单载波频域均衡系统中基于信道频域响应的密钥生成机制研究

孔媛媛　杨 震*　吕 斌　田 峰
(南京邮电大学宽带无线通信与传感网技术教育部重点实验室 南京 210003)

摘　要：单载波频域均衡(SC-FDE)系统中，信道的频域响应可以作为随机源来生成密钥。为了提高密钥容量，该文提出一种利用多径瑞利信道的频域响应来生成密钥的机制(CFR-Key)。首先研究了 CFR-Key 机制的原理和密钥生成速率，通过互信息理论推导出了 CFR-Key 的密钥容量；进而研究了 CFR-Key 机制中算法的量化等级的影响因素，推导验证了量化等级的选择只与信噪比有关，当信噪比确定的情况下通过选择最优的量化等级可以得到最大的密钥生成速率；与基于信道冲激响应生成密钥机制(CIR-Key)对比，证实了 CFR-Key 机制可大幅提高密钥容量。

关键词：密钥生成；信道频域响应；单载波频域均衡系统
中图分类号：TN92　　**文献标识码**：A　　**文章编号**：1009-5896(2018)05-1017-07
DOI: 10.11999/JEIT170772

Study on Secret Key Generation Based on Frequency Domain Response of Channel in Single Carrier Frequency Domain Equalization Systems

KONG Yuanyuan　YANG Zhen　LÜ Bin　TIAN Feng
(*Key Laboratory of Broadband Wireless Communication and Sensor Network Technology*, *Ministry of Education*, *Nanjing University of Posts and Telecommunications*, *Nanjing* 210003, *China*)

Abstract: A secret key generation scheme is proposed in a Single Carrier Frequency Domain Equalization system (SC-FDE). The scheme uses the Channel Frequency Response (CFR) to generate the secret keys, which is termed as CFR-Key. The principle of the CFR-Key scheme is introduced and formulate the secret key capacity is derived based on mutual information theory. The Signal-Noise Ratio (SNR) is proved that is the unique factor and affects the quantization levels. The optimum quantization levels is designed to achieve the best key generation rate when SNR is given. Simulation results show that comparing with the secret key generation scheme based on the Channel Impulse Response (CIR-Key), the proposed scheme can significantly improve the secret key capacity.

Key words: Secret key generation; Frequency domain response of channel; Single Carrier Frequency Domain Equalization system (SC-FDE)

1　引言

在安全通信技术中，密钥是提供通信安全保护的有效手段。在无线通信环境下，利用密钥机制提供机密性、完整性和认证性等服务面临着与有线网络不同的难题。近年来，基于无线信道特性的物理层安全通信技术受到了广泛关注，无线通信中的合法通信双方可以利用无线信道的特性寻求实现安全通信的方案[1]。无线信道通常具有互易性、时变性和空变性的特性[2]。因为信道的互易性和时变性的特点，合法通信双方在时分复用的通信模式下，在信道的相干时间 Δt 内完成一次相互通信，双向信道特征是基本一样的。基于信道的空变性的特点，在多径丰富的无线环境中，距离合法双方半个波长之外的窃听方的信道观察和合法双方的信道观察是统计独立的。因此信道特征可以作为一个公共随机源，并且这个公共随机源对窃听方来说是保密的，称之为信道生成密钥[3]。基于信道的密钥生成与提取方法是一种研究无线物理层固有特性的信息论安全方案，是一种物理层安全技术，与传统的密钥生成有根本的区别，引发了人们极大的兴趣和研究热情。

信道生成密钥的密钥提取技术可以分为基于接收信号特征和基于信道特征两类。基于接收信号特征是将接收信号特征作为随机源来生成密钥，比如

收稿日期：2017-08-02；改回日期：2018-01-22；网络出版：2018-03-14
*通信作者：杨震　yangz@njupt.edu.cn
基金项目：国家自然科学基金(61671252, 61772287)，江苏省高校自然科学研究重大项目(14KJA510003)，江苏省研究生科研与实践创新计划(CXZZ11_0394)
Foundation Items: The National Natural Science Foundation of China (61671252, 61772287), The Key University Science Research Project of Jiangsu Province (14KJA510003), The Postgraduate Research & Practice Innovation Program of Jiangsu Province (CXZZ11_0394)

基于接收信号强度[4]、包络[5]、相位[6]、接收信号和发送信号的频谱差[7]等。基于信道特征是在信道估计的基础上将信道特征作为随机源来生成密钥，比如采用基于信道的冲激响应(Channel Impulse Response, CIR)的相位来生成密钥[8]，利用 CIR 的实部和虚部来生成密钥[9,10]等。目前，基于信道特征生成密钥的研究主要关注信道的时域特征。为表述方便，这里将基于 CIR 的密钥生成方案统称为 CIR-Key。对于多径瑞利衰落的信道，信道的频域具有频率选择性，其频域值分布更分散，与时域冲激响应相比，可以带来更多的信息量。因此，基于信道频域特征提取密钥的相关研究也受到关注。文献 [11] 研究了在正交频分复用 (Orthogonal Frequency Division Multiplexing, OFDM)系统中利用信道频域响应的幅值来生成密钥的方案。但由于 OFDM 系统对相位噪声和频偏较为敏感，且只利用了信道频域幅度来生成密钥，忽略了信道的相位特性。为了构建能同时利用信道频域的幅度特性和相位特性生成密钥的机制，本文着重研究单载波频域均衡 (Single Carrier Frequency Domain Equalization, SC-FDE)系统。SC-FDE 系统在接收端采用频域均衡技术，与 OFDM 系统相比，SC-FDE 系统具有相位噪声和频偏的敏感性低的优点[12−14]。因此，本文提出一种在 SC-FDE 系统中的基于信道频域响应的密钥生成机制，并称这种机制为信道频率响应密钥 CFR-Key。与 CIR-Key 相比，CFR-Key 密钥生成机制可以数倍地提高密钥容量，进而大幅提高密钥生成速率。另外 CFR-Key 生成密钥的量化等级选择只与信噪比有关，在信噪比确定的情况下，可以通过选择最优的量化等级最大化密钥生成速率。这使得 CFR-Key 密钥生成机制在频率选择性衰落信道环境下、在采用频域均衡的系统中有着广泛的应用价值。

