多天线系统中面向物理层安全的极化编码方法

白慧卿 金 梁 肖帅芳 易 鸣*
(国家数字交换系统工程技术研究中心 郑州 450002)

摘 要：该文提出一种基于多输入信道最大容量差映射的极化安全编码方法，通过适当降低信道极化速度达到提高安全传输速率的目的。首先，利用信道极化结构，将极化后的逻辑信道按信道质量划分为好信道与差信道两类；然后，通过具体的逻辑信道删除率迭代分析，提出一种能够有效提升差逻辑信道容量并降低好逻辑信道容量的最大容量差信道映射方法，达到降低信道极化速度的目的；最后，利用加权修正合法信道与窃听信道最大容量差映射结果，实现多输入信道下的极化安全编码。仿真结果表明，在极化阶数 $n=9$ 的二进制删除信道下，所提方法相比随机映射与 Arikan 方法，安全传输速率分别由 0.029, 0.004 提升到了 0.042，并且所提方法同样适用于衰落信道场景。

关键词：极化编码；物理层安全；信道映射；多输入信道
中图分类号： TN918 **文献标识码**： A **文章编号**：1009-5896(2017)11-2587-07
DOI: 10.11999/JEIT170068

Polar Code for Physical Layer Security in Multi-antenna Systems

BAI Huiqing JIN Liang XIAO Shuaifang YI Ming*
(*National Digital Switching System Engineering and Technological Research Center*, *Zhengzhou* 450002, *China*)

Abstract: A maximal-capacity-difference mapping-based secrecy polar coding method is proposed. It improves the secrecy rate by reducing the channel polarization speed. First, the polarized channels are divided into two categoryies based on the polarization structure: the good quality ones and the bad quality ones. By analyzing the eraser rates of the polarized channels, a maximal-capacity-difference mapping method is proposed. Through improving the capacity of the bad polarized channels and reducing that of the good polarized channels, the channel polarization speed decreases efficiently. Finally, weighting is adopted to modify the maximal-capacity-difference mapping results between legitimate channels and wiretap channels, thus the secrecy polar coding in multi-input channel is implemented. Simulation results verify that the secrecy rate of proposed method in binary erasure channels can be increased from 0.029 and 0.004 to 0.042, compared to the random mapping method and Arikan's method at polarization order $n=9$, respectively. And the proposed method also works in fading channels.

Key words: Polar codes; Physical layer security; Channel mapping; Multi-input channel

1 引言

无线物理层安全编码是一种加入了安全约束的特殊信道编码，能够在保证授权双方信息可靠传输的同时防止私密信息被窃听，是一种重要的物理层安全技术[1,2]。目前，实现安全编码的主要方法是在传统纠错码的基础之上，结合信道特征差异化合法接收者与窃听者的接收性能[3–5]。其中，母码的纠错性能和信道的差异性分别保证了传输的可靠性和安全性，是影响安全编码性能的关键。

Arikan[6]基于信道极化理论首次提出的极化编码，是一种能够达到香农限且编译码复杂度低的信道编码方法，目前已被选取为 5G 控制信道增强移动带宽场景的编码方案。由信道极化结构，极化编译码性能与传输信道质量天然耦合绑定，经不同信道传输时对特定信息位恢复能力也大不相同，所以采用极化码作为安全编码的母码具有天然的优势[7,8]。已有学者对极化安全编码的理论限进行了研究，分别在弱安全和强安全条件下逼近了安全容量[9,10]。然而在有限码长下，仍存在一部分极化逻辑信道其容量介于 0 和 1 之间[11]，如何提高实用极化编码的安全传输速率是一个亟待解决的问题。文献[12]在保证编码可靠性的基础上，采用信息打孔方法提升极化编码的传输速率。文献[13]引入安全约束优化打孔位置，将对私密信息位影响程度最低的输

收稿日期：2017-01-19；改回日期：2017-05-12；网络出版：2017-06-27
*通信作者：易鸣 acco666666@sina.com
基金项目：国家863计划项目(2015AA01A708)，国家青年科学基金(61501516)
Foundation Items: The National 863 Program of China (2015AA01A708), The National Natural Science Foundation for Young Scientists of China (61501516)

出位打孔，获得了更好的性能。文献[7]则采用协作干扰极化编码方法，提升系统整体的安全速率。然而，上述研究局限于单天线场景，安全增益仅来源于合法信道与窃听信道的信噪比差异。

实际上，多天线通信系统具有更加丰富的信道特征，信道差异性更加明显，也是未来安全编码技术研究的方向[14]。文献[15]研究了并行信道转移概率不同的多输入信道下的极化编码，提出一种准最优的等容量信道分割方法，在有限码长条件下进一步提高了最好逻辑信道的质量，降低了误码率，但遗憾的是作者在此并没有考虑安全性。当引入安全约束后，在逻辑信道质量最好的位置传输的是随机信息，而私密信息位于合法逻辑信道质量“好”且窃听逻辑信道质量“差”的相应位置。此时，在系统可容忍的限度内适当地降低信道极化速度，牺牲一部分随机信息的传输可靠性，能够换取更高的安全增益。

