基于幅度和相位联合分区的无线物理层密钥生成方法

李楠楠[1]，韩瑜[2]，高宁[1]，金石[1]
（1. 东南大学移动通信国家重点实验室，江苏 南京 210096;
2. 新加坡科技设计大学，新加坡 487372）

摘　要：研究基于无线信道物理层特征的密钥生成方法对于提高无线传输的安全性具有重要意义。考虑多径衰落信道下时分双工（time division duplex，TDD）正交频分复用（orthogonal frequency division multiplexing，OFDM）通信系统，利用 OFDM 多载波优势以及信道互易性，联合使用信道频率响应（channel frequency response，CFR）特征的相位与幅度信息，提出了两种应用于无线物理层密钥生成的算法。理论分析和实验仿真表明，提出的算法生成的初始密钥具有更高的一致性和更小的信息协商开销；可以有效增加密钥长度和增强密钥随机性；此外，对于非法用户的窃听以及主动攻击具有较好的防御能力。

关键词：无线通信；正交频分复用系统；物理层密钥生成；安全
中图分类号：TP309
文献标识码：A
doi: 10.11959/j.issn.1000−0801.2021106

Joint amplitude and phase partition based physical layer key generation method

LI Nannan[1], HAN Yu[2], GAO Ning[1], JIN Shi[1]
1. National Mobile Communications Research Laboratory, Southeast University, Nanjing 210096, China
2. Singapore University of Technology and Design, Singapore 487372, Singapore

Abstract: A key generation method based on wireless channel physical layer features is of great significance for improving security of wireless transmission. An orthogonal frequency division multiplexing (OFDM) communication system based on time division duplex (TDD) with multipath fading channels was considered. Utilizing the advantages of OFDM multicarrier and the channel reciprocity and combining the phase and amplitude information of channel frequency response (CFR), two algorithms for physical layer key generation were proposed. Theoretical analysis and experimental simulation show that the proposed algorithm has more consistent and smaller overhead in information negotiation, in addition, the proposed algorithm can increase the key length and enhance randomness, and has a better defense capability against eavesdropping and active attacks of the illegal user.

Key words: wireless communication, OFDM system, physical-layer secret key generation, security

收稿日期：2020−12−28；**修回日期**：2021−03−19
基金项目：国家自然科学基金资助项目（No. 62001109）；中国博士后科学基金资助项目（No.BX20200083）
Foundation Items: The National Natural Science Foundation of China (No.62001109), The China Postdoctoral Science Foundation (No.BX20200083)

1　引言

无线信道的广播特性使得合法用户很容易受非法用户的攻击，如窃听、流量分析、干扰、重放、拒绝服务等[1]。目前，无线传输安全已引起学术界和工业界的广泛关注[2]。传统的加密算法一般是基于计算的复杂度，如基于大数分解的复杂性的RSA公钥加密算法需要假定攻击者的计算能力有限，从而保证非法用户无法在有效时间内获取密钥，但对于资源受限的设备，算法并不适用[3-4]。同时，传统的公钥基础设施需要依赖可靠的第三方机构来分发密钥，但是在复杂动态的移动无线环境中，依靠证书颁发机构或密钥分发中心的密钥分发方式具有较多的局限性[5]。近年来，无线物理层密钥生成技术受到了广泛关注，相比于传统加密算法，物理层密钥生成算法利用无线信道的特性生成密钥，进而保证无线传输的完整性和保密性[6]。物理层密钥生成算法基于时分双工通信系统的信道短时互易性在信道相干时间内通信双方可以通过发送导频信号，获取高度相似的物理层信道特征，并利用该特征进行物理层密钥生成。物理层密钥生成具有以下优势：一是基于物理层信道特征的密钥生成技术可以作为上层加密技术的必要补充，辅助增强无线通信的安全性；二是物理层密钥生成基于信道短时互易性生成双方一致的密钥，不需要额外的密钥分发和密钥管理机制；三是物理层密钥的安全性基于无线信道的时变性和随机性，不依赖于计算复杂度，非常适用于资源受限的设备。研究表明，基于物理层特征的密钥生成方法理论上可实现“一次一密”通信[7]，能保证通信的绝对安全。

无线信道的互易性是物理层密钥生成的基础，由于接收信号强度（received signal strength，RSS）具有很强的互易性且容易被获取，被广泛应用于窄带和宽带通信系统的物理层密钥生成[8]。参考文献[5]提出使用 level-crossing 算法用于密钥生成，但是由于每个数据包只能获得一个 RSS 值，密钥生成速率受到了限制。为了达到更好的密钥生成率，需要考虑信道的细粒度信息。信道状态信息（channel state information，CSI）描述了信道增益矩阵中每个元素的值，参考文献[9]利用信道冲激响应（channel impulse response，CIR）生成密钥，提出一种增加密钥熵的算法。参考文献[6]利用信道频率响应（channel frequency response，CFR）的相位与幅度信息进行密钥生成，并通过实验证明了可以获得比基于 RSS 信息更长的随机密钥比特。

为了提高物理层密钥的长度，同时降低密钥的协商开销，本文考虑多径衰落信道下时分双工（time division duplex，TDD）正交频分复用（orthogonal frequency division multiplexing，OFDM）通信系统，利用 CSI 来做物理层密钥生成，通过联合使用 CFR 的相位与幅度信息，提出了两种用于密钥生成的算法。通过信息泄露情况、密钥长度和随机性 3 项指标对生成密钥的性能进行了分析。通过仿真实验与参考文献[5-6]所提出的密钥生成算法进行了对比，与已有的串联相位与幅度信息的算法[6]相比，本文提出的算法在量化后生成的初始密钥一致性更高，从而信息协同阶段所需要的开销更小。此外，与单独使用相位信息或者幅度信息的算法相比，所提算法可以达到增加密钥长度以及增强随机性的目的，并且可以防御非法用户的窃听以及主动攻击。

2　系统模型

2.1　信道模型

系统模型如图 1 所示，考虑 TDD 条件下多径衰落信道的 OFDM 通信系统系统中 Alice 和 Bob 为合法通信用户，Eve 为非法用户，Alice 和 Bob 通过合法链路进行物理层密钥生成，Eve 对于物理层密钥生成存在潜在的安全威胁。

在通信过程中，Alice 和 Bob 交替传输信息：

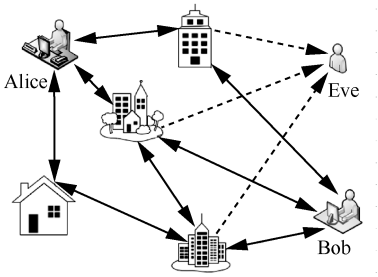


图 1　系统模型

Alice 在时隙 1 发送信道探测信号，Bob 接收信号并存储在本地。Bob 在时隙 2 发送信道探测信号，Alice 收到信号并存储。同时 Eve 在两个时隙中窃听来自 Alice 和 Bob 的信号，并试图对消息进行解密。Alice 和 Bob 的接收信号可以表示为：

$$Y_{\mathrm{A}} = H_{\mathrm{BA}} X_{\mathrm{B}} + N_{\mathrm{B}} \tag{1}$$

$$Y_{\mathrm{B}} = H_{\mathrm{AB}} X_{\mathrm{A}} + N_{\mathrm{A}} \tag{2}$$

其中，X 表示信道探测信号，H 表示信道频率响应，N 表示服从均值为 0、方差为 σ_n^2 的独立同分布的复高斯噪声，Y 表示接收信号，角标 A、B 分别代表 Alice 和 Bob。

在多径环境中，Alice 和 Bob 之间的无线信道会在发送和接收的信号上产生随时间变化的随机映射，该映射是互易的且位置相关的，即 H_{BA} 与 H_{AB} 相同。通过对接收信号做离散傅里叶变换（discrete Fourier transform，DFT），Alice 和 Bob 的离散接收信号可以表示为：

$$Y_{\mathrm{A}}(n_2,k) = H(n_2,k) X_{\mathrm{B}}(n_2,k) + N_{\mathrm{B}}(n_2,k) \tag{3}$$

$$Y_{\mathrm{B}}(n_1,k) = H(n_1,k) X_{\mathrm{A}}(n_1,k) + N_{\mathrm{A}}(n_1,k) \tag{4}$$