本文的内容安排如下：第 1 节为引言；第 2 节给出了 CFR-Key 应用于 SC-FDE 系统的模型；第 3 节阐述了 CFR-Key 的原理；第 4 节根据互信息分析推导出了 CFR-Key 的密钥容量；第 5 节将 CFR-Key 的密钥容量与 CIR-Key 的密钥容量进行对比，证明了 CFR-Key 生成机制的优越性；第 6 节研究了量化等级的选择，给出了在实际应用中不同信噪比下最优量化等级的选择方法，分析其对密钥生成速率的影响；第 7 节为结束语。

2 系统模型

SC-FDE 系统是在接收端采用频域均衡技术的系统，与 OFDM 系统相比，SC-FDE 具有相位噪声和频偏的敏感性低的优点[12−14]。在 SC-FDE 系统中，信道频域响应的幅值和相位信息都可以作为随机源来生成密钥，因此本文研究了在 SC-FDE 系统中基于信道频域响应的密钥生成机制(CFR-Key)，首先给出 CFR-Key 加密 SC-FDE 系统模型，如图 1 所示。

Alice 和 Bob 为双向通信的双方，以 Alice 发 Bob 收为例，在发送端 Alice 将数据经过 Key_A 加密的信号加循环前缀后发送到信道；在接收端 Bob 首先去循环前缀，然后经过 FFT 进行信道频域均衡，利用 Key_B 对 IFFT 后的数据解密得到接收信号，其中 Key_A , Key_B 分别为 Alice 和 Bob 利用 CFR-Key 机制生成的密钥。

$\boldsymbol{x}=[x_0,x_1,\cdots,x_{N-1}]^{\mathrm{T}}$ 为发送信号 s 经过加密后的发送数据(研究加密算法的文献很多，本文不做详细探讨)，发送的数据符号相互独立且具有相同的能量 E_S，即满足 $E\left[\boldsymbol{X}\boldsymbol{X}^{\mathrm{H}}\right]=E_S\boldsymbol{I}_N$。不失一般性，本文令 $E_S=1$。$\boldsymbol{h}=[h_0,h_1,\cdots,h_{L-1}]^{\mathrm{T}}$，$\boldsymbol{h}$ 为多径瑞利信道的冲激响应，L 为路径数。$\boldsymbol{n}=[n_0,n_1,\cdots,n_{N-1}]^{\mathrm{T}}$ 为加性高斯白噪声，其元素为独立同分布，零均值，方差为 σ^2 的复高斯随机过程，系统的信噪比 SNR

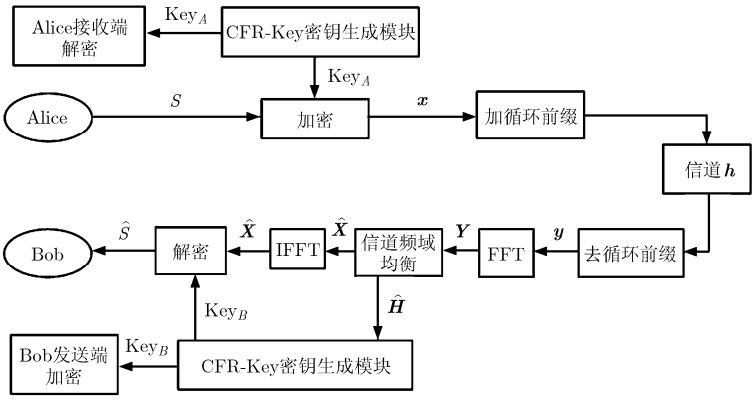

图 1 CFR-Key 加密 SC-FDE 系统模型

$=1/\sigma^2$。

$\boldsymbol{x}$，$\boldsymbol{n}$ 和 $\boldsymbol{y}$ 对应的 N 点离散傅里叶变换(Discrete Fourier Transform, DFT)分别为 $\boldsymbol{X}=[X_0,X_1,\cdots,X_{N-1}]^{\mathrm{T}}$，$\boldsymbol{N}=[N_0,N_1,\cdots,N_{N-1}]^{\mathrm{T}}$ 和 $\boldsymbol{Y}=[Y_0,Y_1,\cdots,Y_{N-1}]^{\mathrm{T}}$。输入信号 $\boldsymbol{x}$ 增加循环前缀后，N 点 DFT 可以使用 N 点 FFT 快速实现。虽然噪声 $\boldsymbol{n}$ 没有增加循环前缀，根据噪声自身的随机性，其 DFT 可以用快速傅里叶变换(Fast Fourier Transform, FFT)近似。$\boldsymbol{h}_{N\times N}$ 为 $N\times N$ 的循环矩阵，其第 1 列为 L 位的信道冲激响应 $\boldsymbol{h}$ 后补充上 $N-L$ 个 0，后面的列为第 1 列的移位，$\boldsymbol{h}_{N\times N}\boldsymbol{x}$ 即为 $\boldsymbol{h}\otimes\boldsymbol{x}$ 的矩阵表示。

