基于极化码的无协商密钥物理层安全传输方案

黄开枝 万 政* 楼洋明 肖帅芳 许晓明
(中国人民解放军战略支援部队信息工程大学 郑州 450001)

摘 要：针对现有的密钥生成方案需要在通信流程中增加额外的密钥协商协议，导致在5G等标准通信系统中应用受限的问题，该文提出一种基于极化码的无协商密钥物理层安全传输方案。首先基于信道特征提取未协商的物理层密钥，然后针对物理信道与密钥加密信道共同构成的等效信道设计极化码，最后利用未协商的物理层密钥对编码后的序列进行简单的模二加加密后传输。该方案通过针对性设计的极化码纠正密钥差异和噪声引起的比特错误，实现可靠的安全传输。仿真表明，该文基于等效信道设计的极化码在保证合法双方以最优的码率可靠传输的同时可以防止窃听者窃听，实现了安全与通信的一体化。

关键词：物理层安全；密钥生成；极化码；信息协商；安全与通信共生
中图分类号：TN918 **文献标识码**：A **文章编号**：1009-5896(2020)12-2946-07
DOI: 10.11999/JEIT190948

Physical Layer Secure Transmission Scheme with Joint Polar Codes and Non-reconciliation Secret Keys

HUANG Kaizhi WAN Zheng LOU Yangming XIAO Shuaifang XU Xiaoming
(*Information Engineering University*, *Zhengzhou* 450001, *China*)

Abstract: The existing key generation scheme requires additional key reconciliation protocol in a communication process, resulting in the limited application to the communication system, such as the Fifth-Generation mobile communication (5G). A physical layer secure transmission scheme with a joint polar code and non-reconciliation secret keys is proposed. Firstly, the non-reconciliation physical layer keys are extracted from the channel feature, and then the polar code is designed based on the equivalent channel, which is formed by the physical channel and the key encryption channel. Finally, the encoded sequence is simply modular plus encrypted and transmitted using the non-reconciliation physical layer key. Key differences and noise-induced bit errors are corrected through a targeted design of polarization codes to achieve reliable and secure transmission. The simulation shows that the polar code based on the equivalent channel can ensure the reliable transmission between two legitimate users at the optimal code rate.

Key words: Physical layer security; Secret key generation; Polar code; Information reconciliation; Communication security integration

1 引言

近年来，随着第5代移动通信(the Fifth Generation mobile communication, 5G)和物联网技术的发展，面向个人和行业的移动应用越来越普及，未来越来越多重要的私密信息将通过5G进行大规模传输。与目前的4G网络相比，5G网络可以通过提供高数据速率、超可靠低时延和海量机器类通信(Machine Type Communication, MTC)来满足日益增长的需求[1]。然而，机遇与挑战并存。无线通信固有的广播性质使得私密信息能被传输范围内的任何用户接收，攻击者可能发起各种被动攻击如窃听、流量分析和监控，或执行主动攻击如干扰、欺骗、修改和拒绝服务(Denial of Service, DoS)攻击。所以通信安全是未来无线网络设计的重中之重。为了保护数据传输，基于计算复杂度的公钥密码技术和相关加密协议广泛应用于现有的加密体制。然而，随着量子计算机的发展，攻击者的计算能力得到了极大的增强，基于计算上安全的加密技术在未来面临被破解的风险。此外，物联网中大量节点受

收稿日期：2019-11-01；改回日期：2020-09-08；网络出版：2020-09-14
*通信作者： 万政 wanzheng18@alumni.hust.edu.cn
基金项目：国家自然科学基金(61701538, 61871404, 61801435)，国家自然科学基金创新群体项目(61521003)
Foundation Items: The National Natural Science Foundation of China (61701538, 61871404, 61801435), The National Natural Science Foundation Innovative Groups Project of China (61521003)

到计算资源、体积和功耗等约束，数据速率低、数据量小，无法部署高复杂度的加密算法。在海量机器类通信场景中，随着节点数的增加，密钥的分发与管理也会变得非常困难[2]。

与现有的安全密钥机制不同，基于无线信道特征的物理层密钥生成技术，无线通信双方可以通过信道估计获取实时更新、无需分发的安全密钥，实现“一次一密”的完美加密效果[3]。无线信道的互易性是产生一致密钥的前提，然而受到实际因素如测量时延、设备差异及加性噪声的影响，合法通信双方测量的上下行信道特征并不完全一致[4]，通常利用信息协商提高密钥一致性。合法通信双方通过在公共信道上双向交互，可以消除不一致的比特。然而信息协商需要在现有的通信流程中设计额外的协议，增加了系统的通信开销和计算复杂度。此外，协商过程交互的校验比特容易泄露量化序列信息，增加了被窃听的风险[5]。

