag{42}$$

同时，式(43)对所有 $s^n\in\mathcal{S}^n$ 都成立。

$$\frac{1}{n!}\sum_{\pi\in\Pi_n}h(\pi s^n)>1-\alpha_n \tag{43}$$

其中，$\alpha_n=\alpha(n+1)^{|\mathcal{S}|}$。

为了应用引理3，令 (n,R,f,g) 为2.2节中构造的用于组合信道的码。定义函数

$$h(s^n)=\frac{1}{|\mathcal{M}|}\sum_{m=1}^{|\mathcal{M}|}P^n_{Y|XS}(\mathcal{D}_m|f(m),s^n)-I(M;Z^n|s^n) \tag{44}$$

根据2.2节中的证明有

$$\sum_{s^n}h(s^n)q^n(s^n)\geqslant 1-2\alpha \tag{45}$$

对所有 $q\in\mathcal{Q}(\mathcal{S})$ 都成立，其中 α 是一个指数级小的数。由引理3可得

$$\frac{1}{n!}\sum_{\pi\in\Pi_n}\frac{1}{|\mathcal{M}|}\sum_{m=1}^{|\mathcal{M}|}\sum_{s^n}P^n_{Y|XS}(\mathcal{D}_m|f(m),\pi s^n)-I(M;Z^n|\pi s^n) \tag{46}$$

对所有的 $s^n\in\mathcal{S}^n$ 都成立。由于用于通信的信道是一个离散无记忆信道，则有

$$\frac{1}{n!}\sum_{\pi}h(\pi s^n)=\frac{1}{n!}\sum_{\pi\in\Pi_n}\frac{1}{|\mathcal{M}|}\sum_{m=1}^{|\mathcal{M}|}\sum_{s^n}P^n_{Y|XS}(\pi^{-1}\mathcal{D}_m|\pi^{-1}f(m),s^n)-I(M;\pi^{-1}Z^n|s^n)\geqslant 1-\alpha_n \tag{47}$$

其中，π^{-1} 表示 π 的逆映射。

此时，得到了一个根据 (n,R,f,g) 构造的用于任意变化信道的随机编码方案 $\left(n,R,f^{\pi^{-1}},g^{\pi^{-1}}\right)_{\pi\in\Pi_n}$，其中 $f^{\pi^{-1}}(m)=\pi^{-1}f(m)$，$g^{\pi^{-1}}(y^n)=g(\pi^{-1}y^n)$。该方案对应的公共随机变量 Γ 在 Π_n 上均匀分布。至此，随机编码容量下界的证明完毕。

接下来，通过去随机性来构造用于该信道的确定性编码。该随机编码方案需要引入巨大数量的公共随机性（即 $|\Pi_n|$，在每次通信前需要将具体实现的置换方案 π 告知编码器和译码器）。而如果将所需要的公共随机性数量减少到多项式级，则不需要额外的通信方式在编码器和译码器之间发送 π。此时，只需要编码器在本地做一次随机试验得到 π，然后通过额外的前缀码将随机试验的结果告知发送方。由于此时需要的公共随机性数量为多项式级，随着 $n\to\infty$ 所需的码率可以忽略不计。而证明只需多项式级的公共随机性需要用到ET。该技术在AVC和AVWC上的应用如文献[4,13,32]，由于空间有限，此处略去。需要额外注意的是由于此时没有公共随机性的存在，而编码器需要确保译码器能够准确译码前缀码的结果 π，该任意变化信道的主信道需要有大于0的确定性编码容量，否则任何编码方案都无法被准确译码。因此，确定性编码容量的下界只有在主信道不可对称化时才成立。证明完毕。

