基于水下噪声信道不确定性的保密通信方案

徐明[1,2]，陈芳[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：针对水下噪声不确定性对信息传输产生的影响和噪声信道中通信面临的安全问题，提出一种基于水下噪声信道不确定性的保密通信方案。该方案由基于哥德尔编码的交互式密钥提取协议和基于 *r*−循环 Toeplitz 矩阵的保密增强协议组成。在密钥提取的过程中，通过引入哥德尔编码，减少了密钥序列的比较次数；在计算保密增强后的密钥长度时，考虑了水下噪声的不确定性，具有更强的实际意义。实验结果表明，在满足协议安全性的条件下，传输的总比特数为 119 940 bit，保密增强后生成的密钥串总长度的下界为 117 331 bit，敌手关于密钥串信息量的上界为 2 609 bit，所需时间为 11.99 s，并且所提出的(*nt*+*s*)×(*nt*+*s*)阶 *r*−循环 Toeplitz 矩阵比传统的同阶 Toeplitz 矩阵减少了(*nt*+*s*)−1 bit 存储空间。

关键词：水下噪声；不确定性；Toeplitz 矩阵；保密增强

中图分类号：TP309

文献标识码：A

doi: 10.11959/j.issn.1000−436x.2019055

Confidential communication scheme based on uncertainty of underwater noisy channels

XU Ming[1,2], CHEN Fang[1]

1. College of Information Engineering, Shanghai Maritime University, Shanghai 201306, China
2. College of Electronics and Information Engineering, Tongji University, Shanghai 201804, China

Abstract: Aiming at the influence of the uncertainty of underwater noise on information transmission and the security problem of the communication over noisy channels, a confidential communication scheme based on the uncertainty of underwater noisy channels was proposed. The proposed scheme was composed of an interactive key extraction protocol based on Godel's code and a privacy amplification protocol based on *r*-circulant Toeplitz matrix. During the process of key extraction, the key sequence comparing number was reduced through the Godel's code. When calculating the key length after privacy amplification, the uncertainty of underwater noise was considered to make the proposed scheme more practical. Experimental results show that under the condition of satisfying protocol security, it takes 11.99 s to transmit 119 940 bit string where the lower bound of the generated secret key length is 117 331 bit after privacy amplification and the upper bound of the adversary's information about the secret key is 2 609 bit. Moreover, the proposed scheme (*nt*+*s*)×(*nt*+*s*)-order *r*-circulant Toeplitz matrix decreases (*nt*+*s*)−1 bit memory space compared to the traditional Toeplitz matrix with the same order.

Key words: underwater noise, uncertainty, Toeplitz matrix, privacy amplification

1 引言

随着信息技术的发展和海洋环境的开发利用，海洋信息通信变得越来越重要。目前，海洋信息在水下主要利用声波进行通信[1]。由于水声信道的开放性和海洋环境的多变性，导致海洋信息通信面临

收稿日期：2018−12−25；**修回日期**：2019−03−10

基金项目：国家自然科学基金资助项目（No.61202370）；中国博士后科学基金资助项目（No.2014M561512）

Foundation Items: The National Natural Science Foundation of China (No.61202370), China Postdoctoral Science Foundation Project (No.2014M561512)

各种安全和攻击问题[1-2]，并且，在复杂多变的海洋环境下，各种噪声的干扰会对信息传输产生很大的影响[3]。按照发声机理可以将海洋环境噪声的声源分为以下 4 类：海洋动力噪声、海洋生物噪声、人为噪声和海洋热噪声[4]。噪声的不确定性给海洋信息的传输带来了严重干扰。如何在水下噪声不确定的情况下对传输的信息进行保密通信，保证信息的完整性、保密性与顽健性已经成为海洋信息安全技术面临的重大挑战。

针对海洋信息的保密通信问题，本文在保证安全性的前提下，基于二元对称通信信道中水下噪声的不可预测性，引入哥德尔编码[5]，提出了基于哥德尔编码的交互式密钥提取协议来进行密钥协商和认证提取。同时，为了提高保密增强[6-7]的存储效率，将 r–循环 Toeplitz 矩阵[8-9]应用于保密增强中，提出了一个基于 r–循环 Toeplitz 矩阵的保密增强协议，使矩阵存储空间比传统的 Toeplitz 矩阵存储空间大大减小，由此形成了一个基于水下噪声信道不确定性的保密通信方案，使敌手无法获得足够的信息来计算密钥，保证了方案的安全性和可靠性。

2 相关知识

2.1 哥德尔编码

哥德尔编码是哥德尔在证明哥德尔不完备定理[5]中引入的，基于质数分解原理，将序列与自然数之间建立起一一对应的关系。给定一个有穷序列 $(z_1,z_2,z_3,\cdots,z_n)$，使 $y=\mathrm{enc}(z_1z_2\cdots z_n)=p_1^{z_1}p_2^{z_2}\cdots p_n^{z_n}=\prod p_i^{z_i}$ $(1\leqslant i\leqslant n, p_i\neq 1)$，则把这种编码方式称为哥德尔编码，$y$ 称为序列 $(z_1,z_2,z_3,\cdots,z_n)$ 所对应的哥德尔数，其中，p_i 表示从小到大排列的第 i 个不同的质数。

2.2 保密增强

保密增强最初由 Bennett[6]提出，并在文献[10]中得到进一步推广。保密增强是指合法的通信双方 A 和 B 共享一个部分保密串 S，并且敌手 Eve 知道关于 S 部分信息的情况下，通过全域散列函数[11-13]，使 A 和 B 得到一个几乎完全保密的密钥串 S'，而敌手 Eve 所知道的关于 S' 的信息量呈指数级减少。

定义 1[14] 假设 A 和 B 共享一个 N bit 密钥串 S，随机变量 V 表示包含 Eve 所知道的关于 S 的所有信息。对于任意的 $\alpha=2$ 或 $\alpha=\infty$，都有子集 $\{P_S\,|\,H_\alpha(S)\geqslant\beta\}$ 构成 $\psi_{N,\alpha,\beta}$ 集合。设 l 是任意一个正整数，ε、$\delta>0$，则在非认证信道上存在一个 $(N,\psi,l,\varepsilon,\delta)$ 保密增强协议满足以下性质。

1) 正确性和保密性。令敌手 Eve 在被动攻击只能进行窃听的情况下，接受特定值 $V=v$ 满足 $P_{S|V=v}\in\psi$，A 和 B 在协议的最后得到一个 l bit 密钥串 S' 使 $S_{\mathrm{A}}'=S_{\mathrm{B}}'=S'$，并且有 $H(S'\,|\,C,V=v)\geqslant l-\varepsilon$ 成立，其中，C 表示信道上的交换信息。在这种情况下，认为保密增强是成功的。

2) 顽健性。令 $P_{S|V=v}\in\psi$，则对敌手 Eve 的任何一种可能攻击策略，A 和 B 都拒绝协议的结果，或者保密增强成功的概率至少为 $1-\delta$。