针对该问题，目前有学者对无协商密钥方案进行研究，文献[6]首次提出了基于无协商密钥的安全通信模型，将有错误比特的密钥加密过程放在信道编码后，利用信道编码的纠错能力在纠正信息传输误差的同时，纠正密钥中的不一致位，实现无差错的安全通信，从而省去了信息协商过程。然而，无协商密钥的安全通信方案也存在不足，方案设计中没有对信道编码参数进行针对性设计。信道编码的纠错能力有限，如果超过纠错能力，不但无法纠正错误比特，反而会导致错误扩散，实际应用中需要针对信道条件选用合适的编解码算法，并设计对应的参数。

针对以上问题，本文提出了一种基于极化码的无协商密钥物理层安全传输方案，在保证通信系统安全性和可靠性的同时使得编码率最优。该方案首先基于无线信道特征提取未协商的物理层初始密钥，然后针对自然噪声信道与初始密钥误差噪声信道共同构成的等效信道设计极化码，最后利用未协商的初始物理层密钥对编码后的序列进行加密传输。该方案基于等效信道针对性地设计极化码，使基于信道编码纠错能力的无协商密钥安全传输方案与合法通信信道本身实现强耦合，保证系统在安全可靠通信的同时达到传输码率最优的效果。由于窃听者不存在上述优势，难以实现窃听。该方案将物理层安全天然寄生于现有的5G通信流程和信号处理技术中，实现了安全与通信的融合。

2　系统模型

与传统采用预先分发的密钥进行加密的安全通信系统不同，本文采用基于无协商密钥的安全通信模型[6]。

如图1所示，物理层密钥生成阶段，Alice和Bob分别对信道估计值采取相同的量化算法进行量化、编码，得到初始密钥$\boldsymbol{K}_{\mathrm{a}}$, $\boldsymbol{K}_{\mathrm{b}}$。为了适配现有的通信机制，Alice和Bob不进行信息协商，所以初始物理层密钥高度相似但未必完全一致。Eve的位置距离Bob大于半波长，窃听信道与合法信道独立。假设Eve知道合法通信双方完整的通信流程，Eve采取相同的方案对私密信息进行窃听。

在安全传输阶段，Alice首先对私密消息$\boldsymbol{M}_{\mathrm{a}}$进行信道编码，然后用初始密钥$\boldsymbol{K}_{\mathrm{a}}$进行模二加加密，经过二进制相移键控(Binary Phase Shift Keying, BPSK)调制在无线信道传输。Bob对接收信号进行解调、用初始密钥$\boldsymbol{K}_{\mathrm{b}}$解密、信道译码等步骤恢复得到私密信息$\boldsymbol{M}_{\mathrm{b}}$。

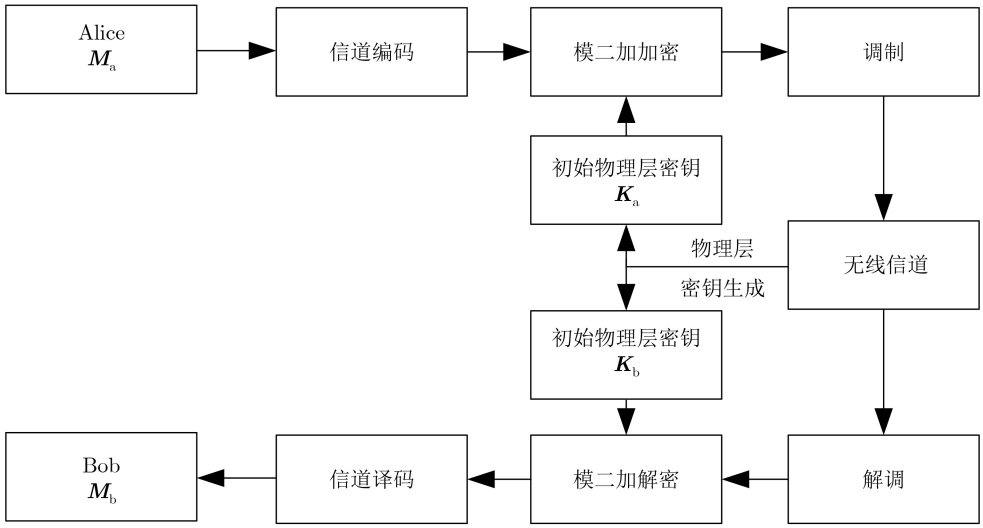

图 1 基于无协商密钥的安全通信模型

本文在上述模型的基础上，提出一种基于极化码的无协商密钥物理层安全传输方案。合法通信双方首先基于无线信道特征提取未协商的初始物理层密钥，然后将自然噪声信道与初始物理层密钥误差噪声信道构建为更加恶劣的等效信道，最后利用基于等效信道设计的极化码来纠正由于未协商密钥引入的错误比特，从而保证私密信息以最优的码率实现无差错安全传输。

