水下声通信物理层密钥生成方案

刘景美，沈志威，韩庆庆，刘景伟
（西安电子科技大学通信工程学院，陕西 西安 710071）

摘 要：为确保水下无人艇的通信安全，提出一种基于正交频分复用系统的水下声信道物理层密钥生成方案。首先，提出一个本地导频辅助信道探测协议，解决了由于水声信道中传播时延较大引起的互易性受损问题，保证密钥随机性，增强对邻近窃听者的防御能力；其次，提出一个双层补偿聚合结合自适应保护间隔的量化方法，提升了密钥一致性且使密钥生成速率维持在较高水平。仿真结果显示，所提方案有效地克服了水声通信中互易性受损的问题，且在密钥一致性优于现有水声密钥生成方案的前提下保证了高密钥生成速率和较高的随机性。

关键词：水下无人艇；本地导频；密钥生成；邻近窃听者；补偿聚合量化
中图分类号：TN918.8^{+}2
文献标识码：A
doi: 10.11959/j.issn.1000−436x.2019027

Underwater acoustic communication physical layer key generation scheme

LIU Jingmei, SHEN Zhiwei, HAN Qingqing, LIU Jingwei
School of Telecommunications Engineering, Xidian University, Xi'an 710071, China

Abstract: To ensure the communication safety of unmanned underwater vehicle, a physical layer key generation scheme of underwater acoustic channel based on orthogonal frequency division multiplexing (OFDM) system was proposed. First, a local pilot assistance channel sounding protocol was proposed to solve the reciprocity impaired caused by the great propagation delay in the underwater acoustic channel, ensure high key randomness and enhance the defenses against nearby eavesdroppers. Secondly, double-layer compensation centralized combined with adaptive guard interval quantization method was proposed to improve key agreement rate and key generation rate. Simulation results show that the scheme effectively overcomes the problems of impaired reciprocity and ensures high key generation rate and high randomness on the premise that the key agreement is superior to the existing schemes.

Key words: unmanned underwater vehicle, local pilot, key generation, nearby eavesdroppers, compensation centralized quantization

1 引言

近年来，物理层密钥生成技术凭借其特有的优点（理论安全、算法简单、不需要预分发等）引起了学术界的广泛关注。目前，已有大量关于密钥生成技术的研究。文献[1]将密钥生成技术应用于跳频系统。文献[2-3]研究了双方不在彼此通信范围内时利用中继节点辅助密钥生成的方案。文献[4-5]研究了小组通信中的密钥生成。文献[6-7]提出了适合应用在频分双工（FDD, frequency division duplex）无互易系统中的物理层密钥生成技术。文献[8-10]将密钥生成技术拓展至水下声系统中。文献[8]首次提出在水声通信系统中应用物理层密钥生成技术。文献[9]提出利用接收信号强度作为信道特征进行水下

收稿日期：2018−02−05；**修回日期**：2018−04−29
通信作者：沈志威，trio_zwshen@163.com
基金项目：教育部联合基金资助项目（No.6141A02022338）
Foundation Item: The Joint Fund of Ministry of Education of China (No.6141A02022338)

密钥生成，利用正交频分复用（OFDM, orthogonal frequency division multiplexing）系统加快密钥生成速率（KGR, key generation rate），利用平滑滤波器提高密钥一致率（KAR, key agreement rate），并比较了几种不同的量化方式下的密钥一致性。文献[10]利用信道频率响应（CFR, channel frequency response）作为信道特征，提出了一种通过自适应导频以及分块密钥认证来提高一致率的方案，并通过水下环境实测，检验了通信双方测量值的相关性。

然而已有的水下密钥生成技术都假设在较为理想的情况。文献[9]只是将一系列传统的密钥生成技术应用于水下环境，OFDM 系统和平滑滤波器都是常见的密钥生成技术[11-14]，没有讨论生成密钥的随机性以及 KGR。文献[10]忽略了多普勒频移影响，即忽略了物体移动，然而实际的应用场景往往都是动态变化的，如水下无人艇的通信。此外，已有研究都没有考虑水下声系统中互易性受损这一问题。由于在水下通信中往往采用水声作为通信载体[15]，而水声的传播速度仅有 1 500 m/s，传播速度较小，导致传播时延极大，从而使得信道的短时互易性不再有效。

目前，常见的密钥生成技术往往分成 4 个步骤：信道探测（获取测量值）、量化（将测量值模数转换）、信息调和（误差纠正）以及隐私放大（密钥确认与随机性放大）[16]。而本文根据水声信道的特点，考虑了文献[9-10]中未考虑的因素，针对密钥生成的前 2 个环节分别提出如下改进方案：1) 从 FDD 系统的密钥生成方案[7]中得到启发，针对互易性受损的情况，提出一种本地导频辅助信道探测协议以适应水下声系统；2)考虑动态环境对密钥生成的影响，将文献[17]的相位偏移量化方法拓展，提出双层补偿聚合结合自适应保护间隔（DLCC_AGI, double-layer compensation centralized and adaptive guard interval quantization）的量化方案以提高 KAR 和 KGR；3)从 KAR、KGR 以及随机性这 3 个方面全面地讨论了本方案的性能。

2 信道探测方案

声波在水中的传播速度很慢，即使通信距离仅有几十米，也会产生远大于相干时间(T_C)的传播时延(T_{delay})，导致通信双方的测量值之间相干性极低，因此基于信道互易性的传统方案很难直接应用。本文受文献[7]中 FDD 非互易系统密钥生成方案的启发，提出应对互易性受损问题的本地导频辅助信道探测协议。