2.4 引理1参数验证

本节验证在2.1中引入的参数以证明确实存在满足引理1的映射 κ。

1) 验证 $P(\mathcal{F})\geqslant 1-\eta$。对于所有分布 $P_{U^n|z^ns^n}$，定义 $\mathcal{F}$ 为 $\mathcal{F}=\{u^n(m,l)\}\cap\mathcal{T}^n_{P_{X|ZS}}[z^n,s^n]$，其中 $z^n\in\mathcal{B}(s^n)$。可以得到

$$\begin{aligned}P_{U^n|z^ns^n}(u^n)&=\frac{P^n_{Z|US}(z^n|u^n,s^n)P_{U^n}(u^n)}{P^n_{Z|S}(z^n|s^n)}\leqslant\\&\frac{2^{-n(H_q(Z|U,S)-\delta)}}{2^{n\tilde{R}}2^{-\frac{nv}{2}}\prod_{i=1}^n P_{(Z|S)(z_i|s_i)}}\leqslant\\&\frac{2^{-n(H_q(Z|U,S)-\delta_1)}}{2^{n\tilde{R}}2^{-\frac{nv}{2}}2^{-n(H_q(Z|S)+\delta_2)}}=\\&2^{-n\left(\tilde{R}-I_q(U;Z|S)-\delta_1-\delta_2-\frac{v}{2}\right)}\leqslant\\&2^{-n\left(\tilde{R}-\max\limits_s I(U;Z|S=s)-\delta_1-\delta_2-\frac{v}{2}\right)}\leqslant\\&2^{-n\left(R-\frac{\tau}{2}\right)}=d^{-1}\end{aligned} \tag{48}$$

其中，第一个不等式是因为码本大小 $|\{u^n(m,l)\}|=2^{n\tilde{R}}$ 和 $\mathcal{B}(s^n)$ 的性质。同时，由于 $\mathcal{B}(s^n)$ 的性质，有 $P_{U^n|z^ns^n}(\mathcal{F})\geqslant 1-2^{-\frac{nv}{2}}$。对于分布 P_{U^n}，定义 $\mathcal{F}$ 为整个码本。由于码字被均匀选取，显然有

$$P_{U^n}(u^n)=2^{-n\tilde{R}}<d^{-1} \tag{49}$$

且$P_{U^n}(\mathcal{F})=1$。

2) 验证$k\text{lb}\,k<\dfrac{\epsilon^2(1-\epsilon)d\,\text{lb}\,e}{2(1+\epsilon)\text{lb}\,2|\mathcal{P}|}$。该条件确保了映射存在的概率大于0。

$$\frac{\epsilon^2(1-\epsilon)d\,\text{lb}\,e}{2(1+\epsilon)\text{lb}\,2|\mathcal{P}|}=\frac{1}{2(1+\epsilon)\text{lb}\,2|\mathcal{P}|}2^{n\left(R-v-\frac{\tau}{2}+\frac{\text{lb}((1-\epsilon)\text{lb}\,e)}{n}\right)}\geqslant 2^{n\left(R-v-\frac{\tau}{2}+\frac{\text{lb}((1-\epsilon)\text{lb}\,e)}{n}-\frac{\text{lb}(2(1+\epsilon)n\text{lb}\,2|\mathcal{S}||\mathcal{Z}|)}{n}\right)}\geqslant 2^{n\left(R-\frac{3}{4}\tau\right)}>k\,\text{lb}\,k \tag{50}$$

其中，第一个不等式是因为$|\mathcal{P}|\leqslant\left(|\mathcal{S}||\mathcal{Z}|\right)^n$。

2.5 上界证明

本节证明定理1中保密容量的上界。已知AVWC的容量永远小于等于信道集合相同的CWC，证明的思路为证明相同信道集合的CWC容量上界，再证明该上界可达。假设存在一个码满足组合信道上的译码错误概率和信息泄露的约束，则有

$$\Pr\left\{M\neq\hat{M}|s^n\right\}\leqslant\epsilon,I\left(M;\,Z^n|s^n\right)\leqslant\epsilon \tag{51}$$

对所有s^n都成立。令S^n为一个随机信道状态序列满足

$$\Pr\left\{S^n=s^n\right\}=\prod\nolimits_{i=1}^{n}q\left(s_i\right),q\in\mathcal{P}(\mathcal{S}) \tag{52}$$