3 基于极化码的无协商密钥物理层安全传输方案

在基于极化码无协商密钥物理层安全传输方案中，首先合法双方进行信道探测、量化等步骤生成初始物理层密钥。然后根据等效信道误比特率和高斯近似法构造出的极化码对私密信息进行编码。编码后的信息经过初始物理层密钥异或加密、调制后发送，接收方采取相同的流程恢复出私密信息。

3.1 无协商密钥生成

首先，Alice和Bob在同一相干时间内互发导频信号，设Alice发送导频信号为x_{A}, Bob发送导频信号为x_{B}，功率分别为${\sigma_{\mathrm{A}}}^2$和${\sigma_{\mathrm{B}}}^2$。假设信道为块衰落信道，不同相干时间的各信道矩阵元素独立同分布，所有信道均服从均值为0方差为1的复高斯随机变量，即$h\sim\mathcal{CN}(0,1)$。合法双方在每一相干时间T内只发送一次导频信号，然后接收导频并估计信道。简化起见，不妨设相干时间内的信道保持不变且合法信道满足互易性。经过N个相干时间后，将信道估计值作为共享随机源样本，表示为$\boldsymbol{S}_{\mathrm{A}}=\{s_{\mathrm{A},i},\ 1\le i\le N\}$和$\boldsymbol{S}_{\mathrm{B}}=\{s_{\mathrm{B},i},\ 1\le i\le N\}$，根据文献[7]的信道估计误差模型，可将两者的信道估计结果表示为

$$\left.\begin{aligned}\boldsymbol{S}_{\mathrm{A}}&=\boldsymbol{h}_{\mathrm{BA}}+\boldsymbol{w}_{\mathrm{Alice}}\\ \boldsymbol{S}_{\mathrm{B}}&=\boldsymbol{h}_{\mathrm{AB}}+\boldsymbol{w}_{\mathrm{Bob}}\end{aligned}\right\}\tag{1}$$

其中，$\boldsymbol{w}_{\mathrm{Alice}}$和$\boldsymbol{w}_{\mathrm{Bob}}$分别表示Alice和Bob信道估计误差，满足$\boldsymbol{w}_{\mathrm{Alice}}\sim\mathcal{CN}\left(0,{\sigma_{\mathrm{w}}}^2/{\sigma_{\mathrm{A}}}^2\right)$和$\boldsymbol{w}_{\mathrm{Bob}}\sim\mathcal{CN}\left(0,{\sigma_{\mathrm{w}}}^2/{\sigma_{\mathrm{B}}}^2\right)$, σ_{w}为无线信道的高斯白噪声方差。与此同时，被动窃听者Eve也可以采用信道估计的方式获得随机源。

为保证任意随机源的样本分布在各量化区间上的概率是相同的，本方案采用等概量化算法[3]量化信道估计值，采用格雷码对量化后的序列编码。为了适配现有的通信机制，Alice和Bob不进行信息协商，所以Alice与Bob的量化误比特率就是初始物理层密钥的不一致率(Key Disagreement Rate, KDR)。

由文献[8]可知，对$\boldsymbol{S}_{\mathrm{A}}$和$\boldsymbol{S}_{\mathrm{B}}$采用1 bit量化时，Alice和Bob量化误比特率为

$$P_{\mathrm{AB}}=\frac{1}{2}-\int_0^{\infty}\mathrm{erf}\left(\frac{u}{\sqrt{2\sigma_{\mathrm{A}}^2}}\right)\mathrm{erf}\left(\frac{u}{\sqrt{2\sigma_{\mathrm{B}}^2}}\right)\cdot\frac{1}{\sqrt{2\pi{\sigma_{\mathrm{w}}}^2}}\exp\left(\frac{-u^2}{2{\sigma_{\mathrm{w}}}^2}\right)\mathrm{d}u\tag{2}$$

假设Eve采取相同的密钥生成流程，则Bob和Eve之间的量化误比特率为

$$P_{\mathrm{AE}}=0.5\tag{3}$$

由于窃听信道和合法信道独立，因此$P_{\mathrm{AB}}<P_{\mathrm{AE}}$，即Bob对Eve具有量化信噪比优势。

3.2 构建等效信道

由图1所示的安全传输模型可知，通信系统的比特错误来源于初始物理层密钥差异和无线信道的噪声。信源采取二进制编码，信道的输入输出字符集$X,Y,Z\in\{0,1\}$，加密过程和传输过程均可看作信息比特经过二进制对称信道(Binary Symmetric Channel, BSC)，可用概率空间$[X,P(z|x),Z]$描述，其中$P(z|x)$为信道转移概率，如图2所示。

