doi:10.3969/j.issn.1000-436x.2013.10.003

基于分离信源信道码的相关信源在有噪广播信道下的可靠和安全传输

郎非[1]，王保云[1,2]，邓志祥[1]
（1. 南京邮电大学 通信与信息工程学院，江苏 南京 210003；2. 东南大学 移动通信国家重点实验室，江苏 南京 210096）

摘 要：从信息论的角度对相关信源在离散无记忆广播信道下可靠和安全传输的问题进行研究。2 个信源经过有噪信道分别到达各自指定的目的节点并被无损恢复，同时还要保证信源信息对于非指定的目的节点要有一定的保密性。采用信源信道分离的随机码策略，得到相关信源在一般广播信道下能够可靠和安全传输的充分条件。当 2 个信源的公共信息为二者的互信息时，可获得最佳压缩传输效率，并且能够做到信源信息传输的部分绝对保密。当广播信道采用退化信源集或满足 more capable 广播信道性质时，得到了可靠和安全传输的充分必要条件，此时分离信源信道码为最优码。

关键词：分离信源信道码；安全传输；广播信道；疑义度；香农理论
中图分类号：TN911.22/TN911.21 **文献标识码：**A **文章编号：**1000-436X(2013)10-0017-11

Secure lossless transmission of correlated sources over noisy broadcast channel using separate source-channel coding

LANG Fei[1], WANG Bao-yun[1,2], DENG Zhi-xiang[1]
(1. College of Communication and Information Engineeri g, Nanjing University of Posts and Telecommunications, Nanjing 210003, China;
2. National Mobile Communications Research Laboratory, Southeast University, Nanjing 210096, China)

Abstract: The problem of secure transmission of correlated sources over broadcast channel was studied from the perspective of information-theoretic security. Each source is only for its intended receiver, but to be kept secret from the unintended receiver. Sufficient condition was provided for secure transmission of correlated sources over broadcast channels from separate source-channel coding perspective. If the mutual information was chosen as common information, optimal compression and partial perfect secrecy were both achieved for two correlated sources. Sufficient and necessary conditions were provided for two special cases: a broadcast channel with degraded source sets and a more capable broadcast channel, and thus it could be seen that the separate source-channel code is optimal.

Key words: separate source-channel coding; secure communication; broadcast channel; equivocation; Shannon theory

1 引言

传统技术实现安全保密通信是通过对明文加密来实现的。收发双方会共享一个密钥，而窃听者是不知道密钥的。这种传统加密系统面临如下问题[1]：理论上无线网络中的窃听者可以拦截任何信息，包括密钥本身；具有主动攻击特性的窃听者能够干扰合法用户之间的信息传输，使得传输质量下降；复杂网络的密钥管理分配非常困难。1948 年，香农开创性地借助信息论(information theory)证明得到了一个惊人的结论：如果密钥的长度不小于明文的长度，则可实现绝对保密(perfect secrecy)。之后 Wyner、Csiszár 和 Körner 等人[2]在没有使用密钥的前提下，证明了在窃听信道或广播信道(BC)下安全通信是可能的。基于上述先驱们的工作，形成了信息理论安全(information-theoretic security)最基本的

收稿日期：2013-06-05；修回日期：2013-08-06
基金项目：国家自然科学基金资助项目(61271232, 60972045, 61071089)；东南大学移动通信国家重点实验室开放研究基金资助项目（2012D05）
Foundation Items: The National Natural Science Foundation of China (61271232, 60972045, 61071089); The Fund for National Mobile Communications Research Laboratory of Southeast University (2012D05)

理论。采用这种方法可以从本质上克服传统加密系统的上述缺陷，并且即使窃听者具有无限的计算资源，其安全容量也不会受到任何影响。近些年来，随着无线终端设备的普遍使用，开放的无线媒介易被非法用户侵入特质，使得无线通信安全问题被日益关注。2008 年之后，越来越多的信息理论学者开始重新关注信息理论安全这一研究方向[3~10]。

基于信息理论方法实现信息安全传输的基本思想：由于信道噪声以及衰落引起信道特性的波动，使得物理层信道产生固有的随机性，利用合法接收者与窃听者所接入信道的随机性不同来实现合法用户之间信息或部分信息的安全传输。例如，信息的发送者可以有意地在原有信息的基础上增加随机信息，在保证合法用户接收信息不受影响的同时，能够阻止窃听者截获有效信息。Csiszár 和 Körner[2]早期研究的广播信道只含 1 个公共消息和 1 个保密消息。近些年来，Liu 等人[9]率先对含有 2 个保密消息的广播信道进行研究，并给出了安全容量区域的内界和外界。紧接着，Xu 等人[10]对于这一模型进一步推广，给出了含有 2 个保密消息和 1 个公共消息的广播信道的速率——疑义度区域的内界和外界。

相关信源传输问题最早起源于无噪网络，有 2 个著名的分布式信源编码的例子。1)相关信源的分离编码，即著名的 Slepian-Wolf 编码[11]。这里的分离编码指相关信源经过压缩映射为 2 个消息集合，再分别经过两路无噪信道到达同一接收端。该编码方案得到一个令人惊讶的结果：当两路信道所能承载的码率不小于 2 个信源的联合熵时，则在接收端能够同时无损恢复 2 个信源。2)Gray-Wyner 系统[12]，该模型对 Slepian-Wolf 模型进行了推广，双信源经过 3 路无噪信道到达 2 个接收端。其中一路为公共信道，能同时到达 2 个接收端，其余两路为私人信道，分别到达 2 个不同的接收端。Gray 和 Wyner 最先给出该模型系统的可达速率区域，并证明了当公共信道能够被最大限度地使用时，可以得到最优码。近期针对 Gray-Wyner 系统，Timo 等人[13]给出当接收端有边信息时信源码率的内界和外界，Kamath 等人[14] 则对该系统的 Gács-Körner 公共信息对偶性质进行了研究；Tandon 等人[3]将这一问题扩展到 N 个接收用户，并考虑不同用户之间的信息保密。

相关信源在有噪广播信道下传输的问题由 Han 和 Coast[15]首先提出，Tuncel 在 2006 年将 Slepian-Wolf 码扩展到有噪广播信道，他们均使用“联合信源信道编码”得到可达界[16]。在这之后其他人[17~22]所提出的编码方案也都是基于联合编码，好像从一开始就没有考虑使用“分离信源信道编码”。这主要因为“香农信源信道分离定理”[23]揭示了对于多用户信道，信源与信道分开独立进行编码在很多情况下得不到最优解。而联合编码将传统的信源编码器与信道编码器整合为一个编码器，直接将信源映射为码字进行发送，不再有信源映射为消息、消息再映射为码字这样“分离”的 2 个过程。对于多址信道(MAC)，联合编码可以利用不同接入节点之间的信源相关性提高节点之间的协作通信能力。对于分离编码，由于消息和码字彼此是独立的，这反而浪费了信源相关性这一特质，使得编码效率降低。对于广播信道，只要不涉及节点之间的协作，似乎使用分离编码没有那么糟糕。但是作者仍然注意到联合编码在整合信源和信道的统计分布特性方面非常方便。

本文研究离散无记忆的 2 个相关信源在有噪广播信道下可靠和安全传输的问题，如图 1 所示，这一问题相当于对前面有关信道安全、分布式信源编码和信源信道编码等问题进行了扩展。本文仍然使用传统的分离信源信道编码策略，并结合叠加码[23]、double binning [9]和安全速率划分[10]等技术，使得传输的可靠性与安全性得到保证。对于可靠性来说，通过引入 Gray-Wyner 系统，明确相关信源中不同信息种类的概率关系，划分一类公共消息 M_0 和二类私人消息 M_1 和 M_2，如图 2 所示。通过优化三类信息的概率分布关系，使得信源编码与信道编码的 2 个过程在结合之后能够得到一个比较高效的编

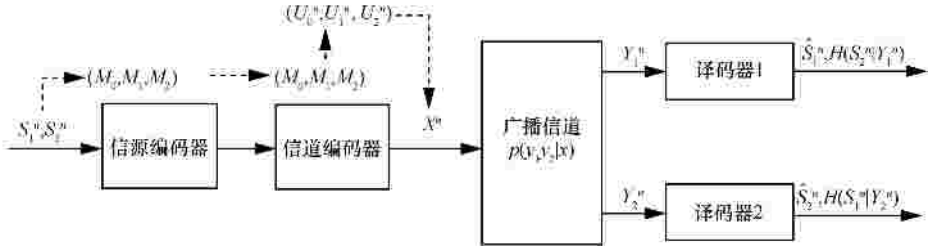

图 1 分离信源信道编码的广播信道模型

码。对于安全性来说，首先，通过引入辅助变量 V 调整信源输出的概率关系，使得消息 M_0、M_1 和 M_2 三者之间相互独立，这能够有效地防止不同消息之间的信息泄露；其次，分离编码本身能够做到消息和发送码字独立，这使得信道本身的安全容量不会受到信源相关性的影响而降低，这也是分离编码相比较联合编码的优势。

