基于细粒度极化的隐蔽密钥分发方案

徐 明[1),2)] 吴佳佳[1)]

[1)](上海海事大学信息工程学院 上海 201306)

[2)](同济大学电子与信息工程学院 上海 201804)

摘 要 针对现有密钥分发协议在水声信道环境下的信息泄露问题,提出了一种基于细粒度极化的隐蔽密钥分发（Covert Secret-key distribution based on Fine-grained Polarization，CSFP）方案. 首先，采用一致最大功效检验方法建立敌手模型，并给出隐蔽密钥分发方案的形式化定义. 考虑到水声信道的非对称性和衰落效应，根据注水原理推导出信息传输速率达到香农极限时最优码字符号分布对应的带宽以及信道容量，并利用莱布尼兹积分法则和黎曼积分的保号性推导出信道容量与信道增益的函数关系，通过计算水声信道增益对极化子信道的容量进行排序实现极化码的码字构造，确保信息传输速率达到香农极限. 其次，对信息比特索引集合进行细粒度极化，采用链式结构将多个消息块依次链接实现信息比特索引序列的对齐,设计出多轮通信下隐蔽密钥分发的编码和解码算法，利用合法发送方和接收方共享的随机种子对首轮传输的消息块进行初始化，并从当前生成的密钥中提取出随机种子对后续消息块进行随机化，确保密钥分发过程的隐蔽性. 最后，通过信息理论证明了 CSFP 方案的可靠性、随机性、保密性和隐蔽性,利用最大熵原理推导出水声信道环境下隐蔽性约束的可达性条件和隐蔽密钥生成速率. 仿真结果表明，与现有方案相比，CSFP 方案的隐蔽密钥生成速率平均提高了 18.78%，隐蔽概率平均提高了 38.29%. 此外，CSFP 方案生成的密钥成功通过了 SP 800-22 测试平台的随机性检测.

关键词 水声信道；信息泄露；细粒度极化；信道增益；隐蔽密钥分发

中图法分类号 TP309 **DOI 号** 10. 11897/SP. J. 1016. 2023. 00147

Covert Secret-Key Distribution Scheme Based on Fine-Grained Polarization

XU Ming[1),2)] WU Jia-Jia[1)]

[1)](*College of Information Engineering, Shanghai Maritime University, Shanghai* 201306)

[2)](*College of Electronics and Information Engineering, Tongji University, Shanghai* 201804)

Abstract Underwater acoustic communication is increasingly being perceived as a promising means for marine life monitoring, ocean exploration, underwater navigation and surveillance. In order to defend against the potential security threats, two legitimate parties in the communication adopt key distribution protocols to negotiate a secret-key to encrypt the transmitted data. However, the characteristics of the underwater acoustic channel (UAC) and its inherent vulnerability make the communication process of secret-key distribution protocols easy to be detected, rendering the inevitable information leakage. Some researchers have introduced covert communication into secret-key distribution protocols to keep them undetectable by a warden based on random codes, and have even extended the ideas of covert communication to quantum key distribution. However, achieving information theoretical security with practical coding schemes is of definite interest. To this end, some covert secret-key distribution protocols based on polar codes are proposed for symmetric channels with uniformly distributed binary sequences. In these scenarios,

收稿日期：2021-11-18；在线发布日期：2022-05-12. 本课题得到国家自然科学基金面上项目(62172269)、中国博士后科学基金项目(2014M561512)资助. **徐 明**(通信作者)，博士，教授，中国计算机学会(CCF)会员，主要研究领域为密码学与信息安全、无线网络安全与移动计算. E-mail: mingxu@shmtu.edu.cn. **吴佳佳**，硕士研究生，主要研究领域为密码学与信息安全.

the legitimate users aim at extracting a common secret-key from their observations through public communications. However, it is not feasible to apply polar codes directly to the UAC since the Bhattacharyya parameters of polarized channels cannot be calculated and sorted over asymmetric channels. To address these problems, a Covert Secret-key distribution scheme based on Fine-grained Polarization (CSFP) is proposed under the environment of UAC. First, a uniformly most powerful test is adopted to build the adversary model, and the formal definition of covert secret-key distribution scheme is given. Considering the asymmetry and fading effects of the UAC, the bandwidth and the channel capacity corresponding to the optimum symbol distributions of codewords are derived by the water-filling principle for the information transmission rate to achieve the Shannon limit theoretically, and the functional dependence between channel capacity and channel gain is derived by the Leibniz Integral rule and the sign-preserving property of Riemann integral. The polar code construction is realized through sorting the capacity of each subchannel after calculating the gains of UAC in order to ensure that the information transmission rate can achieve the Shannon limit theoretically. Second, the encoding and decoding algorithms for covert secret-key distribution over multi-round communication are designed based on the fine-grained polarization and the alignment of index sequence of information bits by linking multiple information blocks through a chain structure. To ensure the covertness of secret-key distribution process, the legitimate transmitter and the legitimate receiver initialize the message block transmitted in the first round of communication using a shared random seed and extract a random seed from the currently generated secret-key to randomize the next message block. Finally, the reliability, randomness, secrecy and covertness of the CSFP scheme are proved through the information theory and the achievability of covertness constraint and the covert secret-key generation rate under the environment of UAC are derived by the maximum entropy principle. The simulation results show that the CSFP scheme improves the covert secret-key generation rate by 18.78% and improves the covert probability by 38.29% on average compared to the existing scheme. Moreover, the generated secret-keys of the CSFP scheme successfully pass the randomness test on the platform of SP 800-22 Test Suite.

Keywords underwater acoustic channel; information leakage; fine-grained polarization; channel gain; covert secret-key distribution

1 引 言

海洋信息网络是人类用于认知海洋、开发海洋和经略海洋的信息网络，包括海洋信息的获取、传输、融合应用等[1]. 水声通信被认为是最适合在水下进行中长距离信息获取和传输的手段，但由于水下节点长时间部署在无人值守的恶劣环境以及水声信道的开放性使得水下信息传输更容易遭受外部攻击[2]. 基于对称密钥的加密技术是保障无线通信安全的主要手段，这种安全机制的关键在于如何将对称密钥安全可靠地分发至合法通信双方[3]. 然而，水声信道的高时延、低带宽和多径效应等特性以及水下节点的硬件资源限制使得传统密钥分发协议更容易遭受信息泄露和非法检测等安全威胁[4-5]. 量子密钥分发协议利用单光子的不可分割性和单光子量子态的测量塌缩性，使得合法通信双方可以在光纤信道中实现基于信息理论安全的密钥分发[6]，但无法直接应用于水声信道.

近年来，一些学者在密钥分发协议中引入隐蔽通信技术，在已知非法检测方存在的前提下，通过限制合法发送方信号传输功率或采用编码等方法，使得非法检测方接收信号的概率分布与背景噪声的概率分布非常接近，从而实现隐蔽密钥分发[7-9]. 其中，通过限制合法发送方信号传输功率的隐蔽密钥分发协议将需要隐藏的信息与背景噪声或人工噪声叠加后发送，确保调制后的信号功率小于非法检测方预设的功率检测阈值，实现信息传输状态对非法检测方的可否认性. Bash 等人证明了在加性高斯白噪声（Additive White Gaussian Noise，AWGN）信道下，发送方经过 n 次信道使用最多能可靠传输 $O(\sqrt{n})$ 比特信息至接收方，同时保证被非法检测方检测到的概率为任意小，即隐蔽容量的平方根定律[10].

然而，在水声传播模型中，由于扩展损耗、吸收损失、粘滞吸收和分子弛豫等因素造成的传播损失和信道衰落使得合法方必须提高信号传输功率才能达到 $O(\sqrt{n})$ 比特的隐蔽容量，但同时也会降低密钥分发过程的隐蔽性甚至暴露合法方的信息传输状态. 此外，基于编码的隐蔽密钥分发协议大多假设编码后的码字是具有渐近等分性的长码字[9]. 然而，在水声信道环境下，信道结构随时间变化剧烈，使得合法节点传输的码字和接收到的观测值不一致概率变大，造成解码性能降低，增加了数据传输的不确定性和误码率，降低了密钥生成速率. 为了提高编解码的性能，部分学者将极化码技术引入密钥分发协议[11]. 极化码作为目前唯一可理论证明达到香农极限，且具有可实用线性复杂度编解码能力的信道编码技术[12]，可以同时满足高速率和低时延等各类物联网的应用需求，并被国际移动通信标准化组织确定为 5G 增强移动宽带场景的控制信道编码方案[13]. 现有基于极化码的隐蔽密钥分发协议利用均匀分布的随机向量将多个码字链接在一起[14]，再通过串行抵消（Successive Cancellation，SC）解码算法进行码字估计，使得合法双方可以生成相同的密钥序列. 然而，随机向量的重复使用不仅会降低密钥序列的独立性，还会使非法检测方更容易检测或分析出密钥分发协议的执行状态.

为了解决现有密钥分发协议在水声信道环境下的信息泄露问题，本文从水声信道的物理特性出发，提出一种基于细粒度极化的隐蔽密钥分发（Covert Secret-key distribution based on Fine-grained Polarization，CSFP）方案.

本文的主要贡献如下:

（1）给出隐蔽密钥分发方案的形式化定义，考虑到水声信道的衰落效应，利用莱布尼兹积分法则和黎曼积分的保号性推导出信道容量与信道增益的函数关系，通过计算水声信道增益对极化子信道的容量进行排序实现极化码的码字构造，确保信息传输速率达到香农极限；

（2）考虑到水声信道的非对称性，对信息比特索引集合进行细粒度极化，采用链式结构将消息块依次链接实现信息比特索引序列的对齐，在此基础上，设计出多轮通信下隐蔽密钥分发的编码和解码算法，利用合法发送方和接收方共享的随机种子对首轮传输的消息块进行初始化，并从当前生成的密钥中提取出随机种子对下一轮传输的消息块进行随机化，确保密钥分发过程的隐蔽性；

（3）采用一致最大功效检验方法建立敌手模型，利用最大熵原理推导出水声信道环境下隐蔽性约束的可达性条件，通过信息理论证明了 CSFP 方案的可靠性、随机性、保密性和隐蔽性，推导出隐蔽密钥生成速率，通过仿真实验验证和分析了 CSFP 方案的性能.

2　相关工作

密钥分发协议允许通信双方在不安全的信道环境下建立共享的对称密钥，为双方的通信安全提供保密性和认证性保护[15]. 文献[16]提出的双场（Twin-field）量子密钥分发系统实现了 833.8 km 的安全通信距离，并能容忍超过 140 dB 的信道损耗，但目前仅适用于光纤信道环境. 文献[17]提出了一种基于等效信道的物理层认证及密钥分发机制，利用多个时隙的信道特征对任意密钥进行加密传输建立等效信道，将信道特征的差异映射为传输畸变，依据密钥传输的正确性判断收发两端信道特征互信息的大小，在完成密钥的分发的同时实现发端身份认证. 文献[18]基于信道模型提出了一个适用于 MIMO（Multiple-Input Multiple-Output）系统的密钥分发协议，并通过信息理论分析带被动窃听者的点到点通信模型所能生成密钥的密钥容量、密钥不一致率、密钥泄漏率和密钥随机性. 文献[19]基于香农密码系统提出了一个有限容量的密钥分发模型，通过疑义度（Equivocation）来表征安全等级，并联合码字的压缩性（Compressibility）以及重建信源的失真（Distortion）来构造“失真-速率-疑义度”三元组，进而给出该三元组可达域（Achievable Region）的充分必要条件与证明. 文献[20]提出了一种基于信源模型的密钥分发方案，并假设合法通信双方与窃听者分别从观测函数集合中选择一个确定的观测函数来观测相同状态下的公共随机源. 如果每一个观测函数都无法获得公共随机源的完备信息，则合法通信双方可以实现密钥分发. 然而，上述协议在密钥分发过程中缺乏隐蔽性，无法满足军事国防等高密级信息系统的安全需求. 通过隐蔽通信技术实现非法检测方的低概率检测（Low Probability of Detection，LPD）为密钥分发的安全问题提供了全新的解决思路[10]. 文献[10]基于非法检测方对于信道知识非因果可知的假设，提出了隐蔽通信的平方根定律，即隐蔽传输的信息理论极限. 进一步，文献[7]提出了一种在噪声不确定环境下基于最大比发送（Maximum Ratio Transmission，MRT）方式的波束成形技术，增强非法检测方接收信号的不确定性. 然而，波束成形技术存在同步精度与能耗的权衡问

题[21]，无法有效移植和应用到水下环境. 文献[22]证明了基于信道不确定性模型下的中继网络可以有效传输 $O(n)$ 比特的隐蔽消息，但消息的放大转发（Amplify-and-Forward，AF）会导致接收方解码时的误码率增高，降低了可靠性. 此外，上述类型的研究方案需要确保合法发送方的信号发送功率小于非法检测方预设的功率检测阈值，但是在实际应用系统中很难进行设定. 文献[9]基于随机编码机制提出了一种非法检测方可以任意选择信道状态的隐蔽密钥分发协议，并从理论上证明了隐蔽密钥生成速率能够达到信息理论极限. 然而，随机编码只是一种理论上的编码机制，无法应用到实际系统中. 文献[11]首次将极化码技术应用到密钥分发协议，利用显式构造的极化码将随机编码实例化并证明了在二进制对称窃听信道下可以达到保密容量. 文献[23]提出了一种基于极化码技术的强安全编码方案，但仅适用于二进制对称信道. 进一步，文献[24]针对速率无限的点到点模型、单向且速率受限的点到点模型、有噪一对多的多终端广播模型和具有均匀边缘的马尔可夫树模型设计了基于极化码的密钥生成方案，展现了极化码在多种应用场景下的适用性和灵活性. 然而，该方案在密钥分发过程中存在随机向量的重复使用问题，导致密钥随机性的降低以及非法检测方检测或分析出密钥分发协议执行状态成功概率的提升. 针对速率无限的点到点模型，文献[25]采用极化子信道分配机制提出了一种基于脉冲位置调制（Pulse-Position Modulation，PPM）和多级编码（Multi-Level Coding，MLC）的隐蔽密钥生成算法，通过在每一级子信道上进行独立编码来降低计算复杂度，但该算法需要假设编码端输入序列服从均匀分布并且仅适用于二进制输入离散无记忆信道（Binary-Input Discrete Memoryless Channel，BI-DMC）. 然而，由于水声信道的非对称性，因此能够实现香农极限的最优码字符号分布并不总是均匀的[26-27]. 本文将重点研究如何在水声信道环境下通过信道的细粒度极化实现隐蔽密钥分发.