其中，P_{AB}为初始物理层密钥的量化误比特率，P_{e}为BPSK信号经过瑞利平衰落信道的传输误比特率。由于密钥量化和信息传输互相独立，该信道的转移概率矩阵为

$$\boldsymbol{P}(z|x)=\begin{array}{c}\\0\\1\end{array}\begin{array}{c}\begin{array}{cc}\quad0\quad&\quad1\quad\end{array}\\\begin{bmatrix}1-P_{\mathrm{e}}-P_{\mathrm{AB}}+2P_{\mathrm{AB}}P_{\mathrm{e}} & P_{\mathrm{e}}+P_{\mathrm{AB}}-2P_{\mathrm{e}}P_{\mathrm{AB}}\\ P_{\mathrm{e}}+p_{\mathrm{AB}}-2P_{\mathrm{AB}}P_{\mathrm{e}} & 1-P_{\mathrm{e}}-P_{\mathrm{AB}}+2P_{\mathrm{e}}P_{\mathrm{AB}}\end{bmatrix}\end{array}\tag{4}$$

对合法通信双方，自然噪声信道与初始密钥误差噪声信道共同构成等效信道，其传输误比特率为

$$P_{\mathrm{Total}}=P_{\mathrm{e}}+P_{\mathrm{AB}}-2P_{\mathrm{e}}P_{\mathrm{AB}}\tag{5}$$

对窃听者而言，由于Eve和Bob的量化误比特率$P_{\mathrm{AE}}=0.5$，故等效窃听信道转移概率

$$\begin{aligned}P(z|x)&=P_{\mathrm{e}}+P_{\mathrm{AE}}-2P_{\mathrm{e}}P_{\mathrm{AE}}\\&=0.5+P_{\mathrm{AE}}-2\times0.5\times P_{\mathrm{AE}}\\&=0.5\end{aligned}\tag{6}$$

因此，基于无协商密钥的安全通信模型可等价为基于等效信道的安全传输模型。如图3所示，在加密阶段，可等效为Alice与Bob采用完全相同的安

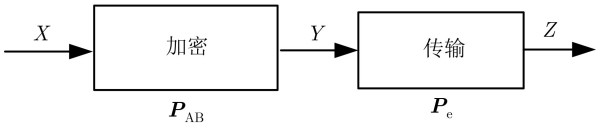

图 2 通信系统信道模型

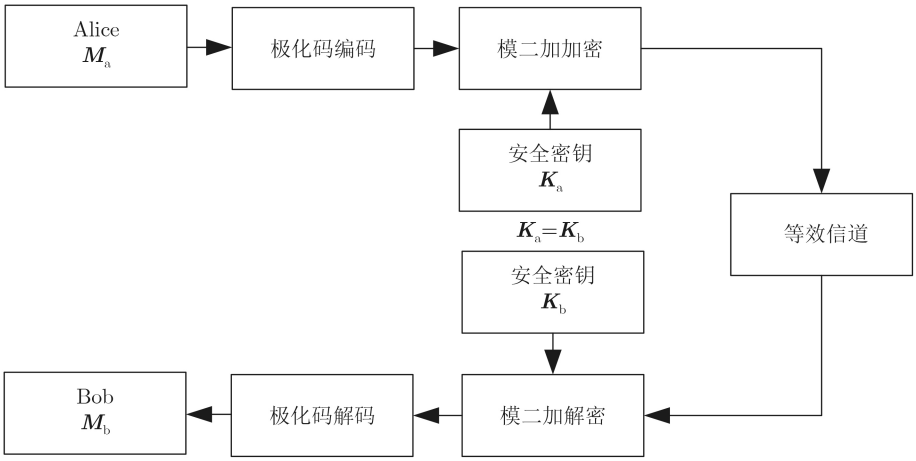

图 3 基于等效信道的安全传输模型

全密钥进行加密，而私密信息经历了更加恶劣的信道传输，该信道由密钥差异噪声和自然信道噪声等效而来。

3.3 极化码设计

当前5G通信系统中主要采用的信道编码有低密度奇偶校验(Low Density Parity Check, LDPC)码[9]和极化码，采用上述编码实现基于无协商密钥的物理层安全传输方案无需增加额外通信协议和计算资源。为了在等效信道条件下实现传输效果与合法信道本身的强绑定，选用的信道编码算法应与信道特性相关。极化码构造方法和译码算法与信道状态信息紧密结合，其编码过程即为信道极化过程，与信道特征天然绑定，是一种生而匹配信道的编码方式。极化码在数学上被证明达到2元对称信道的信道容量[10]，具有非常强的结构化特征和高效的纠错性能。因此本文方案中采取极化码进行信道编码，通过基于等效信道构造最优的极化码保证码率最优，实现安全与通信的一体化设计。

