第 21 卷　第 11 期
2023 年 11 月

太赫兹科学与电子信息学报
Journal of Terahertz Science and Electronic Information Technology

Vol.21，No.11
Nov.，2023

文章编号：2095-4980(2023)11-1306-12

基于信道特征高精度提取的空地信道密钥量化

杨　晨，谢顺钦*，邱　睿，李湘鲁，解　楠

(中国工程物理研究院 电子工程研究所，四川 绵阳 621999)

摘　要：针对无人机空地信道，基于空间期望最大化算法(SAGE)对信道特征参数进行高精确度估计。在提取了多径时延、多径功率等空地信道小尺度衰落特征后，利用均匀量化和非均匀量化方法，对实测数据的主径功率、主径-多径功率差开展无线信道密钥量化。分别针对起飞和巡航场景分析了密钥的量化效率、随机性以及算法运行时间等指标，并与基于大尺度特征的密钥量化结果进行比较。密钥量化效率结果表明：基于非均匀量化优于均匀量化；基于信道特征高精确度估计的量化方法优于传统基于大尺度特征的量化；起飞场景下的量化优于巡航场景的量化。密钥随机性测试结果表明本次量化所获得的密钥都具有较好的随机性；算法运行时间结果则表明不同量化方法的运行时间差异较小。因此基于高精确度提取的2种量化方法复杂度较低。

关键词：空地信道；空间期望最大化算法；密钥量化；非均匀间隔；信道测量

中图分类号：TN918.8+2　　**文献标志码：**A　　**doi：**10.11805/TKYDA2021412

Air-to-ground wireless channel key quantization based on high-precision extraction of channel characteristics

YANG Chen，XIE Shunqin*，QIU Rui，LI Xianglu，XIE Nan

(Institute of Electronic Engineering，China Academy of Engineering Physics，Mianyang Sichuan 621999，China)

Abstract: Aiming at the UAV air-ground channel, based on the Space-Alternating Generalized Expectation-maximization(SAGE), the channel characteristic parameters are estimated with high precision, and the small-scale fading characteristics of the air-ground channel such as multipath delay and multipath power are extracted. Then, using uniform quantization and non-uniform quantization methods, the wireless channel key quantization is carried out on the main path power and the main path-multipath power difference of the measured data. The quantification efficiency, randomness, and algorithm running time of the key are analyzed for takeoff and cruise scenarios respectively, and compared with the key quantification results based on large-scale features. The key quantization efficiency results show that the non-uniform guard quantization is superior to the uniform guard quantization; the quantization method based on high-precision estimation of channel characteristics is better than traditional quantization based on large-scale features; and the quantization in the take-off scenario is better than that in the cruise scenario. The results of the performance test show that the keys obtained in these quantizations have good randomness; the running time difference of different quantization methods is small, therefore, the two quantization methods based on high-precision extraction bear low complicity.

Keywords: air-to-ground channel; Space-Alternating Generalized Expectation-maximization; key quantification; non-uniform guard interval; channel measurement

无人机与地面基站是以视距链路为主的空地信道，易遭恶意窃听者攻击，加剧通信安全隐患。因此，保证无人机测控通信安全才能保障无人机的相关应用。无线通信的传统实现方式是基于密码学加密，要求算法足够

收稿日期：2021-12-10；**修回日期：**2022-01-12

基金项目：国家自然科学基金资助项目(62001441)

***通信作者：**谢顺钦　email:suntrain@163.com

复杂且窃听者计算水平有限，使密钥破解时间大于信息本身的有效性。但随着算法效率和计算能力的飞速发展，该方法的安全性受到威胁[1–4]。相比而言，物理层密钥技术利用无线信道固有而独特的随机性、互易性和空间去相关性，通信双方从公共信道提取出仅两方已知的共享密钥，而窃听者因无法经历与合法用户完全相同的信道衰落，难以得到相同密钥。

空地信道特征随着无人机的运动状态而改变。基于无线信道特征的物理层密钥生成技术从该特性出发，采集接收信号的幅度时延等随信道变化的量生成密钥，接收信号强度(Received Signal Strength，RSS)和信道状态信息(Channel State Information，CSI)为常用信道特征。基于RSS生成的密钥可直接用于现成的无线设备，是物理层密钥生成中最广泛的度量。文献[5–7]提出了基于信号RSS特性的物理层密钥生成方案；文献[8]将无线多径信道中的包络和相位作为密钥的随机源；文献[9–10]利用多径间的相对时延生成密钥；文献[11]提出了基于信道频率响应的特征的密钥提取方式。但上述方法都只通过粗略的信道估计，利用基本的信道特征信息，没有利用信道更加精细、高精确度的估计结果。高精确度的量化能够提供更多随机源，也能够提供与窃听信道更多的差异性，在信道密钥的生成速率和安全性方面都更有优势。

本文利用空地无线信道测量实验所采集的数据，针对不同的无人机飞行场景，基于SAGE高精确度估计方法得到空地信道的小尺度衰落估计结果。随后利用估计结果进行信道密钥量化，并对不同场景下几种不同的量化方法进行了比较分析，综合评估了密钥量化的有效性、随机性以及算法复杂度等性能。

1　测量场景与信号

本次测量实验采用某固定翼无人机，地面接收站位于机场跑道旁，海拔高度约为340 m。取2个场景的数据进行分析：第1个是巡航场景，如图1所示，该场景是飞机在2 400 m的海拔高度上往返飞行中的一段；第2个为起飞场景，如图2所示，此时无人机由机场飞至海拔2 000 m高度。2个场景参数如表1所示，表中所指链路距离是本文所取的测量数据所对应时段内无人机与地面站的通信距离。

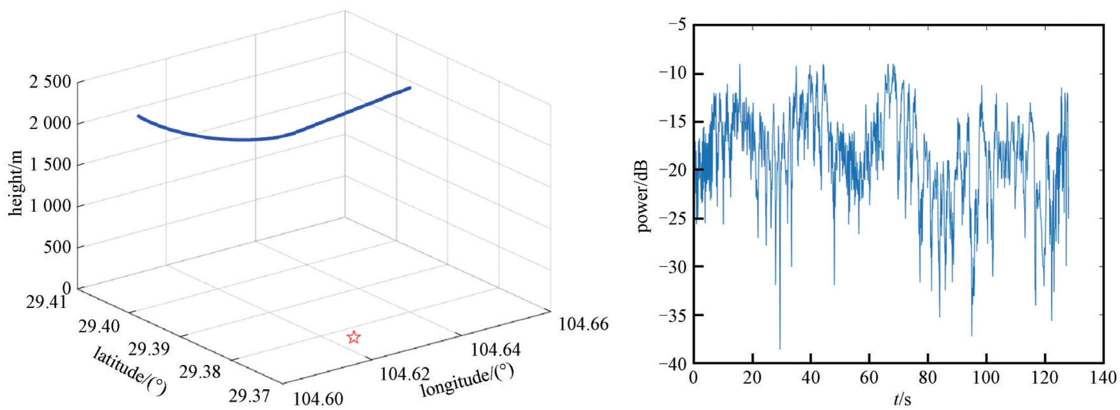

Fig.1 Flight trajectory(left) and received power(right) in cruise scene

图1　巡航场景飞行轨迹(左)与接收功率(右)