2.3 全域散列函数

全域散列函数是实现保密增强的一个重要工具，定义如下[13]。设函数 $G:X\to Y, X=\{0,1\}^n$，$Y=\{0,1\}^l$，$n>l$，$\forall g\in G$，其中，g 是从服从均匀分布的 G 中随机选取的函数，$|X|$和$|Y|$分别表示集合 X 和集合 Y 所含元素的数量，对 $\forall x_1,x_2\in X$，且 $x_1\neq x_2$，使 $g(x_1)=g(x_2)$ 的概率不超过 $\dfrac{1}{|Y|}$，即

$$P\{g(x_1)=g(x_2)\,|\,x_1\neq x_2\}\leqslant\frac{1}{|Y|}$$

用于实现保密增强的全域散列函数有 3 种，分别是模算术[15]、有限域乘法[10]和 Toeplitz 矩阵[15-16]。Toeplitz 矩阵由于具有良好的存储性能，使用最为广泛。

2.4 Toeplitz 矩阵

一般的 $s\times n$ 阶的 Toeplitz 矩阵，满足 $\boldsymbol{T}_{i,j}=\boldsymbol{T}_{i+\varpi,j+\varpi}$，其中，$1\leqslant i,\ i+\varpi\leqslant s$，$1\leqslant j,\ j+\varpi\leqslant n$，即矩阵上每条自左上至右下的斜线上的元素相同。Toeplitz 矩阵的具体表示形式为

$$\boldsymbol{T}(\boldsymbol{D})=\begin{pmatrix} D_n & D_{n-1} & \cdots & D_2 & D_1\\ D_{n+1} & D_n & \cdots & D_3 & D_2\\ \cdots & \cdots & \cdots & \cdots & \cdots\\ D_{n+s-2} & D_{n+s-1} & \cdots & D_s & D_{s-1}\\ D_{n+s-1} & D_{n+s-2} & \cdots & D_{s+1} & D_s \end{pmatrix}_{s\times n}$$

r–循环 Toeplitz 矩阵可表示为

$$\boldsymbol{R}_r(\boldsymbol{D})=\begin{pmatrix} D_0 & D_1 & D_2 & \cdots & D_{n-1}\\ rD_{n-1} & D_0 & D_1 & \cdots & D_{n-2}\\ rD_{n-2} & rD_{n-1} & D_0 & \cdots & D_{n-3}\\ \cdots & \cdots & \cdots & \cdots & \cdots\\ rD_1 & rD_2 & rD_3 & \cdots & D_0 \end{pmatrix}_{n\times n}$$

当 $r=1$ 时，为循环 Toeplitz 矩阵；当 $r=-1$ 时，为

斜循环 Toeplitz 矩阵；当 $r=0$ 时，为上三角 Toeplitz 矩阵[8]。

3　基于哥德尔编码的交互式密钥提取协议

3.1　协议设计

基于哥德尔编码的交互式密钥提取协议包含密钥协商和认证提取两部分。在有限域 GF(q)中选取 q 个元素，其中 q 为素数。节点 A 和节点 B 分别提前选取 Q_1、Q_2 作为标志。其中，Q_1、$Q_2\in$GF(q)，$Q=(Q_1+Q_2)\bmod(q)$，则 $Q\in$GF(q)，并且 Q 作为节点 A 和节点 B 的秘密数。基于哥德尔编码的交互式密钥协商如图 1 所示。

下面，详细描述图 1 中基于哥德尔编码的交互式密钥协商协议。

首先，节点 A 和节点 B 在二元对称信道上分别同时获得 n bit 密钥串 $S_A=x_1x_2\cdots x_n$，$S_B=y_1y_2\cdots y_n$，并将各自获得密钥串中的相邻两位进行异或操作，而且后面的相邻两位不能与前面相邻的任一位重叠。将异或后的所有结果分别组成密钥序列 $Z_A=(z_1,z_2,\cdots,z_{\frac{n}{2}})$，$Z_B=(z_1',z_2',\cdots,z_{\frac{n}{2}}')$，然后分别计算哥德尔数 Ge_A 和 Ge_B，节点 B 将计算好的 Ge_B 发送给节点 A。为了验证传过来的 Ge_B 是否正确，通过只有节点 A 和节点 B 所知道的秘密数 Q 来计算 $G_A=Q\times Ge_B$，$G_B=Q\times Ge_B$，将 G_A 发送给节点 B，若 $G_A=G_B$，则向节点 A 发送一个反馈信息“Yes”，如果 $Ge_A\neq Ge_B$，则发送密钥序列 Z_A，否则停止。节点 B 比较 z_i 与 $z_i'(1\leqslant i\leqslant\frac{n}{2})$，若 $z_i\neq z_i'$，则记录对应的下标组成一个集合 I，并将 I 发送给节点 A，这样节点 A 就知道异或结果不同的位，并且节点 A 和节点 B 都将异或结果不同的位置为 1，使双方的比特串尽可能相同。

重复上述密钥协商协议 t 次，分别获得 nt bit 的密钥串 S_A 和 S_B。此时，S_A 和 S_B 仍然会小概率不同，因此需要对密钥协商后的公共串进行认证并提取出完全一致的安全密钥。

令 $H_{\bar{L}}(S)=\sum_{i=1}^{2|I|}\bar{L}_iS_i$，其中，$\bar{L}_i$、$S_i$ 分别表示串长 $\bar{L}$、S 的第 i 位，$|I|$表示图 1 中集合 I 的元素个数，基于哥德尔编码的交互式密钥认证提取如图 2 所示。首先，从实数有限域 ${}_R$GF(2^{nt})（R 代表实数）任意选取 ∂ 和 $h(h\neq\partial)$，S_{11} 是图 1 中基于哥德尔编码的交互式密钥协商进行 t 次后，不同的异或结果置为 1 的所有位。节点 A 和节点 B 分别计算标识符 Tag_A，Tag_B' 与 Tag_A'，Tag_B。通过标识符之间的比较来进行信道上的消息认证，最后从散列函数族中任意选取散列函数 w 来检查最终获得的 nt bit 的公共密钥串 S_A 与 S_B 是否相等。若 $S_A\neq S_B$，则停止该协议；否则，节点 A 和节点 B 分别通过保密增强中的全域散列函数 g 作用在公共密钥串上，提取最终的安全密钥 $K_A=K_B=K$。全域散列函数 g 满足 $g_{\mathbf{cir}}(S)=\mathbf{cir}S$。其中，$g$ 从服从均匀分布的 G 中随机选取，**cir** 是二进制的 r–循环 Toeplitz 矩阵，S 是密钥串 S_A 或 S_B，K 是对散列函数结果取前 l 位。