3 系统模型

本文考虑一个由合法发送方 Alice，合法接收方 Bob 以及非法检测方 Willie 组成的水声通信系统模型. Alice 和 Bob 通过公开的水声信道执行密钥分发协议生成一致的共享密钥，并确保 Willie 无法检测到密钥分发协议的执行状态.

3.1 信道模型

受复杂海况和海域底部地质特性影响，水声信道通常被建模为多径衰落信道模型. 假设合法发送方 Alice 将长度为 n 的码字 $U^n=[U_1,U_2,...,U_n]$ 发送给合法接收方 Bob，则信道输出可表示为

$$Y_i = R_i U_i + \eta_i, \quad i \in [1,n] \tag{1}$$

其中 Y_i 表示 Bob 的观测值，R_i 表示信道衰落效应，用来刻画衰落过程的幅度和相位，η_i 表示环境噪声. 令 $|R_i|$ 代表衰落过程的包络，则信道增益可表示为[28]

$$\begin{aligned} G^{(i)} &= \mathbb{E}[|R_i|^2] \\ &= \frac{1}{B}\int_{f_c-B/2}^{f_c+B/2} \left| \sum_{p=0}^{\mathcal{P}-1} \frac{\Gamma_p}{\sqrt{A(l_p^{(i)},f)}} e^{-\mathrm{j}2\pi f \tau_p^{(i)}} \right|^2 \mathrm{d}f \end{aligned} \tag{2}$$

其中 B 为传输带宽，f_c 为中心频率，$\mathcal{P}$ 为多径数目，$\tau_p^{(i)}$ 为沿着第 p 条路径传输第 i 个比特时的时延，水下传播损失可表示为[28]

$$A(l_p^{(i)},f) = A_0 (l_p^{(i)})^s \alpha(f)^{l_p^{(i)}} \tag{3}$$

其中 A_0 为单位归一化常量，$l_p^{(i)}$ 为沿路径 p 传输第 i 个比特时的路径长度，s 为扩展因子，浅海环境下取经验值 $s=1.5$[29]；Γ_p 为第 p 条路径的累积反射系数，由海洋表面和底部的反射数所决定；介质吸收系数 $\alpha(f)$ 根据 Thorp 经验公式确定[28]

$$\alpha(f) = \frac{0.11 f^2}{1+f^2} + \frac{44 f^2}{4100+f^2} + 0.000275 f^2 + 0.003 \tag{4}$$

将传输带宽 $B(l,G)$ 划分为多个互不重叠的子频带，即 $B(l,G)=\bigcup_m [f_{ini}^m(l,G), f_{end}^m(l,G)]$，则 Alice 传输单比特的发送功率可归一化表示为

$$P_s = \frac{1}{n}\sum_{i=1}^{n} \mathbb{E}[|U_i|^2] = \int_{B(l,G)} S(l,f)\mathrm{d}f = 1 \tag{5}$$

其中，$S(l,f)$ 为传输距离为 l 时发送信号的功率谱密度.

3.2 敌手模型

本文采用二元假设检验分析非法检测方 Willie 对密钥分发协议执行状态的检测能力. 令 Z^n 表示 Willie 的观测值，其原假设 $\mathcal{H}_0$ 和备择假设 $\mathcal{H}_1$ 可分别表示为

$$\mathcal{H}_0 : Z^n \sim Q_Z^{\otimes n} \quad \mathcal{H}_1 : Z^n \sim P_{Z^n},$$

其中，$n=2^\nu$，$\nu \in \mathbb{N}^+$，$\mathbb{N}$ 为整数，“$\otimes n$”是 n 次 Kronecker 幂. $Q_Z^{\otimes n} = \prod_{i=1}^{n} Q_{Z_i}$ 表示合法双方未执行隐蔽密钥分发协议时 Z^n 的概率分布，$P_{Z^n} = \prod_{i=1}^{n} P_{Z_i|Z_{1:i-1}}$ 表示合法双方执行隐蔽密钥分发协议时 Z^n 的概率

分布. 根据 Neyman-Pearson 引理，似然比检验（Likelihood Ratio Test，LRT）方法对于 $\mathcal{H}_0$ 是一致最大功效检验，因此 Willie 可以采用似然比的对数期望，即相对熵来衡量概率分布 P_{Z^n} 和 $Q_Z^{\otimes n}$ 的相似度，可表示为

$$\mathbb{D}(P_{Z^n}\|Q_Z^{\otimes n})=\sum_{Z\in Z^n}P_{Z^n}(z^n)\log\frac{P_{Z^n}(z^n)}{Q_Z^{\otimes n}(z^n)} \tag{6}$$

当 $\mathbb{D}(P_{Z^n}\|Q_Z^{\otimes n})=0$ 时，概率分布 P_{Z^n} 和 $Q_Z^{\otimes n}$ 相同，此时无论合法双方是否进行隐蔽密钥分发，Willie 非法检测成功的概率都为 $1/2$，相当于随机猜测.

4　方案设计

4.1　方案描述

首先给出隐蔽密钥分发方案的形式化定义. 令 $P_{K_{1:\ell}}$ 和 $P_{K_{1:\ell}}^{\text{unif}}$ 分别表示密钥的真实分布和理想分布，$P_{K_{1:\ell}M_{1:\ell}Z^{\ell n}}$ 表示密钥 $K_{1:\ell}$，消息块 $M_{1:\ell}$ 和码字 $Z^{\ell n}$ 的联合概率分布，$P_{M_{1:\ell}Z^{\ell n}}$ 表示消息块 $M_{1:\ell}$ 和码字 $Z^{\ell n}$ 的联合概率分布. $P_{Z^{\ell n}}$ 为 Willie 在合法双方执行隐蔽密钥分发协议时 $Z^{\ell n}$ 的概率分布，$Q_Z^{\otimes \ell n}$ 为 Willie 在合法双方未执行隐蔽密钥分发协议时 $Z^{\ell n}$ 的概率分布.

定义 1. 存在一个密钥分发方案 $\mathbb{C}$，具体表示为 6 元组 $\mathbb{C}=(M_{1:\ell},n,\epsilon,\upsilon,\xi,\varsigma)$，其中 $M_{1:\ell}$ 代表 ℓ 个消息块，n 表示码长，ϵ，υ，ξ，ς 为任意小的正数. 其中，ϵ 表示可靠性约束，υ 表示随机性约束，ξ 表示保密性约束，ς 表示隐蔽性约束，若密钥分发方案 $\mathbb{C}$ 满足以下 4 个条件，即

可靠性 $P_e(\mathbb{C})=P(K_{1:\ell}\neq\hat{K}_{1:\ell})\leqslant\epsilon$，

随机性 $U(\mathbb{C})=\mathbb{D}(P_{K_{1:\ell}}\|P_{K_{1:\ell}}^{\text{unif}})\leqslant\upsilon$，

保密性 $S(\mathbb{C})=\mathbb{D}(P_{K_{1:\ell}M_{1:\ell}Z^{\ell n}}\|P_{K_{1:\ell}}^{\text{unif}}P_{M_{1:\ell}Z^{\ell n}})\leqslant\xi$，

隐蔽性 $C(\mathbb{C})=\mathbb{D}(P_{Z^{\ell n}}\|Q_Z^{\otimes\ell n})\leqslant\varsigma$，

其中，$P_e(\mathbb{C})$ 代表密钥的解码错误概率，$U(\mathbb{C})$ 代表密钥的随机程度，$S(\mathbb{C})$ 代表密钥泄漏率，$C(\mathbb{C})$ 代表隐蔽概率，则密钥分发方案 $\mathbb{C}$ 被称为隐蔽密钥分发方案.

CSFP 方案由码字构造、编码和解码 3 个阶段组成，通过 ℓ 个消息块的多轮通信生成所需长度的密钥. 首先，Alice 将输入序列 $\{X_j^n,j\in[1,\ell]\}$ 进行极化编码构造出长度为 n 的码字 U_j^n 以及对应的信息比特索引集合和冻结比特索引集合，其中 $U_j^n=X_j^n\boldsymbol{G}_n$ [10]，生成矩阵 $\boldsymbol{G}_n=\boldsymbol{B}_nF^{\otimes\nu}=\boldsymbol{B}_n\begin{bmatrix}1&0\\1&1\end{bmatrix}^{\otimes\nu}$，$\boldsymbol{B}_n$ 为比特置换矩阵. 其次，Alice 通过对信息比特索引集合进行细粒度极化得到若干不同属性的子集，然后从信息比特中提取出密钥并构造出均匀分布的消息块 M_j 发送给 Bob. 最后，Bob 根据接收到的消息块重建码字并提取出密钥. 经过 ℓ 轮通信，Alice 和 Bob 分别获得高度保密的密钥 $K_{1:\ell}$ 和 $\hat{K}_{1:\ell}$. 此时，合法双方的密钥分发过程几乎独立于 Willie 的观测，即 Willie 的最佳统计检验结果相对于盲检验不会存在显著优势，确保 Willie 无法检测到密钥分发协议的执行状态.

4.2　码字构造

对于对称信道，可以采用递归的方式计算出每个极化子信道的巴氏参数（Bhattacharyya Parameter）$\{Z(W_n^{(i)}),i\in[1,n]\}$ 并对其进行排序来构造编码端输入序列 X_j^n，然后挑选出可靠性较高的子信道放置信息比特，其余可靠性较差的子信道放置合法双方都已知的冻结比特. 然而，对于非对称的水声信道，不满足递归计算的前提条件，因此无法直接计算每个极化子信道的巴氏参数. CSFP 方案考虑水声信道的衰落效应，采用信息论的方法推导出信道容量与信道增益的函数关系，通过计算水声信道增益对极化子信道容量进行排序来构造码字.

定理 1.　固定发送功率 $P_s>0$，令最优码字符号分布对应的传输带宽 $B(l,G)=\bigcup_m[f_{ini}^m(l,G),f_{end}^m(l,G)]$，对于信道增益 $G>0$，传输距离 $l>0$，当发送信号的功率谱密度 $S(l,f)>0$ 和噪声功率谱密度 $N(f)>0$ 时，信道容量 $C(l,G)$ 是关于信道增益 G 的严格增函数.

证明.　详见附录 1.

令 $W_n^{(i)}$ 代表第 i 个极化子信道，$I(W_n^{(i)})$ 代表第 i 个极化子信道的信道容量，由于 $C(l,G)$ 是 G 的严格增函数且 $I(W_n^{(i)})=C(l,G^{(i)})$，因此根据式(2)得到的信道增益 $G^{(i)}$ 对极化子信道容量进行排序可以构造出势为 κ 的信息比特索引集合 $\mathcal{A}\subset\{1,...,n\}$ 使得 $\sum_{i\in\mathcal{A}}I(W_n^{(i)})$ 的值最大.

4.3　编码和解码

为了实现水声信道环境下的隐蔽密钥分发，本文将对信息比特索引集合 $\mathcal{A}$ 进行细粒度极化. 首先，定义集合

$$\mathcal{V}_X=\{i\in\mathcal{A}:H(U_i|U^{i-1},R^{i-1})\geqslant1-\delta^n\} \tag{7}$$

$$\mathcal{H}_{X|Y}=\{i\in\mathcal{A}:H(U_i|U^{i-1},R^{i-1},Y^{\mathcal{A}})\geqslant\delta^n\} \tag{8}$$

$$\mathcal{V}_{X|Z}=\{i\in\mathcal{A}:H(U_i|U^{i-1},R_w^{i-1},Z^{\mathcal{A}})\geqslant1-\delta^n\} \tag{9}$$

其中，$\mathcal{H}$ 表示高熵比特索引集合，$\mathcal{V}$ 表示甚高熵比

特索引集合，$U^{i-1}=(U_1,U_2,...,U_{i-1})$，$R_w^{i-1}$ 表示 Alice 与 Willie 之间的信道衰落效应，判决阈值 $\delta^n=2^{-n^\beta}$，其中阈值因子 $0<\beta<1/2$.