接收信号 $\boldsymbol{y}=[y_0,y_1,\cdots,y_{N-1}]^{\mathrm{T}}$，可表示为

$$\boldsymbol{y}=\boldsymbol{h}_{N\times N}\boldsymbol{x}+\boldsymbol{n} \tag{1}$$

将接收信号 $\boldsymbol{y}$ 变换到频域 $\boldsymbol{Y}$：

$$\boldsymbol{Y}=\boldsymbol{F}\boldsymbol{H}_{N\times N}\boldsymbol{x}+\boldsymbol{F}\boldsymbol{n} \tag{2}$$

其中，$\boldsymbol{F}$ 为 $N\times N$ 的 DFT 矩阵，$[\boldsymbol{F}]_{nm}=\frac{1}{\sqrt{N}}\mathrm{e}^{-\frac{\mathrm{j}2\pi(n-1)(m-1)}{N}}$。由于 $\boldsymbol{H}_{N\times N}$ 是一个循环矩阵，其特征值分解可以表示为 $\boldsymbol{H}_{N\times N}=\boldsymbol{F}^{\mathrm{H}}\boldsymbol{\Lambda}\boldsymbol{F}$，其中 $\boldsymbol{\Lambda}$ 是 $N\times N$ 的对角矩阵，$\boldsymbol{\Lambda}=\mathrm{diag}[H_0,H_1,\cdots,H_{N-1}]$，$H_n=\sum_{l=0}^{L-1}h_l\mathrm{e}^{-\frac{\mathrm{j}2\pi nl}{N}}$。也就是说 $\boldsymbol{H}=[H_0,H_1,\cdots,H_{N-1}]^{\mathrm{T}}$ 是 $\boldsymbol{h}$ 补 0 至后 N 长后的 N 点 DFT 变换，$\boldsymbol{H}=\boldsymbol{F}\left[\boldsymbol{h}^{\mathrm{T}},\boldsymbol{0},\cdots,\boldsymbol{0}\right]^{\mathrm{T}}$，则有

$$\boldsymbol{Y}=[Y_0,Y_1,\cdots,Y_{N-1}]^{\mathrm{T}}=\boldsymbol{\Lambda}\boldsymbol{X}+\boldsymbol{F}\boldsymbol{n}=\boldsymbol{H}\times\boldsymbol{X}+\boldsymbol{N} \tag{3}$$

$$Y_n=H_nX_n+N_n \tag{4}$$

使用频域信道估计算法，可以估计出信道参数 $\boldsymbol{\Lambda}^{-1}$，从而求出发送信息的频域 $\widehat{\boldsymbol{X}}=\boldsymbol{\Lambda}^{-1}\boldsymbol{Y}$，再通过离散傅里叶逆变换(Inverse FFT, IFFT)得到发送信号的时域 $\widehat{\boldsymbol{X}}$，经过解密得到 $\widehat{S}$。

CFR-Key 密钥生成模块是 CFR-Key 密钥生成模块使用接收端频域信道 H_n 的估计 $\widehat{H}_n$ 来产生密钥，首先将 $\widehat{H}_n$ 的实部和虚部的数值分别进行量化，再进行二进制转化，最后通过级联生成二进制密钥。以 Alice 端为例，Alice 在接收信号时估计出信道的频域特性 $\widehat{H}_n$，Alice 端的“CFR-Key 密钥生成模块”通过量化 $\widehat{H}_n$ 的实部和虚部产生密钥 Key_A，Alice 在发送信号时使用 Key_A 进行加密，在接收信号时使用 Key_A 解密。Bob 端同样如此。由于无线信道的互易性，在假设信道被精确估计和不考虑计算误差的情况下，密钥的一致性可以满足，即有 $\mathrm{Key}_A=\mathrm{Key}_B$。此时，Alice 和 Bob 不需要密钥交换，即可各自生成相同的密钥，具体原理将在下一节介绍。

3　基于信道频域响应的密钥生成机制 CFR-Key 原理

无线通信环境信道通常是瑞利衰落信道，其包络的 1 维分布服从瑞利分布，信道时域冲激响应的实部和虚部服从于零均值的独立同分布高斯过程。对于多径瑞利信道，L 径瑞利信道的时域冲激响应 $\boldsymbol{h}=[h_0,h_1,\cdots,h_{L-1}]^{\mathrm{T}}$，$h_l=h_{Il}+jh_{Ql}$，则有 h_{Il} 和 h_{Ql} 独立且均服从高斯分布 $\mathcal{N}(0,p_l)$，即 h_l 服从复高斯分布 $\mathcal{CN}(0,p_l)$，p_l 为第 l 径信道的功率。

瑞利信道的信道时域冲激响应的实部和虚部均为高斯随机过程，文献[9]将其作为随机源生成信道密钥，多径瑞利信道的每一径都可以作为一个随机源来生成信道密钥，文献[10]研究了多径信道作为随机源生成信道密钥的密钥容量。瑞利信道的时域冲激响应具有高斯分布的特性，瑞利信道的频域响应是否具有类似特性，是否也可以用来作为随机源生成信道密钥呢？