3.2　协议分析与证明

3.2.1　敌手模型与攻击方式

本文讨论中的敌手模型满足以下条件：

1) 敌手拥有无限的计算能力；

2) 敌手的窃听信道不限制为衰落信道；

3) 信道为二进制对称信道，合法通信双方的误比特率为 λ，敌手窃听信道的误比特率为 θ，敌手预估信息的错误比特率为 θ'。

本文主要讨论以下 2 种攻击方式。

1) 替换攻击。敌手从自己拥有的校验块集合中

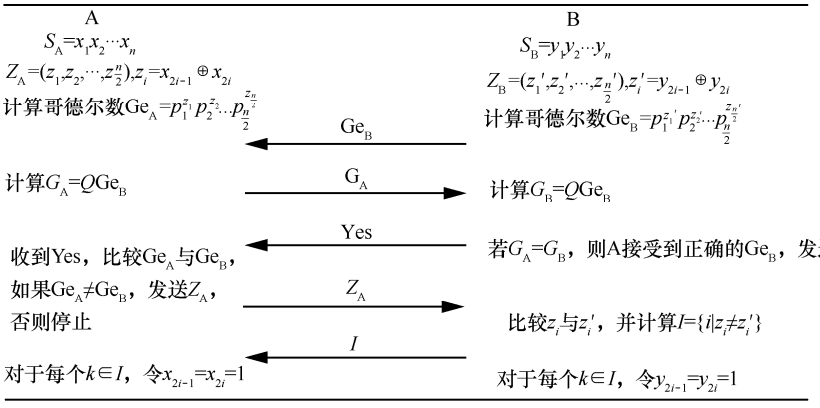

图 1　基于哥德尔编码的交互式密钥协商

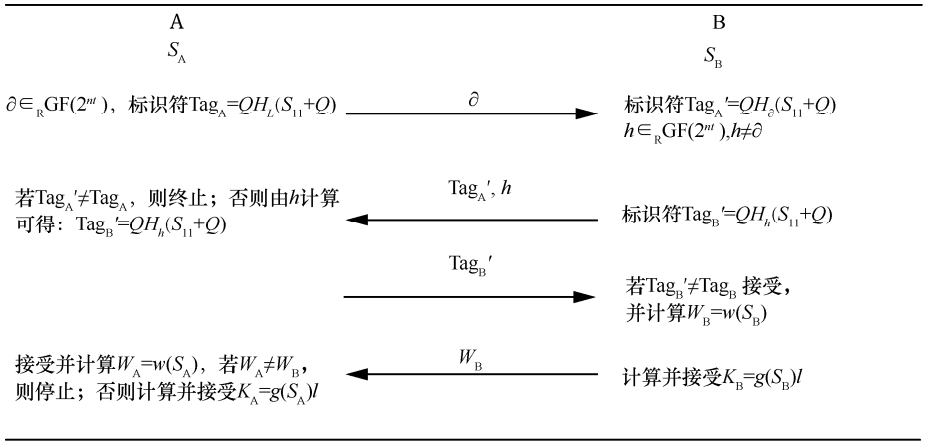

图 2 基于哥德尔编码的交互式密钥认证提取

随机选取一个校验块，不经过任何纠错直接发送给节点 B。

2) 模仿攻击。敌手从校验块集合中随机选取一个校验块，然后根据自己预估信息的错误比特率 θ' 对所选取的校验块随机纠错。由于敌手不知道错误比特的具体位置，所以纠错具有随机性和概率性。执行基于哥德尔编码的交互式密钥协商协议 t 次，共有 t 个校验块。在基于哥德尔编码的交互式密钥提取协议中，敌手每次窃听到节点 A 发送给节点 B 的校验块 Z，与自己所掌握的校验块 Z'' 相比。设每次找到的错误比特个数为 e_i，经过多次窃听，总共窃听了 num 个校验块，则 $\theta'=(1-\theta)\left[\dfrac{\sum_{i=1}^{\text{num}} e_i}{\text{num}\dfrac{n}{2}}\right]$。

3.2.2 安全性分析与证明

由图 1 中密钥协商协议可知，如果 $z_i\neq z_i'$，则敌手可知 $x_{2i-1}=x_{2i}=11$。如果 $z_i=z_i'$，敌手的 z_i'' 与节点 A 和节点 B 的 z_i、z_i' 不同，则敌手正确猜出两位的概率为 $\dfrac{1}{2}$。如果敌手的 z_i'' 与节点 A 和节点 B 的 z_i、z_i' 相同，那么敌手窃听到的两位与节点 A 和节点 B 相同的概率为 $(1-\theta)^2$，$P[z_i\neq z_i']=2\lambda(1-\lambda)$，$P[z_i=z_i']=1-2\lambda+2\lambda^2$，综上所述，敌手正确窃听对应两位的概率为 $2\lambda(1-\lambda)+(1-2\lambda+2\lambda^2)\left[\dfrac{1}{2}2\theta(1-\theta)+(1-\theta)^2\right]$，整理后为 $2\lambda(1-\lambda)+(1-2\lambda+2\lambda^2)(1-\theta)$，令 $\vartheta=2\lambda(1-\lambda)+(1-2\lambda+2\lambda^2)(1-\theta)$，所以敌手在 n bit 密钥串上能够正确窃听的位数平均最多为 $n\vartheta^{\frac{n}{2}}$ $(0<\vartheta^{\frac{n}{2}}+\varphi<1)$。

下面，证明敌手所知道的 $n(\vartheta^{\frac{n}{2}}+\varphi)$ bit 的概率是可以忽略不计的。

定理 1 令 $J\subset\{1,2,3,\cdots,n\}$ 为敌手窃听到的 z_i 的下标索引集合，并且这些下标索引与节点 A 和节点 B 所对应的下标索引一致，则有概率满足 $P[|J|\geqslant n(\vartheta^{\frac{n}{2}}+\varphi)]\leqslant \mathrm{e}^{\frac{-n\varphi^2\vartheta^{\frac{n}{2}}}{3}}$。

证明 设 $\overline{M_i}$ 表示第 i 位随机变量，$\overline{M_i}=1$ 表示敌手窃听到第 i 位的正确值，$\overline{M_i}=0$ 时表示敌手窃听到的第 i 位是错误的。其中 $\overline{M}_1,\overline{M}_2,\cdots,\overline{M}_n$ 为独立泊松事件，$\mathrm{E}(\overline{M}_i)=\eta$，则 $\sum_{i=1}^{n}\overline{M}_i$ 的期望为 $\mathrm{E}(\sum_{i=1}^{n}\overline{M}_i)=n\eta$。由马尔可夫不等式可得，对于任意 $\tau>0,\gamma>0$，将式(1)应用于 $\mathrm{e}^{\gamma\overline{M}}$，来获得随机变量 $\overline{M}$ 的一般切尔诺夫界，从而由乘法切尔诺夫定理可得到更简便常用的切尔诺夫界，即对于任意的 $0\leqslant\varsigma\leqslant1$ 满足式(2)。

$$P[\overline{M}\geqslant\tau]=P[\mathrm{e}^{\gamma\overline{M}}\geqslant\mathrm{e}^{\gamma\tau}]\leqslant\frac{\mathrm{E}(\mathrm{e}^{\gamma\overline{M}})}{\mathrm{e}^{\gamma\tau}}\tag{1}$$

$$P[\sum_{i=1}^{n}\overline{M}_i\geqslant(1+\varsigma)n\tau]\leqslant\mathrm{e}^{\frac{-n\tau\varsigma^2}{3}}\tag{2}$$

所以，有

$$P[|J|\geqslant n(\vartheta^{\frac{n}{2}}+\varphi)]=P[\sum_{i=1}^{n}\overline{M}_i\geqslant n\vartheta^{\frac{n}{2}}(1+\varphi\vartheta^{-\frac{n}{2}})]\leqslant\mathrm{e}^{-\frac{n\varphi^2\vartheta^{-\frac{n}{2}}}{3}}$$

证毕。

当敌手有自己的密钥串 z_i'' 时，与节点 A 传输的密钥串 z_i 相比($1\leqslant i\leqslant \frac{n}{2}$)，相对应的两位 $x_{2i-1}x_{2i}$ 的不确定性可由定理 2 估计。

定理 2　$\overline{S}=\{00,01,10,11\}$，$\overline{X}\in\overline{S}$ 是对应于两位 $x_{2i-1}x_{2i}$ 的随机变量，其中敌手窃听信道的误比特率为 θ，则敌手对 nt bit 密钥串的不确定度为 $R(\overline{X}\,|\,\overline{Y})=P(\overline{Y}=0)R(\overline{X}\,|\,\overline{Y}=0)+P(\overline{Y}=1)R(\overline{X}\,|\,\overline{Y}=1)$。