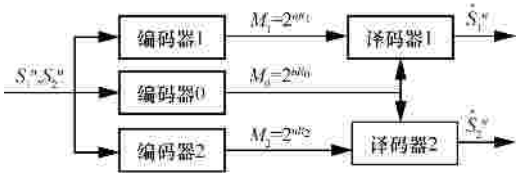

图 2　Gray-Wyner 信源编译码系统

基于上述思想，本文得到了如下结论：1)相关信源在一般广播信道(general BC)下可靠和安全传输的充分条件；2)当相关信源的公共信息为二者互信息时，可获得最佳的压缩传输效率，并在一定条件下传输可做到部分绝对保密；3)退化信源集(degraded source set)在一般广播信道下可靠和安全传输的充分必要条件；4)相关信源在 more capable 广播信道下可靠和安全传输的充分必要条件。以上 4 条结论及其部分证明在本文的第 3 节中进行表述，其中，结论 1)的充分性证明和结论 3)的必要性证明分别在附录 A 和附录 B 中进行表述。

2　基本定义和相关工作

本文符号标记规则：斜体大写字母表示随机变量，如 X；斜体小写字母表示随机变量的一个实例，如 x；X^n 和 x^n 表示分组长度为 n 的随机变量序列及其实例；$X_{1,i+1}^{j}$ 用于表示 $(X_{1i+1}, X_{1i+2}, \mathrm{L}, X_{1j})$，其中，第一个下标“1”标识变量的名称，如 X_1, X_2 等，i 和 j 指单个变量在变量序列中的序号；X_1^i 表示 $(X_{11}, X_{12}, \mathrm{L}, X_{1i})$，变量实例写法亦如此；随机变量 X 的取值集合称为字母集，用 X 表示。随机变量之间的 Markov 关系 $p(x)p(x|y)p(z|y)$ 的简化表示为 $X?\ Y?\ Z$，可以推出 $X?\ Y?\ Z$ 也成立，也可以用合并方式表达 $X-Y-Z$。本文使用 $e, e'>0$ 专门来表示一个小的固定值，且 $e'<e$。使用 $d(e)>0$ 表示 e 的函数，并当 $e\to 0$ 时，$d(e)\to 0$。$e_n \geq 0$ 为 n 的函数，当 $n\to\infty$，$e_n\to 0$。

2.1　问题定义

首先给出通信模型的基本定义，分为信源和信道两部分。

Gray-Wyner 系统如图 2 所示，由六元组 $(\mathsf{S}_1, \mathsf{S}_2, f_{GW}, \mathsf{M}_0, \mathsf{M}_1, \mathsf{M}_2)$ 来表示。$(\mathsf{S}_1, \mathsf{S}_2)$ 指信源字母集，$(\mathsf{M}_0, \mathsf{M}_1, \mathsf{M}_2)$ 是消息字母集。双信源经过三元编码器组 f_{GW} 映射输出 3 个消息。

$$(m_0, m_1, m_2) = f_{GW}(s_1^n, s_2^n)$$

离散无记忆的双信源序列 $(s_1^n, s_2^n) \in (\mathsf{S}_1^n, \mathsf{S}_2^n)$，每一对变量都独立同分布，概率分布满足

$$p(s_1^n, s_2^n) = \prod_{i=1}^{n} p(s_{1i}, s_{2i})$$

信源消息 $(m_0, m_1, m_2) \in (\mathsf{M}_0 \times \mathsf{M}_1 \times \mathsf{M}_2)$。

信源消息 (m_0, m_1, m_2) 经过信道编码器 g 映射输出信道消息。

$$(w_0, w_1, w_2) = g(m_0, m_1, m_2)$$

$(w_0, w_1, w_2) \in (\mathsf{W}_0, \mathsf{W}_1, \mathsf{W}_2)$。一般来说信道消息彼此要求独立，而对于信源消息没有这个要求。

广播信道由七元组 $(\mathsf{X}, p, \mathsf{Y}_1, \mathsf{Y}_2, f, y_1, y_2)$ 来表示，X 是信道输入字母集，Y_1 和 Y_2 是信道输出字母集，p 是广播信道的转移概率 $p(y_1,y_2|x)$，f 为信道编码映射函数，$?_1$ 和 $?_2$ 为 2 个译码映射函数。假设信道是离散无记忆的。

$$p(y_1^n, y_2^n \mid x^n) = \prod_{i=1}^{n} p(y_{1i}, y_{2i} \mid x_i)$$

$y_1^n \in \mathsf{Y}_1^n, y_2^n \in \mathsf{Y}_2^n, x^n \in \mathsf{X}^n$。令 W_0 为公共消息集，W_1 为接收者 1 的私人消息集，W_2 为接收者 2 的私人消息集。编码器 f 由转移概率 $p(x^n|w_0,w_1,w_2)$ 来定义，概率 p 增加了码字 x^n 的随机性，增加的随机信息独立于消息，其分布属性 2 个接收者都知道，只是不能确定哪一个 x^n 作为发送码字。2 个译码器定义为如下两组映射：

$$?_1:\ \mathsf{Y}_1^n \to (\mathsf{W}_0, \mathsf{W}_1) \to (\mathsf{M}_0, \mathsf{M}_1) \to \mathsf{S}_1^n$$

$$?_2:\ \mathsf{Y}_2^n \to (\mathsf{W}_0, \mathsf{W}_2) \to (\mathsf{M}_0, \mathsf{M}_2) \to \mathsf{S}_2^n$$

定义 1　当发送信源为 (s_1^n, s_2^n) 时，分组长度为 n 的序列的译码错误概率定义为

$$P_e^{(n)} = \sum_{(s_1^n, s_2^n) \in (\mathsf{S}_1^n, \mathsf{S}_2^n)} p(s_1^n, s_2^n) \cdot p((s_1^n, s_2^n) \neq (y_1(y_1^n), y_2(y_2^n))) \tag{1}$$

当 n 足够大且 $P_e^{(n)} \leq e$ 时，则认为 n 长序列实现了可靠传输。

定义 2　对于接收者 2，信源 S_1^n 的保密等级（安全性水平）用疑义度 E_{S_1} 来定义

$$E_{S_1} \leq \frac{1}{n} H(S_1^n \mid Y_2^n)，(\text{同理有 } E_{S_2} \leq \frac{1}{n} H(S_2^n \mid Y_1^n) \tag{2}$$

由定义 2 还可以引出如下新的定义。

1) 保密信息容量：$C_{S_1}=\max E_{S_1}$，$C_{S_2}=\max E_{S_2}$。

2) 绝对保密：$C_{S_1}=H(S_1)$，$C_{S_2}=H(S_2)$。

3) 部分绝对保密：$C_{S_1}=H(S_1\mid S_2)$，$C_{S_2}=H(S_2\mid S_1)$。

定义 3 信源(S_1, S_2)被允许经过广播信道传输需满足如下条件，当码字长度 n 足够大时，

$$P_e^{(n)}<e_n,\ E_{S_1}\le\frac{1}{n}H(S_1^n\mid Y_2^n),\ E_{S_2}\le\frac{1}{n}H(S_2^n\mid Y_1^n)$$

满足这样条件的信源集合被称为允许信源区域(admission source region)。这是满足一定可靠性水平 e 和安全性水平 E_{S_1} E_{S_2} 的信源对(S_1,S_2)可达区域，通常有一组不等式来进行限定。定义 3 对 Han 和 Costa 的定义[15]进行了扩展，增加对信源安全的限制。允许信源区域由不等式组来界定，它们可以理解为可靠和安全传输的限制条件。

定义 4 存在一个满足某一限定条件的信源信道码序列，使得相关信源能够可靠且安全地在广播信道中传输，则称该限定条件为充分条件，亦称允许信源区域内界；反之，任何满足可靠且安全传输的信源信道码序列都必须满足某一限定条件，称该限定条件为必要条件，亦称允许信源区域外界。当内界等于外界时，则称该条件为充分必要条件，亦称最优限制条件，此时不等式所界定的区域为最优允许信源区域，对应的码序列为最优码。

2.2 证明使用的相关引理

本节给出联合典型序列的概念和证明要使用到的相关引理，详细内容可参考文献[11,23,24]。

联合典型序列：令 $N(a,b\mid x^n,y^n)$ 标识(a,b) 在序列对$(x_1,y_1),(x_2,y_2),\cdots,(x_n,y_n)$中出现的次数。联合概率分布 $p(x,y)$的联合典型集可表示为

$$T_e^{(n)}(XY)=\left\{(x^n,y^n):\left|\frac{1}{n}N(a,b\mid x^n,y^n)-p(a,b)\right|\le e\cdot p(a,b)\right\}\quad(3)$$