其中，$H(n_i,k), i=1,2$ 是第 n_i 个 OFDM 符号上第 k 个子载波的 CFR（$k \in \{0,1,\cdots,K-1\}$）。$X_{\mathrm{A}}(n_1,k)$ 和 $X_{\mathrm{B}}(n_2,k)$ 是归一化的导频信号。$\eta_{\mathrm{A}}(n_2,k)$ 和 $\eta_{\mathrm{B}}(n_1,k)$ 是服从均值为 0、方差为 σ_n^2 的独立同分布的复高斯噪声。

2.2　攻击模型

无线信道的广播特性使其容易遭受窃听、伪造等攻击，当攻击者 Eve 与合法通信方之间的距离大于 $\lambda/2$ 时，攻击者监听到的信道信息与合法用户之间的信道信息不相关[10]。本文考虑在与合法通信用户距离均大于 $\lambda/2$ 的位置处设立窃听攻击者与伪造攻击者。攻击模型如图 2 所示，窃听攻击者 Eve 的接收信号表示为：

$$Y_{\mathrm{AE}} = H_{\mathrm{AE}} X_{\mathrm{A}} + N_{\mathrm{AE}} \tag{5}$$

$$Y_{\mathrm{BE}} = H_{\mathrm{BE}} X_{\mathrm{B}} + N_{\mathrm{BE}} \tag{6}$$

Bob 可接收 Alice 和伪造攻击者 Eve 发来的消息，来自 Eve 的接收信号可表示为：

$$Y_{\mathrm{EB}} = H_{\mathrm{EB}} X_{\mathrm{E}} + N_{\mathrm{EB}} \tag{7}$$

式（5）~式（7）中，X 表示信道探测信号，H 表示信道频率响应，N 表示服从均值为 0、方差为 σ_n^2 的独立同分布的复高斯噪声，Y 表示接收信号。

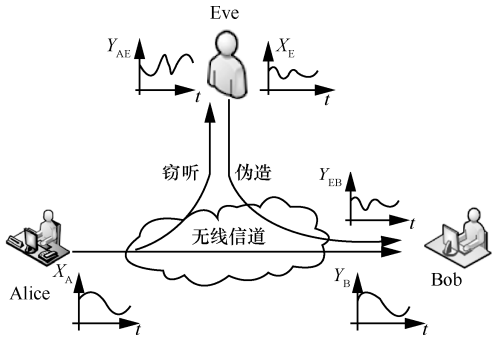


图 2　攻击模型

3　密钥生成流程

物理层密钥生成技术主要包括信道估计、比特量化、信息协同、一致性校验和隐私放大 5 个步骤。

（1）信道估计：Alice 和 Bob 双方相互发送导频探测信号用于获取信道测量值，基于信道的互易性，通信双方可得到高度相关的信道测量值。

（2）比特量化：采用相位和幅度联合分区的方法，将信道测量值量化为 0，1 byte 生成初始密钥 K_{A} 和 K_{B}。其中，算法一首先利用相位信息选择信道估计值，再结合幅度信息生成密钥；算法二首先利用幅度信息选择信道估计值，再结合相

位信息生成密钥。算法的具体流程在第 3.2.1 节和第 3.2.2 节中介绍。

（3）信息协同：由于信道的非同时探测以及信道噪声等因素的影响，通信双方量化后得到的初始密钥 K_{A} 和 K_{B} 通常不完全相同，必须通过信息协同来检测并纠正初始密钥中的不一致问题，最终得到相同的密钥 K'_{A} 和 K'_{B}。信息协同通常使用 Cascade 算法[11]、Winnow 算法[12]或纠错码[13-14]。本文使用 BCH 纠错码对初始密钥进行纠错，具体操作将在第 3.2.3 节中介绍。

（4）一致性校验：Alice 和 Bob 使用相同的哈希函数来生成密钥 K'_{A}、K'_{B} 的哈希值 $H(K'_{\mathrm{A}})$ 和 $H(K'_{\mathrm{B}})$，然后交换哈希值来验证密钥的一致性。如果双方哈希值相同，则表示密钥生成成功；否则密钥生成失败，重用先前的密钥，待下一帧重新开始密钥生成过程。

（5）隐私放大：通过上述步骤 Alice 和 Bob 可得到一致的密钥，最后通过隐私放大消除密钥比特之间的相关性。

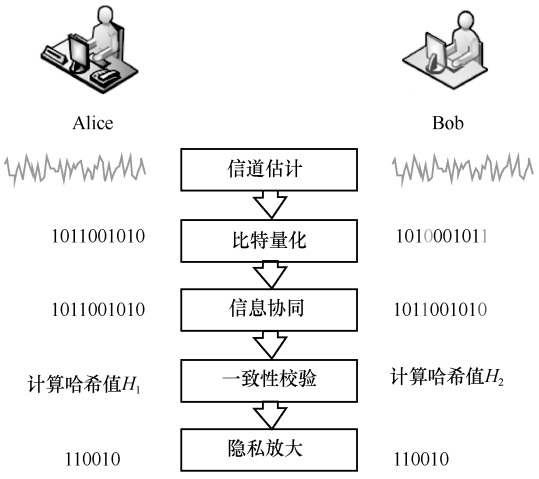


图 3　物理层密钥生成流程

3.1　信道探测及估计

在无线通信中，信道测量值的获取通常要进行信道估计，信道估计分为基于参考信号的估计[15]、盲估计[16]以及半盲估计，本文采用基于参考信号的估计方式。

Alice 和 Bob 相互发送导频探测信号，如图 4 所示，Alice 在某一时刻向 Bob 发送探测信号 1，经过时间 t_1，Bob 接收探测信号 1，接着 Bob 经历 Δt 的收发转换，同时 Alice 经历 Δt 的发收转换；然后，Bob 向 Alice 发送探测信号 2，经过时间 t_2，Alice 接收探测信号，至此完成一次信道的双向探测。假设信道相干时间为 T_c，为了保证双方得到高度相关的探测值，一个探测周期必须满足 $t_1+t_2+\Delta t \leqslant T_{\mathrm{c}}$。

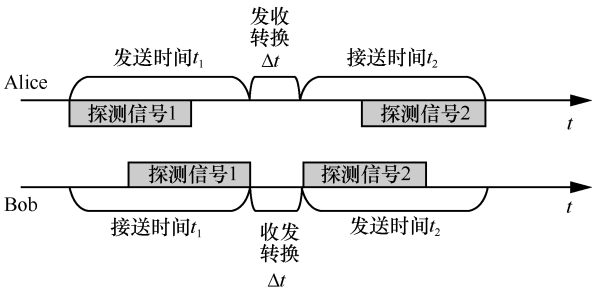


图 4　信道探测时序

在信道探测过程中，假定 Alice 和 Bob 在相干时间内互发探测信号，并利用最小二乘（least-square，LS）估计算法估计得到信道频率响应（CFR），则 Alice 和 Bob 端的 CFR 估计值分别表示为：

$$\hat{H}_{\mathrm{A}}(n_2,k)=H(n_2,k)+E_{\mathrm{A}}(n_2,k) \tag{8}$$

$$\hat{H}_{\mathrm{B}}(n_1,k)=H(n_1,k)+E_{\mathrm{B}}(n_1,k) \tag{9}$$

其中，$E_{\mathrm{B}}(n_1,k)$ 和 $E_{\mathrm{A}}(n_2,k)$ 为估计误差，可将其视为均值为 0、方差为 σ_{E}^2 的独立同分布的复高斯噪声。

3.2　量化

基于通信双方信道探测得到的信道估计值 $\hat{\boldsymbol{H}}_{\mathrm{A}}=[\hat{H}_{\mathrm{A}}(n_2,0),\hat{H}_{\mathrm{A}}(n_2,1),\cdots,\hat{H}_{\mathrm{A}}(n_2,K-1)]^{\mathrm{T}}$，$\hat{\boldsymbol{H}}_{B}=\hat{H}_{\mathrm{B}}(n_1,0),\hat{H}_{\mathrm{B}}(n_1,1),\cdots,\hat{H}_{\mathrm{B}}(n_1,K-1)]^{\mathrm{T}}$，本文采用两种量化算法将信道估计值量化为密钥比特，算法一首先利用相位信息选择信道估计值，再结合幅度信息生成密钥，如图 5 所示；算法二首先用幅度信息选择信道估计值，再结合相位信息生成密钥，如图 6 所示。

