# 复合窃听信道的安全容量

贺转玲　郭大波　王晓凯
山西大学物理电子工程学院, 山西 太原 030006

**摘要**　在Wyner窃听信道和复合信道的基础上,考虑了合法传输信道集为经典信道,窃听信道集为量子信道这种信道模型的信息传输能力。目标是要设计编码译码方案,使得接收方能够完美译出发送的消息(译码错误概率趋于0),同时窃听者对发送消息的疑惑度尽可能的高。在此基础上推导了在发送者知道信道状态信息的情况下有量子窃听时的经典复合信道的安全容量;同时得出了在发送者不知道信道状态信息的情况下这种信道的安全容量的下界。

**关键词**　量子光学; 复合信道; 窃听信道; 量子信道; 安全容量
**中图分类号**　O436　　**文献标识码**　A
**doi:** 10.3788/LOP52.112701

# Security Capacity of Compound Wiretap Channel

He Zhuanling　Guo Dabo　Wang Xiaokai
*College of Physics and Electronic Engineering, Shan'xi University, Taiyuan, Shan'xi* 030006, *China*

**Abstract**　Based on Wyner tapping channel and the composite channel, the information transmission ability of a channel is considered in which legitimate transmission channel set is a classical channel and wiretap channel set is a quantum channel. The goal is to design coding and decoding scheme, so that the receiver can decode the message sent by the sender perfectly (decoding error probability close to zero), while the degree of confusion of eavesdropper to messages is as high as possible. On this basis, it is guaranteed that in the case of Alice′s knowing of information of channel condition, there is the security capacity of classic composite channel when quantum wiretaps; at the same time, the lower bound of security capacity of this channel is known in the case of Alice′s unknowing of information t of channel condition.

**Key words**　quantum optics; compound channel; wiretap channel; quantum channel; security capacity
**OCIS codes**　270.5585; 270.5565; 270.5568

## 1　引　　言

数据传输的高效性和安全性一直是通信中的两个最基本的研究课题[1-2]。高效性意味着对于给定的通信系统模型,要设计出尽可能达到信道容量的编码方案,同时该编码方案对应的译码错误概率要趋近于零;而安全性意味着如果存在窃听者,即使他知道所有的编码方案的细节,他也不能窃听到任何的信息。为了解决好高效性和安全性的关系,引出了安全容量这一概念,即在窃听者得不到任何信息的情况下,消息传输速率的最大值。在点对点信道中安全容量可以计算得出,但在多用户信道模型中由于多个消息对应的信息传输速率不同,所以信道容量也相应地被推广为空间区域。经典信道的容量问题可以根据香农第二定理解决。但是,在更深的层次上,世界可由量子力学所描述,为了理解客观物理规律所允许的人类通讯能力,通讯信道的量子行为[3]必须加以考虑,这就是量子信道容量问题[4]。

随着经典信息、编码、加密和计算复杂性研究的深入和新的精密实验技术的发展促进了人们对量子信息论的研究。从一开始的研究单用户信息论[5-7]推广到了多用户信息论[8-11],从单状态信道推广到了多状态信道。当研究的进一步深入,信道的安全容量也成为了人们的研究热点。2009年Liang等[9]在Alice不知道

**收稿日期**: 2015-04-16; **收到修改稿日期**: 2015-06-04; **网络出版日期**: 2015-09-24
**基金项目**:山西省基础研究项目(2014011007-2)、山西省回国留学人员科研资助项目(2014-012)、山西省国际科技合作项目(2014081027-1)
**作者简介**: 贺转玲(1989—),女,硕士研究生,主要从事量子密钥分发等方面的研究。E-mail: hezhuanling0612@126.com
**导师简介**: 郭大波(1963—),男,博士,副教授,主要从事量子密钥分发方面的研究。
E-mail: dabo_guo@sxu.edu.cn(通信联系人)

信道状态的情况下得出了复合窃听信道的安全容量下界，2011年Bjelakovic等[10]在Alice知道信道状态信息情况下得出了复合窃听信道的安全容量，2013年Bagherikaram等[12]得出了多输入多输出高斯广播信道的安全容量区域，2014年Rezki等[13]研究了合法传输信道为快速衰落信道的安全容量。

在本文中，在Bjelakovic等所研究的经典复合窃听信道的基础上，将经典窃听改为量子窃听，把经典信息论推广到了量子信息论，并分别计算了发送者知道信道状态信息时信道的安全容量和发送者不知道信道状态信息时的安全容量的下界。

## 2 符号及表示

定义一系列信道对 $\{(W_t,V_t):t=1,\cdots,T\}$，其中 $t$ 表示信道对 $(W_t,V_t)$ 的状态。当状态 $t$ 控制信道时，合法的接受者Bob探测信道对中第一部分 $W_t$ 的输出，窃听者Eve探测信道对中第二部分 $V_t$ 的输出。

令 $n\in N$，对于有限集 $A$ 和有限维复合希尔伯特空间 $H$，定义

$$A^n:=\{(a_1,\cdots,a_n):a_i\in A\forall i\in\{1,\cdots,n\}\},\tag{1}$$

$$H^{\otimes n}:=\{\rho_1\otimes\cdots\otimes\rho_n:\rho_i\in H\forall i\in\{1,\cdots,n\}\},\tag{2}$$

$A^n$ 和 $H^{\otimes n}$ 中的元素可写为 $a^n$ 和 $\rho^{\otimes n}$，对于集合 $A$ 中的概率分布 $P$ 和正常数 $\delta$，定义强典型序列集 $T^n_{P,\delta}$。

定义 $n$ 维随机离散无记忆信道的转移矩阵[14] $V^n$，即对于 $x^n=(x_1,\cdots,x_n)\in A^n$ 和 $y^n=(y_1,\cdots,y_n)\in B^n$，$V^n(y^n|x^n)=\prod_{i=1}^{n}V(y_i|x_i)$ 成立。

