概率译码转发中继系统中的安全极化编码方法

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

摘 要：该文针对中继节点依概率辅助译码转发的通信场景，提出一种中继辅助的安全极化编码方法，保证私密信息可靠传输的同时，达到提高安全传输速率的目的。首先，发送端分别进行两层极化编码——中继概率转发行为构成的虚拟二进制删除信道下的极化编码和实际传输信道下的极化编码，并将私密信息分别隐藏在两层码字中，分时隙广播出去。然后，中继依概率译码后提取出合法用户无法直接接收的固定信息再次进行安全极化编码并转发。最后，接收端利用收到的中继转发码字和发端码字依次分层进行译码。理论和仿真分析证明，所提方法下合法用户能够可靠接收私密信息，而窃听者无法获取任何私密信息信息量；安全传输速率随着码长和中继转发概率的增加而增大，且高于一般的安全极化编码方法。

关键词：极化编码；物理层安全；中继；概率译码转发
中图分类号：TN918 **文献标识码**：A **文章编号**：1009-5896(2018)09-2112-07
DOI: 10.11999/JEIT171142

Secrecy Polar Coding in Systems with Probabilistic DF Relay

BAI Huiqing JIN Liang HUANG Kaizhi YI Ming
(*China National Digital Switching System Engineering and Technological R & D Center*, *Zhengzhou* 450002, *China*)

Abstract: A relay aided secrecy polar coding method is proposed for the communication systems where the relay uses Decode-and-Forward (DF) in probability. It ensures the transmission reliability and improves the secrecy rate. First, the transmitter encodes the secrecy bits in two layers: the first layer is designed over the virtual Binary Erasure Channel (BEC) that generated by the probabilistic DF relay, and the second layer is designed over the real transmission channels. After receiving the codeword, relay decodes and extracts the frozen bits which the legitimate user can not obtain directly in probability, and re-encodes them by classical secrecy polar coding. Finally, the receiver decodes the received codewords from the relay and the transmitter in turn. The theory and simulation results verify that the legitimate user is able to decode reliable, while the eavesdropper can not obtain any information about the secrecy bits. Moreover, the secrecy rate increases as the code length and the relay forwarding probability increase, and it outperforms the classical secrecy polar coding method.

Key words: Polar codes; Physical layer security; Relay; Probabilistic Decode-and-Forward (DF)

1 引言

物理层安全技术能够利用无线信道天然的差异性、互易性，使私密信息只在合法通信双方的专属信道中匹配传输，以此保证信息安全，具有重要的现实意义和广阔的应用前景[1,2]。安全编码作为一种重要的物理层安全技术，利用母码的信道耦合特性和纠错能力同时确保合法用户对信息的安全与可靠接收[3,4]。陪集编码[5]、嵌套编码[6]、格码[7]等随机编码方法已被理论证明能够逼近安全容量，然而，实用型安全编码设计仍是一个开放性课题。2009年Arikan[8]提出了信道极化理论，并依据该理论在二进制输入离散无记忆(Binary-input Discrete Memoryless Channel, B-DMC)信道上给出了极化码的编译码方法。信道极化使极化码与传输信道特性强耦合，成为一种极具潜力的安全编码方法。理

收稿日期：2017-12-04；改回日期：2018-04-26；网络出版：2018-07-12
*通信作者： 金梁 liangjin@263.net
基金项目：国家自然科学基金创新群体项目(61521003)，国家863计划(2015AA01A708)，国家青年科学基金(61501516)
Foundation Items: The Science Fund for Creative Research Groups of the National Natural Science Foundation of China (61521003), The National 863 Program of China (2015AA01A708), The National Natural Science Foundation for Young Scientists of China (61501516)

论上已经证明了极化编码能够在不同条件下分别达到弱安全[9]与强安全[10]。然而，在实际应用中由于编码码长有限，信道极化不彻底，仍存在大量极化逻辑信道的容量介于“0”和“1”之间[11]，极化码的安全传输速率亟需提高。

协作转发是一种常用于提高安全传输速率的有效方法。通过利用中继对全部或部分信息的转发，提高合法用户的信号接收质量，增大合法用户与窃听者之间的接收质量差异，进而提高系统整体的安全传输速率。文献[12]发现极化编码的嵌套结构使之天然适用于中继译码转发的场景。Duo等人[13]将中继译码获得的有效信息进行适当重组并编码转发，使合法用户额外获得了一部分私密信息，后续又将该方法扩展到多中继网络模型中[14]。Karas等人[15]在中继处加入了错误检测装置，增加了转发的灵活性。此外，文献[16]在半双工中继模型中，利用极化码的Plotkin结构使接收端对直传信息与转发信息进行联合译码，提高合法用户的接收性能。

上述研究均建立在中继节点完全配合合法双方通信的基础上。然而在一些实际的通信场景中，中继并非完全配合，即中继节点仅在传输中的部分时隙为合法双方提供译码转发服务。此时，若直接采用类似文献[15,16]的方法，合法用户将在中继不为其服务的时隙内完全无法可靠译码，导致安全可靠传输速率降为0。为了解决中继非完全配合场景下的信息安全传输问题，本文将上述非完全配合的中继建模为依概率译码转发，即中继节点只能以概率p为合法收发双方提供译码转发服务，并在此基础上提出了一种概率中继辅助的安全极化编码方法。该方法利用分层极化码的思想，在发端将中继的概率转发行为等效为一组参数一致的虚拟二进制删除信道(Binary Erasure Channel, BEC)，将私密信息分别在虚拟BEC信道和实际传输信道上进行两层极化安全编码，完成时隙内和时隙间的信息校验。然后，中继依概率译码，并再次对合法用户无法收到的固定信息进行极化安全编码并转发。可靠性和安全性分析表明，合法用户能够利用部分时隙中继转发的信息实现可靠译码，并且所提方法可以达到弱安全条件。

2　问题的提出

2.1　安全极化码

极化码的提出源于Arikan的信道极化理论，N个完全相同的B-DMC信道W经过信道合并和信道分割后，可以转化为N个不同的极化逻辑信道$W_N^{(i)}, i=1,2,\cdots,N$。假设编码器输入信息为$\boldsymbol{u}_1^N=(u_1,u_2,\cdots,u_N)$，信道输入输出码字分别为$\boldsymbol{x}_1^N=(x_1,x_2,\cdots,x_N)$和$\boldsymbol{y}_1^N=(y_1,y_2,\cdots,y_N)$，则极化后的逻辑信道可以表示为

$$W_N^{(i)}(\boldsymbol{y}_1^N,\boldsymbol{u}_1^{i-1}|u_i)\triangleq\sum_{\boldsymbol{u}_{i+1}^N}\frac{1}{2^{N-1}}W_N(\boldsymbol{y}_1^N|\boldsymbol{u}_1^N)\tag{1}$$