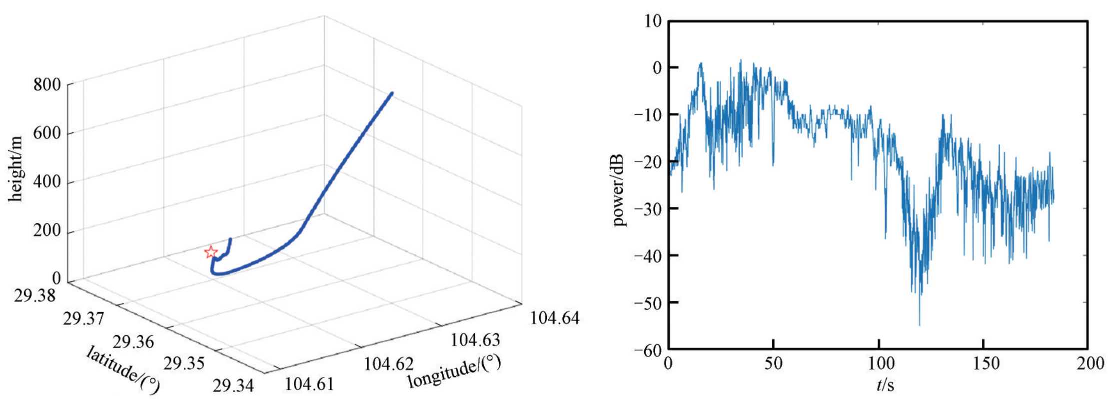

Fig.2 Flight trajectory (left) and received power (right) in the take off scene

图2　起飞场景飞行轨迹(左)与接收功率(右)

表1 各场景参数表

Table1 Parameters of each scenario

scenarios	speed/($m\cdot s^{-1}$)	height/m	link distance/m
cruising	41.94~48.27	2 400	2 537~4 209
take-off	0~47.20	0~2 000	180~3 784

测量试验中机载端发射功率为10 W，发射天线采用全向天线，接收天线为50 dBi的高增益定向天线。测量信号频段28 GHz，共400 MHz带宽，接收端信号采样率2 Gsps。

2 信道特征的高精确度估计

基于信道特征高精确度估计过程主要包括数据分割截取与高精确度特征提取2个阶段。

1) 数据的分割与截取。

通过测量数据和校准数据互相关，获得信道冲击响应，可用式(1)~(2)的复基带模型表示。

$$h(t,\tau)=\sum_{l=1}^{L(t)}\alpha_l(t)\delta(\tau-\tau_l)\exp(\mathrm{j}2\pi\mu_l t) \tag{1}$$

$$P(t,\tau)=E\left[\left|h(t,\tau)\right|^2\right]=E\left[\sum_{l=1}^{L(t)}\left|\alpha_l(t)\right|^2\delta(\tau-\tau_l)\right] \tag{2}$$

式中：τ为当前时间；$L(t)$为t时刻的多径数量；α_l,τ_l,μ_l分别为第l条多径的幅度、时延以及多普勒频率。随后，利用时域分组数据协议(Power Delay Profile，PDP)相关法[12]进行平稳区间估计，进行快拍数据截取。平稳区间由无人机飞行速度所带来的信道状态变化速度决定。根据分析结果，本文取相邻2个快拍之间的间隔为8 ms，每个快拍包含约3 ms采样数据。

2) 基于截取的快拍数据，利用SAGE算法[13]迭代计算，进行参数估计，获得多径分量的幅值、时延及多普勒频率估计[14–15]。

信道估计后，得到了传播路径的时延和幅度，将其作为密钥量化的随机源。采用SAGE算法估计无人机在起飞和巡航场景的信道特征，图3和图4为各场景多径信道的时延功率估计结果(为方便表示路径的相对时延，取直视径时延为0)。图中每个点代表一条多径，其颜色与右侧的相对功率颜色柱对应，表示相对功率大小；其相对主径的偏离程度代表了时延的大小，相对功率即为每个快拍中的多径功率归一化。

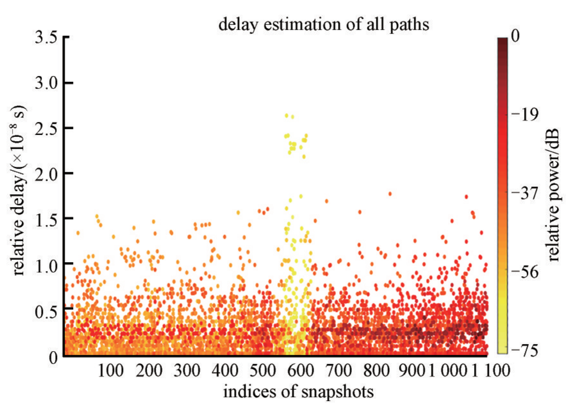

Fig.3 Time delay–power estimation result of cruise scenario

图3 巡航场景时延–功率估计结果

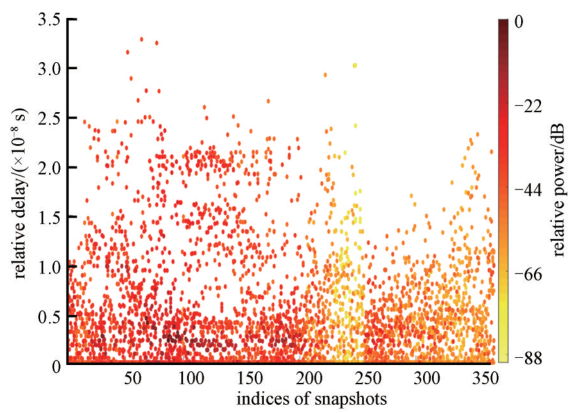

Fig.4 Time delay–power estimation results in take–off scenario

图4 起飞场景时延–功率估计结果

巡航场景无人机周围的散射体很少，因此多径数量也少，且分布较为均匀；起飞场景周围因有较多建筑物和树木等散射体，信号发生较多散射而产生较多多径，且会因散射体的分布使多径分布不均匀。图5和6分别展示了2种场景前3条径的功率变化，不同场景无人机的姿态变化不同，导致产生了不同的阴影衰落。可以看出，起飞场景的多径幅值抖动尤为剧烈，这是因为在起飞阶段，周围散射体较多，多径的分布和动态变化更为丰富；同时，由于距离过近，天线跟踪误差所带来的接收信号功率抖动，促成了多径的幅值变化。此外，由巡航阶段的估计结果也可以看出，本次测量始终存在着一定功率的多径，但是多径的相对时延变化不大，根据测量结果分析，这些多径来自无人机机体或机翼的反射。