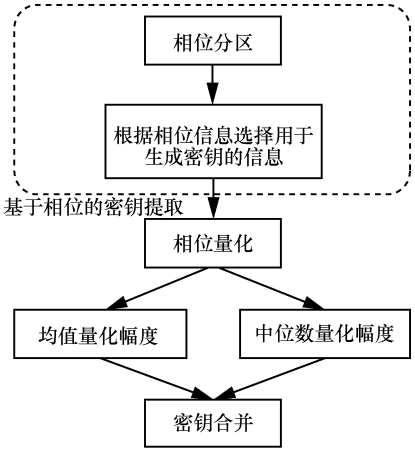


图 5　算法一流程

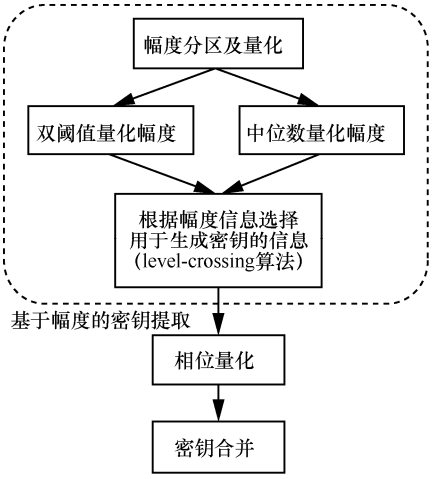


图 6　算法二流程

3.2.1　算法一：相位—幅度联合

（1）基于相位的密钥提取

Alice 和 Bob 利用 CFR 估计值 $\hat{\boldsymbol{H}}_{\mathrm{A}}$ 和 $\hat{\boldsymbol{H}}_{\mathrm{B}}$ 的相位信息，选择用于生成密钥的估计值。首先将相位分为 M 块，如图 7 所示，以 M=8 为例，将整个区域分为 8 份，设置幅度保护阈值 G_A 和相位保护阈值 G_φ。其中，A_i 涵盖相位保护区域（带状区域）和决策域 Z_i（三角形区域）。信道估计值只有落入决策域 Z_i 内，才能被用于生成密钥，落入相位保护区域的信道估计值将会被舍去。相位分区的优点在于：提高密钥生成长度；降低初始量化密钥的不一致率。随后，按照以下 4 个步骤选择用于密钥生成的估计值。

步骤 1　Bob 从 $\hat{\boldsymbol{H}}_{\mathrm{B}}$ 中找到连续 m_1 个位于相同的决策域 Z_i 的值，将该段中间值的位置信息记为 $\rho_{\rho\mathrm{B}}(k)$，并且任意两个中间值的位置距离要大于或等于 B_c，B_c 是相干带宽，即 $\left|p_{p\mathrm{B}}(i)-p_{p\mathrm{B}}(s)\right|\geqslant B_c$，$1\leqslant i,s\leqslant L_{p\mathrm{B}}$，$L_{p\mathrm{B}}$ 是符合条件的总段数。

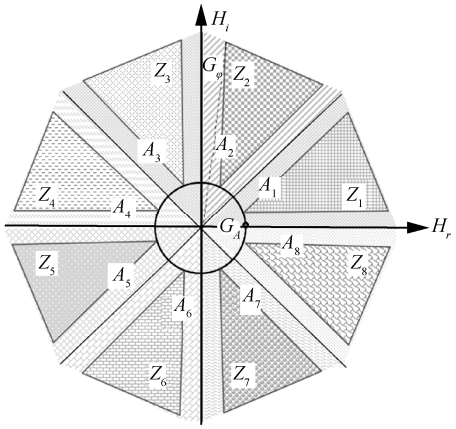


图 7　相位分区

步骤 2　Bob 从 $p_{p\mathrm{B}}$ 中随机选择一个子集 p'_{pB} 将位置索引向量 $p'_{p\mathrm{B}}=[p_{p\mathrm{B}}(1),p_{p\mathrm{B}}(2),\cdots,p_{p\mathrm{B}}(L'_{p\mathrm{B}})]^{\mathrm{T}}$ 发送给 Alice。

步骤 3　根据接收到的 $p'_{p\mathrm{B}}$，Alice 检查 $\hat{\boldsymbol{H}}_{\mathrm{A}}$ 的相应位置处是否存在连续 m_1 个位于相同的决策域 Z_i 的值，若存在则将该位置信息记录在 $p_{p\mathrm{A}}$ 中，若不存在则舍弃该位置信息。$p_{p\mathrm{A}}=[p_{p\mathrm{A}}(1),p_{p\mathrm{A}}(2),\cdots,p_{p\mathrm{A}}(L_{p\mathrm{A}})]^{\mathrm{T}}$，$L_{p\mathrm{A}}$ 是符合条件的总段数。

步骤 4　依据参考文献[5]计算 $L_{p\mathrm{A}}/L'_{p\mathrm{B}}$，若比值小于 0.5+error(0<error<0.5)，则判定存在主动攻击，$p'_{p\mathrm{B}}$ 来自主动攻击者。若比值大于 0.5+error 则判定 $p'_{p\mathrm{B}}$ 来自 Bob。Alice 将 $p_{p\mathrm{A}}$ 发送给 Bob。

值得注意的是，在步骤 2 中，非法用户 Eve 可以冒充 Bob 将虚假索引向量 $p'_{p\mathrm{E}}=[p_{p\mathrm{E}}(1),p_{p\mathrm{E}}(2),\cdots,p_{p\mathrm{E}}(L'_{p\mathrm{E}})]^{\mathrm{T}}$ 发送给 Alice，但由于 Eve 无法获取 $p'_{p\mathrm{B}}$ 的真实信息，只能随机猜测得到 $p'_{p\mathrm{E}}$。此时 Alice 根据 $p'_{p\mathrm{E}}$ 得到 $p_{pA}=[p_{p\mathrm{A}}(1),p_{p\mathrm{A}}(2),\cdots,p_{p\mathrm{A}}(L_{p\mathrm{A}})]^{\mathrm{T}}$。

（2）相位量化

Alice 和 Bob 根据位置索引向量 $p_{p\mathrm{A}}$，对 CFR 估计值 $\hat{\boldsymbol{H}}_{\mathrm{A}}(k)$ 和 $\hat{\boldsymbol{H}}_{B}(k)$ $(k=1,2,\cdots,L_{p\mathrm{A}})$ 的相位进

行量化并生成基于相位的初始密钥 $\boldsymbol{K}_{PA}(k)$ 和 $\boldsymbol{K}_{PB}(k)$ (k =1,2 ,$\cdots, L_{pA}$)，相位信息记为 $\varphi_{A}(k)$ 和 $\varphi_{B}(k)$。根据相位量化阶数 M 的不同，可以将每一位 CFR 估计值量化为 lb$M$ bit 的密钥，例如当 M=4 时，落入 Z_1 区域的估计值被量化为 00，落入 Z_2 区域的估计值被量化为 01，落入 Z_3 区域的估计值被量化为 11，落入 Z_4 区域的估计值被量化为 10。经历以上步骤的生成的初始密钥 $\boldsymbol{K}_{PA}(k)$ 和 $\boldsymbol{K}_{PB}(k)$ 可达到高度一致性，其中可能仅存在少许的比特不一致位，可在后续的信息协同阶段纠正。

$$\boldsymbol{K}_{\mathrm{P}}(k)=\begin{cases}00, \varphi(k)\in Z_1\\ 01, \varphi(k)\in Z_2\\ 11, \varphi(k)\in Z_3\\ 10, \varphi(k)\in Z_4\end{cases} \tag{10}$$

（3）幅度量化

Alice 和 Bob 根据位置索引向量 p_A，计算相应 CFR 估计值 $\hat{\boldsymbol{H}}_{A}(k)$ 和 $\hat{\boldsymbol{H}}_{B}(k)$ (k=1,2,$\cdots, L_{pA}$)的频率幅度响应，设 Alice 和 Bob 幅度响应分别为 $\boldsymbol{M}_{A}(k)$ 和 $\boldsymbol{M}_{B}(k)$ (k =1,2,$\cdots, L_{pA}$)。本文考虑两种幅度量化方法：基于均值的量化方法和基于中位数的量化方法，将幅度响应值量化为二进制比特，生成基于幅度的初始密钥 $\boldsymbol{K}_{MA}(k)$ 和 $\boldsymbol{K}_{MB}(k)$，(k=1,2,$\cdots, L_{pA}$)。基于均值的幅度分区如图 8 所示，基于中位数的幅度分区如图 9 所示。