其中，$W_N(\boldsymbol{y}_1^N|\boldsymbol{u}_1^N)=\prod_{i=1}^N W(y_i|x_i)$, $\boldsymbol{x}_1^N=\boldsymbol{u}_1^N\cdot\boldsymbol{G}$, $\boldsymbol{G}=\boldsymbol{B}_N\cdot\boldsymbol{F}^{\otimes n}$是极化码的生成矩阵[8]；码长$N=2^n, n>0$。

随着$N\to\infty$，$W_N^{(i)}$的对称容量将逐渐趋于“0”或“1”。令$\mathcal{A}$表示对称容量趋于“1”的极化信道索引组成的集合，$\mathcal{A}^c$为$\mathcal{A}$的补集。通常以巴氏参数$Z\left(W_N^{(i)}\right)$[8]代替对称容量作为划分$\mathcal{A}$的依据，即$\forall\beta<0.5$，

$$\mathcal{A}=\left\{i:Z\left(W_N^{(i)}\right)<2^{-N^\beta}/N\right\}\tag{2}$$

则$\{u_i\}_{i\in\mathcal{A}}$为信息比特，而$\{u_i\}_{i\in\mathcal{A}^c}$为已知固定比特，误码率$P_e\le\sum_{i\in\mathcal{A}}Z\left(W_N^{(i)}\right)\le 2^{-N^\beta}$。

定理 1　若$I(W)$为W的对称容量，$\mathcal{A}=\left\{i:Z\left(W_N^{(i)}\right)<2^{-N^\beta}/N\right\}$，则对$\forall\beta<0.5$，有$\lim\limits_{N\to\infty}|\mathcal{A}|/N=I(W)$。

定理 2　若W^*是W的退化信道，则$W^{*(i)}_N$是$W_N^{(i)}$的退化信道，$Z\left(W^{*(i)}_N\right)\ge Z\left(W_N^{(i)}\right)$, $\mathcal{A}^*\subset\mathcal{A}$。

假设窃听信道W^*是合法信道W的退化信道。安全极化编码就是利用定理2，在$\mathcal{A}\backslash\mathcal{A}^*$的位置传输私密信息，在$\mathcal{A}^*$的位置传输随机信息，在$\mathcal{A}^c$的位置传输固定信息，从而确保私密信息的安全与可靠。令$|\mathcal{A}|$表示集合$\mathcal{A}$的势，则安全传输速率可以表示为$R_S=|\mathcal{A}\backslash\mathcal{A}^*|/N$。

2.2　系统模型

本文中的概率转发中继-窃听信道模型如图1所示。发送者Alice(A)在中继(R)的辅助下向合法用户Bob(B)传递私密信息$\boldsymbol{S}$，并确保该信息不能被窃听者Eve(E)获得，并假设中继只能以概率p译码转发某一时隙的接收码字。首先，Alice对私密信息$\boldsymbol{S}$进行安全编码，并将编码后的码字$\boldsymbol{X}$分为T个时隙分别广播发送，每时隙内的码长为N，Bob，

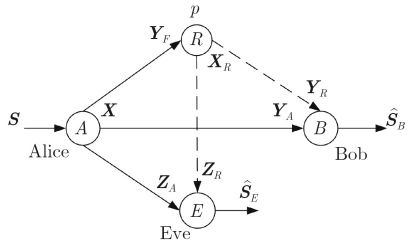

图 1 概率转发中继-窃听信道模型

Eve和中继节点在分别收到码字$\boldsymbol{Y}_A$, $\boldsymbol{Z}_A$和$\boldsymbol{Y}_F$。然后，中继以概率p对$\boldsymbol{Y}_F$中的部分时隙进行译码，并根据系统参数选取部分信息重新编码为$\boldsymbol{X}_R$并转发，Bob和Eve分别收到转发码字$\boldsymbol{Y}_R$, $\boldsymbol{Z}_R$。最后，Bob根据接收的码字$\boldsymbol{Y}_A$, $\boldsymbol{Y}_R$进行联合译码得到私密信息$\hat{\boldsymbol{S}}_B$；Eve则根据接收的码字$\boldsymbol{Z}_A$, $\boldsymbol{Z}_R$进行联合译码得到$\hat{\boldsymbol{S}}_E$。假设所有传输信道均为加性高斯白噪声(Additive White Gaussian Noise, AWGN)信道，W_{ab}表示节点$a\in\{A,R\}$与节点$b\in\{B,E,R\}$之间的信道，各信道之间满足信道退化条件$W_{\mathrm{AE}}\preceq W_{\mathrm{AB}}\preceq W_{\mathrm{AR}}$, $W_{\mathrm{RE}}\preceq W_{\mathrm{RB}}$，其中符号$\preceq$表示前者是后者的退化信道。根据定理2可知，此时$\mathcal{A}_{\mathrm{AE}}\subset\mathcal{A}_{\mathrm{AB}}\subset\mathcal{A}_{\mathrm{AR}}$, $\mathcal{A}_{\mathrm{RE}}\subset\mathcal{A}_{\mathrm{RB}}$。

每一时隙内Alice的传输速率为$R_T=|\mathcal{A}_{\mathrm{AR}}|/N$。此时，中继能够对$\boldsymbol{Y}_F$可靠译码，而Bob由于缺少固定信息$\{u_i\}_{i\in\mathcal{A}_{\mathrm{AB}}^c\backslash\mathcal{A}_{\mathrm{AR}}^c}(i=1,2,\cdots,N)$而无法直接对$\boldsymbol{Y}_A$可靠译码。为了实现信息的安全与可靠传输，本文提出一种概率中继辅助的安全极化编码方法。

3 概率中继辅助的安全极化编码

本节将分层极化编码[17]应用到概率中继辅助场景，首先，将中继的概率转发行为等效为一组虚拟BEC信道，对部分私密信息进行第1层极化编码，完成不同时隙间的信息校验。然后将编码结果连同剩余私密信息进行实际AWGN传输信道下的极化编码(第2层编码)，完成同一时隙内的信息校验。利用这种“交叉”编码校验方式使Bob能够根据部分时隙中继转发的$\{u_i\}_{i\in\mathcal{A}_{\mathrm{AB}}^c\backslash\mathcal{A}_{\mathrm{AR}}^c}$恢复出其余时隙的固定信息，在确保Bob正确译码的同时，获取比一般安全极化编码更高的安全传输速率。