在多传输信道极化编码中，不同的编码信道映射方法对极化编码各逻辑信道的极化影响程度不同。为此，本文提出了一种最大容量差的信道映射方法，即使信道极化过程中每次递归分解的两组信道具有最大的容量差。通过对极化码结构的分析可以证明，该信道映射方法能够提升极化过程中差逻辑信道的容量并降低好逻辑信道的容量，从而降低信道极化速度。最后，基于所提出的基于最大容量差映射，本文通过加权修正进一步给出了多输入信道下的极化安全编码方案，相比于随机编码信道映射，该方案有效增加了私密信息编码位的数量，达到提升安全传输速率的效果。

2 相关概念

2.1 性能指标

Arikan 提出的信道极化过程包含信道合并和信道分割两步。信道合并将单个二进制对称信道 $W:X\to Y$ 重复使用 N 次进行迭代，得到合并信道 $W_N:X^N\to Y^N$；然后再将合并后的信道看作 N 个相互独立的逻辑信道 $W_N^{(i)}$，即实现信道的分割。经上述信道极化操作后，$N\,(N\to\infty)$个完全相同的传输信道 W 可以转化为两类逻辑信道：对称容量趋于 1 的“好”逻辑信道和对称容量趋于 0 的“差”逻辑信道[6]。假设 Alice 为发送者，Bob 为合法接收者，Eve 为窃听者，极化安全编码就是利用上述极化性质，将编码器的输入比特 $\boldsymbol{U}=\{u_1,u_2,\cdots,u_N\}$ 分为 3 类[10]：第 1 类为私密信息 $\boldsymbol{S}$，在 Bob“好”且 Eve“差”的逻辑信道上传输；第 2 类为随机信息 $\boldsymbol{R}$，在两者都“好”的逻辑信道上传输；第 3 类为固定信息 $\boldsymbol{F}$，在两者都“差”的逻辑信道上传输。令合法信道为 W，窃听信道为 W^*，且合法信道好于窃听信道，则有限码长下极化编码的安全规则表示为

$$\left.\begin{aligned}\boldsymbol{S}&\triangleq\left\{u_i:P_{\mathrm{e}}\left(W_N^{(i)}\right)\le P_{\mathrm{e,max}}^{\mathrm{B}},P_{\mathrm{e}}\left(W_N^{*(i)}\right)>P_{\mathrm{e,min}}^{\mathrm{E}}\right\}\\ \boldsymbol{R}&\triangleq\left\{u_i:P_{\mathrm{e}}\left(W_N^{*(i)}\right)\le P_{\mathrm{e,min}}^{\mathrm{E}}\right\}\\ \boldsymbol{F}&\triangleq\left\{u_i:P_{\mathrm{e}}\left(W_N^{(i)}\right)>P_{\mathrm{e,max}}^{\mathrm{B}}\right\}\end{aligned}\right\}\tag{1}$$

其中，$P_{\mathrm{e,max}}^{\mathrm{B}}$，$P_{\mathrm{e,min}}^{\mathrm{E}}$ 分别为 Bob 正常工作和 Eve 不可窃听所要求达到的误比特率门限。令 $|\boldsymbol{A}|$ 表示 $\boldsymbol{A}$ 中元素的个数，则极化编码的母码码率为 $R=(|\boldsymbol{S}|+|\boldsymbol{R}|)/N$，安全传输速率为 $R_S=|\boldsymbol{S}|/N$。

2.2 多输入信道下的极化码结构

当参与信道极化的并行信道具有不同的转移概率函数时，可将 Arikan 提出的单步信道变换单元改写为如图 1(a)所示形式，并记该变换为 $\boldsymbol{G}_2$。将 $a_1,a_2,\cdots,a_N$ 的简写为 a_1^N。输入比特 u_1^2 编码为符号 x_1^2，然后分别经过传输信道 W_1^2 传输到达接收端。那么，经单步变换极化后的逻辑信道可分别表示为

$$\left.\begin{aligned}\mathcal{W}'\left(y_1^2\,|u_1\right)&=\sum_{u_2\in\mathcal{X}}\frac{1}{2}W_1\left(y_1\,|u_1\oplus u_2\right)W_2\left(y_2\,|u_2\right)\\ \mathcal{W}''\left(y_1^2,u_1\,|u_2\right)&=\frac{1}{2}W_1\left(y_1\,|u_1\oplus u_2\right)W_2\left(y_2\,|u_2\right)\end{aligned}\right\}\tag{2}$$

记上述信道变换为 $(W_1,W_2)\mapsto(\mathcal{W}',\mathcal{W}'')$，则存在如下命题：

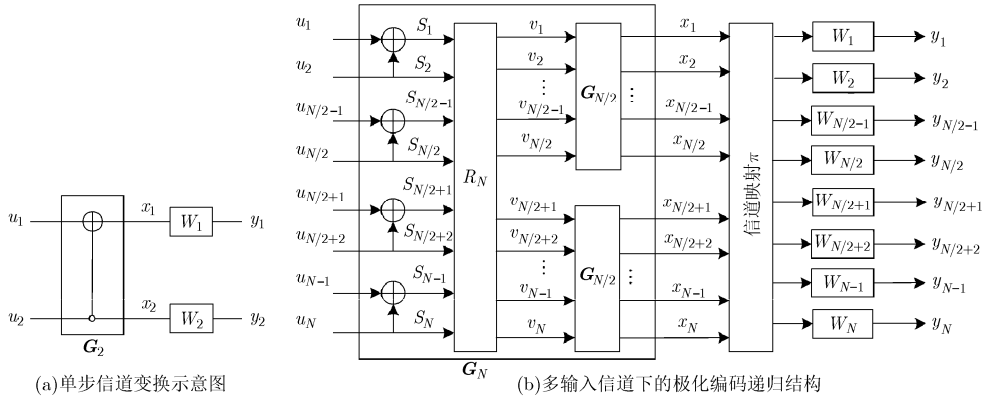
命题 1 若 $(W_1,W_2)\mapsto(\mathcal{W}',\mathcal{W}'')$，如果 W_1 和 W_2 均为二进制删除信道(Binary Erasure Channel, BEC)，删除率分别为 ε_1 和 ε_2，则逻辑信道 $\mathcal{W}'$ 和 $\mathcal{W}''$ 也为 BEC 信道，删除率分别为 $\varepsilon_1+\varepsilon_2-\varepsilon_1\varepsilon_2$ 和 $\varepsilon_1\varepsilon_2$ (证明略)。