证明　设随机变量 $\overline{Y}$ 有以下 3 种情况：1) 当 A 和 B 发送的校验位不等时，即 $z_i\neq z_i'$，此时敌手知道 $x_{2i-1}x_{2i}$=11，则 $\overline{Y}=\Delta$；2) 当 A 和 B 发送的校验位相等时，即 $z_i=z_i'$，若敌手所窃听到的校验位 $z_i''=z_i$，则 $\overline{Y}=0$；3）当节点 A 和节点 B 发送的校验位相等时，即 $z_i=z_i'$，若敌手所窃听到的校验位 $z_i''\neq z_i$，则 $\overline{Y}=1$。

对于情况 1)，显然 $R(\overline{X}\,|\,\overline{Y}=\Delta)=0$；对于情况 2)和情况 3)，不妨假设节点 A 发送的 z_i=1，$x_{2i-1}x_{2i}=10$（$x_{2i-1}x_{2i}$ 为 00、01、11 时情况相同），因为当 z_i=0 时，情况 2)和情况 3)分别与 z_i=1 时的概率一样。对于情况 2)，敌手所接受到的只有 01 或 10，即要么两位都是正确的，要么都是错误的，则

$$P[\overline{Y}=0]=\theta^2+(1-\theta)^2 \tag{3}$$

敌手接收到 $x_{2i-1}x_{2i}=10$ 的概率为

$$P[10\,|\,\overline{Y}=0]=\frac{(1-\theta)^2}{[\theta^2+(1-\theta)^2]} \tag{4}$$

敌手接收到 $x_{2i-1}x_{2i}=01$ 的概率为

$$P[01\,|\,\overline{Y}=0]=\frac{\theta^2}{\theta^2+(1-\theta)^2} \tag{5}$$

对于情况 3)，敌手接受的只有 00 或 11，此时敌手接收到的 $x_{2i-1}x_{2i}$ 只有一位是正确的，所以

$$P[\overline{Y}=1]=2\theta(1-\theta) \tag{6}$$

敌手接收到 $x_{2i-1}x_{2i}=00$ 的概率为

$$P[00\,|\,\overline{Y}=1]=\frac{\theta(1-\theta)}{2\theta(1-\theta)}=\frac{1}{2} \tag{7}$$

敌手接收到 $x_{2i-1}x_{2i}=11$ 的概率为

$$P[11\,|\,\overline{Y}=1]=\frac{(1-\theta)\theta}{2\theta(1-\theta)}=\frac{1}{2} \tag{8}$$

用 Rényi 熵[17]表示信息的不确定性，如式(9)~式(11)所示。

$$R(\overline{X}\,|\,\overline{Y}=0)=\frac{(1-\theta)^2}{\theta^2+(1-\theta)^2}\mathrm{lb}\frac{\theta^2+(1-\theta)^2}{(1-\theta)^2}+\frac{\theta^2}{\theta^2+(1-\theta)^2}\mathrm{lb}\frac{\theta^2+(1-\theta)^2}{\theta^2} \tag{9}$$

$$R(\overline{X}\,|\,\overline{Y}=1)=-\frac{1}{2}\mathrm{lb}\frac{1}{2}-\frac{1}{2}\mathrm{lb}\frac{1}{2}=1 \tag{10}$$

$$R(\overline{X}\,|\,\overline{Y}=\Delta)=0 \tag{11}$$

综上所述，可得

$$\begin{aligned}&R(\overline{X}\,|\,\overline{Y})=P(\overline{Y}=0)R(\overline{X}\,|\,\overline{Y}=0)+\\&P(\overline{Y}=1)R\ (\overline{X}\,|\,\overline{Y}=1)+P(\overline{Y}=\Delta)R(\overline{X}\,|\,\overline{Y}=\Delta)=\\&P(\overline{Y}=0)R(\overline{X}\,|\,\overline{Y}=0)\ +P(\overline{Y}=1)R(\overline{X}\,|\,\overline{Y}=1)=\\&[(\theta^2+(1-\theta)^2][\frac{(1-\theta)^2}{\theta^2+(1-\theta)^2}\ \ \mathrm{lb}\frac{\theta^2+(1-\theta)^2}{(1-\theta)^2}+\\&\frac{\theta^2}{\theta^2+(1-\theta)^2}\mathrm{lb}\frac{\theta^2+(1-\theta)^2}{\theta^2}]\ +2\theta(1-\theta)\end{aligned}$$

由此可得，敌手对 nt bit 密钥串的不确定度为 $\frac{nt}{2}R(\overline{X}\,|\,\overline{Y})$。

证毕。

3.3　协议特点

3.3.1　认证性

基于哥德尔编码的交互式密钥认证提取协议通过标识符是否相等来认证信道是否安全，通过散列函数来认证节点 A 和节点 B 进行 t 次密钥协商后所获得的公共串是否一致，并提取出完全一致的高度保密密钥串 K。

3.3.2　高效性

基于哥德尔编码的交互式密钥协商协议通过哥德尔数是否一致来判断是否需要发送密钥序列 Z_{A}。由哥德尔编码的性质可知，如果通信双方的计算结果 $\mathrm{Ge_A}=\mathrm{Ge_B}$，则说明 $z_i=z_i'$，不需要发送密钥序列 Z_{A}；只有在 $\mathrm{Ge_A}\neq\mathrm{Ge_B}$ 的情况下才需要发送密钥序列 Z_{A} 进行比较，因此可以减少密钥序列的比较次数，降低通信开销，提高通信效率。此外，由模运算的运算规则[18-19]可知

$$a_1a_2 \bmod q=[(a_1 \bmod q)\ (a_2 \bmod q)] \bmod q$$

$$(a_1+a_2) \bmod q=(a_1 \bmod q+\ a_2 \bmod q) \bmod q$$

在计算 $\mathrm{Ge_A}$、$\mathrm{Ge_B}$ 时，通过提前使用模运算，可以降低指数运算带来的数据存储空间问题。在密钥认证提取过程中，通过引入 Q 的模运算，可以提高指数的运算效率。另外，本文所有的计算都基于二元对称信道。因此，所有非二进制结果都要进行取模运算。

本文在密钥协商协议中没有检查密钥串 S_{A} 和 S_{B} 是否相同，而是在密钥认证提取协议中，通过收集 t 个这样的密钥串后再进行认证，并利用散列函数完成密钥串是否相同的检查，减少了认证次数，进一步提高了通信效率。

设 N 是执行图 2 中的完整协议直到建立密钥串 K 为止的次数。定理 3 给出了 N' 的期望值，进一步证明了该协议的高效性。

定理 3 设 N' 是执行次数的随机变量，直到节点 A 和节点 B 建立长度为 nt bit 的公共密钥串，则 N' 的期望值是 $(1-\lambda)^{nt\lambda-\frac{nt}{2}}$。