其中，(x^n,y^n)为联合典型集 $T_e^{(n)}(XY)$ 中的联合典型序列，并能得到 $x^n\in T_e^{(n)}(X)$，$y^n\in T_e^{(n)}(Y)$。

引理 1 令$(X,Y)\sim p(x,y)$，假设 $x^n\in T_{e'}^{(n)}(X)$ 和 $Y^n\sim p(y^n\mid x^n)$，则有

$$\lim_{n\to\infty}\Pr\left\{(x^n,Y^n)\in T_e^{(n)}(XY)\right\}=1$$

引理2 假设 $X^n\sim p(x^n\mid u^n)$ 和$(u^n,y^n)\in T_{e'}^{(n)}(UY)$，$\%^n$ 和 $\wp^n$ 为任意 2 个随机序列，则有

$$\lim_{n\to\infty}\Pr\left\{(\%^n,\wp^n,\&^n)\in T_e^{(n)}(XYU)\right\}=0$$

当且仅当 $R<I(X;Y\mid U)-d(e)$。

引理 3 （费诺不等式） 离散无记忆信道的码书为C，且输入消息 W 服从集合 $\{1,2,\cdots,2^{nR}\}$上的均匀分布，则有 $H(W\mid\hat{W})\le 1+P_e^{(n)}nR$。$\hat{W}$ 是在信道接收端对 W 的估计，$P_e^{(n)}=\Pr(W\ne\hat{W})$。

引理 4 （数据处理不等式）若 $X-Y-Z$ 构成 Markov 链，则有 $I(X;Y)\ge I(X;Z)$ 或 $I(Z;Y)\ge I(X;Z)$。

3 主要贡献

3.1 节中给出本文的主定理，即定理 1，其是针对一般的信源与信道条件而得到的可靠和安全传输限制条件。后面 3 个小节（3.2 节、3.3 节、3.4 节）分别考虑几种特殊情况，其中，定理 2 是在考虑双信源的公共信息满足一定条件下得到的一个较优结果；定理 3 则考虑双信源是退化信源集时得到的一个最优结果；定理 4 是在考虑广播信道满足“more capable”条件下得到的一个最优结果。

3.1 相关信源可靠性和安全性传输的限制条件

定理 1 辅助变量$(V, U_0, U_1, U_2)\in\mathcal{V}\times\mathcal{U}_0\times\mathcal{U}_1\times\mathcal{U}_2$满足如下 Markov 链

$$S_1-V-S_2 \quad (4)$$

$$U_0-U_1U_2-X-Y_1Y_2 \quad (5)$$

信源(S_1,S_2)经过广播信道 $p(y_1,y_2|x)$，到达各自的接收端。系统满足可靠性和安全性传输的充分条件为

$$L_1=\bigcup_{S_1-V-S_2,\,U_0-U_1U_2-X-Y_1Y_2}\left\{\begin{array}{ll}I(S_1,S_2;V)<\min\{I(U_0,Y_1),I(U_0,Y_2)\} & (a)\\ H(S_1\mid V)+I(S_1,S_2;V)<I(U_1;Y_1\mid U_0)+\min\{I(U_0,Y_1),I(U_0,Y_2)\} & (b)\\ H(S_2\mid V)+I(S_1,S_2;V)<I(U_2;Y_2\mid U_0)+\min\{I(U_0,Y_1),I(U_0,Y_2)\} & (c)\\ H(S_1\mid V)+H(S_2\mid V)+I(S_1,S_2;V)<I(U_1;Y_1\mid U_0)+I(U_2;Y_2\mid U_0)- & \\ \quad I(U_1;U_2\mid U_0)+\min\{I(U_0,Y_1),I(U_0,Y_2)\} & (d)\\ E_{S_1}\le\min\{I(U_1;Y_1\mid U_0)-I(U_1;Y_2,U_2\mid U_0),\ H(S_1\mid V)\} & (e)\\ E_{S_2}\le\min\{I(U_2;Y_2\mid U_0)-I(U_2;Y_1,U_1\mid U_0),H(S_2\mid V)\} & (f)\end{array}\right\}\quad(6)$$

L_1 即为充分条件所界定的可达允许信源区域。其中，E_{S_1} 和 E_{S_2} 表示允许信源区域的疑义度（安全性）水平，以 E_{S_1} 为例，考虑以下 2 种情况：

1) 当 S_1 满足 $H(S_1|V) > I(U_1;Y_1|U_0) - I(U_1;Y_2, U_2|U_0)$ 时，则疑义度水平 E_{S_1} 恒等于信道安全容量 $C_S = I(U_1;Y_1|U_0) - I(U_1;Y_2,U_2|U_0)$ 这一固定值；

2) 当 S_1 满足 $H(S_1|S_2) \le I(U_1;Y_1|U_0) - I(U_1;Y_2|U_0)$ 时，则 E_{S_1} 等于 $H(S_1|V)$。

从编码设计的角度，期望允许信源区域尽可能大，即不等式(6a)~(6d)左半部信源压缩界越小越好；而右半部信道可达速率界越大越好。允许信源区域的计算结果，取值于所有符合 Markov 链式(4)和式(5)的联合概率分布。两条 Markov 链式(4)和式(5)彼此是独立的，即将信源与信道概率分布完全独立开来，这是由分离编码设计决定的。辅助变量 V 与 S_1,S_2 均相关，可看作是 S_1 和 S_2 的公共信息。U_0 代表信道传输的公共信息，而 U_1 和 U_2 代表信道传输的私密信息，有一定的保密性要求。

证明　见附录 A。

对于定理 1 考虑一种简化情况，即信道‘无噪”，并且在没有安全性约束的条件下定理 1 会退化为 Gray-Wyner 界[12]。

$$R_{G-W} = \bigcup_{p(v|s_1,s_2)} \begin{Bmatrix} R_0 \ge I(S_1,S_2;V) \\ R_1 \ge H(S_1|V) \\ R_2 \ge H(S_2|V) \end{Bmatrix} \tag{7}$$

式(7)中假设三路无噪信道（一路公共信道和二路私人信道）所能承载的码率分别为 R_0、R_1、R_2。

3.2　公共信息对信源压缩率和疑义度的影响

在 Gray-Wyner 系统中（如式(7)所示），代表公共信息的辅助变量 V 的概率分布特性不仅会影响双信源的压缩效率，而且会影响疑义度水平（如式(6e)、式(6f)所示）。根据定理 1 和 Gray-Wyner 界（式(7)）得到如下 3 个推论，其中，满足推论 1 可以得到双信源的最佳压缩率，而满足推论 2 和推论 3 条件的公共码率 R_0 可以得到次优的保密条件，基于此 3 个推论得到定理 2。

推论 1　Gray-Wyner 系统 $(R_0,R_1,R_2) \in \mathsf{R}_{G\text{-}W}$，当满足 $S_1 - V - S_2$ 时，则 $R_0 + R_1 + R_2 = H(S_1,S_2)$。

证明　显然联合熵 $H(S_1,S_2)$ 代表信源 S_1 和 S_2 的最佳压缩率。

由 Gray-Wyner 系统定义式(7)可得

$$\begin{aligned} R_0 + R_1 + R_2 &\ge I(S_1,S_2;V) + H(S_1|V) + H(S_2|V) \\ &= I(S_1;V) + I(S_2;V|S_1) + H(S_1|V) + H(S_2|V) \\ &= H(S_1) + I(S_2;V|S_1) + H(S_2|V) \end{aligned} \tag{8}$$

又因为 S_1- V- S_2，则有

$$\begin{aligned} &H(S_2|V) = H(S_2|S_1,V) \\ &I(S_2;V|S_1) + H(S_2|V) \\ &= H(S_2|S_1) - H(S_2|V,S_1) + H(S_2|V) = H(S_2|S_1) \end{aligned}$$

所以有

$$I(S_1,S_2;V) + H(S_1|V) + H(S_2|V) = H(S_2,S_1) \tag{9}$$

$$R_0 + R_1 + R_2 \ge H(S_1,S_2)$$

当不等式取等号时，即得推论 1。

推论 2　Gray-Wyner 系统 $(R_0,R_1,R_2) \in \mathsf{R}_{G\text{-}W}$，最大公共信息速率 R_0 满足 $2R_0+R_1+R_2=H(S_1)+H(S_2)$，则 $\max R_0 = I(S_1;S_2)$。

证明　由 Gray-Wyner 系统定义式(7)可得

$$\begin{aligned} &2R_0 + R_1 + R_2 \\ &\ge 2I(S_1,S_2;V) + H(S_1|V) + H(S_2|V) \\ &= I(S_1;V) + I(S_2;V|S_1) + I(S_2;V) + \\ &\quad I(S_1;V|S_2) + H(S_1|V) + H(S_2|V) \\ &= H(S_1) - H(S_1|V) + I(S_2;V|S_1) + \\ &\quad H(S_2) - H(S_2|V) + I(S_1;V|S_2) + \\ &\quad H(S_1|V) + H(S_2|V) \\ &= H(S_1) + I(S_2;V|S_1) + H(S_2) + I(S_1;V|S_2) \end{aligned} \tag{10}$$