对于量子态 $\rho\in S(G)$，定义冯诺依曼熵 $S(\rho)=-\mathrm{tr}(\rho\log_2\rho)$。

对于量子态 $\rho,\sigma\in S(G)$，定义保真度 $F(\rho,\sigma):=\left\|\sqrt{\rho}\sqrt{\sigma}\right\|_1^2$。

空间 $G$ 上的等同算符用 $\mathrm{id}_G$ 表示。

令 $\Phi:=\{\rho_x:x\in A\}$ 是与 $A$ 中元素相应的量子态的集合。对于 $A$ 中的概率分布 $P$，Holevo $\chi$ 量表示为：

$$\chi(P;\Phi):=S\left[\sum_{x\in A}P(x)\rho_x\right]-\sum_{x\in A}P(x)S(\rho_x),\tag{3}$$

令 $n\in N$，$A$ 为有限集，$H$ 为有限维复合希尔伯特空间。对于 $\rho\in S(H)$，$\alpha>0$ 存在正交子空间投影算符 $\Pi_{\rho,\alpha}$ 作用于 $\rho^{\otimes n}$ 上且满足不等式[14]

$$\mathrm{tr}(\rho^{\otimes n}\Pi_{\rho,\alpha})\geqslant 1-\frac{d}{4n\alpha^2},\tag{4}$$

$$\mathrm{tr}(\Pi_{\rho,\alpha})\leqslant 2^{nS(\rho)+Kd\alpha\sqrt{n}},\tag{5}$$

$$\Pi_{\rho,\alpha}\cdot\rho^{\otimes n}\cdot\Pi_{\rho,\alpha}\leqslant 2^{-nS(\rho)+Kd\alpha\sqrt{n}}\Pi_{\rho,\alpha}.\tag{6}$$

式中 $d$ 表示 $H$ 的维数，$K$ 为正常数。

令 $v:A\to S(G)$ 为经典—量子信道。对于 $p\in p(A)$，$\alpha>0$，$x^n\in A^n$ 存在正交子空间投影算符 $\Pi_{v,\alpha}(x^n)$ 作用于 $v^{\otimes n}(x^n)$ 上满足[14]

$$\mathrm{tr}\left[v^{\otimes n}(x^n)\Pi_{v,\alpha}(x^n)\right]\geqslant 1-\frac{ad}{4n\alpha^2},\tag{7}$$

$$\mathrm{tr}\left[\Pi_{v,\alpha}(x^n)\right]\leqslant 2^{nS(v|P)+Kad\alpha\sqrt{n}},\tag{8}$$

$$\Pi_{v,\alpha}(x^n)\cdot v^{\otimes n}(x^n)\cdot\Pi_{v,\alpha}(x^n)\leqslant 2^{-nS(v|P)+Kad\alpha\sqrt{n}}\Pi_{v,\alpha}(x^n),\tag{9}$$

$$\mathrm{tr}\left[v^{\otimes n}(x^n)\cdot\Pi_{P_v,\alpha\sqrt{a}}\right]\geqslant 1-\frac{ad}{4n\alpha^2}.\tag{10}$$

式中 $a$ 表示集合 $A$ 中元素的个数，$K$ 为正常数，$S(v|P)=\sum_{x\in A}P(x)S[v(x)]$ 是当输入分布为 $P$ 时信道的条件熵，在(10)式中 $\Pi_{P_v,\alpha\sqrt{a}}$ 类似于在(4)式、(5)式、(6)式中的 $\Pi_{\rho,\alpha}$，$P_v$ 是当输入服从概率 $P$ 时信道 $v$ 输出的量子态。

令 $A$，$B$，$C$ 为有限集，$H$ 为希尔伯特空间，$\theta:=\{1,\cdots,T\}$ 为有限集，对于每个 $t\in\theta$ 定义：经典信道：$W_t:A\to P(B)$ $V_t:A\to P(C)$，经典—量子信道：$v_t:A\to S(H)$。

经典信道对的集合 $(W_t,V_t)_{t\in\theta}$ 称为(经典)复合窃听信道。当信道状态为 $t$ 时,发送者将序列 $x^n\in A^n$ 输入信道,接受者收到序列 $y^n\in B^n$ 的概率记为 $W_t^n(y^n|x^n)$,窃听者收到序列 $z_n\in Z_n$ 的概率记为 $V_t^n(z^n|x^n)$。

定义经典—量子信道对 $(W_t,v_t)_{t\in\theta}$ 为带有量子窃听的复合信道,当信道状态为 $t$ 时,发送者将序列 $x^n\in A^n$ 输入信道,接受者以概率 $W_t^n(y^n|x^n)$ 收到序列 $y^n\in B^n$,窃听者收到量子态 $v_t^{\otimes n}(x^n)\in S(H^{\otimes n})$。

复合窃听信道 $(W_t,V_t)_{t\in\theta}$ 的 $(n,J_n)$ 码由随机编码 $E:\{1,\cdots,J_n\}\to P(A^n)$ 和互不相交的译码集合 $\{D_j\subset B^n:j\in\{1,\cdots,J_n\}\}$ 组成,其中 $E$ 可表示为条件概率矩阵 $E(\cdot|\cdot)$。

如果发送者知道信道状态信息 $t$,可以采取如下策略:对于 $t\in\theta$,发送者和接收者构造 $(n,J_n)$ 码 $\left(E_t,\{D_j:j=1,\cdots,J_n\}\right)$ 使得所有在 $\left\{\left(E_t,\{D_j:j=1,\cdots,J_n\}\right):t\in\theta\right\}$ 中的码字有相同的译码集 $\{D_j:j=1,\cdots,J_n\}$。