在 $N=2^n\ (n>0)$个输入信道上构造码长为 N 的极化码，如图 1(b)所示。R_N 表示对长度为 N 的序列进行奇偶排序变换[6]。传输信道 W_1^N 各自具有不同的删除率，首先需根据信道映射规则 π 完成极化变换的输入信道 w_1^N 到传输信道 W_1^N 的一一映射；然后，依据递归结构进行信道变换 $\boldsymbol{G}_N$。令映射 $\pi:w\{1,2,\cdots,N\}\to W\{1,2,\cdots,N\}$ 表示极化变换输入信道 w_i 经 $\pi(i)=j$ 映射为传输信道 W_j，即 $w_i=W_{\pi(i)}=W_j$。则极化变换后 N 个逻辑信道 $\mathcal{W}_N^{(i)}$ 的信道转移概率函数表示为

$$\mathcal{W}_N^{(i)}\left(y_1^N,u_1^{i-1}\,|u_i\right)=\sum_{u_{i+1}^N\in\mathcal{X}^{N-i}}\frac{1}{2^{N-1}}W_N\left(y_1^N\,|u_1^N\right)\tag{3}$$

需要注意的是，此时编码输入信道不再是单个传输信道的重复使用，而是多个不同传输信道的映射，因此，

$$W_N\left(y_1^N\,|u_1^N\right)=\prod_{i=1}^{N}w_i\left(y_i\,|x_i\right)=\prod_{i=1}^{N}W_{\pi(i)}\left(y_i\,|x_i\right)\tag{4}$$



(a)单步信道变换示意图　　(b)多输入信道下的极化编码递归结构

图 1 多输入信道下极化编码

其中，$x_1^N = \boldsymbol{G}\cdot u_1^N$，$\boldsymbol{G} = \boldsymbol{B}\cdot \boldsymbol{F}^{\otimes n}$ 为极化码生成矩阵[6]。

图 2 仿真了 BEC 下各子信道删除率 $W_1^N = \{0.2, 0.3, 0.4, 0.5, 0.6, 0.7, 0.8, 0.9\}$，码长 $N = 8$ 时，不同信道映射顺序下对各输入信息位删除率的影响。其中，横轴为输入信息位序号 1 至 N，依次对应于各比特输入信息；纵轴为删除率。仿真采取随机映射的方式。从图 2 可以看出，不同信道映射顺序对同一位置的输入信息删除率的影响不同；并且相同映射顺序对不同位置的删除率影响也不同。由此可见，信道映射规则是影响多输入信道下极化编码性能的关键因素。

3　多输入信道下的极化安全编码

信道的极化速度是衡量编码器阶数相同时的逻辑信道极化程度。极化速度越快，那么在相同阶数下逻辑信道容量越趋于 0 和 1 两极；反之，极化速度越慢则有更多的逻辑信道容量位于两极之间。当仅考虑极化编码的传输可靠性时，由于信息比特在质量最好的逻辑信道上传输，因此加快信道极化的速度能够降低该部分信息比特的错误率。然而引入安全约束后，私密信息位于合法逻辑信道质量“较好”(达到可靠门限 $P_{\mathrm{e,max}}^{\mathrm{B}}$)且窃听逻辑信道质量“较差”(达到安全门限 $P_{\mathrm{e,min}}^{\mathrm{E}}$)的相应位置。因此，在系统可容忍的限度内适当降低信道极化速度，增多“较好”和“较差”逻辑信道的数量，能够增加私密信息数量，达到提升安全传输速率的效果。降低极化速度会使母码的可靠性下降，但私密信息始终满足式(1)的可靠度约束，实际上降低的是随机信息的可靠性。因此，降低极化速度是一种确保私密信息可靠的同时提升安全速率的方法。

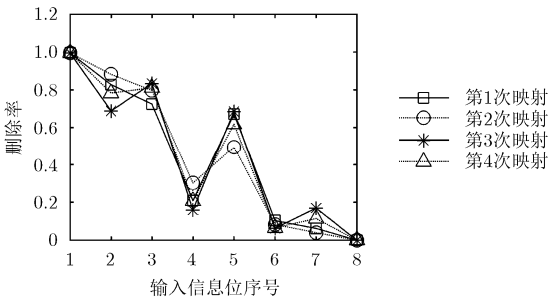


图 2 信道映射顺序对输入信息位删除率的影响

本节将通过对好逻辑信道与差逻辑信道的相对位置进行讨论，利用极化编码的递归结构进行逻辑信道质量分析，提出一种可以降低信道极化速度的信道映射方法，并在此基础上给出具体的极化安全编码方案。