令 $I(S_2;V|S_1)=0$ 和 $I(S_1;V|S_2)=0$，当且仅当 S_1、S_2、V 同时满足 Markov 链

$$S_2\text{-}\,S_1\text{-}\,V \text{ 和 } S_1\text{-}\,S_2\text{-}\,V$$

并由此会有如下不等式和等式。

$$2R_0+R_1+R_2 \ge H(S_1)+H(S_2)$$

$$\begin{aligned} &\max_{S_2-S_1-V,\,S_1-S_2-V} I(S_1,S_2;V) \\ &= \max_{S_1-S_2-V} I(S_1;V) = \max_{S_2-S_1-V} I(S_2;V) = I(S_1;S_2) \end{aligned} \tag{11}$$

以上过程均满足可逆性，即存在一反向结论：当 $(R_0,R_1,R_2) \in \mathsf{R}_{G\text{-}W}$ 且 $I(S_1;S_2)=R_0$ 时，有

$$S_2\text{-}\,S_1\text{-}\,V，\ S_1\text{-}\,S_2\text{-}\,V \tag{12}$$

进一步会得到

$$2R_0+R_1+R_2=H(S_1)+H(S_2)$$

推论 3　当定理 1 中的 S_1 和 S_2 的公共信息等于两者之间的互信息，并满足

$$I(U_1;Y_1|U_0) - I(U_1;Y_2,U_2|U_0) \ge H(S_1|V)$$
$$I(U_2;Y_2|U_0) - I(U_2;Y_1,U_1|U_0) \ge H(S_2|V)$$

则相关信源传输可达到部分绝对保密，即

$$C_{S_1} = H(S_1 \mid S_2)\text{，}\ C_{S_2} = H(S_2 \mid S_1)$$

证明　公共信息的大小会直接影响疑义度，显然由于公共信息可被任意接收用户所识别，而公共信息又与信源 S_1 和 S_2 相关，会引发信息泄露。所以从安全性的角度考虑，本文期望公共信息尽量地小，同时还要满足 Markov 约束条件 S_1- V- S_2。后者约束条件保证了接收用户在得到公共信息之后，不能够利用已知信源（如 S_1）信息再获取不同于公共信息的有关另一信源（如 S_2）的信息。从安全性的角度来看，推论 3 所设置的约束条件是在定理 1 的基础上，尽可能地减少了公共信息量，从而获得更高水平的安全性。

根据定理 1 和推论 2，得到 Markov 链

$$S_1\text{-}\,V\text{-}\,S_2\text{，}\ S_2\text{-}\,S_1\text{-}\,V\text{，}\ S_1\text{-}\,S_2\text{-}\,V$$

再根据数据处理不等式，由 S_1- V- S_2 得到

$$H(S_2 \mid V) \le H(S_2 \mid S_1)\text{，}\ H(S_1 \mid V) \le H(S_1 \mid S_2)$$

由 S_2- S_1- V 得到

$$H(S_2 \mid V) \ge H(S_2 \mid S_1)$$

由 S_1- S_2- V 得到

$$H(S_1 \mid V) \ge H(S_1 \mid S_2)$$

故有

$$H(S_2 \mid S_1) = H(S_2 \mid V)\text{，}\ H(S_1 \mid S_2) = H(S_1 \mid V) \tag{13}$$

定理 2　在定理 1 中，当 $I(S_1,S_2;V)=I(S_1;S_2)$ 时，则 L_1 退化为 L_2。

$$\mathsf{L}_2 = \bigcup_{\substack{S_1-V-S_2,\,S_2-S_1-V,\,S_1-S_2-V \\ U_0-U_1U_2-X-Y_1Y_2}} \left\{ \begin{array}{ll} I(S_1;S_2) < \min\{I(U_0;Y_1), I(U_0;Y_2)\} & \text{(a)} \\ H(S_1) < I(U_1;Y_1 \mid U_0) + \min\{I(U_0;Y_1), I(U_0;Y_2)\} & \text{(b)} \\ H(S_2) < I(U_2;Y_2 \mid U_0) + \min\{I(U_0;Y_1), I(U_0;Y_2)\} & \text{(c)} \\ H(S_1,S_2) < I(U_1;Y_1 \mid U_0) + I(U_2;Y_2 \mid U_0) - I(U_1;U_2 \mid U_0) + \min\{I(U_0;Y_1), I(U_0;Y_2)\} & \text{(d)} \\ E_{S_1} \le \min\{I(U_1;Y_1 \mid U_0) - I(U_1;Y_2,U_2 \mid U_0),\ H(S_1 \mid S_2)\} & \text{(e)} \\ E_{S_2} \le \min\{I(U_2;Y_2 \mid U_0) - I(U_2;Y_1,U_1 \mid U_0), H(S_2 \mid S_1)\} & \text{(f)} \end{array} \right\} \tag{14}$$

证明

根据推论 1~推论 3，有如下结论

$$\begin{aligned} & I(S_1,S_2;V) + H(S_1 \mid V) \\ &= I(S_1;V) + I(S_2;V \mid S_1) + H(S_1 \mid V) \\ &= I(S_1;V) + H(S_1 \mid V) \\ &= H(S_1) - H(S_1 \mid V) + H(S_1 \mid V) = H(S_1) \end{aligned} \tag{15}$$

同理可得

$$I(S_1,S_2;V) + H(S_2 \mid V) = H(S_2) \tag{16}$$

综合式(9)、式(13)、式(15)、式(16)，得到不等式组式(14)，定理 2 得证。

相比较定理 1，定理 2 得到允许信源区域 L_2 的信源压缩界（不等式(14a)~不等式(14d)的左半部）是最优的，并且满足推论 3 中相关信源传输可达到部分绝对保密的条件。

3.3　退化信源集

定理 3　信源 S_1 和 S_2 经广播信道发送给译码器 1，同时只将 S_1 发送给译码器 2，称该系统为具有退化信源集[17]的广播信道，满足可靠性和安全性传输的充分必要条件为

$$\mathsf{L}_3 = \bigcup_{U_0-U_1-X-Y_1Y_2} \left\{ \begin{array}{l} H(S_2) < \min\{I(U_0;Y_1), I(U_0;Y_2)\} \\ H(S_1,S_2) < I(U_1;Y_1 \mid U_0) + \\ \qquad \min\{I(U_0;Y_1), I(U_0;Y_2)\} \\ E_{S_1} \le \min\{I(U_1;Y_1 \mid U_0) - \\ \qquad I(U_1;Y_2 \mid U_0),\ H(S_1 \mid S_2)\} \end{array} \right\} \tag{17}$$

证明　见附录 B。

充分必要条件所确定的区域 L_3 为最优允许信源区域，此时分离信源信道编码为最优码。当满足 $I(U_1;Y_1|U_0)$- $I(U_1;Y_2|U_0) \ge H(S_1|S_2)$ 时，此时系统可以做到对 S_1 “部分绝对保密”。

当不考虑信源编码仅对信道来说，系统简化为具有一个公共消息 W_0 和一个秘密消息 W_1 的广播信道，W_0 和 W_1 的熵分别为 $nH(S_2)$ 和 $nH(S_2|S_1)$。L_3 退化为 Csiszár 和 Körner 的容量——疑义度界[2]。

$$\mathsf{R}_{C-K} = \bigcup_{U_0-U_1-X-Y_1Y_2} \left\{ \begin{array}{ll} R_0 \le \min\{I(U_0;Y_1), I(U_0;Y_2)\} & \text{(a)} \\ R_0 + R_1 < I(U_1;Y_1 \mid U_0) + & \\ \qquad \min\{I(U_0;Y_1), I(U_0;Y_2)\} & \text{(b)} \\ R_e \le I(U_1;Y_1 \mid U_0) - I(U_1;Y_2 \mid U_0) & \text{(c)} \end{array} \right\} \tag{18}$$

3.4 More capable 广播信道

定理 4 对于广播信道 $p(y_1,y_2|x)$，假设 Y_1 的能力大于 Y_2 的能力，即对于所有输入分布 $p(x)$，都有 $I(X;Y_1)\geq I(X;Y_2)$，则称该信道为 more capable 广播信道[23]，相关信源 S_1 和 S_2 在该信道上满足可靠性和安全性传输的充分必要条件：

$$\text{L}_4=\bigcup_{p(u,x)}\left\{\begin{array}{l}H(S_1,S_2)<I(X;Y_1)\\H(S_1,S_2)<I(X;Y_1|U)+I(U;Y_2)\\H(S_2)<I(U;Y_2)\\E_{S_1}<\min\{I(X;Y_1|U)-I(X;Y_2|U),\\\qquad H(S_1|S_2)\}\end{array}\right\} \tag{19}$$