可以得到

$$\begin{aligned}
nR=H(M)&\leqslant I\left(M;\,Y_q^n\right)-I\left(M;\,Z^n,S^n\right)+n\delta\overset{(a)}{=}\\
&\sum_{i=1}^{n}I\left(M,S_{i+1}^n,Z_{i+1}^n\,;\,Y^i\right)-I\left(M,S_i^n,Z_i^n\,;\,Y^{i-1}\right)-\\
&I\left(M;\,Z_i,S_i|Z_{i+1}^n,S_{i+1}^n\right)+n\delta=\\
&\sum_{i=1}^{n}I\left(M;\,Y_q^i|S_{i+1}^n,Z_{i+1}^n\right)+I\left(S_{i+1}^n,Z_{i+1}^n\,;\,Y_q^i\right)-\\
&I\left(M,S_i^n,Z_i^n\,;\,Y_q^{i-1}\right)-I\left(M;\,Z_i,S_i|Z_{i+1}^n,S_{i+1}^n\right)+n\delta=\\
&\sum_{i=1}^{n}I\left(M;\,Y_q^i|S_{i+1}^n,Z_{i+1}^n\right)+I\left(S_i^n,Z_i^n\,;\,Y_q^{i-1}\right)-\\
&I\left(M,S_i^n,Z_i^n\,;\,Y_q^{i-1}\right)-I\left(M;\,Z_i,S_i|Z_{i+1}^n,S_{i+1}^n\right)+n\delta=\\
&\sum_{i=1}^{n}I\left(M;\,Y_q^i|S_{i+1}^n,Z_{i+1}^n\right)-I\left(M;\,Y_q^{i-1}|S_i^n,Z_i^n\right)-\\
&I\left(M;\,Z_i,S_i|Z_{i+1}^n,S_{i+1}^n\right)+n\delta=\\
&\sum_{i=1}^{n}I\left(M;\,Y_q^i|S_{i+1}^n,Z_{i+1}^n\right)-\\
&I\left(M;\,Z_i,S_i,Y_q^{i-1}|Z_{i+1}^n,S_{i+1}^n\right)+n\delta=\\
&\sum_{i=1}^{n}I\left(M;\,Y_q^i,S_{i+1}^n,Z_{i+1}^n\right)-\\
&I\left(M;\,Z_i,S_i,Y_q^{i-1},Z_{i+1}^n,S_{i+1}^n\right)+n\delta=\\
&\sum_{i=1}^{n}I\left(M;\,Y_{q,i}|Y_q^{i-1},Z_{i+1}^n,S_{i+1}^n\right)-\\
&I\left(M;\,Z_i,S_i,Y_q^{i-1},Z_{i+1}^n,S_{i+1}^n\right)+n\delta\leqslant\\
&\sum_{i=1}^{n}I\left(M;\,Y_{q,i}|Y_q^{i-1},Z_{i+1}^n,S_{i+1}^n\right)-\\
&I\left(M;\,Z_i|Y_q^{i-1},Z_{i+1}^n,S_{i+1}^n,S_i\right)+n\delta\overset{(b)}{=}\\
&nI\left(M;\,Y_{q,T}|Y_q^{T-1},Z_{T+1}^n,S_{T+1}^n,T\right)-\\
&I\left(M,Z_T|Y_q^{T-1},Z_{T+1}^n,S_{T+1}^n,S_T,T\right)+n\delta\overset{(c)}{=}\\
&nI\left(U;\,Y_q|V\right)-I\left(U;\,Z|V,S\right)
\end{aligned}\tag{53}$$

其中，第一个不等式是因为费诺不等式和信息泄露约束，不等式(a)是因为文献[39]中的不等式(9)，不等式(b)中引入了均匀分布的时分变量T，在不等式(c)中定义随机变量$V=\left(Y_q^{T-1},Z_{T+1}^n,S_{T+1}^n,T\right),U=(V,M),Y_q=Y_{q,T},Z=Z_T$。最后，关于输入分布取最大值和关于信道状态分布$q$以及信道状态$s$取最小，上界证明完毕。