2.1 探测协议

图 1 为本方案的信道探测过程，其中，Alice、Bob 代表通信双方。

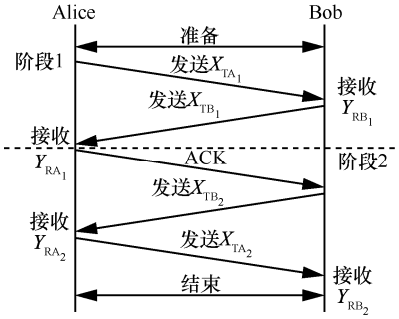


图 1 本地导频辅助协议

阶段 1 和阶段 2 类似，因此仅描述阶段 1 的过程。收发信号中，$\boldsymbol{X}_{\mathrm{TA}_1}$ 表示 Alice 的探测信号，$\boldsymbol{X}_{\mathrm{TB}_1}$ 表示 Bob 的探测信号，$\boldsymbol{Y}_{\mathrm{RB}_1}$ 表示 Bob 的接收信号，$\boldsymbol{Y}_{\mathrm{RA}_1}$ 表示 Alice 的接收信号，$\boldsymbol{W}_{\mathrm{A}}$ 与 $\boldsymbol{W}_{\mathrm{B}}$ 表示高斯白噪声信号，且上述信号都是 N 维列向量；$\boldsymbol{X}_{\mathrm{P}}$ 表示公共导频信号，$\boldsymbol{X}_{\mathrm{R}}$ 与 $\boldsymbol{V}_{\mathrm{A}}$ 表示 Alice 的本地导频信号，$\boldsymbol{V}_{\mathrm{B}}$ 表示 Bob 的本地导频信号，$\boldsymbol{Y}_{\mathrm{B}_1}$ 表示 Bob 接收信号的奇数行集合，$\boldsymbol{Y}_{\mathrm{B}_2}$ 表示 Bob 接收信号的偶数行集合，$\boldsymbol{Y}_{\mathrm{A}_1}$ 表示 Alice 接收信号的奇数行集合，$\boldsymbol{Y}_{\mathrm{A}_2}$ 表示 Alice 接收信号的偶数行集合，$\boldsymbol{M}_{\mathrm{A}}$ 是一个中间变量，$\boldsymbol{R}_{\mathrm{A}_1}$ 与 $\boldsymbol{R}_{\mathrm{B}_1}$ 分别表示 Alice 与 Bob 在第一阶段获得的估计值，上述信号都是 $\frac{N}{2}$ 维的列向量。

在时不变多径信道（保证一个相干时间内不变）中一个具有 N 个子载波的 OFDM 符号，所经历的多径信道在频域表现为一个对角阵[18]。而水声信道往往可以抽象为一个多径信道。因此，以 $\boldsymbol{X}_{\mathrm{TA}_1}$ 发送的过程为例（如式(1)所示），结合信道探测流程可以得到图 2 所示的忽略噪声影响的收发信号帧结构。

$$\begin{bmatrix} Y_{\mathrm{RB}_1}(1) \\ \vdots \\ Y_{\mathrm{RB}_1}(N) \end{bmatrix} = \begin{bmatrix} H_{\mathrm{AB}}(1) & & \\ & \ddots & \\ & & H_{\mathrm{AB}}(N) \end{bmatrix} \begin{bmatrix} X_{\mathrm{TA}_1}(1) \\ \vdots \\ X_{\mathrm{TA}_1}(N) \end{bmatrix} + \begin{bmatrix} W_{\mathrm{B}}(1) \\ \vdots \\ W_{\mathrm{B}}(N) \end{bmatrix} = \begin{bmatrix} H_{\mathrm{AB}}(1)X_{\mathrm{R}}(1) + W_{\mathrm{B}}(1) \\ H_{\mathrm{AB}}(2)V_{\mathrm{A}}(1)X_{\mathrm{P}}(1) + W_{\mathrm{B}}(2) \\ \vdots \\ H_{\mathrm{AB}}(N-1)X_{\mathrm{R}}\left(\frac{N}{2}\right) + W_{\mathrm{B}}(N-1) \\ H_{\mathrm{AB}}(N)V_{\mathrm{A}}\left(\frac{N}{2}\right)X_{\mathrm{P}}\left(\frac{N}{2}\right) + W_{\mathrm{B}}(N) \end{bmatrix} \tag{1}$$