CSFP 方案的编码和解码采用图 1 所示的链式结构将 ℓ 个消息块依次链接实现信息比特索引序列的对齐，通过多轮通信生成所需长度的密钥. 在每一轮通信中，对于非对称的水声信道，由于输入序列非先验等概，Alice 将 $U_j^n[\mathcal{A}]$ 中的元素索引划分为甚高熵比特索引集合 $\mathcal{V}_X$ 和近似确定性集合 $\mathcal{V}_X^C$，通过细粒度极化得到以下不同属性的信息比特序列

$$F_j=U_j^n[\mathcal{V}_X\cap\mathcal{H}_{X|Y}\cap\mathcal{V}_{X|Z}] \tag{10}$$

$$\tilde{F}_j=U_j^n[\mathcal{V}_X\cap\mathcal{H}_{X|Y}\setminus\mathcal{V}_{X|Z}] \tag{11}$$

$$E_j=U_j^n[\mathcal{V}_X^C\cap\mathcal{H}_{X|Y}] \tag{12}$$

其中，$j\in[1,\ell]$ 表示通信轮数，F_j 表示满足保密性约束条件但 Bob 无法可靠解码的信息比特序列，$\tilde{F}_j$ 表示不满足保密性约束条件且 Bob 无法可靠解码的信息比特序列，E_j 表示近似确定性集合 $\mathcal{V}_X^C$ 中 Bob 无法可靠解码的信息比特序列. 然后，Alice 根据式(13)从信息比特序列中提取出密钥 K_j，

$$K_j=U_j^n[\mathcal{V}_X\setminus\mathcal{H}_{X|Y}\cap\mathcal{V}_{X|Z}] \tag{13}$$

并根据式(10)~式(13)构造出均匀分布的消息块 M_j 发送给 Bob. Bob 根据接收到的消息块与随机种子构造出其无法可靠解码的码字序列估计值 $\hat{U}_j^n[\mathcal{H}_{X|Y}]$，并通过对数似然比和最大后验概率构造出其能够可靠解码的码字序列估计值 $\hat{U}_j^n[\mathcal{H}_{X|Y}^C]$，最后从重建的码字中提取出与 Alice 相同的密钥.

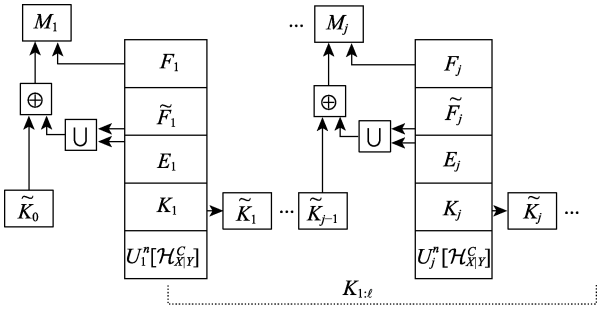

图 1 CSFP 方案编码和解码的链式结构示意图

算法 1 描述了 Alice 的编码过程，共分为 3 个阶段：（1）码字生成；（2）密钥提取；（3）消息生成与发送. 算法的第 1 行开始执行 ℓ 轮循环，第 2 行对编码端输入序列 X_j^n 进行极化编码生成码字 U_j^n，第 3 行从码字 U_j^n 中提取出密钥 K_j，第 4 行~第 6 行获得不同属性的信息比特序列 F_j，$\tilde{F}_j$ 和 E_j，第 7 行~第 8 行生成用于构造链式结构消息块的随机种子 $\tilde{K}_j$，其长度为 $|\mathcal{V}_X\cap\mathcal{H}_{X|Y}\setminus\mathcal{V}_{X|Z}|+|\mathcal{V}_X^C\cap\mathcal{H}_{X|Y}|$，第 9 行~第 10 行将共享随机种子 $\tilde{F}_j$ 与非均匀的信息比特序列 $\tilde{F}_j$ 和 E_j 按比特进行异或生成第 1 个消息块. 其中，$|\tilde{K}_0|=|\mathcal{V}_X\cap\mathcal{H}_{X|Y}\setminus\mathcal{V}_{X|Z}|+|\mathcal{V}_X^C\cap\mathcal{H}_{X|Y}|$，通过消息块的均匀性确保通信的保密性. 第 11 行~第 12 行将第 $j-1$ 轮生成的随机种子 $\tilde{K}_{j-1}$ 与非均匀的信息比特序列 $\tilde{F}_j$ 和 E_j 按比特进行异或生成第 j 轮的消息块，第 13 行~第 16 行将消息块 M_j 发送给 Bob 并获得最终的密钥序列 $K_{1:\ell}=[K_1,K_2,...,K_\ell]$.

算法 1. Alice 编码算法.

输入：码长 n，通信轮数 ℓ，共享随机种子 $\tilde{K}_0$，输入序列 $X_{1:\ell}^n$

输出：密钥序列 $K_{1:\ell}$

(1) FOR $j=1:\ell$

(2) $U_j^n=X_j^n\boldsymbol{G}_n$;

(3) $K_j=U_j^n[\mathcal{V}_X\setminus\mathcal{H}_{X|Y}\cap\mathcal{V}_{X|Z}]$;

(4) $F_j=U_j^n[\mathcal{V}_X\cap\mathcal{H}_{X|Y}\cap\mathcal{V}_{X|Z}]$;

(5) $\tilde{F}_j=U_j^n[\mathcal{V}_X\cap\mathcal{H}_{X|Y}\setminus\mathcal{V}_{X|Z}]$;

(6) $E_j=U_j^n[\mathcal{V}_X^C\cap\mathcal{H}_{X|Y}]$;

(7) $|\tilde{\mathcal{K}}|=|\mathcal{V}_X\cap\mathcal{H}_{X|Y}\setminus\mathcal{V}_{X|Z}|+|\mathcal{V}_X^C\cap\mathcal{H}_{X|Y}|$;

(8) $\tilde{K}_j=U_j^n[\tilde{\mathcal{K}}]$，$\tilde{\mathcal{K}}\subset\mathcal{V}_X\setminus\mathcal{H}_{X|Y}\cap\mathcal{V}_{X|Z}$;

(9) IF $j=1$ THEN

(10) $M_j=[F_j,(\tilde{F}_j\cup E_j)\oplus\tilde{K}_0]$;

(11) ELSE

(12) $M_j=[F_j,(\tilde{F}_j\cup E_j)\oplus\tilde{K}_{j-1}]$;

(13) 发送消息块 M_j 给 Bob;

(14) END IF

(15) END FOR

(16) RETURN $K_{1:\ell}=[K_1,K_2,...,K_\ell]$.

算法 2 描述了 Bob 的解码过程，共分为 2 个阶段：（1）码字重建；（2）密钥提取. 算法的第 1 行开始执行 ℓ 轮循环，第 2 行~第 3 行根据第 1 轮通信接收到的消息块 M_1 与共享随机种子 $\tilde{K}_0$ 构造出高熵比特索引集合 $\mathcal{H}_{X|Y}$ 对应的码字序列估计值 $\hat{U}_1^n[\mathcal{H}_{X|Y}]$，第 4 行~第 6 行 Bob 根据第 j 轮接收到的消息块 M_j 与随机种子 $\hat{\tilde{K}}_{j-1}$ 构造出 $\hat{U}_j^n[\mathcal{H}_{X|Y}]$. 为了构造出剩余的码字序列估计值 $\hat{U}_j^n[\mathcal{H}_{X|Y}^C]$，第 7 行~第 12 行 Bob 利用观测值 y_j^n，已解码出的前序比特 $u_j^{i-1}[\theta]$ 和信道增益 g_j^{i-1}，根据 $\hat{U}_j^n[\mathcal{H}_{X|Y}^C]$ 中的第 i 个比特 $u_{i,j}=0$ 和 $u_{i,j}=1$ 两种情况对解码序列 u_j^{i-1} 进行扩展，计算出解码器列表大小为 θ 时对数似然比 $L_n^{(i,j)}[\theta]$ 以及最大后验概率 $\Pr_{j,\theta}^i$ 对应的码字序列 u_j^i，然后构造出 $\mathcal{H}_{X|Y}^C$ 对应的码字序列估计值 $\hat{U}_j^n[\mathcal{H}_{X|Y}^C]$，使其码字序列的估计值与 Alice 的码字序列之间具有更高的相关性，并根据 $\hat{U}_j^n[\mathcal{H}_{X|Y}]$ 和

$\hat{U}_j^n[\mathcal{H}_{X|Y}^C]$重建码字. 第 13 行从对应属性的信息比特序列估计值中提取出密钥 $\hat{K}_j$，第 14 行~第 16 行生成用于链式构造的随机种子 $\hat{\tilde{K}}_j$，并获得最终的密钥序列 $\hat{K}_{1:\ell}=[\hat{K}_1,\hat{K}_2,...,\hat{K}_\ell]$. Bob 获得的密钥序列 $\hat{K}_{1:\ell}$ 与 Alice 获得的密钥序列 $K_{1:\ell}$ 的一致性将通过 5.1 节中隐蔽密钥分发方案的可靠性进行证明.

算法 2. Bob 解码算法.

输入：码长 n，通信轮数 ℓ，共享随机种子 $\tilde{K}_0$，观测值 $Y_{1:\ell}^n$，接收序列 $M_{1:\ell}$，解码器列表大小 θ

输出：密钥序列 $\hat{K}_{1:\ell}$

(1) FOR $j=1:\ell$

(2) IF $j=1$ THEN

(3) 根据 $(M_1,\tilde{K}_0)$ 构造 $\hat{U}_1^n[\mathcal{H}_{X|Y}]$;

(4) ELSE

(5) 根据 $(M_j,\hat{\tilde{K}}_{j-1})$ 构造 $\hat{U}_j^n[\mathcal{H}_{X|Y}]$;

(6) END IF

(7) IF $i\in\mathcal{H}_{X|Y}^C$ THEN

(8) $L_n^{(i,j)}[\theta]=\ln\dfrac{W_n^{(i)}(y_j^n,g_j^{i-1},u_j^{i-1}[\theta]\,|\,u_{i,j}=0)}{W_n^{(i)}(y_j^n,g_j^{i-1},u_j^{i-1}[\theta]\,|\,u_{i,j}=1)}$;

(9) $\arg\max_\theta \Pr_{j,\theta}^i=\prod_{q=1}^{i}(1+e^{-(1-2u_{q,j}[\theta])*L_n^{(q,j)}[\theta]})^{-1}$;

(10) 根据 $L_n^{(i,j)}[\theta]$ 和 $\arg\max_\theta \Pr_{j,\theta}^i$ 构造 $\hat{U}_j^n[\mathcal{H}_{X|Y}^C]$;

(11) END IF

(12) $\hat{U}_j^n=\hat{U}_j^n[\mathcal{H}_{X|Y}\cup\mathcal{H}_{X|Y}^C]$; //重建码字

(13) $\hat{K}_j=\hat{U}_j^n[\mathcal{V}_X\setminus\mathcal{H}_{X|Y}\cap\mathcal{V}_{X|Z}]$;

(14) $\hat{\tilde{K}}_j=\hat{U}_j^n[\tilde{\mathcal{K}}]$，$\tilde{\mathcal{K}}\subset\mathcal{V}_X\setminus\mathcal{H}_{X|Y}\cap\mathcal{V}_{X|Z}$;

(15) END FOR

(16) RETURN $\hat{K}_{1:\ell}=[\hat{K}_1,\hat{K}_2,...,\hat{K}_\ell]$.

算法 1 和算法 2 中共享随机种子 $\tilde{K}_0$ 的速率可表示为

$$\begin{aligned}
&\lim_{\ell\to\infty}\lim_{n\to\infty}\frac{|\tilde{K}_0|}{n\ell}\\
&=\lim_{\ell\to\infty}\lim_{n\to\infty}\frac{|\mathcal{V}_X\cap\mathcal{H}_{X|Y}\setminus\mathcal{V}_{X|Z}|+|\mathcal{V}_X^C\cap\mathcal{H}_{X|Y}|}{n\ell}\\
&=\lim_{\ell\to\infty}\lim_{n\to\infty}\frac{|\mathcal{H}_{X|Y}|-|\mathcal{V}_X\cap\mathcal{H}_{X|Y}\cap\mathcal{V}_{X|Z}|}{n\ell}\\
&=\lim_{\ell\to\infty}\lim_{n\to\infty}\frac{|\mathcal{H}_{X|Y}|-|\mathcal{H}_{X|Y}\cap\mathcal{V}_{X|Z}|}{n\ell}\\
&=\lim_{\ell\to\infty}\lim_{n\to\infty}\frac{|\mathcal{H}_{X|Y}\setminus\mathcal{V}_{X|Z}|}{n\ell}\\
&\le\lim_{\ell\to\infty}\lim_{n\to\infty}\frac{H(X^{\mathcal{A}}|Y^{\mathcal{A}})}{n\ell}\le\lim_{\ell\to\infty}\lim_{n\to\infty}\frac{\kappa}{n\ell}\to 0.
\end{aligned}$$

由此可见，CSFP 方案所需的共享随机种子 $\tilde{K}_0$ 的速率随着码长或通信轮数的增加而趋近于 0. 因此，CSFP 方案中共享随机种子 $\tilde{K}_0$ 的速率相对于密钥生成速率而言是可以忽略的. 此外，CSFP 方案利用 Alice 和 Bob 共享的随机种子 $\tilde{K}_0$ 对首轮传输的消息块 M_1 进行初始化，第 2 轮至第 ℓ 轮通信时从上一轮生成的密钥 K_{j-1}（$j\in[2,\ell]$）中提取出随机种子 $\tilde{K}_{j-1}$ 对当前轮的消息块 M_j 进行随机化，避免了随机向量的重复使用问题，确保了密钥分发过程的隐蔽性.