证明

首先给出定理 3 的另外一种等价表达形式。

$$\text{L}'_3=\bigcup_{U_0-U_1-X-Y_1,Y_2}\left\{\begin{array}{ll}H(S_1,S_2)<I(U_1;Y_1) & \text{(a)}\\H(S_1,S_2)<I(U_1;Y_1|U_0)+I(U_0;Y_2) & \text{(b)}\\H(S_2)<I(U_0;Y_2) & \text{(c)}\\E_{S_1}\leq\min\{I(U_1;Y_1|U_0)- & \\\quad I(U_1;Y_2|U_0),\ H(S_1|S_2)\} & \text{(d)}\end{array}\right\} \tag{20}$$

注释 L'_3 仍是充分必要条件，并且在不考虑安全的情况下，用 (R_0,R_1) 替换不等式组(20a)~不等式组(20c)的左半部的压缩界，则 L'_3 退化为具有退化消息集或 more capable 广播信道的一个容量界[23]。这里由于篇幅限制，不再对 L'_3 进行证明。

充分性 将不等组(20)中 U 替换 U_0，X 替换 U_1，即得不等式组(19)。

必要性 只需证明不等组(20)中的信道外界（不等式右侧）都不大于不等式组(19)右侧的互信息表达式，则 L_4 也是一个外界。

当满足 L'_3 中 $U_0\to U_1\to X\to(Y_1;Y_2)$ 和定理 4 中 $I(X;Y_1)>I(X;Y_2)$ 的条件时，则有

$$I(U_1;Y_1)\leq I(X;Y_1) \tag{21}$$

$$I(U_1;Y_1|U_0)\leq I(X;Y_1|U_0)$$
$$I(X;Y_1|U_1=u_1,U_0=u_0)>I(X;Y_2|U_1=u_1,U_0=u_0)$$

进一步会有

$$I(U_1;Y_1|U_0)+I(U_0;Y_2)\leq I(X;Y_1|U_0)+I(U_0;Y_2) \tag{22}$$
$$I(X;Y_1|U_1,U_0)>I(X;Y_2|U_1,U_0)$$

进一步考虑疑义度限制条件

$$\begin{aligned}&I(U_1;Y_1|U_0)-I(U_1;Y_2|U_0)\\&=I(U_1X;Y_1|U_0)-I(X;Y_1|U_1,U_0)-\\&\quad I(U_1X;Y_2|U_0)+I(X;Y_2|U_1,U_0)\\&<I(U_1X;Y_1|U_0)-I(U_1X;Y_2|U_0)\\&=I(X;Y_1|U_0)-I(X;Y_2|U_0)\\&=I(X;Y_1|U)-I(X;Y_2|U)\end{aligned} \tag{23}$$

综合式(21)~式(23)，L_4 是 L'_3 的一个外界，证毕。

在衡量广播信道 $p(y_1,y_2|x)$ 的 Y_1 和 Y_2 的能力差异时，more capable 是比较弱的约束条件，对于较强的约束条件 less noisy 或退化关系时，L_4 也成立。

4 结束语

本文研究相关信源在广播信道下可靠安全传输的问题。基于分离信源信道码，得到了相关信源在一般广播信道下可靠和安全传输的可达允许信源区域的内界，并给出了达到信源信息部分绝对保密的条件。当满足退化信源集或 $I(X;Y_1)>I(X;Y_2)$ 时，分别得到了可靠和安全传输的最优限制条件，此时分离信源信道码为最优码，香农信源信道分离定理依然成立。未来下一步的任务可以结合如下工作：如采用联合信源信道编码[18]，这会突破传统的编码结构，虽然会带来在编码效率上的提升，但也会给安全传输带来挑战；Tandon 在文献[3]中讨论了在 Gray-Wyner 系统中不同种类的公共信息对疑义度的影响；Villard 在文献[4]中提出了带边信息的有损单信源在窃听信道中保密传输的问题。

附录 A　定理 1 证明

对充分性证明。对所用的信源信道编译策略码做简要描述，分为如下几个步骤。

1) 信源编码器：使用 Gray-Wyner 码将双信源序列 (S_1^n,S_2^n) 映射成信源消息组 (M_0,M_1,M_2)。通过码率分别为 R_0、R_1、R_2 的三路无噪线路分别将 M_0、M_1、M_2 发送到信道编码器。

2) 信道编码器：将 M_0、M_1、M_2 分别一一映射为信道消息 W_0、W_1、W_2。再基于 Xu 等人的保密编码策略[10]对消息进行信道编码，产生信道传输码字 x^n。

3) 接收端译码器 1：利用接收序列 Y_1^n，采用联合典型译码规则完成对消息 (W_0,W_1) 译码，并在此基础上最终完成对 S_1^n 译码。同时要给出使得译码错误概率接近为 0 的限制

条件集。最后计算条件熵 $H(S_2^n \mid Y_1^n)$，即译码器 1 在接收到序列 Y_1^n 之后对信源 S_2^n 的不确定度。译码器 2 工作亦如此。

上述编码策略可看作由 2 个环节组成：信源编译码与信道编译码。其中，信道编码策略与 Xu 相似，只是本文删除了如下限制条件[10]

$$\begin{cases} R_1 \geqslant I(U_1;Y_1 \mid U_0) - I(U_1;Y_2,U_2 \mid U_0) \\ R_2 \geqslant I(U_2;Y_2 \mid U_0) - I(U_2;Y_1,U_1 \mid U_0) \end{cases} \tag{24}$$

即本文不再要求消息速率 R_1 和 R_2 一定要大于信道的安全容量，这是因为在本文中信道消息速率还要受到信源编码的影响。在信道编码环节中，对变量的使用称谓基本延续 Xu 在文献[10]中的定义。

$W_0 \in \mathsf{W}_0 = \{1, \mathsf{L}, 2^{nR_0}\}$ 作为信道传输的公共消息，$W_1 \in \mathsf{W}_1 = \{1, \mathsf{L}, 2^{nR_1}\}$ 和 $W_2 \in \mathsf{W}_2 = \{1, \mathsf{L}, 2^{nR_2}\}$ 作为信道的私密消息分别发送给译码器 1 和译码器 2。进一步将 W_1 划分为 $W_{10} \in \mathsf{W}_{10} = \{1, \mathsf{L}, 2^{nR_{10}}\}$ 和 $W_{11} \in \mathsf{W}_{11} = \{1, \mathsf{L}, 2^{nR_{11}}\}$，$W_2$ 划分为 $W_{20} \in \mathsf{W}_{20} = \{1, \mathsf{L}, 2^{nR_{20}}\}$ 和 $W_{22} \in \mathsf{W}_{22} = \{1, \mathsf{L}, 2^{nR_{22}}\}$，其中，$R_1$=$R_{10}$+$R_{11}$，$R_2$=$R_{20}$+$R_{22}$，$W_{10}$ 和 W_{20} 指能够同时被译码器 1 和译码器 2 进行消息译码。这种速率划分的目的是考虑到当 $R_0 < \min\{I(U_0;Y_1), I(U_0;Y_2)\}$，公共消息的传输不能充分地利用公共信道，故将 W_{10} 和 W_{20} 也作为公共消息借助于该信道进行传输。说明：这里的公共信道或私人信道是一种逻辑上的表达，实际上都是同一物理信道；与 Xu 不同的是，本文还将讨论W_{10}和W_{20}为空集时的情况。

1) 随机码生成

① 信源码字：固定某一输入分布 $p(v \mid s_1, s_2)$。随机生成 2^{nR_0} 个码字 $v^n(m_0)$，$m_0 \in \{1, \mathsf{L}, 2^{nR_0}\}$，码字由独立同分布的 n 个字母 V 构成，V 服从分布 $p(v)$；均匀地将含有 S_1^n 序列集合等分割成 2^{nR_1} 个小舱（记为 bin），bin 的下标为 m_1，$m_1 \in \{1, \mathsf{L}, 2^{nR_1}\}$；相似地均匀地将 S_2^n 序列等分割成 2^{nR_2} 个 bin，bin 的下标为 m_2，$m_2 \in \{1, \mathsf{L}, 2^{nR_2}\}$。

$(R_0,R_1,R_2) \in \mathsf{R}_{G\text{-}W}$（见式(7)）且满足 Markov 链 $S_1 - V - S_2$，易知消息 M_0、M_1、M_2 互相独立。