3.1 编码信道映射方案设计

在一定码长下，信道极化速度降低反映为：差逻辑信道的容量升高，好逻辑信道的容量降低。根据图 1(b)，由于信道映射规则 π 未知无法准确划分两类逻辑信道，这里根据引理 1 对逻辑信道质量进行粗略分类。

引理 1　任给一组 $N = 2^n$ 个 BEC 信道，经信道极化后编码器输入节点 u_i 所对应的逻辑信道表示为 $\mathcal{W}_N^{(i)}, i = 1,2,\cdots,N$。令 $I\left(\mathcal{W}_N^{(j)}\right)$ 为 $\mathcal{W}_N^{(j)}$ 的对称容量，则有 $I\left(\mathcal{W}_N^{(j)}\right) < I\left(\mathcal{W}_N^{(j+N/2)}\right)$，$j = 1,2,\cdots,N/2$ (证明略)。

根据引理 1 可以认为差逻辑信道大多处于编码输入的前半部分，而好逻辑信道则大多处于后半部分，即：$\mathcal{W}_1^{N/2}$ 为差逻辑信道，$\mathcal{W}_{N/2+1}^{N}$ 为好逻辑信道。因此问题转化为寻找一种信道映射方式，使 $\mathcal{W}_1^{N/2}$ 的容量提升而 $\mathcal{W}_{N/2+1}^{N}$ 的容量降低。下面首先提出引理 2，然后以传输信道数量 $J = N = 8$ 为例，利用引理 2 的结论对信道映射规则 π 与逻辑信道质量间的关系进行讨论，提出一种满足要求的最大容量差信道映射方法。

引理 2　任意集合 $A = \{\varepsilon_1, \varepsilon_2, \cdots, \varepsilon_N\}$，$0 < \varepsilon_i < 1$ ($i = 1,2,\cdots,N$)，$N = 2^n$，$n > 0$。若 $p_i \in A$

($i=1,2,\cdots,N$)，且对任意 $j\neq i$ 有 $p_j\neq p_i$，令 $\sum p_i^j \triangleq p_i+p_{i+1}+\cdots+p_j$，$\prod p_i^j \triangleq p_i p_{i+1}\cdots p_j$，则当 $\left|\sum p_1^{N/2}-\sum p_{N/2+1}^{N}\right|$ 取最大时：(1) $\sum p_1^{N/2}\cdot\sum p_{N/2+1}^{N}$ 取得最小值；(2) $\prod p_1^{N/2}+\prod p_{N/2+1}^{N}$ 取得最大值(证明略)。

图 3 假设各 BEC 传输信道删除率 $\varepsilon(W_i)=\varepsilon_i$，$i=1,2,\cdots,8$。由于极化变换的输入信道 w_1^8 与传输信道 W_1^8 间存在映射关系 π，所以令 $\varepsilon(w_i)=p_i$，$p_i\in\{\varepsilon_1,\varepsilon_2,\cdots,\varepsilon_8\}$ 且对任意 $j\neq i$ 有 $p_j\neq p_i$。根据命题 1，信道极化后各逻辑信道 $\mathcal{W}_1^8$ 的删除率表达式如图 3 最左列所示。由于 p_i,p_j 的值很小，计算中令 $p_i+p_j-p_ip_j\approx p_i+p_j$。

从图 3 中可以看到，逻辑信道 $\mathcal{W}_1^4$ 的删除率表达式主要由因子 $\sum p_i^j$ 间进行乘法运算获得。由引理 1 的逻辑信道质量分类，为降低信道极化速度，需使逻辑信道 $\mathcal{W}_1^4$ 的容量升高，即 $\mathcal{W}_1^4$ 的删除率降低。将 $N=8$ 代入引理 2(1)，可知当 $\left|\sum p_1^4-\sum p_5^8\right|$ 最大时，$\sum p_1^4\sum p_5^8$ 最小，即 $\varepsilon(\mathcal{W}_2)$ 最小；将 $N=4$ 代入引理 2(1)，可知当 $\left|\sum p_1^2-\sum p_3^4\right|$ 和 $\left|\sum p_5^6-\sum p_7^8\right|$ 最大时，$\sum p_1^2\sum p_3^4$ 和 $\sum p_5^6\sum p_7^8$ 分别最小，即此时 $\varepsilon(\mathcal{W}_3)$ 取得最小值，$\varepsilon(\mathcal{W}_4)$ 取得局部最小值。

同样地，从图 3 中看到，逻辑信道 $\mathcal{W}_5^8$ 的删除率表达式主要由因子 $\prod p_i^j$ 间进行加法运算获得。由引理 1 的逻辑信道质量分类，为降低信道极化速度，需使逻辑信道 $\mathcal{W}_5^8$ 的容量降低，即 $\mathcal{W}_5^8$ 的删除率提高。将 $N=8$ 代入引理 2(2)，可知当 $\left|\sum p_1^4-\sum p_5^8\right|$ 最大时，$\prod p_1^4+\prod p_5^8$ 最大，即 $\varepsilon(\mathcal{W}_7)$ 最大；将 $N=4$ 代入引理 2(2)，可知当 $\left|\sum p_1^2-\sum p_3^4\right|$ 和 $\left|\sum p_5^6-\sum p_7^8\right|$ 最大时，$\prod p_1^2+\prod p_3^4$ 和 $\prod p_5^6+\prod p_7^8$ 分别最大，即此时 $\varepsilon(\mathcal{W}_3)$ 取得最大值，$\varepsilon(\mathcal{W}_4)$ 取得局部最大值。