如果对于任意的正数 $\varepsilon,\delta$,和足够大的 $n$,对每个 $t\in\theta$ 存在 $(n,J_n)$ 码 $\left(E_t,\{D_j:j=1,\cdots,J_n\}\right)$,当 $\frac{1}{n}\log_2 J_n\geqslant R-\delta$ 时有:

$$\max_{t\in\theta}\max_{j\in\{1,\cdots,J_n\}}\sum_{x^n\in A^n}E_t(x^n|j)W_t^n(D_j^c|x^n)\leqslant\varepsilon, \tag{11}$$

$$\max_{t\in\theta}I(X_{\text{uni}};K_t^n)\leqslant\varepsilon, \tag{12}$$

则非负数 $R$ 是在编码端知道信道状态信息情况下复合窃听信道 $(W_t,V_t)_{t\in\theta}$ 可达的传输速率。式中 $X_{uni}$ 表示在 $\{1,\cdots,J_n\}$ 上随机变量的均匀分布,$K_t^n$ 是窃听信道 $V_t^n$ 的输出。

如果对于任意的正数 $\varepsilon$,$\delta$ 和足够大的 $n$,存在 $(n,J_n)$ 码 $\left(E,\{D_j:j=1,\cdots,J_n\}\right)$,当 $\frac{1}{n}\log_2 J_n\geqslant R-\delta$ 时,有:

$$\max_{t\in\theta}\max_{j\in\{1,\cdots,J_n\}}\sum_{x^n\in A^n}E(x^n|j)W_t^n(D_j^c|x^n)\leqslant\varepsilon, \tag{13}$$

$$\max_{t\in\theta}I(X_{\text{uni}};K_t^n)\leqslant\varepsilon, \tag{14}$$

则非负数 $R$ 是在编码端不知道信道状态信息情况下复合窃听信道 $(W_t,V_t)_{t\in\theta}$ 可达的传输速率。

带有量子窃听的复合信道 $(W_t,v_t)_{t\in\theta}$ 的 $(n,J_n)$ 码由随机编码 $E:\{1,\cdots,J_n\}\to P(A^n)$ 和互不相交的译码集合 $\{D_j\subset B^n:j\in\{1,\cdots,J_n\}\}$ 组成。

如果对于任意的正数 $\varepsilon,\delta;t\in\theta$,和足够大的 $n$,存在 $(n,J_n)$ 码 $\left(E_t,\{D_j:j=1,\cdots,J_n\}\right)$,当 $\frac{1}{n}\log_2 J_n\geqslant R-\delta$ 时,有:

$$\max_{t\in\theta}\max_{j\in\{1,\cdots,J_n\}}\sum_{x^n\in A^n}E_t(x^n|j)W_t^n(D_j^c|x^n)\leqslant\varepsilon, \tag{15}$$

$$\max_{t\in\theta}\chi(X_{\text{uni}};Z_t^{\otimes n})\leqslant\varepsilon, \tag{16}$$

则非负数 $R$ 是在编码端知道信道状态信息情况下带有量子窃听的复合信道 $(W_t,v_t)_{t\in\theta}$ 可达的传输速率,式中 $Z_t^n$ 是窃听信道 $v_t^n$ 的输出。

如果对于任意的正数 $\varepsilon,\delta$,和足够大的 $n$,存在 $(n,J_n)$ 码 $\left(E,\{D_j:j=1,\cdots,J_n\}\right)$,当 $\frac{1}{n}\log_2 J_n\geqslant R-\delta$ 时,有:

$$\max_{t\in\theta}\max_{j\in\{1,\cdots,J_n\}}\sum_{x^n\in A^n}E(x^n|j)W_t^n(D_j^c|x^n)\leqslant\varepsilon, \tag{17}$$

$$\max_{t\in\theta}\chi(X_{\text{uni}};Z_t^{\otimes n})\leqslant\varepsilon, \tag{18}$$

则非负数 $R$ 是在编码端不知道信道状态信息情况下带有量子窃听的复合信道 $(W_t,v_t)_{t\in\theta}$ 可达的传输速率,其中 $Z_t^n$ 是窃听信道 $v_t^n$ 的输出。

## 3 经典复合窃听信道

$A$,$B$,$C$,$\theta$ 在第二部分中定义,对于每个 $t\in\theta$,规定 $A^n$ 上的概率分布 $p_t$,令

$$\begin{cases} p_t'(x^n):=\begin{cases}\dfrac{p_t^n(x^n)}{p_t^n(T^n_{p_t,\delta})}, x^n\in T^n_{p_t,\delta}\\ 0, x^n\notin T^n_{p_t,\delta}\end{cases}\\ X^{(t)}:=\left\{X^{(t)}_{j,l}\right\}_{j\in\{1,\cdots,J_n\},l\in\{1,\cdots,L_{n,t}\}}\end{cases}, \tag{19}$$

是当输入服从 $p_t'$ 的独立同分布时的随机矩阵的集合。$L_{n,t}$ 是自然数，下面将确定。

对任意的正数 $\omega$，如果 $J_n=\left\lfloor 2^{n\left(\min_{t\in\theta}\left[I(p_t;W_t)-\frac{1}{n}\log_2 L_{n,t}-\mu\right]\right)}\right\rfloor$，式中 $\mu$ 是与 $j$，$t$ 无关的正常数，且当 $\omega$ 趋于0时 $\mu$ 可以任意小[10]。

对于 $t\in\theta$，$L_{n,t}\in N$ 存在 $\{D_j:j=1,\cdots,J_n\}$ 使得

$$P\left[\max_{j\in\{1,\cdots,J_n\}}\sum_{l=1}^{L_{n,t}}\frac{1}{L_{n,t}}W_t^n\left(D_j^c|X^{(t)}_{j,l}\right)>\sqrt{T}\,2^{-n\omega/2}\right]\leqslant\sqrt{T}\,2^{-n\omega/2}, \tag{20}$$

成立。该式分析了传输信道 $W_t$ 的错误概率，而没考虑窃听信道。

考虑(20)式，通过选择 $L_{n,t}=\left\lfloor 2^{n\left[I(p_t;V_t)+\tau\right]}\right\rfloor$，对于任意的正常数 $\tau$，在信道状态信息已知的情况下复合窃听信道的安全容量为：

$$C_{S,\mathrm{CSI}}=\min_{t\in\theta}\max_{u\to A\to(BK)_t}\left[I(u;B_t)-I(u;K_t)\right], \tag{21}$$