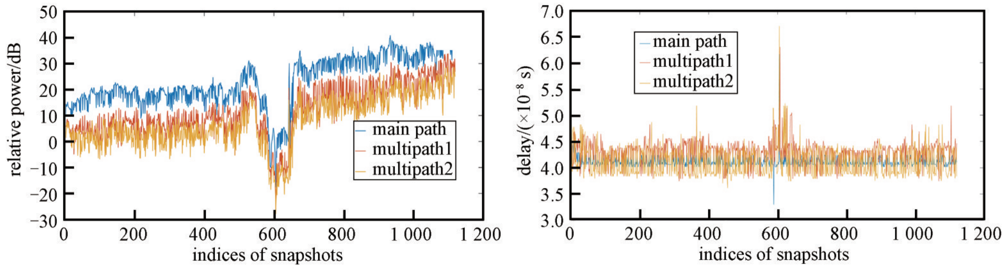

Fig.5 Power curve and multipath delay of the first three paths during cruise

图5　巡航前3条径的功率变化曲线及多径时延

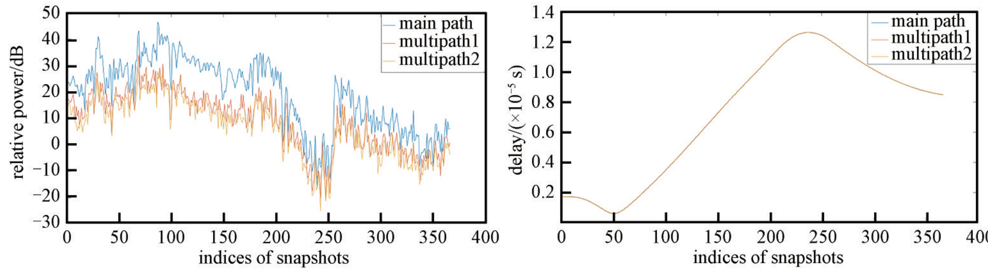

Fig.6 Power curve and multipath delay of the three paths before takeoff

图6　起飞前3条径的功率变化曲线及多径时延

3　基于信道估计结果的密钥量化

3.1　量化方法

基于幅值的密钥量化通常有均匀间隔量化和非均匀间隔量化2种。

3.1.1　多比特均匀量化

$$q_1^{+}(i)=\mu_1^{+}(i)+\alpha\sigma(i) \tag{3}$$

$$q_1^{-}(i)=\mu_1^{+}(i)-\alpha\sigma(i) \tag{4}$$

式中：$q_1^{+}(i)$为上阈值；$q_1^{-}(i)$为下阈值；$\mu(i)$为第i条径的均值；$\sigma(i)$为第i条径的方差；q为量化参数，取值保证各个保护间隔之间不能互相覆盖。对每个量化区间进行m位编码，将幅度区间用0/1 bit依次编码。均匀量化计算所有数据的均值和方差，数据全程采用同种量化条件，处理过程较简单。但对于存在大尺度衰落变化范围较大的情况，会出现量化效率低的问题[16]，此时可通过非均匀量化解决这一问题。

3.1.2　基于柯尔莫可洛夫—斯米洛夫(Kolmogorov–Smirnov，KS)统计检验的多比特非均匀量化

采用KS统计检验方法，将幅值聚为不同的类，假设类的理论分布，并计算每个类的经验累积分布函数(Cumulative Distribution Function，CDF)。将第1个类中的CDF作为参考值，依次比较各类CDF与参考CDF间的最大垂直差，即比较D_{stat}和$D_{\text{stat, critical}}$以检验初始假设的分布是否成立，如式(5)~(6)所示。若$D_{\text{stat}}>D_{\text{stat, critical}}$，说明该类符合初始假设，分布成立；否则，不成立。将符合初始假设分布或相同分布的类划分成一个区间，单独计算每个区间的均值和方差，并将各个区间均匀划分为2^m个量化区域，依据式(3)~(4)计算上下阈值，再对每个量化区域进行m位0/1比特编码，量化得到初始密钥[17−18]。

$$D_{\text{stat}}=\arg\max_{\alpha=\tau,\,\text{amplitude}}\left\{\left|F_n(\alpha)-F'(\alpha)\right|\right\} \tag{5}$$

$$D_{\text{stat, critical}}=T\sqrt{\frac{M_n+M'}{M_nM'}} \tag{6}$$

$$T=\alpha\times\sqrt{(N_1+N_2)/(N_1\times N_2)} \tag{7}$$

式中：α为时延幅度等特征值；F为分布函数；F'为参考分布函数；M_n为第n次估计的路径数；M'为参考路径数；T为临界值；n为当前区间。

具体的量化步骤如下：

1) 确定量化区域的个数2^m，即每个信道测量值的量化位数为$\log_2 2^m$。

2) 量化参数 q 由区间中幅值分布决定，幅值分布较为分散，量化参数取值较大；幅值分布较为密集，量化参数取值较小。

3) 求出量化区域宽度。量化区域以幅值的均值为中心，幅值分布较为分散，增大量化区域间隔；幅值分布较为密集，减小量化区域间隔。

4) 对每个量化区域进行 m 比特编码，即将幅度区间用0/1比特依次编码，再依次将各个幅值按其对应的区域进行编码，以得到密钥。

3.2 实测数据的量化结果

起飞场景含有183 s的数据，以8 ms为间隔，截取持续的45 s数据，其中包含2条多径。巡航场景亦以相同方式提取量化数据。

3.2.1 基于SAGE估计的主径幅度量化

图7和图8为起飞场景下SAGE估计的主径幅度量化过程及其结果，其中图7为均匀量化，图8为非均匀量化。图中由上到下，共分为4个量化区域，依次用0、1、2、3表示该区域内的量化编码结果。在图8所示的时间段内，根据非均匀量化的区间划分原则，共划分为7个动态量化区间，采用字母ABCDEFG对量化区间进行编号，每个区间内的量化阈值根据统计结果进行动态调整。两图的底部均为其量化编码结果。

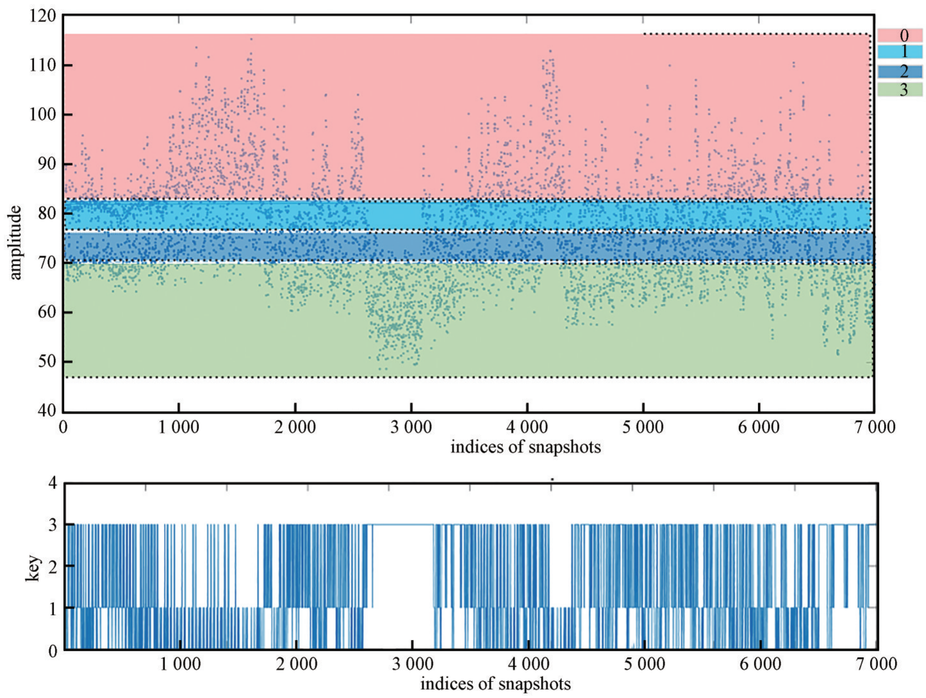

Fig.7 Uniform quantification process and results of the main path of the takeoff scenario