② 信道码字：固定某一信道输入分布 $p(u_0)\,p(u_1 \mid u_0) \cdot p(u_2 \mid u_0)\;\; p(x \mid u_1, u_2)$。首先做如下定义：

$$\begin{cases} L_{11} = I(U_1;Y_1 \mid U_0) - I(U_1;Y_2,U_2 \mid U_0) \\ L_{12} = I(U_1;Y_2 \mid U_2,U_0) \\ L_{21} = I(U_2;Y_2 \mid U_0) - I(U_2;Y_1,U_1 \mid U_0) \\ L_{22} = I(U_2;Y_1 \mid U_1,U_0) \\ L_3 = I(U_1;U_2 \mid U_0) \end{cases} \tag{25}$$

随机生成 $2^{n(R_{10}+R_{20}+R_0)}$ 个码字 $u_0^n(w_{10}, w_{20}, w_0)$，码字由独立同分布的 n 个字母 U_0 构成，U_0 服从分布 $p(u_0)$。然后针对每一个 u_0^n 生成 $2^{n(L_{11}+L_{12}+L_3)}$ 个码字 $u_1^n(i,i',i'')$，$i \in \{1, \mathsf{L}, 2^{nL_{11}}\}$，$i' \in \{1, \mathsf{L}, 2^{nL_{12}}\}$，$i'' \in \{1, \mathsf{L}, 2^{nL_3}\}$，码字由独立同分布的 n 个字母 U_1 构成，U_1 服从分布 $p(u_1 \mid u_0)$；相似地生成 $2^{n(L_{21}+L_{22}+L_3)}$ 个码字 $u_2^n(j,j',j'')$，$j \in \{1, \mathsf{L}, 2^{nL_{21}}\}$，$j' \in \{1, \mathsf{L}, 2^{nL_{22}}\}$，$j'' \in \{1, \mathsf{L}, 2^{nL_3}\}$，码字由独立同分布的 n 个字母 U_2 生成，U_2 服从分布 $p(u_2 \mid u_0)$。对码字索引 (i,i',i'') 和 (j,j',j'') 可通过“binning”技术来解释。例如，可以随机地将 u_1^n 放置到 $2^{nL_{11}}$ 个 bin 中，每个 bin 由 i 进行标识，记作 bin(i)；进一步把 bin(i) 划分成 $2^{nL_{12}}$ 个 sub-bin，u_1^n 被随机划分到其中一个 sub-bin 中，记为 sub-bin(i')。i''则是 u_1^n sub-bin(i')中的随机序号。Liu 把这一编码技术称为“double-binning”[9]，如表 1 所示。

2) 编码

① 信源编码：给定双信源序列 $(s_1^n, s_2^n) \in T_e^n(S_1S_2)$。编码器 0 寻找一序列 $v^n(m_0)$ 满足

$$(v^n(m_0), s_1^n, s_2^n) \in T_e^{(n)}(VS_1S_2) \tag{26}$$

编码器 0 再将消息 m_0 发送给信道编码器。编码器 1 根据要发送的信源序列 s_1^n，选择其所在 bin，将 bin 的下标 m_1 发送给信道编码器。同理编码器 2 将 s_2^n 所在 bin 的下标 m_2 发送给信道编码器。

② 信道编码：定义 3 个一一映射函数 g_0, g_1, g_2，其逆映射为 $g_0^{-1}, g_1^{-1}, g_2^{-1}$。

$$W_0 = g_0(M_0) \in \{1, \mathsf{L}, 2^{nR_0}\},\;\; W_1 = g_2(M_1) \in \{1, \mathsf{L}, 2^{nR_1}\},$$

$$W_2 = g_2(M_2) \in \{1, \mathsf{L}, 2^{nR_2}\}$$

信道编码器根据信源编码器发送过来的消息 m_0、m_1、m_2，分别经过函数 g_0、g_1、g_2 映射，得到信道消息 w_0、w_1、w_2，再经过消息划分得到 w_0、w_{11}、w_{10}、w_{22}、w_{20}。由此，可以首先得到 $u_0^n(w_{10}, w_{20}, w_0)$，然后从 $2^{n(L_{11}+L_{12}+L_3)}$ 个码字

表 1 double-binning

sub-bin(1)			…	sub-bin(i')			…	sub-bin($2^{nL_{12}}$)			bin
$u_1^n(1,1,1)$	…	$u_1^n(1,1,2^{nL_3})$	…	$u_1^n(1,i',1)$	…	$u_1^n(1,i',2^{nL_3})$	…	$u_1^n(1,2^{nL_{12}},1)$	…	$u_1^n(1,2^{nL_{12}},2^{nL_3})$	bin(1)
$u_1^n(i,1,1)$	…	$u_1^n(i,1,2^{nL_3})$	…	$u_1^n(i,i',1)$	…	$u_1^n(i,i',2^{nL_3})$	…	$u_1^n(i,2^{nL_{12}},1)$	…	$u_1^n(i,2^{nL_{12}},2^{nL_3})$	bin(i)
	M		M		M		M		M		M
$u_1^n(2^{nL_{11}},1,1)$	…	$u_1^n(2^{nL_{11}},1,2^{nL_3})$	…	$u_1^n(2^{nL_{11}},i',1)$	…	$u_1^n(2^{nL_{11}},i',2^{nL_3})$	…	$u_1^n(2^{nL_{11}},2^{nL_{12}},1)$	…	$u_1^n(2^{nL_{11}},2^{nL_{12}},2^{nL_3})$	bin($2^{nL_{11}}$)

$u_1^n(i,i',i'')$ 中挑选一个码字用来传输 w_{11}。码字 $u_1^n(i,i',i'')$ 的确定分为 3 种情况，其中，后 2 种情况采用和 Xu[10]一样的方式。

a) $R_{11}< L_{11}$。$2^{nL_{11}}$ 个 bin 被均匀地划分为 $2^{nR_{11}}$ 个 cell，每个 w_1 对应一个 cell。cell(w_1)中有 bin 的数量为 $2^{n(L_{11}-R_{11})}$，随机挑选一个 bin (i)。再从 bin(i)的 $2^{n(L_{12}+L_3)}$ 个码字中随机地挑选一个 $u_1^n(i,i',i'')$。

b) $L_{11}\leq R_{11}\leq L_{11}+L_{12}$。每个 bin 含有消息 w_1 的个数为 $2^{n(R_{11}-L_{11})}$，把 $2^{nL_{12}}$ 个 sub-bin 放入到 $2^{n(R_{11}-L_{11})}$ 个 cell 中，从 cell(w_1)中随机挑选一个 sub-bin，再从此 sub-bin 中随机挑选一个 $u_1^n(i,i',i'')$。

c) $L_{11}+L_{12}<R_{11}\leq L_{11}+L_{12}+L_3$。每一个 sub-bin 含有 w_1 的个数为 $2^{n(R_{11}-L_{11}-L_{12})}$，把 2^{nL_3} 个 u_1^n 放入到 $2^{n(R_{11}-L_{11}-L_{12})}$ 个 cell 中，从 cell(w_1)中随机挑选一个 $u_1^n(i,i',i'')$ 作为码字。

相同的步骤可根据 w_{22} 来挑选码字 $u_2^n(j,j',j'')$。此外还要求所挑选的码字 $u_1^n(i,i',i'')$ 和 $u_2^n(j,j',j'')$ 满足联合典型

$$(u_1^n(i,i',i''),u_2^n(j,j',j''),u_0^n(w_{10},w_{20},w_0))\in T_e^{(n)}(U_1U_2U_0) \quad (27)$$

最后编码器 f 由分布 $p(x^n\mid u_1^n,u_2^n)p(u_1^n,u_2^n\mid w_0,w_1,w_2)$ 来输出信道码字 x^n。

3) 译码

随机码的译码方法采用联合典型序列译码方法，借助引理 1 和引理 2。

① 信道译码：译码器 1 根据从信道中接收到的序列 y_1^n，寻找一组消息 (w_{10},w_{20},w_0) 满足

$$(u_0^n(w_{10},w_{20},w_0),y_1^n)\in T_e^{(n)}(U_0Y_1) \quad (28)$$

进一步，根据 (w_{10},w_{20},w_0)，寻找一组消息 (i,i',i'') 满足

$$(u_0^n(w_{10},w_{20},w_0),u_1^n(i,i',i''),y_1^n)\in T_e^{(n)}(U_0U_1Y_1) \quad (29)$$

根据 (i,i',i'') 计算出 w_{11}。再由(w_{10},w_{11})得到消息 w_1。

② 信源译码：从信道译码中得到消息(w_0,w_1)，经过映射 (g_0^{-1},g_1^{-1}) 得到信源消息 (m_0,m_1)。从 bin(m_1)中挑选唯一 s_1^n 满足

$$(s_1^n,v^n(m_0))\in T_e^{(n)}(S_1V) \quad (30)$$

由此完成了译码器 1 对信源 S_1^n 的译码。同理，译码器 2 可对信源 s_2^n 实现译码。

4) 错误概率分析

除了信源编码和信源译码的错误概率计算，其他与 Xu 一致，略作说明。

根据式(26)，信源编码器会以错误概率接近于 0 的可能性找到一个消息 m_0，只要满足

$$R_0>I(S_1,S_2;V) \quad (31)$$

根据式(27)，信道编码器会以错误概率接近于 0 的可能性找到一对消息(i',i'')，只要满足

$$I(U_1;Y_1\mid U_0)-R_{11}+I(U_2;Y_2\mid U_0)-R_{22}\geq I(U_1;U_2\mid U_0) \quad (32)$$