4.4 时间复杂度

Alice 编码算法的时间复杂度由极化编码 $U_j^n=X_j^n\boldsymbol{G}_n$ 的时间复杂度和异或运算的时间复杂度构成. 其中，n 表示码字的长度. 在最坏情况下，极化编码 $U_j^n=X_j^n\boldsymbol{G}_n$ 的时间复杂度为 $O(n\log n)$，异或运算的时间复杂度为 $O(n)$. 经过 ℓ 轮通信，得出 Alice 编码算法的时间复杂度为 $O(\ell n(\log n+1))$.

Bob 解码算法的时间复杂度主要由计算最大后验概率 $Pr_{j,\theta}^i$ 的时间复杂度决定. 令 $\chi_\theta(n)$ 表示解码器列表大小为 θ，长度为 n 的码字在最坏情况下每一轮通信中解码算法的时间复杂度. 当 $\theta=1$，$n=2$ 时，$L_2^{(1,j)}[1]=\ln\dfrac{W_2^{(1)}(y_j^2\,|\,u_{1,j}=0)}{W_2^{(1)}(y_j^2\,|\,u_{1,j}=1)}$，$L_2^{(2,j)}[1]=\ln\dfrac{W_2^{(2)}(y_j^2,g_j^1,u_j^1[1]\,|\,u_{2,j}=0)}{W_2^{(2)}(y_j^2,g_j^1,u_j^1[1]\,|\,u_{2,j}=1)}$，因此 $\chi_1(2)=2$；由于 $Pr_{j,\theta}^i$ 的计算包含 $O(\theta n/2\log n)$ 次 $\ln\dfrac{W_n^{(2i-1)}(y_j^n,g_j^{2i-2},u_j^{2i-2}[\theta]\,|\,u_{2i-1,j}=0)}{W_n^{(2i-1)}(y_j^n,g_j^{2i-2},u_j^{2i-2}[\theta]\,|\,u_{2i-1,j}=1)}$ 的计算和 $O(\theta n/2\log n)$ 次 $\ln\dfrac{W_n^{(2i)}(y_j^n,g_j^{2i-1},u_j^{2i-1}[\theta]\,|\,u_{2i,j}=0)}{W_n^{(2i)}(y_j^n,g_j^{2i-1},u_j^{2i-1}[\theta]\,|\,u_{2i,j}=1)}$ 的计算，因此 $\chi_\theta(n)\le 2\chi_\theta(n/2)+O(\theta n)$，再通过递归运算可以推导出 $\chi_\theta(n)\le\theta n\log n$. 经过 ℓ 轮通信，得出 Bob 解码算法的时间复杂度为 $O(\ell\theta n\log n)$.

5 性能分析

本小节从隐蔽密钥分发方案的可靠性、随机性、保密性和隐蔽性 4 个方面对 CSFP 方案进行分析并推导出隐蔽密钥生成速率.

5.1 可靠性

由定义 1 可知，隐蔽密钥分发方案的可靠性 $P_e(\mathbb{C})$ 取决于接收方密钥的解码错误概率，即

$$P_e(\mathbb{C})=P(K_{1:\ell}\ne\hat{K}_{1:\ell}).$$

定义错误事件 $\varepsilon_j\triangleq\{U_j^n\ne\hat{U}_j^n\}$，$f_j\triangleq\{\tilde{F}_j\ne\hat{\tilde{F}}_j\}$ 和 $e_j\triangleq\{E_j\ne\hat{E}_j\}$，可以得到

$$
\begin{aligned}
&P(K_{1:\ell}\neq\hat{K}_{1:\ell})\leqslant P[\bigcup_{j=1}^{\ell}(U_j^n\neq\hat{U}_j^n)]=P\left[\bigcup_{j=1}^{\ell}\varepsilon_j\right]\\
&\overset{(a)}{=}\sum_{j=1}^{\ell}P\left[\varepsilon_j\cap\left(\bigcup_{\varphi=1}^{j-1}\varepsilon_{\varphi}^{C}\right)\right]\overset{(b)}{\leqslant}\sum_{j=1}^{\ell}P(\varepsilon_j)\\
&\overset{(c)}{=}\sum_{j=1}^{\ell}P[\varepsilon_j\,|\,(f_j^C\cap e_j^C)]P(f_j^C\cap e_j^C)\\
&+\sum_{j=1}^{\ell}P[\varepsilon_j\,|\,(f_j\cup e_j)]P(f_j\cup e_j)\\
&\leqslant\sum_{j=1}^{\ell}[P[\varepsilon_j\,|\,(f_j^C\cap e_j^C)]+P(f_j\cup e_j)]\\
&\overset{(d)}{\leqslant}\sum_{j=1}^{\ell}[\kappa\delta^n+P(\varepsilon_{j-1})]\\
&\overset{(e)}{\leqslant}\sum_{j=1}^{\ell}[(j-1)\kappa\delta^n+P(\varepsilon_1)]\\
&=\frac{1}{2}\ell(\ell+1)\kappa\delta^n,
\end{aligned}
$$

其中，(*a*)成立是因为对于每个码字 U_j^n，ε_j 等价为前 $j-1$ 轮解码正确且第 j 轮解码错误；(*b*)成立是由于 $\left[\varepsilon_j\cap\left(\bigcup_{\varphi=1}^{j-1}\varepsilon_{\varphi}^{C}\right)\right]\subset\varepsilon_j$；(*c*)成立是根据全概率公式；(*d*)成立是由于 Bob 通过 $\hat{F}_j$，$\hat{\tilde{F}}_j$ 和 $\hat{E}_j$ 重建码字 $\hat{U}_j^n$ 的错误概率上界为 $\kappa\delta^n$，并且错误事件 f_j 和 e_j 发生的概率取决于Bob对上一轮密钥 $\tilde{K}_{j-1}$ 估计的错误概率，所以 $P_e(\mathbb{C})$ 的上界随着码长增加呈指数下降趋势，当 n 足够大时，$P_e(\mathbb{C})\leqslant\epsilon$.

5.2 随机性

本文采用密钥的真实分布 $P_{K_{1:\ell}}$ 与理想分布 $P_{K_{1:\ell}}^{\text{unif}}$ 的相对熵来衡量密钥的随机性. 根据定义 1，

$$
\begin{aligned}
&U(\mathbb{C})=\mathbb{D}(P_{K_{1:\ell}}\,\|\,P_{K_{1:\ell}}^{\text{unif}})\overset{(a)}{=}|K_{1:\ell}|-H(K_{1:\ell})\\
&\overset{(b)}{=}|K_{1:\ell}|-\sum_{j=1}^{\ell}H(K_j\,|\,K^{j-1})\overset{(c)}{=}|K_{1:\ell}|-\sum_{j=1}^{\ell}H(K_j)\\
&\overset{(d)}{\leqslant}|K_{1:\ell}|-\sum_{j=1}^{\ell}\sum_{i\in\mathcal{V}_{X|Z}\setminus\mathcal{H}_{X|Y}}H(U_{i,j}\,|\,U_j^{i-1},R_{w,j}^{i-1})\\
&\overset{(e)}{\leqslant}|K_{1:\ell}|-|K_{1:\ell}|(1-\delta^n)=|K_{1:\ell}|\delta^n\\
&\leqslant\kappa\ell\delta^n,
\end{aligned}
$$

其中，(*a*)成立是根据信息熵与相对熵的关系；(*b*)成立是根据信息熵的链式法则；(*c*)成立是由于 K_j 独立于 K^{j-1}；(*d*)和(*e*)成立是根据条件减小熵的性质和密钥索引集合的定义，所以 $U(\mathbb{C})$ 的上界随着码长增加呈指数下降趋势，当 n 足够大时，$U(\mathbb{C})\leqslant\upsilon$.

5.3 保密性

当 Willie 能够完全监听合法双方之间的信道时，若密钥 $K_{1:\ell}$ 仍能保持与消息块 $M_{1:\ell}$ 和 Willie 的观测值 $Z^{\ell n}$ 之间的渐近独立性且密钥 $K_{1:\ell}$ 满足均匀分布条件，那么密钥泄漏率 $\lim\limits_{n\to\infty}S(\mathbb{C})=0$. 由算法 1 和算法 2 可得

$$
\begin{aligned}
&S(\mathbb{C})=\mathbb{D}\left(P_{K_{1:\ell}M_{1:\ell}Z^{\ell n}}\,\|\,P_{K_{1:\ell}}^{\text{unif}}P_{M_{1:\ell}Z^{\ell n}}\right)\\
&\overset{(a)}{=}|K_{1:\ell}|-H(K_{1:\ell}\,|\,M_{1:\ell},Z^{\ell n})\overset{(b)}{=}|K_{1:\ell}|-H(K_{1:\ell})+\\
&I(F_{1:\ell},(\tilde{F}_{1:\ell}\cup E_{1:\ell})\oplus\tilde{K}_{0:\ell-1},Z^{\ell n};K_{1:\ell})\\
&\overset{(c)}{\leqslant}\kappa\ell\delta^n+H(K_{1:\ell})-H(K_{1:\ell}\,|\,F_{1:\ell},Z^{\ell n})+\\
&I((\tilde{F}_{1:\ell}\cup E_{1:\ell})\oplus\tilde{K}_{0:\ell-1};K_{1:\ell}|F_{1:\ell},Z^{\ell n})\\
&\overset{(d)}{\leqslant}\kappa\ell\delta^n+|K_{1:\ell}|+|F_{1:\ell}|-H(K_{1:\ell},F_{1:\ell}\,|\,Z^{\ell n})+\\
&I((\tilde{F}_{1:\ell}\cup E_{1:\ell})\oplus\tilde{K}_{0:\ell-1};K_{1:\ell}|F_{1:\ell},Z^{\ell n})\\
&\overset{(e)}{\leqslant}\kappa\ell\delta^n+|K_{1:\ell}|+|F_{1:\ell}|\\
&-\sum_{j=1}^{\ell}\sum_{i\in\mathcal{V}_{X|Z}}H(U_{i,j}\,|\,U_j^{i-1},R_{w,j}^{i-1},Z^{\ell n})\\
&+I((\tilde{F}_{1:\ell}\cup E_{1:\ell})\oplus\tilde{K}_{0:\ell-1};K_{1:\ell}|F_{1:\ell},Z^{\ell n})\\
&=2\kappa\ell\delta^n+I((\tilde{F}_{1:\ell}\cup E_{1:\ell})\oplus\tilde{K}_{0:\ell-1};K_{1:\ell}|F_{1:\ell},Z^{\ell n})\\
&\leqslant 2\kappa\ell\delta^n+I((\tilde{F}_{1:\ell}\cup E_{1:\ell})\oplus\tilde{K}_{0:\ell-1};K_{1:\ell},F_{1:\ell},Z^{\ell n})\\
&\overset{(f)}{\leqslant}2\kappa\ell\delta^n+I(\tilde{K}_{0:\ell-1};K_{1:\ell},F_{1:\ell},Z^{\ell n})\\
&=2\kappa\ell\delta^n+H(\tilde{K}_{0:\ell-1})-H(\tilde{K}_{0:\ell-1}|K_{1:\ell},F_{1:\ell},Z^{\ell n})\\
&\leqslant 2\kappa\ell\delta^n+|\tilde{K}_{0:\ell-1}|-H(\tilde{K}_{0:\ell-1},K_{1:\ell},F_{1:\ell}|Z^{\ell n})+\\
&H(K_{1:\ell},F_{1:\ell}\,|\,Z^{\ell n})\\
&\leqslant 2\kappa\ell\delta^n+|\tilde{K}_{0:\ell-1}|+|K_{1:\ell}|+|F_{1:\ell}|-\\
&\sum_{j=1}^{\ell}\sum_{i\in\mathcal{V}_{X|Z}}H(U_{i,j}\,|\,U_j^{i-1},R_{w,j}^{i-1},Z^{\ell n})\\
&\overset{(g)}{\leqslant}3\kappa\ell\delta^n,
\end{aligned}
$$

其中，(*a*)成立是根据互信息的定义；(*b*)成立是根据信息熵与互信息的关系以及算法 1 中消息块 $M_{1:\ell}$ 的定义；(*c*)成立是由于信息熵与相对熵的关系；(*d*)成立是根据信息熵的链式法则以及 $H(K_{1:\ell})\leqslant|K_{1:\ell}|$，$H(F_{1:\ell}\,|\,Z^{\ell n})\leqslant H(F_{1:\ell})\leqslant|F_{1:\ell}|$；(*e*)成立是根据 $K_{1:\ell}$ 和 $M_{1:\ell}$ 的定义；(*f*) 成立是由于 $\tilde{K}_{0:\ell-1}$ 与 $\tilde{F}_{1:\ell}\cup E_{1:\ell}$ 按比特进行异或操作和互信息的性质；(*g*)成立是根据 $\tilde{K}_{0:\ell-1}$，$K_{1:\ell}$ 和 $F_{1:\ell}$ 的定义以及 $\tilde{\mathcal{K}}\subset\mathcal{V}_X\setminus\mathcal{H}_{X|Y}\cap\mathcal{V}_{X|Z}$，因此 $S(\mathbb{C})$ 的上界随着码长增加呈指数下降趋势，当 n 足够大时，$S(\mathbb{C})\leqslant\xi$.