基于信道极化的极化码是针对特定信道条件的编码技术[11]，从N个极化子信道中挑选出K个信道容量最高的子信道，在信道容量高的子信道上传输私密信息，在噪声较大的子信道上传送冻结比特，因此首先需要计算各极化子信道的传输错误概率[12]。Alice与Bob, Eve各极化子信道的传输错误概率$P_{\mathrm{e}}^{\mathrm{AB}}\left(W_N^{(i)}\right)$和$P_{\mathrm{e}}^{\mathrm{AE}}\left(W_N^{(i)}\right)$可由高斯近似构造方法求解[13]。极化码串行抵消(Successive Cancellation, SC)译码算法[14]针对极化码结构特点进行译码，具有较低的译码复杂度。SC译码过程为

$$\hat{u}_i=\begin{cases}h_i\left(y_1^N,\hat{u}_1^{i-1}\right), & i\in A^c\\ 0, & i\in A\end{cases} \tag{7}$$

其中，$\hat{u}_i$为译码估计值，A为冻结比特索引集合。当$i\in A$时，第i位为冻结比特，可以根据事先约定直接译码，本文方案冻结比特取0。A^c为A的补集，当$i\in A^c$时，第i位为信息比特。极化码译码采用对数似然比(Log-Likelihood Ratio, LLR)进行判决

$$h_i\left(y_1^N,\hat{u}_1^{i-1}\right)=\begin{cases}0, & LLR_N^{(i)}\left(y_1^N,\hat{u}_1^{i-1}\right)\geq 0\\ 1, & \text{其他}\end{cases} \tag{8}$$

由于串行抵消译码时u_i的译码受前$i-1$个比特的译码u_1^{i-1}的影响，会导致出现错误扩散的出现，难以精确地求解极化码的译码误比特率。因此可采取极化码的误比特率上下界进行代替。记$v_{\mathrm{worst}}(\xi_i)_{A^c}$为译码错误的信息比特数，译码误比特率上界为

$$P^{\mathrm{UB}}=\frac{\sum_{i=1}^{N}p_i v_{\mathrm{worst}}(\xi_i)_{A^c}}{K} \tag{9}$$

此时错误完全扩散，ξ_i表示第1个错误比特译码发生在第i个比特，即当事件ξ_i发生时，后续$N-i+1$个除冻结比特外的所有未知比特均以概率1译码错误。p_i为其对应的概率

$$p_i=\begin{cases}P_{\mathrm{d}}\left(W_N^{(1)}\right), & i=1\\ P_{\mathrm{d}}\left(W_N^{(i)}\right)\prod_{j=1}^{i-1}\left(1-P_{\mathrm{d}}\left(W_N^{(j)}\right)\right), & i\geq 2\end{cases} \tag{10}$$

记$v_{\mathrm{best}}(\xi_i)_{A^c}$为译码错误的信息比特数，译码误比特率下界为

$$P^{\mathrm{LB}}=\frac{\sum_{i=1}^{N}p_i v_{\mathrm{best}}(\xi_i)_{A^c}}{K}=\mathrm{mean}\left(P_{\mathrm{e}}\left(W_N^{(i)}\right)_{A^c}\right) \tag{11}$$

此时错误完全不扩散，即当事件ξ_i发生时，后续$N-i$个比特译码错误概率为$P_{\mathrm{d}}\left(W_N^{(j)}\right)$。

为满足通信系统的可靠性需求和安全要求，Bob的译码误比特率P'_{AB}用其上界$P'^{\mathrm{UB}}_{\mathrm{AB}}$代替，Eve的

译码误比特率P'_{AE}用其下界$P'^{\mathrm{LB}}_{\mathrm{AE}}$代替，则极化码最优设计问题可归结为

$$\max_{K\in\{1,2,\cdots,N\}} \eta=\frac{K}{N},\quad \text{s.t. } P'^{\mathrm{UB}}_{\mathrm{AB}}\le P_{\mathrm{QoS}},\ \ P'^{\mathrm{LB}}_{\mathrm{AE}}\ge P_{\mathrm{Sec}} \tag{12}$$