证明 设合法通信双方的误比特率为 λ，敌手窃听信道的误比特率为 θ。Ω_1 表示节点 B 能正确接收到节点 A 发送密钥序列 $Z_{\mathrm{A}}=(z_1,z_2,\cdots,z_{\frac{n}{2}})$ 的事件，Ω_2 表示节点 A 和节点 B 得到的 nt bit 密钥串相同的事件。

$$\lambda=\frac{\sum_{i=1}^{t}|I|_i}{\frac{nt}{2}} \tag{12}$$

在图 1 中的密钥协商协议中有

$$P(\Omega_1)=(1-\lambda)^{\frac{nt}{2}} \tag{13}$$

第 t 次密钥协商协议中节点 A 和节点 B 的校验位相同的个数为 $\frac{n}{2}-|I|_t$，其节点 A 和节点 B 的 n bit 密钥串相同的概率为

$$((1-\lambda)^2)^{\frac{n}{2}-|I|_t}=(1-\lambda)^{n-2|I|_t} \tag{14}$$

所以，t 次基于哥德尔编码的交互式密钥协商协议执行完成后，节点 A 和节点 B 得到的 nt bit 密钥串相同的概率为

$$P(\Omega_2\mid\Omega_1)=\frac{\prod_{i=1}^{t}(1-\lambda)^{n-2|I|_i}}{(1-\lambda)^{\frac{nt}{2}}}=$$

$$(1-\lambda)^{\frac{nt}{2}-2\sum_{i=1}^{t}|I|_i}=(1-\lambda)^{\frac{nt}{2}-nt\lambda} \tag{15}$$

令

$$\upsilon=(1-\lambda)^{\frac{nt}{2}-nt\lambda} \tag{16}$$

则

$$\mathrm{E}(N')=\frac{1}{\upsilon} \tag{17}$$

所以 $\mathrm{E}(N')=(1-\lambda)^{nt\lambda-\frac{nt}{2}}$。

证毕。

由 3.2.1 节可知，合法通信双方的误比特率为 λ，敌手窃听信道的误比特率为 θ，正确窃听到密钥序列 $Z_{\mathrm{A}}=(z_1,z_2,\cdots,z_{\frac{n}{2}})$ 的概率为 $(1-\theta)^{\frac{nt}{2}}$，当执行完协议 N' 次后，被敌手可能窃听到的概率为 $1-[1-(1-\theta)^{\frac{nt}{2}}]^{N'}$，当执行完协议 N' 次建立密钥串 K 时，节点 A 和节点 B 的通信信道相当于无噪声信道，因为执行完协议 N' 次后合法通信双方已建立了相同一致的密钥串，而敌手的窃听信道可等价于一个新的二元对称信道，其新的误比特率 $\overline{\theta}$ 满足 $(1-\overline{\theta})^{\frac{nt}{2}}=1-1-[1-(1-\theta)^{\frac{nt}{2}}]^{N'}$，整理可得 $\overline{\theta}=1-\{1-[1-(1-\theta)^{\frac{nt}{2}}]^{N'}\}^{\frac{2}{nt}}$，其中，$N'$ 即为定理 3 中的期望值。

由以上分析可得，原来的 $(\lambda>0,\theta>0)$ 信道可等价于 $(\lambda=0,\overline{\theta}>0)$ 信道，即无噪声的合法通信信道和一个较低误比特率的窃听信道，即使窃听信道的误比特率比合法通信双方的误比特率更低，敌手也始终无法避免由噪声产生的极小误比特率。

3.3.3 抗主动攻击

结合 3.2.1 节中的分析，可以得到定理 4。

定理 4 节点 A 和节点 B 共享 nt bit 的公共串，敌手预估信息的错误比特率为 θ'，每个校验块中敌手与节点 A 和节点 B 不一致的位数为 υ，则敌手采取第一种方式主动攻击成功的最大概率为 $(1-\theta')^{\frac{n}{2}}$，敌手采取第二种方式主动攻击成功的最大概率为 $\frac{1}{\sum_{\upsilon=0}^{\frac{n}{2}}C_{\frac{n}{2}}^{\upsilon}}\theta'^{\upsilon}(1-\theta')^{\frac{n}{2}-\upsilon}$。

证明 若敌手采取替换攻击方式进行主动攻击，由于在二元对称信道中敌手预估信息的错误比特率为 θ'，且每个校验块的长度为 $\frac{n}{2}$，则敌手所选取的校验块与节点 A 和节点 B 相同的概率为 $(1-\theta')^{\frac{n}{2}}$，即敌手采取第一种方式主动攻击成功的最大概率为 $(1-\theta')^{\frac{n}{2}}$。

若敌手采取模仿攻击方式进行主动攻击，其不知道每个校验块中有多少个不一致位，只能随机猜

测，而正确猜出不一致位个数的概率为 $\frac{1}{\sum_{\upsilon=0}^{\frac{n}{2}} C_{\frac{n}{2}}^{\upsilon}}$，故正确猜出并修正 υ 个不一致位的概率为

$$\frac{1}{\sum_{\upsilon=0}^{\frac{n}{2}} C_{\frac{n}{2}}^{\upsilon}} \cdot \frac{1}{C_{\frac{n}{2}}^{\upsilon}} C_{\frac{n}{2}}^{\upsilon} \theta'^{\upsilon} (1-\theta')^{\frac{n}{2}-\upsilon} \tag{18}$$

整理得

$$\frac{1}{\sum_{\upsilon=0}^{\frac{n}{2}} C_{\frac{n}{2}}^{\upsilon}} \theta'^{\upsilon} (1-\theta')^{\frac{n}{2}-\upsilon} \tag{19}$$

故敌手采取第二种方式主动攻击成功的最大概率为 $\frac{1}{\sum_{\upsilon=0}^{\frac{n}{2}} C_{\frac{n}{2}}^{\upsilon}} \theta'^{\upsilon} (1-\theta')^{\frac{n}{2}-\upsilon}$。证毕。

4　基于 *r*–循环 Toeplitz 矩阵的保密增强协议

保密增强的核心是构造全域散列函数。目前，广泛用于保密增强的是基于一般的 Toeplitz 矩阵的全域散列函数。一般的 *s*×*n* 阶 Toeplitz 矩阵需要(*s*+*n*−1) bit 的存储空间，为了提高存储效率，本文将 *n* 阶 *r*–循环 Toeplitz 矩阵用于保密增强中仅需 *n* bit 的存储空间和参数 *r* 的信息。同时在保密增强协议中考虑到了噪声的不确定性，使其协议具有更高的实用价值，并得出了提取密钥的最大长度和敌手关于密钥信息量的上界。

4.1　*r*–循环 Toeplitz 矩阵

任何一个 Toeplitz 矩阵都可以嵌入在一个循环矩阵中[20]，同样也可以嵌入在一个 *r*–循环 Toeplitz 矩阵中。为了提高保密增强的存储效率，故将一个一般的 *s*×*nt* 阶 Toeplitz 矩阵扩展成(*nt*+*s*)×(*nt*+*s*)阶 *r*–循环 Toeplitz 矩阵(*s*<*nt*)。具体表示形式为

$$\mathbf{cir} = \begin{pmatrix} \boldsymbol{R}_1 & \boldsymbol{R}_2 \\ \boldsymbol{R}_3 & \boldsymbol{R}_4 \end{pmatrix}_{(nt+s)\times(nt+s)}$$