5.4 隐蔽性

CSFP 方案通过编解码算法使得 Willie 在合法方执行隐蔽密钥分发协议时观测值 $Z^{\ell n}$ 的概率分布 $P_{Z^{\ell n}}$ 与合法方未执行隐蔽密钥分发协议时观测值 $Z^{\ell n}$ 的概率分布 $Q_Z^{\otimes\ell n}$ 之间的差异足够小，从而实现密钥分发过程的隐蔽性. 令 $\Psi=\{\tilde{K}_0,K_{1:\ell-1}\}$，则隐蔽

概率的期望可表示为

$$\begin{aligned}
&\mathbb{E}[C(\mathbb{C})]=\mathbb{E}[\mathbb{D}(P_{Z^{\ell n}}\|Q_Z^{\otimes \ell n})]\\
&\overset{(a)}{=}\mathbb{E}[\mathbb{D}(P_{Z^{\ell n}}\|P_{Z^n}^{\otimes \ell})+\sum_{j=1}^{\ell}\mathbb{D}(P_{Z_j^n}\|Q_{Z_j^n})]\\
&\overset{(b)}{\leqslant}\mathbb{E}[3\kappa\ell\delta^n+\sum_{j=1}^{\ell}\mathbb{D}(P_{Z_j^n}\|Q_{Z_j^n})]\\
&\overset{(c)}{=}3\kappa\ell\delta^n+\mathbb{E}[\sum_{j=1}^{\ell}\log\frac{\sum_{i\in\Psi}\frac{1}{2^{|\Psi|}}Q_{Z_j^n|U_j^n}(z_j^n\,|\,u_j^n(i))}{Q_{Z_j^n}(z_j^n)}]\\
&=3\kappa\ell\delta^n+\\
&\sum_{\psi\in\Psi}\frac{1}{2^{|\Psi|}}\mathbb{E}\left[\sum_{j=1}^{\ell}\log\frac{\sum_{i\in\Psi}Q_{Z_j^n|U_j^n}(z_j^n\,|\,u_j^n(i))}{2^{|\Psi|}Q_{Z_j^n}(z_j^n)}\,|\,\Psi=\psi\right]\\
&\overset{(d)}{\leqslant}3\kappa\ell\delta^n+\\
&\sum_{\psi\in\Psi}\frac{1}{2^{|\Psi|}}\mathbb{E}\left[\sum_{j=1}^{\ell}\log\left(\frac{Q_{Z_j^n|U_j^n}(z_j^n\,|\,u_j^n(\psi))}{2^{|\Psi|}Q_{Z_j^n}(z_j^n)}+1\right)\,|\,\Psi=\psi\right]\\
&=3\kappa\ell\delta^n+\mathbb{E}\left[\sum_{j=1}^{\ell}\log\left(\frac{Q_{Z_j^n|U_j^n}(z_j^n\,|\,u_j^n)}{2^{|\Psi|}Q_{Z_j^n}(z_j^n)}+1\right)\right]\\
&\overset{(e)}{\leqslant}3\kappa\ell\delta^n+\sum_{j=1}^{\ell}\left\{\mathbb{E}\left[\log\frac{Q_{Z_j^n|U_j^n}(z_j^n\,|\,u_j^n)}{2^{|\Psi|}Q_{Z_j^n}(z_j^n)}\right]+1\right\},
\end{aligned}$$

其中，(a)成立是根据 $Q_Z^{\otimes \ell n}=\prod_{j=1}^{\ell}Q_{Z_j^n}$ 时相对熵的链式法则并且 $P_{Z^n}^{\otimes \ell}=\prod_{j=1}^{\ell}P_{Z_j^n}$，$P_{Z^{\ell n}}=\prod_{j=1}^{\ell}P_{Z_j^n|Z_{1:j-1}^n}$；$(b)$成立是由于 $S(\mathbb{C})\leqslant 3\kappa\ell\delta^n$ 且

$$\begin{aligned}
&\mathbb{D}(P_{Z^{\ell n}}\|P_{Z^n}^{\otimes \ell})\overset{(b1)}{\leqslant}\sum_{j=1}^{\ell}\mathbb{E}_{P_{Z_{1:j-1}^n}}[\mathbb{D}(P_{Z_j^n|Z_{1:j-1}^n}\|P_{Z_j^n})]\\
&=\sum_{j=1}^{\ell}\mathbb{D}(P_{Z_{1:j}^n}\|P_{Z_{1:j-1}^n}P_{Z_j^n})\\
&\overset{(b2)}{\leqslant}\sum_{j=1}^{\ell}\mathbb{D}(P_{Z_{1:j}^nF_jK_j}\|P_{Z_{1:j-1}^nF_jK_j}P_{Z_j^n})\\
&\overset{(b3)}{\leqslant}\sum_{j=1}^{\ell}\mathbb{D}(P_{K_jM_jZ_{1:j}^n}\|P_{K_jM_jZ_{1:j-1}^n}P_{Z_j^n})\\
&\leqslant\mathbb{D}(P_{K_{1:\ell}M_{1:\ell}Z^{\ell n}}\|P_{K_{1:\ell}}P_{M_{1:\ell}Z^{\ell n}})\leqslant\\
&\quad\mathbb{D}(P_{K_{1:\ell}M_{1:\ell}Z^{\ell n}}\|P_{K_{1:\ell}}^{\text{unif}}P_{M_{1:\ell}Z^{\ell n}}),
\end{aligned}$$

其中，$(b1)$成立是由于条件增加散度的性质和相对熵的链式法则；$(b2)$成立是根据相对熵的单调性；$(b3)$成立是根据相对熵的链式法则；(c)成立是根据数学期望的性质和信道的转移概率；(d)和(e)成立是由于底数为 2 的对数函数的上凸性质和 Jensen 不等式.

综上可得 $|\Psi|\geqslant\sum_{j=1}^{\ell}I(Z_j^n;U_j^n)+\ell(3\kappa\delta^n+1)$. 当 n 足够大时，$\mathbb{E}[C(\mathbb{C})]$ 趋近于 0，$C(\mathbb{C})\leqslant\varsigma$. 在此基础上，定理 2 给出了隐蔽性约束的可达性条件.

定理 2. 在本文的水声通信系统模型下，若 CSFP 方案中信息比特索引集合的势 κ 和通信轮数 ℓ 满足以下条件，则当码长 n 足够大时，任意小的隐蔽概率 ς 是可达的

$$\kappa\geqslant\frac{(n+1)\ell}{2\ell-3},\ \ell>3.$$

证明.　详见附录 2.

5.5　隐蔽密钥生成速率

经过 ℓ 轮通信后，CSFP 方案的隐蔽密钥生成速率可表示为

$$\begin{aligned}
&\frac{|K_{1:\ell}|}{n\ell}=\frac{\sum_{j=1}^{\ell}|K_j|}{n\ell}=\frac{\sum_{j=1}^{\ell}|\mathcal{V}_X\setminus\mathcal{H}_{X|Y}\cap\mathcal{V}_{X|Z}|}{n\ell}\\
&\overset{(a)}{=}\frac{\sum_{j=1}^{\ell}|\mathcal{V}_{X|Z}\setminus\mathcal{H}_{X|Y}|}{n\ell}=\frac{\sum_{j=1}^{\ell}[|\mathcal{V}_{X|Z}|-|\mathcal{H}_{X|Y}\cap\mathcal{V}_{X|Z}|]}{n\ell}\\
&\geqslant\frac{\sum_{j=1}^{\ell}[|\mathcal{V}_{X|Z}|-|\mathcal{H}_{X|Z}\cap\mathcal{V}_{X|Y}|]}{n\ell}\\
&\geqslant\frac{\sum_{j=1}^{\ell}[|\mathcal{V}_{X|Z}|-|\mathcal{V}_{X|Y}|]}{n\ell}\\
&\overset{(b)}{\geqslant}\frac{\sum_{j=1}^{\ell}[H(X^{\mathcal{A}}|Z^{\mathcal{A}})-\alpha_w^{\kappa}-H(X^{\mathcal{A}}|Y^{\mathcal{A}})]}{n\ell}\\
&\overset{(c)}{\geqslant}\frac{\kappa}{n}\left[\int_{B(l,G)}\log\frac{\rho(l,G)}{\gamma^{-1}N(f)}\mathrm{d}f-\int_{B(l,G_w)}\log\frac{\rho(l,G_w)}{\gamma_w{}^{-1}N_w(f)}-\alpha_w^{\kappa}\right]\\
&\overset{(d)}{\geqslant}\frac{\ell\left[\int_{B(l,G)}\log\frac{\rho(l,G)}{\gamma^{-1}N(f)}\mathrm{d}f-\int_{B(l,G_w)}\log\frac{\rho(l,G_w)}{\gamma_w{}^{-1}N_w(f)}-\alpha_w^{\kappa}\right]}{2\ell-3},
\end{aligned}$$

其中，(a)成立是根据甚高熵索引集合的定义以及 $\mathcal{V}_{X|Z}\subset\mathcal{V}_X$；$(b)$成立是根据附录 2 中 $|\mathcal{V}_{X|Z}|$ 的上下界；(c)成立是根据定理 1 中信息熵与信道容量的关系；(d)成立是根据定理 2 中隐蔽性约束的可达性条件.

6　仿真实验与分析

本节对 CSFP 方案进行仿真实验与结果分析，并通过与文献[25]提出的方案进行对比来验证CSFP方案的性能优势. 文献[25]首次在隐蔽密钥分发方案的编码算法中采用极化码来降低计算复杂度，并通过脉冲位置调制和多级编码构造超级信道实现二进制矢量输入，具有一定的代表性.

6.1 实验环境设置

本文采用 Matlab R2020a 仿真平台和 Bellhop 水声工具箱[30]进行仿真实验. 首先,在 Bellhop 水声工具箱中输入海洋环境参数从而得到多径数目，幅值和时延等信息. 其中，声场环境数据采用了 2018 年 4 月 13 日至 23 日在距离美国罗得岛州纽波特港口 113 km 的东北大陆架附近以 40°15′36″N, 71°05′60″W 为中心的 10 km×10 km 范围进行的海试实测数据[31]，水体环境配置部分采用了 2018 年 4 月 21 日在水体深度 110 m 范围内的声速剖面数据，试验时的海况等级为 3 级，浪高 0.5-1.25 m，风速 10 m/s，海底沉积物层的地质声学特征为泥沙型底质，水流的最高速度为 2.5 m/s，发送方布放位置的水体深度为 38 m，接收方和非法检测方布放位置的水体深度为 40 m，信号的中心频率为 18.75 kHz，采样频率为 80 kHz,探测信号持续时间为 0.528 s. 其它实验参数的默认值设置如表 1 所示，其中，合法方共享的随机种子采用水声信道环境中的热噪声作为随机源来生成[32]，其统计特性服从高斯分布，确保所产生的随机序列无法预知且不可再现，所选海域传播损失变化情况如图 2 所示.

表 1 环境参数设置

参数	值
发送方与接收方的传输距离	500 m
发送方与非法检测方的传输距离	800 m
环境噪声	47.9 dB/ Hz re 1μPa
带宽	4 kHz
极化码码长	2^6-2^{10}
随机种子长度	64 bits
通信轮数	10
调制方式	BPSK
解码器列表大小	2

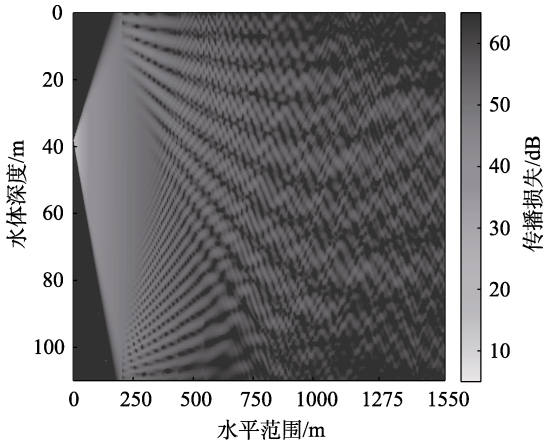

图 2 所选海域传播损失变化情况示意图

6.2 实验结果与分析

实验首先考察了图 2 条件下发送方与接收方在不同传输距离下信道冲激响应（Channel Impulse Response，CIR）的幅值，即信道衰落过程的幅度变化. 从图 3 中可以看出，(a)和(b)两种情况下，CIR 的归一化峰值出现的位置近似相同. 然而，随着传输距离的增大，CIR 曲线的波动幅度更大，并且波动持续时间更长，说明多径分量构成的散射分量功率在总接收功率中的比例增加，信道容量会随之减少.

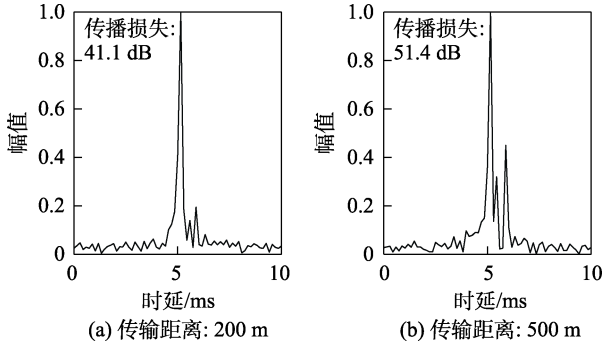

图 3 发送方与接收方在不同传输距离下的信道冲激响应

图 4 描绘了不同阈值因子下判决阈值与码长的函数关系. 从图 4 中可以看出，当阈值因子 β 固定时，判决阈值随着码长的增加而减少，这是因为判决阈值作为信息比特解码错误概率的上界，是一个底数小于 1,指数与码长正相关的下凸函数. 根据大数定理,随着码长的增加,解码错误概率会降低. 此外，当码长固定时，阈值因子越大，判决阈值越小，这是因为判决阈值是一个底数小于 1，指数与阈值因子正相关的下凸函数，随着阈值因子的增加，解码错误概率也会降低.