3.1 发送端

在发送端，Alice将私密信息$\boldsymbol{S}$分为$\boldsymbol{S}_1$和$\boldsymbol{S}_2$两部分，先后完成两层极化编码，如图2所示。首先对私密信息$\boldsymbol{S}_2$进行BEC信道下的极化编码，实现时隙间的信息校验；然后在此基础上对私密信息$\boldsymbol{S}_1$进行AWGN信道下的安全极化编码，使信息$\boldsymbol{S}_1$在合法信道上安全可靠传输。

步骤1 BEC信道下的极化编码。由于中继仅依概率对每时隙处于$\mathcal{A}_{\mathrm{AB}}^c\backslash\mathcal{A}_{\mathrm{AR}}^c$中的信息进行译码转发，可以将中继的转发行为等效为信息经过了一个虚拟BEC信道，将未被转发的信息看做删除比特。由于中继的转发概率为p，则该BEC信道的删除率为$(1-p)$。记$\mathcal{A}_{1-p}$为每次编码私密信息位组成的集合，则$\mathcal{A}_{1-p}^c$传输固定信息“0”。这样，Alice首先在发送端进行$|\mathcal{A}_{\mathrm{AB}}^c\backslash\mathcal{A}_{\mathrm{AR}}^c|$次码长为$T$的极化编码，$\boldsymbol{S}_2$的维度为$|\mathcal{A}_{\mathrm{AB}}^c\backslash\mathcal{A}_{\mathrm{AR}}^c|\times|\mathcal{A}_{1-p}|$, $\boldsymbol{S}_2$的每行信息分别置于$j\in\mathcal{A}_{\mathrm{AB}}^c\backslash\mathcal{A}_{\mathrm{AR}}^c$的相应位置，$j=1,2,\cdots,T$。记$[\boldsymbol{S}_2|\boldsymbol{0}]$为按照极化信道质量排序后的待编码码字，对$[\boldsymbol{S}_2|\boldsymbol{0}]$的每一行分别进行码长为$T$的极化编码，则第1层编码表示为

$$\boldsymbol{C}=[\boldsymbol{S}_2|\boldsymbol{0}]\cdot\boldsymbol{G}_T \tag{3}$$

其中，$\boldsymbol{G}_T$为$T\times T$的生成矩阵；$\boldsymbol{C}$为编码器输出。

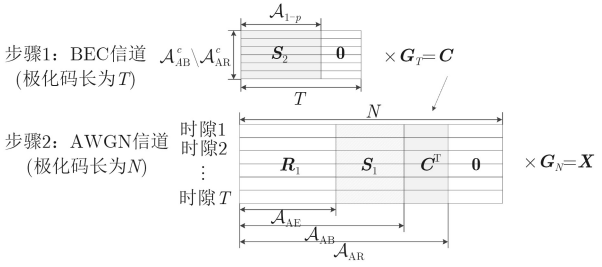

图 2 发送端——多层安全极化编码示意图

步骤2 AWGN信道下的安全极化编码。在每个时隙内，采用码长为N的安全极化编码，其中私密信息$\boldsymbol{S}_1$、随机信息$\boldsymbol{R}_1$以及第1层编码输出$\boldsymbol{C}^{\mathrm{T}}$分别对应于传输位置$i\in\mathcal{A}_{\mathrm{AB}}\backslash\mathcal{A}_{\mathrm{AE}}$, $i\in\mathcal{A}_{\mathrm{AE}}$和$i\in\mathcal{A}_{\mathrm{AB}}^c\backslash\mathcal{A}_{\mathrm{AR}}^c$，其余位置为固定信息“0”。$\boldsymbol{S}_1$的维度为$T\times|\mathcal{A}_{\mathrm{AE}}^c\backslash\mathcal{A}_{\mathrm{AB}}^c|$。记$\left[\boldsymbol{R}_1|\boldsymbol{S}_1|\boldsymbol{C}^{\mathrm{T}}|\boldsymbol{0}\right]$为按照极化信道质量排序后的待编码码字，对$\left[\boldsymbol{R}_1|\boldsymbol{S}_1|\boldsymbol{C}^{\mathrm{T}}|\boldsymbol{0}\right]$的每一行分别进行码长为$N$的极化编码，则第2层编码表示为

$$\boldsymbol{X}=\left[\boldsymbol{R}_1|\boldsymbol{S}_1|\boldsymbol{C}^{\mathrm{T}}|\boldsymbol{0}\right]\cdot\boldsymbol{G}_N \tag{4}$$

其中，$\boldsymbol{G}_N$为$N\times N$的生成矩阵；$\boldsymbol{X}$为编码器输出。最终，Alice分别将$\boldsymbol{X}$行向量$\boldsymbol{x}_{(t)}$在时隙t广播出去，$t=1,2,\cdots,T$。

3.2 中继

令$\mathcal{T}_1$表示所有中继转发时隙所构成的集合，则$|\mathcal{T}_1|=T\cdot p$。假设中继在t时隙对收到的码字进行连续抵消(Successive Cancelation, SC)译码，并从译码结果中提取出索引$i\in\mathcal{A}_{\mathrm{AB}}^c\backslash\mathcal{A}_{\mathrm{AR}}^c$的部分$\hat{\boldsymbol{c}}_{(t)}$再次进行编码转发，并记所有的$\hat{\boldsymbol{c}}_{(t)}(t\in\mathcal{T}_1)$组成的待编码转发信息矩阵为$\boldsymbol{C}_{\mathrm{part}}$，其中$\hat{\boldsymbol{c}}_{(t)}$对应于$\boldsymbol{C}_{\mathrm{part}}$的每一行，如图3所示。为使$\boldsymbol{C}_{\mathrm{part}}$无法被窃听者获得，中继分别将$\boldsymbol{C}_{\mathrm{part}}$和随机信息$\boldsymbol{R}_2$置于$i\in\mathcal{A}_{\mathrm{RE}}^c\backslash\mathcal{A}_{\mathrm{RB}}^c$和$i\in\mathcal{A}_{\mathrm{RE}}$位置内，并在其余位置存放固定信息“0”，再次进行AWGN信道下安全极化编码，转发码率$R_F=|\mathcal{A}_{\mathrm{RB}}|/N$(为便于分析这里仍令码长为$N$，并假设$|\mathcal{A}_{\mathrm{AB}}^c\backslash\mathcal{A}_{\mathrm{AR}}^c|=|\mathcal{A}_{\mathrm{RE}}^c\backslash\mathcal{A}_{\mathrm{RB}}^c|$)。记$[\boldsymbol{R}_2|\boldsymbol{C}_{\mathrm{part}}|\boldsymbol{0}]$为按照极化信道质量排序后的待编码码字，对$[\boldsymbol{R}_2|\boldsymbol{C}_{\mathrm{part}}|\boldsymbol{0}]$的每一行分别进行码长为$N$的极化编码，则转发码字$\boldsymbol{X}_R$表示为

$$\boldsymbol{X}_R=[\boldsymbol{R}_2|\boldsymbol{C}_{\mathrm{part}}|\boldsymbol{0}]\cdot\boldsymbol{G}_N \tag{5}$$