3 推论1证明

本节证明推论1，为此，需要继续使用2.5节中得到的外界表达式。

$$\begin{aligned}
nR&\leqslant\sum_{i=1}^{n}I\left(M;\,Y_{q,i}|Y_q^{i-1},Z_{i+1}^n,S_{i+1}^n\right)-\\
&I\left(M;\,Z_i|Y_q^{i-1},Z_{i+1}^n,S_{i+1}^n,S_i\right)+n\delta=\\
&\sum_{i=1}^{n}I\left(M,X_i;\,Y_{q,i}|Y_q^{i-1},Z_{i+1}^n,S_{i+1}^n\right)-\\
&I\left(M,X_i;\,Z_i|Y_q^{i-1},Z_{i+1}^n,S_{i+1}^n,S_i\right)+n\delta-\\
&\sum_{i=1}^{n}I\left(X_i;\,Y_{q,i}|Y_q^{i-1},Z_{i+1}^n,S_{i+1}^n,M\right)+\\
&I\left(X_i;\,Z_i|Y_q^{i-1},Z_{i+1}^n,S_{i+1}^n,S_i,M\right)\overset{(a)}{\leqslant}\\
&\sum_{i=1}^{n}I\left(X_i;\,Y_{q,i}|Y_q^{i-1},Z_{i+1}^n,S_{i+1}^n\right)-\\
&I\left(X_i;\,Z_i|Y_q^{i-1},Z_{i+1}^n,S_{i+1}^n,S_i\right)+n\delta=\\
&\sum_{i=1}^{n}I\left(X_i;\,Y_{q,i}\right)-I\left(X_i;\,Z_i|S_i\right)+n\delta-\\
&I\left(Y_q^{i-1},Z_{i+1}^n,S_{i+1}^n;\,Y_{q,i}\right)+I\left(Y_q^{i-1},Z_{i+1}^n,S_{i+1}^n;\,Z_i|S_i\right)\overset{(b)}{\leqslant}\\
&\sum_{i=1}^{n}I\left(X_i;\,Y_{q,i}\right)-I\left(X_i;\,Z_i|S_i\right)+n\delta=\\
&n\left(I\left(X;\,Y_q\right)-I\left(X;\,Z|S\right)\right)+n\delta
\end{aligned}\tag{54}$$

其中，不等式(a)和(b)是因为严格低噪。由于式(54)需要对组合信道中任意的分布都成立，则有

$$C \leqslant \max_{P_{X|S}} \min_{q} I\left(X; Y_q\right) - \max_{s} I\left(X; Z|S\right) \quad (55)$$

该上界显然可以通过令定理1下界中$U = X$达到，证毕。

4 结束语

本文讨论了AVWC-CCSI上的强保密通信问题。对于一般模型，本文给出了强保密约束下随机编码可达速率的上下界。证明使用了ET和RT，从组合信道入手，先构造用于组合信道的窃听编码。利用RT，通过置换码字中的符号顺序可以构造出一个用于AVWC-CCSI的随机编码方案，满足对于任意的信道状态序列，信息泄露都趋近于0，因此满足强保密约束。最后，利用ET，用于可靠且保密通信的公共随机性数量只需为一个关于码长n多项式级大小的数。通过构造一个码长趋近于0的前缀码，本文还证明了不可对称化的AVWC-CCSI的确定性编码速率。进一步，本文证明了当考虑的AVWC是严格低噪时，即主信道的信道在任意信道状态下都优于窃听信道，所给出的内界与外界重合为信道容量，证明了所提方案在这种情况下是最优方案。

当前，通信与感知一体化的研究进展迅速。本文主要定理虽然假设了完美的信道状态信息，但也同样适用于不完美信道状态信息的情况，因此可以看作是对感知结果的应用。本文的结论是对存在干扰的通信系统保密通信能力极限的刻画，对实际通信系统设计时的性能期望有指导作用。

目前，一般条件下AVWC的强保密容量问题依旧没有解决。本文工作拓展了AVWC强保密通信的研究，以及RT和ET在AVWC上的应用。未来可以考虑的研究方向还包括当CSI以非因果方式被编码器观测到时，AVWC上的保密（弱保密/强保密/语义安全）通信问题。

参考文献：

[1] Shannon C E, Weaver W. The mathematical theory of communication[M]. Urbana: University of Illinois Press, 1964.