$B_t$ 是 Bob 端输出的随机变量，$K_t$ 是 Eve 端输出的随机变量，此处当随机变量满足 Markov 链关系 $u\to A\to(BK)_t$ 时，取得最大值[10]。

类似地，在信道状态未知的情况下，规定 $A^n$ 上的概率分布 $p$，令

$$\begin{cases} p'(x^n):=\begin{cases}\dfrac{p^n(x^n)}{p^n(T^n_{p,\delta})}, x^n\in T^n_{p,\delta}\\ 0, x^n\notin T^n_{p,\delta}\end{cases}\\ X^n:=\left\{X_{j,l}\right\}_{j\in\{1,\cdots,J_n\},l\in\{1,\cdots,L_n\}}\end{cases}, \tag{22}$$

是当输入服从 $p'$ 的独立同分布时的随机矩阵的集合，$L_n$ 为自然数随后将确定。对于任意的 $\omega>0$，如果 $J_n=\left\lfloor 2^{n\left(\min_{t\in\theta}\left[I(p;W_t)-\frac{1}{n}\log_2 L_n-\mu\right]\right)}\right\rfloor$，式中 $\mu$ 是与 $j,t$ 无关的正常数，且当 $\omega$ 趋于0时 $\mu$ 可任意小。

对于 $t\in\theta$，$L_n\in N$ 存在 $\{D_j:j=1,\cdots,J_n\}$ 使得：

$$P\left[\max_{j\in\{1,\cdots,J_n\}}\sum_{l=1}^{L_n}\frac{1}{L_n}W_t^n\left(D_j^c|X_{j,l}\right)>\sqrt{T}\,2^{-n\omega/2}\right]\leqslant\sqrt{T}\,2^{-n\omega/2}, \tag{23}$$

成立。考虑(23)式，选择 $L_n=\left\lfloor 2^{n\left[\max_t I(p_t;V_t)\right]+\frac{\tau}{4}}\right\rfloor$，$\tau$ 是正常数，在信道状态信息未知的情况下复合窃听信道的安全容量的下界为[10]：

$$C_S\geqslant\max_{u\to A\to(BK)_t}\left[\min_{t\in\theta}I(u;B_t)-\max_{t\in\theta}I(u;K_t)\right]. \tag{24}$$

## 4 带有量子窃听的复合信道

对于以上部分定义的 $A$，$B$，$H$，$\theta$ 和 $(W_t,v_t)_{t\in\theta}$ 可得如下定理：当Alice知道信道状态的情况下带有量子窃听的复合信道 $(W_t,v_t)_{t\in\theta}$ 的安全容量为(sup: 上确界)：

$$C_{S,\mathrm{CSI}}=\min_{t\in\theta}\max_{u\to A\to(BZ)_t}\left[I(u;B_t)-\mathrm{limsup}_{n\to\infty}\frac{1}{n}\chi\left(u;Z_t^{\otimes n}\right)\right], \tag{25}$$

当Alice不知道信道状态信息情况下带有量子窃听的复合信道 $(W_t,v_t)_{t\in\theta}$ 的安全容量下界为

$$C_S \geqslant \max_{u\to A\to (BZ)_t}\left[\min_{t\in\theta} I(u;B_t) - \max_{t\in\theta}\chi(u;Z_t)\right], \tag{26}$$

$B_t$ 为Bob端输出的随机变量，$Z_t$ 为Eve端输出的随机量子态。

证明：

1) Alice知道信道状态信息 $t$ 时的下界：

对于每个 $t\in\theta$，在 $A^n$ 上设定概率分布 $p_t$，令 $J_n=\left\lfloor 2^{n\left(\min_{t\in\theta}\left[I(p_t;W_t)-\frac{1}{n}\log_2 L_{n,t}-\mu\right]\right)}\right\rfloor$，$L_{n,t}$ 是自然数，$\mu$ 的确定方法同上。令 $p_t^{'}$，$X^{(t)}$，$D_j$ 与经典情形相同，由于Alice通过经典信道传送信息给Bob，所以(20)式仍成立。

令

$$Q_t(x^n) := \Pi_{p_t v_t,\alpha\sqrt{a}}\Pi_{v_t,\alpha}(x^n)\cdot v_t^{\otimes n}(x^n)\cdot\Pi_{v_t,\alpha}(x^n)\Pi_{p_t v_t,\alpha\sqrt{a}}, \tag{27}$$

$\alpha$ 之后将被确定。

由于 $\Pi_{p_t v_t,\alpha\sqrt{a}}$ 和 $\Pi_{v_t,\alpha}(x^n)$ 均为投影矩阵，结合(4)式，(10)式和引理[15-16]可得：对于任意的 $t$ 和 $x^n$ 有：

$$\left\|Q_t(x^n)-v_t^{\otimes n}(x^n)\right\| \leqslant \sqrt{\frac{2(ad+d)}{n\alpha^2}}, \tag{28}$$

设定 $\theta_t := \sum_{x^n\in T^n_{p_t,\delta}} p_t'^n(x^n)Q_t(x^n)$，对于给定的 $z^n$ 和 $t$，$\left\langle z^n\middle|\theta_t\middle|z^n\right\rangle$ 是在条件 $x^n\in T^n_{p_t,\delta}$ 下 $\left\langle z^n\middle|Q_t(x^n)\middle|z^n\right\rangle$ 的期望值。