图7 起飞场景主径均匀量化过程及结果

图9~图10为巡航场景下SAGE估计的主径幅值量化过程及其结果，其中图9为均匀量化，图10为非均匀量化(含5个动态量化区间)。

3.2.2 基于SAGE的多径差值量化

除主径外，SAGE估计的其他多径参数也可参与密钥量化。本文选用功率最强的2条多径，利用其幅值差进行量化。这一做法的好处在于，通过多径幅值差值计算，可以将2个径中由于大尺度衰落带来的幅值变化抵消，只利用多径本身的相对幅值进行量化。而多径相对幅值比大尺度衰落信息更难被窃听方预测，因此得到的密钥更具安全性。

图11~图12为起飞场景下基于SAGE的多径差值量化及其结果，图11为均匀量化，图12为非均匀量化过程(含7个动态量化区间)。

图13~图14为高空巡航场景下基于SAGE的多径差值量化及其结果，图13为均匀量化，图14为非均匀量化(含6个动态量化区间)。

3.2.3 大尺度特征量化——接收信号功率的量化

为比较基于高精确度参数估计的密钥量化与传统基于接收信号功率的量化方法之间的差异，对信号接收功

率开展非均匀量化。接收功率表征的是空地信道由于路径损耗、飞机姿态等带来的大尺度衰落特征，这种方法本文称为大尺度特征量化。本次信道测量系统为适应测量信号的动态变化，采用自动增益控制(Automatic Gain Control，AGC)调整AD采样前的信号幅度，因此AGC的结果可以表征信道大尺度衰落的变化。因此可根据AGC实现大尺度量化，本次试验的AGC时间常数为10 ms，与小尺度下的快拍间隔相当。

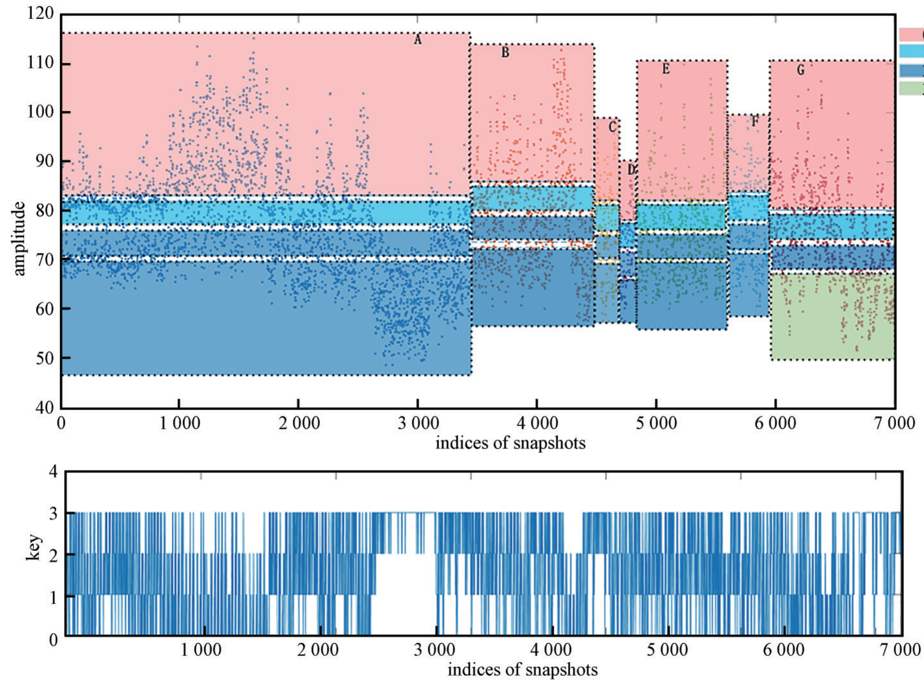

Fig.8 Non-uniform quantification and results of the main path of the takeoff scenario

图8　起飞场景主径非均匀量化及结果

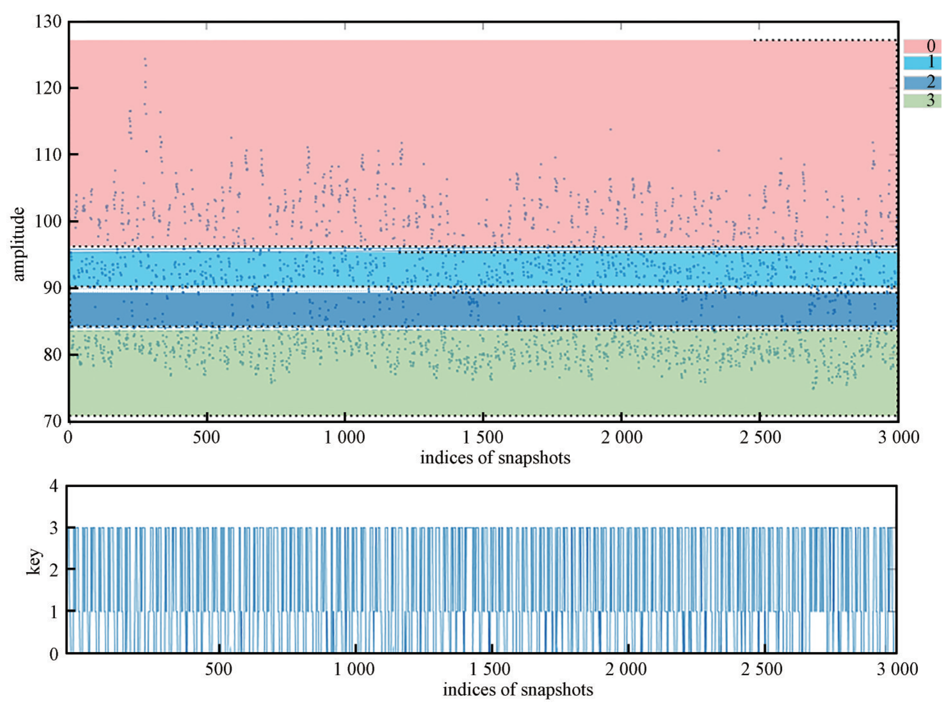

Fig.9 SAGE main path uniform quantification process and results in cruise scenario

图9　巡航场景SAGE主径均匀量化过程及结果

图15和图16分别为起飞和巡航场景下的量化过程和量化结果。由于针对大尺度量化的均匀量化与非均匀量化的结果相当，故此处仅给出非均匀量化结果。可以看出，由于大尺度特征变化相对较缓，出现了长时间连续不变的量化值。