[2] Shannon C E. Channels with side information at the transmitter[J]. IBM Journal of Research and Development, 1958, 2(4): 289-293.

[3] Blackwell D, Breiman L, Thomasian A J. The capacities of certain channel classes under random coding[J]. The Annals of Mathematical Statistics, 1960, 31(3): 558-567.

[4] Ahlswede R. Elimination of correlation in random codes for arbitrarily varying channels[J]. Zeitschrift für Wahrscheinlichkeitstheorie und Verwandte Gebiete, 1978, 44(2): 159-175.

[5] Csiszar I, Narayan P. The capacity of the arbitrarily varying channel revisited: positivity, constraints[J]. IEEE Transactions on Information Theory, 1988, 34(2): 181-193.

[6] Torres-Figueroa L, Mönich U J, Voichtleitner J, et al. Experimental evaluation of a modular coding scheme for physical layer security[C]// Proceedings of the 2021 IEEE Global Communications Conference (GLOBECOM). Piscataway: IEEE Press, 2021: 1-6.

[7] Wiese M, Boche H. Semantic security via seeded modular coding schemes and Ramanujan graphs[J]. IEEE Transactions on Information Theory, 2021, 67(1): 52-80.

[8] Frank A, Voichtleitner J, Wiese M, et al. Implementation of a modular coding scheme for secure communication[C]//Proceedings of the ICC 2022 - IEEE International Conference on Communications. Piscataway: IEEE Press, 2022: 2900-2905.

[9] Ezzine R, Wiese M, Deppe C, et al. Common randomness generation from finite compound sources[C]//Proceedings of the 2024 IEEE International Symposium on Information Theory (ISIT). Piscataway: IEEE Press, 2024: 2317-2322.

[10] Ezzine R, Wiese M, Deppe C, et al. Uniform common randomness generation over arbitrary point-to-point channels[J]. IEEE Transactions on Information Theory, 2025, 71(7): 5312-5329.

[11] Ahlswede R, Csiszar I. Common randomness in information theory and cryptography. I. Secret sharing[J]. IEEE Transactions on Information Theory, 1993, 39(4): 1121-1132.

[12] Ahlswede R, Csiszar I. Common randomness in information theory and cryptography. II. CR capacity[J]. IEEE Transactions on Information Theory, 1998, 44(1): 225-240.

[13] Ahlswede R. Arbitrarily varying channels with states sequence known to the sender[J]. IEEE Transactions on Information Theory, 1986, 32 (5): 621-629.

[14] Wyner A D. The wire-tap channel[J]. Bell System Technical Journal, 1975, 54(8): 1355-1387.

[15] Csiszar I, Korner J. Broadcast channels with confidential messages[J]. IEEE Transactions on Information Theory, 1978, 24(3): 339-348.

[16] Yassaee M H, Aref M R. Multiple access wiretap channels with strong secrecy[C]//Proceedings of the 2010 IEEE Information Theory Workshop. Piscataway: IEEE Press, 2010: 1-5.

[17] Liang Y B, Poor H V. Multiple-access channels with confidential messages[J]. IEEE Transactions on Information Theory, 2008, 54(3): 976-1002.

[18] Helal N, Bloch M, Nosratinia A. Cooperative resolvability and secrecy in the cribbing multiple-access channel[J]. IEEE Transactions on Information Theory, 2020, 66(9): 5429-5447.

[19] Liang Y B, Kramer G, Poor H V, et al. Compound wiretap channels[J]. EURASIP Journal on Wireless Communications and Networking, 2009, 2009: 142374.

[20] Bjelaković I, Boche H, Sommerfeld J. Secrecy results for compound wiretap channels[J]. Problems of Information Transmission, 2013, 49 (1): 73-98.