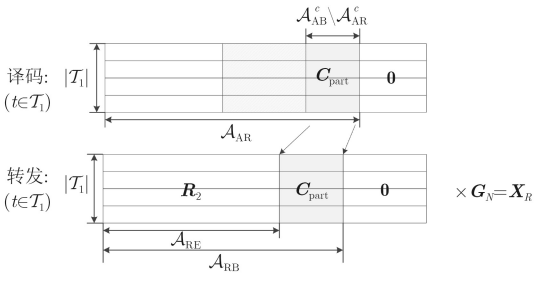

图 3 中继——译码转发示意图

3.3 接收端

假设接收端具有正交接收器，能够互不干扰地分别接收来自发送端和中继的码字。以合法用户Bob为例，接收到的Alice和中继发送码字分别为$\boldsymbol{Y}_A$和$\boldsymbol{Y}_R$，需依次进行3次译码，如图4所示。

步骤1　对AWGN信道下中继转发码字译码。分别对接收到的中继转发码字$\boldsymbol{Y}_R$的每一行进行SC译码，并提取出信息索引$j\in\mathcal{A}_{\text{RE}}^c\backslash\mathcal{A}_{\text{RB}}^c$位置上的信息，记为$\hat{\boldsymbol{C}}_{\text{part}}$，$\hat{\boldsymbol{C}}_{\text{part}}$是对$\boldsymbol{C}_{\text{part}}$的估计。

步骤2　BEC信道下译码私密信息$\boldsymbol{S}_2$及$\boldsymbol{C}$。将$\hat{\boldsymbol{C}}_{\text{part}}^{\text{T}}$作为未删除码字，$\boldsymbol{C}$中剩余中继未转发的比特作为删除信息，并将$\hat{\boldsymbol{C}}_{\text{part}}^{\text{T}}$的每一行元素置于$j\in\mathcal{T}_1$的位置，分别进行BEC信道下的SC译码。这样，接收端译码得到对私密信息$\boldsymbol{S}_2$的估计值$\hat{\boldsymbol{S}}_2$。对$\left[\hat{\boldsymbol{S}}_2|\mathbf{0}\right]$反向进行BEC信道下的极化编码，得到$\boldsymbol{C}$的估计值$\hat{\boldsymbol{C}}$。

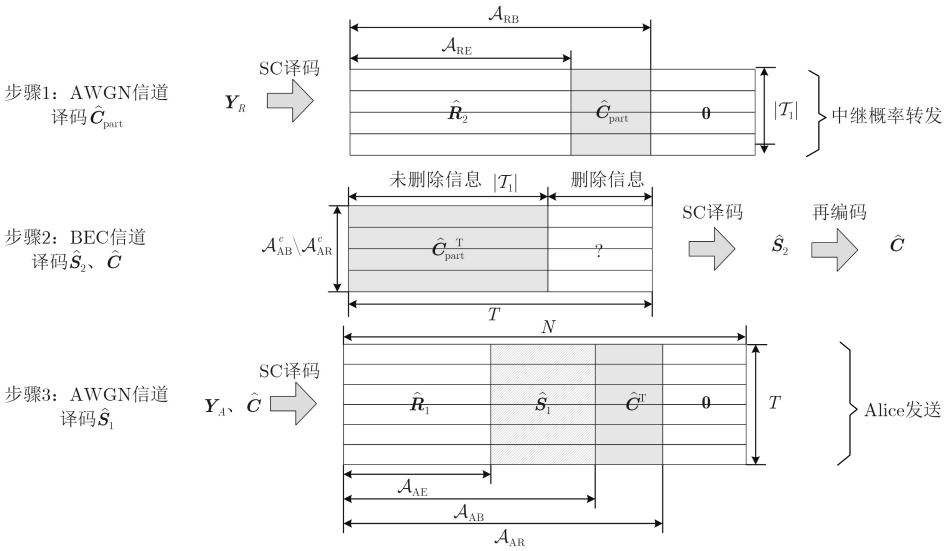

图 4 接收端——译码示意图

步骤3　对AWGN信道下Alice发送的码字译码。根据步骤2译码得到的$\hat{\boldsymbol{C}}$，接收端可以获得处于$i\in\mathcal{A}_{\text{AB}}^c$位置的所有固定信息$\left[\hat{\boldsymbol{C}}^{\text{T}}|\mathbf{0}\right]$，这样就能够对每一时隙Alice发送的码字进行SC译码，记对私密信息$\boldsymbol{S}_1$的译码估计值为$\hat{\boldsymbol{S}}_1$。

4　私密信息的安全可靠性分析

4.1 可靠性

令事件ε_2和ε_1分别表示Bob对来自Alice的第1层码字$[\boldsymbol{S}_2|\mathbf{0}]$和第2层码字$\left[\boldsymbol{R}_1|\boldsymbol{S}_1|\boldsymbol{C}^{\text{T}}|\mathbf{0}\right]$译码错误；$\varepsilon_{\text{AR}}$表示中继译码错误；$\varepsilon_{\text{RB}}$表示Bob对来自中继的码字译码错误。则错误率$\Pr(\varepsilon_2)$可表示为

$$\begin{aligned}\Pr(\varepsilon_2)&=\Pr(\varepsilon_2|\varepsilon_{\text{AR}})\Pr(\varepsilon_{\text{AR}})+\Pr(\varepsilon_2|\varepsilon_{\text{AR}}^c)\Pr(\varepsilon_{\text{AR}}^c)\\&\le\Pr(\varepsilon_{\text{AR}})+\Pr(\varepsilon_2|\varepsilon_{\text{AR}}^c)\end{aligned}\tag{6}$$