其中 $\boldsymbol{R}_1$、$\boldsymbol{R}_2$、$\boldsymbol{R}_3$、$\boldsymbol{R}_4$ 分别为

$$\boldsymbol{R}_1 = \begin{pmatrix} D_s & D_{s+1} & \cdots & D_{s+nt-1} \\ rD_{s-1} & D_s & \cdots & D_{s+nt-2} \\ \cdots & \cdots & \cdots & \cdots \\ rD_1 & rD_2 & \cdots & D_{nt} \end{pmatrix}_{s\times nt}$$

$$\boldsymbol{R}_2 = \begin{pmatrix} D_0 & D_1 & \cdots & D_{s-1} \\ D_{s+nt-1} & D_0 & \cdots & D_{s-2} \\ \cdots & \cdots & \cdots & \cdots \\ D_{nt+1} & D_{nt+2} & \cdots & D_0 \end{pmatrix}_{s\times s}$$

$$\boldsymbol{R}_3 = \begin{pmatrix} rD_0 & rD_1 & \cdots & D_{nt-1} \\ rD_{nt+s-1} & rD_0 & \cdots & D_{nt-2} \\ \cdots & \cdots & \cdots & \cdots \\ rD_{s+1} & rD_n & \cdots & rD_0 \end{pmatrix}_{nt\times nt}$$

$$\boldsymbol{R}_4 = \begin{pmatrix} D_{nt} & D_{nt+1} & \cdots & D_{nt+s-1} \\ D_{nt-1} & D_{nt} & \cdots & D_{nt+s-2} \\ \cdots & \cdots & \cdots & \cdots \\ rD_1 & rD_2 & \cdots & D_s \end{pmatrix}_{nt\times s}$$

将 *nt*×1 阶的公共串 $S = (S_1, S_2, \cdots, S_{nt})^{\mathrm{T}}$ 扩展为 $\overline{\boldsymbol{S}} = \begin{pmatrix} S \\ 0 \end{pmatrix}_{(nt+s)\times 1}$，则提取出的密钥计算式如下

$$\overline{\boldsymbol{K}} = \mathbf{cir}\overline{\boldsymbol{S}} \tag{20}$$

其中，$\overline{\boldsymbol{K}} = (k_1, k_2, \cdots, k_{nt+s})$。取 $\overline{\boldsymbol{K}}$ 的前 *l* 位作为保密增强后的最终密钥 *K*，即 $K = (\overline{\boldsymbol{K}})_l$，而

$$k_i = \mathbf{cir}_{i1}\overline{S}_{11} \oplus \mathbf{cir}_{i2}\overline{S}_{21} \oplus \cdots \oplus \mathbf{cir}_{i(nt+s)}\overline{S}_{(nt+s)1}$$

其中，⊕ 表示异或操作，$\mathbf{cir}_{ij}$ 表示矩阵 **cir** 中第 *i* 行第 *j* 列元素，$\overline{S}_{j1}$ 表示向量 $\overline{\boldsymbol{S}}$ 中第 *j* 行第一列元素，由快速傅里叶变换 [20]可得

$$F\mathbf{cir} = \mathrm{diag}(F\boldsymbol{D})F \tag{21}$$

其中，$\boldsymbol{D}$ 是一个(*nt*+*s*)维向量，$\boldsymbol{D} = (D_0, D_1, \cdots, D_{nt+s-1})$，$F = (f_{k'})$，$f_{k'} = w_{nt+s}^{k'}$，$w_{nt+s} = \mathrm{e}^{-\frac{2\pi i}{nt+s}}$，由式(20)和式(21)可得

$$K = F^{-1}\mathrm{diag}(F\boldsymbol{D})F\overline{\boldsymbol{S}} = F^{-1}(F\boldsymbol{D}.*F\overline{\boldsymbol{S}}) \tag{22}$$

其中，(.*)表示哈达玛积，即 $(\xi.*\zeta)_j = \xi_j\zeta_j$。

本文采用 *r*–循环 Toeplitz 矩阵用于保密增强的全域散列函数中，是因为 *r*–循环 Toeplitz 矩阵取决于矩阵元素的第一行和参数 *r*。对于传统的(*nt*+*s*)×(*nt*+*s*)阶 Toeplitz 矩阵需要 2(*nt*+*s*)−1 bit 才能完整描述整个矩阵，而本文的(*nt*+*s*)×(*nt*+*s*)阶 *r*–循环 Toeplitz 矩阵只需要(*nt*+*s*) bit 和参数 *r* 就可以完整描述整个矩阵，从而减少了矩阵的存储空间。

4.2　基于传播距离的噪声不确定性

水下环境通信比陆地环境通信要复杂得多。为了对水下噪声的不确定性进行定量分析，本文采用

马尔可夫链蒙特卡罗（MCMC, Markov chain Monte Carlo）方法[21]来捕捉噪声的不确定性。MCMC 方法适用于非标准的多变量形式，可实现动态模拟，通常用于水声参数概率分布的获取。通过产生若干条独立并行的马尔可夫链来探索模型参数空间，并不断更新样本信息使马尔可夫链收敛于高概率密度区，也就是贝叶斯方法中的最大后验估计[4]。设水下通信的应用域 $u\in U$，距离域 $d\in D'$，环境域 $m\in M$，三者之间的关系如图 3 所示。

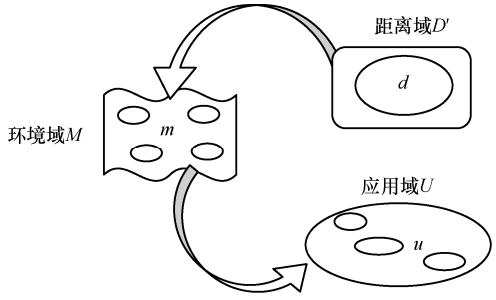

图 3 距离域、环境域和应用域三者之间的关系

噪声本身就是一种随机过程，本文把噪声看成属于应用域 U 的随机变量 u。由贝叶斯理论可得

$$p(m\,|\,\boldsymbol{d})=\frac{p(\boldsymbol{d}\,|\,m)p(m)}{p(\boldsymbol{d})}\propto L(m)p(m) \tag{23}$$

其中，$p(\boldsymbol{d})$为归一化因子，$L(m|\boldsymbol{d})$是 $p(\boldsymbol{d}|m)$的似然函数。若距离域中的数据矢量表示为 $\boldsymbol{d}=D'(m)+\boldsymbol{\mathcal{A}}$，其中，$D'(m)=d(m)\bar{s}$，$\boldsymbol{\mathcal{A}}$ 为服从正态分布$(0,\ \overline{C})$的误差项，$\overline{C}$ 为协方差。则似然函数为

$$L(m,\overline{C},\bar{s})=\frac{1}{\pi^{\overline{N}}\,|\,\overline{C}\,|}\exp\{-[\boldsymbol{d}-d(m)\bar{s}]^{\odot}\overline{C}^{-1}[\boldsymbol{d}-d(m)\bar{s}]\} \tag{24}$$

其中，$\overline{N}$ 表示数据点的数量，上标$^{\odot}$为共轭转置，由水声传播模型[4]可获得转换函数 $d(m)$，$\bar{s}$ 是水下噪声源，对于数据的不确定性可用服从独立同分布的误差 $\overline{C}=vI$ 来描述。当 $\dfrac{\partial\log L}{\partial\bar{s}}=0$ 时，

$$\bar{s}_{ML}=\frac{\boldsymbol{d}^{\odot}d(m)}{\|\,d(m)\,\|^2} \tag{25}$$

将式(25)代入式(24)中，似然函数变为

$$L(m,v)=\frac{1}{\pi^{\overline{N}}v^{\overline{N}}}\exp\left(-\frac{\Phi(m)}{v}\right) \tag{26}$$

其中，目标函数为

$$\Phi(m)=\|\,\boldsymbol{d}\,\|^2-\frac{|\,\boldsymbol{d}^{\odot}d(m)\,|^2}{\|\,d(m)\,\|^2} \tag{27}$$