根据式(28)，译码器 1 以错误概率接近于 0 的可能性找到唯一一组 (w_0,w_{10},w_{20})，只要满足

$$R_0+R_{10}+R_{20}\leq I(U_0;Y_2) \quad (33)$$

根据信道码字的定义式(25)可以得到

$$L_{11}+L_{12}+L_3<I(U_1;Y_1\mid U_0) \quad (34)$$

进一步根据式(29)、式(34)，译码器 1 以错误概率接近于 0 的可能性找到唯一一组 (i,i',i'')。由此

$$R_{11}<I(U_1;Y_1\mid U_0) \quad (35)$$

进一步可以有无差错译码 (i,i',i'')？w_{11}？(w_0,w_1)？(m_0,m_1)。

由信源编码可知，典型集势 $|T_e^n(S_1)|=2^{nH(S_1)}$，用来划分 S_1^n 的 bin 个数为 2^{nR_1}，故每一个 bin 中序列 s_1^n 的个数为 $2^{n(H(S_1)-R_1)}$。由 Gray-Wyner 系统的可达域 $R_{G\text{-}W}$(见不等式组(7))可知

$$R_1>H(S_1\mid V) \quad (36)$$

则有

$$2^{n(H(S_1)-R_1)}<2^{n(H(S_1)-H(S_1|V))}=2^{nI(S_1;V)}$$

由引理 2、式(30)和式(36)可知，译码器 1 会以错误概率接近于 0 的可能性找到唯一 s_1^n。

5) 疑义度计算

$$\begin{aligned}H(S_1^n\mid Y_2^n)&\overset{(a)}{=}H(S_1^n\mid M_1M_0Y_2^n)+I(S_1^n;M_1M_0\mid Y_2^n)\\&\overset{(b)}{=}0+I(S_1^n;M_1M_0\mid Y_2^n)\overset{(c)}{=}H(M_1M_0\mid Y_2^n)\\&\overset{(d)}{=}H(W_1W_0\mid Y_2^n)\overset{(e)}{=}H(W_1\mid Y_2^n)\end{aligned} \quad (37)$$

对式(37)中步骤(a)～步骤(e)做如下解释。

步骤(a)　将疑义度拆分为两项，前项是信源编码带来的疑义度，后项是信道传输带来的疑义度。

步骤(b)　根据编码规则二元消息组(M_1,M_0)完全可以确定 S_1^n。

步骤(c)　根据 Y_2^n 可译出 S_2^n，那么通过某一确定性映射函数可以将 (S_1^n,S_2^n) 映射为 (M_0,M_1)。

步骤(d)　由一一映射 $W_0=g_0(M_0)$，$W_1=g_2(M_1)$。

步骤(e)　公共信息 W_0 可被任意接收者所译码，因此对疑义度不产生影响。

情况 1　当 $H(S_1\mid V)>I(U_1;Y_1\mid U_0)-I(U_1;Y_2,U_2\mid U_0)$，即 $R_1>L_{11}$。

$$\begin{aligned}H(W_1\mid Y_2^n)&=H(W_{11},W_{10}\mid Y_2^n,U_0^n)=H(W_{11}\mid Y_2^n)\\&\overset{(a)}{=}n(I(U_1;Y_1\mid U_0)-I(U_1;Y_2,U_2\mid U_0))\end{aligned} \quad (38)$$

步骤(38a)直接使用了 Xu[10]的证明结果。由疑义度定义式(2)可得

$$E_{S_1}\leq I(U_1;Y_1\mid U_0)-I(U_1;Y_2,U_2\mid U_0) \quad (39)$$

情况 2　当 $H(S_1\mid V)\leq I(U_1;Y_1\mid U_0)-I(U_1;Y_2,U_2\mid U_0)$，

即 $R_1 \le L_{11}$。此时消息 w_1 在广播信道中传输可以保证绝对安全。也就是说，译码器 2 通过无线信道无法知道关于 w_1 的任何信息，但是这不等于 S_1^n 绝对安全，因为译码器 2 可以通过对序列 y_2^n 的译码得到公共消息 M_0，M_0 含有 S_1^n 的信息。另一方面，由 Markov 链 S_1- V- S_2 可以推出 M_1 和 M_0 是独立的，由此 M_1 是绝对安全，因此有

$$H(W_1 \mid Y_2^n) = H(W_1) = nH(S_1 \mid V)$$

$$E_{S_1} \le H(S_1 \mid V) \tag{40}$$

同理，在译码器 2 上的错误率分析和疑义度计算中，作者可以得到与译码器 1 对称的结果。

$$R_{22} < I(U_2; Y_2 \mid U_0) \tag{41}$$

$$E_{S_2} \le \min[I(U_2; Y_2 \mid U_0) - I(U_2; Y_1, U_1 \mid U_0), H(S_2 \mid V)] \tag{42}$$

综合式(31)~式(36)和式(38)~式(42)，得到L_1。

附录 B 定理 3 证明

充分性证明：要求在定理 1 的不等式组中 V=S_2，去掉 U_2 即得定理 3。

必要性证明：首先考虑有一个 $(2^{nH(S_2)}, 2^{nH(S_1|S_2)}, n)$ 码可使得 n 长分组序列的译码错误率为 $P_e^{(n)}$。在 $\mathrm{S}_1^n \times \mathrm{S}_2^n \times \mathrm{X}^n \times \mathrm{Y}_1^n \times \mathrm{Y}_2^n$ 上的概率分布为

$$p(s_1^n, s_2^n)\, p(x^n \mid s_1^n, s_2^n) \prod_{i=1}^{n} p(y_{1i}, y_{2i} \mid x_i) \tag{43}$$

根据费诺不等式(引理 3)，再由 $(2^{nH(S_2)}, 2^{nH(S_1|S_2)}, n)$ 码映射为消息的数目为 M_0 个数为 $2^{nH(S_2)}$，M_1 个数为 $2^{nH(S_1|S_2)}$，则有如下不等式

$$H(S_2^n \mid Y_1^n) = H(M_0 \mid Y_1^n) \le 1 + P_e^{(n)} nH(S_2) = ne_n \tag{44}$$

$$H(S_2^n \mid Y_2^n) = H(M_0 \mid Y_2^n) \le 1 + P_e^{(n)} nH(S_2) = ne_n \tag{45}$$

$$H(S_1^n \mid Y_1^n, S_2^n) = H(M_1 \mid Y_1^n, M_0) \le 1 + P_e^{(n)} nH(S_1 \mid S_2) = ne_n \tag{46}$$

定义辅助变量 $U_{0i} = (Y_1^{i-1}, Y_{2,i+1}^n, S_2^n)$，$U_{1i} = S_1^n$，且满足 Markov 链

$$U_{0i} \to U_{1i} \to X_i \to (Y_{1i}, Y_{2i})$$

1) 允许信源区域外界计算

$$\begin{aligned}
&nH(S_1, S_2) \\
&\overset{(a)}{=} H(S_1^n, S_2^n) \\
&= H(S_1^n \mid S_2^n) + H(S_2^n) \\
&= I(S_1^n; Y_1^n \mid S_2^n) + H(S_1^n \mid Y_1^n, S_2^n) + \\
&\quad \min\{I(S_2^n; Y_1^n) + H(S_2^n \mid Y_1^n),\ I(S_2^n; Y_2^n) + H(S_2^n \mid Y_2^n)\} \\
&\overset{(b)}{\le} I(S_1^n; Y_1^n \mid S_2^n) + \min\{I(S_2^n; Y_1^n),\ I(S_2^n; Y_2^n)\} + 2ne_n \\
&= \sum_{i=1}^{n} I(S_1^n; Y_{1i} \mid Y_1^{i-1}, S_2^n) + \\
&\quad \min\{\sum_{i=1}^{n} I(S_2^n; Y_{1i} \mid Y_1^{i-1}),\ \sum_{i=1}^{n} I(S_2^n; Y_{2i} \mid Y_{2,i+1}^n)\} + 2ne_n \\
&\le \sum_{i=1}^{n} I(S_1^n; Y_{1i} \mid Y_1^{i-1}, S_2^n) + \\
&\quad \min\{\sum_{i=1}^{n} I(S_2^n, Y_1^{i-1}, Y_{2,i+1}^n; Y_{1i}),\ \sum_{i=1}^{n} I(S_2^n, Y_1^{i-1}, Y_{2,i+1}^n; Y_{2i})\} + 2ne_n \\
&\le \sum_{i=1}^{n} I(S_1^n; Y_{1i} \mid Y_1^{i-1}, Y_{2,i+1}^n, S_2^n) + \\
&\quad \min\{\sum_{i=1}^{n} I(S_2^n, Y_1^{i-1}, Y_{2,i+1}^n; Y_{1i}),\ \sum_{i=1}^{n} I(S_2^n, Y_1^{i-1}, Y_{2,i+1}^n; Y_{2i})\} + 2ne_n \\
&= \sum_{i=1}^{n} I(U_{1i}; Y_{1i} \mid U_{0i}) + \min\{\sum_{i=1}^{n} I(U_{0i}; Y_{1i}),\ \sum_{i=1}^{n} I(U_{0i}; Y_{2i})\} + 2ne_n \\
&= nI(U_1; Y_1 \mid U_0) + \min\{nI(U_0; Y_1),\ nI(U_0; Y_2)\} + 2ne_n
\end{aligned} \tag{47}$$