根据图 1(b)所示的递归极化结构，对任意 $N>2$，极化变换单元 $\boldsymbol{G}_N$ 都可以利用奇偶排序分解为两个尺寸相同的变换单元 $\boldsymbol{G}_{N/2}$，极化后逻辑信道的删除率表达式具有与 $N=8$ 示例相同的形式。上述分析表明，利用引理 2 使每次递归分解的两个变换单元中的信道质量之差最大，能够有效提升差逻辑信道的容量并降低好逻辑信道的容量，实现降低信道极化速度的目的。为不失一般性，下面算法描述中采用信道容量作为信道质量的度量。

算法 1 最大容量差信道映射

给定一组 J ($J=N$，N 为码长)个并行传输信道，记容量分别为 $I(W_i)$，$i=1,2,\cdots,N$。输入信息序列 u_1^N 经信道变换 $\boldsymbol{G}_N$ 编码为 x_1^N，并将 x_i 通过信道 $W_{\pi(i)}$ 进行传输。则信道映射规则 π 根据以下步骤决定：

步骤 1 令集合 $S=\{W_1,W_2,\cdots,W_N\}$，将 S 平均分割成两个子集，$S_{b_1=0}$ 与 $S_{b_1=1}$，使两子集中的信道容量和 $\overline{I}_0=\sum_{j\in S_0}I(W_j)$ 与 $\overline{I}_1=\sum_{j\in S_1}I(W_j)$ 之差最大，即 $\left|\overline{I}_0-\overline{I}_1\right|$ 最大；

步骤 2 将各个 $S_{b_1b_2\cdots b_i}$ 进一步分割为 $S_{b_1b_2\cdots b_i0}$ 和 $S_{b_1b_2\cdots b_i1}$，同样地使 $\left|\overline{I}_{b_1b_2\cdots b_i0}-\overline{I}_{b_1b_2\cdots b_i1}\right|$ 最大；

步骤 3 重复步骤 2，直到子集数量增加到 N，此时每一个子集 $S_{b_1b_2\cdots b_d}$ 仅包含一个信道；

步骤 4 假设集合 $S_{b_1b_2\cdots b_d}$ 中的信道为 W_j，那么信道映射 π 满足：$\pi^{-1}(j)=\sum_{i=1}^{d}\left(b_i\cdot 2^{d-i}\right)+1$。

当所有 $I(W_i)$ 相等时，极化问题退化为 Arikan 的单一信道极化[6]，此时 π 不影响极化速度。当算法

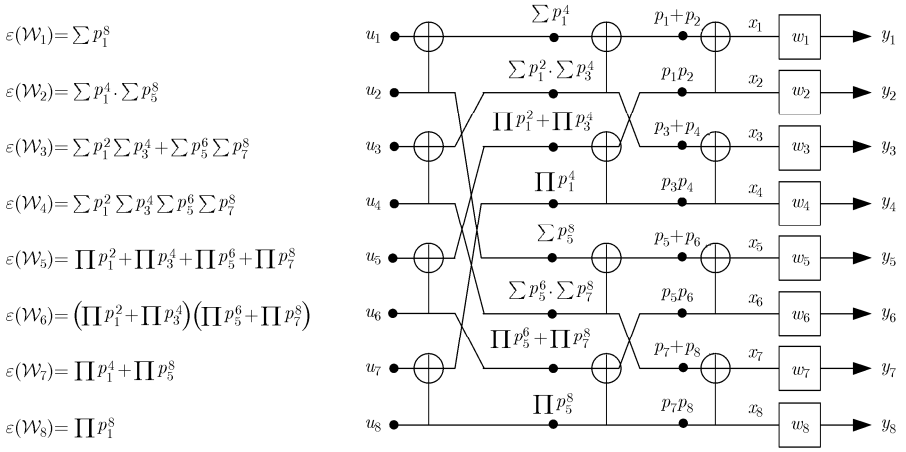


图 3 $N=8$ 时各逻辑信道的删除率计算示意图

1 中 $J<N$ 时，只要满足 $J=2^d$，可以将各个并行信道重复使用 N/J 次实现信道映射[15]，这里不再赘述。

3.2 极化安全编码方案

在实际通信中，发送端分别根据合法信道质量和窃听信道质量进行算法 1 运算得到的最优信道映射顺序(天线映射顺序)不完全相同，因此在编码中需要兼顾合法信道与窃听信道的最优映射结果。算法 2 利用权重修正信道映射结果并进行极化安全编码的可行方案，提出一种基于最大容量差映射的极化安全编码(Maximal-Capacity-Difference Mapping-based Secrecy Polar Coding, MCDMSPC)，具体描述如下。

算法 2　MCDMSPC

假设发射端天线数为 N_A，极化编码码长为 N，且满足 N/N_A 为整数；系统的安全可靠门限分别为 $P_{\mathrm{e,min}}^{\mathrm{E}}$ 与 $P_{\mathrm{e,max}}^{\mathrm{B}}$。通信开始前，收发双方互发训练序列获取各信道的信道状态信息。假设各合法信道 W_i 的容量分别为 $I(W_i)$，窃听信道 W_i^* 的容量分别为 $I\left(W_i^*\right)$，$i=1,2,\cdots,N_A$。