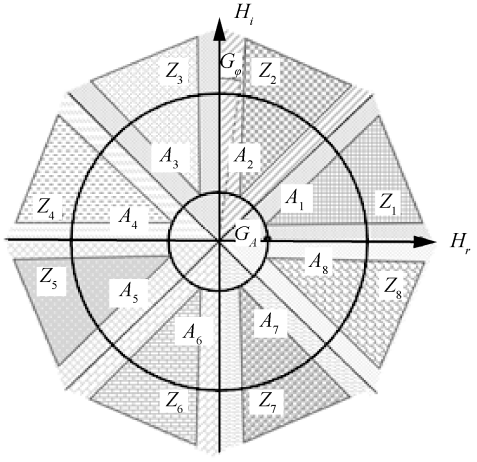


图 8　基于均值的幅度分区

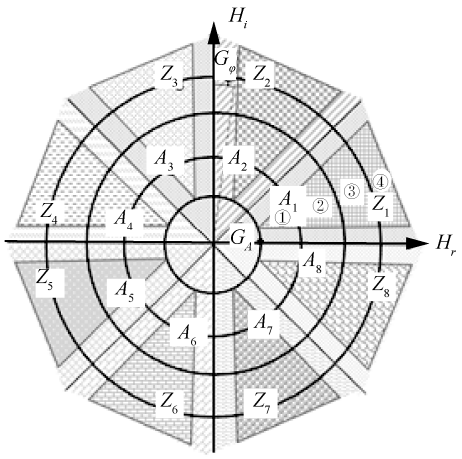


图 9　基于中位数的幅度分区

① 基于均值的量化：

$$\boldsymbol{K}_{\mathrm{M}}(k)=\begin{cases}1, M(k)>\mathrm{mean}\\ 0, G_{\mathrm{A}}<M(k)\leqslant \mathrm{mean}\\ x, \text{其他}\end{cases} \tag{11}$$

其中，G_{A} 是幅度阈值，mean 是幅度响应 $\boldsymbol{M}_{\mathrm{A}}(k)$ 或 $\boldsymbol{M}_{\mathrm{B}}(k)$ 的均值。当 $M(k)>\mathrm{mean}$ 时，$M(k)$ 被量化为 1；当 $G_{\mathrm{A}}<M(k)\leqslant \mathrm{mean}$ 时，$M(k)$ 被量化为 0；当 $M(k)\leqslant G_{\mathrm{A}}$ 时，x 该值被舍弃。

②基于中位数的量化：将幅度响应 $\boldsymbol{M}_{\mathrm{A}}(k)$ 和 $\boldsymbol{M}_{\mathrm{B}}(k)$ 从小到大排序，记前一半为 $\boldsymbol{M}_{\mathrm{FA}}$ 和 $\boldsymbol{M}_{\mathrm{FB}}$，后一半为 $\boldsymbol{M}_{\mathrm{BA}}$ 和 $\boldsymbol{M}_{\mathrm{BB}}$。$\boldsymbol{M}_{\mathrm{F}}$ 的中位数记为 median0，$M(k)$的中位数记为 median1，$\boldsymbol{M}_{\mathrm{B}}$ 的中位数记为 median2。

$$\boldsymbol{K}_{\mathrm{M}}(k)=\begin{cases}00, M(k)<\mathrm{median0}\\ 01, \mathrm{median0}\leqslant M(k)<\mathrm{median1}\\ 11, \mathrm{median1}\leqslant M(k)<\mathrm{median\,2}\\ 10, M(k)\geqslant \mathrm{median2}\end{cases} \tag{12}$$

（4）密钥合并

交叉合并基于相位生成的密钥和基于幅度生成的密钥，最终生成的密钥为：$\boldsymbol{K}(k)=[K_P(k), K_{\mathrm{M}}(k)]$,($k$=1,2$\cdots L_{pA}$)。假设 M=8，CFR 估计值的相位落入 Z_3 决策域（量化为 011），幅度落入图 9 所示区域②被量化为 01，即此 CFR 估计值被量化为 01101。

3.2.2 算法二：幅度—相位联合

（1）基于幅度的密钥提取

CFR 估计值 $\hat{\boldsymbol{H}}_{\mathrm{A}}$ 和 $\hat{\boldsymbol{H}}_{\mathrm{B}}$ 的幅度信息记为 $M_{\mathrm{A}}(k)=[M_{\mathrm{A}}(0),M_{\mathrm{A}}(1),\cdots,M_{\mathrm{A}}(K-1)]$ 和 $M_{\mathrm{B}}(k)=[M_{\mathrm{B}}(0),M_{\mathrm{B}}(1),\cdots,M_{\mathrm{B}}(K-1)]$。首先使用两种量化方法进行幅度分区量化。

① 双阈值量化

$$K_{\mathrm{M}}(k)=\begin{cases}1, M(k)>q_{+}\\ 0, M(k)<q_{-}\\ x, \text{其他}\end{cases} \tag{13}$$

$q_{+}=\mathrm{mean}+a^{*}\sigma$，$q_{-}=\mathrm{mean}-a^{*}\sigma$，其中 mean 是 $\boldsymbol{M}_{\mathrm{A}}(k)$ 或 $\boldsymbol{M}_{\mathrm{B}}(k)$ 的均值，a 是阈值参数，σ 是 $\boldsymbol{M}_{\mathrm{A}}(k)$ 或 $\boldsymbol{M}_{\mathrm{B}}(k)$ 的标准差。双阈值量化幅度如图 10 所示。当 $M(k)>q_{+}$ 时，$M(k)$ 被量化为 1，当 $M(k)<q_{-}$ 时，$M(k)$ 被量化为 0，当 $q_{-}\leqslant M(k)\leqslant q_{+}$ 时该值被舍弃。

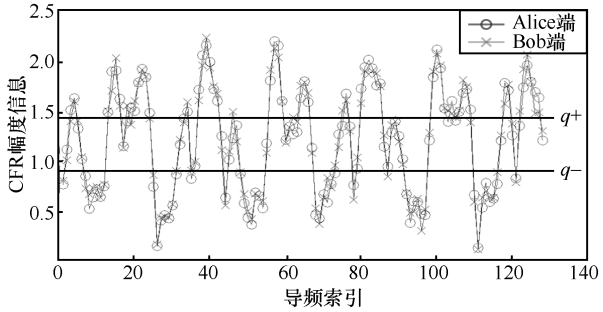


图 10 双阈值量化幅度

② 中位数量化

$$\boldsymbol{K}_{M}(k)=\begin{cases}00, M(k)<\mathrm{median0}\\ 01, \mathrm{median0}\leqslant M(k)<\mathrm{median1}\\ 11, \mathrm{median1}\leqslant M(k)<\mathrm{median2}\\ 10, M(k)\geqslant\mathrm{median2}\end{cases} \tag{14}$$

同样地，幅度分区的优点在于：提高密钥生成长度；降低初始量化密钥的不一致率。中位数量化幅度如图 11 所示。随后，基于量化值使用 level-crossing 算法[5]选出待使用的信道估计值。level-crossing 算法的具体步骤如图 12 所示。

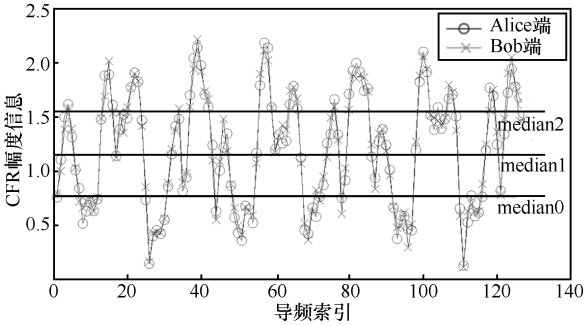


图 11 中位数量化幅度

（2）相位量化

根据 $p_{m\mathrm{A}}$ 对 CFR 估计值的相位信息 $\varphi_{\mathrm{A}}(k)$ 和 $\varphi_{\mathrm{B}}(k)$ 进行量化并生成基于相位的初始密钥 $\boldsymbol{K}_{\mathrm{PA}}(k)$ 和 $\boldsymbol{K}_{\mathrm{PB}}(k)$ (k=1,2,⋯, $L_{m\mathrm{A}}$)。根据相位量化阶数 M 的不同，可以将每一位 CFR 估计值量化为 lb$M$ bit 的密钥。