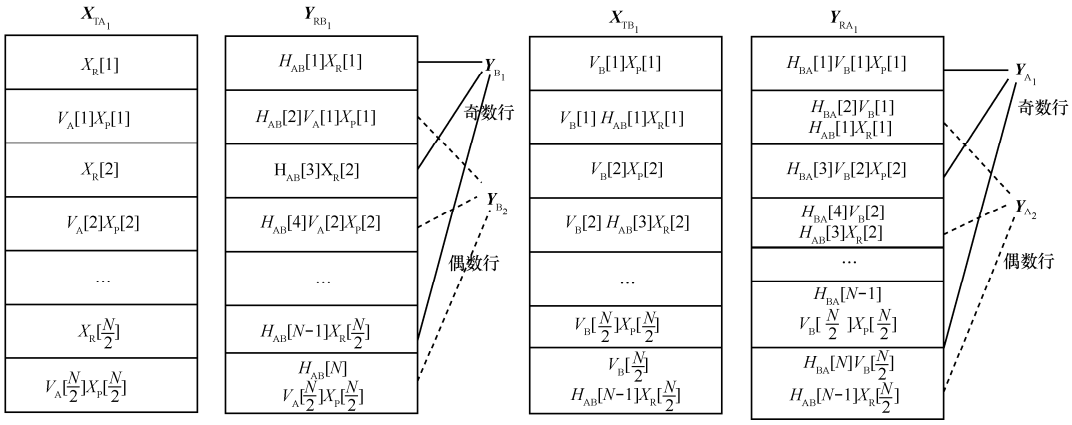


图 2　阶段 1 收发信号

步骤 1　Alice 与 Bob 生成一个公开导频 $\boldsymbol{X}_{\mathrm{P}}$，Alice 生成本地导频 $\boldsymbol{X}_{\mathrm{R}}$ 与 $\boldsymbol{V}_{\mathrm{A}}$，Bob 生成本地导频 $\boldsymbol{V}_{\mathrm{B}}$。

步骤 2　Alice 生成并发送如图 2 所示导频信号 $\boldsymbol{X}_{\mathrm{TA}_1}$，如式(2)所示，其中 f 表示频率。

$$X_{\mathrm{TA}_1}(f)=\begin{cases} X_{\mathrm{R}}\left(\left\lfloor\dfrac{f}{2}\right\rfloor+1\right) \\ V_{\mathrm{A}}\left(\left\lfloor\dfrac{f}{2}\right\rfloor\right)X_{\mathrm{P}}\left(\left\lfloor\dfrac{f}{2}\right\rfloor\right)\end{cases}=\begin{cases} X_{\mathrm{R}}(j), & f=2j-1 \\ V_{\mathrm{A}}(j)X_{\mathrm{P}}(j), & f=2j\end{cases},\quad j=1,2,\cdots,\frac{N}{2} \tag{2}$$

步骤 3　Bob 接收 $\boldsymbol{Y}_{\mathrm{RB}_1}$，如式(3)所示。

$$Y_{\mathrm{RB}_1}(f)=\begin{cases} Y_{\mathrm{B}_1}(j)=H_{\mathrm{AB}}(f)X_{\mathrm{R}}\left(\left\lfloor\dfrac{f}{2}\right\rfloor+1\right)+W_{\mathrm{B}}(f) \\ Y_{\mathrm{B}_2}(j)=H_{\mathrm{AB}}(f)V_{\mathrm{A}}\left(\left\lfloor\dfrac{f}{2}\right\rfloor\right)X_{\mathrm{P}}\left(\left\lfloor\dfrac{f}{2}\right\rfloor\right)+W_{\mathrm{B}}(f)\end{cases}=\begin{cases} H_{\mathrm{AB}}(2j-1)X_{\mathrm{R}}(j)+W_{\mathrm{B}}(2j-1), f=2j-1 \\ H_{\mathrm{AB}}(2j)V_{\mathrm{A}}(j)X_{\mathrm{P}}(j)+W_{\mathrm{B}}(2j), f=2j\end{cases},\quad j=1,2,\cdots,\frac{N}{2} \tag{3}$$

将 $\boldsymbol{Y}_{\mathrm{RB}_1}$ 的奇数行合并为 $\boldsymbol{Y}_{\mathrm{B}_1}$，偶数行合并为 $\boldsymbol{Y}_{\mathrm{B}_2}$，根据 $\boldsymbol{Y}_{\mathrm{B}_2}$ 与 $\boldsymbol{X}_{\mathrm{P}}$ 以最小二乘估计得到 $\boldsymbol{R}_{\mathrm{B}_1}$，如式(4)所示。

$$R_{\mathrm{B}_1}(j)=\frac{Y_{\mathrm{B}_2}(j)}{X_{\mathrm{P}}(j)}=H'_{\mathrm{AB}}(2j)V'_{\mathrm{A}}(j),\quad j=1,2,\cdots,\frac{N}{2} \tag{4}$$

步骤 4　Bob 生成并发送如图 2 所示的导频信号 $\boldsymbol{X}_{\mathrm{TB}_1}$，如式(5)所示。

$$X_{\mathrm{TB}_1}(f)=\begin{cases} V_{\mathrm{B}}\left(\left\lfloor\dfrac{f}{2}\right\rfloor+1\right)X_{\mathrm{P}}\left(\left\lfloor\dfrac{f}{2}\right\rfloor+1\right) \\ V_{\mathrm{B}}\left(\left\lfloor\dfrac{f}{2}\right\rfloor\right)Y_{\mathrm{B}_1}\left(\left\lfloor\dfrac{f}{2}\right\rfloor\right)\end{cases}=\begin{cases} V_{\mathrm{B}}(j)X_{\mathrm{P}}(j), & f=2j-1 \\ V_{\mathrm{B}}(j)\left\{H_{\mathrm{AB}}(2j-1)X_{\mathrm{R}}(j)+W_{\mathrm{B}}(2j-1)\right\}, & f=2j\end{cases},j=1,2,\cdots,\frac{N}{2} \tag{5}$$