式(12)的物理意义为在Bob的译码误比特率满足服务质量(Quality of Service, QoS)需求和Eve的译码误比特率满足安全要求的条件下，设计一个码率最优的极化码。该方案利用初始物理层密钥和构造的极化码保证了通信系统传输的安全性和可靠性，依托现有的5G通信机制可实现无差错的高效传输。

窃听信道和合法信道独立，由式(6)可知，Eve的等效信道误比特率为0.5。由高斯近似可求得各窃听极化子信道的传输误比特率$P_{\mathrm{e}}^{\mathrm{AE}}\left(W_N^{(i)}\right)=0.5$。因此对于任意构造的极化码而言，由式(11)可求得Eve的译码误比特率下界$P'^{\mathrm{LB}}_{\mathrm{AE}}=0.5$，再由译码误比特率本身不大于0.5可知，Eve的译码误比特率为$P'_{\mathrm{AE}}=0.5$，所以安全要求始终满足。

对于合法通信双方，利用高斯近似法和等效信道误比特率分别计算各极化子信道的传输误比特率。记各合法极化子信道的传输误比特率$P_{\mathrm{e}}^{\mathrm{AB}}\left(W_N^{(i)}\right)$按照从小到大的排序为$V(i)$，对应的索引为$I(i)$，则式(12)的优化问题可进一步简化为

$$K=\arg\left\{\max_{K\in\{1,2,\cdots,N\}}\left(P'^{\mathrm{UB}}_{\mathrm{AB}}\left(I(i)\big|_1^K\right)\le P_{\mathrm{QoS}}\right)\right\} \tag{13}$$

其中，$P'^{\mathrm{UB}}_{\mathrm{AB}}\left(I(i)\big|_1^K\right)$代表合法极化子信道索引为$I(i)$, $i=1,2,\cdots,K$的极化子信道承载信息比特而其余极化子信道承载冻结比特时的极化码译码误比特率上界。由式(13)即可求得极化码信息比特数K及对应各极化子信道的传输误比特率$P_{\mathrm{e}}^{\mathrm{AB}}\left(W_N^{(i)}\right)$。在合法极化子信道索引为$I(i)\big|_1^K$的极化子信道上放置信息比特，其余极化子信道放置冻结比特，从而构造出最优的极化码。

3.4 轻量级加密传输

在利用基于等效信道设计的极化码对私密信息进行编码后，直接采用无协商的物理层密钥对编码后的序列进行模二加加密，再经过BPSK调制在无线信道传输，如图4所示。Bob对接收信号进行解调、用初始物理层密钥$\boldsymbol{K}_{\mathrm{b}}$解密、极化码译码等步骤恢复得到私密信息。该方案初始物理层密钥和极化码分别保证了传输的安全性和可靠性，通过针对性地设计极化码可以实现最优的码率。

4 仿真结果及分析

本节对第3节所提的基于极化码的无协商密钥物理层安全传输方案进行仿真，通过蒙特卡罗方法验证所提方案的有效性。Alice, Bob与Eve均配备单天线，表1展示了仿真参数设定值。

4.1 安全性和可靠性分析

图5展示了合法通信双方的密钥不一致率和窃听方密钥不一致率随信噪比的变化。从图中可以看出，当采用1 bit量化时，Alice和Bob的量化不一致率随着信噪比的增大而降低，而Alice和Eve的量化不一致率始终保持在0.5左右。合法信道量化不一致率远远低于窃听信道，说明在利用无协商的物理层密钥进行加解密时合法信道相比窃听信道存在天然的优势。

图6展示了等效合法信道和等效窃听信道的传输误比特率随信噪比的变化情况。从图中可以看出，等效合法信道的传输误比特随着信噪比的增加而降低，说明在信道条件较好的情况下，Alice和Bob可以通过极化编码实现无差错的安全传输。而等效窃听信道的传输误比特始终保持在0.5左右，因此即使窃听者存在信噪比优势，也无法正确接收Alice发送的私密信息。

4.2 极化码构造及实际性能

根据3GPP对极化码长的建议[15]，下行最大码长为1024，上行最大码长为512，本文取极化码码长$N=512$。图7展示了译码后的比特错误率随信噪比、极化码码率的变化。从图中可以看出，Alice和Bob的比特错误率随着信噪比增加而减小，这是