由于$R_T=|\mathcal{A}_{\text{AR}}|/N$，所以中继的译码错误概率$P_e^{\text{AR}}\le\sum\limits_{i\in\mathcal{A}_{\text{AR}}}Z\left(W_N^{(i)}\right)\le N\cdot\dfrac{1}{N}2^{-N^\beta}=2^{-N^\beta}$，中继共译码了$|\mathcal{T}_1|=T\cdot p$个时隙，故式(6)的第1项满足$\Pr(\varepsilon_{\text{AR}})\le|\mathcal{T}_1|\cdot P_e^{\text{AR}}\le Tp\cdot2^{-N^\beta}$。式(6)的第2项可以表示为

$$\begin{aligned}\Pr(\varepsilon_2|\varepsilon_{\text{AR}}^c)&=\Pr(\varepsilon_2|\varepsilon_{\text{AR}}^c,\varepsilon_{\text{RB}})\Pr(\varepsilon_{\text{RB}}|\varepsilon_{\text{AR}}^c)\\&\quad+\Pr(\varepsilon_2|\varepsilon_{\text{AR}}^c,\varepsilon_{\text{RB}}^c)\Pr(\varepsilon_{\text{RB}}^c|\varepsilon_{\text{AR}}^c)\\&=\Pr(\varepsilon_2|\varepsilon_{\text{AR}}^c,\varepsilon_{\text{RB}})\Pr(\varepsilon_{\text{RB}})\\&\quad+\Pr(\varepsilon_2|\varepsilon_{\text{AR}}^c,\varepsilon_{\text{RB}}^c)\Pr(\varepsilon_{\text{RB}}^c)\\&\le\Pr(\varepsilon_{\text{RB}})+\Pr(\varepsilon_2|\varepsilon_{\text{AR}}^c,\varepsilon_{\text{RB}}^c)\end{aligned}\tag{7}$$

由于$R_F=|\mathcal{A}_{\text{RB}}|/N$，所以在译码步骤1中Bob的译码错误率$P_e^{\text{RB}}\le\sum_{i\in\mathcal{A}_{\text{RE}}^c\backslash\mathcal{A}_{\text{RB}}^c}Z\left(W_N^{(i)}\right)\le2^{-N^\beta}$，$t\in\mathcal{T}_1$。所以式(7)的第1项满足$\Pr(\varepsilon_{\text{RB}})\le|\mathcal{T}_1|\cdot P_e^{\text{RB}}\le Tp\cdot2^{-N^\beta}$。若中继节点及Bob在第1步译码中全部正确，则译码步骤2的错误率$P_e^{\text{BEC}}\le\sum_{i\in\mathcal{A}_{1-p}}Z\left(W_T^{(i)}\right)\le2^{-T^\beta}$。已知步骤2共进行了$|\mathcal{A}_{\text{AB}}^c\backslash\mathcal{A}_{\text{AR}}^c|$次BEC信道下的译码，故式(7)的第2项

满足 $\Pr(\varepsilon_2|\varepsilon_{\mathrm{AR}}^c,\varepsilon_{\mathrm{RB}}^c)\le|\mathcal{A}_{\mathrm{AB}}^c\backslash\mathcal{A}_{\mathrm{AR}}^c|\cdot2^{-T^\beta}$。综合之，事件$\varepsilon_2$的错误率式(6)可以表示为

$$\Pr(\varepsilon_2)\le 2Tp\cdot2^{-N^\beta}+|\mathcal{A}_{\mathrm{AB}}^c\backslash\mathcal{A}_{\mathrm{AR}}^c|\cdot2^{-T^\beta} \tag{8}$$

同理，事件ε_1的错误率$\Pr(\varepsilon_1)$可表示为

$$\begin{aligned}\Pr(\varepsilon_1)&=\Pr(\varepsilon_1|\varepsilon_2)\Pr(\varepsilon_2)+\Pr(\varepsilon_1|\varepsilon_2^c)\Pr(\varepsilon_2^c)\\&\le\Pr(\varepsilon_2)+\Pr(\varepsilon_1|\varepsilon_2^c)\end{aligned} \tag{9}$$

若在译码步骤2中Bob正确译码，则Bob获得了所有$i\in\mathcal{A}_{\mathrm{AB}}^c$的固定信息，那么在译码步骤3中Bob对每一时隙Alice发送码字的译码错误率$P_e^{\mathrm{AWGN}}\le\sum_{i\in\mathcal{A}_{\mathrm{AE}}^c\backslash\mathcal{A}_{\mathrm{AB}}^c}Z\left(W_N^{(i)}\right)\le2^{-N^\beta}$。已知共有$T$个时隙，故式(9)的第2项满足$\Pr(\varepsilon_1|\varepsilon_2^c)\le T\cdot2^{-N^\beta}$。将式(8)代入式(9)得

$$\Pr(\varepsilon_1)\le(2p+1)\,T\cdot2^{-N^\beta}+|\mathcal{A}_{\mathrm{AB}}^c\backslash\mathcal{A}_{\mathrm{AR}}^c|\cdot2^{-T^\beta} \tag{10}$$

根据文献[17]，在$N,T\to\infty$时，式(8)和式(10)分别满足$\lim\limits_{N,T\to\infty}\Pr(\varepsilon_2)=0$，$\lim\limits_{N,T\to\infty}\Pr(\varepsilon_1)=0$。在Bob端误码率$\Pr\left(\hat{\boldsymbol{S}}_2\ne\boldsymbol{S}_2\right)=\Pr(\varepsilon_2)$，$\Pr\left(\hat{\boldsymbol{S}}_1\ne\boldsymbol{S}_1\right)\le\Pr(\varepsilon_1)$，所以Bob能够对私密信息可靠译码。

4.2 安全性

在第3节所提方法下，安全传输速率可以表示为$\boldsymbol{S}_1$与$\boldsymbol{S}_2$的信息比特总和与编码码长NT之比，即

$$R_S=\frac{1}{NT}(|\mathcal{A}_{\mathrm{AE}}^c\backslash\mathcal{A}_{\mathrm{AB}}^c|\times T+|\mathcal{A}_{1-p}|\times|\mathcal{A}_{\mathrm{AB}}^c\backslash\mathcal{A}_{\mathrm{AR}}^c|) \tag{11}$$

假设Eve分别收到来自Alice和中继的码字$\boldsymbol{Z}_A$和$\boldsymbol{Z}_R$，则互信息

$$\begin{aligned}I(\boldsymbol{S};\boldsymbol{Z}_A,\boldsymbol{Z}_R)&=I(\boldsymbol{S}_1;\boldsymbol{Z}_A,\boldsymbol{Z}_R)+I(\boldsymbol{S}_2;\boldsymbol{Z}_A,\boldsymbol{Z}_R|\boldsymbol{S}_1)\\&\overset{a}{=}I(\boldsymbol{S}_1;\boldsymbol{Z}_A,\boldsymbol{Z}_R)+I(\boldsymbol{S}_2;\boldsymbol{Z}_A,\boldsymbol{Z}_R)\end{aligned} \tag{12}$$