步骤 5　Alice 接收 $\boldsymbol{Y}_{\mathrm{RA}_1}$，如式(6)所示。

$$\begin{aligned} Y_{\mathrm{RA}_1}(f)&=\begin{cases} Y_{\mathrm{A}_1}(j)=H_{\mathrm{BA}}(f)V_{\mathrm{B}}\left(\left\lfloor\dfrac{f}{2}\right\rfloor+1\right)X_{\mathrm{P}}\left(\left\lfloor\dfrac{f}{2}\right\rfloor+1\right)+W_{\mathrm{A}}(f) \\ Y_{\mathrm{A}_2}(j)=H_{\mathrm{BA}}(f)V_{\mathrm{B}}\left(\left\lfloor\dfrac{f}{2}\right\rfloor\right)\left\{H_{\mathrm{AB}}(f-1)X_{\mathrm{R}}\left(\left\lfloor\dfrac{f}{2}\right\rfloor\right)+W_{\mathrm{B}}(f-1)\right\}+W_{\mathrm{A}}(f)\end{cases} \\ &=\begin{cases} H_{\mathrm{BA}}(2j-1)V_{\mathrm{B}}(j)X_{\mathrm{P}}(j)+W_{\mathrm{A}}(2j-1), f=2j-1 \\ H_{\mathrm{BA}}(2j)V_{\mathrm{B}}(j)\left\{H_{\mathrm{AB}}(2j-1)X_{\mathrm{R}}(j)+W_{\mathrm{B}}(2j-1)\right\}+W_{\mathrm{A}}(2j), f=2j\end{cases},\quad j=1,2,\cdots,\frac{N}{2}\end{aligned} \tag{6}$$

将 $\boldsymbol{Y}_{\mathrm{RA}_1}$ 的奇数行合并为 $\boldsymbol{Y}_{\mathrm{A}_1}$，偶数行合并为 $\boldsymbol{Y}_{\mathrm{A}_2}$，由 $\boldsymbol{Y}_{\mathrm{A}_1}$ 与 $\boldsymbol{X}_{\mathrm{P}}$ 通过最小二乘估计可以得到 $\boldsymbol{M}_{\mathrm{A}}$。

$$M_{\mathrm{A}}(j)=\frac{Y_{\mathrm{A}_1}(j)}{X_{\mathrm{P}}(j)}=H'_{\mathrm{BA}}(2j-1)V'_{\mathrm{B}}(j),\quad j=1,2,\cdots,\frac{N}{2} \tag{7}$$

由于相邻子载波的载波间隔很小，即相干性很大，可得如下关系。

$$\begin{aligned}&H_*(2j)\approx H_*(2j-1),\\&j=1,2,\cdots,\frac{N}{2},*\in\{\mathrm{AB},\mathrm{BA}\}\end{aligned} \tag{8}$$

因此，可以根据 $\boldsymbol{M}_{\mathrm{A}}$、$\boldsymbol{X}_{\mathrm{R}}$、$\boldsymbol{Y}_{\mathrm{A}_2}$ 以及 $\boldsymbol{V}_{\mathrm{A}}$ 求得 $\boldsymbol{R}_{\mathrm{A}_1}$。

$$R_{\mathrm{A}_1}(j)=\frac{Y_{\mathrm{A}_2}(j)V_{\mathrm{A}}(j)}{M_{\mathrm{A}}(j)X_{\mathrm{R}}(j)}=H'_{\mathrm{AB}}(2j-1)V_{\mathrm{A}}(j),\ j=1,2,\cdots,\frac{N}{2} \tag{9}$$

由于子载波之间的相干性，通信双方的测量值近似相等（$\boldsymbol{R}_{\mathrm{A}_1}\approx\boldsymbol{R}_{\mathrm{B}_1}$），阶段 2 中同理可得 $\boldsymbol{R}_{\mathrm{A}_2}\approx\boldsymbol{R}_{\mathrm{B}_2}$。由于受到噪声的影响，最小二乘估计的准确性下降，尤其在信噪比较差时噪声将会严重影响密钥生成技术的 KAR 性能，因此本文采用平滑滤波器以减小噪声影响。此外，本方案中采用频域插值以增大相邻子载波间的相关性。

2.2 安全性分析

本探测方案中，窃听者 Eve（距离合法通信者半波长以上）已知公共导频 $\boldsymbol{X}_{\mathrm{P}}$，可针对 $\boldsymbol{X}_{\mathrm{TA}_1}$ 发送过程中的偶数行估计得到 $H_{\mathrm{AE}}(2j)V_{\mathrm{A}}(j)$。然而随机数向量 $\boldsymbol{V}_{\mathrm{A}}$ 仅 Alice 可知，所以窃听者无法获取其自身与合法通信者之间的任何信道信息（$\boldsymbol{H}_{\mathrm{AE}}$ 和 $\boldsymbol{H}_{\mathrm{BE}}$），因此窃听者也无法获得 $\boldsymbol{X}_{\mathrm{TA}_1}$ 奇数行中的 $\boldsymbol{X}_{\mathrm{R}}$ 导频信号。同理在后续步骤中利用奇数行中的 $\boldsymbol{V}_{\mathrm{B}}$ 保护信道以及 $\boldsymbol{X}_{\mathrm{TB}_1}$ 偶数行中的信息。窃听者无法获取通信双方用于生成密钥的测量值，所以本方案是在保证密钥生成安全的前提下解决了互易性受损的问题。