故通过式(26)求积，将协方差看作多余参量求积消掉 v，可得

$$L(m)=\int_0^{\infty}L(m,v)p(v)\mathrm{d}v \tag{28}$$

其中，$p(v)=\dfrac{1}{v}$，所以似然函数可写成式(29)。

$$L(m)=\frac{(\overline{N}-1)!}{\pi^{\overline{N}}\Phi(m)^{\overline{N}}} \tag{29}$$

由上述推导和贝叶斯模型平均法可得式(30)。

$$p(u\,|\,\boldsymbol{d})=\int_M p(u,m\,|\,\boldsymbol{d})\mathrm{d}m=\int_M p(u\,|\,m,d)p(m\,|\,\boldsymbol{d})\mathrm{d}m \tag{30}$$

如果 $\boldsymbol{d}$ 中包含所有的不确定性，而且 $\boldsymbol{d}$ 中所有信息都映射到 m，则有 $p(u|m,\boldsymbol{d})=p(u|m)$。

传统描述噪声的统计量有概率密度函数、数学期望、方差或功率谱等统计量，其中功率谱是均匀噪声，即白噪声，不适用于复杂动态的水下环境噪声。目前水下数值模拟不确定性研究中，一般都将变量的方差定义为不确定性大小的度量[21]，但方差不是一种通用的不确定性度量函数，具有局限性。故本文将引入信息论中的信息熵来定量分析噪声的不确定性。对于连续变量 x，信息熵 H 定义为[22]

$$H(x)=-\int\phi(x)\mathrm{lb}\phi(x)\mathrm{d}x \tag{31}$$

由式(30)和式(31)可得应用域噪声变量 u 的信息熵为

$$H_b(p)=H(p(u\,|\,\boldsymbol{d}))=-\int_U p(u\,|\,\boldsymbol{d})\mathrm{lb}p(u\,|\,\boldsymbol{d})\mathrm{d}u \tag{32}$$

4.3 保密增强后的密钥长度下界

推论 1[10] 设 P_{VS} 是一个任意的概率分布，设 v 是敌手观测到 V 的一个特定值，若敌手关于 S 的 Rényi 熵 $R(S|V=v)$至少为 c，且节点 A 和节点 B 选择 $K=g(S)$作为其密钥，其中 g 是从 S 到$\{0,1\}^l$的全域散列函数类中随机选取的，$g\in G$，则

$$H(K\,|\,G,V=v)\geqslant H_2(K\,|\,G,V=v)\geqslant l-\mathrm{lb}(1+2^{l-c})\geqslant l-\frac{2^{l-c}}{\ln 2}$$

由文献[10]可知，$R(S|G)>R(S)$。由定理 2 可得，$c=\dfrac{nt}{2}R(S\,|\,G)>\dfrac{nt}{2}R(S)$，根据推论 1 可得

$$H(K\,|\,G,V=v)\geqslant l-\mathrm{lb}(1+2^{l-\frac{ntR(S)}{2}})\geqslant l-\frac{2^{l-\frac{ntR(S)}{2}}}{\ln 2} \tag{33}$$

令 $c'=\frac{nt}{2}R(S)-l$，由以上分析可知，当 $l<\frac{nt}{2}R(S)$ 时，敌手关于密钥 K 的不确定性接近于最大，即敌手关于密钥 K 的概率分布接近于均匀分布，节点 A 和节点 B 此时可获得密钥 l 满足式(34)。

$$l\geqslant\frac{nt}{2}R(S)+\frac{2^{l-\frac{ntR(S)}{2}}}{\ln 2} \tag{34}$$

而敌手所知道的信息与最终密钥的互信息量为

$$I(K,GV)=H(K)-H(K\mid GV)\leqslant\frac{2^{l-c'}}{\ln 2} \tag{35}$$

即敌手所知道的关于密钥 K 的信息量至多为 $\frac{2^{l-c'}}{\ln 2}$，并以 $\frac{nt}{2}R(S)-l$ 为指数递减。

定理 5　对于任意的整数 nt，存在正数 $\tau'<1$ 和使 $(1-H_b(p)-\Gamma)nt-\wp$ 为正整数的 Γ，其中，$H_b(p)$ 是 4.2 节中计算的噪声的不确定性，$\wp$ 为安全系数，在一个不安全的信道上可以执行一个保密增强协议，具体参数如下

$$(nt,D_{nt,2,\tau'\mathrm{n}t},(1-H_b(p)-\Gamma)nt-\wp,\frac{2^{l-\frac{ntR(S)}{2}}}{\ln 2},\delta)$$

其中，$\delta=\max((1-\theta')^{\frac{n}{2}},\left(\frac{1}{\sum_{\mho=0}^{\frac{n}{2}}C_{\frac{n}{2}}^{\mho}}\right)\theta'^{\mho}(1-\theta')^{\frac{n}{2}-\mho})$，$\theta'$ 为敌手预估信息的错误比特率，$\mho$ 为每个校验块中敌手与节点 A 和节点 B 不一致的位数，l 是最终提取的密钥长度，$R(S)$是原来部分保密串 S 的 Rényi 熵，nt 是节点 A 和节点 B 密钥协商时所获得的公共串。

证明　设 V 是敌手所窃听到的关于原串 S 信息的随机变量，某个特定的 $v\in V$，由定义 1 可知，$H_2(S|V=v)\geqslant\tau' nt$，由式(32)可知 $H_b(p)$的值，令

$$l=(1-H_b(p)-\Gamma)nt-\wp \tag{36}$$

由推论 1 知：

$$H_2(K\mid G,V=v)\geqslant l-\frac{2^{l-\frac{ntR(S)}{2}}}{\ln 2} \tag{37}$$

即定义 1 中的 $\varepsilon=\frac{2^{l-\frac{ntR(S)}{2}}}{\ln 2}$，由定理 4 可知，敌手主动攻击成功的最大概率为

$$\delta=\max((1-\theta')^{\frac{n}{2}},\left(\frac{1}{\sum_{\mho=0}^{\frac{n}{2}}C_{\frac{n}{2}}^{\mho}}\right)\theta'^{\mho}(1-\theta')^{\frac{n}{2}-\mho})$$

综上，可得定义 1 中的对应参数值，从而得到定理 5 中的保密增强协议。证毕。

5　实验结果与分析

该实验使用的硬件环境是 Intel® Core™ i5-3337U CPU@1.80 GHz，4 GB RAM，编程环境是 Matlab R2014*a*。令每一次密钥协商过程中传输的位数 n=300，密钥协商次数 t 分别取 t_1=20，t_2=30，t_3=40，敌手获取信息的不确定度的实验结果如图 4 所示。