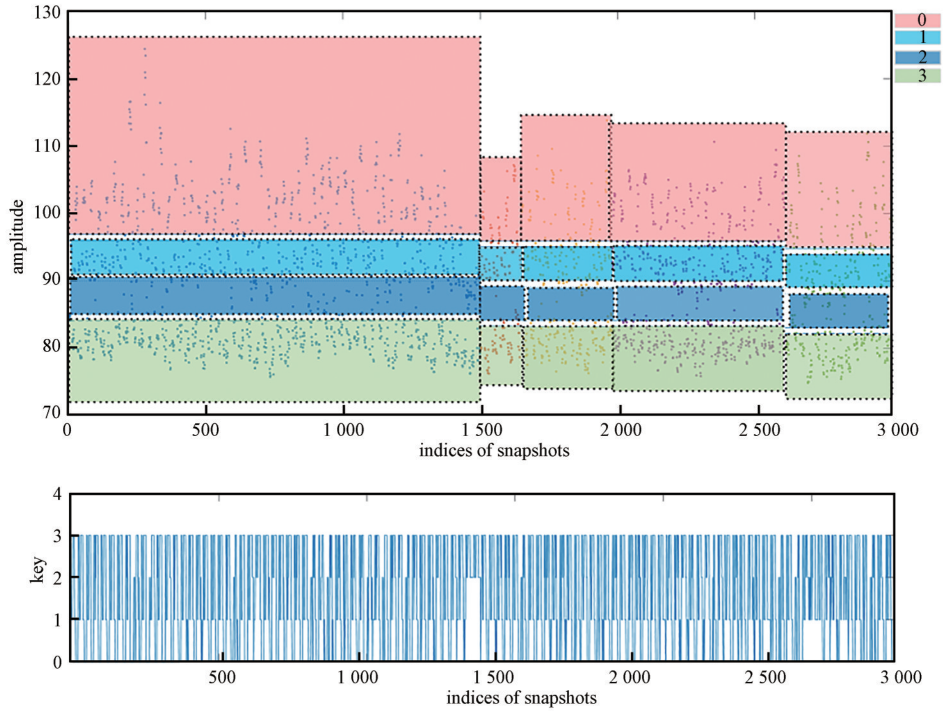

Fig.10 SAGE main path non–uniform quantification process and results in cruise scenario
图10 巡航场景SAGE主径非均匀量化过程及结果

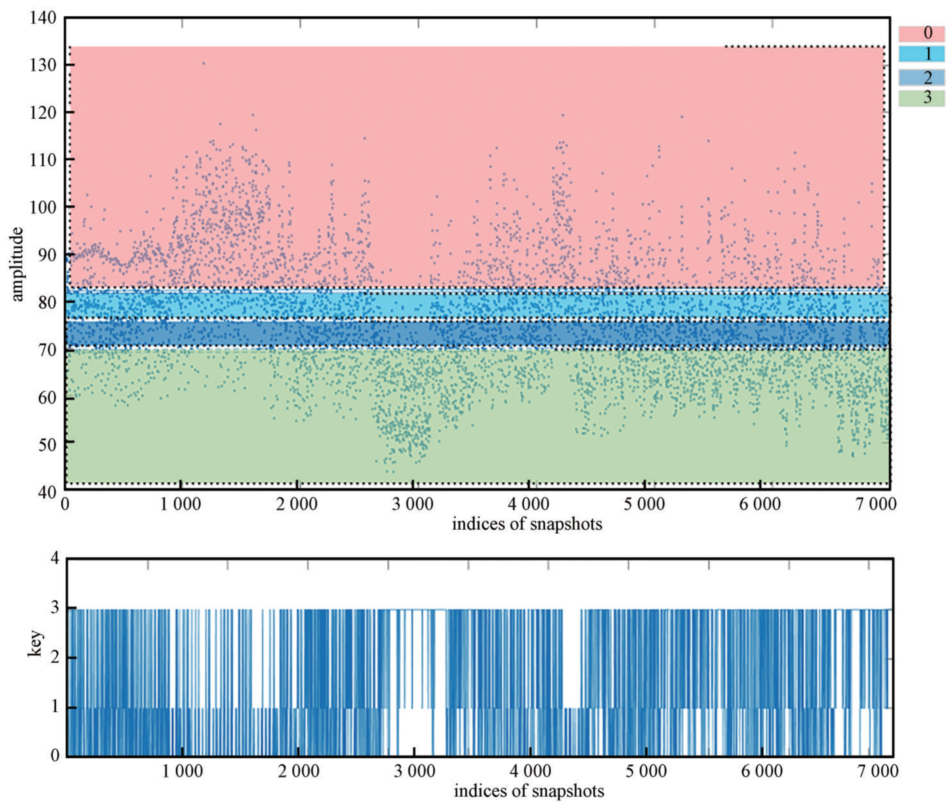

Fig.11 The uniform quantification process and results of SAGE multipath difference in the take–off scenario
图11 起飞场景SAGE多径差值均匀量化过程及结果

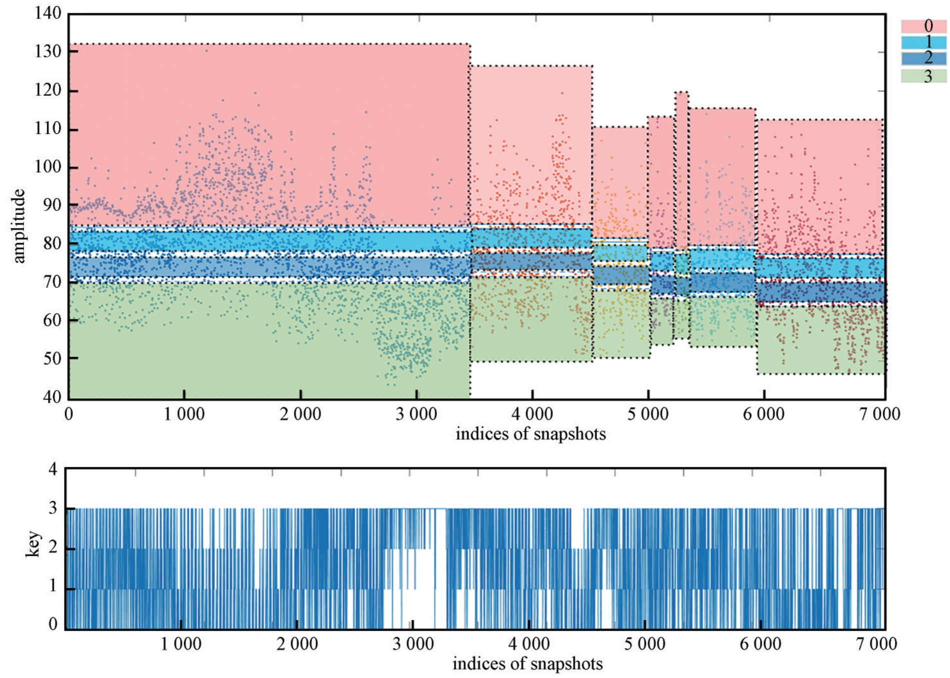

Fig.12 Non-uniform quantification of SAGE multipath difference in take-off scenario
图 12　起飞场景 SAGE 多径差值非均匀量化