引理[17]：令 $\nu$ 是有限维的希尔伯特空间，$\varepsilon\subset S(\nu)$ 为满足对任意的 $\sigma\in\varepsilon$ 有 $\sigma\leqslant\mu\cdot id_\nu$ 的密度算符集，$p$ 是 $\varepsilon$ 上的概率分布。对于任意的正数 $\lambda$，定义取值于 $\varepsilon$ 上的独立同分布随机变量序列 $X_1,\cdots,X_L$，使得当 $\sigma\in\varepsilon$ 时，有 $p(\sigma)=\Pr\left\{X_i=\Pi_{\rho,\lambda}^{'}\cdot\sigma\cdot\Pi_{\rho,\lambda}^{'}\right\}$ 成立。此处 $\rho := \sum_{\sigma\in\varepsilon}p(\sigma)\sigma$，$\Pi_{\rho,\lambda}^{'}$ 是由 $\rho$ 的大于 $\frac{\lambda}{\dim\nu}$ 的特征值相应的特征向量张成的子空间(dim: 维度)。对于任意的 $\xi\in[0,1]$，有：

$$P\left(\left\|L^{-1}\sum_{i=1}^{L}X_i-\Pi_{\rho,\lambda}^{'}\cdot\rho\cdot\Pi_{\rho,\lambda}^{'}\right\|>\xi\right)\leqslant 2\cdot(\dim\nu)\exp\left[-L\frac{\xi^2\lambda}{2\ln 2(\dim\nu)\mu}\right], \tag{29}$$

令 $\nu$ 是 $\Pi_{p_t v_t,\alpha\sqrt{a}}$ 的投影空间范围。

由(5)式得：$\dim\nu\leqslant 2^{nS(p_t)+Kd\alpha\sqrt{an}}$，此外对所有的 $x^n$，有：

$$\begin{aligned} Q_t(x^n)=\Pi_{p_t v_t,\alpha\sqrt{a}}\Pi_{v_t,\alpha}(x^n)\cdot v_t^{\otimes n}(x^n)\cdot\Pi_{v_t,\alpha}(x^n)\Pi_{p_t v_t,\alpha\sqrt{a}}\leqslant 2^{-nS(v_t|p_t)+Kad\alpha\sqrt{n}}\Pi_{p_t v_t,\alpha\sqrt{a}}\Pi_{v_t,\alpha}(x^n)\Pi_{p_t v_t,\alpha\sqrt{a}}\leqslant \\ 2^{-nS(v_t|p_t)+Kad\alpha\sqrt{n}}\cdot\Pi_{p_t v_t,\alpha\sqrt{a}}\leqslant 2^{-nS(v_t|p_t)+Kad\alpha\sqrt{n}}\cdot id_\nu \end{aligned}, \tag{30}$$

式中第一个不等号由(9)式得出，第二个不等号是由于 $\Pi_{v_t,\alpha}$，$\Pi_{p_t v_t,\alpha\sqrt{a}}$ 是投影矩阵，第三个不等号是由于 $\Pi_{p_t v_t,\alpha\sqrt{a}}$ 是 $\nu$ 上的投影矩阵。

令 $\lambda=\xi$，运用引理2在(29)式中设置 $\mu := 2^{-n\cdot S(v_t|p_t)+Kad\alpha\sqrt{n}}$，考虑(30)式，当 $n$ 足够大时有：

$$\begin{aligned} P\left(\left\|\sum_{l=1}^{L_{n,t}}\frac{1}{L_{n,t}}Q_t(X_{j,l})-\theta_t\right\|>\xi\right)\leqslant 2^{n[S(p_t)+Kd\alpha\sqrt{an}]}\cdot\exp\left\{-L_{n,t}\frac{\xi^2}{2\ln 2}\lambda\cdot 2^{n[S(v_t|p_t)-S(p_t)+Kd\alpha\sqrt{n}(\sqrt{a}-1)]}\right\}= \\ 2^{n[S(p_t)+Kd\alpha\sqrt{an}]}\cdot\exp\left\{-L_{n,t}\frac{\xi^2}{2\ln 2}\lambda\cdot 2^{n[-\chi p_t;Z_t+Kd\alpha\sqrt{n}(\sqrt{a}-1)]}\right\}\leqslant\exp\left\{-L_{n,t}\cdot 2^{-n[\chi(p_t;Z_j)+\varsigma]}\right\} \end{aligned}, \tag{31}$$

$\varsigma$ 是与 $j,t$ 无关的正常数，且当 $\xi$ 趋于0时，$\varsigma$ 可任意小。式中最后一行用到了

$$S(p_t)-S(v_t|p_t)=S\left[\sum_j p_t(j)\sum_l\frac{1}{L_{n,t}}v_t^{\otimes n}\left(X_{j,l}^{(t)}\right)\right]-\sum_j p_t(j)S\left[\sum_l\frac{1}{L_{n,t}}v_t^{\otimes n}\left(X_{j,l}^{(t)}\right)\right]=\chi(p_t;Z_t), \tag{32}$$

令 $L_{n,t}=\left\lceil 2^{n[\chi(p_t;Z_t)+2\varsigma]}\right\rceil$，$n$ 足够大，由(31)式可得，对所有的 $j$ 有：

$$P\left(\left\|\sum_{l=1}^{L_{n,t}}\frac{1}{L_{n,t}}Q_t\left(X_{j,l}^{(t)}\right)-\theta_t\right\|>\xi\right)\leqslant\exp\left(-2^{n\varsigma}\right), \tag{32}$$

$$P\left(\left\|\sum_{l=1}^{L_{n,t}}\frac{1}{L_{n,t}}Q_t\left(X_{j,l}^{(t)}\right)-\theta_t\right\|\leqslant\xi\forall t\forall j\right)=1-P\left\{\bigcup_t\bigcup_j\left\{\left\|\sum_{l=1}^{L_{n,t}}\frac{1}{L_{n,t}}Q_t\left(X_{j,l}^{(t)}\right)-\theta_t\right\|>\xi\right\}\right\}\geqslant 1-TJ_n\exp\left(-2^{n\varsigma}\right)\geqslant$$
$$1-T2^{n\left\{\min_{t\in\theta}\left[I(p_t;W_t)-\frac{1}{n}\log_2 L_{n,t}\right]\right\}}\exp\left(-2^{n\varsigma}\right)\geqslant 1-2^{-n\upsilon} \tag{33}$$