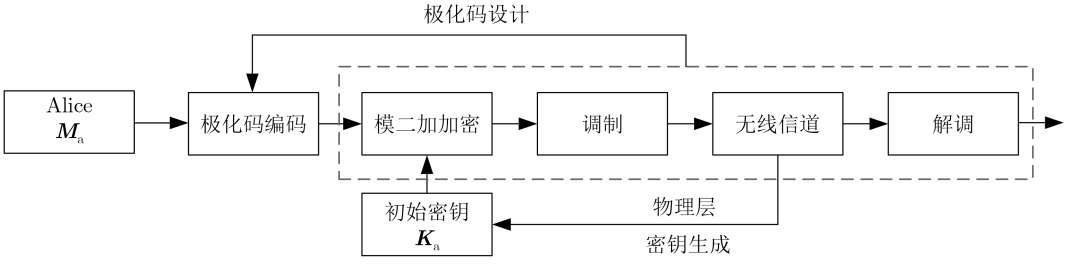

图 4 轻量级加密传输流程

表 1　仿真参数列表

仿真参数	设定值
天线数	单天线
无线信道	瑞利平衰落信道
极化码长	$N = 512$
蒙特卡洛实验次数	10^8
量化级数	1 bit量化
噪声功率	$\sigma_{\mathrm{w}}^2 = 1$
功率分配	$\sigma_{\mathrm{A}}^2 = \sigma_{\mathrm{B}}^2$

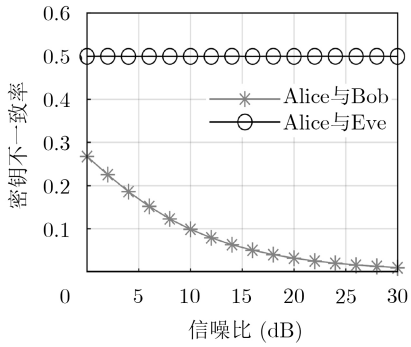

图 5 量化不一致率与信噪比关系

由于随着信噪比增加，密钥不一致率和自然信道的误比特率都会减小，系统的传输误比特也跟着降低，所以Alice和Bob的比特错误率会随着信噪比的增加而降低。另一方面，Alice和Bob的比特错误率随着着极化码码率的降低而降低，说明在信道条件较好的情况下，Alice和Bob可以通过极化码的纠错能力实现无差错的安全传输。

表2展示了利用等效信道设计的极化码参数和

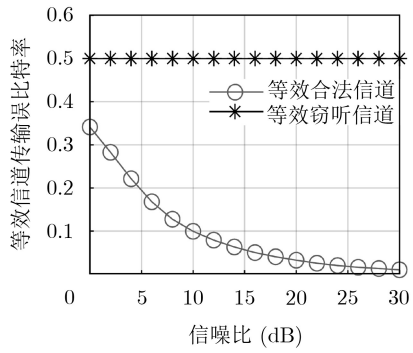

图 6 等效信道的传输误比特与信噪比关系

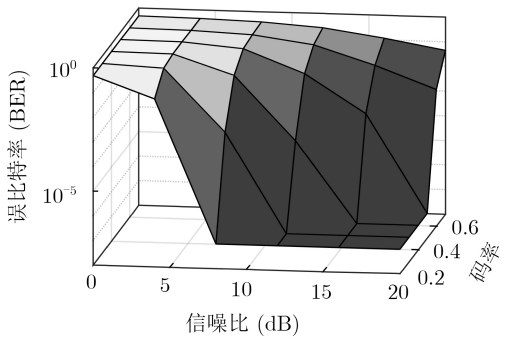

图 7 译码后的比特错误率随信噪比、极化码码率的关系

对应的实际性能。当信噪比已知时，由式(13)可求得极化码的信息比特数，由对应的信息比特索引即可构造出相应得极化码。从表中可以看出，构造的极化码均能够满足QoS需求和安全要求，证明基于等效信道的极化码构造方法的有效性，设计的极化码在最大化码率的同时保证了通信系统的安全性和可靠性。

表 2　极化码参数与设计性能

信道条件	极化码设计参数				极化码实际性能	
SNR(dB)	N	K	P_{QoS}	P_{Sec}	$P_{\mathrm{e}}^{\mathrm{AB}}$	$P_{\mathrm{e}}^{\mathrm{AE}}$
2	512	27	10^{-6}	10^{-1}	9.2368×10^{-7}	0.4865
6		156			2.5952×10^{-7}	0.4973
10		203			1.1011×10^{-7}	0.4799

5　结束语

本文针对现有密钥生成方案与通信流程不兼容的问题，提出了基于极化码的无协商密钥物理层安全传输方案。该方案将初始物理层密钥差异和自然信道噪声等效成更为恶劣的信道条件，针对该等效信道设计最优的极化码纠正比特错误，在满足QoS需求和安全要求的同时使得系统的码率最优，有效避免了密钥协商带来的通信开销和信息泄露。该方案可以依托现有的5G通信机制，无需增加额外的协议和流程，实现了安全与通信的融合和一体化设计。

参 考 文 献

[1] JI Xinsheng, HUANG Kaizhi, JIN Liang, *et al*. Overview of 5G security technology[J]. *Science China Information Sciences*, 2018, 61(8): 081301. doi: 10.1007/s11432-017-9426-4.