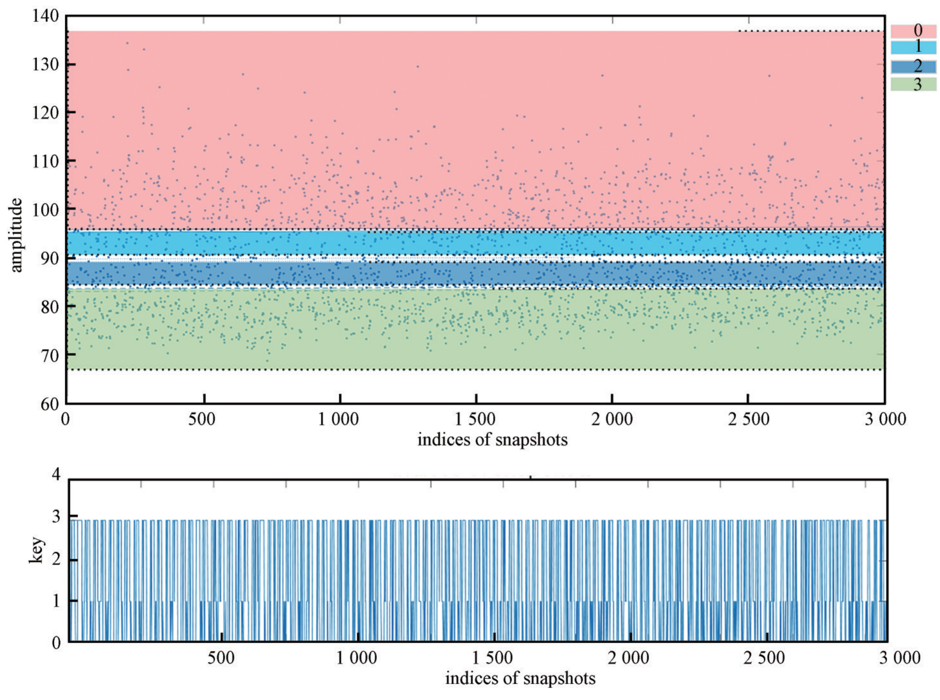

Fig.13 SAGE multipath difference uniform quantization process and results in cruise scenario
图 13　巡航场景 SAGE 多径差值均匀量化过程及结果

4　密钥性能评估

4.1　量化速率

从上述量化过程可以看出，在某些场景或量化方法下，获取的密钥出现了“长连”量化值(连续出现相同的量化值)的情况，显然这种“长连”量化值在密钥生成过程中应尽量避免。为方便对密钥出现非“长连”值的情况进行评价，本文定义了密钥的有效量化效率和有效量化速率。有效量化效率是指对量化得到的所有密钥进行

统计，对出现连续5个及以上的长连0/1/2/3，统计成1个有效值，有效值的个数$N_{cont}<5$与总量化数N_{total_key}之比则为初始密钥的密钥量化效率，即：

$$\eta_{cont<5}=N_{cont<5}/N_{total\_key} \tag{8}$$

有效比特数$N_{cont}<5$与生成密钥所用时间T_{total_key}之比称为有效密钥速率$v_{cont<5}$，即：

$$v_{cont<5}=N_{cont<5}/T_{total\_key} \tag{9}$$

2种场景下的密钥有效率以及有效密钥速率如表2所示。

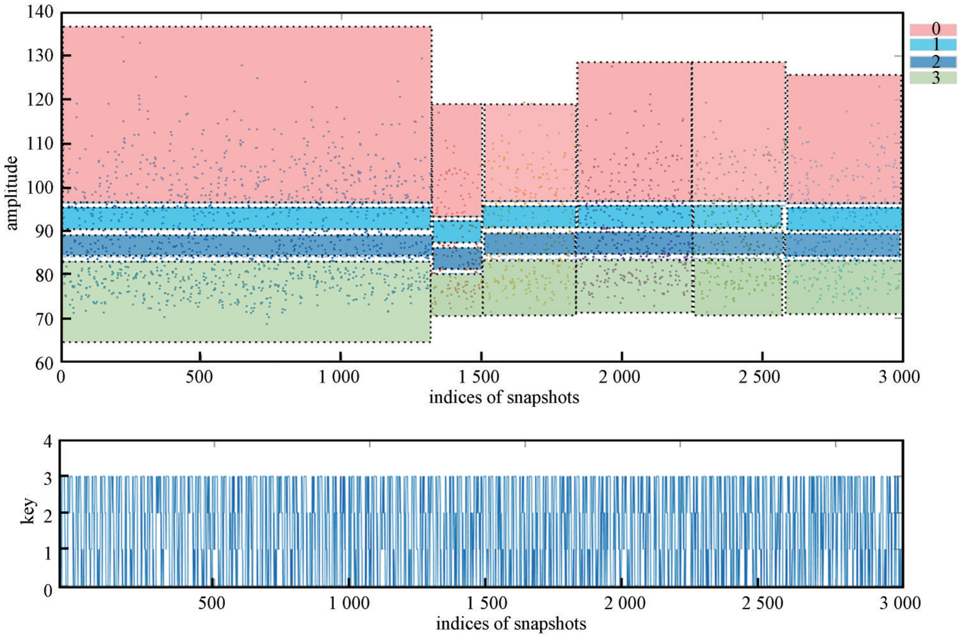

Fig.14 SAGE multipath difference non-uniform quantization process and results in cruise scenario
图14 巡航场景SAGE多径差值非均匀量化过程及结果

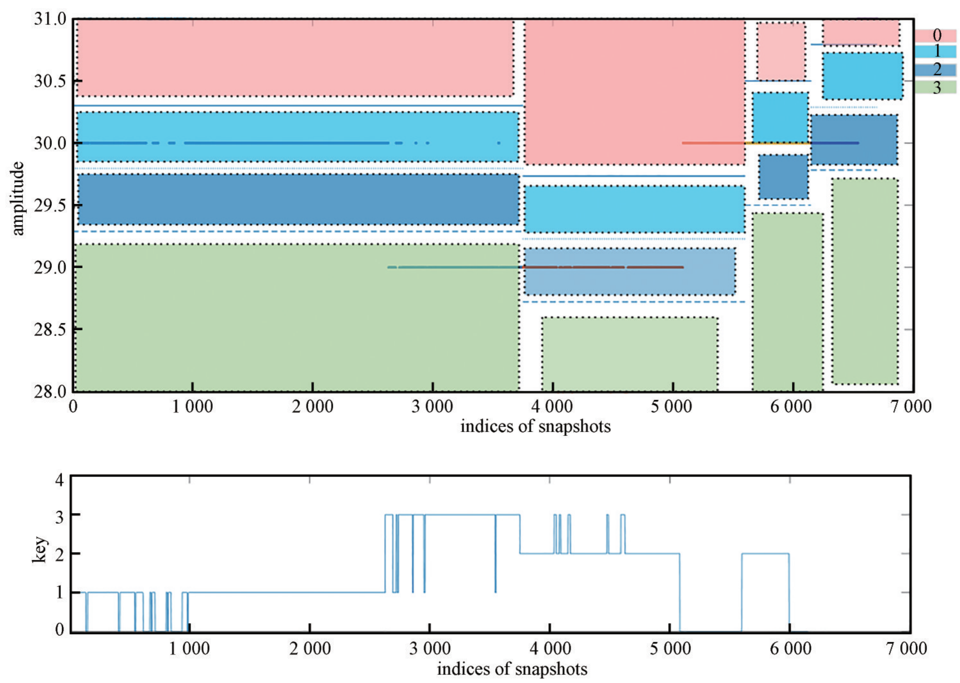

Fig.15 Non-uniform quantification process and results of take-off scenario
图15 起飞场景非均匀量化过程及结果