$\upsilon$ 为与 $j$，$t$ 无关的正常数。

由(20)式，(33)式可知，对任意的 $\xi>0$，$n$ 足够大，

$$\left\{\bigcap_t\left[\max_{j\in\{1,\cdots,J_n\}}\sum_{l=1}^{L_{n,t}}\frac{1}{L_{n,t}}W_t^n\left(D_j^c(\chi)|X_{j,l}^{(t)}\right)\leqslant\xi\right]\right\}\cap\left\{\left\{\left\|\sum_{l=1}^{L_{n,t}}\frac{1}{L_{n,t}}Q_t\left(X_{j,l}^{(t)}\right)-\theta_t\right\|\leqslant\xi\forall t\forall j\right\}\right\}, \tag{34}$$

存在一个正概率，这意味着可以从 $X_{j,l}^{(t)}$ 中找到一个 $x_{j,l}^{(t)}$ 使得对于所有的 $t\in\theta$，$j\in\{1,\cdots,J_n\}$，有：

$$\sum_{l=1}^{L_{n,t}}\frac{1}{L_{n,t}}W_t^n\left(D_j^c|x_{j,l}^{(t)}\right)\leqslant\xi, \tag{35}$$

$$\left\|\sum_{l=1}^{L_{n,t}}\frac{1}{L_{n,t}}Q_t\left(x_{j,l}^{(t)}\right)-\theta_t\right\|\leqslant\xi. \tag{36}$$

对于任意的 $\gamma>0$ 令 $R:=\min_{t\in\theta}\max_{u\to A\to(BZ)_t}\left[I(u;B_t)-\limsup_{n\to\infty}\frac{1}{n}\chi\left(u;Z_t^{\otimes n}\right)\right]-\gamma$，选取 $\mu<\frac{1}{2}\gamma$，对每个 $t\in\theta$，存在 $(n,J_n)$ 码 $\left\{\left(x_{j,l}^{(t)}\right)_{j=1,\cdots,J_n,l=1,\cdots,L_{n,t}},\{D_j;j=1,\cdots,J_n\}\right\}$ 使得

$$\frac{1}{n}\log_2 J_n\geqslant R, \tag{37}$$

$$\lim_{n\to\infty}\max_{t\in\theta}\max_{j\in\{1,\cdots,J_n\}}\sum_{l=1}^{L_{n,t}}\frac{1}{L_{n,t}}W_t^n\left(D_j^c|x_{j,l}^{(t)}\right)=0, \tag{38}$$

在(28)式中选择适当的 $\alpha$ 使得对所有的 $j$，满足 $\left\|v_t^{\otimes n}\left(x_{j,l}^{(t)}\right)-Q_t\left(x_{j,l}^{(t)}\right)\right\|<\xi$。

对任意给定的 $j'\in\{1,\cdots,J_n\}$，由(28)式和(29)式可以得出

$$\left\|\sum_{l=1}^{L_{n,t}}\frac{1}{L_{n,t}}v_t^{\otimes n}\left(x_{j',l}^{(t)}\right)-\theta_t\right\|\leqslant\left\|\sum_{l=1}^{L_{n,t}}\frac{1}{L_{n,t}}v_t^{\otimes n}\left(x_{j',l}^{(t)}\right)-\sum_{l=1}^{L_{n,t}}\frac{1}{L_{n,t}}Q_t\left(x_{j',l}^{(t)}\right)\right\|+\left\|\sum_{l=1}^{L_{n,t}}\frac{1}{L_{n,t}}Q_t\left(x_{j',l}^{(t)}\right)-\theta_t\right\|\leqslant\sum_{l=1}^{L_{n,t}}\frac{1}{L_{n,t}}\left\|v_t^{\otimes n}\left(x_{j',l}^{(t)}\right)-Q_t\left(x_{j',l}^{(t)}\right)\right\|+$$
$$\left\|\sum_{l=1}^{L_{n,t}^{(t)}}\frac{1}{L_{n,t}}Q_t\left(x_{j',l}^{(t)}\right)-\theta_t\right\|\leqslant 2\xi \tag{39}$$

且 $\left\|\sum_{j=1}^{J_n}\frac{1}{J_n}\sum_{l=1}^{L_{n,t}}\frac{1}{L_{n,t}}v_t^{\otimes n}\left(x_{j,l}^{(t)}\right)-\theta_t\right\|\leqslant\xi$ 成立。

对取值在 $\{1,\cdots,J_n\}$ 中的均匀分布 $X_{\text{uni}}$，由引理[15]和 (39)式可得：

$$\chi\left(X_{\text{uni}};Z_t^{\otimes n}\right)=S\left[\sum_{j=1}^{J_n}\frac{1}{J_n}\sum_{l=1}^{L_{n,t}}\frac{1}{L_{n,t}}v_t^{\otimes n}\left(x_{j,l}^{(t)}\right)\right]-\sum_{j=1}^{J_n}\frac{1}{J_n}S\left[\sum_{l=1}^{L_{n,t}}\frac{1}{L_{n,t}}v_t^{\otimes n}\left(x_{j,l}^{(t)}\right)\right]\leqslant$$
$$\left|S\left[\sum_{j=1}^{J_n}\frac{1}{J_n}\sum_{l=1}^{L_{n,t}}\frac{1}{L_{n,t}}v_t^{\otimes n}\left(x_{j,l}^{(t)}\right)\right]-S(\theta_t)\right|+\left|S(\theta_t)-\sum_{j=1}^{J_n}\frac{1}{J_n}S\left[\sum_{l=1}^{L_{n,t}}\frac{1}{L_{n,t}}v_t^{\otimes n}\left(x_{j,l}^{(t)}\right)\right]\right|\leqslant \tag{40}$$
$$\xi\log_2 d-\xi\log_2\xi+\left|\sum_{j=1}^{J_n}\frac{1}{J_n}\left\{S(\theta_t)-S\left[\sum_{l=1}^{L_{n,t}}\frac{1}{L_{n,t}}v_t^{\otimes n}\left(x_{j,l}^{(t)}\right)\right]\right\}\right|\leqslant 3\xi\log_2 d-\xi\log_2\xi-2\xi\log_2 2\xi$$