根据高斯分布的基本性质，高斯信号经过任意线性变换(或线性系统处理)后仍是高斯信号[15]。傅里叶变换和 DFT 均为线性变换，因此高斯信号的 DFT 仍然服从高斯分布。基于此性质可以证明出引理 1 和引理 2，证明过程略。

引理 1　服从复高斯分布 $\mathcal{CN}\left(0,\sigma^2\right)$ 的随机信号在 DFT 后得到的频域信号，其实部和虚部分别服从高斯分布 $\mathcal{N}\left(0,N\sigma^2/2\right)$，但实部和虚部不相互独立。

引理 2　L 径瑞利信道 $\boldsymbol{h}=[h_0,h_1,\cdots,h_{L-1}]^{\mathrm{T}}$，在 DFT 后得到的频域响应 $\boldsymbol{H}=[H_0,H_1,\cdots,H_{N-1}]^{\mathrm{T}}$，$H_n=H_{In}+H_{Qn}=\sum_{l=0}^{L-1}h_l\mathrm{e}^{-\frac{\mathrm{j}2\pi nl}{N}}$，$H_{In}$ 和 H_{Qn} 均服从高斯分布 $\mathcal{N}(0,P/2)$，$P=\sum_{l=0}^{L-1}p_l$，P 为瑞利信道的总功率。

引理 1 和引理 2 表明，多径瑞利信道的频域响应的实部和虚部都是服从高斯分布 $\mathcal{N}(0,P/2)$ 的随机变量，这充分说明利用信道的频域响应的实部和虚部来进行密钥生成是可行的，值得特别注意的是，其实部和虚部不相互独立的，因此多径瑞利信道的频域响应不服从复高斯分布，这将是下一节推导 CFR-Key 密钥容量的依据。

假设发送 $\boldsymbol{x}$ 为双方均已知的训练序列，接收端先估计出信道的频域响应 $\widehat{\boldsymbol{H}}$，$\widehat{\boldsymbol{H}}=\left[\widehat{H}_0,\widehat{H}_1,\cdots,\widehat{H}_{N-1}\right]^{\mathrm{T}}$，假设使用迫零(Zero Forcing, ZF)估计，式(4)两侧分别乘以 $X_n^*/\|X_n\|^2$ 得到信道的频域响应的估计 $\widehat{H}_n$：

$$\widehat{H}_n = \frac{Y_n X_n^*}{\| X_n \|^2} = \frac{H_n X_n X_n^*}{\| X_n \|^2} + \frac{N_n X_n^*}{\| X_n \|^2} = H_n + \frac{N_n X_n^*}{\| X_n \|^2} \tag{5}$$

根据引理 2, H_n 的实部和虚部分布服从高斯分布，同时根据引理 1，高斯噪声 DFT 后 N_n 的实部和虚部也服从高斯分布。信道频域响应的估计 $\widehat{H}_n$ 为复数 $\widehat{H}_n = \widehat{H}_{na} + j\widehat{H}_{nb}$，实部 $\widehat{H}_{na}$ 和虚部 $\widehat{H}_{nb}$ 分别为两个不同分布的高斯随机变量之和，具有一定的随机性，可以用作随机源来生成密钥。由此，本文提出了 CFR-Key 密钥生成机制，即对信道频域估计的实部 $\widehat{H}_{na}$ 和虚部 $\widehat{H}_{nb}$ 分别进行量化来生成密钥，该密钥既包含了信道频域响应的幅度信息也包含了其相位信息。如果使用均匀量化，令量化等级为 Q，量化比特数 $q = \log_2 Q$，则每次信道估计后可以得到的密钥长度，也就是密钥生成速率为 $R_{\text{key}} = 2Nq = 2N\log_2 Q$，单位是每进行一次信道观察所得到的密钥比特数(bit/信道观察)。

基于 CFR-Key 的密钥生成速率与 FFT 长度 N 和量化等级 Q 有关，N 和 Q 越大，密钥生成速率越大，但 N 和 Q 的取值也有一定的约束。其中，N 的取值需满足 $NT_S < \Delta t/2$，T_S 为传码率，Δt 为信道的相干时间，这是为了保证双方的信道估计过程要在 Δt 内完成，即保证信道观察期间信道特性不变。虽然信道特性在 Δt 内保持不变，但由于信道噪声和信道估计算法的影响，Alice 和 Bob 双方得到的信道估计也不会完全一致，这就决定了量化等级 Q 的取值不能无限大。C_{key} 影响双方密钥生成的一致性，即 C_{key} 越大，双方密钥生成的一致性越差；$R_A = S + Z_A$ 越小，双方密钥生成的一致性越好。本文第 6 节将重点研究如何选择最优的 $R_B = S + Z_B$ 值，在能保证密钥生成一致性的前提下，达到最高的密钥生成速率。

4 密钥容量分析

系统的密钥容量 C_{key} 是指系统能够达到的最大密钥生成速率，是密钥生成速率的上界，是衡量密钥生成机制好坏的重要指标。根据互信息理论，密钥生成速率与合法通信双方所观察到的相关随机源的互信息有关，由于收发双方公共通信能力的限制，最大密钥生成速率不能超过互信息，密钥容量就是观察随机源的互信息。