步骤 1　由算法 1，分别得到合法信道映射 $\pi_A\{1,2,\cdots,N_A\}=\left\{a_1,a_2,\cdots,a_{N_A}\right\}$ 与窃听信道映射 $\pi_B\{1,2,\cdots,N_A\}=\left\{b_1,b_2,\cdots,b_{N_A}\right\}$，其中 $a_i,b_i\in\{1,2,\cdots,N_A\}$，且对任意 $i\neq j$ 有 $a_i\neq a_j$，$b_i\neq b_j$；

步骤 2　分别计算合法并行信道容量的均方差 $I_{\mathrm{std}}^{\mathrm{B}}=\left(\dfrac{1}{N_A}\sum\limits_{i=1}^{N_A}\left(I(W_i)-\overline{I}(W)\right)^2\right)^{1/2}$，及窃听并行信道容量的均方差 $I_{\mathrm{std}}^{\mathrm{E}}=\left(\dfrac{1}{N_A}\sum\limits_{i=1}^{N_A}\left(I\left(W_i^*\right)-\overline{I}\left(W^*\right)\right)^2\right)^{1/2}$，其中 $\overline{I}(W)$ 和 $\overline{I}\left(W^*\right)$ 分别表示合法信道与窃听信道的平均容量；

步骤 3　将 a_i,b_i 分别赋予权重 $\mathrm{Wt}(a_i)=i\cdot\dfrac{I_{\mathrm{std}}^{\mathrm{B}}}{I_{\mathrm{std}}^{\mathrm{B}}+I_{\mathrm{std}}^{\mathrm{E}}}$，$\mathrm{Wt}(b_i)=i\cdot\dfrac{I_{\mathrm{std}}^{\mathrm{E}}}{I_{\mathrm{std}}^{\mathrm{B}}+I_{\mathrm{std}}^{\mathrm{E}}}$；

步骤 4　选取 a_1，并找到与之对应的 b_k，即 $a_1=b_k$，更新 a_1 的权重为 $\left(\mathrm{Wt}(a_1)+\mathrm{Wt}(b_k)\right)\big/2$；

步骤 5　依次选取 $a_2,a_3,\cdots,a_{N_A}$，重复步骤 4，得到全部 a_i 权重的更新；

步骤 6　将 $a_1,a_2,\cdots,a_{N_A}$ 按更新后的权重从小到大依次排列，得到序列 $c_1,c_2,\cdots,c_{N_A}$，则并行极化安全编码的信道映射为 $\pi\{1,2,\cdots,N_A\}=\left\{c_1,c_2,\cdots,c_{N_A}\right\}$；

步骤 7　根据步骤 6 确定的信道映射 π 得到信道极化输入信道 $\{w_1,w_1,\cdots,w_N\}$，结合 3.1 节的并行信道变换 $\boldsymbol{G}_N$，迭代计算合法逻辑信道 $W_N^{(i)}$ 与窃听逻辑信道 $W^{*(i)}_N$ 的信道转移概率，$i=1,2,\cdots,N$；

步骤 8　判断。将满足式(1) $\boldsymbol{S}\triangleq\left\{i:P_{\mathrm{e}}\left(W_N^{(i)}\right)<P_{\mathrm{e,max}}^{\mathrm{B}},P_{\mathrm{e}}\left(W_N^{*(i)}\right)>P_{\mathrm{e,min}}^{\mathrm{E}}\right\}$ 和 $\boldsymbol{F}\triangleq\left\{i:P_{\mathrm{e}}\left(W_N^{(i)}\right)>P_{\mathrm{e,max}}^{\mathrm{B}}\right\}$ 的输入信息位分别设置为私密信息和固定信息，其余为随机信息；

步骤 9　编码。根据步骤 8 中 3 类信息的划分，利用 $\boldsymbol{G}_N$ 和映射 π，完成并行信道下的极化安全编码。

映射顺序影响信道极化速度快慢的本质是并行信道间的差异性，差异性越大则映射对极化的影响越大，而当输入并行信道完全相同时，差异性不存在，极化问题退化为 Arikan 的模型。因此，算法 2 中采用信道容量均方差分别衡量 Bob 和 Eve 的并行信道差异性，并使得具有更大均方差的信道映射排序在最终的映射 π 中具有更大的权重(步骤 3)。

3.3 复杂度分析

一般情况下，一个码长为 N 的极化码在采用串行抵消(Successive Cancellation, SC)译码时，编译码计算复杂度和译码器所需的空间复杂度均为 $O(N\cdot\log_2 N)$[6,16]。算法 2 在传统极化安全编码的基础上，利用算法 1 在收发双方增加了映射与解映射步骤。而映射的本质是按信道质量进行排序，当并行信道数为 N_A 时该部分的平均计算复杂度为 $O(N_A\cdot\log_2 N_A)$，因此算法 2 的计算复杂度为 $O(N_A\cdot\log_2 N_A)+O(N\cdot\log_2 N)$。同样地，由于算法 2 要额外存储 N_A 路并行信道的信道状态信息，该部分的空间复杂度为 $O(N_A)$。因此，算法 2 的空间复杂度为 $O(N_A)+O(N\cdot\log_2 N)$。一般情况下 $N_A\ll N$，因此本文编码方案相对普通极化编码方法的编译码计算复杂度和空间复杂度没有明显提升。