通过(40)式，对于任意的 $\lambda>0$，如果 $n$ 足够大，则有：

$$\max_{t\in\theta}\chi\left(X_{\text{uni}};Z_t^{\otimes n}\right)\leqslant\lambda, \tag{41}$$

对于每个 $t\in\theta$，定义 $(n,J_n)$ 码 $(E_t,\{D_j;j=1,\cdots,J_n\})$，$E_t$ 满足对 $l\in\{1,\cdots,L_{n,t}\}$ 有 $P\left(E_t(j)=x_{j,l}^{(t)}\right)=\frac{1}{L_{n,t}}$

结合(38)式，(41)式有：

$$C_{S,\mathrm{CSI}} \geqslant \min_{t\in\theta} \max_{u\to A\to (BZ)_t}\left[I(u;B_t)-\limsup_{n\to\infty}\frac{1}{n}\chi\left(u;Z_t^{\otimes n}\right)\right]. \tag{42}$$

2) 知道信道状态信息情况时的上界：

令 $(C_n)$ 是一系列满足如下条件的 $(n,J_n)$ 码：

$$\max_{t\in\theta}\max_{j\in\{1,\cdots,J_n\}}\sum_{x^n\in A^n}E\left(x^n|j\right)W_t^n\left(D_j^c|x^n\right)=:\xi_{1,n}, \tag{43}$$

$$\max_{t\in\theta}\chi\left(J;Z_t^{\otimes n}\right)=:\xi_{2,n}, \tag{44}$$

这里 $\lim\limits_{n\to\infty}\xi_{1,n}=0,\lim\limits_{n\to\infty}\xi_{2,n}=0$，$J$ 表示在 $\{1,\cdots,J_n\}$ 上均匀分布的随机变量。

定义窃听信道 $(W_t,v_t)$ 的安全容量为 $C(W_t,v_t)$，选择 $t'\in\theta$ 使得 $C(W_{t'},v_{t'})=\min_{t\in\theta}C(W_t,v_t)$ [14]。

即使在没有窃听的情况下(仅有一条经典信道 $W_{t'}$)，信道容量不可能超出 $I\left(X_{\mathrm{uni}};B_t\right)+\eta$，$\eta$ 为大于零的任意常数[18]。因此对于任意的 $\xi>0$，选取 $\eta=\frac{1}{2}\xi$，如果 $n$ 足够大，则带有量子窃听的经典信道 $(W_{t'},v_{t'})$ 的容量不大于:

$$I\left(X_{\mathrm{uni}};B_t\right)+\eta\leqslant\left[I\left(X_{\mathrm{uni}};B_t\right)-\limsup_{n\to\infty}\chi\left(X_{\mathrm{uni}};Z_t^{\otimes n}\right)\right]+\eta+\xi_{2,n}\leqslant\left[I\left(X_{\mathrm{uni}};B_t\right)-\limsup_{n\to\infty}\frac{1}{n}\chi\left(X_{\mathrm{uni}};Z_t^{\otimes n}\right)\right]+\xi, \tag{45}$$

因此不可能超出最糟糕窃听信道的安全容量，即:

$$C_{S,\mathrm{CSI}}\leqslant\min_{t\in\theta}\max_{u\to A\to (BZ)_t}\left[I(u;B_t)-\limsup_{n\to\infty}\frac{1}{n}\chi\left(u;Z_t^{\otimes n}\right)\right], \tag{46}$$

结合(42)式与(46)式可得(35)式。

3) 不知道信道状态情况时的下界：

在 $A^n$ 上设定概率分布 $p$，令 $J_n=\left\lfloor 2^{\min_{t\in\theta}[nI(p;W_t)-\log L_n-n\mu]}\right\rfloor$，$L_n$ 为自然数随后将确定，$\mu$ 在文中已被定义，令 $p'$，$X^n$ 和 $D_j$ 与经典信道情况相同，(23)式仍成立。

对于正数 $\alpha$ 定义：$Q_t\left(x^n\right):=\Pi_{pv_t,\alpha\sqrt{a}}\Pi_{v_t,\alpha}\left(x^n\right)\cdot v_t^{\otimes n}\left(x^n\right)\cdot\Pi_{v_t,\alpha}\left(x^n\right)\Pi_{pv_t,\alpha\sqrt{a}}$，$\theta_t:=\sum\limits_{x^n\in\mathrm{T}_{p,\delta}^n}p'^n\left(x^n\right)Q_t\left(x^n\right)$。

对于任一正 $\delta$，令 $L_n=\left\lceil 2^{n\max_t[\chi(p;Z_t)+\delta]}\right\rceil$，$n$ 足够大，与证明(33)式相同，存在正常数 $\upsilon$ 使:

$$P\left(\left\|\sum_{l=1}^{L_n}\frac{1}{L_n}Q_t\left(X_{j,l}^{(t)}\right)-\theta_t\right\|\leqslant\xi\forall t\forall j\right)\geqslant 1-2^{-n\upsilon}. \tag{47}$$

对任意的正数 $\xi$ 选取适当的 $\alpha$，由(23)式和(47)式知 $X_{j,l}$ 中存在 $x_{j,l}$ 使得对所有的 $t\in\theta$ 和 $j\in\{1,\cdots,J_n\}$ 下式成立：

$$\begin{aligned}&\sum_{l=1}^{L_n}\frac{1}{L_n}W_t^n\left(D_j^c|x_{j,l}\right)\leqslant\xi,\\&\left\|\sum_{l=1}^{L_n}\frac{1}{L_n}Q_t\left(x_{j,l}\right)-\theta_t\right\|\leqslant\xi,\end{aligned} \tag{48}$$