文献[9]推导并证明了复高斯分布随机变量的互信息计算公式。假设 $R_A = S + Z_A$ 和 $R_B = S + Z_B$，$S \sim \mathcal{CN}(0, N_S)$，$Z_A \sim \mathcal{CN}(0, N_A)$，$Z_B \sim \mathcal{CN}(0, N_B)$，3 个随机过程是复高斯分布且互相独立，则 R_A 和 R_B 的互信息为

$$I(R_A; R_B) = \log_2\left(1 + \frac{N_S}{N_A + N_B + \dfrac{N_A N_B}{N_S}}\right) \tag{6}$$

根据式(6)，文献[10]得到 L 径信道利用 CIR-Key 机制的密钥容量，其表达式如式(7)所示。

$$\text{Ch}_{\text{key}} = I_h = \sum_{l=0}^{L-1} \log_2\left(1 + \frac{p_l}{\dfrac{2\sigma^2}{\|x\|^2} + \dfrac{\sigma^4}{\|x\|^4\, p_l}}\right) \tag{7}$$

式(6)是复数表示的复高斯分布随机变量的互信息计算公式。第 3 节已经证明了多径瑞利信道频域响应不服从复高斯分布，但多径瑞利信道频域响应的实部和虚部分别服从高斯分布，式(6)无法直接使用，可以将式(6)复随机变量的互信息计算推广到实数的随机变量。由于复高斯分布随机变量的实部和虚部相互独立，且均服从高斯分布，实部的互信息是复数的互信息的一半，因此可以得到引理 3。

引理 3 高斯分布随机变量的互信息计算公式。假设 $R_{AI} = S_I + Z_{AI}$ 和 $R_{BI} = S_I + Z_{BI}$，$S_I \sim \mathcal{N}(0, N_S)$，$Z_{AI} \sim \mathcal{N}(0, N_A)$，$Z_{BI} \sim \mathcal{N}(0, N_B)$，3 个随机过程是高斯分布且互相独立，则 R_{AI} 和 R_{BI} 的互信息为

$$I(R_{AI}; R_{BI}) = \frac{1}{2}\log_2\left(1 + \frac{N_S}{N_A + N_B + \dfrac{N_A N_B}{N_S}}\right) \tag{8}$$

基于信息论中的互信息分析来推导出 CFR-Key 的密钥容量。假设 Alice 得到的信道频域响应为

$$\begin{aligned} H_{An} &= H_n + \frac{N_n X_n^*}{\|X_n\|^2} = H_n + Z_{An} \\ &= (H_{In} + Z_{AIn}) + j(H_{Qn} + Z_{AQn}) \end{aligned} \tag{9}$$

Bob 得到的信道频域响应为

$$\begin{aligned} H_{Bn} &= H_n + \frac{N_n X_n^*}{\|X_n\|^2} = H_n + Z_{Bn} \\ &= (H_{In} + Z_{BIn}) + j(H_{Qn} + Z_{BQn}) \end{aligned} \tag{10}$$

求解 CFR-Key 密钥生成的容量也就是求解信道频域响应 H_{An} 和 H_{Bn} 的互信息。首先分别计算信道频域响应的实部和虚部互信息，然后二者求和后得到总互信息。

根据引理 1，假设服从 $\mathcal{CN}(0, \sigma^2)$ 的复高斯噪声对应的频域表达为 N_n，N_n 的实部和虚部都服从 $\mathcal{N}(0, N\sigma^2/2)$。式(9)中得到信道估计噪声的频域为 $Z_{An} = Z_{AIn} + jZ_{AQn} = N_n X_n^* / \|X_n\|^2$，可以得出 Alice

接收到的噪声频域特性的实部的分布特性为 $Z_{AIn}\sim\boldsymbol{\mathcal{N}}(0,N_A)$，其中 $N_A=N\sigma^2/2\|X_n\|^2$。同样得到 Bob 接收到的噪声频域特性的实部的分布特性为 $Z_{BIn}\sim\boldsymbol{\mathcal{N}}(0,N_B)$，其中 $N_B=N\sigma^2/2\|X_n\|^2$。另外，根据引理 2 得到信道频域响应的实部为 $H_{In}\sim\boldsymbol{\mathcal{N}}(0,N_S)$，其中 $N_S=P/2$。

根据引理 3 求出实部的互信息：

$$I_{In}=I(H_{AIn};H_{BIn})=\frac{1}{2}\log_2\left(1+\frac{P}{\dfrac{2N\sigma^2}{\|X_n\|^2}+\dfrac{N^2\sigma^4}{P\|X_n\|^4}}\right)\tag{11}$$

同样可以求得虚部的互信息，即 $I_{Qn}=I_{In}$。因此，总互信息为 $I_n=2I_{In}$。

由于信道频域响应 $\boldsymbol{H}$ 有 N 个变量，CFR-Key 机制的密钥容量为

$$\begin{aligned}\mathrm{CH}_{\mathrm{key}}&=I_H=\sum_{n=1}^{N}I_n\\&=N\log_2\left(1+\frac{P}{\dfrac{2N\sigma^2}{\|X_n\|^2}+\dfrac{N^2\sigma^4}{P\|X_n\|^4}}\right)\end{aligned}\tag{12}$$

从式(12)可以看出，CFR-Key 的密钥容量与信道总功率、FFT 长度、发送信号功率和信道噪声功率等因素有关，与信道的多径数量和各径的功率分布无关。从式(7)可以看出 CIR-Key 的密钥容量与信道各径功率、信道的多径数、发送信号功率、信道噪声功率等因素有关。在第 5 节，将对 CFR-Key 和 CIR-Key 的密钥容量进行比较和分析。