4 性能仿真与分析

假设发射端天线数 $N_A=8$；安全可靠门限分别为 0.45 和 10^{-7}。为验证本文所提方法的安全性能，仿真分别与信道随机映射下的多输入极化安全编码方法 (Random Mapping-based Secrecy Polar Coding, RMSPC)和 Arikan 单一输入信道下的极化安全编码方法(Arikan's Secrecy Polar Coding, ASPC)进行对比。

图 4 仿真了 BEC 信道下安全传输速率随最大极化阶数 n 的变化，码长 $N=2^n$。假设合法与窃听传输信道平均容量分别为 $\overline{C}_W=0.85$, $\overline{C}_{W^*}=0.5$。具体地，在本文方法与 RMSPC 方法中各合法传输信道

容 量 为 $C_W=\{0.71,0.75,0.79,0.83,0.87,0.91,0.95,0.99\}$，各窃听容量为 $C_{W^*}=\{0.1,0.2,0.3,0.4,0.6,0.7,0.8,0.9\}$；在 ASPC 方法中，各合法信道容量均为 0.85，各窃听信道容量均为 0.5。从图 4 中可以看到，同一极化阶数下本文方法的安全速率明显高于另两种方法，这是由于本文方法不仅利用了信道平均容量的差异，还将编码与并行传输信道之间的差异性结合。然而，当极化阶数较大时，信道极化基本完成，此时本文方法性能逐渐接近 RMSPC 方法性能。作为对比，图 4 中还仿真了 $\overline{C}_W=0.85$, $\overline{C}_{W^*}=0.6$ 的情况。此时由于合法信道与窃听信道间的平均容量差变小，因而整体安全传输速率有所下降，但本文方法依旧具有明显的安全速率优势。仿真表明，本文方法能够提升较短码长下的极化编码安全传输速率；在 $\overline{C}_W=0.85$, $\overline{C}_{W^*}=0.5$ 的仿真条件下，当 $n=9$ 时，本文方法的安全速率为 0.042，高于随机映射方法(0.029)与 Arikan 方法(0.004)。

为便于理论分析，本文选取 BEC 信道进行编码方案设计分析，但该方法同样适用于衰落信道场景。图 5 在衰落信道下对所提极化安全编码方案进行了仿真。假设发射总功率为 1，各合法信道与窃听信道的信噪比分别为 $\mathrm{SNR}_W=\{1.2,1.7,2.3,2.8,3.4,4.1,5,6.9\}$ dB, $\mathrm{SNR}_{W^*}=\{-9.4,-6.1,-4.1,-2.5,0,1.1,2.4,3.9\}$ dB。除 RMSPC 方法和 ASPC 方法外，图 5 还对比了常用以提高多天线系统安全性能的人工噪声方法(Artificial Noise, AN)[17]，控制发射总功率仍为 1。从图中可以看到，本文方法在短码长下依旧具有明显的安全传输速率优势。

图 6 仿真了本文方法在多输入并行信道容量具有不同的均方差时的安全传输速率。同样取 $\overline{C}_W=0.85$, $\overline{C}_{W^*}=0.5$，随机生成满足图 6 均方差要求的 C_W 与 C_{W^*}。可以看到，在 n 相同时，$I_{\mathrm{std}}^{\mathrm{B}}$ 和 $I_{\mathrm{std}}^{\mathrm{E}}$ 越大，安全传输速率越大，这也说明了本文方法利用了并行传输信道之间的差异性，差异越大本方法效果越明显。

5 结论

为了提升有限码长下并行极化安全编码的传输速率，需要适当减缓信道极化速度，因此调节信道映射规则 π 是一种有效的方法。本文根据信道极化理论，提出了一种最大容量差信道映射方案，该方案令每次极化递归分解中的两信道集合具有最大的容量差，达到降低信道极化速度的目的，并在此基础上得到了安全传输速率较高的实用极化安全编码方法。该方法不显著增加极化编译码复杂度，并在保证私密信息传输可靠性的基础上，获得了相比 RMSPC 方法与 ASPC 方法更佳的安全传输速率。

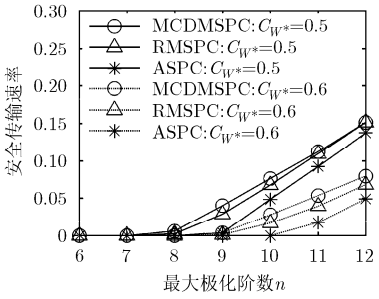


图 4 BEC 信道下极化安全编码的安全传输速率

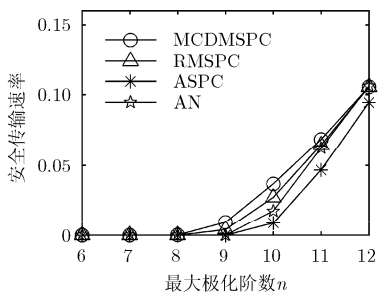


图 5 衰落信道下极化安全编码的安全速率

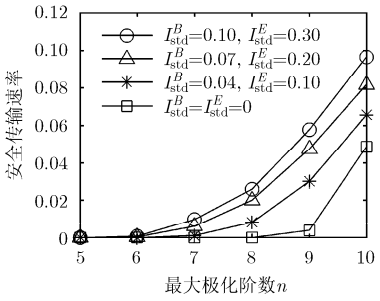


图 6 不同信道均方差下极化安全编码的安全速率

参 考 文 献

[1] KOLOKOTRONIS N, KATSIONTIS A, and KALOUPTSIDIS N. Secretly pruned convolutional codes: Security analysis and performance results[J]. *IEEE Transactions on Information Forensics and Security*, 2016, 11(7): 1500–1514. doi: 10.1109/TIFS.2016.2537262.