[2] JIAO Long, WANG Ning, WANG Pu, *et al*. Physical layer key generation in 5G wireless networks[J]. *IEEE Wireless*

Communications, 2019, 26(5): 48–54. doi: 10.1109/MWC.001.1900061.

[3] WU Yongpeng, KHISTI A, XIAO Chengshan, *et al*. A survey of physical layer security techniques for 5G wireless networks and challenges ahead[J]. *IEEE Journal on Selected Areas in Communications*, 2018, 36(4): 679–695. doi: 10.1109/JSAC.2018.2825560.

[4] LI Guyue, SUN Chen, ZHANG Junqing, *et al*. Physical layer key generation in 5G and beyond wireless communications: Challenges and opportunities[J]. *Entropy*, 2019, 21(5): 497. doi: 10.3390/e21050497.

[5] LI Guyue, ZHANG Zheying, Yu Yi, *et al*. A hybrid information reconciliation method for physical layer key generation[J]. *Entropy*, 2019, 21(7): 688. doi: 10.3390/e21070688.

[6] PENG Linning, LI Guyue, ZHANG Junqing, *et al*. Securing M2M transmissions using nonreconciled secret keys generated from wireless channels[C]. 2018 IEEE Globecom Workshops, Abu Dhabi, The United Arab Emirates, 2018: 1–6.

[7] ASSALINI A, DALL'ANESE E, and PUPOLIN S. Linear MMSE MIMO channel estimation with imperfect channel covariance information[C]. 2009 IEEE International Conference on Communications, Dresden, Germany, 2009: 1–5.

[8] HU Xiaoyan, JIN Liang, and ZHONG Zhou. A scrambling scheme based on random wireless channel characteristics for secure transmission[C]. The 2020 12th International Conference on Communication Software and Networks, Chongqing, China, 2020: 29–38.

[9] ISLAM N, GRAUR O, FILIP A, *et al*. LDPC code design aspects for physical-layer key reconciliation[C]. 2015 IEEE Global Communications Conference, San Diego, USA, 2015: 1–7.

[10] ARIKAN E. Channel polarization: A method for constructing capacity-achieving codes for symmetric binary-input memoryless channels[J]. *IEEE Transactions on information Theory*, 2009, 55(7): 3051–3073. doi: 10.1109/TIT.2009.2021379.

[11] TRIFONOV P. Efficient design and decoding of polar codes[J]. *IEEE Transactions on Communications*, 2012, 60(11): 3221–3227. doi: 10.1109/TCOMM.2012.081512.110872.

[12] 张胜军, 钟州, 金梁, 等. 基于安全极化码的密钥协商方法[J]. 电子与信息学报, 2019, 41(6): 1413–1419. doi: 10.11999/JEIT180896.

ZHANG Shengjun, ZHONG Zhou, JIN Liang, *et al*. Secret key agreement based on secure polar code[J]. *Journal of Electronics & Information Technology*, 2019, 41(6): 1413–1419. doi: 10.11999/JEIT180896.

[13] ZHANG Shengjun, JIN Liang, HUANG Yu, *et al*. Nonagreement secret key generation based on spatial symmetric scrambling and secure polar coding[J]. *Scientia Sinica Informationis*, 2019, 49(4): 486–502. doi: 10.1360/N112018-00119.

[14] 白慧卿, 金梁, 肖帅芳. 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): 2587–2593. doi: 10.11999/JEIT170068.

BAI Huiqing, JIN Liang, XIAO Shuaifang, *et al*. Polar code for physical layer security in multi-antenna systems[J]. *Journal of Electronics & Information Technology*, 2017, 39(11): 2587–2593. doi: 10.11999/JEIT170068.

[15] Final report of 3GPP TSG RAN WG1 #88bis v1.0. 0[R]. 2017.

黄开枝：女，1973年生，教授、博士生导师，研究方向为移动通信网络及信息安全.

万 政：男，1996年生，硕士生，研究方向为物理层安全及信息安全.

楼洋明：男，1991年生，助理研究员，研究方向为信息论、物理层安全.

肖帅芳：男，1989年生，助理研究员，研究方向为无线物理层安全.

许晓明：男，1988年生，助理研究员，研究方向为移动通信网络及信息安全.

责任编辑：余 蓉