5　CFR-Key 和 CIR-Key 密钥容量比较

本文研究在多径瑞利信道下 SC-FDE 系统的密钥容量。噪声为加性高斯白噪声，L 径瑞利信道的时域冲激响应为 $\boldsymbol{h}=[h_0,h_1,\cdots,h_{L-1}]^{\mathrm{T}}$，$h_l=h_{Il}+jh_{Ql}$，$h_l$ 服从复高斯分布 $\boldsymbol{\mathcal{CN}}(0,p_l)$，$p_l$ 为第 l 径信道的功率。假设信道的总功率 $P=1$，$L=4$，比较 CFR-Key 和 CIR-Key 在以下 3 种场景下的密钥容量。由于 CFR-Key 密钥容量与信道多径数和各径功率分配无关，因此这 3 种场景下 CFR-Key 密钥容量相同，但 CIR-Key 密钥容量互相不同。

信道 A：各径等功率信道 $p_0=p_1=p_2=p_3=1/4$；

信道 B：各径非等功率信道 $p_0=0.5$, $p_1=0.2$, $p_2=0.2$, $p_3=0.1$；

信道 C：单径信道 $p_0=1$, $p_1=p_2=p_3=0$。

使用训练序列进行信道估计时，加密模块使用恒 1 序列作为密钥，即不加密，待信道估计生成信道密钥后，发送数据利用生成的密钥进行加密。本文采用的训练序列为恒定幅度零周期自相关序列(CAZAC 序列)，其具有时域恒模和频域恒模的性质。时域和频域均恒模使其抗噪声能力强，自相关特性好使其具有良好的相位特性，因此 CAZAC 序列常被用作训练序列估计信道[16]。假设 CAZAC 序列长度为 N，时域恒模 $\|x_m\|^2=1$, $\|x\|^2=1$，频域恒模 $\|X_n\|^2=N$，系统的信噪比 $\mathrm{SNR}=1/\sigma^2$。根据式(12)，该系统中 CFR-Key 的密钥容量为

$$\begin{aligned}\mathrm{CH}_{\mathrm{key}}&=N\log_2\left(1+\frac{P}{2\sigma^2+\dfrac{\sigma^4}{P}}\right)\\&=N\log_2\left(1+\frac{\mathrm{SNR}}{2+\dfrac{1}{\mathrm{SNR}}}\right)\end{aligned}\tag{13}$$

根据式(7)，该系统中 CIR-Key 的密钥容量为

$$\begin{aligned}\mathrm{Ch}_{\mathrm{key}}&=\sum_{l=0}^{L-1}\log_2\left(1+\frac{p_l}{\dfrac{2\sigma^2}{\|x\|^2}+\dfrac{\sigma^4}{\|x\|^4\,p_l}}\right)\\&=\sum_{l=0}^{L-1}\log_2\left(1+\frac{p_l\mathrm{SNR}}{2+\dfrac{1}{p_l\mathrm{SNR}}}\right)\end{aligned}\tag{14}$$

对于不同的多径信道长度 L 和 FFT 长度 N, CFR-Key 和 CIR-Key 的密钥容量如图 2 所示。对于 CIR-Key 机制，各径的功率分配影响其密钥容量。当各径功率相同时，密钥容量最大。各径功率之间差距越大，容量越小。当多径信道退化到单径信道(单径信道可以看做是各径功率差距最大的多径信道)时，容量最小。对于 CFR-Key 机制，L 一定时，N 越大密钥容量越大。CFR-Key 的密钥容量与信道各径的功率分配无关，只与多径信道的总功率有关。当 $N=L$ 时，CFR-Key 和各径等功率信道 CIR-Key 的容量相同(图 2 中 $N=L=4$ 时 CFR-Key 容量和 CIR-Key 容量两条线重合)。密钥容量比较时，对于 $L=4$ 的多径瑞利信道，本文采用的 FFT 长度 N 为 4 和 16。但在实际 SC-FDE 系统中，为了抵消数据块之间的影响，N 的取值应该远远大于 L。由此可知，CFR-Key 的密钥容量将远远超过 CIR-Key 的密钥容量。

6 CFR-Key 机制中算法的量化等级选择

从图 2 可以看出一个有趣的现象，当 SNR 的值较大时，密钥容量的曲线呈现出线性的特性。因此可以考虑用线性函数来逼近 CFR-Key 的密钥容量，下面给出证明过程。

根据式(13)，在 SNR 很大时，$\mathrm{CH}_{\mathrm{key}} \approx N\log_2\left(1+\dfrac{\mathrm{SNR}}{2}\right) \approx N\log_2\left(\dfrac{\mathrm{SNR}}{2}\right)$。令 $\widetilde{\mathrm{CH}}_{\mathrm{key}} = N\log_2\left(\dfrac{\mathrm{SNR}}{2}\right)$，$\widetilde{\mathrm{CH}}_{\mathrm{key}}$ 为 $\mathrm{CH}_{\mathrm{key}}$ 的逼近。将 $\mathrm{SNR} = 10^{\mathrm{SNRdB}/10}$ 代入 $\widetilde{\mathrm{CH}}_{\mathrm{key}}$ 得

$$\begin{aligned}\widetilde{\mathrm{CH}}_{\mathrm{key}} &= \frac{\log_2 10}{10} N \times \mathrm{SNRdB} - N \\ &= 0.3322N \times \mathrm{SNRdB} - N \end{aligned} \tag{15}$$