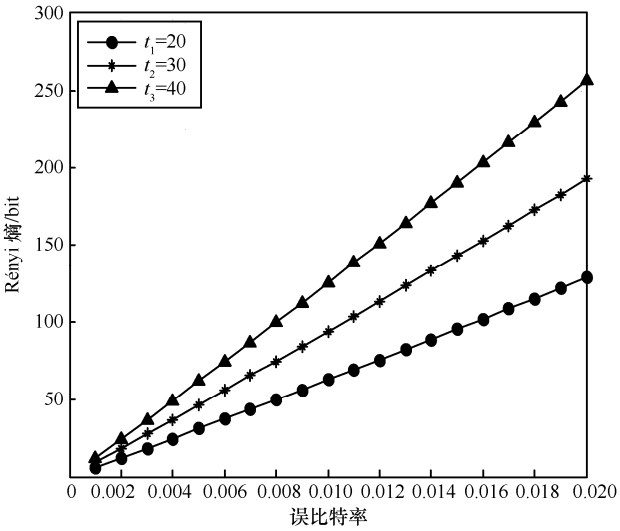

图 4　敌手关于 *nt* bit 密钥串信息的不确定度

图 4 中 3 条曲线均为 n=300 条件下，分别对应不同密钥协商次数时敌手关于 *nt* bit 密钥串信息的不确定度。其中，横轴表示敌手在水下噪声信道中产生的误比特率，纵轴表示敌手关于 *nt* bit 密钥串信息的 Rényi 熵，即信息的不确定度。从图 4 可以看出 3 条曲线的拟合程度均近似为一次函数，并且敌手关于信息的 Rényi 熵均随着误比特率和密钥协商次数的增加而增加，说明进行多次密钥协商可以增加敌手对密钥串的不确定性，使密钥的安全性更高。

当节点 A 和节点 B 的误比特率 λ 及密钥协商次数 t 取不同值时，建立密钥执行协议次数 N'的期望值如表 1 所示。

表 1　密钥执行协议次数 N'的期望值

次数	λ=0.001	λ=0.0015	λ=0.002
t_1=20	19.99	89.41	399.81
t_2=30	89.11	841.18	7 940.54
t_3=40	396.23	7 887.04	156 994.80

从表 1 可以得出，N'的期望值与误码率 λ、次数 t 及密钥串的长度 n 均有关系。当 λ=0.001 时，协议的执行效率最高。在水声通信中，数据传输速率最大可达 10 kbit/s[23]。当 n=300，t=20，N'=19.99 时，密钥协商传输的总位数为 119 940 bit，保密增强后生成的密钥串总长度的下界为 117 331 bit，敌手关于密钥串信息量的上界为 2 609 bit，所需时间为 11.99 s。表明在现有技术条件下，该协议是切实可行的。

6　结束语

本文设计了海洋噪声不确定性环境下基于哥德尔编码的交互式密钥提取协议和基于 r–循环 Toeplitz 矩阵的保密增强协议，从而构成了基于水下噪声信道不确定性的保密通信方案。理论分析和实验结果表明，该方案不仅安全可靠，而且通信效率较高，通信开销较小，同时降低了矩阵的存储空间，提高了保密增强的存储效率，并且得出了保密增强后密钥串长度的下界和敌手关于密钥串信息量的上界。

参考文献：

[1] HAN G, JIANG J, SUN N, et al. Secure communication for underwater acoustic sensor networks[J]. IEEE Communications Magazine, 2015, 53(8): 54-60.

[2] LAL C, PETROCCIA R, PELEKANAKIS K, et al. Toward the development of secure underwater acoustic networks[J]. IEEE Journal of Oceanic Engineering, 2017, 42(4):1075-1087.

[3] CHEN K, MA M, CHENG E, et al. A survey on MAC protocols for underwater wireless sensor networks[J]. IEEE Communications Surveys & Tutorials, 2014, 16(3): 1433-1447.

[4] 笪良龙. 海洋水声环境效应建模与应用[M]. 北京：科学出版社, 2012.
DA L L. Modeling and application of oceanic acoustic environmental effect[M]. Beijing: Science Press, 2012.

[5] GÖDEL K. On formally undecidable propositions of principia mathematica and related systems[M]. Courier Corporation, 1992.

[6] BENNETT C H, BRASSARD G, ROBERT J M. Privacy amplification by public discussion[J]. Siam Journal on Computing, 1988, 17(2): 210-229.

[7] HAYASHI M, TAN Y F. Equivocations, exponents, and second-order coding rates under various Rényi information measures[J]. IEEE Transactions on Information Theory, 2017, 63(2): 975-1005.

[8] JIANG Z, ZHOU J. A note on spectral norms of even-order r-circulant matrices[J]. Applied Mathematics and Computation, 2015, 250: 368-371.

[9] KRESSNER D, LUCE R. Fast computation of the matrix exponential for a Toeplitz matrix[J]. SIAM Journal on Matrix Analysis and Applications, 2018, 39(1): 23-47.

[10] BENNETT C H, BRASSARD G, CREPEAU C, et al. Generalized privacy amplification[J]. IEEE Transactions on Information Theory, 1995, 41(6):1915-1923.

[11] ANCEAUME E, BUSNEL Y. A distributed information divergence estimation over data streams[J]. IEEE Transactions on Parallel and Distributed Systems, 2014, 25(2): 478-487.

[12] HAYASHI M. Security analysis of ε-almost dual universal$_2$ hash functions: smoothing of min entropy vs. smoothing of Rényi entropy of order 2 [J]. IEEE Transactions on Information Theory, 2016, 62(6): 3451-3476.

[13] WEGMAN M N, CARTER J L. New hash functions and their use in authentication and set equality[J]. Journal of Computer and System Sciences, 1981, 22(3): 265-279.

[14] MAURER U, WOLF S. Secret-key agreement over unauthenticated public channels-part Ⅲ: privacy amplification[J]. IEEE Transactions on Information Theory, 2003, 49(4): 832-838.

[15] BERTA M, FAWZI O, SCHOLZ V. Quantum-proof randomness extractors via operator space theory[J]. IEEE Transactions on Information Theory, 2017, 63(4): 2480-2503.

[16] MILLER C A, SHI Y. Robust protocols for securely expanding randomness and distributing keys using untrusted quantum devices[J]. Journal of the ACM, 2016, 63(4): 33.

[17] TAN Y F, HAYASHI M. Analysis of remaining uncertainties and exponents under various conditional Rényi entropies[J]. IEEE Transactions on Information Theory, 2018, 64(5): 3734-3755.

[18] ISHII M, DETREY J, GAUDRY P, et al. Fast modular arithmetic on the Kalray MPPA-256 processor for an energy-efficient implementation of ECM[J]. IEEE Transactions on Computers, 2017, 66(12): 2019-2030.

[19] KRAFT J, WASHINGTON L. An introduction to number theory with cryptography[M]. Chapman and Hall/CRC Press, 2018.

[20] HAYASHI M, TSURUMARU T. More efficient privacy amplification with less random seeds via dual universal hash function[J]. IEEE Transactions on Information Theory, 2016, 62(4): 2213-2232.

[21] BARDENET R, DOUCET A, HOLMES C. On Markov chain Monte Carlo methods for tall data[J]. The Journal of Machine Learning Research, 2017, 18(1): 1515-1557.

[22] 王栋, 吴吉春. 信息熵理论在水系统中的研究与应用[M]. 北京：中国水利水电出版社, 2012.
WANG D, WU J C. Research and application of Information entropy theory in water system[M]. Beijing: China Water and Power Press, 2012.

[23] AMAR A, AVRASHI G, STOJANOVIC M. Low complexity residual doppler shift estimation for underwater acoustic multicarrier communication[J]. IEEE Transactions on Signal Processing, 2017, 65(8): 2063-2076.

[作者简介]

徐明（1977– ），男，安徽马鞍山人，博士，上海海事大学副教授，主要研究方向为无线通信网络、网络空间安全等。

陈芳（1994– ），女，安徽安庆人，上海海事大学硕士生，主要研究方向为保密增强、网络空间安全等。