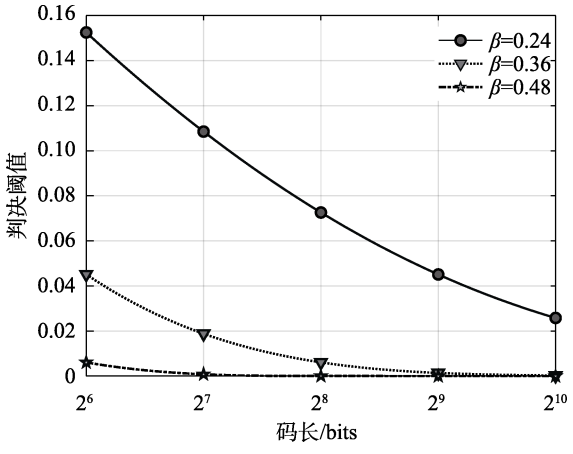

图 4 不同阈值因子下判决阈值与码长的函数关系

图 5 描绘了不同阈值因子下误码率与码长的函数关系. 由图 5 可知,随着码长的增加或阈值因子 β 的增加，误码率会随之下降. 在码长和阈值因子相同的情况下，CSFP 方案的误码率比文献[25]的误码率更低，这是因为在 CSFP 方案中，接收方根据观测值和信道增益计算出最大后验概率对应的码字序列，使其密钥序列的估计值与发送方的密钥序列之间的相关性提高，而文献[25]采用 SC 解码算法，其当前比特的错误判决会影响到下一个比特的判决从而导致误码扩散.

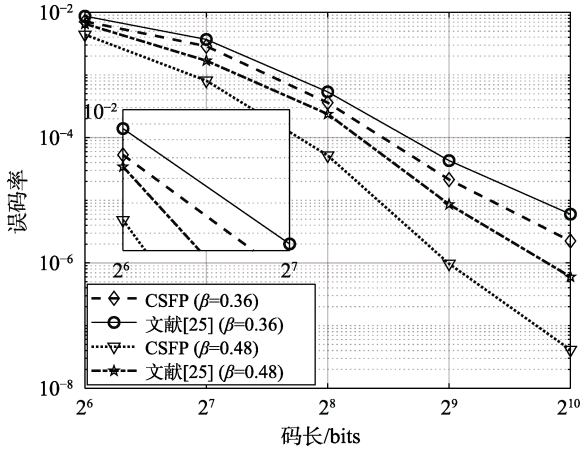

图 5　不同阈值因子下误码率与码长的函数关系

本文采取每次信道使用所传输的密钥比特（Bits Per Channel Use，BPCU）[33]作为隐蔽密钥生成速率的评价指标. 图 6 描绘了不同阈值因子下隐蔽密钥生成速率与码长的函数关系. 由图 6 可见，当阈值因子固定时，隐蔽密钥生成速率随着码长的增加而增加，这是因为随着码长的增加，极化子信道的容量更接近信息传输速率的香农极限，因此隐蔽密钥生成速率也随之增加. 此外，当码长固定时，阈值因子越大，隐蔽密钥生成速率越低，这是因为阈值因子的增大会导致信息比特索引集合细粒度极化后的密钥子集中满足条件的比特数减少，因此隐蔽密钥生成速率会降低.

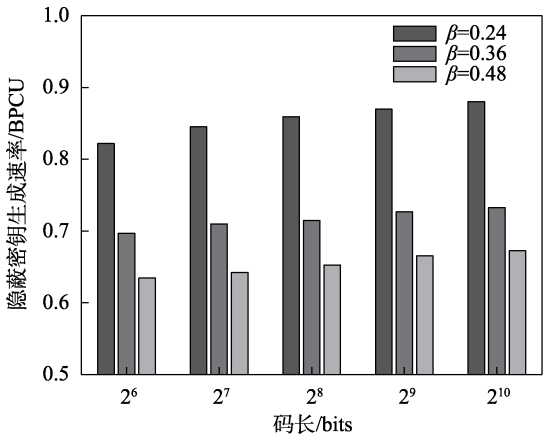

图 6　隐蔽密钥生成速率与码长的函数关系

图 7 描绘了码长为 1024 比特，阈值因子 β 为 0.36时的隐蔽密钥生成速率与传输距离的函数关系. 从图 7 中可以看出，当传输距离最短时，隐蔽密钥生成速率最大，这是因为此时水声信道环境下由传输距离导致的路径损失最小. 随着传输距离的增加，水下传播损失整体呈波动性上升趋势，导致隐蔽密钥生成速率整体呈波动性下降趋势，这是因为水声环境下的吸收损耗也会对传播损失产生影响并导致波动性. 与文献[25]相比，CSFP 方案的隐蔽密钥生成速率平均提升了 18.78%，并且波动幅度比文献[25]中的方案低 23.63%，说明 CSFP 方案在水声信道环境下具有更高的稳定性，这是因为在 CSFP 方案中，接收方在计算密钥序列估计值时利用了信道增益信息，因此与 Alice 的密钥序列之间具有更高的相关性，隐蔽密钥生成速率也就更高. 此外，由于信道增益的计算过程中考虑了多径数目、传输时延和水下传播损失等因素，因此 CSFP 方案的隐蔽密钥生成速率整体变化幅度更为平缓.

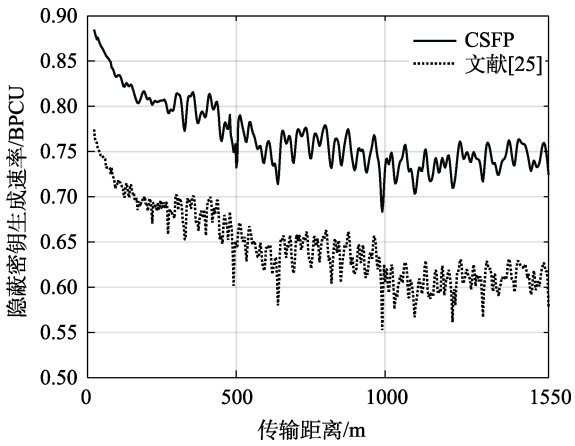

图 7　隐蔽密钥生成速率与传输距离的函数关系

本文采用隐蔽概率来衡量隐蔽密钥分发方案的隐蔽性. 隐蔽概率越低，说明 Willie 在合法方未执行密钥分发协议时观测到的概率分布与合法方执行密钥分发协议时观测到的概率分布之间的差异越小，因此方案的隐蔽性越高. 图 8 描绘了不同阈值因子下隐蔽概率与码长的函数关系. 从图 8 可以看出，当阈值因子固定时，隐蔽概率随着码长增加呈指数下降趋势，此时合法方执行密钥分发协议时的隐蔽性会随之提高. 当码长固定时，隐蔽概率会随

着阈值因子的增加而降低，这是因为阈值因子的增加会导致式(9)中判决阈值的减少，因此甚高熵索引集合 $\mathcal{V}_{X|Z}$ 中满足条件的索引元素对应的比特信息熵更高，使得 Willie 对于合法方传输的消息块的不确定性增加，因此隐蔽性也随之提高. 与文献[25]相比，CSFP 方案的隐蔽性平均提高了 38.29%，这是因为 CSFP 方案考虑了水声信道的非对称性，通过细粒度极化将密钥分发过程中所有非均匀的信息比特序列进行异或处理，使得生成的消息块的概率分布与合法方未执行密钥分发协议时非法检测方观测到的概率分布差异变小.

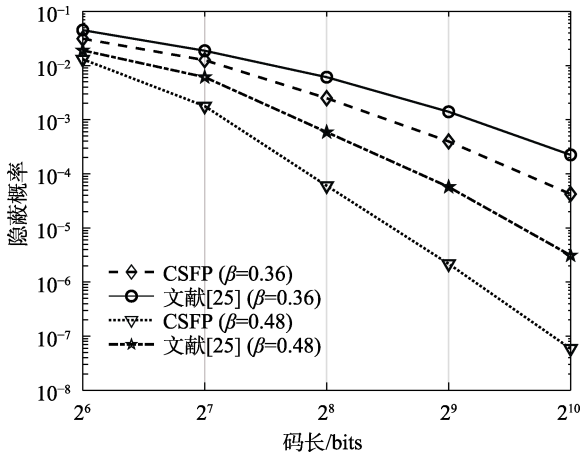

图 8 不同阈值因子下隐蔽概率与码长的函数关系

本文采用美国国家标准与技术研究院（National Institute of Standards and Technology，NIST）发布的 SP 800-22 随机性测试平台对不同方案生成的密钥序列进行随机性检测[34]. 随机性评价标准包括密钥序列的分布一致性和不可预测性. NIST 每一项统计测试都对应一类统计假设检验，零假设表示被检测的序列为随机序列，将拒绝零假设的错误概率称为测试的显著性水平，其缺省值为 0.01. 表 2 给出了 CSFP 方案与文献[25]在 NIST SP 800-22 随机性测试平台上的随机性检测结果. 实验设定码长为 1024 比特，通信轮数为 10，表中的每一项数据为对应的统计测试项目的 p 值. 若 p 值大于 0.01，则接受零假设；若 p 值小于 0.01，则拒绝零假设.

当阈值因子为 0.36 时，文献[25]平均提取出 6450 比特密钥序列，CSFP 方案平均提取出 7500 比特密钥序列；当阈值因子为 0.48 时，文献[25]平均提取出 6069 比特密钥序列，CSFP 方案平均提取出 6885 比特密钥序列，说明在阈值因子相同的情况下，CSFP 方案具有更高的密钥生成速率，并且阈值因子越小，密钥生成速率越高.

表 2 NIST SP 800-22 随机性检测结果

统计测试	CSFP (β=0.36) 7500 比特	文献[25] (β=0.36) 6450 比特	CSFP (β=0.48) 6885 比特	文献[25] (β=0.48) 6069 比特
频数	**0.515859**	**0.130908**	**0.869939**	**0.255519**
块内频数（m=128）	**0.522930**	**0.101478**	**0.804337**	**0.132917**
离散傅里叶变换	0.475406	0.265254	0.576177	0.351528
近似熵（m=2）	0.582340	0.253394	0.992998	0.496032
累加和（前向）	**0.458089**	**0.039670**	**0.812694**	**0.060044**
累加和（后向）	**0.774091**	**0.169473**	**0.917579**	**0.193323**
序列（m=5）	0.657213 0.494657	0.280207 0.167993	0.714594 0.793150	0.321369 0.303950
块内游程（m=8）	0.758925	0.245619	0.889396	0.309855
游程	0.150875	0.148689	0.646303	0.634087

在表 2 的 9 项测试中，在阈值因子相同的情况下，相较于文献[25]，CSFP 方案取得了更高的 p 值，说明 CSFP 方案提取出的密钥序列具有更强的随机性. 下面针对 p 值提升最大的 4 项测试进行分析. 其中，频数测试与块内频数测试用于评价密钥序列的分布一致性，即密钥序列中“0”码和“1”码分布的均衡性. 由于文献[25]采用的 SC 解码算法存在的误码扩散问题会导致较高的误码率，使得满足可靠性约束的密钥序列比特数随之减少，导致密钥的真实分布与理想分布的差异增加，因此 p 值低于 CSFP 方案. 累加和测试用于评价密钥序列的不可预测性，分为前向和后向两种情况. CSFP 方案基于水声信道的衰落效应进行码字构造，其物理层信道固有的随机性确保了密钥序列的前向不可预测性，即对当前密钥序列不存在任何先验知识的情况下，无法预测密钥序列的下一比特输出，并且 CSFP 方案采用链式结构在每一轮传输中生成新的密钥，通过避免随机种子的重复使用实现后向不可预测性，即从当前生成的密钥序列无法推导出以前的密钥序列，因此比文献[25]的方案具有更强的不可预测性.

接下来分析不同阈值因子对 CSFP 方案的影响. 由表 2 可知，当 β=0.48 时，各项统计测试的 p 值均高于 β=0.36 时的 p 值，说明提取出的密钥序列具有更强的随机性，这是因为合法方基于阈值因子进行信息比特索引集合的细粒度极化来构造消息块，随着阈值因子的增加，合法方的保密性约束增强，导

致 Willie 对该消息块的不确定性增加.

6.3 讨　论

声波在海水中传播时，由于海水分层介质的折射以及海面与海底的反射，发送方与接收方之间的信道存在多个路径分量（视距分量和散射分量），且不同路径分量的幅度峰值直接影响到信道增益的计算结果. 由定理 1 可知，信道容量是关于信道增益的严格增函数，因此信道增益的大小也会影响到信道容量的取值. 相对而言，浅海边界条件复杂，水中散射体多，介质分布不均匀，因此声传播条件较深海恶劣. 在浅海远距离传播情况下，视距分量的幅度峰值趋近于零，水声信号的衰落趋于瑞利（Rayleigh）分布，表征衰落最严重，信道增益和信道容量取得最小值；在深海近距离传播情况下，视距分量的幅度峰值趋近于最大，水声信号的衰落趋于高斯分布，表示视距分量非常强，信道增益和信道容量取得最大值；在浅海近距离和深海远距离传播情况下，发送方与接收方之间存在一个占支配地位的视距分量和若干散射分量，水声信号的衰落呈现莱斯（Rician）分布，信道增益和信道容量的取值介于两者之间.