（3）密钥合并

交叉合并相位生成的密钥和基于幅度生成的密钥。最终生成的密钥为：$\boldsymbol{K}(k)=[K_{\mathrm{M}}(k),K_{\mathrm{P}}(k)]$，$k$=1,2,⋯, $L_{m\mathrm{A}}$。

根据上述分析，算法一与算法二选择信道估计值的时间复杂度是 $O(K)$，在相位量化阶段或幅度量化阶段的时间复杂度分别为 $O(L'_{p\mathrm{B}})$ 或 $O(L_{p'_{m\mathrm{B}}})$，由于 $K\gg L'_{p\mathrm{B}}$ 且 $K\gg L_{p'_{m\mathrm{B}}}$，故算法一与算法二的时间复杂度均为 $O(K)$。由分析可知，所提

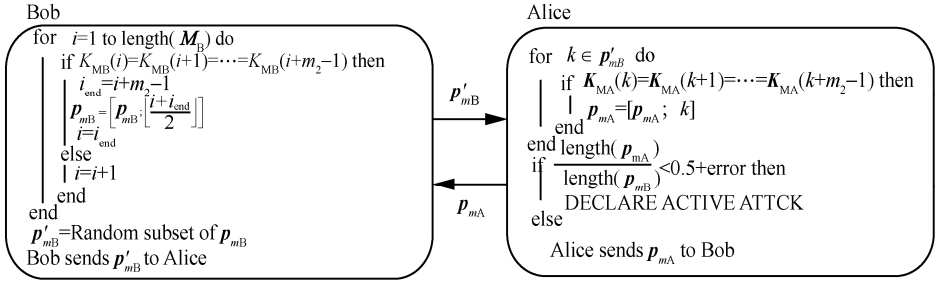


图 12 level-crossing 算法

算法的复杂度随 K 值呈线性增加，算法复杂度较低。

3.3　信息协同

尽管采用信号预处理算法可提高信道测量的互相关性，但量化后 Alice 和 Bob 之间仍然存在潜在的密钥不一致情况。本文使用 BCH 纠错码对 $\boldsymbol{K}(k)$ 进行纠错，BCH(n, k, t)码具有 n 位码字和 k 位信息，可以纠正 t 位错误。BCH 纠错流程如图 13（a）所示：首先 Alice 选择随机数组 r，经过 BCH 编码得到码字 c，然后 Alice 根据异或运算 $s=\mathrm{XOR}(K_{\mathrm{A}},c)$ 计算校验子，再将校验子 s 发送给 Bob，假设 Bob 正确接收 s，Bob 计算码字 $c_{\mathrm{B}}=\mathrm{XOR}(K_{\mathrm{B}},s)$，如果 K_{A} 和 K_{B} 的错误比特数在纠错范围内，则 c_{B} 解码后得到的 c'_{B} 与码字 c 相同。最后经过异或运算 $K'_{\mathrm{B}}=\mathrm{XOR}(c'_{\mathrm{B}},s)$，Alice 得到密钥 K'_{A}，（$K'_{\mathrm{A}}=K_{\mathrm{A}}$），Bob 得到密钥 K'_{B}。图 13（b）以 BCH(7,4,1)码为例说明了纠错过程，其中码字长度为 7 bit，信息位为 3 bit，可以纠正 1 bit 错误。K_{A} 和 K_{B} 有 1 bit 的错误，导致码字 c 和 c_{B} 之间存在 1 bit 的错误，错误 bit 数在 BCH 码的纠错范围之内，所以经过 BCH 解码得到与 c 相同的码字 c'_{B}。

3.4　一致性校验及隐私放大

Alice 和 Bob 使用相同的哈希函数来生成密钥 K'_{A}、K'_{B} 的哈希值 $H(K'_{\mathrm{A}})$ 和 $H(K'_{\mathrm{B}})$，然后交换哈希值来验证密钥的一致性。如果双方哈希值相同，则表示密钥生成成功；否则密钥生成失败，重用先前的密钥，待下一帧重新开始密钥生成过程。

通过上述步骤 Alice 和 Bob 可得到一致的密钥，最后 Alice 和 Bob 按照一定的规则从 K'_{A}、K'_{B} 中选取一部分 bit 作为最终的密钥。通过隐私放大消除密钥比特之间的相关性以及降低信息协调阶段发送校验子可能存在的密钥泄露的风险。

4　性能分析及实验仿真

本节通过 MATLAB 对所提出的基于幅度和相位联合分区的物理层密钥生成算法进行性能分析，仿真采用的 OFDM 系统基于 TDD 的长期演进（long term evolution，LTE）系统，信道模型采用 3GPP Vehicle Type-A 信道模型[17]，主要仿真参数见表 1。

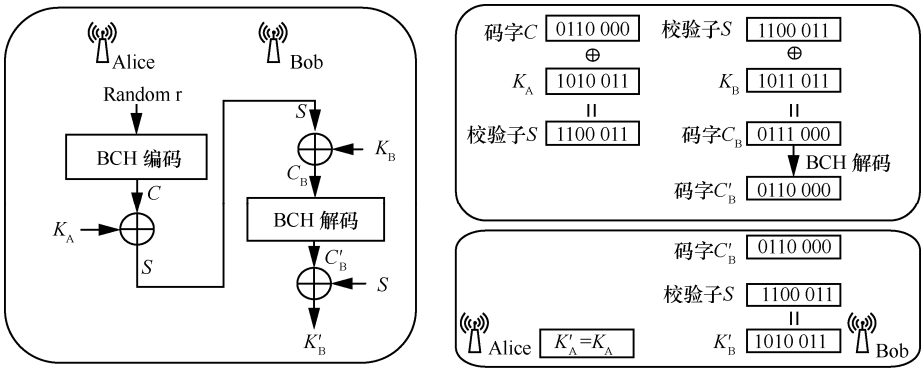
表 1　仿真参数

参数	值
信号带宽	W=10 MHz
采样频率	f_s=19.2 MHz
子载波数	K=1 024
信道模型	时延(ns):0, 310, 710, 1 090, 1 730, 2 510
	增益(dB):0, −1, −9, −10, −15, −20
	多普勒频移: 10 Hz

4.1　安全性分析

（1）窃听攻击

由于 Eve 与 Alice 和 Bob 之间的距离均大于 $\lambda/2$，即窃听信道与合法通信信道的信道特征不相关，Eve 无法通过窃听获取有用信息。



（a）BCH纠错流程　　（b）BCH纠错码示例

图 13　BCH 纠错流程及 BCH 纠错码示例

设 Alice、Bob 和 Eve 对信道的探测分别为 H_{A}、H_{B} 和 H_{E}，那么 Alice 和 Bob 之间的互信息为 $I_{\mathrm{AB}}=I(H_{\mathrm{A}};H_{\mathrm{B}})$；Eve 获取的 Alice 到 Bob 信道探测的互信息为 $I_{\mathrm{AE}}=I(H_{\mathrm{A}}\mid H_{\mathrm{E}})$；Eve 获取 Bob 到 Alice 信道探测的互信息为 $I_{\mathrm{BE}}=I(H_{\mathrm{B}}\mid H_{\mathrm{E}})$；且满足 $I_{\mathrm{AB}}>0$，$I_{\mathrm{AE}}=I_{\mathrm{BE}}=0$。

为了进一步验证上述分析的正确性，以下进行了仿真实验分析。在仿真实验中，假设 Eve 端与合法通信双方采用相同的信道估计方法，得到的物理层信道特征值如图 14 所示。