由于$\boldsymbol{S}_1$与$\boldsymbol{S}_2$相互独立，且已知$\boldsymbol{S}_1$不会对Eve译码$\boldsymbol{S}_2$有任何帮助，因此$I(\boldsymbol{S}_2;\boldsymbol{Z}_A,\boldsymbol{Z}_R|\boldsymbol{S}_1)=I(\boldsymbol{S}_2;\boldsymbol{Z}_A,\boldsymbol{Z}_R)$，等式a成立。下面对式(12)中的两项$I(\boldsymbol{S}_2;\boldsymbol{Z}_A,\boldsymbol{Z}_R)$与$I(\boldsymbol{S}_1;\boldsymbol{Z}_A,\boldsymbol{Z}_R)$分别进行分析。

4.2.1 私密信息$\boldsymbol{S}_2$的安全性 私密信息$\boldsymbol{S}_2$的安全性可以用互信息$I(\boldsymbol{S}_2;\boldsymbol{Z}_A,\boldsymbol{Z}_R)$表示，即

$$\begin{aligned}I(\boldsymbol{S}_2;\boldsymbol{Z}_A,\boldsymbol{Z}_R)&\le I(\boldsymbol{C};\boldsymbol{Z}_A,\boldsymbol{Z}_R)\\&=I(\boldsymbol{C};\boldsymbol{Z}_R)+I(\boldsymbol{C};\boldsymbol{Z}_A|\boldsymbol{Z}_R)\\&\le I(\boldsymbol{C}_{\mathrm{part}};\boldsymbol{Z}_R)+I(\boldsymbol{C};\boldsymbol{Z}_A)\end{aligned} \tag{13}$$

本文中$\boldsymbol{S}_2$首先被编码为码字$\boldsymbol{C}$，经由Alice和中继分别处理后Eve接收到$\boldsymbol{Z}_A$和$\boldsymbol{Z}_R$，由信息处理不等式，有$I(\boldsymbol{S}_2;\boldsymbol{Z}_A,\boldsymbol{Z}_R)\le I(\boldsymbol{C};\boldsymbol{Z}_A,\boldsymbol{Z}_R)$，$I(\boldsymbol{C};\boldsymbol{Z}_R)\le I(\boldsymbol{C}_{\mathrm{part}};\boldsymbol{Z}_R)$。又因为$\boldsymbol{Z}_A$，$\boldsymbol{Z}_R$中共同含有关于$\boldsymbol{C}$的信息量，所以$I(\boldsymbol{C};\boldsymbol{Z}_A|\boldsymbol{Z}_R)\le I(\boldsymbol{C};\boldsymbol{Z}_A)$，故式(13)成立。式(13)中的第1项：

$$\begin{aligned}I(\boldsymbol{C}_{\mathrm{part}};\boldsymbol{Z}_R)&=I(\boldsymbol{C}_{\mathrm{part}},\boldsymbol{R}_2;\boldsymbol{Z}_R)-H(\boldsymbol{R}_2|\boldsymbol{C}_{\mathrm{part}})\\&\quad+H(\boldsymbol{R}_2|\boldsymbol{Z}_R,\boldsymbol{C}_{\mathrm{part}})\le Tp\cdot N\cdot I(W_{\mathrm{RE}})\\&\quad-Tp\cdot|\mathcal{A}_{\mathrm{RE}}|+H(\boldsymbol{R}_2|\boldsymbol{Z}_R,\boldsymbol{C}_{\mathrm{part}})\end{aligned} \tag{14}$$

由定理1可知，$I(\boldsymbol{C}_{\mathrm{part}},\boldsymbol{R}_2;\boldsymbol{Z}_R)\le Tp\cdot N\cdot I(W_{\mathrm{RE}})$，且当$N\to\infty$时$I(W_{\mathrm{RE}})-|\mathcal{A}_{\mathrm{RE}}|/N\to0$，故式(14)成立。当Eve已知$\boldsymbol{Z}_R$和$\boldsymbol{C}_{\mathrm{part}}$时，对$\boldsymbol{R}_2$的译码错误率$P_{e1}\le\Pr(\varepsilon_{\mathrm{RB}})\le Tp\cdot2^{-N^\beta}$。由范诺不等式$H(\boldsymbol{R}_2|\boldsymbol{Z}_R,\boldsymbol{C}_{\mathrm{part}})\le H(P_{e1})+P_{e1}\cdot Tp|\mathcal{A}_{\mathrm{RE}}|$可知，随着$N,T\to\infty$，有$P_{e1}\to0$[17]，$H(\boldsymbol{R}_2|\boldsymbol{Z}_R,\boldsymbol{C}_{\mathrm{part}})\to0$。因此，

$$\lim_{N,T\to\infty}\frac{1}{NT}I(\boldsymbol{C}_{\mathrm{part}};\boldsymbol{Z}_R)=0 \tag{15}$$

式(13)中的第2项：

$$\begin{aligned}I(\boldsymbol{C};\boldsymbol{Z}_A)&=I(\boldsymbol{C},\boldsymbol{R}_1,\boldsymbol{S}_1;\boldsymbol{Z}_A)-I(\boldsymbol{R}_1,\boldsymbol{S}_1;\boldsymbol{Z}_A|\boldsymbol{C})\\&=I(\boldsymbol{C},\boldsymbol{R}_1,\boldsymbol{S}_1;\boldsymbol{Z}_A)-H(\boldsymbol{R}_1|\boldsymbol{S}_1,\boldsymbol{C})\\&\quad-H(\boldsymbol{S}_1|\boldsymbol{C})+H(\boldsymbol{S}_1|\boldsymbol{Z}_A,\boldsymbol{C},\boldsymbol{R}_1)\\&\quad+H(\boldsymbol{R}_1|\boldsymbol{Z}_A,\boldsymbol{C},\boldsymbol{S}_1)\\&\le T\cdot N\cdot I(W_{\mathrm{AE}})-T\cdot|\mathcal{A}_{\mathrm{AE}}|\\&\quad+H(\boldsymbol{R}_1|\boldsymbol{Z}_A,\boldsymbol{C},\boldsymbol{S}_1)\end{aligned} \tag{16}$$