此外，假设 Eve 距离 Bob 足够近，便可以接收到和 Bob 一样的信号，即 $\boldsymbol{Y}_{\mathrm{RB}_1}$（阶段 1）与 $\boldsymbol{Y}_{\mathrm{RB}_2}$（阶段 2），且由于 $\boldsymbol{X}_{\mathrm{P}}$ 是公开的，Eve 可以根据 $\boldsymbol{Y}_{\mathrm{RB}_1}$ 中的偶数行 $\boldsymbol{Y}_{\mathrm{B}_2}$ 获得阶段 1 的测量值 $\boldsymbol{R}_{\mathrm{B}_1}$。但在阶段 2 中，Bob 地位类似于阶段 1 中的 Alice，若要获取 $\boldsymbol{R}_{\mathrm{B}_2}$ 需要 Bob 的本地信号 $\boldsymbol{X}_{\mathrm{R}}$ 和 $\boldsymbol{V}_{\mathrm{A}}$，而 Eve 无法获知，因此 Eve 无法获得阶段 2 的测量值。换言之，当存在一个窃听者足够靠近 Bob 或 Alice 时，该窃听者可以获得一半的测量值信息，但是无法获取全部的信道测量值。综上所述，窃听者可获信息如表 1 所示。

表 1 窃听者可获信息

窃听者位置	窃听者获得信息
距离被窃听者足够远	$H_{\mathrm{AE}}(2j)V_{\mathrm{A}}(j)$，$H_{\mathrm{BE}}(2j-1)V_{\mathrm{B}}(j)$
靠近 Alice	$H_{\mathrm{AE}}(2j)V_{\mathrm{A}}(j)$，$H_{\mathrm{BA}}(2j-1)V_{\mathrm{B}}(j)$ $(\boldsymbol{R}_{\mathrm{A}_2})$
靠近 Bob	$H_{\mathrm{AB}}(2j)V_{\mathrm{A}}(j)$ $(\boldsymbol{R}_{\mathrm{B}_1})$，$H_{\mathrm{BE}}(2j-1)V_{\mathrm{B}}(j)$

2.3 本地导频辅助信道探测协议的优点

根据 2.1 节和 2.2 节对本地导频辅助信道探测协议的分析，可知该协议具有如下优势。

1) 通过子载波之间的相关性将密钥生成技术有效地拓展至时分双工水下声通信系统，解决了水声信道互易性受损的问题.

2) 在通信双方探测信号生成的过程中加入本地随机数矢量 $\boldsymbol{V}_{\mathrm{A}}$ 和 $\boldsymbol{V}_{\mathrm{B}}$，提高了生成密钥的随机性，使得生成密钥的随机性在信道环境变化极其缓慢的情况下也可以得到保证。

3) 传统密钥生成方案无法防范邻近窃听者的窃听，但是本方案可以在存在一个邻近窃听者的情况下依旧保持安全。

3 补偿聚合量化

引入量化环节是为了将信道测量值转换成 0、1 比特序列，适当的量化方法可以有效提高 KAR 与 KGR。本文将相位偏移量化方法[17]拓展到 CFR 情况，并提出双层补偿聚合量化以提高密钥一致性与密钥生成速率，同时利用了测量值的实部与虚部，进一步提高了 KGR，具体步骤如下。

步骤 1 Alice：根据 Alice 的测量值序列 $\boldsymbol{A}$，通过累积分布函数（CDF, cumulative distribution function）[16]自适应生成量化门限，将测量值序列 $\boldsymbol{A}$ 判决为其所在量化域的中心，得到中心序列 $\boldsymbol{A}'$。

步骤 2 Alice：计算 $\boldsymbol{\Delta}_{\mathrm{a}}=\boldsymbol{A}-\boldsymbol{A}'$，并将其发送给 Bob。

步骤 3 Bob：计算 $\boldsymbol{B}'=\boldsymbol{B}-\boldsymbol{\Delta}_{\mathrm{a}}=\boldsymbol{B}-\boldsymbol{A}+\boldsymbol{A}'=\boldsymbol{W}+\boldsymbol{A}'$。

步骤 4 Bob：根据补偿后的测量值 $\boldsymbol{B}'$，通过 CDF 生成量化门限，并生成中心序列 $\boldsymbol{B}''$。

步骤 5 Bob：计算 $\boldsymbol{\Delta}_{\mathrm{b}}=\boldsymbol{B}'-\boldsymbol{B}''$，并将其发送给 Alice。

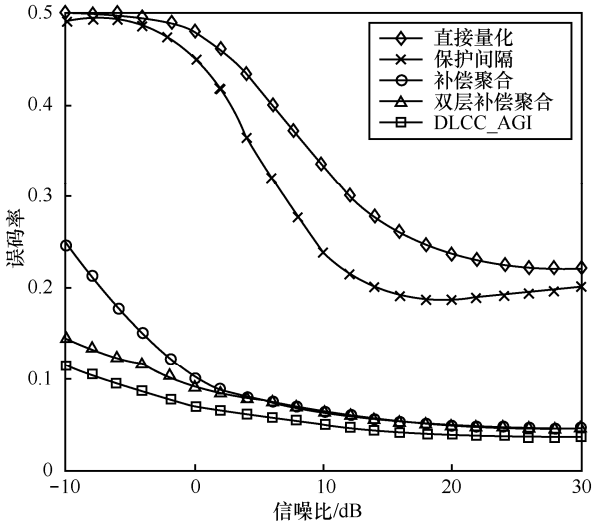
步骤 6 Alice：计算 $\boldsymbol{A}''=\boldsymbol{A}'-\boldsymbol{\Delta}_{\mathrm{b}}=\boldsymbol{A}'-\boldsymbol{B}'+\boldsymbol{B}''=\boldsymbol{A}'-\boldsymbol{W}-\boldsymbol{A}'+\boldsymbol{B}''=\boldsymbol{B}''-\boldsymbol{W}$。