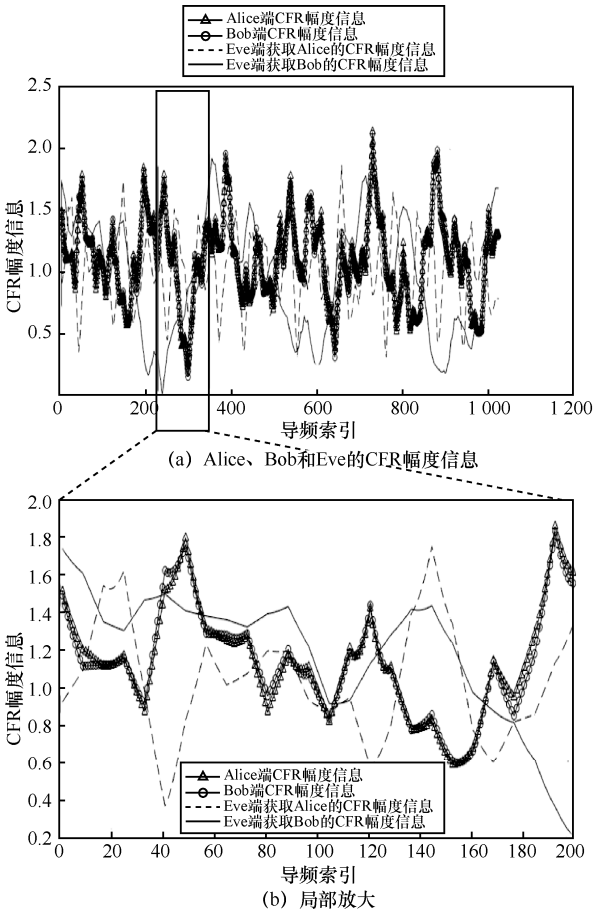


图 14 Alice、Bob 和 Eve 的 CFR 幅度信息及局部放大

从图 14 中可以看出 Alice 和 Bob 得到的信道估计值高度相似，同时 Eve 端得到的信道估计值与合法通信方的信道估计值相关性较弱。

（2）伪造攻击

本文提出的算法可以有效地避免伪造攻击，由上述算法中步骤二可知，Eve 可以冒充 Bob 将随机猜测获得的虚假索引向量 $p'_{p\mathrm{E}}=[p_{p\mathrm{E}}(1),p_{p\mathrm{E}}(2),\cdots,p_{p\mathrm{E}}(L'_{p\mathrm{E}})]^{\mathrm{T}}$ 发送给 Alice，Alice 接收后根据 $p'_{p\mathrm{E}}$ 得到 $p_{p\mathrm{A}}=[p_{p\mathrm{A}}(1),p_{p\mathrm{A}}(2),\cdots,p_{p\mathrm{A}}(L_{p\mathrm{A}})]^{\mathrm{T}}$，由于 $p'_{p\mathrm{E}}$ 没有反映真实的信道特性，根据步骤 4 计算得到的 $L_{p\mathrm{A}}/L'_{p\mathrm{E}}$ 一定小于 0.5+error(0<error<0.5)，故 Alice 将索引向量 $p'_{p\mathrm{E}}$ 判定为伪造攻击，进而中断本轮的物理层密钥生成过程。

4.2 密钥长度分析

对于给定的相位量化阶数 M，算法一的平均密钥长度由式（15）给出：

$$\tilde{L}=L_A\left(\mathrm{lb}M+\mathrm{lb}N\right)\cdot \left[\Pr\left(\left\{\bigcup_{i=1}^{NM}\left(\hat{H}_{\mathrm{A}}(k)\in Z_i,\hat{H}_{\mathrm{B}}(k)\in Z_i\right)\right\}\right)\Pr\left(\left\{\bigcup_{\substack{i,j=1\\ i\neq j}}^{NM}\left(\hat{H}_{\mathrm{A}}(k)\in Z_i,\hat{H}_{\mathrm{B}}(k)\in Z_j\right)\right\}\right)\cdot \mathrm{Pc}\right] \quad (15)$$

其中，L_{A} 是根据相位信息选择的信道估计值的总段数，$\mathrm{lb}M$ 是根据相位信息量化的信息量。N 是幅度的量化阶数，例如使用均值量化时 N=1，使用中位数量化时 N=2。$\Pr\left(\left\{\bigcup_{i=1}^{NM}\left(\hat{H}_{\mathrm{A}}(k)\in Z_i,\hat{H}_{\mathrm{B}}(k)\in Z_i\right)\right\}\right)$ 表示信道估计值 $\hat{H}_{\mathrm{A}}(k)$ 和 $\hat{H}_{\mathrm{B}}(k)$ 落入相同决策域的概率。$\Pr\left(\left\{\bigcup_{\substack{i,j=1\\ i\neq j}}^{NM}\left(\hat{H}_{\mathrm{A}}(k)\in Z_i,\hat{H}_{\mathrm{B}}(k)\in Z_j\right)\right\}\right)\mathrm{Pc}$ 表示 $\hat{H}_{\mathrm{A}}(k)$ 和 $\hat{H}_{\mathrm{B}}(k)$ 落入不同决策域但在信息协同阶段被成功纠错的概率。

算法一的密钥长度的上界为：

$$\tilde{L}<L_{\mathrm{A}}\left(\mathrm{lb}M+\mathrm{lb}N\right)\Pr\left(\left\{\bigcup_{i=1}^{NM}\left(\hat{H}_{\mathrm{A}}(k)\in Z_i\right)\right\}\right)<L_{\mathrm{A}}(\mathrm{lb}M+\mathrm{lb}N)\Pr\left(\left\{\bigcup_{i=1}^{NM}\left(\hat{H}_{\mathrm{A}}(k)\in A_i\right)\right\}\right)<L_{\mathrm{A}}\left(\mathrm{lb}M+\mathrm{lb}N\right)\Pr\left(\left|\hat{H}_{\mathrm{A}}(k)\right|>G_{\mathrm{A}}\right) \quad (16)$$

从式（15）～式（16）可以看出密钥长度与 L_A、相位和幅度的分区数（M 和 N）、估计值落入相同决策域的概率、信息协同阶段成功纠错的概率以及幅度保护阈值 G_A 的选取有关。其中相位和幅度的分区数越大，估计值落入相同决策域的概率越低，同时 L_A 会越小。此外，m_1 和 m_2 的取值也会影响密钥长度，当 m_1 和 m_2 取值过大时，L_A 会减小，但双方估计值落入相同决策域的概率会升高。综上所述，每个参数的选择需要考虑各部分的均衡。

基于上述理论分析，对所提两种算法的密钥长度进行了仿真验证。根据算法一每次信道探测得到的密钥长度的仿真结果如图 15 所示。其中纵轴为每次信道探测生成的密钥长度，单位为 bit/probe，仿真中设置子载波数为 1 024；采样频率为 19.2 MHz；信道模型的时延为 0 ns、310 ns、710 ns、1 090 ns、1 730 ns、2 510 ns；信道增益为 0 dB、−1 dB、−9 dB、−10 dB、−15 dB、−20 dB；多普勒频移 $f_d=10$ Hz。m_1 和 m_2 均设为 6。图 15 中有 3 组曲线，每组曲线由一条仿真曲线和一条理论上界曲线组成。理论上界曲线由式（16）给出。3 组曲线分别为相位与幅度联合，并使用中位