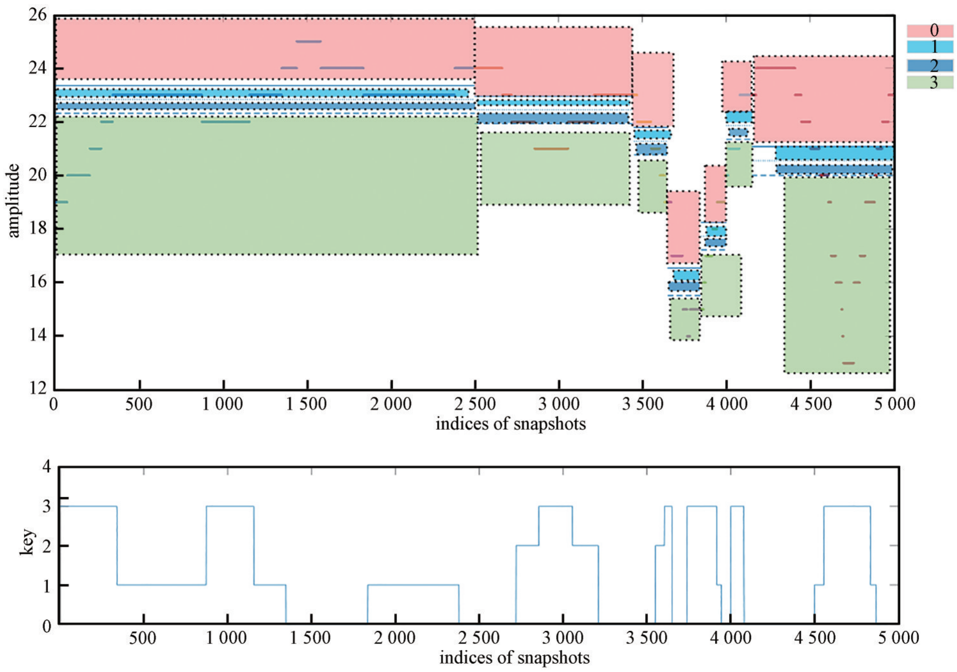

Fig.16 AGC non-uniform quantization process and results in cruise scenario
图16 巡航场景AGC非均匀量化过程及结果

表2 密钥评价指标
Table2 Key evaluation indicators

scenes	quantification method	take-off SAGE	cruise SAGE	take-off difference	cruise difference	take-off large-scale quantification	cruise large-scale quantification
key efficiency	uniform quantization	0.582 7	0.609 5	0.609 6	0.624 4	0.500 4	0.335 5
	non-uniform quantization	0.616 2	0.604 3	0.629 1	0.639 4	0.503 6	0.336 3
effective key rate/(bit·s^{-1})	uniform quantization	83.000 0	53.233 3	75.340 0	56.133 3	45.980 0	37.533 3
	non-uniform quantization	85.311 1	55.033 3	77.260 0	58.700 0	69.020 0	38.750 0

由密钥量化效率可以得出以下4个结论：

1) 非均匀量化优于均匀量化。在起飞和巡航2种场景中，非均匀量化方式的密钥量化效率和有效密钥速率均大于均匀量化方式，这符合非均匀量化的预期。

2) 起飞场景的量化优于巡航量化。从密钥量化效率看，巡航和起飞场景的初始密钥有效性相当；有效密钥速率间的差距是因为起飞场景的信号持续时间长于巡航场景的信号持续时间，使起飞场景用于量化的数据多于巡航场景，且量化得到的密钥位数也多于巡航场景，因而起飞场景的有效密钥速率大于巡航场景的有效密钥速率。

3) 差值量化优于主径量化。在起飞和巡航两种场景中，差值量化的密钥有效率均大于主径量化，是因为多径的相对幅值波动较为明显，量化得到的密钥中长连0/1/2/3出现次数更少。因此，初始密钥中的有效比特数更多，密钥有效率更高。

4) 基于高精确度信道估计的量化方法优于信号接收功率的量化。在起飞和巡航场景中，大尺度量化的密钥量化效率都低于相应场景下的高精确度信道特征的量化结果。尤其在巡航场景中这种优势更加明显。这是由于大尺度量化的幅度变化较小，更易出现长连0/1/2/3，因此大尺度量化得到的密钥的有效性更低。

4.2 密钥随机性

采用美国国家标准与技术研究院(National Institute of Standards and Technology，NIST)随机性测试，其共包含16项指标。该标准按照一定的测试算法，通过对待检测序列与理想随机序列进行偏离程度比较，得到各项指标的P-value作为随机性测试结果。若所有检测项的P-value值大于等于0.01，则待检测序列通过随机性测试。量化使用的信道测量值来自SAGE估计结果，鉴于无线信道的随机性，信道测量值都是随机的。虽然量化过程中对信道测量值进行了删减，但本方法保证了信道测量值落在每一个量化区间的概率都是相同的，生成每个码字都是等概率的(2^m个量化区间使所有的m比特的01序列都能进行编码，即所有的码字中，01出现的概率相同)，从理论

上说，本方法是随机的[19-20]。

3种估计场景中的密钥，先将各自的无效比特剔除后，再将密钥中的0/1/2/3比特分别用00、01、11、10表示，然后利用NIST随机性测试。从表3中可以看出，所有测试项的值都大于0.01，因此，本方法生成的密钥具有随机性。

表3 密钥随机性测试表

Table3 Key randomness test table

NIST test items	take-off SAGE	cruise SAGE	take-off difference	cruise difference
frequency	0.395 0	0.398 6	0.385 9	0.396 2
block frequency	0.375 0	0.246 3	0.843 7	0.406 2
runs	0.301 8	0.300 3	0.307 0	0.303 8
longest run	0.225 1	0.218 6	0.377 3	0.146 6
DFT	0.029 3	0.406 5	0.882 3	0.465 7
linear complexity	0.517 8	0.650 9	0.217 9	0.513 5
	0.484 0	0.743 1	0.759 5	0.223 2
approximate entropy	0.693 1	0.361 1	0.693 1	0.314 7
cumulative sums	0.928 0	0.796 8	0.987 9	0.898 6
	0.523 8	0.987 4	0.865 5	0.883 8

4.3 密钥复杂性

对两种场景的4种量化方式计算了其运行时间，如表4所示。均匀量化因数据处理方式比非均匀量化简单，因此起飞和巡航场景中的均匀量化用时均较短，非均匀量化用时均较长，但二者差异较小，即起飞场景中各量化方法的复杂度相当。巡航场景由于采用的数据量较少，因此其量化算法的时间少于起飞场景，但二者差异较小，因此，2种场景下的量化方法复杂度相当。

表4 算法运行时间

Table4 Algorithm running time

	running time for uniform quantization of the main path/s	running time for non-uniform quantization of the main path/s	running time for uniform quantization of differences/s	running time for non-uniform quantization of differences/s
take-off	0.022 8	0.062 0	0.023 8	0.063 2
cruising	0.021 8	0.049 0	0.023 2	0.055 8

5 结论

本文利用SAGE算法高精确度地分析了基于无人机和地面基站的空地信道的信道特征，采用了KS统计检验方法对幅值依据CDF划分区间，并每个区间单独计算量化的各类参数以实现非均匀间隔量化，与均匀量化比较，得到了无人机在起飞和巡航两种场景下对实测数据的主径功率、主径-多径功率差开展无线信道密钥量化的结果，分析了密钥的量化效率、随机性指标以及算法复杂度，后续任务将会考虑信道的互易性，实现保证密钥一致性且完成安全通信的过程。

参考文献：

[1] DIN F U,LABEAU F. Physical layer security through secure channel estimation[C]// 2018 IEEE the 87th Vehicular Technology Conference(VTC Spring). Porto,Portugal:IEEE, 2018:1-5. doi:10.1109/VTCSpring.2018.8417694.