由定理1可知，$I(\boldsymbol{C},\boldsymbol{R}_1,\boldsymbol{S}_1;\boldsymbol{Z}_A)\le T\cdot N\cdot I(W_{\mathrm{AE}})$，且当$N\to\infty$时$I(W_{\mathrm{AE}})-|\mathcal{A}_{\mathrm{AE}}|/N\to0$。由于Eve在已知$\boldsymbol{Z}_A$，$\boldsymbol{C}$和$\boldsymbol{R}_1$时无法获得关于$\boldsymbol{S}_1$的信息量，所以$H(\boldsymbol{S}_1|\boldsymbol{Z}_A,\boldsymbol{C},\boldsymbol{R}_1)=H(\boldsymbol{S}_1|\boldsymbol{C})$，故式(16)成立。当Eve已知$\boldsymbol{Z}_A$，$\boldsymbol{C}$和$\boldsymbol{S}_1$时，对$\boldsymbol{R}_1$的译码错误率$P_{e2}\le T\cdot2^{-N^\beta}$。由范诺不等式$H(\boldsymbol{R}_1|\boldsymbol{Z}_A,\boldsymbol{C},\boldsymbol{S}_1)\le H(P_{e2})+P_{e2}\cdot Tp|\mathcal{A}_{\mathrm{AE}}|$可知，随着$N,T\to\infty$，有$P_{e2}\to0$，$H(\boldsymbol{R}_1|\boldsymbol{Z}_A,\boldsymbol{C},\boldsymbol{S}_1)\to0$。因此，

$$\lim_{N,T\to\infty}\frac{1}{NT}I(\boldsymbol{C};\boldsymbol{Z}_A)=0 \tag{17}$$

将式(15)，式(17)代入式(13)，则

$$\lim_{N,T\to\infty}\frac{1}{NT}I(\boldsymbol{S}_2;\boldsymbol{Z}_A,\boldsymbol{Z}_R)=0 \tag{18}$$

即，私密信息$\boldsymbol{S}_2$满足弱安全条件。

4.2.2 私密信息$\boldsymbol{S}_1$的安全性 私密信息$\boldsymbol{S}_1$的安全性可以用互信息$I(\boldsymbol{S}_1;\boldsymbol{Z}_A,\boldsymbol{Z}_R)$表示，即

$$\begin{aligned}I(\boldsymbol{S}_1;\boldsymbol{Z}_A,\boldsymbol{Z}_R)&\le I(\boldsymbol{S}_1;\boldsymbol{Z}_A,\boldsymbol{C})\\&=I(\boldsymbol{S}_1,\boldsymbol{R}_1;\boldsymbol{Z}_A,\boldsymbol{C})-H(\boldsymbol{R}_1|\boldsymbol{S}_1)\\&\quad+H(\boldsymbol{R}_1|\boldsymbol{S}_1,\boldsymbol{Z}_A,\boldsymbol{C})\\&\le T\cdot N\cdot I(W_{\mathrm{AE}})-T\cdot|\mathcal{A}_{\mathrm{AE}}|\\&\quad+H(\boldsymbol{R}_1|\boldsymbol{S}_1,\boldsymbol{Z}_A,\boldsymbol{C})\end{aligned} \tag{19}$$

本文中Eve的接收码字$\boldsymbol{Z}_R$来自于$\boldsymbol{C}$，$\boldsymbol{Z}_A$来自于私密信息$\boldsymbol{S}_1$与$\boldsymbol{C}$，因而由信息处理不等式，有$I(\boldsymbol{S}_1;\boldsymbol{Z}_A,\boldsymbol{Z}_R)\le I(\boldsymbol{S}_1;\boldsymbol{Z}_A,\boldsymbol{C})$。此外，由定理1可知，$I(\boldsymbol{S}_1,\boldsymbol{R}_1;\boldsymbol{Z}_A,\boldsymbol{C})\le T\cdot N\cdot I(W_{\mathrm{AE}})$，且当$N\to\infty$

时$I(W_{\mathrm{AE}})-|\mathcal{A}_{\mathrm{AE}}|/N\to 0$，故式(19)成立。前面已证当$N, T\to\infty$时，$H(\boldsymbol{R}_1|\boldsymbol{Z}_A,\boldsymbol{C},\boldsymbol{S}_1)\to 0$。因此，

$$\lim_{N,T\to\infty}\frac{1}{NT}I(\boldsymbol{S}_1;\boldsymbol{Z}_A,\boldsymbol{Z}_R)=0 \tag{20}$$

即，私密信息私密信息$\boldsymbol{S}_1$满足弱安全条件。

式(18)和式(20)表明，本文方法下的私密信息$\boldsymbol{S}_1$, $\boldsymbol{S}_2$均满足弱安全条件，将其代入式(12)得

$$\lim_{N,T\to\infty}\frac{1}{NT}I(\boldsymbol{S};\boldsymbol{Z}_A,\boldsymbol{Z}_R)=0 \tag{21}$$

即，本文方法满足弱安全条件。

5　性能仿真与分析

为验证所提方法的有效性，采用蒙特卡洛方法对安全传输速率及私密信息的错误率分别进行仿真。假设$N=1024$，巴氏参数门限$2^{-N^{\beta}}/N=10^{-3}$。为满足条件$W_{\mathrm{AE}}\preceq W_{\mathrm{AB}}\preceq W_{\mathrm{AR}}$, $W_{\mathrm{RE}}\preceq W_{\mathrm{RB}}$，不妨令信道$W_{\mathrm{AE}}$, W_{AB}, W_{AR}的信噪比分别为1 dB, 5 dB, 8 dB，信道W_{RE}, W_{RB}的信噪比分别为5 dB, 8 dB。

图5仿真了总时隙数T变化时，不同转发概率p下本文方法的安全传输速率。可以看到，安全传输速率曲线随着T和p的增大而增大。这是由于，p增大导致了编码过程中的虚拟BEC信道容量提升，$|\mathcal{A}_{1-p}|$增大，因此$\boldsymbol{S}_2$的比特数增加；在p相同时，T增大则码长NT的增大，容量介于“0”和“1”之间的未完全极化的逻辑信道减少，安全传输速率的取值向安全容量逼近。而作为对比文献[13]的方法中，由于Bob在缺少中继转发信息时无法正确译码当前时隙码字，所以当中继转发概率下降时，安全传输速率急剧下降。

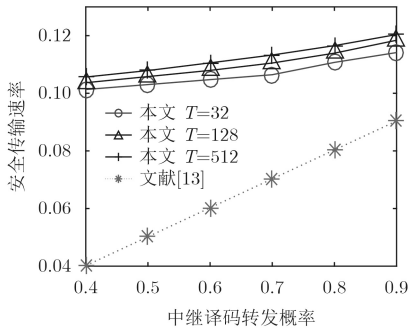

图 5 不同中继译码转发概率下的安全传输速率($N=1024$)