7 总 结

为了解决现有密钥分发协议在水声信道环境下的信息泄露问题，本文从水声信道的物理特性出发，提出一种基于细粒度极化的隐蔽密钥分发方案. 该方案由码字构造、编码和解码 3 个阶段组成，通过多轮通信生成所需长度的密钥. 码字构造阶段，利用莱布尼兹积分法则和黎曼积分的保号性推导出信道容量与信道增益的函数关系，通过计算水声信道增益对极化子信道的容量进行排序来构造码字，确保信息传输速率达到香农极限；编码阶段，合法发送方通过对信息比特索引集合进行细粒度极化得到若干不同属性的子集，然后从信息比特中提取出密钥序列并构造出均匀分布的消息块发送给合法接收方，确保密钥分发过程的隐蔽性；解码阶段，合法接收方首先根据接收到的消息块与随机种子构造出一部分码字序列估计值，然后根据观测值和信道增益，利用对数似然比计算出最大后验概率对应的码字序列构造出另一部分码字序列估计值，来重建码字并提取出密钥序列. 理论分析和实验结果验证了该方案的性能.

致　谢　衷心感谢评审专家和编辑们对本文提出的宝贵意见和建议!

参　考　文　献

[1] Duan Rui-Yang, Wang Jing-Jing, Du Jun, et al. New marine information network for realizing all-coverage over sea. Journal on Communications, 2019, 40(4): 10-20 (in Chinese)
(段瑞洋, 王景璟, 杜军等. 面向“三全”信息覆盖的新型海洋信息网络. 通信学报, 2019, 40(4): 10-20)

[2] Diamant R, Casari P, Tomasin S. Cooperative authentication in underwater acoustic sensor networks. IEEE Transactions on Wireless Communications, 2019, 18(2): 954-968

[3] Zhang Sheng-Jun, Jin Liang, Huang Yu, et al. Nonagreement secret key generation based on spatial symmetric scrambling and secure polar coding. SCIENTIA SINICA Informationis, 2019, 49(4): 486-502 (in Chinese)
(张胜军, 金梁, 黄宇等. 基于空域对称加扰和安全极化编码的无协商密钥生成方法. 中国科学:信息科学, 2019, 49(4): 486-502)

[4] Wei Zhi-Qiang, Yang Guang, Cong Yan-Ping. Research on the security of underwater sensor networks. Chinese Journal of Computers, 2012, 35(8): 1594-1606 (in Chinese)
(魏志强, 杨光, 丛艳平. 水下传感器网络安全研究. 计算机学报, 2012, 35(8): 1594-1606)

[5] Lal C, Petroccia R, Pelekanakis K, et al. Toward the development of secure underwater acoustic networks. IEEE Journal of Oceanic Engineering, 2017, 42(4): 1075-1087

[6] Wu Hua, Wang Xiang-Bin, Pan Jian-Wei. Quantum communication: status and prospects. SCIENTIA SINICA Informationis, 2014, 44(3): 296-311 (in Chinese)
(吴华, 王向斌, 潘建伟. 量子通信现状与展望. 中国科学:信息科学, 2014, 44(3): 296-311)

[7] Lin Yu-Da, Jin Liang, Zhou You, et al. Performance analysis of covert wireless communication based on beam forming with noise uncertainty. Journal on Communications, 2020, 41(7): 49-58 (in Chinese)
(林钰达, 金梁, 周游等. 噪声不确定时基于波束成形的隐蔽无线通信性能分析. 通信学报, 2020, 41(7): 49-58)

[8] Kadampot A, Tahmasbi M, Bloch M R. Multilevel-coded pulse-position modulation for covert communications over binary-input discrete memoryless channels. IEEE Transactions on Information Theory, 2020, 66(10): 6001-6023

[9] Tahmasbi M, Bloch M R. Covert secret key generation with an active warden. IEEE Transactions on Information Forensics and Security, 2020, 15: 1026-1039

[10] Bash B A, Goeckel D, Towsley D. Limits of reliable communication with low probability of detection on AWGN channels. IEEE Journal on Selected Areas in Communications, 2013, 31(9): 1921-1930

[11] Koyluoglu O O, El Gamal H. Polar coding for secure transmission and key agreement//Proceedings of the 21st Annual IEEE International Symposium on Personal, Indoor and Mobile Radio Communications. Istanbul, Turkey, 2010: 2698-2703

[12] Arikan E. Channel Polarization: A method for constructing capacity-achieving codes for symmetric binary-input memoryless channels. IEEE Transactions on Information Theory, 2009, 55(7): 3051-3073

[13] Bioglio V, Condo C, Land I. Design of polar codes in 5G new radio. IEEE Communications Surveys & Tutorials, 2021, 23(1):

29-40
[14] Hassani S H, Urbanke R. Universal polar codes//Proceedings of the IEEE International Symposium on Information Theory. Honolulu, USA, 2014: 1451-1455
[15] Chan H, Gligor V D, Perrig A, et al. On the distribution and revocation of cryptographic keys in sensor networks. IEEE Transactions on Dependable and Secure Computing, 2005, 2(3): 233-247
[16] Wang S, Yin Z Q, He D Y, et al. Twin-field quantum key distribution over 830-km fibre. Nature Photonics. 2022, 16: 154-161
[17] Dai Qiao, Song Hua-Wei, Jin Liang, et al. Physical-layer authentication and key distribution mechanism based on equivalent channel. SCIENTIA SINICA Informationis, 2014, 44(12): 1580-1592 (in Chinese)
(戴峤, 宋华伟, 金梁等. 基于等效信道的物理层认证和密钥分发机制. 中国科学:信息科学, 2014, 44(12): 1580-1592)
[18] Liu B, Hu A. Secret key distribution protocol in MIMO systems with 3D-3GPP channel model//Proceedings of the 6th IEEE International Conference on Computer and Communications. Chengdu, China, 2020: 177-181
[19] Merhav N. On the Shannon cipher system with a capacity-limited key-distribution channel. IEEE Transactions on Information Theory, 2006, 52(3): 1269-1273
[20] Muramatsu J, Yoshimura K, Davis P, et al. Secret-key distribution based on bounded observability. Proceedings of the IEEE, 2015, 103(10): 1762-1780
[21] Hussain M, Michelusi N. Energy-efficient interactive beam alignment for millimeter-wave networks. IEEE Transactions on Wireless Communications, 2019, 18(2): 838-851
[22] Wang J, Tang W, Zhu Q, et al. Covert communication with the help of relay and channel uncertainty. IEEE Wireless Communications Letters, 2019, 8(1): 317-320
[23] Mahdavifar H, Vardy A. Achieving the secrecy capacity of wiretap channels using polar codes. IEEE Transactions on Information Theory, 2011, 57(10): 6428-6443
[24] Chou R A, Bloch M R, Abbe E. Polar coding for secret-key generation. IEEE Transactions on Information Theory, 2015, 61(11): 6213-6237
[25] Kadampot I A, Bloch M R. Forward reconciliation for covert key generation//Proceedings of the IEEE Information Theory Workshop. Visby, Sweden, 2019: 1-5
[26] Honda J, Yamamoto H. Polar coding without alphabet extension for asymmetric models. IEEE Transactions on Information Theory, 2013, 59(12): 7829-7838
[27] Petroccia R, Petrioli C, Potter J. Performance evaluation of underwater medium access control protocols: at-sea experiments. IEEE Journal of Oceanic Engineering, 2018, 43(2): 547-556
[28] Qarabaqi P, Stojanovic M. Statistical characterization and computationally efficient modeling of a class of underwater acoustic communication channels. IEEE Journal of Oceanic Engineering, 2013, 38(4): 701-717
[29] Han G, Shen S, Song H, et al. A stratification-based data collection scheme in underwater acoustic sensor networks. IEEE Transactions on Vehicular Technology, 2018, 67(11): 10671-10682
[30] Porter M B. The BELLHOP manual and user's guide: preliminary draft. La Jolla, CA, USA: Heat, Light, and Sound Research Incorporated, Technical Report: HLS-2010-1 , 2011
[31] Liu Z, Emokpae L E, Schindall J A, et al. Experimental study of acoustic channel reciprocity in the shallow ocean. IEEE Journal of Oceanic Engineering, 2021, 46(3): 1034-1044
[32] Robson S, Leung B, Gong G. Truly random number generator based on a ring oscillator utilizing last passage time. IEEE Transactions on Circuits and Systems II: Express Briefs. 2014, 61(12): 937-941
[33] Xu P, Cumanan K, Ding Z, et al. Group secret key generation in wireless networks: algorithms and rate optimization. IEEE Transactions on Information Forensics and Security, 2016, 11(8): 1831-1846
[34] Bassham L E, Rukhin A L, Soto J, et al. A statistical test suite for random and pseudorandom number generators for cryptographic applications. Gaithersburg, MD, USA: Department of Commerce, National Institute of Standards and Technology, Technical Report: Special Publication 800-22 revision 1a, 2010
[35] Proakis J G, Salehi M. Digital communications. Fifth Edition, New York, USA: McGraw-Hill, 2001

附录1. 定理1的证明

证明. 根据式(5)可将接收功率表示为 $P_r = GP_s = G = P_{los} + P_{dif}$，其中 P_{los} 表示在多径信号中占支配地位的视距（Line Of Sight，LOS）分量功率，P_{dif} 表示由其余多径分量构成的散射分量功率，因此

$$G = \int_{B(l,G)} S_{los}(l,G,f)\mathrm{d}f + \int_{B(l,G)} S_{dif}(l,G,f)\mathrm{d}f \tag{14}$$

根据条件 $B(l,G) = \cup_m [f_{ini}^m(l,G), f_{end}^m(l,G)]$，为了使得信息传输速率达到香农极限，利用注水原理推导出信道容量为

$$C(l,G) = \int_{B(l,G)} \log \frac{\rho(l,G)}{(S_{los}(l,G,f) + S_{dif}(l,G,f))^{-1} N(f)} \mathrm{d}f \tag{15}$$

功率谱密度可表示为[35]

$$S(l,f) = [\rho(l,G) - \frac{N(f)}{S_{los}(l,G,f) + S_{dif}(l,G,f)}]^+ \tag{16}$$

其中 $\rho(l,G)$ 能够使得发送功率 $P_s = \int_{B(l,G)} S(l,f)\mathrm{d}f$.

令 $\gamma_{ini}^m \triangleq S_{los}(l,G,f_{ini}^m(l,G)) + S_{dif}(l,G,f_{ini}^m(l,G))$，$\gamma_{end}^m \triangleq S_{los}(l,G,f_{end}^m(l,G)) + S_{dif}(l,G,f_{end}^m(l,G))$，$\gamma \triangleq S_{los}(l,G,f) + S_{dif}(l,G,f)$，则发送功率可表示为

$$P_s = \sum\nolimits_m \int_{f_{ini}^m(l,G)}^{f_{end}^m(l,G)} S(l,f)\mathrm{d}f \tag{17}$$

式(14)可简化表示为

$$G = \sum\nolimits_m \int_{f_{ini}^m(l,G)}^{f_{end}^m(l,G)} \gamma \mathrm{d}f \tag{18}$$

式(15)可简化表示为

$$C(l,G)=\sum\nolimits_m\int_{f_{ini}^m(l,G)}^{f_{end}^m(l,G)}\log\left(\frac{\rho(l,G)}{\gamma^{-1}N(f)}\right)\mathrm{d}f \tag{19}$$

其中，$S(l,f)$ 和 $N(f)$ 独立于 G. 根据莱布尼兹积分法则以及条件 $\rho(l,G)=(\gamma_{ini}^m)^{-1}N(f_{ini}^m(l,G))$ 和 $\rho(l,G)=(\gamma_{end}^m)^{-1}\cdot N(f_{end}^m(l,G))$，式(17)~(19)分别对 G 求导可得

$$0=\sum\nolimits_m\left[S(l,f_{end}^m(l,G))\frac{\partial f_{end}^m(l,G)}{\partial G}-S(l,f_{ini}^m(l,G))\frac{\partial f_{ini}^m(l,G)}{\partial G}\right] \tag{20}$$

$$1=\sum\nolimits_m\left(\gamma_{end}^m\frac{\partial f_{end}^m(l,G)}{\partial G}-\gamma_{ini}^m\frac{\partial f_{ini}^m(l,G)}{\partial G}+\int_{f_{ini}^m(l,G)}^{f_{end}^m(l,G)}\frac{\partial\gamma}{\partial G}\mathrm{d}f\right) \tag{21}$$

$$\begin{aligned}\frac{\partial C(l,G)}{\partial G}=&\sum\nolimits_m\left(\log\frac{\rho(l,G)}{(\gamma_{end}^m)^{-1}N(f_{end}^m(l,G))}\frac{\partial f_{end}^m(l,G)}{\partial G}\right.\\&-\log\frac{\rho(l,G)}{(\gamma_{ini}^m)^{-1}N(f_{ini}^m(l,G))}\frac{\partial f_{ini}^m(l,G)}{\partial G}\\&\left.+(\ln 2)^{-1}\int_{f_{ini}^m(l,G)}^{f_{end}^m(l,G)}\frac{S(l,f)}{\rho(l,G)\gamma}\frac{\partial\gamma}{\partial G}\mathrm{d}f\right)\end{aligned} \tag{22}$$