步骤 7 分别对 $\boldsymbol{B}'$和 $\boldsymbol{A}''$进行量化。

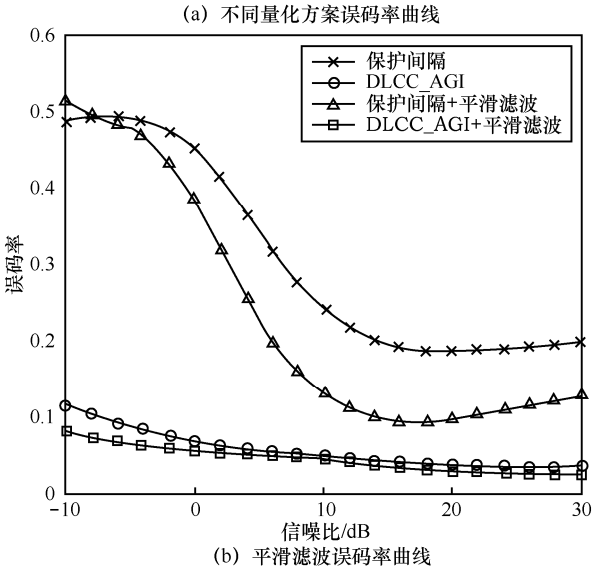
经过步骤 1~步骤 3 处理后（称为单层聚合补偿），测量值序列 $\boldsymbol{B}$ 被聚合到测量值序列 $\boldsymbol{A}$ 的量化域中心附近，得到测量值序列 $\boldsymbol{B}'$。步骤 4~步骤 6 同理将 Alice 的测量值 $\boldsymbol{A}$ 聚合到测量值序列 $\boldsymbol{B}'$的量

化域中心附近。由于通信双方的测量值都在对方根据测量值自适应生成的量化域的中心附近噪声振幅范围内，因此只需保证最小量化域 $\min\{R_{\text{ange}}\}$的一半大于噪声的振幅，即可无误差量化。

图 3(a)比较了 5 种量化方法，可以发现本文提出的补偿聚合量化方案在 KAR 方面明显优于文献[9]采用的单比特直接量化和保护间隔量化，且双层补偿的方式能更进一步提升密钥一致性，将双层补偿聚合的方法与文献[16]提出的自适应保护间隔结合提出 DLCC_AGI 量化，得到了极高的密钥一致性，验证了本文提出的 DLCC_AGI 在 KAR 方面的优越性。图 3(b)比较了有无采用平滑滤波的方案，验证了平滑滤波能够适用于本文提出的水下声密钥生成方案中，即使信道互易性极差。



(a) 不同量化方案误码率曲线



(b) 平滑滤波误码率曲线

图 3　未加工密钥一致率曲线

4　仿真结果与性能分析

在第 2 和第 3 节中已经详细介绍了本文采用的信道探测技术与量化技术，但应注意量化后生成的比特序列仅是未加工的密钥，还需要进行信息调和与隐私放大 2 个步骤来获取最终密钥。由于本文的重点在于探究信道探测和量化环节，因此对于信息调和与隐私放大仅选用已有的（31，16，3）BCH 码以及文献[10]提出的散列函数分块确认机制。

本文采用Matlab进行数值仿真，仿真参数见表2。

表 2　　仿真参数

项目	说明
OFDM 水下声系统参数	子载波数 N=256，循环前缀 CP=64，载频 F_C=10 000 Hz，带宽 B=18 000 Hz，符号总长 $T_{\text{sym}}=T_{\text{sub}}+T_{\text{cp}}$=0.017 8 s
通信双方参数	移动速度 5 节，v=2.5 m/s，通信距离 d_{AB}=500 m，传播时延 $T_{\text{delay}}\approx$0.333 s
水下声信道参数	最大多普勒频移 F_{d}=16.67 Hz，相干时间 $T_{\text{C}}\approx$0.03 s，多径数 N_{ray}=25

4.1　误码率

本节主要比较了本方案在不同移动速度下的密钥一致性，图 3 比较了不同量化方案下未加工密钥的一致性，可知本文提出的 DLCC_AGI 量化方法能够有效提高密钥一致性。

图 4 比较了水下无人艇相对移速分别为 1 节、5 节、10 节时调和后密钥的 KAR。本文首先对密钥序列进行交织，而后采用（31，16，3）BCH 码调和。图 4(a)比较了密钥的误码率(BER, bit error rate)，图 4(b)比较了子密钥错误率(SKER, sub-key error rate) ,即子密钥出现错误的概率，取子密钥长度 N_{Block} = 16。由仿真结果可知，移速越高，密钥一致性越差，因为移速提高将会导致多普勒频移升高，从而降低一致性。但是本文方案生成的密钥可以确保即使在信噪比较低且移速较快的情况下，依旧保持 BER<0.1，SKER<0.05。

4.2　密钥生成速率

由于经过信息调和后得到的密钥序列中依旧会存在错误比特，因而不能直接将其作为密钥使用，本文通过文献[10]提出的散列函数分块确认方法来获得最终的密钥。该方法可以保证获得一致的密钥，但是需要丢弃部分子密钥。由于本文方案已经可以保证即使在信噪比极低的高速移动环境中，