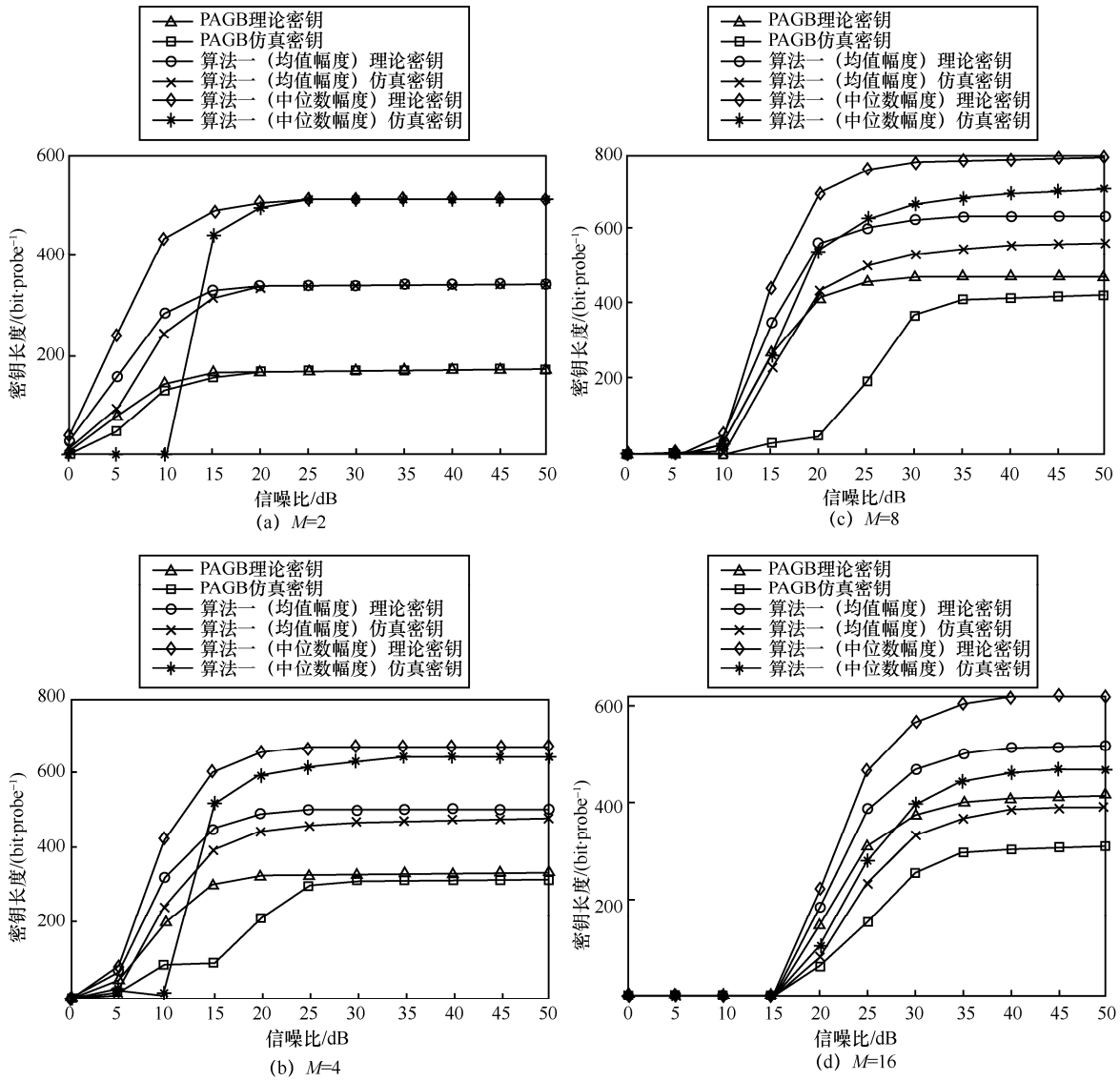


图 15　依据算法一的密钥长度

数量化幅度信息的密钥长度曲线（双划线），相位与幅度联合并使用均值量化幅度信息的密钥长度曲线（虚线），以及单独使用相位信息的密钥长度曲线（实线）。从图 15 中可以看出联合使用相位与幅度信息能增加密钥长度。值得注意的是，利用中位数量化幅度的密钥长度曲线与均值量化幅度的密钥长度曲线存在交点，如图 15（a）所示，当信噪比低于 13 dB 时，使用中位数量化幅度生成的密钥长度曲线低于使用均值量化幅度的密钥长度曲线，这是由于在信噪比相对较低时双方估计值的不一致性较高，使用中位数量化幅度时，幅度被划分得更加精细，信道估计值落入同一量化区域的可能性降低，因此利用均值量化幅度信息得到的密钥长度高于利用中位数量化幅度信息得到的密钥长度。利用中位数量化能将每位信道估计值的幅度信息量化为 2 bit 密钥，而使用均值量化时每位估计值的幅度信息只能被量化成 1 bit 的密钥。当信噪比高于 13 dB 时，通信双方的信道估计值高度一致，此时多比特量化的优势凸显，利用中位数量化幅度信息得到的密钥长度要长于利用均值量化幅度信息得到的密钥长度。为了观察相位量化阶数 M 对生成密钥长度的影响，将 M 分别设置为 2、4、8、16，由图 15 可知，M 取值越小仿真结果与理论上界越紧。随着 M 的增大密钥长度先增大后减小。如图 15（d）所示，当 M=16 时，与 M=2、4、8 的密钥长度相比，M=16 时的密钥长度不增反降，这是因为随着 M 增大，相位信息被划分得更精细，$\hat{\boldsymbol{H}}_{\mathrm{A}}(k)$ 和 $\hat{\boldsymbol{H}}_{\mathrm{B}}(k)$ 落入相同决策域的概率变小，由相位信息选择的信道估计值段数 L_{A} 就会减小，因此随着 M 的增加，密钥长度呈现先增大后变小的趋势。

4 种密钥生成算法对比如图 16 所示，以参考文献[5]提出的 level-crossing（LC）算法和参考文献[6]提出的 PAGB 算法作为基准算法，对本文提出的两种算法进行了性能比较。仿真所设置的参数与算法一的参数一致。从仿真结果可以看出，本文提出的两种算法在密钥长度方面优于 PAGB 算法以及 LC 算法[5]。针对本文提出的两种算法如图 16（a）和图 16（b）所示，当 M=2 或 4 且在信噪比较低时，根据算法二得到的密钥长度高于根据算法一得到的密钥长度，在信噪比较高时算法一的性能优于算法二。此现象说明相位信息受噪声的影响更大，相位估计通常会受到时间和频率偏移的影响而幅度信息更稳定。当 M=16 时，如图 16（d）所示，由算法二生成的密钥长度明显高于使用算法一得到的密钥长度，原因在于算法二是依据幅度信息选择信道估计值。幅度的分区数 N 为 2 或 4 相对较小，信道估计值落入相同量化区域的概率相对较高，因此在信噪比相对较低或 M 较大时，算法二比算法一得到的密钥长度更长。

4.3 随机性分析

美国国家标准技术研究院（The National Institute of Standards and Technology，NIST）随机测试套件被广泛用于评估随机数生成器和伪随机数生成器的随机性。物理层密钥生成得到的随机密钥也可以使用此套件测量随机性。该套件包含 15 个测试，每个测试返回一个 P 值，若 P 值大于 0.01，则判定通过该项测试。为了验证所生成物理层密钥的随机性，对使用不同算法生成的密钥进行了 NIST 随机性测试，测试结果见表 2。表 2 结果表明，根据算法一和算法二生成的密钥通过了随机性测试，联合使用相位和幅度信息生成的密钥，其随机性优于单独使用相位信息生成密钥的随机性，其中使用中位数量化幅度和相位的方法通过的随机性测试指标最多，随机性最好。

5 结束语

基于时分双工信道的短时互易性，本文基于无线信道的频率响应进行了物理层密钥生成的研究，通过相位信息与幅度信息相结合的方式提出了两种量化算法用于物理层密钥生成。同时，对