对任意 $\gamma>0$，令 $R:=\max_{u\to A\to (BZ)_t}[\min_{t\in\theta}I(u;B_t)-\max_t\chi(u;Z_t)]-\gamma$，存在 $(n,J_n)$ 码 $\left(E,\left\{D_j:j=1,\cdots,J_n\right\}\right)$，其中 $E$ 满足对于所有的 $l\in\left\{1,\cdots,L_{n,t}\right\}$ 有 $P\left[E(j)=x_{j,l}\right]=\frac{1}{L_{n,t}}$，使得 $\liminf_{n\to\infty}\frac{1}{n}\log_2 J_n\geqslant R$，

$$\lim_{n\to\infty}\max_{t\in\theta}\max_{j\in\{1,\cdots,J_n\}}\sum_{l=1}^{L_n}\frac{1}{L_n}W_t^n\left(D_j^c|x_{j,l}\right)=0, \tag{49}$$

与证明(41)式相同，对于取值在 $\{1,\cdots,J_n\}$ 上的均匀分布 $X_{\mathrm{uni}}$ 可得：

$$\max_{t\in\theta}\chi\left(X_{\mathrm{uni}};Z_t^{\otimes n}\right)\leqslant\xi, \tag{50}$$

由(49)和(50)式知

$$C_S\geqslant\max_{u\to A\to (BZ)_t}\left[\min_{t\in\theta}I\left(u;B_t\right)-\max_{t\in\theta}\chi\left(u;Z_t\right)\right]. \tag{51}$$

## 5 结 论

在经典复合窃听信道的基础上,将经典窃听改为量子窃听,把经典信息论与量子信息论结合起来,并证明存在这样的编码译码方案:在保证窃听者得不到任何信息的情况下,当Alice知道信道状态信息 $t$ 时,多用户信道就退化为点对点信道,可以计算出带有量子窃听的经典复合信道的安全容量;此外,当Alice不知道信道状态信息 $t$ 时,由于在多用户信道模型中,多个消息对应的信息传输速率表示为向量,所以信道容量也相应地表示为空间区域,在此得出了这种信道模型的安全容量的下界。

## 参 考 文 献


1 Guo Dabo, Zhang Yanhuang, Wang Yunyan. Performance optimization for the reconciliation of Gaussian quantum key distribution[J]. Acta Optica Sinica, 2014, 34(1) : 0127001.
郭大波, 张彦煌, 王云艳. 高斯量子密钥分发数据协调的性能优化[J]. 光学学报, 2014, 34(1): 0127001.

2 Wang Yunyan, Guo Dabo, Zhang Yanhuang, *et al*.. Algorithm of multidimensional reconciliation for continuous-variable quantum key distribution[J]. Acta Optica Sinica, 2014, 34(8): 0827002.
王云艳, 郭大波, 张彦煌, 等. 连续变量量子密钥分发多维数据协调算法[J]. 光学学报, 2014, 34(8): 0827002.

3 Zhu Feng, Wang Qin. Quantum key distribution protocol based on heralded single photon source[J]. Acta Optica Sinica, 2014, 34(6): 0627002.
朱 峰, 王 琴. 基于指示单光子源的量子密钥分配协议[J]. 光学学报, 2014, 34(6): 0627002.

4 Li Ke. Aspects of Quantum Channel Capacities[D]. Hefei: University of Science and Technology of China, 2009: 1-5.
李 科. 关于量子信道容量的研究[D]. 合肥: 中国科学技术大学, 2009: 1-5.

5 P Sen. Achieving the Han-Kobayashi inner bound for the quantum interference channel[C]. IEEE International Symposium on Information Theory Proceedings, 2012: 736-740.

6 S Lloyd. Capacity of the noisy quantum channel[J]. Physical Review A, 1997, 55(3): 1613-1622.

7 R Konig, G Smith. Classical capacity of quantum thermal noise channels to within 1.45 bits[J]. Phys Rev Let, 2013, 110 (4): 040501.

8 D Blackwell, L Breiman, A Thomasian. The capacity of a class of channels[J]. The Annals of Mathematical Statistics, 1959, 30(4): 1229-1241.

9 Yingbin Liang, Gerhard Kramer, H Vincent Poor, *et al*.. Compound wiretap channels[J]. EURASIP Journal on Wireless Communications and Networking, 2009, 2009(5): 142374.

10 I Bjelakovic, H Boche, J Sommerfeld. Capacity results for compound wiretap channels[C]. IEEE Information Theory Workshop, 2011: 60-64.

11 M M Wilde. Sequential decoding of a general classical- quantum channel[J]. Proceedings of the Royal Society A: Mathematical, Physical and Engineering Science, 2013, 469(2157): 20130259.

12 G Bagherikaram, A S Motahari, A K Khandani. The secrecy capacity region of the Gaussian MIMO broadcast channel[J]. IEEE Transactions on Information Theory, 2013, 59(5): 2673-2682.

13 Z Rezki, A Khisti, M Alouini. On the secrecy capacity of the wiretap channel with imperfect main channel estimation[J]. IEEE Transactions on Communications, 2014, 62(10): 3652-3664.

14 M M Wilde. From Classical to Quantum Shannon Theory[M]. Cambridye: Cambridge University Press, 2013: 363-386.

15 A Winter. Coding theorem and strong converse for quantum channels[J]. IEEE Transactions on Information Theory, 1999, 45(7): 2481-2485.

16 T Ogawa, H Nagaoka. Making good codes for classical-quantum channel coding via quantum hypothesis testing[J]. IEEE Transactions on Information Theory, 2007, 53(6): 2261-2266.

17 R Ahlswede, A Winter. Strong converse for identification via quantum channels[J]. IEEE Transactions on Information Theory, 2002, 48(3): 569-579.

18 M A Nielsen, I L Chuang. Quantum Computation and Quantum Information[M]. Cambridge: Cambridge University Press, 2000: 500-514.


栏目编辑: 刘丰瑞