SKER 依旧保持在 0.05 以下，因此在大多数场景中将会获得较好的 KGR。

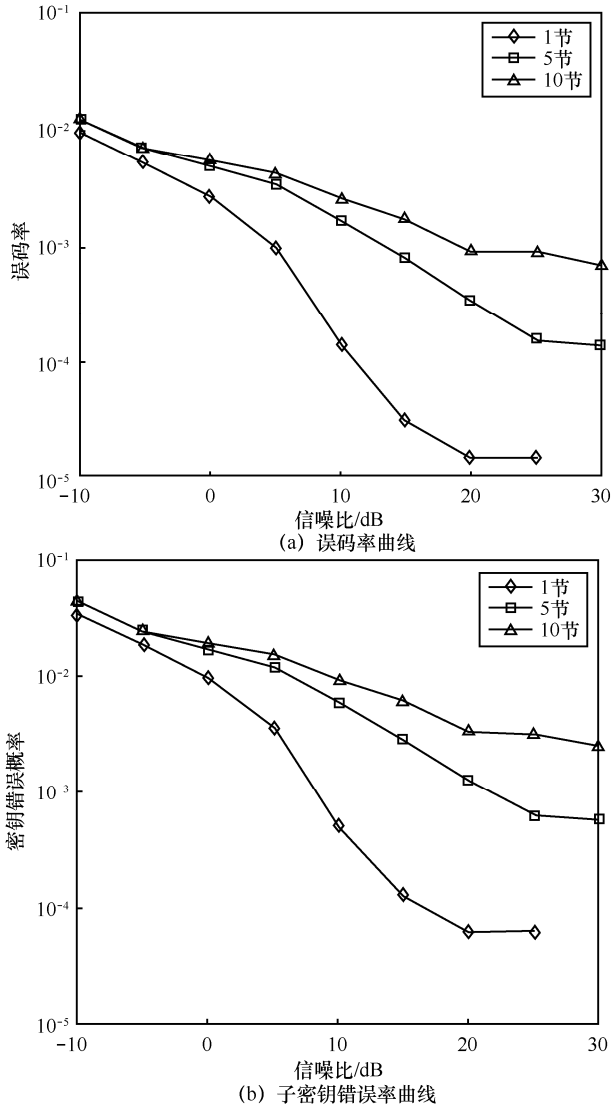


图 4　不同移动速度下的密钥一致性曲线

观察图 5 可得出以下结论。1)对比移动速度为 5 节时采用不同量化方法的 KGR 可知，采用 DLCC_AGI 量化的方案 KGR 远高于采用保护间隔量化的方案，尤其是在低信噪比情况下。这是因为低信噪比情况下，自适应得到的保护间隔将会很大，导致大量的有效测量值被丢弃，而 DLCC_AGI 量化方法经过双层补偿聚合后再生成的保护间隔仅丢弃少量错误测量值。仿真结果验证了 DLCC_AGI 量化在 KGR 方面的优越性。2) 比较不同移速下的密钥生成速率可知,移速较慢情况下的 KGR 略高于移速较快时的，但没有明显差距。

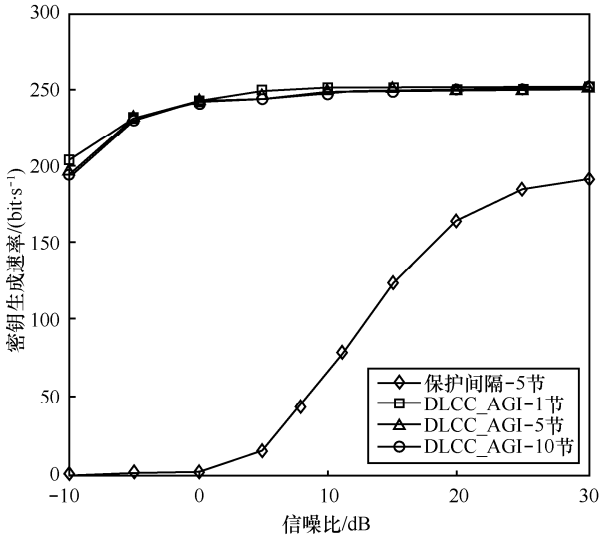


图 5　不同方案的密钥生成速率曲线

4.3　密钥随机性

本小节通过美国国家标准与技术研究所(NIST, National Institute of Standards and Technology)随机性测验中的 10 项测试（其余几项对序列长度要求过高，在物理层密钥生成技术的研究中往往忽略），说明本方案生成的密钥的随机性。取密钥长度为 256 bit，依据蒙特卡洛思想重复 1 000 次测试，得到表 3 测试结果。由表 3 可知生成的密钥以大概率通过 10 项测试中的 7 项，以 50%的概率通过其中一项，以小概率通过剩余 2 项，随机性较好，且因为在信道探测环节中加入了本地随机数，所以可以保证即使在低速移动的情况下依旧能够保持相对稳定的密钥熵水平，而不会随着移动速度的降低而变差。

5　结束语

本文主要研究了物理层密钥生成技术在时分双工水声通信中的应用。首先，针对水声信道与电

表 3　　**NIST 测试**

项目	频数	块内频数	游程	块内游程	傅里叶变换	近似熵	累加和		序列	
1 节	0.985	0.892	0.986	0.989	0.388	0.958	0.987	0.986	0.254	0.570
5 节	0.986	0.894	0.988	0.987	0.350	0.959	0.987	0.990	0.228	0.515
10 节	0.985	0.882	0.992	0.987	0.381	0.964	0.985	0.986	0.282	0.543