[2] WANG Bo, MU Pengcheng, WANG Chao, *et al*. Combining dirty-paper coding and artificial noise for secrecy[C]. IEEE International Communication on Acoustics, Speech and Signal Processing, Shanghai, China, 2016: 2034–2038.

[3] KLINC D, JEONGSEOK H, MCLAUGHLIN S W, *et al*. LDPC codes for the Gaussian wiretap channel[J]. *IEEE Transactions on Information Forensics Security*, 2011, 6(3): 532–540. doi: 10.1109/TIFS.2011.2134093.

[4] BALDI M, BIANCHI M, and CHIARALUCE F. Coding with scrambling, concatenation, and HARQ for the AWGN wire-tap channel: A security gap analysis[J]. *IEEE Transactions on Information Forensics Security*, 2012, 7(3): 883–894. doi: 10.1109/TIFS.2012.2187515.

[5] YI Ming, JI Xinsheng, HUANG Kaizhi, *et al*. Achieving strong security based on fountain code with coset precoding[J]. *IET Communications*, 2014, 8(14): 2476–2483. doi: 10.1049/iet-com.2013.1033.

[6] ARIKAN E. Channel polarization: A method for constructing capacity-achieving codes for symmetry binary input memoryless channels[J]. *IEEE Transactions on Information Theory*, 2009, 55(7): 3051–3073. doi: 10.1109/TIT.2009. 2021379.

[7] HAJIMOMENI M, AGHAEINIA H, KIM I M, *et al*. Cooperative jamming polar codes for multiple-access wiretap channels[J]. *IET Communications*, 2016, 10(4): 407–415. doi: 10.1049/iet-com.2015.0624.

[8] WEI Yipeng and ULUKUS S. Polar coding for the general wiretap channel with extensions to multiuser scenarios[J]. *IEEE Journal on Selected Areas in Communications*, 2016, 34(2): 278–291. doi: 10.1109/JSAC.2015.2504275.

[9] ANDERSSON M, RATHI V, THOBABEN R, *et al*. Nested polar codes for wiretap and relay channels[J]. *IEEE Communications Letters*, 2010, 14(4): 752–754. doi: 10.1109/LCOMM.2010.08.100875.

[10] MAHDAVIFAR H and VARDY A. Achieving the secrecy capacity of wiretap channels using polar codes[J]. *IEEE Transactions on Information Theory*, 2011, 57(10): 6428–6443. doi: 10.1109/TIT.2011.2162275.

[11] MIRGHASEMI H and BELFIORE J. The un-polarized bit-channels in the wiretap polar coding scheme[C]. International Conference on Wireless Communications, Vehicular Technology, Information Theory and Aerospace & Electronic Systems, Manchester, Denmark, 2014: 1–5.

[12] NIU K, CHEN K, and LIN J R. Beyond turbo codes: Ratecompatible punctured polar codes[C]. IEEE International Conference on Communications, Budapest, Hungary, 2013: 3423–3427.

[13] 易鸣, 季新生, 黄开枝, 等. 面向物理层安全的一种打孔极化编码方法[J]. 电子与信息学报. 2014, 36(12): 2835–2841. doi: 10.3724/SP.J.1146.2014.00013.
YI Ming, JI Xinsheng, HUANG Kaizhi, *et al*. A method based on puncturing polar codes for physical layer security[J]. *Journal of Electronics & Information Technology*, 2014, 36(12): 2835–2841. doi: 10.3724/SP.J.1146.2014.00013.

[14] GAO Y, CAI Y, SHI Q, *et al*. Joint transceiver designs for secure communications over MIMO relay[C]. IEEE International Conference on Acoustics, Speech and Signal Processing, Shanghai, China, 2016: 3851–3855.

[15] CHEN K, NIU K, and LIN J. Practical polar code construction over parallel channels[J]. *IET Communications*, 2013, 7(7): 620–627. doi: 10.1049/iet-com.2012.0428.

[16] ARIKAN E and TELATAR E. On the rate of channel polarization[C]. IEEE International Symposium on Information Theory, Seoul, South Korea, 2009: 1493-1495.

[17] WANG W, TEH K C, and LI K H. Artificial noise aided physical layer security in multi-antenna small-cell networks [J]. *IEEE Transactions on Information Forensics and Security*, 2017, 12(6): 1470–1482. doi: 10.1109/TIFS.2017. 2663336.

白慧卿：　女，1988 年生，博士生，研究方向为无线物理层安全技术.

金　梁：　男，1969 年生，教授，研究方向为移动通信、无线物理层安全技术.

肖帅芳：　男，1989 年生，博士生，研究方向为无线通信安全.

易　鸣：　男，1986 年生，讲师，研究方向为无线物理层安全编码.