由于对数函数的等价无穷小 $\lim\limits_{a\to0}\log(1+a)\sim a/\ln 2$ 并且 $\gamma^{-1}N(f)>0$，将式(20)代入式(22)可得

$$\begin{aligned}\frac{\partial C(l,G)}{\partial G}\cong&(\ln 2)^{-1}\sum\nolimits_m\left[\left(\frac{S(l,f_{end}^m(l,G)(\gamma_{end}^m))}{N(f_{end}^m(l,G))}\right)\right.\\&\cdot\frac{\partial f_{end}^m(l,G)}{\partial G}-\left(\frac{S(l,f_{ini}^m(l,G)(\gamma_{ini}^m))}{N(f_{ini}^m(l,G))}\right)\frac{\partial f_{ini}^m(l,G)}{\partial G}\\&\left.+\int_{f_{ini}^m(l,G)}^{f_{end}^m(l,G)}\frac{S(l,f)}{\rho(l,G)\gamma}\frac{\partial\gamma}{\partial G}\mathrm{d}f\right]\\=&(\ln 2)^{-1}\sum\nolimits_m[(S(l,f_{end}^m(l,G))\rho^{-1}(l,G))\frac{\partial f_{end}^m(l,G)}{\partial G}\\&-(S(l,f_{ini}^m(l,G)\rho^{-1}(l,G))\frac{\partial f_{ini}^m(l,G)}{\partial G}\\&+\int_{f_{ini}^m(l,G)}^{f_{end}^m(l,G)}\frac{S(l,f)}{\rho(l,G)\gamma}\frac{\partial\gamma}{\partial G}\mathrm{d}f]\\=&\frac{(\ln 2)^{-1}}{\rho(l,G)}\sum\nolimits_m\int_{f_{ini}^m(l,G)}^{f_{end}^m(l,G)}S(l,f)\gamma^{-1}\frac{\partial\gamma}{\partial G}\mathrm{d}f\end{aligned} \tag{23}$$

由式(4)易得介质吸收系数 $\alpha(f)$ 为 f 的增函数，因此 γ 为 f 的减函数，再由式(20)可得

$$\sum\nolimits_m\left(\gamma_{end}^m\frac{\partial f_{end}^m(l,G)}{\partial G}-\gamma_{ini}^m\frac{\partial f_{ini}^m(l,G)}{\partial G}\right)<0 \tag{24}$$

根据黎曼积分的保号性，并将式(21)和式(24)代入式(23)可得

$$\frac{\partial C(l,G)}{\partial G}>\frac{(\ln 2)^{-1}}{\rho(l,G)}\sum\nolimits_m\int_{f_{ini}^m(l,G)}^{f_{end}^m(l,G)}S(l,f)\gamma^{-1}\mathrm{d}f>0.$$

证毕.

附录 2. 定理 2 的证明

证明. 由 5.4 节推导结果可知，对于 ℓ 轮传输过程，CSFP 方案满足隐蔽性约束 $C(\mathbb{C})\leqslant\varsigma$ 时，

$$|\Psi|=|\tilde{K}_0|+|K_{1:\ell-1}|\geqslant\sum_{j=1}^{\ell}I(Z_j^n;U_j^n)+\ell(3\kappa\delta^n+1) \tag{25}$$

将式(11)~式(13)代入式(25)可得

$$\begin{aligned}&(\ell-1)|\mathcal{V}_X\setminus\mathcal{H}_{X|Y}\cap\mathcal{V}_{X|Z}|+|\mathcal{V}_X\cap\mathcal{H}_{X|Y}\setminus\mathcal{V}_{X|Z}|+\\&|\mathcal{V}_X^C\cap\mathcal{H}_{X|Y}|-\sum_{j=1}^{\ell}I(Z_j^n;U_j^n)-\ell(3\kappa\delta^n+1)\geqslant0\end{aligned} \tag{26}$$

由于 $|\mathcal{H}_{X|Y}\cap\mathcal{V}_{X|Z}|\leqslant|\mathcal{H}_{X|Y}\cap\mathcal{V}_{X|Y}|=|\mathcal{V}_{X|Y}|$，故式(26)左边可表示为

$$\begin{aligned}&(\ell-1)[|\mathcal{V}_{X|Z}|-|\mathcal{V}_{X|Z}\cap\mathcal{H}_{X|Y}|]+|\mathcal{H}_{X|Y}|-|\mathcal{V}_{X|Z}\cap\mathcal{H}_{X|Y}|-\\&\sum_{j=1}^{\ell}I(Z_j^n;U_j^n)-\ell(3\kappa\delta^n+1)\geqslant(\ell-1)[|\mathcal{V}_{X|Z}|-|\mathcal{V}_{X|Y}|]+\\&|\mathcal{H}_{X|Y}|-|\mathcal{V}_{X|Y}|-\sum_{j=1}^{\ell}I(Z_j^n;U_j^n)-\ell(3\kappa\delta^n+1)\end{aligned} \tag{27}$$

为了分析 $|\mathcal{V}_{X|Z}|$ 和 $|\mathcal{V}_{X|Y}|$ 的上下界，首先计算出 $\sum\limits_{i\in\mathcal{A}}H(U_i|U^{i-1},R^{i-1},Y^{\mathcal{A}})$ 取值范围的上下界. 根据信息熵的链式法则和互信息的定义，可得

$$\begin{aligned}&\sum_{i\in\mathcal{A}}H(U_i|U^{i-1},R^{i-1},Y^{\mathcal{A}})\geqslant\sum_{i\in\mathcal{A}}H(U_i|U^{i-1},R^{\mathcal{A}},Y^{\mathcal{A}})\\&=H(U^{\mathcal{A}}|R^{\mathcal{A}},Y^{\mathcal{A}})=H(U^{\mathcal{A}}|Y^{\mathcal{A}})-I(U^{\mathcal{A}};R^{\mathcal{A}}|Y^{\mathcal{A}})\\&=\sum_{i\in\mathcal{A}}H(U_i|U^{i-1},Y^{\mathcal{A}})-I(U^{\mathcal{A}};R^{\mathcal{A}}|Y^{\mathcal{A}})\end{aligned} \tag{28}$$

再根据互信息的定义和信息熵的非负性，式(28)可转化为

$$\begin{aligned}&\sum_{i\in\mathcal{A}}H(U_i|U^{i-1},R^{i-1},Y^{\mathcal{A}})\geqslant\\&\sum_{i\in\mathcal{A}}H(U_i|U^{i-1},Y^{\mathcal{A}})-H(R^{\mathcal{A}}|Y^{\mathcal{A}})\\&+H(R^{\mathcal{A}}|U^{\mathcal{A}},Y^{\mathcal{A}})\geqslant\sum_{i\in\mathcal{A}}H(U_i|U^{i-1},Y^{\mathcal{A}})-H(R^{\mathcal{A}})\\&\overset{(a)}{=}\sum_{i\in\mathcal{A}}H(U_i|U^{i-1},Y^{\mathcal{A}})-\sum_{i\in\mathcal{A}}H(R_i)\\&\overset{(b)}{=}H(U^{\mathcal{A}}|Y^{\mathcal{A}})-\frac{1}{2}\sum_{i\in\mathcal{A}}(\log 2\pi\mathrm{e}G^{(i)})\end{aligned} \tag{29}$$

其中，(*a*)成立是由于 R_i 为独立同分布的随机变量；(*b*)成立是根据链式法则和最大熵原理，当 $P_{los}\gg P_{dif}$，即 LOS 分量足够大时，信道衰落服从高斯分布，得到 $\sum\limits_{i\in\mathcal{A}}H(R_i)$ 的上界

$$\sum_{i\in\mathcal{A}}H(R_i)\leqslant\frac{1}{2}\sum_{i\in\mathcal{A}}(\log 2\pi\mathrm{e}G^{(i)}) \tag{30}$$

因此，令 $\alpha^{\kappa}=\frac{1}{2}\sum\limits_{i\in\mathcal{A}}(\log 2\pi\mathrm{e}G^{(i)})$，可得

$$\sum_{i\in\mathcal{A}}H(U_i|U^{i-1},R^{i-1},Y^{\mathcal{A}})\geq H(U^{\mathcal{A}}|Y^{\mathcal{A}})-\alpha^{\kappa} \tag{31}$$

同理，可以得到

$$\sum_{i\in\mathcal{A}}H(U_i|U^{i-1},R^{i-1},Y^{\mathcal{A}})=\sum_{i\in\mathcal{A}}H(U_i|U^{i-1},Y^{\mathcal{A}})$$
$$-\sum_{i\in\mathcal{A}}I(U_i;R^{i-1}|U^{i-1},Y^{\mathcal{A}})\leqslant H(U^{\mathcal{A}}|Y^{\mathcal{A}}) \tag{32}$$

因此，令 $\alpha_w^{\kappa}=\frac{1}{2}\sum_{i\in\mathcal{A}}(\log 2\pi eG^{(i)})$，式(27)可转化为

$$(\ell-1)[|\mathcal{V}_{X|Z}|-|\mathcal{V}_{X|Y}|]+|\mathcal{H}_{X|Y}|-|\mathcal{V}_{X|Y}|-\sum_{j=1}^{\ell}I(Z_j^n;U_j^n)$$
$$-\ell(3\kappa\delta^n+1)\geq(\ell-1)[H(X^{\mathcal{A}}|Z^{\mathcal{A}})-H(X^{\mathcal{A}}|Y^{\mathcal{A}})]-\alpha_w^{\kappa}$$
$$-\sum_{j=1}^{\ell}I(Z_j^n;U_j^n)-\ell(3\kappa\delta^n+1)$$
$$=(\ell-1)[I(Y^{\mathcal{A}};X^{\mathcal{A}})-I(Z^{\mathcal{A}};X^{\mathcal{A}})]-\alpha_w^{\kappa}$$
$$-\sum_{j=1}^{\ell}I(Z_j^n;X_j^n)-\ell(3\kappa\delta^n+1) \tag{33}$$

对于 $i\in\mathcal{A}$，由保密性约束可得，$I(Z_i;X_i)\to 0$；对于冻结比特索引集合 $i\in\mathcal{A}^C$，假设 Willie 能够获得或事先已知，那么 $I(Z_j^n;X_j^n)\to n-\kappa$. 因此，信息比特索引集合的势的下界满足

$$\kappa\geqslant\frac{(n+1)\ell}{2\ell-1-\frac{1}{2}\log 2\pi e\text{-}3\ell\delta^n} \tag{34}$$

当 $n\to\infty$ 时，$\kappa\geqslant\frac{(n+1)\ell}{2\ell-3}$，且 $\frac{(n+1)\ell}{2\ell-3}\leqslant n$，则 $\ell>3$，此时便能实现隐蔽性约束. 同时由 5.3 节保密性分析可得 $S(\mathbb{C})\leqslant 3\ell\kappa\delta^n$. 给定一组参数 $(M_{1:\ell},n,\epsilon,\upsilon,\xi,\varsigma)$，当 CSFP 方案达到可靠性约束与保密性约束，且冻结比特索引集合 $\mathcal{A}^C$ 的势满足 $|\mathcal{A}^C|<\frac{(\ell-3)n-\ell}{2\ell-3}$，且 $\ell>3$ 时能够实现隐蔽性.

证毕.

XU Ming, Ph.D., professor. His main research interests include cryptography and information security, wireless network security and mobile computing.

WU Jia-Jia, master candidate. Her main research interests include cryptography and information security.

Background

Underwater acoustic communication is considered to be the most suitable technology for underwater information acquisition and transmission over middle and long distance. However, the underwater acoustic channel (UAC) is considered one of the most challenging environments to establish secure and reliable communications due to the fact that underwater communication nodes are usually deployed in unattended and even hostile environments. Commonly used key distribution protocols allow two parties in the communication to negotiate a secret-key to encrypt all the data they transmit. However, the characteristics of the UAC and its inherent vulnerability make the communication process of key distribution protocols easy to be detected, rendering inevitable information leakage.

In recent years, some researchers introduced covert communication into key distribution protocols. These protocols enable the adversary almost ignore the process of key distribution by setting the transmission power constraints or exploiting some coding methods. However, the methods of setting the transmission power constraints may expose the information transmission status of legitimate nodes for the reasons of transmission losses and fading effects of the UAC. Moreover, most coding based covert secret-key distribution protocols assume that the encoded codes are with the asymptotic equipartition property, which are impracticable in the UAC.

To address these problems, this paper proposes a Covert Secret-key distribution scheme based on Fine-grained Polarization (CSFP). The CSFP scheme is composed of three phases: code construction, encoding and decoding. The polar code construction is realized through sorting the capacity of each subchannel after calculating the gains of UAC in order to ensure that the information transmission rate can achieve the Shannon limit theoretically. Moreover, the encoding and decoding algorithms for covert secret-key distribution over multi-round communication are designed based on the fine-grained polarization and the alignment of index sequence of information bits by linking multiple information blocks through a chain structure. To ensure the covertness of secret-key distribution process, the legitimate transmitter and the legitimate receiver initialize the message block transmitted in the first round of communication using a shared random seed and extract a random seed from the currently generated secret-key to randomize the next message block. The reliability, randomness, secrecy and covertness of the CSFP scheme are proved through the information theory and the achievability of covertness constraint and the covert secret-key generation rate are derived by the maximum entropy principle. The theoretical analysis and simulation results demonstrate the performance of CSFP.

This work is supported by the National Natural Science Foundation of China under Grant No. 62172269 and the China Postdoctoral Science Foundation under Grant No. 2014M561512. The full name of No. 62172269 is “Research on key technologies of secret-key agreement with unconditional security for underwater acoustic sensor networks”. We have published several papers to address various secure problems in the UAC in IEEE TMC, IEEE TETC, IEEE WCL, and IEEE CL.