磁波信道的区别，通过提出的本地导频辅助信道探测协议解决了水声通信中由于测量值互易性受损引起的问题。其次，本文提出了 DLCC_AGI 量化方法代替传统的保护间隔量化，提高了生成密钥的 KAR 与 KGR。最后，通过仿真与分析证明了本方案生成的密钥在 KAR、KGR 以及随机性三方面都达到了较高的水准，即提供了一种可行的水声物理层密钥生成方案。然而，本文方案的 KAR 虽然已经优于已有的水声密钥方案，但是相较于陆上密钥生成方案仍有一定差距。因此，下一步的研究将考虑从信息调和的角度进一步优化密钥一致性。

参考文献：

[1] LIU C Y, HONG Y W P, LIN P H, et al. Jamming-resistant frequency hopping system with secret key generation from channel observations [C]//2016 IEEE Information Theory Workshop. 2016: 46-50.

[2] ZHOU H, HUIE L M, LAI L F. Secret key generation in the two-way relay channel with active attackers[J]. IEEE Transactions on Information Forensics and Security, 2014, 9(3): 476-488.

[3] XIAO S F, GUO Y F, HUANG K Z, et al. High-rate secret key generation aided by multiple relays for Internet of things[J]. Electronics Letters, 2017, 53(17): 1198-1200.

[4] XU P, CUMANAN K, DING Z G, et al. Group secret key generation in wireless networks: algorithms and rate optimization[J]. IEEE Transactions on Information Forensics & Security, 2016, 11(8): 1831-1846.

[5] THAI C D T, LEE J, QUEK T Q S. Secret group key generation in physical layer for mesh topology[C]// IEEE Global Communications Conference. 2015:1-6.

[6] WU X H, PENG Y X, HU C J, et al. A secret key generation method based on CSI in OFDM-FDD system[C]//2013 IEEE Globecom Workshops (GC WKSHPS). 2013: 1297-1302.

[7] QIN D R, DING Z. Exploiting multi-antenna non-reciprocal channels for shared secret key generation[J]. IEEE Transactions on Information Forensics and Security，2016，11(12): 2693-2705.

[8] LIU Y C, JING J W, YANG J. Secure underwater acoustic communication based on a robust key generation scheme[C]// 2008 9th International Conference on Signal Processing. 2008: 1838-1841.

[9] LUO Y, PU L N, PENG Z, et al. RSS-based secret key generation in underwater acoustic networks: advantages, challenges, and performance improvements[J]. IEEE Communications Magazine, 2016, 54(2): 32-38.

[10] HUANG Y, ZHOU S L, SHI Z J, et al. Channel frequency response-based secret key generation in underwater acoustic systems[J]. IEEE Transactions on Wireless Communications, 2016, 15(9): 5875-5888.

[11] KITAURA A, SASAOKA H. A scheme of private key agreement based on the channel characteristics in OFDM land mobile radio[J]. Electronics & Communications in Japan, 2005, 88(9):1-10.

[12] LI G Y, HU A Q, PENG L N, et al. The optimal preprocessing approach for secret key generation from OFDM channel measurements[C]//2016 IEEE Globecom Workshops. 2016: 1-6.

[13] ZHANG J Q, MARSHALL A, WOODS R, et al. Secure key generation from OFDM subcarriers' channel responses[C]//2014 IEEE Globecom Workshops. 2014: 1302-1307.

[14] PENG Y X, WANG P, XIANG W, et al. Secret key generation based on estimated channel state information for TDD-OFDM systems over fading channels[J]. IEEE Transactions on Wireless Communications, 2017, 16(8): 5176-5186.

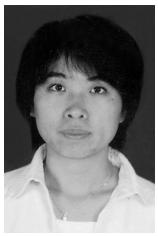
[15] QIAO G, BABAR Z, MA L, et al. MIMO-OFDM underwater acoustic communication systems—A review[J]. Physical Communication, 2017, 23:56-64.

[16] 沈志威, 刘景美, 韩庆庆. 一种高度自适应的物理层密钥生成方案[J]. 西安电子科技大学学报, 2018(1): 1-7.
SHEN Z W, LIU J M, HAN Q Q. Scheme for generation of a highly adaptive physical layer secret key[J]. Journal of Xidian University, 2018(1): 1-7.

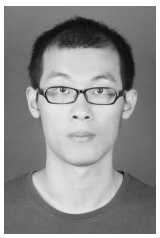
[17] SHEHADEH Y E H, ALFANDI O, TOUT K, et al. Intelligent mechanisms for key generation from multipath wireless channels[C]// 2011 Wireless Telecommunications Symposium. 2011:1-6.

[18] YONG S C, KIM J, YANG W Y, et al. MIMO-OFDM wireless communications with Matlab[M]. Singapore: Wiley Publishing, 2010: 190-195.

[作者简介]



刘景美（1979− ），女，山东烟台人，博士，西安电子科技大学副教授，主要研究方向为密码分析。



沈志威（1993− ），男，浙江湖州人，西安电子科技大学硕士生，主要研究方向为物理层密钥生成技术。

韩庆庆（1994− ），男，陕西延安人，西安电子科技大学硕士生，主要研究方向为物理层密钥生成技术。

刘景伟（1978− ），男，山东滨州人，博士，西安电子科技大学副教授，主要研究方向为网络安全。