图6仿真了N变化时，不同转发概率p下本文方法的安全传输速率。可以看到，本文方法下的安全传输速率曲线随随着N与p的增大而增大。这是由于，N增大使编码过程中安全传输速率的取值向安全容量逼近，$\boldsymbol{S}_1$的比特数增加；p增大使虚拟BEC信道容量提升，$\boldsymbol{S}_2$的比特数增加。

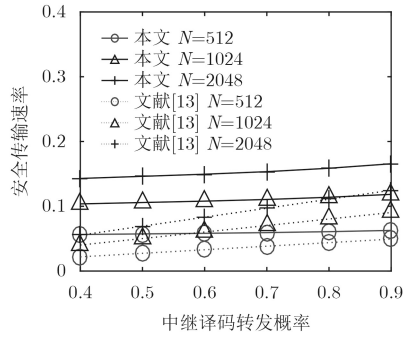

图 6 不同中继译码转发概率下的安全传输速率(T=128)

图7仿真了中继的译码转发概率p取不同值时，本文方法的私密信息的平均误比特率(Bit Error Rate, BER)，仿真条件与图6相同。可以看到，无论T和p取何值，Bob的BER始终保持在10^{-3}左右，而Eve的BER均为0.5。仿真再次说明了，本文方法能同时确保私密信息传输的安全性与可靠性。

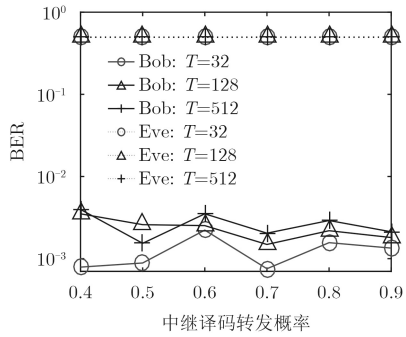

图 7 不同中继译码转发概率下的私密信息误比特率

6　结论

本文研究了中继概率译码转发系统中信息的安全可靠传输，提出了一种概率中继辅助的安全极化编码方法，在发送端采用分层极化编码，分别实现时隙内和时隙间的信息校验，使合法用户能够利用有限的辅助信息安全可靠地译码全部私密信息。理论分析证明，当码长$NT\to\infty$时，合法用户对私密信息的译码错误率趋于0，且窃听者获得的私密信息平均信息量趋于0，即私密信息可靠传输并满足弱安全条件。同时仿真表明，该方法下的安全传输速率始终好于一般的安全极化编码方法。

参 考 文 献

[1] ZOU Yulong, ZHU Jia, WANG Xinbin, *et al*. A survey on wireless security: Technical challenges, recent advances, and future trends[J]. *Proceedings of the IEEE*, 2016, 104(9): 1727–1765. doi: 10.1109/JPROC.2016.2558521.

[2] XIAO Shuaifang, GUO Yunfei, HUANG Kaizhi, *et al*. High-rate secret key generation aided by multiple relays for Internet of things[J]. *Electronics Letters*, 2017, 53(17):

1198–1200. doi: 10.1049/el.2017.2346.

[3] ZHANG Yingxian, YANG Zhen, LIU Aijun, *et al*. Secure transmission over the wiretap channel using polar codes and artificial noise[J]. *IET Communications*, 2017, 11(3): 377–384. doi: 10.1049/iet-com.2016.0429.

[4] 白慧卿, 金梁, 肖帅芳, 等. 多天线系统中面向物理层安全的极化编码方法[J]. 电子与信息学报, 2017, 39(11): 2587–25931. doi: 10.11999/JEIT170068.
BAI Huiqing, JIN Liang, XIAO Shuaifang, *et al*. Polar codes for physical layer security in multi-antenna systems[J]. *Journal of Electronics & Information Technology*, 2017, 39(11): 2587–25931. doi: 10.11999/JEIT170068.

[5] OZAROW L H and WYNER A D. Wire-tap channel II[J]. *AT&T Bell System Technical Journal*, 1984, 63(10): 2135–2137.

[6] CASSITO Y and BANDIC Z. Low complexity wiretap codes with security and error-correction guarantees [C]. IEEE Information Theory Workshop, Dublin, Ireland, 2010: 1–5.

[7] BELFIORE J C and OGGIER F. Lattice codes design for the Rayleigh fading wire-tap channel [C]. IEEE International Conference on Communications Workshops, Kyoto, Japan, 2011: 1–5.

[8] 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.

[9] 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.

[10] SASOGLU E and VARDY A. A new polar coding scheme for strong security on wiretap channels[C]. IEEE Internationnal Symposium on Information Theory Proceedings (ISIT), Istanbul, Turkey, 2013: 1117–1121.

[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] SERRANO R B, THOBABEN R, ANDERSSON M, *et al*. Polar codes for cooperative relaying[J]. *IEEE Transactions on Communications*, 2012, 60(11): 3263–3273. doi: 10.1109/TCOMM.2012.081412.110266.

[13] DUO Bin, WANG Peng, LI Yonghui, *et al*. Secure transmission for relay-eavesdropper channels using polar coding [C]. IEEE International Conference on Communications, Sydney, Australia, 2014: 2197–2202.

[14] DUO Bin, ZHONG Xiaoling, and GUO Yong. Practical polar code construction for degraded multiple-relay networks[J]. *China Communications*, 2017, 14(4): 127–139. doi: 10.1109/CC.2017.7927571.

[15] KARAS D S, PAPPI K N, and KARAGIANNIDIS G K. Smart decode-and-forward relaying with polar codes[J]. *IEEE Wireless Communications Letters*, 2014, 3(1): 62–65. doi: 10.1109/WCL2013.111213.130639.

[16] SOLIMAN T, YANG F, EJAZ S, *et al*. Decode and forward polar coding scheme for receive diversity: A relay partially perfect retransmission for half-duplex wireless relay channels[J]. *IET Communications*, 2017, 11(2): 185–191. doi: 10.1049/iet-com.2016.0915.

[17] SI Hongbo, KOYLUOGLU O O, and VISHWANATH S. Hierarchical polar coding for achieving secrecy over state-dependent wiretap channels without any instantaneous CSI[J]. *IEEE Transactions on Communications*, 2016, 64(9): 3609–3623. doi: 10.1109/TCOMM.2016.2592523.

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，博士生导师，研究方向为移动通信、无线物理层安全技术.

黄开枝：女，1973 年生，教授，博士生导师，研究方向为移动通信、无线物理层安全技术.

易 鸣：男，1986 年生，讲师，研究方向为无线物理层安全编码.