从式(15)可以看出 $\widetilde{\mathrm{CH}}_{\mathrm{key}}$ 与 SNRdB 确实呈现出线性关系。图 3 给出了 $\mathrm{CH}_{\mathrm{key}}$ 和 $\widetilde{\mathrm{CH}}_{\mathrm{key}}$ 的比较，其中分别考虑了 $N=16, L=4$；$N=4, L=4$ 两种场景。由图 3 可知，当 SNRdB 较小时，两者差距较大；当 SNRdB 较大时，两者基本重合，总体趋势上 $\widetilde{\mathrm{CH}}_{\mathrm{key}} < \mathrm{CH}_{\mathrm{key}}$。密钥容量是系统能够达到的最大的密钥生成速率，实际的密钥生成速率应该小于密钥容量，因而在应用中可以使用 $\widetilde{\mathrm{CH}}_{\mathrm{key}}$ 代替 $\mathrm{CH}_{\mathrm{key}}$。

根据第 3 节的介绍，CFR-Key 的密钥生成速率为 $R_{\mathrm{key}} = Nq$，密钥生成速率需要小于密钥容量 $R_{\mathrm{key}} < \widetilde{\mathrm{CH}}_{\mathrm{key}}$，即

$$Nq < 0.3322N \times \mathrm{SNRdB} - N \tag{16}$$

根据式(16)，可以推导出满足条件的最大 q 值，由 $q = \log_2 Q$，可求得最大的量化等级 Q：

$$Q_{\max} = 2^{q_{\max}} \tag{17}$$

其中，$q_{\max} = \left\lfloor \dfrac{\widetilde{\mathrm{CH}}_{\mathrm{key}}}{N} \right\rfloor = \lfloor 0.3322 \times \mathrm{SNRdB} - 1 \rfloor$。

由此，得到一个重要结论：对于 CFR-Key 机制，量化比特数 q 和量化等级 Q 的取值与 FFT 长度 N 无关，只与信噪比有关。在实际应用中，可以根据信道的信噪比来决定最优量化等级，以达到系统的最大密钥生成速率。$L=4$ 的多径信道下以 $N=16$ 和 $N=32$ 的 SC-FDE 系统为例，图 4 给出了 $L=4$ 时量化比特数及对应的密钥生成速率与信噪比的关系曲线。如图 4 所示，随着信噪比的增加，量化比特也逐渐增加。最优量化比特数的选取，既能保证密钥生成速率最大，又保证一直小于密钥容量的线性逼近。量化比特数的选取和 N 无关，只与信噪比有关。在信噪比一定的情况下，无论 N 值多少，最优的量化比特数 q 是确定的，比如当信噪比在 13 dB 至 16 dB 时，最优 q 值为 3，最优量化等级 Q 值为 8。从图 4 还可以看出，SNRdB $\geq$ 7 dB 的情况下 $q \geq 1$，也就是说，本文提出的 CFR-Key 只能在信噪比 7 dB 以上的系统中才能使用。

7 结束语

在 SC-FDE 系统中，信道的频域响应可以作为密钥生成的随机源。本文在多径瑞利信道加高斯白噪声的 SC-FDE 系统中，首先证明了信道频域响应的实部和虚部都是服从高斯分布的随机变量，提出了基于信道频域响应的密钥生成机制 CFR-Key。然后，通过互信息理论推导出了 CFR-Key 的密钥容量，与基于信道冲击响应生成秘钥机制 CIR-Key 对比，证明了 CFR-Key 的密钥生成机制可以大幅提高密钥容量。另外，本文得到 CFR-Key 的密钥生成速率与 FFT 长度 N 和量化等级 Q 有关。在 N 一定的情况下，密钥生成速率与 Q 成正比。通过对密钥容量表达式的分析，推导出了密钥容量的线性逼近表示形式，进而得出 Q 的最优取值的数学表达式，从而得出 Q 的最优值只与 SNR 有关。上述结论对于 CFR-Key 的实际应用有着重要的指导意义。

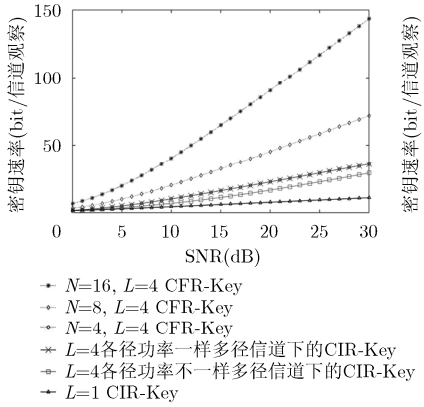

图 2 CFR-Key 和 CIR-Key 的密钥容量比较

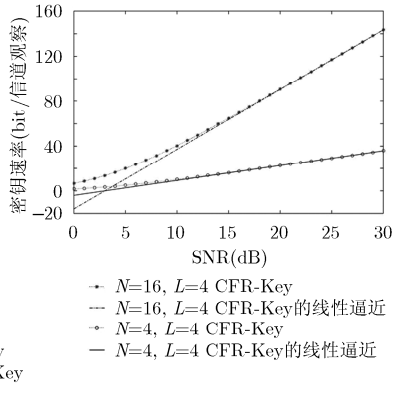

图 3 CFR-Key 密钥容量及其线性逼近

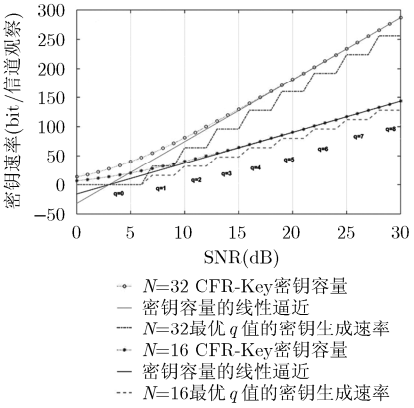

图 4 CFR-Key 的量化等级选择及其密钥速率

参 考 文 献

[1] ZHANG J, DUONG T Q, MARSHALL A, *et al*. Key generation from wireless channels: a review[J]. *IEEE Access*, 2016, 4(3): 614–626. doi: 10.1109/ACCESS.2016.2521718.