步骤(47a)：$S_1^n = (S_{1,1}, S_{1,2}, \mathrm{L}, S_{1,n})$，当序列中每一个元素之间都相互独立时等号成立；

步骤(47b)：应用费诺不等式性质(见式(44)~式(46))。

2) 疑义度外界计算

$$\begin{aligned}
nE_{S_1} &\le H(S_1^n \mid Y_2^n) \\
&= H(S_1^n \mid S_2^n Y_2^n) + I(S_1^n; S_2^n \mid Y_2^n) \\
&\le H(S_1^n \mid S_2^n) + I(S_1^n; Y_2^n \mid S_2^n) + H(S_2^n \mid Y_2^n) \\
&\le I(S_1^n; Y_1^n \mid S_2^n) + I(S_1^n; Y_2^n \mid S_2^n) + H(S_1^n \mid Y_1^n S_2^n) + H(S_2^n \mid Y_2^n) \\
&= \sum_{i=1}^{n} \left[I(S_1^n; Y_{1i} \mid S_2^n Y_1^{i-1}) - I(S_1^n; Y_{2i} \mid S_2^n Y_{2,i+1}^n) \right] + 2ne_n \\
&= \sum_{i=1}^{n} \left[I(S_1^n, Y_{2,i+1}^n; Y_{1i} \mid S_2^n Y_1^{i-1}) - I(S_1^n, Y_1^{i-1}; Y_{2i} \mid S_2^n Y_{2,i+1}^n) \right] + 2ne_n \\
&= \sum_{i=1}^{n} \left[I(S_1^n; Y_{1i} \mid S_2^n Y_1^{i-1} Y_{2,i+1}^n) - I(S_1^n; Y_{2i} \mid S_2^n Y_{2,i+1}^n Y_1^{i-1}) \right] + 2ne_n \\
&= \sum_{i=1}^{n} \left[I(U_{1i}; Y_{1i} \mid U_{0i}) - I(U_{1i}; Y_{2i} \mid U_{0i}) \right] + 2ne_n
\end{aligned} \tag{48}$$

同时

$$\begin{aligned}
nE_{S_1} &\le H(S_1^n \mid Y_2^n) \\
&= H(S_1^n \mid Y_2^n, S_2^n) + I(S_1^n; S_2^n \mid Y_2^n) \\
&\le H(S_1^n \mid Y_2^n, S_2^n) + H(S_2^n \mid Y_2^n) \\
&\le H(S_1^n \mid S_2^n) + ne_n \\
&= \sum_{i=1}^{n} H(S_{1i} \mid S_{2i}) + ne_n
\end{aligned} \tag{49}$$

综合式(47)、式(48)和式(49)，即得L_3。定理 3 证毕。

参考文献：

[1] LIANG Y, POOR H V, SHAMAI S. Information theory security[J]. Foundations and Trends in Communication and Informatio Theory, 2009, 5(4-5): 2009.355-580.

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

[3] TANDON R, SANKAR L, POOR H V. Multi-user privacy: the Gray-Wyner system and generalized common information[A]. Proc IEEE International Symposium on Information Theory[C]. Saint- Petersburg, Russia, 2011. 563-567.

[4] VILLARD J, PIANTANIDA P, SHAMAI S. Secure lossy source-

channel wiretapping with side information at the receiving terminals[A]. IEEE International Symposium on Information Theory[C]. Saint-Petersburg, Russia, 2011. 1141-1145.

[5] WYREMBELSKI R F, BOCHE H. Strong secrecy in compound broadcast channels with confidential messages[A]. IEEE International Symposium on Information Theory[C]. Cambridge, MA, USA, 2012. 76-80.

[6] CZAP L, PRABHAKARAN V M, DIGGAVI S. Broadcasting private messages securely[A]. IEEE International Symposium on nformation Theory[C]. Cambridge, MA, USA, 2012. 428-432.

[7] LY H D, LIU T, LIANG Y. Multiple-input multiple-output Gaussian broadcast channels with common and confidential messages[J]. IEEE Transactions on Information Theory, 2010, 56(11):5477-5487.

[8] KHISTI A, LIU T. On private broadcasting over independent parallel channels[A]. IEEE International Symposium on Information Theory[C]. Cambridge, MA, USA, 2012. 433-437.

[9] LIU R, MARIC I, SPASOJEVIC P, *et al*. Discrete memoryless interference and broadcast channels with confidential messa : secrecy rate regions[J]. IEEE Transactions on Information Theory, 2008, 54(6):2493-2507.

[10] XU J, CAO Y, CHEN B. Capacity bounds for broadcast cha nels with confidential messages[J]. IEEE Transactions on Information Theory, 2009, 55(10):4529-4542.

[11] KRAMER G. Topic in multi-user information theory[J]. Foundations and Trends in Communication and Information Theory, 2008,4(4-5): 265-444.

[12] GRAY R, WYNER A. Source coding for a simple network[J]. Bell System Technical Journal, 1974, 53(9):1681-1721.

[13] TIMO R, GRANT A, CHAN T, *et al*. Source coding for a simple network with receiver side information[A]. Proc IEEE I ternational Symposium on Information Theory[C]. Toronto, Canada, 2008. 2307-2311.

[14] KAMATH S, ANANTHARAM V. A new dual to the Gács-Körner common information defined via the Gray-Wyner system[A]. Conference on Communication, Control, and Computing (Allerton)[C]. Monticello, USA, 2010.1340-1346.

[15] HAN T S, COSTA M H M. Broadcast channels with arbitrar ly correlated sources[J]. IEEE Transactions on Information Theory, 1987, 33(5):641-650.

[16] TUNCEL E. Slepian-Wolf coding over broadcast channels[J]. IEEE Transactions on Information Theory, 2006, 52(4):1469-1482.

[17] KANG W, KRAMER G. Broadcast channel with degraded source random variables and receiver side information[A]. Proc IEEE International Symposium on Information Theory[C]. Toronto, Canada, 2008. 1711-1715.

[18] MINERO P, KIM Y H. Correlated sources over broadcast c nels[A]. IEEE International Symposium on Information Theory[C]. Seoul, Korea, 2009. 2780-2784.

[19] MURIN Y, DABORA R, GUNDUZ D. Joint source-channel coding for the multiple-access relay channel[A]. IEEE International Symposium on Information Theory[C]. 2012. 1937-1941.

[20] YANG Z, ZHAO S, MA X, *et al*. A new joint source-channel coding scheme based on nested lattice codes[J]. IEEE Communications Letters, 2012, 16(5):730-733.

[21] GUNDUZ D, ERKIP E, GOLDSMITH A, *et al*. Reliable joint source-channel cooperative transmission over relay networks[J]. IEEE Transactions on Information Theory, 2013, 59(4):2442-2458.

[22] LIU N, GUNDUZ D, GOLDSMITH A J. Interference channels ith correlated receiver side information[J]. IEEE Transact ns on Information Theory, 2010, 56(12):5984-5999.

[23] GAMAL A E, KIM Y H. Network Information Theory[M]. Cambridge University Press, 2011.

[24] COVER T, THOMAS J. Elements of Information Theory[M]. New York: Wiley, 2006.

[25] GEL'FAND S I, PINSKER M S. Capacity of a broadcast channel with one deterministic component[J]. Problems of Information Transmission, 1980, 16(1):17-25.

作者简介：

郎非（1977-），男，吉林长春人，南京邮电大学博士生，主要研究方向为无线通信网络与香农信息理论。

王保云（1967-），男，河南信阳人，南京邮电大学教授、博士生导师，主要研究方向为香农信息论、无线通信中的博弈与协作、无线通信中的信号处理技术、视频信息的分析与理解等。

邓志祥（1980-），男，江苏南通人，南京邮电大学博士生，主要研究方向为无线通信网络与香农信息理论。