[2] LIU Ruoheng, TRAPPE W. Securing wireless communications at the physical layer[M]. New York, NY: Springer, 2010. doi: 10.1007/978-1-4419-1385-2.

[3] 王晓敏. 基于无线信道物理层特性的密钥生成方法的研究[D]. 杭州:浙江工业大学, 2019:66. (WANG Xiaomin. Research on key generation method based on physical layer characteristics of wireless channel[D]. Hangzhou, China:Zhejiang University of Technology, 2019:66.) doi:10.27463/d.cnki.gzgyu.2019.000135.

[4] 张永伟. 基于无线信道的物理层加密技术研究[D]. 南京:南京邮电大学, 2020:68. (ZHANG Yongwei. Research on physical layer encryption technology based on wireless channel[D]. Nanjing, China: Nanjing University of Posts and Telecommunications, 2020:68.) doi:10.27251/d.cnki.gnjdc.2020.000306.

[5] 胡晓言,金梁,黄开枝,等. 基于信号传播特性的物理层密钥生成方案[J]. 电子学报, 2019,47(2):483-488. (HU Xiaoyan,JIN Liang, HUANG Kaizhi, et al. Physical layer secret key generation scheme based on signal propagation characteristics[J]. Acta Electronica Sinica, 2019,47(2):483-488.) doi:10.3969/j.issn.0372-2112.2019.02.032.

[6] 李浩男. 基于接收信号强度的无线物理层密钥提取方法研究[D]. 成都:西南交通大学, 2019:67. (LI Haonan. Research on wireless physical layer key generation based on received signal strength[D]. Chengdu, China: Southwest Jiaotong University, 2019:67.) doi:10.27414/d.cnki.gxnju.2019.000846.

[7] 杜文杰. 基于接收信号强度的无线网络自适应密钥提取方法[J]. 中北大学学报(自然科学版), 2021,42(1):44-49,55. (DU Wenjie. An adaptive key extraction method for wireless networks based on received signal strength[J]. Journal of North University of China(Natural Science Edition), 2021,42(1):44-49,55.) doi:10.3969/j.issn.1673-3193.2021.01.008.

[8] 张新蜜,徐明. 基于无线多径信道参数的密钥生成方案[J]. 计算机工程, 2018,44(2):177-181. (ZHANG Xinmi,XU Ming. Key generation scheme based on wireless multipath channel parameter[J]. Computer Engineering, 2018,44(2):177-181.) doi:10.3969/j.issn.1000-3428.2018.02.031.

[9] 陈许星,何遵文,张焱,等. 一种基于信道特征参数的无线通信密钥生成方法[J]. 太赫兹科学与电子信息学报, 2017,15(5):834-840. (CHEN Xuxing, HE Zunwen, ZHANG Yan, et al. A key generation scheme for wireless communication based on channel characteristics[J]. Journal of Terahertz Science and Electronic Information Technology, 2017,15(5):834-840.) doi:10.11805/TKYDA201705.0834.

[10] 李楠楠,韩瑜,高宁,等. 基于幅度和相位联合分区的无线物理层密钥生成方法[J]. 电信科学, 2021,37(5):100-112. (LI Nannan, HAN Yu, GAO Ning, et al. Joint amplitude and phase partition based physical layer key generation method[J]. Telecommunications Science, 2021,37(5):100-112.) doi:10.11959/j.issn.1000-0801.2021106.

[11] 张启星,付敬奇. 基于信道特征提取的物理层安全密钥生成方法[J]. 电子测量与仪器学报, 2019,33(1):16-22. (ZHANG Qixing,FU Jingqi. Physical layer security key generation method based on channel feature extraction[J]. Journal of Electronic Measurement and Instrumentation, 2019,33(1):16-22.) doi:10.13382/j.jemi.B1801725.

[12] MATOLAK D W. Air-ground channels & models:comprehensive review and considerations for unmanned aircraft systems[C]// 2012 IEEE Aerospace Conference. Big Sky,MT,USA:IEEE, 2012:1-17. doi:10.1109/AERO.2012.6187152.

[13] FLEURY B H,TSCHUDIN M,HEDDERGOTT R,et al. Channel parameter estimation in mobile radio environments using the SAGE algorithm[J]. IEEE Journal on Selected Areas in Communications, 1999,17(3):434-450. doi:10.1109/49.753729.

[14] FESSLER J A,HERO A O. Space-alternating generalized expectation-maximization algorithm[J]. IEEE Transactions on Signal Processing, 1994,42(10):2664-2677. doi:10.1109/78.324732.

[15] OUYANG Luxia,YIN Xuefeng. An SAGE algorithm for channel estimation using signal eigenvectors for direction-scan sounding[C]// 2016 IEEE the 27th Annual International Symposium on Personal,Indoor,and Mobile Radio Communications(PIMRC). Valencia, Spain:IEEE, 2016:1-6. doi:10.1109/PIMRC.2016.7794622.

[16] 宋晓青. 无线信道密钥生成方法研究[D]. 西安:西安电子科技大学, 2017:92. (SONG Xiaoqing. Research on key generation method with wireless channel[D]. Xi'an,China:Xidian University, 2017:92.) doi:10.7666/d.D01386021.

[17] TIAN Li, YIN Xuefeng, LU S X. Automatic data segmentation based on statistical hypothesis testing for stochastic channel modeling[C]// The 21st Annual IEEE International Symposium on Personal, Indoor and Mobile Radio Communications. Instanbul:IEEE, 2010:741-745.) doi:10.1109/PIMRC.2010.5671917.

[18] EGHBALI H J. K-S test for detecting changes from landsat imagery data[J]. IEEE Transactions on Systems, Man, and Cybernetics, 1979,9(1):17-23. doi:10.1109/TSMC.1979.4310069.

[19] 徐沛帆. 随机性测试方法实现与应用[D]. 成都:电子科技大学, 2019:110. (XU Peifan. Implementation and application of the methods of randomness test[D]. Chengdu,China:University of Electronic Science and Technology of China, 2019:110.)

[20] 王超,温涛,段冉阳. NIST随机性检测方法研究[J]. 信息技术与网络安全, 2018,37(11):5-8,15. (WANG Chao,WEN Tao,DUAN Ranyang. Research of NIST statistical test[J]. Information Technology and Network Security, 2018,37(11):5-8,15.) doi:10.19358/j.issn.2096-5133.2018.11.002.

作者简介：

杨　晨(1996-)，女，在读硕士研究生，主要研究方向为无线通信物理层安全.email:1552606917@qq.com.

谢顺钦(1987-)，男，博士，副研究员，主要研究方向为遥测新体制、无线信道测量与建模、无线物理层安全传输等.

邱　睿(1998-)，男，硕士，研究实习员，主要研究方向为无线物理层安全传输.

李湘鲁(1983-)，男，博士，研究员，主要研究方向为无线电测控通信、物理层安全等.

解　楠(1975-)，男，博士，研究员，主要研究方向为测控通信、卫星导航.