[2] MAURER U M. Secret key agreement by public discussion from common information[J]. *IEEE Transactions on Information Theory*, 1993, 39(3): 733–742. doi: 10.1109/18.256484.

[3] AHLSWEDE R and CSISEAR I. Common randomness in information theory and cryptography. I: Secret sharing[J]. *IEEE Transactions on Information Theory*, 1993, 39(4): 1121–1132. doi: 10.1109/18.243431.

[4] PREMNATH S N, JANA S, CROFT J, *et al*. Secret key extraction from wireless signal strength in real environments [J]. *IEEE Transactions on Mobile Computing*, 2013, 12(5): 917–930. doi: 10.1109/TMC.2012.63.

[5] WILSON R, TSE D, and SCHOLTZ R A. Channel identification: Secret sharing using reciprocity in ultrawideband channels[J]. *IEEE Transactions on Information Forensics and Security*, 2007, 2(3): 364–375. doi: 10.1109/TIFS.2007.902666.

[6] WANG Q, SU H, REN K, *et al*. Fast and scalable secret key generation exploiting channel phase randomness in wireless networks[C]. IEEE INFOCOM, Shanghai, China, 2011: 1422–1430. doi: 10.1109/INFCOM.2011.5934929.

[7] HAROUN M F and GULLIVER T A. Secret key generation using chaotic signals over frequency selective fading channels[J]. *IEEE Transactions on Information Forensics and Security*, 2015, 10(8): 1764–1775. doi: 10.1109/TIFS.2015.2428211.

[8] SATEED A and PERRIG A. Secure wireless communications: secret keys through multipath[C]. IEEE International Conference on Acoustics, Speech and Signal Processing, Las Vegas, NV, USA, 2008: 3013–3016. doi: 10.1109/ICASSP.2008.4518284.

[9] YE C, REZNIK A, and SHAH Y. Extracting secrecy from jointly Gaussian random variables[C]. IEEE International Symposium on Information Theory, Seattle, WA, USA, 2006: 2593–2597. doi: 10.1109/ISIT.2006.262101.

[10] YE C, REZNIK A, STERNBERG G, *et al*. On the secrecy capabilities of ITU channels[C]. IEEE 66th Vehicular Technology Conference, Baltimore, MD, USA, 2007: 2030–2034. doi: 10.1109/VETECF.2007.426.

[11] LIU H, WANG Y, YANG J, *et al*. Fast and practical secret key extraction by exploiting channel response[C]. IEEE INFOCOM, Turin, Italy, 2013: 3048–3056. doi: 10.1109/INFCOM.2013.6567117.

[12] 吴钊, 张彧, 姜龙, 等. 基于宽带突发单载波频域均衡传输的时域精细信道估计方法[J]. 电子与信息学报, 2016, 38(5): 1166–1172. doi: 10.11999/JEIT150682.
WU Zhao, ZHANG Yu, JIANG Long, *et al*. Time-domain fine channel estimation based on broadband burst single-carrier frequency domain equalization transmission[J]. *Journal of Electronics & Information Technology*, 2016, 38(5): 1166–1172. doi: 10.11999/ JEIT150682.

[13] 乔良, 辛吉荣, 郑辉. 单载波通信系统的迭代频域合成均衡算法[J]. 电子与信息学报, 2015, 37(8): 1950–1956. doi: 10.11999/JEIT141507.
QIAO Liang, XIN Jirong, and ZHENG Hui. Iterative frequency domain combining equalization algorithm for single carrier systems[J]. *Journal of Electronics & Information Technology*, 2015, 37(8): 1950–1956. doi: 10.11999/JEIT 141507.

[14] ASIM M, GHOGHO M, and MCLERNON D. Mitigation of phase noise in single carrier frequency domain equalization systems[C]. IEEE Wireless Communications and Networking Conference, Shanghai, China, 2012: 920–924. doi: 10.1109/WCNC.2012.6214505.

[15] 李晓峰. 随机信号分析[M]. 北京: 电子工业出版社, 2011: 54–60.
LI Xiaofeng. Stochastic Signal Analysis[M]. Beijing: Electronic Industry Press, 2011: 54–60.

[16] LI L and YAO W. A novel timing synchronization for CO-OFDM systems using CAZAC sequences[J]. *Optoelectronics Letters*, 2017, 2(3): 225–228. doi: 10.1007/s11801-017-7017-6.

孔媛媛：　女，1982 年生，博士生，研究方向为无线通信技术.

杨　震：　男，1961 年生，教授，研究方向为通信信号处理.

吕　斌：　男，1989 年生，博士生，研究方向为无线能量通信.

田　峰：　男，1979 年生，副教授，研究方向为通信网络安全.