[21] Lai L F, Gamal H E. Cooperation for secure communication: the relay

wiretap channel[C]//Proceedings of the 2007 IEEE International Conference on Acoustics, Speech and Signal Processing - ICASSP'07. Piscataway: IEEE Press, 2007: III-149-III-152.

[22] Dai B, Ma Z. Multiple-access relay wiretap channel[J]. IEEE Transactions on Information Forensics and Security, 2015, 10(9): 1835-1849.

[23] Dai B, Li C, Liang Y B, et al. Impact of action-dependent state and channel feedback on Gaussian wiretap channels[J]. IEEE Transactions on Information Theory, 2020, 66(6): 3435-3455.

[24] Dai B, Luo Y. An improved feedback coding scheme for the wire-tap channel[J]. IEEE Transactions on Information Forensics and Security, 2019, 14(1): 262-271.

[25] Xia D F, Li K, Deng H, et al. Capacity-achieving coding schemes of Gaussian finite-state Markov wiretap channels with delayed feedback[J]. IEEE Transactions on Information Forensics and Security, 2025, 20: 7029-7044.

[26] Chen Y L, Vinck A J H. Wiretap channel with side information[J]. IEEE Transactions on Information Theory, 2008, 54(1): 395-402.

[27] Goldfeld Z, Cuff P, Permuter H H. Wiretap channels with random states non-causally available at the encoder[J]. IEEE Transactions on Information Theory, 2020, 66(3): 1497-1519.

[28] Chia Y K, Gamal A E. Wiretap channel with causal state information[J]. IEEE Transactions on Information Theory, 2012, 58(5): 2838-2849.

[29] Han T S, Sasaki M. Wiretap channels with causal state information: strong secrecy[J]. IEEE Transactions on Information Theory, 2019, 65 (10): 6750-6765.

[30] Chen Y Q, Oechtering T J, Skoglund M, et al. On strong secrecy for multiple access channels with states and causal CSI[J]. IEEE Transactions on Information Theory, 2025, 71(4): 3070-3099.

[31] MolavianJazi E, Bloch M, Laneman J N. Arbitrary jamming can preclude secure communication[C]//Proceedings of the 2009 47th Annual Allerton Conference on Communication, Control, and Computing (Allerton). Piscataway: IEEE Press, 2009: 1069-1075.

[32] Bjelaković I, Boche H, Sommerfeld J. Capacity results for arbitrarily varying wiretap channels[C]//Information Theory, Combinatorics, and Search Theory: In Memory of Rudolf Ahlswede. Berlin: Springer, 2013: 123-144.

[33] Goldfeld Z, Cuff P, Permuter H H. Arbitrarily varying wiretap channels with type constrained states[J]. IEEE Transactions on Information Theory, 2016, 62(12): 7216-7244.

[34] Chen Y Q, He D, Luo Y. Strong secrecy of arbitrarily varying multiple access channels[J]. IEEE Transactions on Information Forensics and Security, 2021, 16: 3662-3677.

[35] Chen Y Q, He D, Ying C H, et al. Strong secrecy of arbitrarily varying wiretap channel with constraints[J]. IEEE Transactions on Information Theory, 2022, 68(7): 4700-4722.

[36] Csiszár I, Körner J. Information theory[M]. Cambridge New York: Cambridge University Press, 2011.

[37] Gamal A E, Kim Y H. Network information theory[M]. Cambridge, UK: Cambridge University Press, 2011.

[38] He D, Guo W M. Strong secrecy capacity of a class of wiretap networks[J]. Entropy, 2016, 18(7): 238.

[39] Kramer G. Teaching IT: an identity for the Gelfand-Pinsker converse[J]. IEEE Information Theory Society Newsletter, 2021, 61(4): 4-6.

[作者简介]

陈一齐（1996– ），男，浙江杭州人，博士，慕尼黑工业大学在站博士后，主要研究方向为信息论、信息理论安全等。

董晨（1994– ），男，湖北宜昌人，上海交通大学博士生，主要研究方向为信息论、联邦学习等。

骆源（1971– ），男，上海人，博士，上海交通大学教授、博士生导师，主要研究方向为信息论、信息通信、区块链技术等。