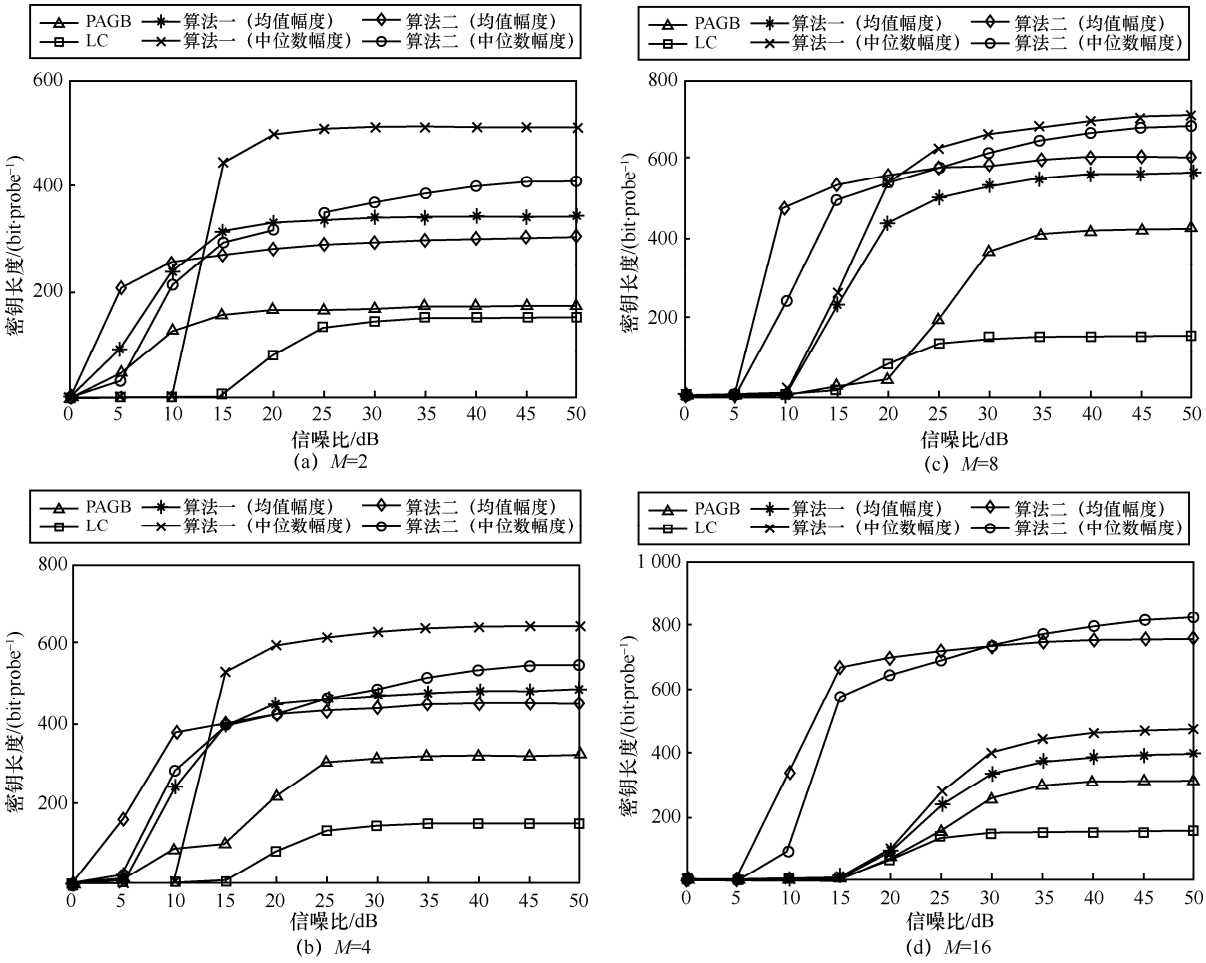


图 16　4 种密钥生成算法对比

表 2　NIST 测试结果

测试项	PAGB	算法一（均值量化幅度）	算法一（中位数量化幅度）	算法二（双阈值量化幅度）	算法二（中位数量化幅度）
Rank	0	0	0.350 485	0.534 146	0.534 146
FFT	0	0	0	0	0.213 309
NonOverlappingTemplate	0	0.534 146	0.739 918	0.911 413	0.911 413
LinearComplexity	0.213 309	0.066 882	0.739 918	0.066 882	0.739 918

所生成物理层密钥的安全性、密钥长度、随机性进行了理论和仿真分析。仿真分析结果表明，与已有的串联相位与幅度信息的算法相比，所提算法在量化后生成的初始密钥具有更高的一致性，在信息协同阶段所需要的开销更小；与单独使用 CSI 的相位信息或幅度信息生成密钥的算法相比，所提算法能增强密钥的随机性和增加密钥的长度。此外，NIST 随机性测试表明，所提算法生成的物理层密钥满足随机性的要求，可以用于无线通信的信息加密和安全无线传输。

本文所提密钥生成算法是基于单天线用户通信场景，在未来 B5G/6G 大规模 MIMO TDD 系统中，在相干时间内完成信道探测将变得极具挑战性[18]，同时基于大规模 MIMO 的复杂动态通信环

境为物理层密钥生成带来了新的机遇，因此，未来计划在大规模 MIMO 场景下，开展单用户及多用户的物理层密钥生成研究工作。

参考文献：

[1] WU B, CHEN J, CARDEI M, et al. A survey of attacks and countermeasures in mobile Ad Hoc networks[J]. Springer, 2007: 103-105.

[2] ZOU Y, JIA Z, WANG X, et al. A survey on wireless security: technical challenges, recent advances, and future trends[J]. Proceedings of the IEEE, 2016, 104(9):1727-1765.

[3] ZHANG J, DUONG T, MARSHALL A, et al. Key generation from wireless channels: a review[J]. IEEE Access, 2017, 4(3):614-626.

[4] 闫富朝, 刘怡良, 韩帅, 等. 空天地通信网络中物理层安全技术综述[J].电信科学, 2020, 36(9):1-13.
YAN F C, LIU Y L, HAN S, et al. A survey of physical layer security in space-air-ground communication and networks[J]. Telecommunications Science, 2020, 36(9):1-13.

[5] MATHUR S, TRAPPE W, MANDAYAM N, et al. Radio-telepathy: extracting a secret key from an unauthenticated wireless channel[C]//Proceedings of the ACM International Conference on Mobile Computing and Networking. New York: ACM Press, 2008:128-139.

[6] PENG Y, 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.

[7] UPADHYAY G, NENE M J. One time pad generation using quantum superposition states[C]//Proceedings of IEEE International Conference on Recent Trends in Electronics Information & Communication Technology (RTEICT). Piscataway: IEEE Press, 2017: 1882-1886.

[8] SUDARSONO A, YULIANA M, KRISTALINA P. A reciprocity approach for shared secret key generation extracted from received signal strength in the wireless networks[C]//Proceedings of International Electronics Symposium on Engineering Technology and Applications. Piscataway: IEEE Press, 2018: 170-175.

[9] LI H, SHEN C, ZHAO Y, et al. High entropy secrecy generation from wireless CIR[J]. Journal of Communications and Networks, 2019, 21(2): 177-191.

[10] LI G, HU A, ZHANG J, et al. High-agreement uncorrelated secret key generation based on principal component analysis preprocessing[J]. IEEE Transactions on Communications, 2018, 66(7): 3022-3034

[11] BRASSARD G, SALVAIL L. Secret-key reconciliation by public discussion[C]//Proceedings of the 1993 Workshop on the Theory and Application of Cryptographic Techniques on Advances in Cryptology. Heidelberg: Springer, 1994: 410-423.

[12] ZHAO F, FU M, WANG F, et al. Error reconciliation for practical quantum cryptography[J]. Optik-International Journal for Light and Electron Optics, 2007, 118(10):502-506.

[13] ZHANG S, JIN L,ZHU S, et al. Information reconciliation based on systematic secure polar code for secret key generation[C]//Proceedings of IEEE 88th Vehicular Technology Conference(VTC-Fall). Piscataway: IEEE Press, 2018:1-6.

[14] EPIPHANIOU G, KARADIMAS P, ISMAIL D K B, et al. Non-reciprocity compensation combined with Turbo codes for secret key generation in vehicular Ad Hoc social IoT networks[J]. IEEE Internet of Things Journal, 2018,5(4): 2496-2505.

[15] SIMEONE O, BAR-NESS Y, SPAGNOLINI U. Pilot-based channel estimation for OFDM systems by tracking the delay-subspace[J]. IEEE Transactions on Wireless Communications, 2004, 3(1):315-325.

[16] SHIN C, HEATH R W, POWERS E J. Blind channel estimation for MIMO-OFDM systems[C]//Proceedings of the IEEE Global Telecommunications Conference. Piscataway: IEEE Press, 2007:670-685.

[17] Guidelines for evaluation of radio transmission technologies for IMT-2000[J]. Rec. ITU-R M.1225, 1997

[18] LI G, SUN C, ZHANG J, et al. Physical layer key generation in 5G and beyond wireless communications: challenges and opportunities[J]. Entropy, 2019, 21(5):1-16.

[作者简介]

李楠楠（1997− ），女，东南大学移动通信国家重点实验室硕士生，主要研究方向为物理层密钥生成等。

韩瑜（1991− ），女，博士，现就职于新加坡科技设计大学，主要研究方向为大规模 MIMO 技术、智能反射面等。

高宁（1989− ），男，博士，东南大学移动通信国家重点实验室助理研究员，主要研究方向为物理层通信安全、无人机集群通信等。

金石（1974− ），男，博士，东南大学移动通信国家重点实验室教授、博士生导师，主要研究方向为 5G/6G 理论与关键技术、物联网理论与关键技术以及机器学习与大数据处理在移动通信中的应用等。